МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.1720

(09/2003)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Аспекты протокола Интернет – Общая эксплуатация, административное управление и техническое обслуживание

Защитная коммутация для сетей MPLS

Рекомендация МСЭ-Т Y.1720

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТА И СЕТИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Службы, приложения и промежуточные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и именование	Y.500–Y.599
Общая эксплуатация, административное управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Службы и приложения	Y.1100–Y.1199
Архитектура, доступ, сетевые возможности и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Общая эксплуатация, административное управление и техническое обслуживание	**Y.1700–Y.1799**
Начисление платы	Y.1800–Y.1899
СЕТИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ	
Структуры и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: потенциал служб и архитектура служб	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие служб и сетей в NGN	Y.2250–Y.2299
Нумерация, наименование и адресация	Y.2300–Y.2399
Управление сетями	Y.2400–Y.2499
Архитектура и протоколы контроля сети	Y.2500–Y.2599
Безопасность	Y.2700–Y.2799
Обобщенная подвижность	Y.2800–Y.2899

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

Рекомендация МСЭ-Т Y.1720

Защитная коммутация для сетей MPLS

Резюме

В настоящей Рекомендации изложены описания требований и механизмов для реализации методов защитной коммутации 1+1, 1:1, совместно используемой сети пакетов 1+1 в плоскости пользователя в сетях MPLS. Определенный здесь механизм предназначен для поддержки сквозных двухточечных LSP. Формы защитной коммутации для веерных и радиальных многоточечных LSP подлежат дальнейшему изучению. Защитная коммутация m:n также подлежит дальнейшему изучению. Бесконтактная защитная коммутация в настоящей версии Рекомендации не рассматривается.

Источник

Рекомендация МСЭ-Т Y.1720 была утверждена 13-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) согласно процедуре Рекомендации МСЭ-Т A.8 13 сентября 2003 года.

Ключевые слова

Неисправность, отказ, LSP, MPLS, PML, защитная коммутация, PSL, изменение маршрута

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи (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.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет 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 настоящей Рекомендации носит добровольный характер. Однако Рекомендация может содержать определенные обязательные положения (например, по обеспечению возможности взаимодействия или применимости), и в этом случае соблюдение Рекомендации достигается при выполнении всех этих обязательных положений. Слово "должен" и обозначающие долженствование другие выражения, а также их отрицательные эквиваленты используются для выражения требований. Употребление этих слов не означает, что соблюдение Рекомендации требуется от какой-либо стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое осуществление или реализация данной 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 получал извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации данной Рекомендации. Однако те, кто будут 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

Стр.

Рекомендация МСЭ-Т Y.1720

Защитная коммутация для сетей MPLS

1 Область применения

В настоящей Рекомендации изложены описания требований и механизмов для реализации методов защитной коммутации 1+1, 1:1, совместно используемой сети и пакетов 1+1 для плоскости пользователя в сетях MPLS. Определенный здесь механизм предназначен для поддержки сквозных двухточечных LSP. Формы защитной коммутации для веерных и радиальных многоточечных LSP подлежат дальнейшему изучению. Защитная коммутация m:n также подлежит дальнейшему изучению. Бесконтактная защитная коммутация в настоящей версии Рекомендации не рассматривается.

2 Ссылки

Следующие Рекомендации МСЭ-Т и другие документы содержат положения, которые посредством ссылок в настоящем тексте составляют положения настоящей Рекомендации. На время публикации обозначенные издания были в силе. Все Рекомендации и другие документы могут пересматриваться, и ввиду этого пользователям настоящей Рекомендации предлагается изучить возможность применения последнего по времени издания Рекомендаций и других документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в рамках настоящей Рекомендации не придает ему как отдельному документу статус Рекомендации.

[1] Рекомендация МСЭ-Т Y.1710 (2002), *Требования к функциям общей эксплуатации и технического обслуживания для MPLS-сетей.*

[2] Рекомендация МСЭ-Т Y.1711 (2002), *Механизм общей эксплуатации и технического обслуживания MPLS-сетей.*

[3] Рекомендация МСЭ-Т G.805 (2000), *Обобщенная функциональная архитектура транспортных сетей.*

ПРИМЕЧАНИЕ – Существует ограничение применимости архитектуры, указанной в Рекомендации G.805. Она не применима к LDP на основе веерной LSP и для случая, где PHP действует с выходом, не поддерживающим плоскость данных MPLS.

[4] Рекомендация МСЭ-Т G.841 (1998), *Типы и характеристики защитных архитектур сетей SDH.*

[5] Рекомендация МСЭ-Т I.630 (1999), *Защитная коммутация ATM.*

[6] Рекомендация МСЭ-Т M.495 (1988), *Восстановление передачи и распределение направления связи передачи: Терминология и общие принципы.*

[7] Рекомендация МСЭ-Т M.20 (1992), *Концепция технической эксплуатации для сетей электросвязи.*

[8] IETF RFC 3031 (2001), *Архитектура мультипротокольной коммутации на основе меток, Категория: Канал стандартов.*

[9] IETF RFC 3032 (2001), *Кодирование набора маркера MPLS, Категория: Канал стандартов.*

3 Определения

3.1 защита 1+1: Механизм защиты, в котором трафик дублируется в защитном канале (постоянно подключенном). Канал, соединяющий платформы LSR, выполняет переключение трафика между рабочим и защитным каналами.

3.2 защита 1:1: Механизм защиты, в котором трафик передается только по рабочему каналу или защитному каналу. Коммутатор канала LSR выполняет переключение трафика между рабочим и защитным каналами.

3.3 защита совместно используемой сети: Защитная коммутация совместно используемой сети может считаться расширенным вариантом защиты 1:1. Она обеспечивает совместное использование полосы пропускания защитными LSP, которые соответствуют рабочим LSP, находящимся в непересекающихся линиях, узлах или SRG.

3.4 группа общих рисков (SRG): SRG – это группа линий или узлов, которые могут выйти из строя одновременно из-за единичного случая отказа. Например, стекловолокна в кабеле относятся к SRG, потому что единичная поломка кабеля может привести к разрушению всех проходящих по нему стекловолокон.

3.5 пакетная защита 1+1: Подобно защите 1+1, трафик передается по обоим LSP. Уровень пакетов 1+1 позволяет выбрать входящий пакет от одного из двух LSP независимо от того, от какого LSP был получен последний пакет. Таким образом, пакетная защита 1+1 рассматривает оба LSP в качестве рабочих каналов в противоположность обозначению одного LSP как рабочего, а другого – как защитного.

3.6 двунаправленная защитная коммутация: Архитектура защитной коммутации, в которой при однонаправленном отказе оба направления LSP, как пораженное, так и невредимое, переключаются на защиту.

3.7 мост: Действие или функция передачи идентичного трафика по рабочему и защитному LSP.

3.8 неисправность: Прерывание способности LSP передавать пользовательскую или OAM информацию (см. Примечание 1).

3.9 дополнительный трафик: Трафик, который специально помещен в ресурс того же сетевого уровня, что и защитный LSP (но в отдельном LSP, который является параллельным защитному LSP), в предположении того, что при отказе этот (дополнительный) трафик будет отклонен, чтобы освободить канал для защищенного трафика вышедшего из строя рабочего подключения.

3.10 отказ: Прекращение способности LSP передавать пользовательскую или OAM информацию. Отказ может быть вызван сохраняющейся неисправностью (см. Примечание 1).

3.11 принудительная коммутация рабочего LSP: Операция коммутации, инициируемая командой оператора. Коммутация проводится, если отсутствует запрос на коммутацию более высокого приоритета (т. е. LoP).

3.12 время удержания: Время между объявлением ухудшения или сбоя сигнала и инициацией алгоритма защитной коммутации.

3.13 ручная коммутация: Операция коммутации, инициируемая командой оператора. Операция коммутации проводится, если отсутствует запрос на коммутацию равного или более высокого приоритета (т. е. LoP, FS, SF или MS).

3.14 область защиты MPLS: Набор LSR, через который направляется рабочий канал и соответствующий ему защитный канал.

3.15 невозвратная защитная коммутация: Метод защитной коммутации, при котором обратное действие (обратное переключение на рабочий LSP) не предпринимается после восстановления рабочего LSP.

3.16 отсутствие запроса: Состояние, в котором отсутствует какой-либо запрос на защитную коммутацию.

3.17 LSR коммутации канала: LSR, который отвечает за переключение или дублирование трафика между рабочим LSP и защитным LSP.

3.18 LSR слияния каналов: LSR, который отвечает за прием трафика защитного канала и либо направляет трафик назад в рабочий канал, либо, если сам является областью назначения, передает трафик на протоколы более высокого уровня.

3.19 защитный LSP: LSP в пределах области защиты, из которой рабочий трафик принимается в точке выхода области защиты, где отказал рабочий LSP.

3.20 защитная коммутация: Механизм восстановления, в котором защитный LSP или сегменты канала создаются до обнаружения неисправности в рабочем канале. Другими словами, механизм защиты, в котором защитный LSP заранее рассчитан, его пропускная способность задана и защитный LSP предустановлен.

3.21 изменение маршрута: Механизм восстановления, в котором канал восстановления или сегменты канала создаются динамически после обнаружения неисправности в рабочем канале. Другими словами, механизм восстановления, в котором канал восстановления не устанавливается заранее.

3.22 возвратная защитная коммутация: Метод защитной коммутации, в котором предпринимается обратное действие (обратное переключение на рабочий LSP) после восстановления рабочего LSP.

3.23 селектор: Коммутатор, в котором осуществляется выбор – принимать трафик от рабочего LSP или от защитного LSP в точке выхода области защиты, либо коммутатор, в котором осуществляется выбор – отправлять трафик рабочему LSP или защитному LSP в источнике области защиты.

3.24 источник области защиты: Оконечная точка передачи (вход) в LSR коммутации канала области защиты.

3.25 точка выхода области защиты: Оконечная точка выхода в LSR слияния каналов области защиты.

3.26 транспортный объект: Компонент архитектуры, который передает информацию между ее входами и выходами в пределах уровня сети (см. Примечание 2). LSP используется как транспортный объект в сети MPLS.

3.27 однонаправленная защитная коммутация: Архитектура защитной коммутации, в которой при однонаправленном отказе (т. е. отказе, воздействующим только на одно направление передачи) только пострадавшее направление LSP переключается на защиту.

3.28 ожидание восстановления: Автоматически инициируемая команда, которая отдается, когда рабочий LSP выходит из состояния SF. Она используется для поддержания состояния, пока не окончится период ожидания восстановления, если раньше не получен более приоритетный запрос на мост.

3.29 таймер ожидания восстановления: Таймер с перестраиваемой конфигурацией, который используется для задержки возврата к исходному состоянию.

3.30 рабочий LSP: LSP в пределах области защиты, из которого рабочий трафик принимается в точке выхода области защиты при безотказном состоянии в обратном режиме.

ПРИМЕЧАНИЕ 1 - В Рекомендации МСЭ-Т M.20 приводится более общее и подробное определение.

ПРИМЕЧАНИЕ 2 - В Рекомендации МСЭ-Т G.805 приводится более общее и подробное определение.

