

# МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

# G.873.1

(03/2006)

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

Цифровые сети – Оптические транспортные сети

---

**Оптическая транспортная сеть (OTN):  
Линейная защита**

Рекомендация МСЭ-Т G.873.1

## 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 И ОПТИЧЕСКИХ СИСТЕМ	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
<b>Оптические транспортные сети</b>	<b>G.870–G.879</b>
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
АСПЕКТЫ ПЕРЕДАЧИ ПАКЕТОВ ПО ТРАНСПОРТНЫМ СЕТЯМ	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.873.1

### Оптическая транспортная сеть (OTN): Линейная защита

#### Резюме

В данной Рекомендации определяется протокол APS (автоматическое защитное переключение) и защита операции коммутации для схем линейной защиты для Оптической транспортной сети на уровне Блока данных оптического канала (ODUk). В данной Рекомендации рассмотрены следующие схемы защиты:

- защита соединения подсети ODUk с самоконтролем (1+1, 1:n);
- защита соединения подсети ODUk с контролем, не меняющим основной режим работы (1+1);
- защита соединения подсети ODUk с контролем в подуровне (1+1, 1:n).

#### Источник

Рекомендация МСЭ-Т G.873.1 утверждена 15-й Исследовательской комиссией МСЭ-Т 29 марта 2006 г. (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т А.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.

© ITU 2009

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких-либо средств без предварительного письменного разрешения МСЭ.

## СОДЕРЖАНИЕ

	Стр.
1 Сфера применения .....	1
2 Справочная литература.....	1
3 Определения .....	1
4 Сокращения .....	2
5 Характеристики защиты .....	2
5.1 Условия и методы контроля.....	2
6 Команды для группы защиты.....	3
6.1 Сквозные команды и состояния .....	3
6.2 Местные команды .....	4
7 Архитектуры защиты.....	4
7.1 Однонаправленная и двунаправленная коммутация.....	5
7.2 Необходимость использования канала APS/PCC.....	5
7.3 Обратимая и необратимая коммутация.....	5
7.4 Несоответствия при инициализации .....	6
8 Протокол APS.....	6
8.1 Формат канала APS .....	6
8.2 Передача и принятие протокола APS.....	7
8.3 Тип запроса .....	7
8.4 Типы защиты.....	8
8.5 Сигнал запроса.....	9
8.6 Сигнал мостового соединения .....	9
8.7 Проверка моста.....	9
8.8 Проверка селектора.....	9
8.9 Сигнал неисправности объекта защиты.....	10
8.10 Запросы равенства приоритетов .....	10
8.11 Команда принятия и удержания.....	10
8.12 Таймер отложенного срабатывания (Hold-off).....	10
8.13 Операция Выполнить .....	11
8.14 Сигнал тревоги для канала APS.....	11
Приложение I – Примеры функционирования .....	11
I.1 Однонаправленная коммутация 1+1.....	11
I.2 Двунаправленная коммутация 1+1 .....	13
I.3 Двунаправленная коммутация 1:n .....	14
I.4 Операция команды Выполнить .....	15



# Рекомендация МСЭ-Т G.873.1

## Оптическая транспортная сеть (OTN): Линейная защита

### 1 Сфера применения

В данной Рекомендации определяется протокол APS (автоматическое защитное переключение) и операция коммутации защиты для схем линейной защиты для Оптической транспортной сети на уровне Блока данных оптического канала (ODUk). В данной Рекомендации рассмотрены следующие схемы линейной защиты:

- защита соединения подсети ODUk с самоконтролем (1+1, 1:n);
- защита соединения подсети ODUk с контролем, не меняющим основной режим работы (1+1);
- защита соединения подсети ODUk с контролем в подуровне (1+1, 1:n).

Протокол APS и защита операции коммутации для защиты кольца OTN находятся в настоящее время на стадии изучения.

### 2 Справочная литература

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другая справочная литература являются предметом корректировки, в связи с чем пользователям данной Рекомендации настоятельно рекомендуется изыскать возможность для использования самых последних изданий Рекомендации и справочной литературы, перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему как отдельному документу статуса Рекомендации.

- ITU-T Recommendation G.709/Y.1331 (2003), *Interfaces for the Optical Transport Network (OTN)*.
- ITU-T Recommendation G.798 (2004), *Characteristics of optical transport network hierarchy equipment functional blocks*.
- ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.
- ITU-T Recommendation G.806 (2006), *Characteristics of transport equipment – Description methodology and generic functionality*.
- ITU-T Recommendation G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection*.
- ITU-T Recommendation G.841 (1998), *Types and characteristics of SDH network protection architectures*.
- ITU-T Recommendation G.872 (2001), *Architecture of optical transport networks*.

### 3 Определения

В этой Рекомендации определены следующие термины:

- 3.1 канал APS:** См. Рек. МСЭ-Т G.870/Y.1352.
- 3.2 объект:** См. Рек. МСЭ-Т G.870/Y.1352.
- 3.3 сигнал дополнительного трафика:** См. Рек. МСЭ-Т G.870/Y.1352.
- 3.4 головной узел сети:** См. Рек. МСЭ-Т G.870/Y.1352.
- 3.5 сигнал обычного трафика:** См. Рек. МСЭ-Т G.870/Y.1352.

- 3.6 нулевой сигнал: См. Рек. МСЭ-Т G.870/Y.1352.
- 3.7 канал защиты связи: См. Рек. МСЭ-Т G.870/Y.1352.
- 3.8 группа защиты: См. Рек. МСЭ-Т G.870/Y.1352.
- 3.9 сигнал: См. Рек. МСЭ-Т G.870/Y.1352.
- 3.10 хвостовая часть: См. Рек. МСЭ-Т G.870/Y.1352.

## 4 Сокращения

В этой Рекомендации используют следующие сокращения:

APS	Automatic Protection Switching	Автоматическая коммутация защиты
DNR	Do Not Revert	Не возвращаться в предшествующее состояние
EXER	Exercise	Выполнить
FS	Forced Switch	Подключить принудительно
LO	Lockout for protection	Блокировать для защиты
MS	Manual Switch	Подключить вручную
NR	No Request	Отсутствие запроса
ODUk	Optical Channel Data Unit k	Блок данных k оптического канала
OTN	Optical Transport Network	Оптическая транспортная сеть
OTUk	Optical Channel Transport Unit k	Транспортный блок k оптического канала
PCC	Protection Communication Channel	Канал защиты связи
RR	Reverse Request	Запрос на возврат в предшествующее состояние
SD	Signal Degrade	Ухудшение качества сигнала
SF	Signal Fail	Пропадание сигнала
WTR	Wait-to-Restore	Ожидать восстановления

## 5 Характеристики защиты

### 5.1 Условия и методы контроля

Коммутация защиты будет происходить при обнаружении определенных дефектов на транспортируемых объектах (рабочих или защитных) в пределах защищаемой области. Способы обнаружения этих дефектов являются предметом рассмотрения для Рекомендаций, относящихся к оборудованию (например, Рек. МСЭ-Т G.806 и G.798). Для контроллера коммутации защиты объект в защищаемой области может иметь следующие состояния: не имеющий дефектов = ОК, ухудшенный (с ухудшенным качеством сигнала = SD), или поврежденный (пропадание сигнала = SF).