4 Символы и сокращения

В настоящей Рекомендации используются следующие сокращения:

APS	Автоматическая защитная коммутация
BDI	Обратная индикация неисправности
CV Packet	Пакет проверки наличия соединения
FDI	Прямая индикация неисправности
FFD Packet	Пакет оперативного обнаружения неисправности
FS	Принудительная коммутация
LDP	Протокол распределения меток
LOCV	Проверка потери связности
LoP	Блокировка защиты
LSP	Канал коммутации по метке

LSR	Коммутатор-маршрутизатор
MPLS	Многопротокольная коммутация на основе меток
MS	Ручная коммутация
OAM	Общая эксплуатация, административное управление и техническое обслуживание
PHP	Предпоследний произведенный переход
PML	LSR слияния каналов
PS	Защитная коммутация
PSL	LSR коммутации канала
SDH	Синхронная цифровая иерархия
SF	Потеря сигнала
SLA	Соглашение об уровне обслуживания
TTSI	Идентификатор источника завершения трассы

5 Требования

Методы повышения надежности работы сети посредством обеспечения возможности восстановления работоспособности после прерывания обслуживания (например, из-за неисправностей), определяются как методы живучести. К методам живучести относятся защитная коммутация и изменение маршрута передачи. В настоящей Рекомендации рассматриваются конкретные методы защитной коммутации. В настоящей Рекомендации различие между защитной коммутацией и изменением маршрута передачи определено следующим образом:

- Защитная коммутация: Подразумевается, что как маршрутизация, так и ресурсы заранее рассчитываются и распределяются выделенному защитному LSP до момента отказа. Ввиду этого защитная коммутация дает надежную гарантию возможности вновь получить требуемые сетевые ресурсы после отказа.
- Изменение маршрута передачи: Подразумевается, что выделенный защитный LSP не определен, поэтому ни маршрутизация, ни ресурсы не рассчитываются и не распределяются до момента отказа. Термин "изменение маршрута передачи" обычно применяется к случаям, когда используются функции маршрутизации и сигнализации и когда "запрос на восстановление соединения" должен быть подан при отказе (сетью или пользователем), и этот "запрос на восстановление соединения" должен конкурировать с другими аналогичными типами трафика в отношении получения требуемого ресурса. Поэтому изменение маршрута передачи не дает гарантии возможности вновь получить требуемый сетевой ресурс после отказа, и обычно этот метод медленнее, чем защитная коммутация.

Защитная коммутация необходима для быстрого восстановления после отказа и таким образом улучшает надежность и готовность к работе сетей MPLS. Для защитной коммутации требуются следующие характеристики:

1) Защитная коммутация должна применяться ко всему LSP.
2) Приоритизированная защита между сигналом отказа (SF) и запросами оператора на коммутацию (см. Таблицу 1).
3) Необходимо обеспечить возможность защиты на MPLS уровне максимально оперативно (в зависимости от временно́й разрешающей способности детектора обнаружения неисправности).
4) Коэффициент защиты равен 100%, т. е. 100% рабочего трафика, которому может быть причинен ущерб, защищено от отказа в одном работающем LSP.
5) При возможности должна поддерживаться дополнительная пропускная способность.

6 Принципы

Защитная коммутация – это полностью распределенный механизм защиты, который может использоваться при любой топологии. Она полностью распределена в том смысле, что направление связи и полоса пропускания защитного LSP зарезервированы для выбранного рабочего LSP. Однако чтобы эффективно противостоять всем возможным отказам рабочего LSP, защитный LSP должен заведомо обладать полным физическим разнесением во всех режимах типичных отказов. Это может быть не всегда осуществимо. К тому же для этого могло бы потребоваться, чтобы рабочий LSP не следовал по самому короткому маршруту.

Архитектура MPLS PS может быть типа 1+1, 1:1, совместно используемой сети или пакетного 1+1. Другие типы подлежат дальнейшему изучению.

В архитектуре типа 1+1 для каждого рабочего LSP выделяется защитный LSP, причем рабочий LSP присоединяется к защитному LSP в источнике области защиты. Трафик в рабочем и защитном LSP передается одновременно к точке выхода области защиты, где делается выбор между рабочим и защитным LSP на основе некоторых заданных критериев, таких как индикация неисправности.

В архитектуре типа 1:1 для каждого рабочего LSP выделен защитный LSP. Рабочий трафик передается рабочим или защитным LSP. Метод выбора между рабочим и защитным LSP зависит от механизма. Защитный LSP может использоваться для пропуска "дополнительного трафика", когда он не используется для передачи рабочего трафика.

В архитектуре типа совместно используемой сети возможное совместное использование ресурса защиты при отказах непересекающихся линий, узла или SRG в сети достигается при гарантии восстановления от единичного отказа. Для каждого соединения в сети отслеживаются все рабочие каналы, чей трафик будет переключен после данного отказа. Благодаря отслеживанию требуется лишь резервировать максимум ресурса защиты для защиты от единичного отказа в сети.

В архитектуре пакетного типа 1+1 трафик передается одновременно по двум возможно независимо маршрутизированным LSP к точке выхода области защиты. Каждой паре дублируемых передающихся пакетов назначается один идентификатор (порядковый номер), но отличный от других пар дублируемых пакетов. В точке выхода области защиты механизм выбора уровня пакета используется для выбора одного из двух возможно полученных экземпляров каждого пакета. В нижеприведенном списке перечислены принципы защитной архитектуры MPLS и разработки механизмов выбора.

1) Неисправности на уровнях выше MPLS не должны вызывать защитную коммутацию уровня сервера. Например, в случае использования ATM в MPLS неисправности на уровне ATM не должны вызывать защитную коммутацию MPLS.
2) В общем случае, если механизмы защиты нижнего уровня (например, СЦИ или оптического) используются в совокупности с механизмами защиты уровня MPLS, то нижние уровни должны иметь шанс восстановления рабочего трафика, прежде чем уровень MPLS инициирует действия защиты (например, используя десинхронизирующий таймер). Цель здесь состоит в том, чтобы избежать дублирования защитной коммутации в сетях различных уровней.
3) Действия защитной коммутации в одной области защиты не должны отрицательно влиять на сетевые операции, показатели деятельности и защитную коммутацию в других областях.
4) Механизм защитной коммутации должен способствовать оперативному восстановлению рабочего трафика для сведения к минимуму перебоя в работе сети, и в идеальном случае восстановление должно быть обеспечено до того, как будет достигнут порог недоступности входа.

7 Механизмы

В данном разделе описываются механизмы однонаправленной и двунаправленной защитной коммутации.

7.1 Однонаправленная защитная коммутация

7.1.1 Прикладные архитектуры

7.1.1.1 Прикладная архитектура однонаправленной защитной коммутации 1+1

Архитектура линейной защитной коммутации 1+1 показана на Рисунке 1. В случае описываемой в данном разделе операции однонаправленной защитной коммутации защитная коммутация выполняется селектором в точке выхода области защиты только на основе локальной (т. е. в защитной точке выхода) информации. Рабочий трафик постоянно соединен с рабочим и защитным LSP в источнике области защиты. Если для обнаружения неисправностей рабочего или защитного LSP используется CV-пакеты, FFD-пакеты или другие пакеты проверки безобрывности, они вставляются в источник области защиты как с рабочей, так и с защитной стороны, а обнаруживаются и извлекаются в точке выхода области защиты. Следует отметить, что их необходимо посылать независимо от того, выбран ли LSP селектором.

Например, если однонаправленная неисправность (в направлении передачи от PSL к PML) происходит в рабочем LSP, как показано на Рисунке 2, то эта неисправность будет обнаружена в точке выхода области защиты в PML, а селектор в PML переключится на защитный LSP.

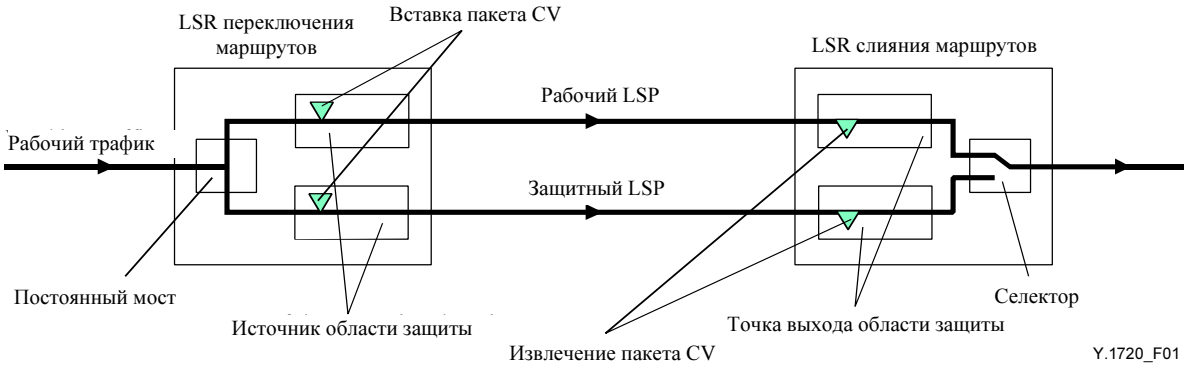

Рисунок 1/Y.1720 – Архитектура однонаправленной защитной коммутации 1+1

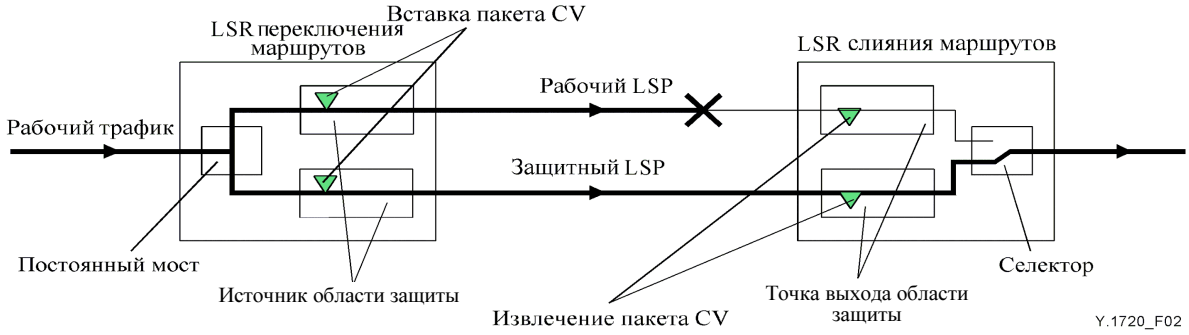

Рисунок 2/Y.1720 – Архитектура однонаправленной защитной коммутации 1+1 – отказ рабочего LSP

7.1.1.2 Прикладная архитектура однонаправленной защитной коммутации 1:1

Архитектура линейной защитной коммутации 1:1 показана на Рисунке 3. В случае операции однонаправленной защитной коммутации, описываемой в данном разделе, защитная коммутация выполняется селектором в источнике области защиты только на основе локальной (т. е. в источнике защиты) информации. Рабочий и защитный трафик постоянно соединены в точке выхода области защиты.

Если для обнаружения неисправностей рабочего или защитного LSP используютсяCV-пакеты, FFD-пакеты или другие пакеты проверки безобрывности, они вставляются в источник области защиты как с рабочей, так и с защитной стороны, а обнаруживаются и извлекаются в точке выхода области защиты. Следует отметить, что их необходимо посылать независимо от того, выбран ли LSP селектором.

Например, если однонаправленная неисправность (в направлении передачи от PSL к PML) происходит в рабочем LSP, как показано на Рисунке 4, эта неисправность будет обнаружена в точке выхода области защиты в PML, а затем будет сообщена посредством BDI источнику области защиты в PSL. По приеме такого сообщения селектор в PSL переключится на защитный LSP.

ПРИМЕЧАНИЕ – dTTSI_Mismerge не может быть защищен защитной коммутацией 1:1.

Когда сообщение SF для рабочего LSP объявлено и трафик пользователя передается по защитному LSP, пакет FDI и трафик пользователя могут быть объединены в точке выхода области защиты. Последующие узлы сети по ходу трафика могут принимать пакеты FDI, CV или FFD и трафик пользователя одновременно. Так же дело обстоит, когда объявляется сообщение SF для защитного LSP. Один из способов решения данной проблемы состоит в том, чтобы использовать селектор слияния. Работа селектора слияния при обнаружении неисправности в рабочем LSP заключается в следующем:

1) Принять пакеты FDI или обнаружить неисправность нижнего уровня на выходе рабочего LSP.
2) Переключить селектор слияния на выходе (т. е. подключиться к рабочему LSP и отключиться от защитного LSP).
3) Послать BDI-пакеты по рабочему LSP.
4) Переключить селектор на входе (т. е. подключить рабочий LSP к защитному LSP и отключить дополнительный трафик).

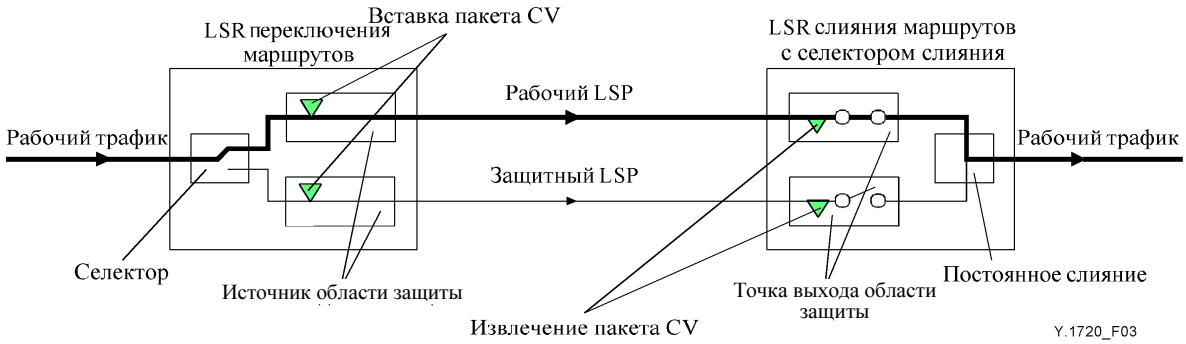

Рисунок 3/Y.1720 – Архитектура однонаправленной защитной коммутации 1:1

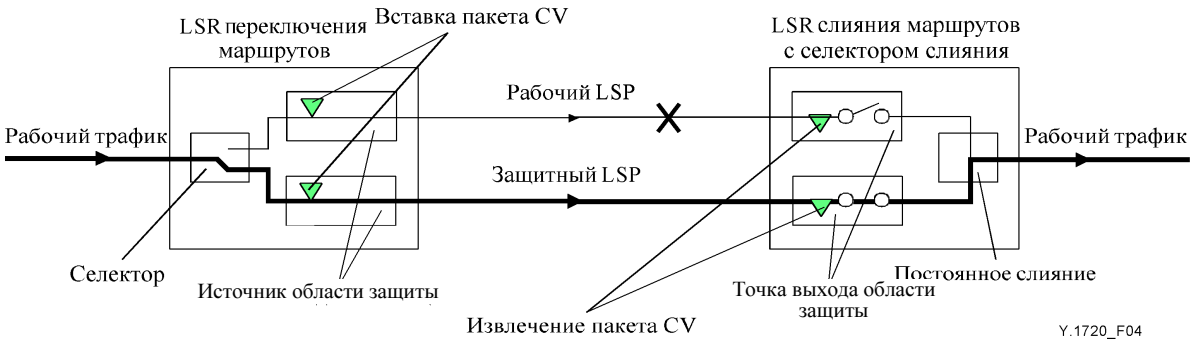

Рисунок 4/Y.1720 – Архитектура однонаправленной защитной коммутации 1:1 – отказ рабочего LSP

Дополнительный трафик

Архитектура 1:1 может поддерживать дополнительный трафик. Поскольку трафик рабочего и защитного LSP объединяется в точке выхода области защиты, дополнительный трафик должен передаваться через отдельный LSP, для которого физический маршрут совпадает с маршрутом защитного LSP (см. Рисунок 5). Это необходимо, чтобы избежать слияния дополнительного и рабочего трафика и совместно использовать полосу пропускания. Когда рабочий трафик переключается на защитный LSP, дополнительный трафик отсоединяется, чтобы освободить маршрут для защищенного трафика отказавшего рабочего подключения (см. Рисунок 6). Обычно для этого требуется протокол координации защитной коммутации. В настоящей Рекомендации BDI используется как однофазный протокол (см. также Рекомендацию МСЭ-Т I.630). Проверка наличия соединения дополнительного трафика LSP необязательна. Если требуется уведомление об отключении дополнительного трафика, должна использоваться проверка наличия соединения.

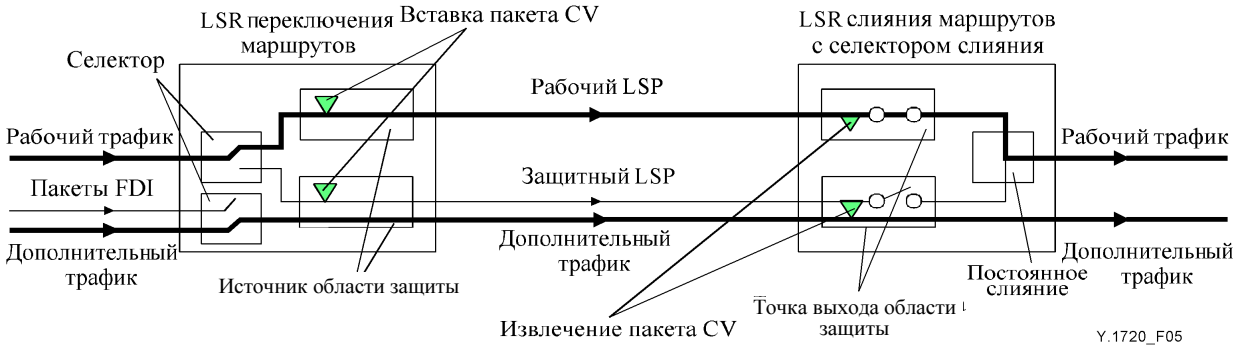

Рисунок 5/Y.1720 – Архитектура 1:1 с дополнительным трафиком

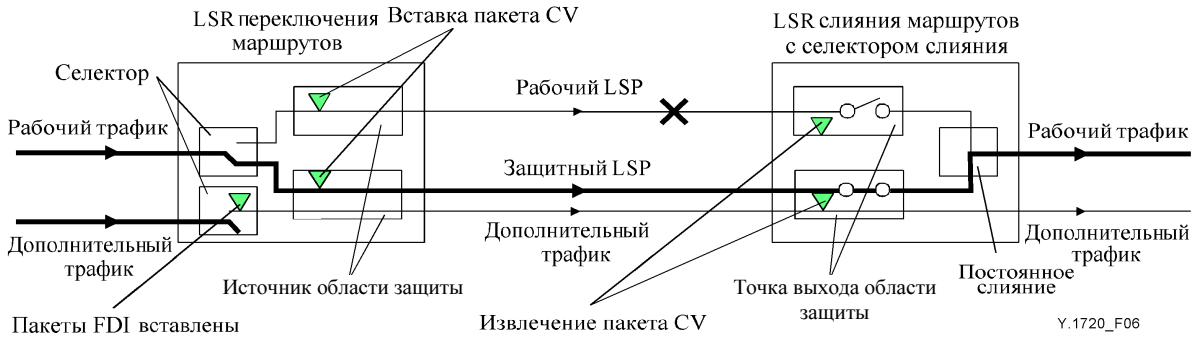

Рисунок 6/Y.1720 – Архитектура 1:1 с дополнительным трафиком – отказ рабочего LSP

7.1.1.3 Прикладная архитектура однонаправленной защитной коммутации совместно используемой сети

Защитную коммутацию совместно используемой сети можно рассматривать как расширенный вариант защиты 1:1. При этом для реализации защиты 1:1 необходимы все функциональные возможности, а также дополнительные функциональные возможности для распределения отказов среди непересекающихся линий, узлов и групп общих рисков (SRG).

Функциональные требования

Ниже приведены необходимые функциональные требования для реализации схемы защиты совместно используемой сети в режиме реального времени:

1) Защитная коммутация совместно используемой сети должна обладать потенциалом для реализации возможного совместного использования ресурса защиты при отказах непересекающихся линий, узлов и SRG в сети, гарантируя восстановление в случае единичного отказа.

2) Защитная коммутация совместно используемой сети должна обладать потенциалом для резервирования (выделения) требуемого ресурса для защиты каждого соединения без распределения его какому-либо LSP.

3) Защитная коммутация совместно используемой сети должна обладать потенциалом для обнаружения отказа (уведомления об отказе) в конечных узлах (на входе и на выходе).

4) Защитная коммутация совместно используемой сети должна обладать потенциалом для распределения ресурса защиты защитным LSP во время отказа.

5) Защитная коммутация совместно используемой сети должна обладать потенциалом для переключения подачи трафика на входе и выбора трафика на выходе из рабочего (защитного) канала в защитный (рабочий) LSP.

6) Защитная коммутация совместно используемой сети должна поддерживать восстановление в пределах ограниченного периода времени и может соответствовать обычно используемым периодам восстановления.

7) Защитная коммутация совместно используемой сети должна обеспечивать эффективное использование полосы пропускания рабочего LSP, применяя такие меры, как оптимизация маршрута с учетом зависимостей маршрутов рабочего канала и его защитного канала.

Прикладная архитектура

Схема защиты совместно используемой сети применяется, чтобы обеспечить гарантированное восстановление при использовании минимальной защиты полосы пропускания в общей топологии сети. При этом резервируется пул выделенного ресурса защиты, достаточного для восстановления всего защищаемого трафика от любого возможного единичного отказа в сети. Для каждого защищенного рабочего подключения ресурс защиты распределяется во время его активизации. Получение запроса на установление службы защиты совместно используемой сети между двумя узлами инициирует вычисление пары непересекающихся каналов между ними с двумя необходимыми ограничениями. Во-первых, должна иметься достаточная полоса пропускания по направлению связи рабочего подключения, чтобы принять трафик, относительно которого получен запрос, во-вторых, либо уже зарезервированная защитная полоса пропускания по каналу защиты должна быть достаточна для гарантии восстановления от любого единичного отказа по первичному маршруту, либо имеющаяся полоса пропускания по каналу защиты должна быть достаточна для обеспечения дополнительной полосы пропускания, необходимой для защиты нового рабочего подключения. Следует заметить, что для обеспечения совместного использования всегда сначала проводится попытка удовлетворения нового запроса уже распределенным ресурсом защиты. Это можно осуществить сохранением данных (для каждого соединения в сети) о требуемом ресурсе для восстановления после каждого отказа узла или соединения в сети. Следует отметить, что поскольку общепризнанно и доказано, что вероятность множественных одновременных отказов в большинстве сетей невелика, данная схема описана, с тем чтобы гарантировать защиту от любого единичного отказа в сети. Защита от отказов нескольких элементов может быть достигнута через прямое расширение.