Обычными методами контроля являются следующие:

*Самоконтроль* – Коммутация защиты включается при обнаружении дефектов на линии подключения ODUk (например, при выполнении адаптации хвостовой части уровня сервера и сервер/блок ODUk). На самом уровне блока ODUk обнаружение дефектов не производится.

**ПРИМЕЧАНИЕ.** – В противоположность соединению SNC/I в иерархии SDH, в случае SNC/I в блоке ODUk можно протянуть только одиночную линию связи, т. к. дефект интерфейса FDI, являющийся результатом последующих дефектов уровня сервера восходящего потока, не обнаруживается в процессе адаптации сервер/блок ODUk.

*Без изменения режима работы* – Коммутация защиты включается с помощью контрольного устройства, не меняющего режим работы, на уровне ODUkP или подуровнях ODUkT в конце хвостовой части группы защиты.



*Подуровень* – Коммутация защиты включается при обнаружении дефектов в хвостовой части подуровня ODUk (TCM). Хвостовая часть подуровня ODUkT устанавливается для каждого рабочего объекта или объекта защиты. Коммутация защиты, таким образом, включается только из-за дефектов в защищаемой области.

Для контроллера коммутации защиты не имеет значения, какой именно метод контроля используется, при условии, что ему может быть предоставлена информация (OK, SD, SF) для транспортируемых объектов в пределах защищаемой области. У некоторых контрольных устройств или уровней сети может отсутствовать метод обнаружения SD. Там, где дело обстоит именно так, нет необходимости использовать другой протокол APS – может просто случиться так, что SD нельзя будет получить от оборудования, которое не может его обнаружить. Там, где используется протокол APS, реализация не должна препятствовать заявлениям дальнего конца линии и SD по всему каналу APS, даже если контрольное устройство на ближнем конце линии не может обнаружить SD.

## **6 Команды для группы защиты**

### **6.1 Сквозные команды и состояния**

В этом пункте описываются команды, которые применяются к группе защиты в целом. Если присутствует APS, то эти команды передаются сигналами на дальний конец линии связи. При двунаправленной коммутации эти команды воздействуют на мост и селектор с обоих концов.

*Блокировать для защиты* – Эта команда предотвращает отбор рабочего сигнала от объекта защиты. Она фактически блокирует группу защиты. Сигнал дополнительного трафика, если таковой присутствует на объекте защиты, отбрасывается.

*Принудительно подключить сигнал обычного трафика #n к защите* – Сигнал обычного трафика #n должен быть принудительно снят с объекта защиты после того, как появится требуемый мост.

*Принудительно подключить нулевой сигнал* – Для архитектур 1:n она подключает нулевой сигнал к объекту защиты, если не действует команда коммутации с равным или более высоким приоритетом. Сигнал обычного трафика, присутствующий на объекте защиты, передается к его рабочему объекту и снимается с него. Для архитектур 1+1 она снимает сигнал обычного трафика с рабочего объекта.

*Принудительно подключить сигнал дополнительного трафика* – Она подключает сигнал дополнительного трафика к объекту защиты, если не действует команда коммутации с равным или более высоким приоритетом. Сигнал обычного трафика, присутствующий на объекте защиты передается к его рабочему объекту и снимается с него.

*Подключить вручную сигнал обычного трафика #n к защите* – В отсутствии сбоя в работе объекта защиты, она инициирует снятие Сигнала обычного трафика #n с объекта защиты после того, как появится требуемый мост.

*Подключить вручную нулевой сигнал* – Для архитектур 1:n она подключает нулевой сигнал к объекту защиты, если не действует команда коммутации с равным или более высоким приоритетом. Сигнал обычного трафика, присутствующий на объекте защиты, передается к его рабочему объекту и снимается с него. Для архитектур 1+1 она снимает сигнал обычного трафика с рабочего объекта.

*Подключить вручную сигнал дополнительного трафика* – Она подключает сигнал дополнительного трафика к объекту защиты, если не действует команда коммутации с равным или более высоким приоритетом. Сигнал обычного трафика, присутствующий на объекте защиты передается к его рабочему объекту и снимается с него.

*Ожидать восстановления сигнала обычного трафика #n* – В обратимых операциях, после обнуления сигналов SF или SD на рабочем объекте #n, Сигнал обычного трафика #n сохраняется в качестве снимаемого с объекта защиты до тех пор, пока не закончится время таймера Ожидать восстановления. Если время таймера закончится до любого другого события или команды, то состояние будет изменено на NR. Это условие используется, для того чтобы предотвратить частое срабатывание селектора на случай перемежающихся отказов.

*Сигнал Выполнить #n* – Выполнить протокол APS. Сигнал выбирается таким образом, чтобы не изменять селектор.

*Не возвращать сигнал обычного трафика #n* – В необратимой операции эта команда используется для поддержания сигнала обычного трафика, снимаемого с объекта защиты.

*Отсутствие запроса* – Все сигналы обычного трафика снимаются с их соответствующих рабочих транспортных объектов. Объект защиты переносит нулевой сигнал, дополнительный трафик или мост одного сигнала обычного трафика в группу защиты 1+1.

*Обнулить* – Обнуляет действующие команды Блокировать защиту, Подключить принудительно, Подключить вручную, состояние WTR, или команду Выполнить от ближнего конца линии.

## 6.2 Местные команды

Эти команды применимы только к ближнему концу линии группы защиты. Если присутствует APS, значит о них не было сообщено на дальний конец линии через канал APS.

*Фиксировать* – Фиксирует состояние группы защиты. До тех пор, пока фиксация не обнулится, добавочные команды ближнего конца линии отклоняются. Изменения условий и принятые байты APS не учитываются. Если команда Фиксировать обнуляется, то состояние группы защиты пересчитывается в зависимости от условия и принятых байтов APS.

*Обнулить фиксацию*

*Блокировать сигнал обычного трафика #n от защиты* – Не допускает снятие Сигнала обычного трафика #n с объекта защиты. Команды для Сигнала обычного трафика #n будут отклонены. Команды SF или SD для Сигнала обычного трафика #n не будут учитываться. При двунаправленной коммутации 1:n, запросы от удаленных мостов для Сигнала обычного трафика #n будут выполняться, чтобы не допустить сбоев протокола. В результате Сигнал нормального трафика должен быть заблокирован от защиты с обоих концов, чтобы не допустить его снятия с объекта защиты из-за команды или сбоя в любом конце линии. Множество таких команд могут сосуществовать для разных Сигналов обычного трафика.

*Обнулить блокировку сигнала обычного трафика #n от защиты*

## 7 Архитектуры защиты

В архитектуре линейной защиты защитная коммутация происходит на двух различных конечных точках защищенной хвостовой части или защищенного соединения подсети. Между этими конечными точками будут находиться как "рабочие" объекты, так и объекты "защиты".

Для заданного направления передачи данных "головной узел" сигнала защиты способен выполнять функции моста, который будет размещать копию сигнала обычного трафика на объекте защиты, когда это потребуется. "Хвостовая часть" будет выполнять функцию селектора там, где он способен снять сигнал обычного трафика с его обычного рабочего объекта, или с объекта защиты. В случае двунаправленной передачи данных, где защищены оба направления передачи, оба конца защищенного сигнала будут обеспечивать функции как моста, так и селектора.