Защитная коммутация и механизм запуска для каждого пораженного рабочего LSP аналогичны схеме защиты 1:1. Пример защиты совместно используемой сети приведен на Рисунке 7. На Рисунке 8 показана защита трафика после конкретного отказа.

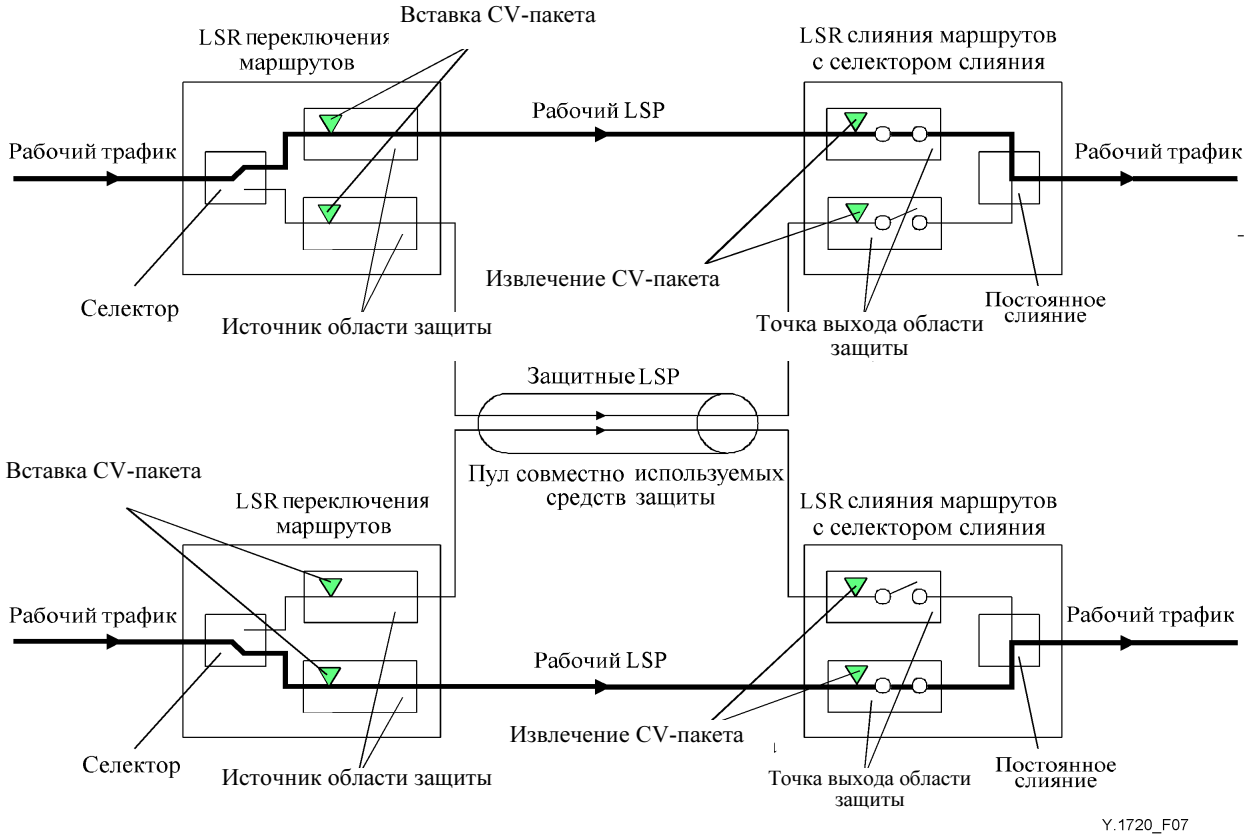

Рисунок 7/Y.1720 –Архитектура однонаправленной защитной коммутации совместно используемой сети

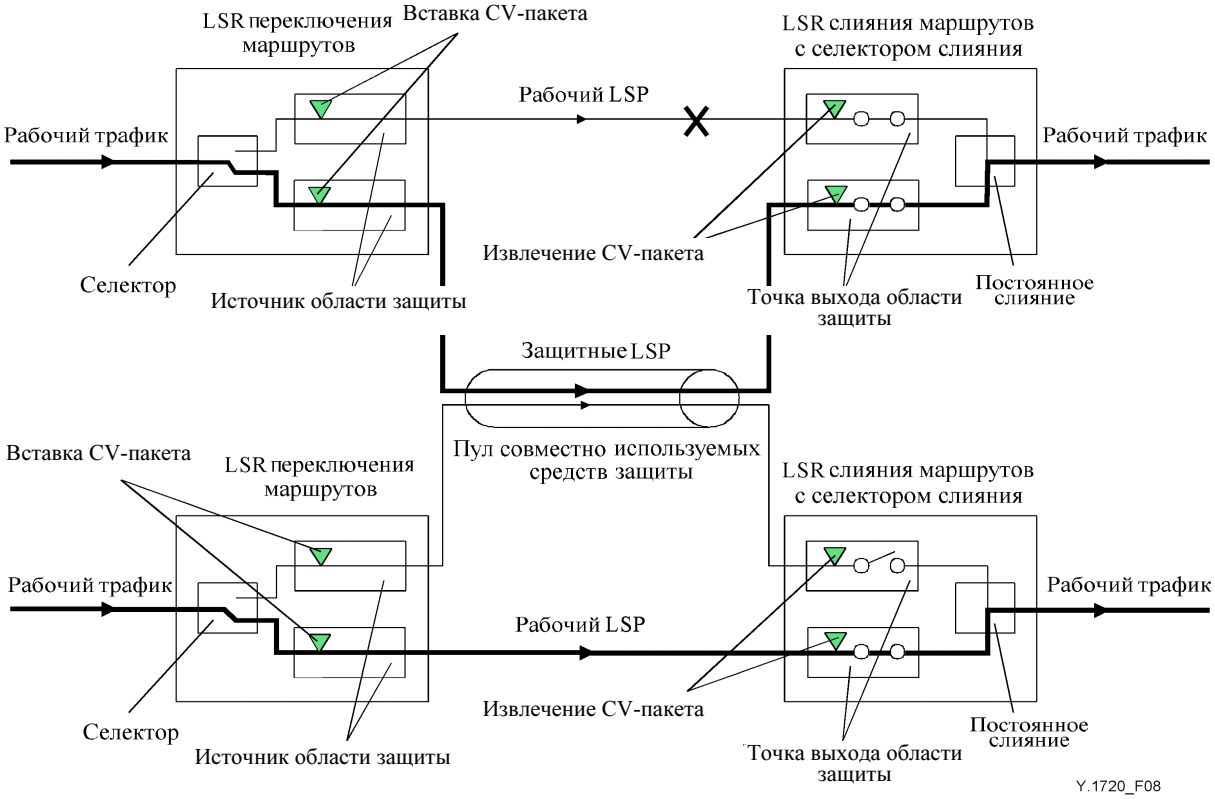

Рисунок 8/Y.1720 – Архитектура однонаправленной защитной коммутации совместно используемой сети – единичный отказ

7.1.1.4 Прикладная архитектура однонаправленной пакетной защитной коммутации 1+1

Пакетная защита каналов 1+1 обеспечивает услугу защиты уровня пакета, которая аналогична в некоторых отношениях услуге обычного подключения уровня 1+1 с несколькими важными различиями. Уровень пакетов 1+1 позволяет сделать выбор входящего пакета от любого подключения независимо от подключения, с которого последний пакет был выбран. Таким образом, пакетная защита 1+1 рассматривает оба подключения как рабочее подключение, а не считает одно подключение рабочим, а другое – защитным. В последнем случае пакеты выбираются из рабочего подключения, пока обнаружение отказа в рабочем подключении не вызовет переключение на защитное подключение. Напротив, пакет 1+1 не требует обнаружения неисправности и защитной коммутации в явной форме. Это позволяет пакетной схеме уровня 1+1 мгновенно и прозрачным образом восстановиться после любого отказа. Как и при защите уровня подключений 1+1, только граничные узлы должны пользоваться этой услугой.

Для обеспечения пакетной службы защиты 1+1 между двумя узлами в сети MPLS между ними формируется пара LSP по непересекающимся каналам. Пакеты от потока клиента, являющегося абонентом услуги, одновременно поступают на входной узел в два LSP. Непересекающиеся каналы в простейшем случае могут быть непересекающимися соединениями или узлами, но в целом могут быть связаны с таким более сложным понятием, как группы соединений совместного риска. В выходном граничном узле одна из двух возможных полученных из непересекающихся каналов копий пакетов выбирается и отправляется далее. Учитывая это, любой единичный отказ в сети, кроме отказа самогó входного или выходного узла, может повлиять максимум на одну копию каждого пакета. Это позволяет услуге прозрачным образом выдержать единичный отказ. В отношении времени восстановления работоспособности это может быть определено как мгновенное восстановление после отказа, так как нет необходимости в явной форме обнаруживать, уведомлять и переключаться на канал защиты.

Функциональные требования

Минимальные требования для обеспечения пакетной службы защиты 1+1 заключаются в следующем:

a) Отсутствует новое требование в отношении внутренних узлов сети.

b) Сеть должна поддерживать установку разнонаправленных LSP.

c) *Входной узел*

   1) Должен быть в состоянии связывать два LSP, которые используются для обеспечения пакетной защиты уровня 1+1 между двумя конечными узлами.
   2) Должен поддерживать передачу в пакете идентификатора, который будет использоваться для идентификации дубликатов пакета в выходном узле.
   3) Должен быть в состоянии обеспечивать одновременную подачу каждого пакета на два совместных LSP.

d) *Выходной узел*

   1) Должен быть в состоянии связывать два LSP, которые используются для обеспечения пакетной защиты уровня 1+1 между двумя конечными узлами.
   2) Должен быть в состоянии идентифицировать дубликаты пакета с использованием идентификатора.
   3) Должен быть в состоянии выбирать и отправлять только одну из копий пакета.

Вышеперечисленные требования описывают минимальные функциональные возможности, необходимые для осуществления схемы пакетной защиты уровня 1+1.

Эталонная модель

На Рисунке 9 показана реализация схемы пакетной защиты 1+1 с использованием порядковых номеров в качестве идентификаторов. После прохождения через классификатор каждому пакету, который должен быть отправлен на совмещенный LSP, назначается уникальный порядковый номер во входном узле. Этот пакет с уникальной идентификацией затем дублируется и направляется по двум непересекающимся LSP. В выходном узле используется счетчик для отслеживания ожидаемого порядкового номера следующего пакета. Подробности выполнения примера описаны в Добавлении.

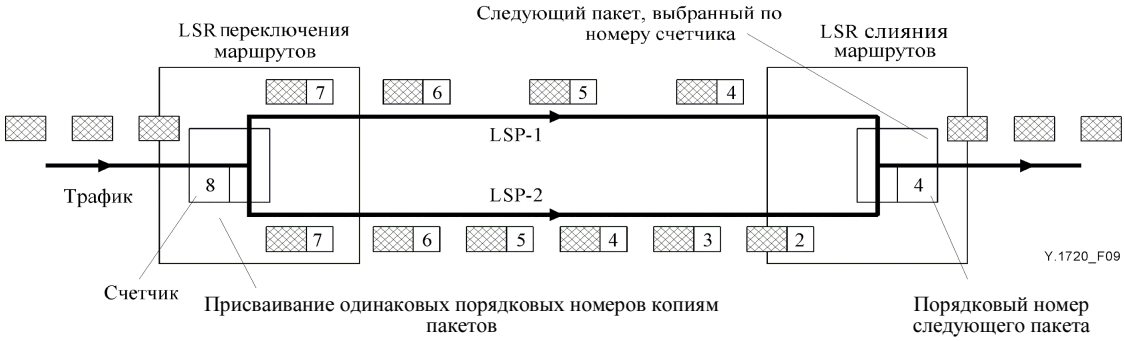

Рисунок 9/Y.1720 – Архитектура однонаправленной защитной пакетной коммутации 1+1

7.1.2 Механизм запуска защитной коммутации

Операция защитной коммутации должна проводиться, когда:

1) она инициирована действиями оператора (например, ручной коммутацией, принудительной коммутацией или блокировкой защиты) в отсутствии действующего более приоритетного запроса на коммутацию;
2) сообщение SF объявлено на подсоединенном LSP (т. е. на рабочем LSP или защитном LSP) и не объявлено на другом LSP, и десинхронизирующий таймер сработал; или
3) время срабатывания таймера ожидания восстановления (обратный режим) истекло, а сообщение SF не объявлено на рабочем LSP.

7.1.2.1 Ручное управление

Ручное управление функцией защитной коммутации может быть передано от операционной системы.

7.1.2.2 Условия объявления о потере сигнала

7.1.2.2.1 Архитектура 1+1

Для архитектуры 1+1 о потере сигнала (SF) объявляется, когда точка выхода области защиты достигает "состояния неисправности ближнего конца" следа LSP при вводе условий dServer, dLOCV, dTTSI_Mismatch, dTTSI_Mismerge, dExcess или dUnknown.

Для достижения быстрой защиты (требование для быстрой защиты находится в стадии изучения) о SF может быть объявлено, когда пакет FDI получен точкой выхода области защиты, прежде чем он войдет в другие состояния неисправности (например, dLOCV). Это позволяет обеспечить быструю защиту от неисправностей, источники которых расположены на уровнях ниже уровня MPLS (для этого нужно, чтобы входящий FDI имел пункт кода DT 0x0101).

Кроме того, функция FDD может использоваться для достижения более быстрого объявления состояния потери сигнала.

ПРИМЕЧАНИЕ – Этот вариант используется только при условии, что нижний уровень не защищен. Если нижний уровень также защищен, то это может привести к ненужной защитной коммутации посредством объявления о SF при получении пакетов FDI.

В случае когда функция CV или FFD не активирована, о SF объявляется, если пакет FDI получен точкой выхода области защиты. Этот вариант применяется только к неисправностям, источники которых на уровнях ниже уровня MPLS (для этого нужно, чтобы входящий FDI имел пункт кода DT 0x0101).

7.1.2.2.2 Архитектура 1:1

Для архитектуры 1:1 сообщение о потере сигнала (SF) объявляется, когда:

- источник области защиты входит в состояние неисправности дальнего конца точки выхода следа при получении пакета BDI (от обратного LSP или вне диапазона).

7.1.2.2.3 Архитектура совместно используемой сети

Архитектура совместно используемой сети – это расширенный вариант архитектуры 1:1. О потере сигнала (SF) объявляется так же, как и в архитектуре 1:1.

ПРИМЕЧАНИЕ – Защита против неисправности двунаправленного LSP подлежит дальнейшему изучению.

7.1.3 Соответствие целям сети

Применяются следующие цели сети:

1) *Режимы работы*

   Обеспечивается возвратная и невозвратная коммутация.

2) *Ручное управление*

   Оператор управляет посредством поддерживаемых команд: "блокировка защиты", "принудительная коммутация" и "ручная коммутация".

3) *Другие критерии инициирования коммутации*

   Сообщения "потеря сигнала", "ожидание восстановления" и "отсутствие запроса" поддерживаются в дополнение к командам ручного управления, перечисленным выше, в качестве критериев для активации (или предотвращения) защитной коммутации.

7.1.4 Критерии инициирования коммутации

Существуют следующие критерии инициирования коммутации:

1) Инициируемая извне команда ("очистка", "блокировка защиты", "принудительная коммутация", "ручная коммутация");
2) автоматически инициируемая команда ("потеря сигнала"), связанная с областью защиты;
3) состояние ("ожидание восстановления", "отсутствие запроса") функции защитной коммутации.

Все запросы являются локальными (т. е. точка выхода защиты для архитектуры 1+1 и источник защиты для архитектуры 1:1). Приоритетность локальных запросов приводится в Таблице 1.

Таблица 1/Y.1720 - Приоритетность локальных запросов

Локальный запрос (т. е. автоматически инициируемая команда, состояние или внешне инициируемая команда)	**Порядок очередности**
Очистка	Самый высокий
Блокировка защиты	|
Принудительная коммутация	|
Потеря сигнала	|
Ручная коммутация	|
Ожидание восстановления,	|
Отсутствие запроса	Самый низкий

ПРИМЕЧАНИЕ 1 – Принудительная коммутация для рабочего LSP не должна отменяться сообщением "потеря сигнала" в защитном LSP. Так как выполняется однонаправленная защитная коммутация и протокол APS в защитном LSP не поддерживается, то сообщение "потеря сигнала" в защитном LSP не влияет на способность выполнения принудительной коммутации для рабочего LSP.

ПРИМЕЧАНИЕ 2 – Принудительная коммутация для защитного LSP не определена, так как эта функция может быть выполнена посредством команды "блокировка защиты".

7.1.4.1 Инициируемые извне команды

Инициируемые извне команды перечислены ниже в порядке убывания приоритета. Функциональные возможности каждой из них описаны ниже.

Очистка: Эта команда очищает все инициируемые извне команды коммутации, перечисленные ниже.

Блокировка защиты (LoP): Фиксирует позицию селектора на рабочем LSP. Предотвращает переключение селектора на защитный LSP, когда выбирается рабочий LSP. Переключает селектор с защитного на рабочий LSP, когда выбирается защитный LSP.

Принудительная коммутация (FS) для рабочего LSP: Переключает селектор с рабочего LSP на защитный LSP (если отсутствует более приоритетный запрос на коммутацию (т. е. LoP)).

Ручная коммутация (MS) для рабочего LSP: Переключает селектор с рабочего LSP на защитный LSP (если отсутствует равный или более приоритетный запрос на коммутацию (т. е. LoP, FS, SF или MS)).

Ручная коммутация (MS) для защитного LSP: Переключает селектор с защитного LSP на рабочий LSP (если отсутствует равный или более приоритетный запрос на коммутацию (т. е. LoP, FS, SF или MS)).

7.1.4.2 Инициируемая FDI защитная коммутация

В случае инициирования защитной коммутации посредством FDI, если LSP с SF не входит в состояние неисправности ближнего конца, может потребоваться предотвратить частые переходы. В этом случае может быть определен некоторый интервал времени, который должен пройти до выполнения еще одной операции защитной коммутации. Это определяется как FFS.

7.1.4.3 Состояния

Команда "ожидание восстановления" применима только для обратного режима и относится к рабочему LSP. Это состояние вводится локальной функцией защитной коммутации в условиях, когда рабочий трафик принимается по защитному LSP, а рабочий LSP восстановлен, если запросы на локальную защитную коммутацию ранее были активны, а теперь стали неактивны. Это предотвращает возврат к выбору рабочего LSP, пока не срабатывает таймер ожидания восстановления. Время ожидания восстановления может быть установлено оператором между 1 и 30 минутами с шагом в 1 минуту; значение "по умолчанию" равно 12 минутам.

"Отсутствие запроса" – это состояние, вводимое локальной функцией защитной коммутации при всех условиях, когда запросы на локальную защитную коммутацию (включая команду "ожидание восстановления") не являются активными.

7.1.5 Протокол защитной коммутации

В однонаправленной архитектуре защитной коммутации 1+1, 1:1 и совместно используемой сети отсутствует потребность в протоколе APS.

7.1.6 Алгоритм операции однонаправленной защитной коммутации

7.1.6.1 Управление селектором

В операции однонаправленной архитектуры защитной коммутации 1+1, 1:1 и совместно используемой сети селектор управляется наиболее приоритетным локальным (т. е. точка выхода области защиты для архитектуры 1+1; источник области защиты для архитектуры 1:1) запросом (автоматически инициируемая команда, состояние или инициируемая извне команда). Таким образом, каждый конец канала работает независимо от другого. Если в обоих LSP наличествует состояние равного приоритета (например, SF), то коммутация не производится.

В пакетном режиме 1+1 пакеты выбираются на базе селектора уровня пакета, который использует идентификаторы (порядковые номера), содержащиеся в передаваемых пакетах.

7.1.6.2 Возвратный режим

В возвратном режиме работы в условиях, когда рабочий трафик передается по защитному LSP, а рабочий LSP восстановлен, если запросы на локальную защитную коммутацию ранее были активны, а теперь стали неактивны, устанавливается локальное состояние "ожидание восстановления".

Это состояние обычно завершается и переходит в состояние "отсутствие запроса", после того как сработает таймер ожидания восстановления. Тогда происходит возврат к выбору рабочего LSP. Таймер ожидания восстановления деактивируется раньше, если какой-либо локальный запрос более высокого приоритета вытесняет это состояние.

7.1.6.3 Невозвратный режим

Если неисправный LSP больше не находится в состоянии SF и другие инициируемые извне команды отсутствуют, устанавливается состояние "отсутствие запроса". В этом состоянии коммутация не происходит.

7.2 Механизмы двунаправленной защитной коммутации

Подлежат дальнейшему изучению.

8 Вопросы безопасности

В настоящей Рекомендации не рассматриваются те проблемы защиты, которые уже не присутствуют в архитектуре MPLS или в архитектуре протоколов уровня клиента.

Защитная коммутация может укрепить защиту сетей MPLS, поскольку она автоматически переключает трафик с неисправных LSP, которые могут быть неправильно соединены или сконфигурированы на другие LSP, должным образом работающие LSP. Это предотвращает раскрытие клиентского трафика для других пользователей.

Добавление I

Пример совместного использования ресурса защиты для защитной коммутации совместно используемой сети

Для гарантируемого восстановления с аналогичным качеством обслуживания требуется, чтобы для целей восстановления в сети была выделена необходимая полоса пропускания. Для схемы совместно используемой сети требуется, чтобы эта защитная полоса пропускания была достаточна для размещения всего трафика, на который воздействует любой единичный отказ в сети. Это может быть достигнуто вычислением и резервированием ресурса защиты во время запуска рабочего LSP. Запрос на обеспечение услуги совместно используемой сети между двумя узлами требует вычисления пары непересекающихся каналов между этими узлами с двумя необходимыми требованиями. Во-первых, должна быть в наличии достаточная полоса пропускания по первичному маршруту LSP, чтобы вместить требуемую полосу пропускания. Во-вторых, либо уже зарезервированная защитная полоса пропускания по защитному каналу является достаточной для гарантии восстановления LSP от любого одиночного отказа по первичному маршруту, либо имеющаяся полоса пропускания по защитному каналу должна быть достаточна, чтобы вместить дополнительную полосу пропускания, необходимую для его защиты.