Возможны следующие архитектуры:

**1+1** – В архитектуре 1+1 один сигнал обычного трафика защищен одним объектом защиты. Мост в головном узле является постоянным. Коммутация происходит полностью на конце хвостовой части.

**1:n** – В архитектуре 1:n, 1 или более сигналов обычного трафика защищены одним объектом защиты. Мост в головном узле не устанавливается до тех пор, пока требуется включение защиты. В случае, если  $n > 1$ , неизвестно, какой из сигналов обычного трафика должен быть установлен с помощью моста на объект защиты, пока не обнаружится дефект на одном из защищенных сигналов. В архитектурах 1:n есть возможность переносить сигнал дополнительного (с низким приоритетом, вытесняемого) трафика на объект защиты, если он не используется для защиты какого-либо сигнала обычного трафика. Архитектура 1:n может использоваться даже для  $n = 1$  (1:1). Она может быть предпочтительней, чем более простая архитектура 1+1 (которой не требуются никакие действия в головном узле алгоритма защиты), т. к. 1:1 способна переносить дополнительный трафик там, где архитектура 1+1 этого сделать не может.

**m:n** – В этой архитектуре, m объектов защиты используются, для того чтобы защитить n рабочих объектов. Эта архитектура требует дальнейшего изучения.

Если предположить, что канал APS большего размера, то при кодировании для объекта с номером "n" потребуется целый байт, а не несколько битов в SDH. Два из 256 значений зарезервированы: 0 используется, для того чтобы указать на нулевой сигнал или объект защиты, а 0xFF (255) используется, для того чтобы указать на дополнительный трафик.

Архитектура с каждой стороны соединения должна быть согласована.

### **7.1 Однонаправленная и двунаправленная коммутация**

В случае двунаправленной передачи данных можно выбрать однонаправленную или двунаправленную коммутацию. При однонаправленной коммутации селекторы с каждой стороны полностью независимы. При двунаправленной коммутации предпринимается попытка согласовать два конца таким образом, чтобы у обоих были одинаковые установочные параметры моста и селектора, даже при однонаправленном сбое. Для двунаправленной коммутации всегда требуется канал APS и/или PCC, чтобы согласовать две конечные точки. Однонаправленная коммутация может предотвратить два однонаправленных сбоя в противоположных направлениях на разных объектах.

### **7.2 Необходимость использования канала APS/PCC**

Единственный тип коммутации, которому НЕ требуется канал APS и/или PCC, – это однонаправленная коммутация 1+1. С постоянным мостом в головном узле и при отсутствии необходимости согласования положения селектора с двух концов, селектором конца хвостовой части можно управлять исключительно на основании дефектов и команд, принятых на конце хвостовой части.

Двунаправленной коммутации всегда требуется канал APS. Однонаправленной коммутации 1:n требуется канал APS для координации моста головного узла с селектором конца хвостовой части.

### **7.3 Обратимая и необратимая коммутация**

При обратимом процессе трафик возвращается к рабочим объектам, после устранения причины коммутации. В случае обнуления команды (например, Подключить принудительно), это происходит немедленно. В случае устранения дефекта, это обычно происходит после того, как закончится время таймера "Ожидать восстановления", который используется, для того чтобы избежать дрожания селекторов в случае перемежающихся дефектов.

При необратимом процессе обычный трафик может сохраняться на объекте защиты даже после устранения причины коммутации. Этот процесс обычно завершается заменой предыдущего запроса на коммутацию запросом "Не возвращаться в предшествующее состояние (DNR)", который имеет низкий приоритет.

Защита 1+1 часто обеспечивается как необратимая, так как защита полностью специализирована в любом случае, и это позволяет избежать повторного "аппаратного сбоя" в трафике. Однако возможно существуют причины, для того чтобы сделать эту защиту обратимой (например, для того чтобы трафик пользовался "коротким" направлением по кольцу, за исключением неисправных состояний. Определенным стратегиям оператора также требуется обратимый процесс даже для 1+1).

Обычно защита 1:n является обратимой. Разумеется, в тех случаях, когда происходит перенос сигнала дополнительного трафика на объект защиты, процесс всегда будет обратимым, для того чтобы отложенный сигнал дополнительного трафика мог быть восстановлен. Конечно, можно определить протокол таким образом, чтобы сделать возможным использование необратимого процесса для защиты 1:n, но предполагается, что лучше вернуть и застопорить трафик, когда рабочий объект восстанавливается, чем когда какой-либо другой объект группы дает сбой, что требует использования объекта защиты для переноса другого сигнала обычного трафика.

Вообще выбор обратимого/необратимого будет одинаковым с обоих концов группы защиты. Однако несогласованность этого параметра не препятствует взаимодействию – просто будет необычно, если одна сторона обратится к WTR для обнуления коммутаций, инициированных с этой стороны, в то время как другая обратится к DNR за своими коммутациями. См. также 8.4.

## 7.4 Несоответствия при инициализации

Во всех опциях для инициализации групп защиты существуют возможности для несогласованности между инициализацией с двух концов линии. Эти несоответствия инициализации принимают одну из нескольких форм:

- Несоответствия, где правильная работа невозможна.
- Несоответствия, где одна или обе стороны могут адаптировать свою работу для обеспечения какой-то степени взаимодействия, несмотря на несогласованность.
- Несоответствия, которые не препятствуют взаимодействию. Примером является несогласованность: обратимый/необратимый, рассмотренная в п. 8.4.

Не все несоответствия при инициализации могут быть переданы и обнаружены с помощью информации, прошедшей по каналу APS. С потенциальным количеством до 254 рабочих объектов включительно в одной группе защиты 1:n, существует слишком много комбинаций допустимого количества объектов, для того чтобы обеспечить полную видимость всех опций конфигурации. Однако действительно желательно обеспечить видимость для средней категории, где стороны могут адаптировать свою работу для взаимодействия, несмотря на несогласованность. Например, оборудование, оснащенное для двусторонней коммутации, может перейти на более низкий уровень односторонней коммутации, чтобы сделать взаимодействие возможным. Оборудование, оснащенное для коммутации 1+1 с каналом APS, может перейти на более низкий уровень, чтобы работать в односторонней коммутации 1+1 без канала APS. Пользователь по-прежнему может быть уведомлен о несоответствии при инициализации, но уровень защиты все же будет обеспечен этим оборудованием.

## 8 Протокол APS

### 8.1 Формат канала APS

Канал APS переносится первыми тремя байтами поля APS/PCC служебных сигналов блока ODUk. Четвертый байт поля APS/PCC зарезервирован. Имеются в наличии восемь независимых каналов APS для поддержания защиты ODUkP, шести уровней ODUkT (TCM) и одного уровня защиты SNC/I блока ODUk, как определено в 15.8.2.4/G.709/Y.1331.

Формат самих четырех байтов APS в пределах каждого кадра определен на Рисунке 1. Значения поля для каналов APS определены в Таблице 1.

1				2				3				4											
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Запрос/ состояние				Тип защиты				Сигнал запроса				Сигнал мостового соединения				Зарезервировано							
				A	B	D	R																

Рисунок 1/G.873.1 – Формат канала APS

**Таблица 1/G.873.1 – Значения поля для канала APS**

Поле		Значение	Описание
Запрос/Состояние		1111	Блокировка защиты (LO)
		1110	Подключить принудительно(FS)
		1100	Пропадание сигнала (SF)
		1010	Ухудшение качества сигнала (SD)
		1000	Подключить вручную(MS)
		0110	Ожидать восстановления (WTR)
		0100	Выполнить (EXER)
		0010	Запрос на возврат в предшествующее состояние (RR)
		0001	Не возвращаться в предшествующее состояние (DNR)
		0000	Отсутствие запроса (NR)
		Другие	Зарезервировано для будущей международной стандартизации
Тип защиты	A	0	Нет канала APS
		1	Канал APS
	B	0	(Постоянный мост)
		1	(нет Постоянного моста) 1:n
	D	0	Однонаправленное переключение
		1	Двунаправленное переключение
	R	0	Необратимый процесс
		1	Обратимый процесс
Запрашиваемый сигнал		0	Нулевой сигнал
		1–254	Сигнал обычного трафика 1–254
		255	Сигнал дополнительного трафика
Сигнал мостового соединения		0	Нулевой сигнал
		1–254	Сигнал обычного трафика 1–254
		255	Сигнал дополнительного трафика

## 8.2 Передача и принятие протокола APS

Протокол APS/PCC передается через объект защиты. Хотя их можно передать таким же образом на рабочие объекты, приемники не должны допускать этого и не должны учитывать эту информацию на рабочих объектах.

Процесс независимого приема должен быть выполнен для каждого из восьми уровней. Так как протокол APS переносится только первыми тремя байтами четырехбайтного канала APS/PCC, то только эти три байта учитываются в процессе приема. Новое значение протокола APS должно быть принято, если идентичное значение получено в этих трех байтах данного уровня последовательно три раза.

**ПРИМЕЧАНИЕ.** – Так как четвертый байт сообщения APS "зарезервирован", то он не должен учитываться в процессе приема байтов APS.

## 8.3 Тип запроса

Типы запросов, которые могут быть отражены в байтах AP, являются "стандартными" типами, традиционно поддерживаемыми коммутацией защиты для SONET и SDH. В этих запросах отражен самый высокий приоритет условия, команды или состояния (см. Таблицы 2 и 3). В случае однонаправленной коммутации это значение самого высокого приоритета, установленное только со стороны ближнего конца линии связи. При двунаправленной коммутации местный запрос будет указан только в том случае, когда он имеет такой же высокий приоритет или выше, чем любой другой запрос, принятый от дальнего конца линии связи по каналу APS. При двунаправленной коммутации,

если запрос от дальнего конца линии связи имеет самый высокий приоритет, то ближний конец линии связи будет подавать сигнал Запрос на возврат в предшествующее состояние.

**Таблица 2/G.873.1 – Приоритеты запрос/состояние с протоколом APS**

Запрос/состояние	Приоритет
Блокировка для защиты (LO)	1 (высший)
Пропадание сигнала (SF) – защита	2 (см. 8.9)
Подключить принудительно (FS)	3
Пропадание сигнала (SF) – рабочее	4
Ухудшение качества сигнала (SD)	5
Подключить вручную (MS)	6
Ожидать восстановления (WTR)	7
Выполнить (EXER)	8
Запрос на возврат в предшествующее состояние (RR)	9
Не возвращаться в предшествующее состояние (DNR)	10
Отсутствие запроса (NR)	11 (низший)

**Таблица 3/G.873.1 – Приоритеты запрос/состояние без протокола APS**

Запрос/состояние	Приоритет
Блокировка для защиты (LO)	1 (высший)
Подключить принудительно(FS)	2
Пропадание сигнала (SF)	3
Ухудшение качества сигнала (SD)	4
Подключить вручную (MS)	5
Ожидать восстановления (WTR)	6
Не возвращаться в предшествующее состояние (DNR)	7
Отсутствие запроса (NR)	8 (низший)

#### 8.4 Типы защиты

Действующими Типами защиты являются:

- 000x Однонаправленный 1+1, нет APS
- 100x Однонаправленный 1+1 с/APS
- 101x Двухнаправленный 1+1 с/APS
- 110x Однонаправленный 1:n с/APS
- 111x Двухнаправленный 1:n с/APS

Значения выбираются таким образом, чтобы значение по умолчанию (все нули) соответствовало только одному типу защиты, который может работать без канала APS (Однонаправленный 1+1).

Заметим, что 010x, 001x, и 011x являются недействующими, т. к. 1:n и Двухнаправленный типы требуют APS.

Если бит "B" не соответствует, то селектор разъединяется, т. к. 1:n и 1+1 несовместимы. Это приведет к появлению сигнала тревоги.

При условии, что бит "B" соответствует:

Если бит "A" не соответствует, то предполагается, что на этой стороне APS перейдет на более низкий уровень однонаправленной коммутации 1+1 без APS.

ПРИМЕЧАНИЕ 1. – В том случае, если узел не поддерживает канал APS, то в поле APS/PCC будет присутствовать модель, состоящая из всех нулей, как это определено в пункте 15/G.709/Y.1331.

Если бит "D" не соответствует, то двунаправленная сторона перейдет на более низкий уровень однонаправленной коммутации.

Если бит "R" не соответствует, то, с одной стороны, произойдет обнуление переключателей в "WTR", а, с другой стороны, произойдет обнуление в "DNR". Две стороны будут взаимодействовать, и трафик будет защищен.

ПРИМЕЧАНИЕ 2. – Каждая сторона всегда подает сигнал о своих максимальных возможностях в поле типа защиты, даже если она переходит на более низкий уровень, чтобы работать с меньшими возможностями (например, сторона, которая поддерживает двунаправленную коммутацию, переходит на более низкий уровень, чтобы работать как однонаправленный коммутатор на случай взаимодействия со стороной, которая поддерживает только однонаправленную коммутацию, но все же подает сигнал "1" в бите "D").

ПРИМЕЧАНИЕ 3. – Сообщения об условиях несоответствия отложены для дальнейшего изучения.

## 8.5 Сигнал запроса

Он указывает сигнал, который требуется перенести для ближнего конца линии связи посредством объектом защиты. Для запроса NR это или Нулевой сигнал (0), или Сигнал дополнительного трафика (255). Для запроса LO это может быть только Нулевой сигнал (0). Для запроса Выполнить это может быть Нулевой сигнал (0) или Сигнал дополнительного трафика (255), если запрос Выполнить заменяет запрос NR, или численное значение сигнала обычного трафика в случае, если запрос Выполнить заменяет DNR. Для запросов SF или SD это будет численное значение сигнала обычного трафика, или Нулевой сигнал (0), чтобы указать на то, что защита нарушена или ее характеристики ухудшились. Для всех других запросов это будет численное значение сигнала обычного трафика, который нужно перенести посредством объекта защиты.