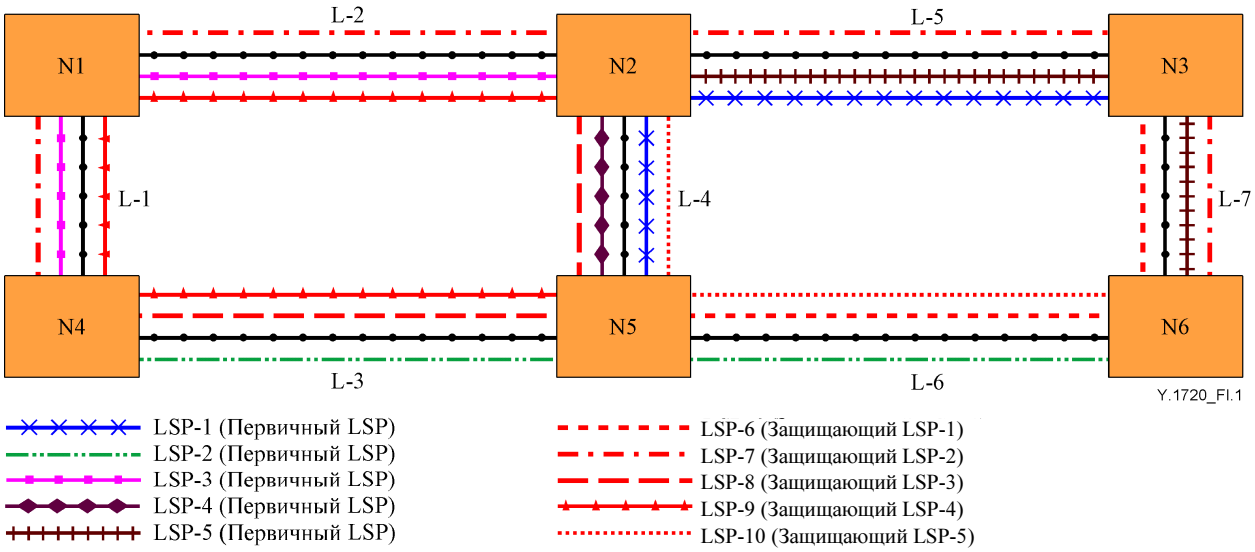

Рисунок I.1/Y.1720 – Примеры рабочих и защитных маршрутов

Реализация совместного использования ресурса защиты при различных отказах может достигаться отслеживанием для каждого соединения объема ресурса, требуемого для восстановления после каждого из отказов. Это может быть показано на примере сети MPLS. На Рисунке I.1 приведен пример сети с пятью двунаправленными рабочими соединениями и их пятью непересекающимися двунаправленными защитными соединениями. (Следует отметить, что каждое соединение состоит из пары однонаправленных LSP.) Для демонстрационных целей предположим, что для каждого рабочего соединения требуется одна единица полосы пропускания.

В Таблице I.1 показан объем ресурса защиты, требуемый для каждого соединении в случае любого возможного единичного отказа соединения или узла в сети. Для понимания содержания Таблицы I.1 рассмотрим первую строку, связанную с соединением L-1. Ячейка в столбце L-3 для этой строки указывает, что имеется одна единица трафика, обусловленная LSP-2, на соединении L-3, которое использует соединение L-1 на своем восстановительном маршруте, когда соединение L-3 выходит из строя из-за неисправности. Аналогичным образом ячейка в столбце N5 относится к случаю отказа узла N5 и его воздействия на соединение L-1. В последнем столбце, озаглавленном Max, представлено максимальное значение всех ячеек в этой строке. Данное значение – величина защитной полосы пропускания, которая должна быть зарезервирована в этом соединении для единичного отказа по наихудшему варианту в сети. Например, для соединения L-6 это значение равно 2 единицам компенсации отказа соединения L-5.

Таблица I.1/Y.1720 –Таблица отслеживания отказов и требуемой защитной полосы пропускания

Соеди-нение	L-1	L-2	L-3	L-4	L-5	L-6	L-7	N1	N2	N3	N4	N5	N6	Max
L-1			1	1		1						1		1
L-2			1	1		1						1		1
L-3	1	1		1				1						1
L-4	1	1			1		1	1		1				1
L-5			1			1						1		1
L-6				1	2		1		1	1				2
L-7			1	1	1	1			1			1		1

Информация в Таблице I.1 дает возможность рассчитать для данного маршрута связи и полосы пропускания рабочего LSP, сколько дополнительного защитного ресурса должно быть зарезервировано в каждом соединении по этому направлению связи, чтобы гарантировать его защиту во время отказа.

Для нового защищенного подключения содержание Таблицы I.1 может быть обновлено посредством обновления строк, соответствующих соединениям по защитному каналу. Для такого обновления проводится увеличение (на требуемую полосу пропускания соединения) значения каждого столбца, соответствующее узлам и соединениям по рабочему направлению связи. Затем вычисляется максимальное значение каждой обновленной строки, как показано в последнем столбце Таблицы I.1.

Таблица I.2/Y.1720 – Обновленная таблица, учитывающая запрос на дополнительное обслуживание

Соединение	L-1	L-2	L-3	L-4	L-5	L-6	L-7	N1	N2	N3	N4	N5	N6	Max
L-1			2	2		1						2		2
L-2			2	2		1						2		2
L-3	1	1		1				1						1
L-4	1	1			1		1	1		1				1
L-5			1			1						1		1
L-6				1	2		1		1	1				2
L-7			1	1	1	1			1			1		1

В качестве примера рассмотрим получение запроса на услугу защиты совместно используемой сети между узлами N4 и N2 сети, показанной на Рисунке I.1. Предположим, что при получении запроса сеть была в состоянии, показанном на Рисунке I.1 и в Таблице I.1. Далее предположим, что (N4-L3-N5-L4-N2) и (N4-L1-N1-L2-N2) – это рассчитанные рабочие и защитные маршруты, соответственно, обслуживающие данный запрос. Учитывая эти непересекающиеся маршруты, соединения L-1 и L-2 Таблицы I.1 будут изменены. Модифицированная таблица показана в Таблице I.2. Следует отметить, что теперь в обоих соединениях L-1 и L-2 одна дополнительная единица полосы пропускания необходима для гарантии восстановления после отказа по рабочему маршруту этого нового запроса на подключение.

Добавление II
Реализация примера пакета 1+1

Схема пакета 1+1 может быть осуществлена с использованием последовательности в качестве идентификатора. Порядковый номер можно записать как первые четыре байта внутри раздела заголовка LSP, обеспечивающего схему пакета 1+1. Так как входные и выходные узлы должны знать каждый LSP, участвующий в пакете 1+1, выходной узел будет знать, что внутри метки имеется порядковый номер. Он будет использовать порядковый номер для выбора, а затем удалять его перед пересылкой принятого пакета. Следует отметить, что пакет 1+1 можно обеспечивать на любом уровне иерархии гнездового LSP. На Рисунке II.1 показана позиция порядкового номера позади 4-байтного внутреннего заголовка пакета MPLS.

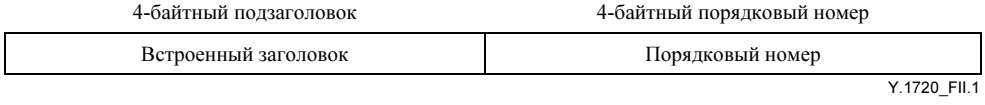

Рисунок II.1/Y.1720 – Пример переноса порядкового номера

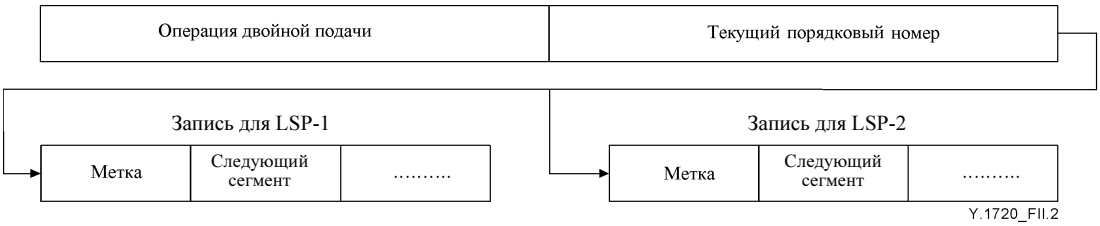

Рисунок II.2/Y.1720 – Расширенные функциональные возможности NHLFE для поддержки двойной подачи

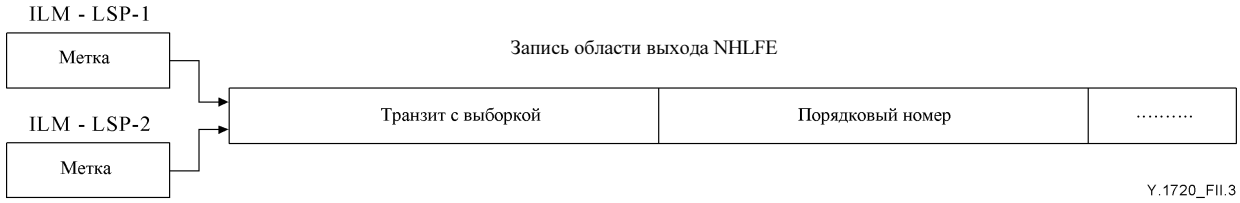

Рисунок II.3/Y.1720 – Расширенные функциональные возможности NHLFE для поддержки выбора

Потенциал двойной подачи и выбора можно реализовать в промежуточном уровне MPLS путем совершенствования записей: "запись, содержащая адрес следующего шага при коммутации меток" (NHLFE). Во входном узле, чтобы обеспечить функциональные возможности двойной подачи, NHLFE должна поддерживать два исходящих LSP вместо одного. Это легко достигается использованием двух записей адреса следующего шага при коммутации меток вместо одной, при этом каждая запись соответствует одному из совмещенных различных LSP. На Рисунке II.2 показан такой случай. При этом, когда пакет клиентского уровня пересылается NHLFE, поддерживающей двойную подачу, она сначала копирует пакет, а затем пересылает его на следующие сегменты с соответствующими метками согласно его двум записям адреса следующего шага/меток. В середине сети каждая копия пакета пересекает LSP стандартным способом, как и любой другой пакет пересек бы LSP; таким образом, эта пересылка прозрачна для LSR. В выходном узле таблица соответствия входящих меток (ILM) должна отобразить метки двух разных LSP в одной записи NHLFE, что дает возможность принимающей стороне выбрать одну из возможно двух полученных копий. На Рисунке II.3 показан такой случай.

II.1 Механизм двойной подачи и выбора

Два компонента требуются для любого механизма двойной подачи и выбора:

1) возможность двойной подачи на одном конце; и
2) возможность производить соответствующий выбор из поданного методом двойной подачи сигнала на другом конце. В общем случае осуществление двойной подачи не представляет затруднений, в то время как произведение выбора требует осторожных и зачастую нетривиальных действий. В источнике двойная подача пакетов может осуществляться копированием в два потока пакетов. В пунктах назначения каждый пакет может быть получен дважды в разное время (или лишь единожды, или никогда), по одному от каждого из двух LSP. Чтобы выбрать каждый пакет единожды, адресат должен быть в состоянии идентифицировать дублирующие пакеты и затем выбрать один, а также учесть все возможные комбинации. Этот процесс выбора на уровне пакетов нетривиален, поскольку дублирующие пакеты могут прибывать не в одно и то же время (из-за задержки распространения и буферизации), а также эти пакеты могут теряться (из-за ошибок при передаче и переполнения буфера).

Нижеприведенный пример алгоритма показывает метод, которым решаются все эти проблемы.