## 8.6 Сигнал мостового соединения

Он указывает сигнал, который подключается с помощью моста на объект защиты. Для защиты 1+1 он всегда должен указывать сигнал обычного трафика 1, точно отражая постоянное мостовое соединение. Это дает возможность 2-х фазной, а не 3-х фазной коммутации в случае архитектуры 1+1. Для защиты 1:n он будет указывать, что в действительности подсоединено с помощью моста к объекту защиты (Нулевой сигнал (0), Дополнительный трафик (255) или численное значение сигнала обычного трафика). В общем случае это будет мостовое соединение, запрашиваемое дальним концом линии связи.

## 8.7 Проверка моста

В архитектурах 1+1 сигнал обычного трафика постоянно подключен с помощью моста к защите. Численное значение "1" сигнала обычного трафика всегда будет указываться в поле сигнала мостового соединения канала APS.

В архитектурах 1:n мост будет установлен в ту, которая указывается с помощью поля "Сигнал запроса" входного канала APS. Когда мост установлен, то это указывается в поле "Сигнал мостового соединения" выходного канала APS.

## 8.8 Проверка селектора

В Однонаправленных архитектурах 1+1 (с каналом APS или без него) селектор устанавливается целиком в соответствии с местным запросом наивысшего приоритета. Эта однофазная коммутация.

В Двунаправленных архитектурах 1+1 сигнал обычного трафика будет сниматься с объекта защиты, если оба: выходной "Сигнал запроса" и входной "Сигнал мостового соединения" указывают сигнал обычного трафика "1" (Входной "Сигнал мостового соединения" должен всегда указывать "1" в этой архитектуре). Это двухфазная коммутация, т. к. дальний конец линии связи не переключится до тех пор, пока не поступят байты APS, указывающие на то, что двунаправленная коммутация инициируется дальним концом линии связи.

В одно- или двунаправленных архитектурах 1:n сигнал обычного трафика "n" или сигнал дополнительного трафика 255 будут сниматься с объекта защиты, если то же самое число "n" (или 255) появится в полях как выходного "Сигнала запроса", так и входного "Сигнала мостового соединения". Это приводит в общем случае к трехфазной коммутации.

### **8.9 Сигнал неисправности объекта защиты**

Сигнал неисправности на объекте защиты имеет более высокий приоритет, чем любой дефект, который вызвал бы снятие сигнала обычного трафика с объекта защиты. Для случая, когда используется сигнал APS, команда SF на объекте защиты (через который проходит сигнал APS) имеет приоритет над командой Переключить принудительно. Команда блокировки имеет более высокий приоритет, чем SF. При сбое состояние блокировки должно поддерживаться в активном состоянии.

### **8.10 Запросы равенства приоритетов**

В общем случае, если коммутация по запросу совершена, то она не может быть отменена другим запросом с тем же приоритетом (первым пришел, первым обслужен). Если запросы с равными приоритетами приходят одновременно, то конфликт разрешается в пользу запроса от объекта с наименьшим номером. При двунаправленной коммутации запрос, поступивший по каналу APS от объекта с меньшим номером, будет всегда превосходить идентичный приоритет местного запроса от объекта с большим номером. Оба запроса с равным приоритетом и одинаковым номером объектов, поступившие с двух сторон двунаправленной группы защиты, считаются действующими и эквивалентны получению команды "RR" с места обработки данных на ближнем конце линии связи.

### **8.11 Команда принятия и удержания**

Команды CLEAR, LO, FS, MS, EXER принимаются или отвергаются в контексте предшествующих им команд, состояний рабочих объектов и объектов защиты в группе защиты, и (только для двунаправленной коммутации) принятых байтов APS.

Команда CLEAR является действующей только тогда, когда применяется команда LO, FS, MS или EXER на ближнем конце линии связи, или когда на нем присутствует состояние WTR, и отвергается в остальных случаях. Эта команда заменит команду ближнего конца линии связи или состояние WTR, разрешая следующее состояние с более низким приоритетом, или (в двунаправленной коммутации) утврждая запрос APS.

Другие команды отвергаются, если у них нет более высокого приоритета, чем у ранее появившейся команды, состояния или (в двунаправленной коммутации) запроса APS. Если принимается новая команда, то пренебрегают любой предыдущей командой с более низким приоритетом, который превзойден. Если команда с более высоким приоритетом превосходит состояние с более низким приоритетом или (в двунаправленной коммутации) запрос APS, то другой запрос будет подтвержден, если он еще присутствует на момент обнуления команды.

Если приоритет команды превзойден состоянием или (в двунаправленной коммутации) запросом APS, то такой командой пренебрегают.

### **8.12 Таймер отложенного срабатывания (Hold-off)**

Для синхронизации переключений защиты на большом количестве уровней или в каскадах областей защиты может потребоваться таймер отложенного срабатывания. Цель состоит в том, чтобы дать возможность коммутатору защиты уровня сервера определить местоположение сбоя до переключения на уровень клиента, или дать разрешение области защиты восходящего потока переключиться до подключения области нисходящего потока (например, дать разрешение кольцу восходящего потока переключиться раньше кольца нисходящего потока во взаимосвязанной конфигурации двойного узла таким образом, чтобы переключение произошло в том же кольце, что и сбой).

В каждой группе защиты должен быть временный таймер отложенного срабатывания. Предлагаемый диапазон и значения: 0, 20 мс, и 100 мс до 10 секунд с шагом 100 мс (с точностью  $\pm 5$  мс, согласно Рек. МСЭ-Т G.808.1).



В работе таймера отложенного срабатывания используется метод "двойного считывания", определенный в стандартах SDH. В особых случаях, если обнаружен новый или более серьезный дефект (новый SD или SF, или SD становится SF), то об этом событии не будет сообщено немедленно коммутации защиты, если значение временного таймера переключения ненулевое. Вместо этого, будет включен таймер отложенного срабатывания. Когда время таймера отложенного срабатывания закончится, то будет проверено, присутствует ли еще в хвостовой части тот дефект, который запустил таймер. Если это так, то о дефекте будет сообщено коммутации защиты. Дефект необязательно должен быть тем же дефектом, который запустил таймер.

### 8.13 Операция Выполнить

Выполнить – это команда проверки правильности работы канала APS. У нее более низкий приоритет, чем у любого "реального" запроса на переключение. Она является действующей только при двунаправленной коммутации, так как это единственное место, где вы можете получить показательный тест, отыскивая ответный сигнал.

Команда Выполнить должна выдавать команду с теми же, запрошенными и установленными с помощью моста, номерами объектов запросов NR или DNR, которые она заменяет. Действующим ответным сигналом будет RR с соответствующими, запрошенными и установленными с помощью моста, номерами объектов. Для того чтобы RR можно было обнаружить, предпочтительнее, если стандартный ответный сигнал на запрос DNR будет DNR, а не RR. Когда команда на выполнение обнуляется, то она будет заменена командой NR, если запрошенный номер объекта 0 или 255, и DNR для любого номера сигнала обычного трафика от 1 до 254.

ПРИМЕЧАНИЕ. – Операция выполнения для сети OTN определена иначе, чем операция выполнения для иерархии SDH.

### 8.14 Сигнал тревоги для канала APS

Ситуации "Сбоя протокола" для групп, требующих канал APS, являются следующими:

- Полностью несовместимое обеспечение (несоответствие бита "В"), описанное в п. 8.4.
- Отсутствие ответного сигнала на запрос об установке моста (т. е. отсутствие совместимости отправленного сигнала "Запрашиваемый объект" и полученного сигнала "Объект с мостовым соединением") в течение > 50 мс.

Если получен неизвестный запрос или запрос для недействующего номера объекта, то он не будет учитываться. Сигнал тревоги о неполучении данных от ближнего конца линии связи будет передаваться до дальнего конца линии связи.

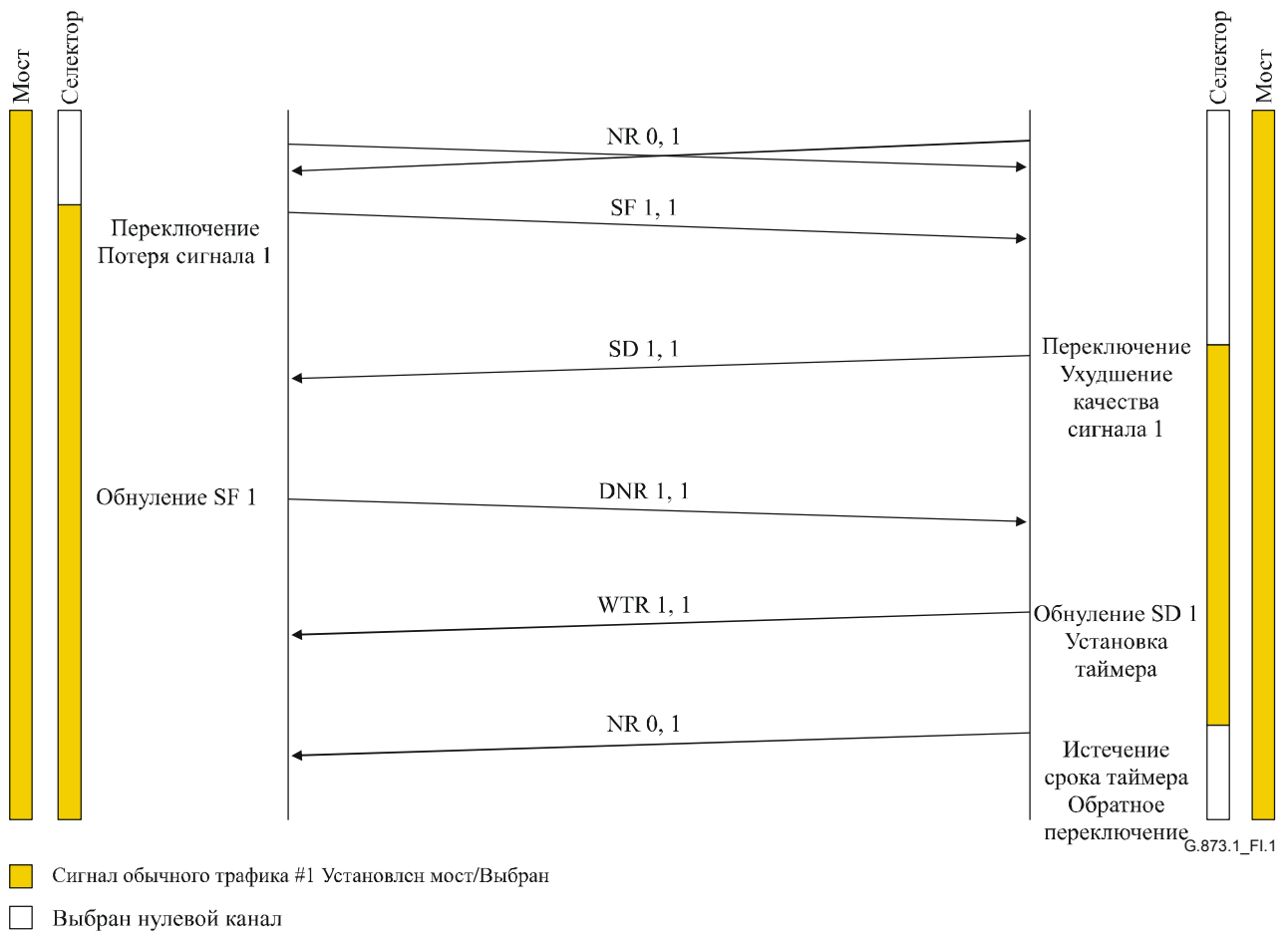
## Приложение I

### Примеры функционирования

#### I.1 Однонаправленная коммутация 1+1

Канал APS может присутствовать, а может и отсутствовать. Даже если канал APS отсутствует, мост считается постоянно установленным, поэтому переключения выполняются сразу по местному запросу. Байты APS, если они присутствуют, являются лишь информативными и не управляют работой группы защиты. Если они присутствуют, то оборудование может разрешить запрос о состоянии дальнего конца канала связи.

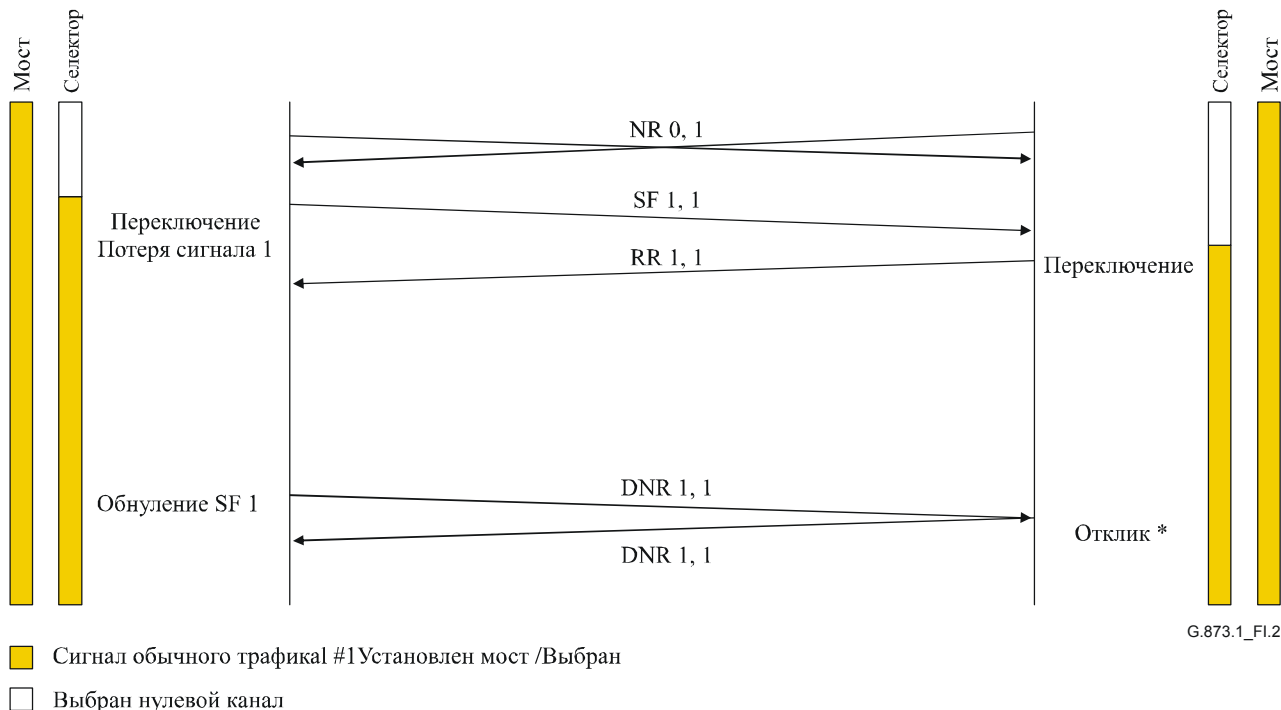
В этом примере показано наложение запросов SF и SD с противоположных сторон. Для иллюстрации в примере на Рисунке I.1 показано несовместимое обеспечение, при котором сторона А является необратимой, а сторона В является обратимой.