Алгоритм

Переменные:

N /* число битов, которые нужно использовать для порядкового номера */

```
rec_seq_no      /* порядковый номер полученного пакета */
select_counter  /* N-битный счетчик приемника, который отслеживает порядковый номер
                   следующего ожидаемого пакета */
window_sz       /* размер окна; должен быть меньше, чем 2^N */
```

Инициализация:

```
Rec_seq_no = 0;
select_counter = 0;
```

Алгоритм:

Отправитель

```
вставить rec_seq_no во внутреннюю "метку" пакета;
передать одну копию пакета по каждому совмещенному LSP;
rec_seq_no ++;
```

Селектор

```
Если (rec_seq_no вне скользящего окна, определенного
  [select_counter, select_counter+window_sz]),
  отклонить пакет;
иначе       /* rec_seq_no находится в окне */
{
        принять пакет;
        select_counter = rec_seq_no +1;
}
```

II.2 Анализ схемы пакета 1+1

Входной узел вставляет порядковый номер. Пакет затем дублируется и передается по различным LSP. Из-за разнесения LSP будет ведущий LSP и ведомый LSP. Ведущий LSP доставит пакеты к выходному узлу быстрее, чем ведомый LSP. Поэтому в условиях отсутствия отказов выходной узел выберет пакеты из ведущего LSP. Пакеты, полученные из ведомого LSP, будут дублирующими пакетами и поэтому будут отклонены.

Решение о приеме или отклонении полученного пакета принимается на основе порядкового номера полученного пакета и на значении счетчика + скользящее окно в выходном узле. Счетчик указывает порядковый номер следующего пакета, который он ожидает. Счетчик + скользящее окно обеспечивают окно приемлемых порядковых номеров. Скользящее окно необходимо, чтобы нужным образом принимать и отклонять пакеты. Если полученный пакет попадает в окно, он считается допустимым и может быть принят, в противном случае он отклоняется. Размер окна должен быть больше, чем максимальное число последовательных пакетов, которые рабочий (действующий) LSP может потерять.

Скользящее окно используется, чтобы решить проблему потери пакетов в ведущем LSP, когда порядковый номер пакета в ведущем LSP очень близок к циклической точке. На Рисунке II.4 показан ведущий LSP (LSP-1), который доставляет пакет с порядковым номером 29. Пакет принимается, и показания счетчика увеличиваются до 30. Если мы предположим, что 2 последовательных пакета потеряны (т. е. пакеты с порядковыми номерами 30 и 31), то следующий полученный пакет в LSP-1 будет с номером 0. Без скользящего окна выходной узел отклонит пакет, так как $0 < 30$. При формировании скользящего окна, большего чем максимальное число последовательных пакетов, которое рабочий (действующий) LSP может потерять, эта проблема может быть решена. Например, пусть максимальное число последовательных пакетов, которые рабочий LSP может потерять, равно 5, тогда может быть определено скользящее окно с размером, равным 6. Рассмотрим тот же пример, однако теперь, используя скользящее окно, выходной узел примет пакеты в диапазоне {30, 31, 0, 1,

2, 3}. Таким образом, даже если 5 пакетов потеряны (т. е. максимальное число последовательных пакетов, которые могут быть потеряны в рабочем LSP), следующий полученный пакет будет иметь порядковый номер 3 и он будет принят.

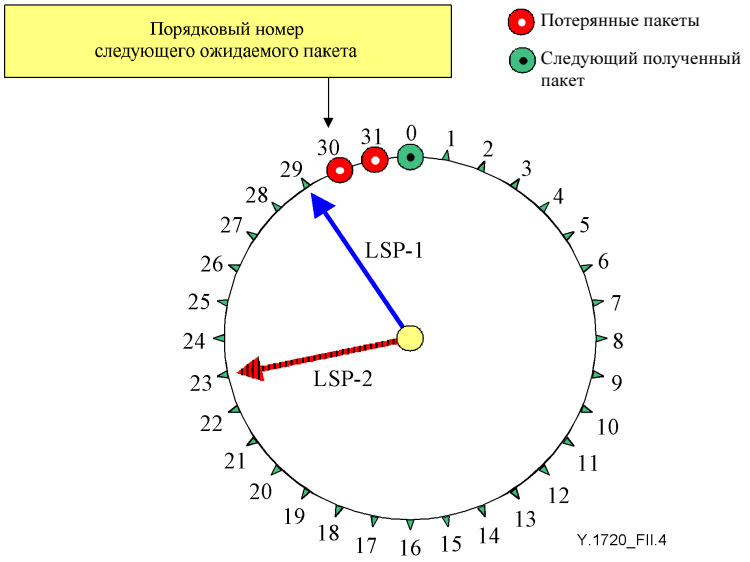

Рисунок II.4/Y.1720 – Потеря пакета в сочетании с циклическим переходом

Следует отметить, что идея скользящего окна действует только тогда, когда отстающий LSP не может попасть в диапазон скользящего окна. Если пакет с порядковым номером в диапазоне скользящего окна получен из отстающего LSP, то он будет ошибочно принят. Отстающий LSP может принимать пакет только с порядковым номером в диапазоне скользящего окна, если он отстает больше, чем на (2^N – размер подвижного окна). Таким образом, число N битов, используемых для порядкового номера, должно удовлетворять следующему уравнению:

$$2^N > \text{SlidingWindow} + \text{DelayWindow},$$

где:

SlidingWindow > максимальное число последовательных пакетов, которые могут быть потеряны в LSP,

а

DelayWindow = максимальное число пакетов, на которое ведомый LSP может отстать от ведущего LSP.

Следует отметить, что 4-битное поле обеспечивает последовательность более 4 миллиардов номеров, что является достаточно большим числом для учета потерь последовательных пакетов при наихудшем варианте и различиях в задержках.

Один из разумных способов установки размеров скользящего окна и окна задержки состоит в том, чтобы делать размер скользящего окна равным размеру окна задержки. (Следует отметить, что считается, что размер окна задержки обычно больше, чем размер скользящего окна.) Это гарантирует выбор пакетов из ведущего LSP при всех сценариях, после того как отказавший LSP восстановлен. Этот вопрос далее рассматривается в следующем разделе, где обсуждаются различные сценарии отказа.

II.2.1 Действия механизма выбора при различных сценариях отказа

Один из способов рассмотрения действия механизма выбора состоит в том, чтобы представить себе часы с интервалами 2^N. На Рисунке II.5 показан пример, где N = 4 (т. е. с 4-битным порядковым номером), и поэтому порядковый номер находится в диапазоне от 0 до 15. В данном примере скользящее окно установлено равным окну задержки, размер которого равен 5.

На Рисунке II.5 показано, что ведущий LSP на 3 порядковых номера опережает ведомый LSP. Ведущий LSP доставляет пакет с порядковым номером = 1, и показания счетчика теперь становятся равными 2.

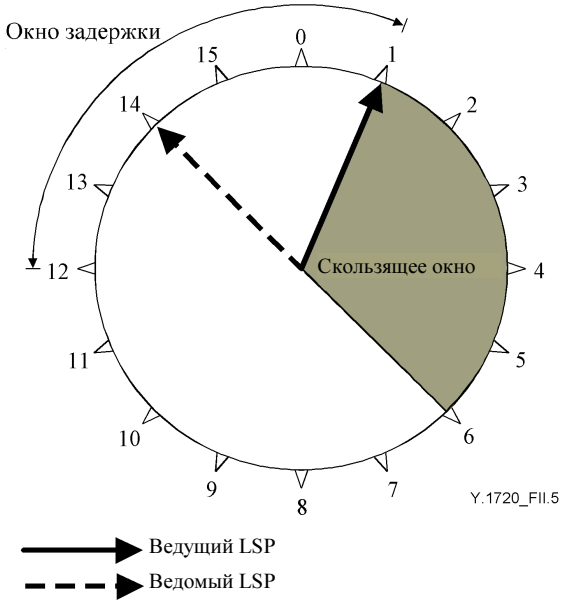

Рисунок II.5/Y.1720 – Концепция скользящего окна и окна задержки

На Рисунке II.6 показано, что ведущий LSP выходит из строя до получения пакета с порядковым номером 2 из ведущего LSP. До тех пор пока пакет с порядковым номером 2 не доставлен из ведомого LSP, выходной узел не будет выбирать каких-либо пакетов, а показания счетчика останутся равными 2.

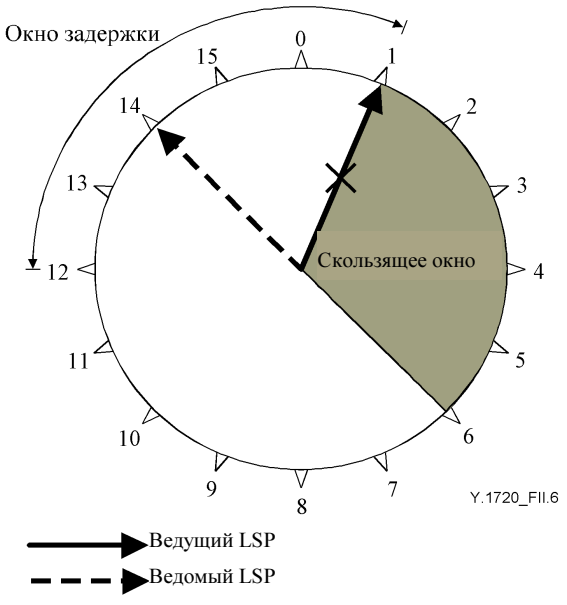

Рисунок II.6/Y.1720 –Сценарий отказа ведущего LSP

На Рисунке II.7 показано, что когда пакет с порядковым номером 2 получен из ведомого LSP, выходной узел увеличивает показания счетчика до 3, а скользящее окно сдвигается таким образом, чтобы пакет с порядковым номером в диапазоне от 3 до 7 мог быть принят.

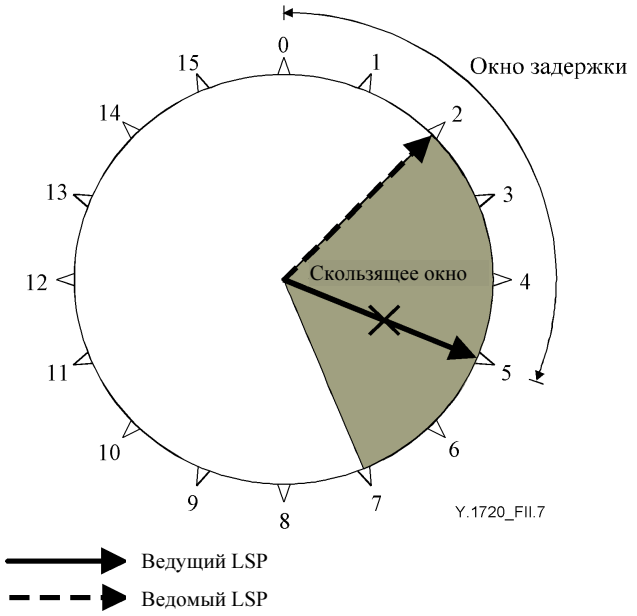

Рисунок II.7/Y.1720 – Восстановление трафика после отказа ведущего LSP

На Рисунке II.8 показано, что до получения пакета с порядковым номером 3 из ведомого LSP ведущий LSP восстанавливается и пакет с порядковым номером 6 принимается из ведущего LSP. Так как 6 находится в диапазоне скользящего окна, то пакет принимается. Следует отметить важность того, что, когда ведущий LSP работает, пакеты принимаются из ведущего LSP. Поэтому для гарантии того, что, когда ведущий LSP восстановится, он доставит пакет со значением порядкового номера, которое расположено в диапазоне скользящего окна, скользящее окно должно быть равно или больше, чем окно задержки, что и наблюдается в данном примере.