**Рисунок I.1/G.873.1 – Пример потока сообщений APS для однонаправленной коммутации 1+1**

## 1.2 Двухнаправленная коммутация 1+1

Пример на Рисунке 1.2 иллюстрирует двухнаправленную необратимую коммутацию 1+1. Так как постоянный мост указывается в байтах канала APS с самого начала, то коммутация может быть двухфазной вместо трехфазной.

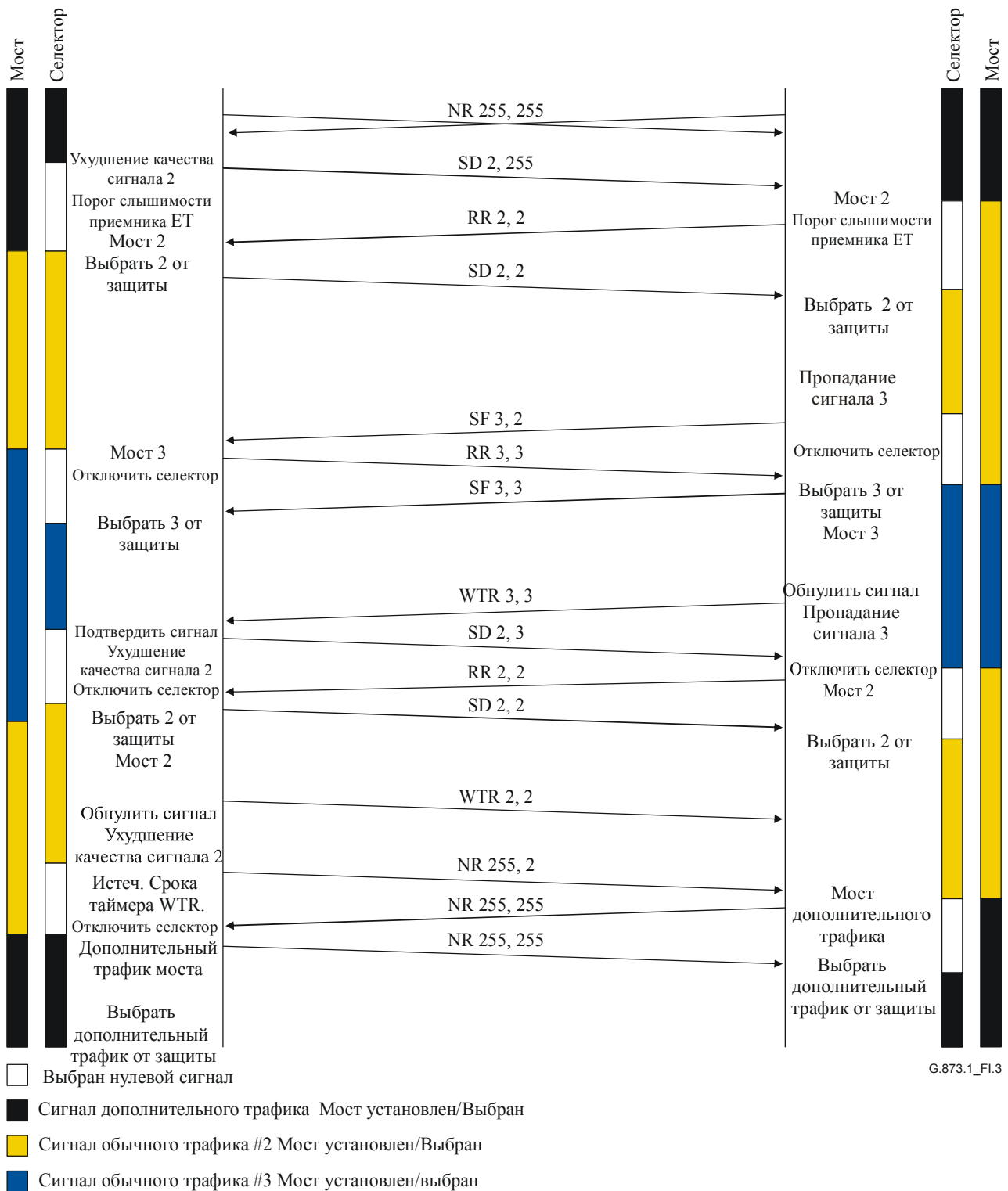


**Рисунок 1.2/G.873.1 – Пример потока сообщений APS для двухнаправленной коммутации 1+1**

**ПРИМЕЧАНИЕ.** – Исторически DNR подтверждался запросом RR. Здесь из-за того, что ответом на DNR является DNR, существенное различие в состояниях двух сторон отсутствует, а также становится возможным реализация показательного выполнения.

### I.3 Двухнаправленная коммутация 1:n

На Рисунке I.3 показан пример Двухнаправленной коммутации 1:n с дополнительным трафиком. То что здесь проиллюстрировано, это случай, в котором SD при работе #2 заменена SF при работе #3.



G.873.1\_FI.3

Рисунок I.3/G.873.1 – Пример потока сообщений APS для двухнаправленной коммутации 1:n

#### I.4 Операция команды Выполнить

Команда Выполнить – это проверка отклика дальнего конца линии связи на запрос канала APS при двунаправленной коммутации без участия селектора. У этой команды низкий приоритет, для того чтобы она не вмешивалась в действующие операции группы защиты. Она является действующей только при текущих запросах NR или DNR, т. к. ее приоритет ниже, чем у всех остальных запросов.

На Рисунках I.4, I.5, I.6 и I.7 даны примеры операции Выполнить. Во всех случаях номера объектов, как запрошенных, так и установленных с помощью моста, не меняются для команды Выполнить. Успешным откликом является прием "RR" с тем же самым номером объекта. Заметим, что если на запрос DNR приходит ответ с DNR, то это дает возможность проверить прием подходящего отклика RR на команду Выполнить.