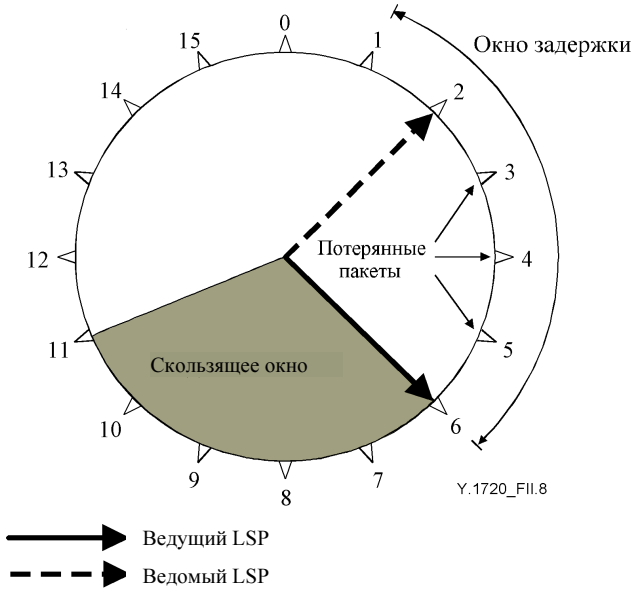

Рисунок II.8/Y.1720 – Сценарий восстановления ведущего LSP

На рисунках II.9, II.10 и II.11 показана проблема, которая возникает, если размер скользящего окна устанавливается меньше, чем размер окна задержки. В этом случае возможно, что, когда ведущий LSP восстановлен, он доставляет пакеты с порядковыми номерами, которые выходят за пределы скользящего окна, и поэтому выходной узел продолжает принимать пакеты из ведомого LSP. Если позднее ведомый LSP отказывает,

существует вероятность потери большого числа пакетов (в наихудшем случае это количество равно 2^N, *размер_подвижного_окна*, где N – число битов, используемых для формирования порядкового номера).

На Рисунке II.9 показан пример, где размер скользящего окна равен 3, в то время как размер окна задержки может иметь значение до 6. В этом примере ведомый LSP отстает от ведущего LSP на 4 порядковых номера. Так как ведущий LSP вышел из строя, то пакеты выбираются из ведомого LSP.

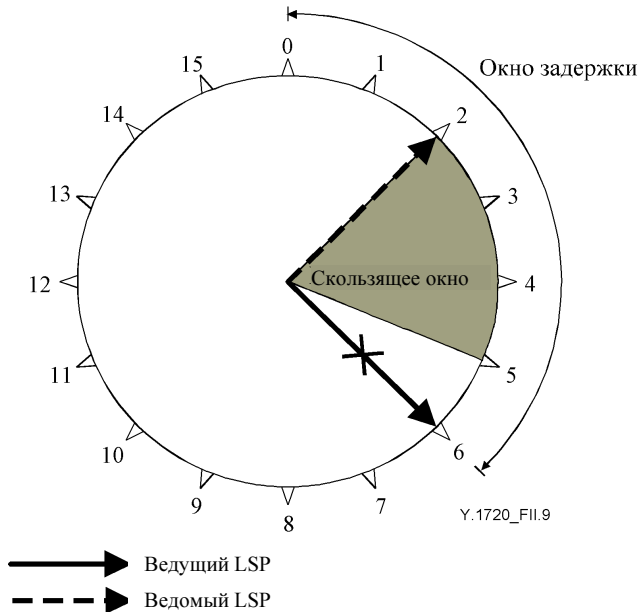

Рисунок II.9/Y.1720 – Сценарий, когда скользящее окно < окно задержки

На Рисунке II.10 показано, что после восстановления ведущего LSP доставляет пакет с порядковым номером, равным 7, который находится вне скользящего окна, и поэтому пакет отклоняется. Пакеты по-прежнему выбираются из ведомого LSP.

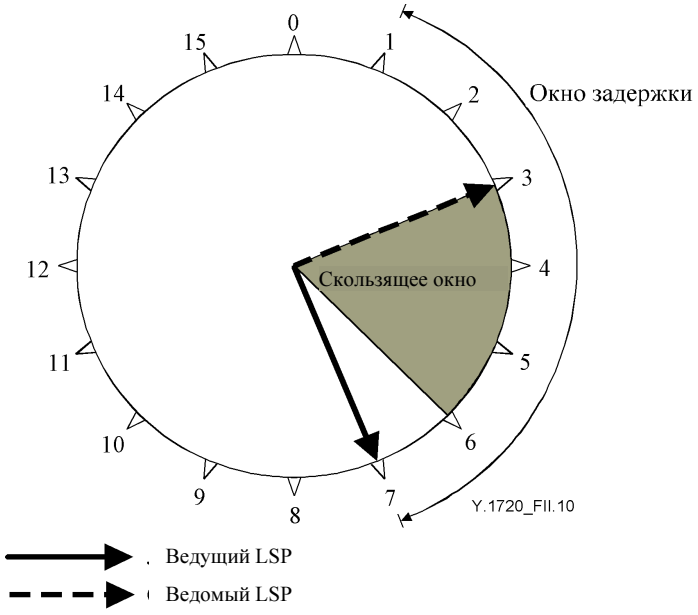

Рисунок II.10/Y.1720 – Восстановление LSP: скользящее окно < окно задержки

На Рисунке II.11 показан отказ ведомого LSP. Так как ведущий LSP доставляет пакеты вне скользящего окна, вследствие чего эти пакеты отклоняются, то выходной узел не будет принимать пакеты, пока ведущий LSP не пройдет цикл полностью и не начнет доставлять пакеты с порядковым номером, который попадает в скользящее окно. Это может приводить к существенной потере пакетов. Поэтому для предотвращения такого явления рекомендуется, чтобы в данном типе алгоритма селектора размер скользящего окна устанавливался равным размеру окна задержки.

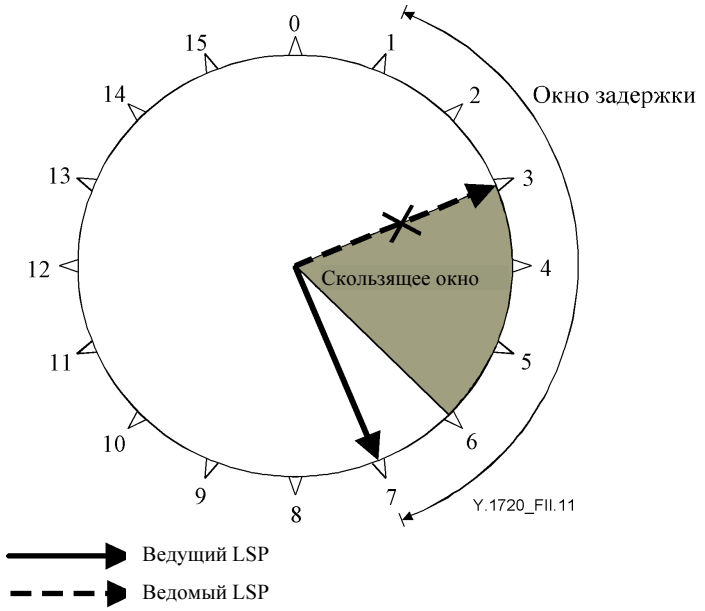

Рисунок II.11/Y.1720 – Возможная проблема: скользящее окно < окно задержки

II.2.2 Дополнительные замечания

a) Схема требует сложных действий только в граничных узлах. Далее схема не требует явного обнаружения сбоев или уведомления о них. Это подразумевается в соответствии со схемой выбора пакета на выходе, которая работает на основе порядкового номера и локально поддерживаемых счетчиков.

b) Двойная подача требует дублирования пакетов на входе. Это предполагает некоторую дополнительную минимальную обработку на входе. Для выбора требуется сравнение порядкового номера, который содержится в пакете, с показаниями счетчика, поддерживаемыми в приемнике, и результат выбора приводит к условию принятия или отклонения пакета. В отношении установки аппаратного или программного обеспечения стоимость обработки минимальна. Еще одно последствие для показателей работы – это стоимость полосы пропускания, связанная с порядковым номером, который содержится в пакетах. Это представляет некоторую дополнительную нагрузку на пакет в зависимости от длины порядкового номера. С 32-битным порядковым номером, использующим всю метку из 4 битов, дополнительная полоса пропускания составляет только 4% для коротких пакетов длиной в 100 битов.

c) Показатели потерь предлагаемой услуги можно рассматривать следующим образом. Поскольку механизм выбора в выходном узле берет пакеты из любого из двух LSP, услуга фактически может компенсировать, хотя от нее это не требуется, потери пакетов в сети. В наилучшем случае это может приводить к нулевой потере, хотя каждый LSP может нести потери. С другой стороны, в наихудшем случае чистая потеря пакетов была бы суммой потерь обоих LSP. Другими словами, показатели потерь услуги не хуже и того порядка величины, как у LSP с наихудшими показателями, а иногда могут быть намного лучше.

d) Показатели задержки предлагаемой услуги можно рассматривать следующим образом. Так как алгоритм всегда выбирает первый приемлемый прибывающий пакет пары без буферизации, то эффективность задержки всегда лучше, чем у любого из двух LSP.

e) Размер окна должен быть больше, чем максимальное число последовательных пакетов, которое может потерять рабочий LSP. В результате обеспечивается, что порядковый номер следующего пакета из того же LSP всегда будет попадать в окно и будет принят.

f) Размер окна должен быть таким, чтобы при отсутствии потери разница задержки пар пакетов, передаваемым по спаренным LSP, никогда не превышала бы (2^N – размер окна) пакетов. В результате гарантируется, что старый пакет не будет принят за новый, что вызвало бы ошибочную доставку.

g) В случае единичного отказа в сети, за исключением входных и выходных узлов, воздействие оказывается только на один из спаренных различных LSP. Неповрежденный LSP продолжит доставлять пакеты. Если неповрежденный LSP – это ведущий LSP, т. е. последний полученный и выбранный пакет был из этого LSP, то функция выбора в выходном узле продолжит принимать пакеты из него, если же неповрежденный LSP – это ведомый LSP, то функция выбора будет отклонять пакеты, пока не обнаружит пакет, чей порядковый номер попадает в скользящее окно. После успешного восстановления отказавшего LSP он при желании может быть вновь введен в действие. При этом "возвращаемом режиме восстановления" простейший подход состоял бы в том, чтобы первый переданный методом двойной передачи пакет получил бы обычный порядковый номер, следующий за номером, присвоенным последнему пакету, поданному только по неповрежденному LSP. При желании можно произвести различные усовершенствования для управления показателями потерь услуги в течение такой операции.

h) Если отказали оба LSP, следует определить дополнительные механизмы поддержки услуги и соответствующих состояний LSP, чтобы обеспечить надежность операций.

Добавление III

Справочная литература

IETF, RFC 3469 (2003), *Структура для восстановления на базе MPLS*, *Категория: Информационная*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия B	Средства выражения: определения, символы, классификация
Серия C	Общая статистика электросвязи
Серия D	Общие 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, звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, установка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническая эксплуатация сетей: международные системы передачи, телефонные каналы, телеграфные, факсимильные и арендованные каналы
Серия N	Техническая эксплуатация: 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 и взаимосвязь открытых систем
Серия Y	**Глобальная информационная инфраструктура, аспекты протокола Интернет и сети следующего поколения**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2004 г.