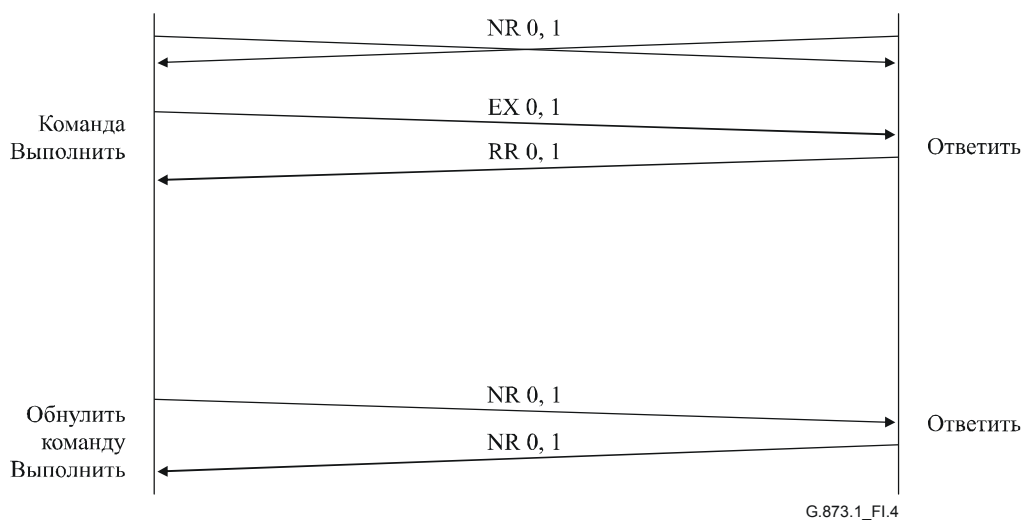


Рисунок I.4/G.873.1 – Пример команды выполнения из состояния NR 1+1

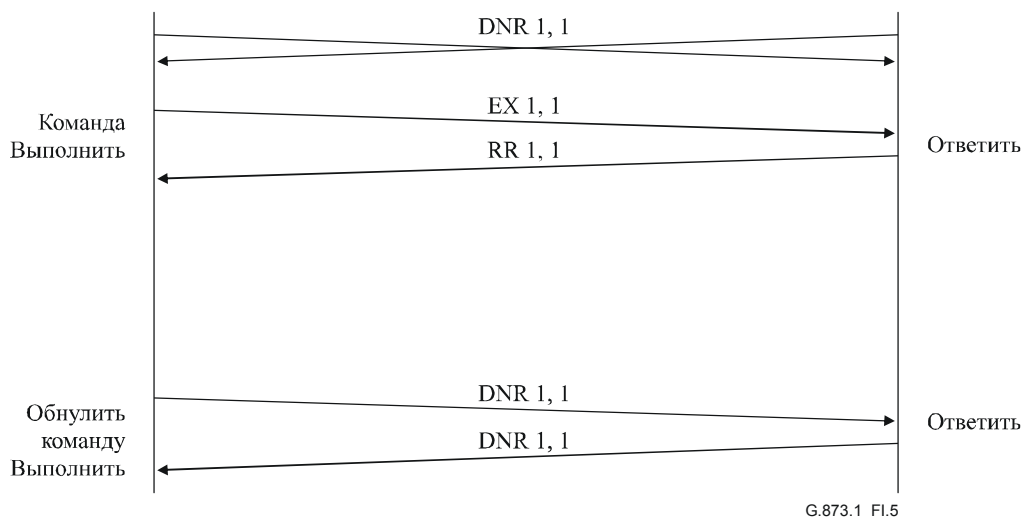
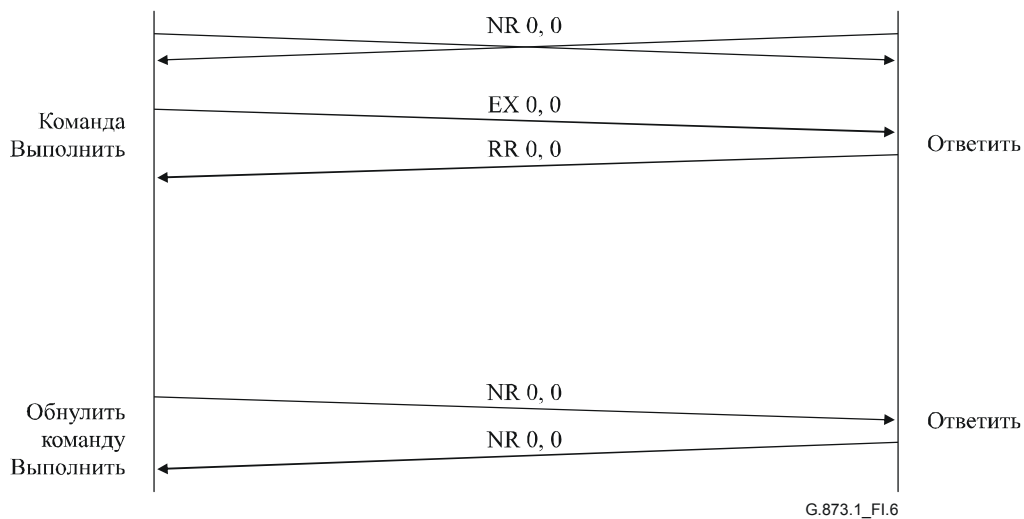
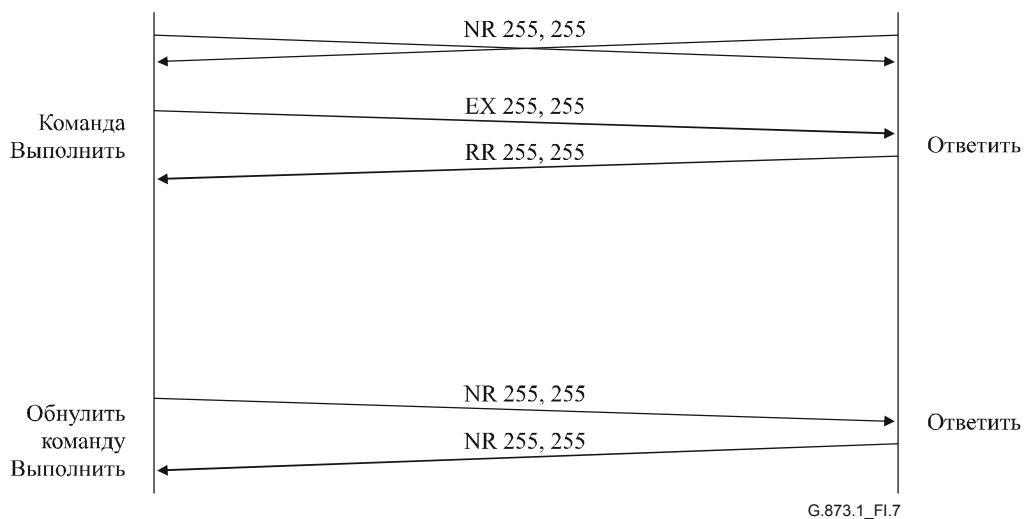


Рисунок I.5/G.873.1 – Пример команды выполнения из состояния DNR 1+1



**Рисунок I.6/G.873.1 – Пример команды выполнения из состояния NR 1:n без дополнительного трафика**



**Рисунок I.7/G.873.1 – Пример команды выполнения из состояния NR 1:n с дополнительным трафиком**



## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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
<b>Серия G</b>	<b>Системы и среда передачи, цифровые системы и сети</b>
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 протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи