

Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2614

(08/2011)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА
ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – "Умные" повсеместно
распространенные сети

**Надежность сети пакетной передачи данных
электросвязи общего пользования**

Рекомендация МСЭ-Т Y.2614

ITU-T

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, 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
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей 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
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по NGN	Y.1900–Y.1999
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699
Безопасность	Y.2700–Y.2799
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
БУДУЩИЕ СЕТИ	Y.3000–Y.3499
ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ	Y.3500–Y.3999
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА	
Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
Идентификация и безопасность	Y.4800–Y.4899
Анализ и оценка	Y.4900–Y.4999

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

Рекомендация МСЭ-Т Y.2614

Надежность сети пакетной передачи данных электросвязи общего пользования

Резюме

В Рекомендации МСЭ-Т Y.2614 определены цели, архитектура и механизмы обеспечения надежности сети пакетной передачи данных электросвязи общего пользования (PTDN), включая описание механизмов защиты линии связи, защиты трассы, обнаружения отказов сети, запуска защитного переключения и координирования защиты.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2614	06.08.2011 г.	13-я	11.1002/1000/11363

Ключевые слова

FPBN, защита линии связи, PTDN, надежность, защита трассы.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: <http://handle.itu.int/>, после которого следует уникальный идентификатор Рекомендации. Например, <http://handle.itu.int/11.1002/1000/11830-en>.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). 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 в целях 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 осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу <http://www.itu.int/ITU-T/ipr/>.

© ITU 2019

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Термины и определения	1
3.1 Термины, определенные в других документах	1
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы	2
5 Показатели надежности сети.....	3
5.1 Время переключения	3
5.2 Время удержания	3
5.3 Типы защиты	3
5.4 Типы переключения	3
5.5 Типы операций.....	3
5.6 Ручная защита	4
5.7 Критерии инициирования переключения.....	4
6 Архитектура обеспечения надежности сети.....	4
6.1 Защита линии связи	4
6.2 Защита трассы	4
6.3 Типы переключения	5
6.4 Типы операций.....	5
6.5 Механизм обнаружения отказов в сети	5
6.6 Механизм запуска защитного переключения	6
7 Защита линии связи.....	6
8 Защита трассы.....	6
8.1 Двухпутевая модель маршрутизации.....	6
8.2 Модель маршрутизации по кратчайшему пути	7
8.3 Модель альтернативной маршрутизации	8
9 Механизм координирования защиты	8
10 Вопросы безопасности.....	8
Дополнение I – Ушная декомпозиция	9
Библиография	10

Введение

Надежность сети пакетной передачи данных электросвязи общего пользования (PTDN) обеспечивается с применением механизмов защиты линии связи и защиты трассы. В обоих механизмах рассматриваются два типа защиты – защита 1 : 1 и защита 1 : n . В механизме защиты трассы могут быть реализованы три модели маршрутизации.

Для реализации механизма защиты трассы в PTDN также могут использоваться три модели маршрутизации – двухпутевая модель, модель маршрутизации по кратчайшему пути и модель альтернативной маршрутизации.

- Двухпутевая модель маршрутизации предполагает предварительный расчет на основе ушной декомпозиции двух непересекающихся путей – рабочего и защитного, чтобы обеспечить защиту 1 : 1 от исходного узла до узла назначения с использованием информации о топологии и ресурсах сети.
- Модель маршрутизации по кратчайшему пути и модель альтернативной маршрутизации работают вместе, обеспечивая защиту 1 : n .
- Модель альтернативной маршрутизации может обеспечить защиту 1 : n самостоятельно. Рассчитываются несколько путей, один из которых представляет собой рабочий путь, а остальные – защитные пути.

Рекомендация МСЭ-Т Y.2614

Надежность сети пакетной передачи данных электросвязи общего пользования

1 Сфера применения

В настоящей Рекомендации определены цели, архитектура и механизмы обеспечения надежности сети пакетной передачи данных общего пользования (PTDN), включая описание механизмов защиты линии связи, защиты трассы, обнаружения отказов сети, запуска защитной коммутации и координирования защиты.

2 Справочные документы

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

- [ITU-T Y.2601] Рекомендация МСЭ-Т Y.2601 (2006 г.), *Основные характеристики и требования к будущим пакетным сетям.*
- [ITU-T Y.2611] Рекомендация МСЭ-Т Y.2611 (2006 г.), *Архитектура высокого уровня будущих пакетных сетей.*
- [ITU-T Y.2612] Рекомендация МСЭ-Т Y.2612 (2009 г.), *Общие требования и структура адресации, маршрутизации и переадресации в будущих пакетных сетях.*
- [ITU-T Y.2613] Рекомендация МСЭ-Т Y.2613 (2010 г.), *Общая техническая архитектура сети пакетной передачи данных электросвязи общего пользования.*

3 Термины и определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 двунаправленное защитное переключение (**bidirectional protection switching**)

[b-ITU-T I.630]: Архитектура защитного переключения, при которой для защиты в случае отказа одного направления переключаются оба направления (трассы, соединения подсети и т. п.) – как затронутое, так и не затронутое.

3.1.2 **время удержания (hold-off time)** [b-ITU-T G.870]: Время между объявлением ухудшения качества или ошибки сигнала и иницированием алгоритма защитного переключения.

3.1.3 **ручная защита (manual protection)** [b-ITU-T M.2102]: Восстановление иницируется принудительным или ручным переключением на альтернативный маршрут; возврат к исходной конфигурации осуществляется путем принудительного или ручного переключения на обычный маршрут.

3.1.4 **невозвратная (защитная) операция (non-revertive (protection) operation)** [b-ITU-T G.870]: Операция защитного переключения, при которой функции транспортировки и выборки сигнала нормального трафика не возвращаются на рабочий транспортный объект, если запросы на переключение выполнены.

3.1.5 **защитное переключение (protection switching)** [b-ITU-T I.630]: Метод обеспечения надежности сети с использованием специальной политики выделения ресурсов для защиты.

3.1.6 сеть пакетной передачи данных электросвязи общего пользования (public packet telecommunication data network (PTDN)) [ITU-T Y.2613]: Пакетная сеть передачи данных, предназначенная для страты транспортирования СПП, которая должна быть безопасной, надежной, контролируемой и управляемой и может отвечать всем требованиям, указанным в [ITU-T Y.2601]. PTDN – это иерархическая сеть, которую можно разделить на несколько сетевых уровней.

3.1.7 возвратная (защитная) операция (revertive (protection) operation) [b-ITU-T G.870]: Операция защитного переключения, при которой функции транспортировки и выборки сигнала нормального трафика (услуг) всегда возвращаются в рабочий транспортный объект (или остаются в нем), если запросы на переключение выполнены, то есть когда рабочий транспортный объект восстанавливается после неисправности или внешний запрос отменяется.

3.1.8 время переключения (switching time) [b-ITU-T G.870]: Время между инициализацией алгоритма защитного переключения и моментом выборки трафика из резервного транспортного объекта.

3.1.9 защита трассы (trail protection) [b-ITU-T G.780]: Нормальный трафик переносится по защитной трассе/выбирается из нее вместо рабочей, если рабочая трасса вышла из строя или ее пропускная способность опустилась ниже требуемого уровня.

3.1.10 однонаправленное защитное переключение (unidirectional protection switching) [b-ITU-T I.630]: Архитектура защитного переключения, при которой для защиты от отказа одного направления (то есть отказа, затрагивающего только одно направление передачи), переключается только затронутое направление (трасса, соединение подсети и т. д.).

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 защита 1 : 1 (1 : 1 protection): Механизм защиты, при котором трафик передается только по рабочему или по защитному пути.

3.2.2 модель альтернативной маршрутизации (alternative routing model): Модель маршрутизации, обеспечивающая несколько путей между исходным узлом сети пакетной передачи данных электросвязи общего пользования (PTDN) и конечным узлом PTDN.

ПРИМЕЧАНИЕ. – Эти пути не обязательно должны быть детерминированными и уникальными. В этой модели путь передачи и путь приема не обязательно состоят из одних и тех же узлов и линий связи.

3.2.3 двухпутевая модель маршрутизации (dual path routing model): Модель маршрутизации, обеспечивающая два непересекающихся пути между исходным узлом сети пакетной передачи данных электросвязи общего пользования (PTDN) и конечным узлом PTDN.

ПРИМЕЧАНИЕ. – Оба эти пути могут не быть кратчайшими.

3.2.4 защита линии связи (link protection): Механизм защиты точка-точка.

ПРИМЕЧАНИЕ. – Защитное переключение и перемаршрутизация на уровне сети не инициируются, если только не нарушена защита линии связи.

3.2.5 модель маршрутизации по кратчайшему пути (shortest path routing model): Модель маршрутизации, обеспечивающая кратчайший детерминированный и уникальный путь из исходного узла сети пакетной передачи данных электросвязи общего пользования (PTDN) в конечный узел PTDN.

ПРИМЕЧАНИЕ. – В этой модели пути из исходного узла в конечный и из конечного узла в исходный совпадают.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

IP	Internet Protocol	Протокол Интернет
ОАМ	Operations, Administration and Maintenance	Эксплуатация, управление и техническое обслуживание

PTDN	Public packet Telecommunication Data Network		Сеть пакетной передачи данных электросвязи общего пользования
QoS	Quality of Service		Качество обслуживания
SDH	Synchronous Digital Hierarchy	СЦИ	Синхронная цифровая иерархия
WDM	Wavelength Division Multiplexing		Мультиплексирование с разделением по длине волны

5 Показатели надежности сети

В этом разделе описываются показатели надежности сети PTDN.

5.1 Время переключения

В соответствии с моделями маршрутизации, поддерживаемыми в PTDN, в случае отказа линии или узла связи трафик услуг может переключаться с рабочего пути на защитный. Время переключения состоит из двух частей – времени получения узлом уведомления об отказе в сети, отправленного узлом, ближайшим к точке отказа; и времени выполнения защитного переключения с рабочего пути на защитный.

В PTDN время переключения не должно превышать 50 мс.

5.2 Время удержания

PTDN представляет собой уровневую сеть. Схема защиты обеспечивается каждым уровнем. Таким образом необходимо рассмотреть координирование защиты между уровнями во избежание переключения в обоих направлениях. Время удержания полезно для взаимодействия схем защиты. При объявлении состояния отказа запускается таймер удержания, и период времени таймера может быть сконфигурирован. По истечении периода таймера удержания инициируется защитное переключение при условии, что состояние отказа в этой точке все еще присутствует. Отметим, что состояние отказа не обязательно должно присутствовать в течение всего периода удержания; достаточно его присутствия в момент истечения периода времени таймера удержания.

В PTDN время удержания должно превышать время переключения нижележащего уровня сети.

5.3 Типы защиты

Возможна защита типа $1:1$ и $1:n$. Трафик услуг передается по рабочему либо по защитному пути. При защите типа $1:1$ имеются два непересекающихся пути между исходным узлом и узлом назначения. Один из них – рабочий путь, а другой – защитный. При защите типа $1:n$ между исходным узлом и узлом назначения существует $1+n$ путей, один из которых – рабочий, а другие – защитные.

В PTDN для защиты трассы рекомендуется использовать защиту типа $1:1$ и защиту тип $1:n$.

5.4 Типы переключения

Существует два типа переключения – однонаправленное и двунаправленное. При однонаправленном переключении путь передачи и путь приема трафика различаются, поэтому переключается только затронутый путь. При двунаправленном переключении путь передачи и путь приема трафика обычно совпадают, поэтому можно переключать оба пути.

В PTDN рекомендуется обеспечить одно- и двунаправленное защитное переключение.

5.5 Типы операций

Существуют защитные операции двух типов: невозвратные и возвратные. При невозвратных операциях трафик услуг не возвращается на рабочий путь после его восстановления. Трафик услуг возвращается на рабочий путь только в случае отказа текущего защитного пути. При возвратных операциях трафик услуг всегда возвращается на рабочий путь после его восстановления.

В PTDN должны быть предусмотрены операции возвратного и невозвратного типа.

5.6 Ручная защита

В РТДН поддерживаются автоматическое защитное переключение и ручное защитное переключение. Оператор может выполнить ручное защитное переключение, которое обычно имеет более высокий приоритет по сравнению с автоматическим.

5.7 Критерии инициирования переключения

В РТДН поддерживаются следующие критерии инициирования защитного переключения:

- команды, иницируемые извне (например, при ручном управлении);
- отказ линии или узла на рабочем пути, когда защитный путь готов и истек период времени таймера удержания;
- восстановление рабочего пути при возвратной операции.

6 Архитектура обеспечения надежности сети

В РТДН требуются следующие типы защиты линии связи и трассы:

- должна быть обеспечена защита трассы 1 : 1 и 1 : n;
- должно поддерживаться одно- и двунаправленное переключение;
- должны поддерживаться возвратные и невозвратные операции.

6.1 Защита линии связи

Схема защиты обеспечивается каждым уровнем сети РТДН, которая состоит из множества уровней. Защита линии связи работает на уровне канала. Для защиты линии связи используется механизм точка-точка. Пока не нарушена защита линии связи, защитное переключение и перемаршрутизация на уровне сети не иницируются.

Архитектура защиты линии связи показана на рисунке 6-1.

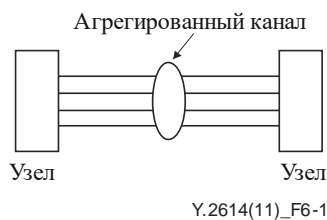


Рисунок 6-1 – Архитектура защиты линии связи

В РТДН существуют два механизма распределения трафика услуг по агрегированным каналам:

- 1) трафик распределяется по всем физическим агрегированным каналам, но часть ресурса каждого канала зарезервирована с возможностью суммирования ресурсов одного или нескольких каналов для защиты в случае отказа одного или нескольких каналов;
- 2) пока все каналы исправны, по одному или нескольким агрегированным каналам трафик не передается.

Конечные узлы агрегированных каналов могут обнаруживать отказ определенных физических линий и перераспределять трафик отказавших линий между другими физическими линиями.

6.2 Защита трассы

Защита трассы – это механизм сквозной защиты. На основе топологии сети и информации о ресурсах РТДН предварительно рассчитываются по крайней мере два пути от исходного узла до того же узла назначения. Один из них – рабочий путь, а другой (другие) – защитный (защитные).

Для обнаружения отказов рабочего или защитного пути используются последовательные контрольные пакеты. Когда получено сообщение об отказе в сети, после истечения времени таймера удержания трафик услуг переключается с рабочего пути на защитный.

Архитектура защиты трассы показана на рисунке 6-2.

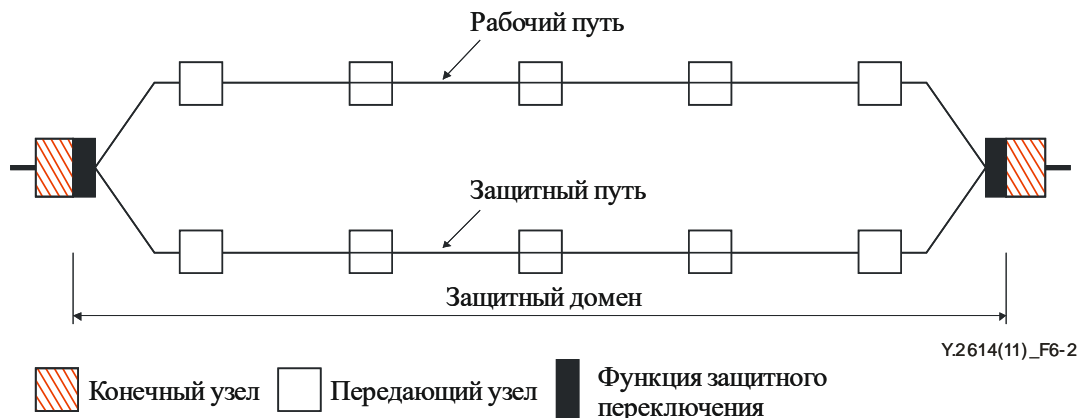


Рисунок 6-2 – Архитектура защиты трассы

В PTDN для защиты трассы рекомендуется использовать механизм защиты типа 1 : 1 и типа 1 : n .

При защите типа 1 : 1 применяется двухпутевая модель маршрутизации с предварительным расчетом двух непересекающихся путей на основе ушной декомпозиции.

Существуют два способа реализации защиты типа 1 : n :

- 1) совместное применение модели маршрутизации по кратчайшему пути и модели альтернативной маршрутизации. Модель маршрутизации по кратчайшему пути дает один рабочий путь, а модель альтернативной маршрутизации – n защитных путей;
- 2) модель альтернативной маршрутизации применяется для расчета нескольких путей; один из них служит рабочим путем, остальные – защитными.

Для обнаружения отказов рабочего или защитного пути используются последовательные контрольные пакеты. Они вставляются в исходном узле защитной трассы и обнаруживаются и извлекаются в приемном узле защитной трассы.

6.3 Типы переключения

Может применяться одно- или двунаправленное защитное переключение.

В PTDN, если маршрут рассчитывается на основе модели маршрутизации по кратчайшему пути или двухпутевой модели маршрутизации, путь передачи и путь приема обычно совпадают. В обоих случаях применяется двунаправленное переключение. Однако если маршрут рассчитывается на основе модели альтернативной маршрутизации, пути передачи и приема могут различаться. В этом случае применяется однонаправленное переключение.

6.4 Типы операций

По типу операции защита может быть невозвратной или возвратной.

При невозвратных операциях, когда рабочий путь восстанавливается после переключения с рабочего пути на защитный, трафик услуг не возвращается на рабочий путь, если только не произошел отказ текущего защитного пути.

При возвратных операциях трафик услуг всегда возвращается на рабочий путь после его восстановления. В PTDN рекомендуется использовать возвратные операции.

6.5 Механизм обнаружения отказов в сети

В PTDN существует два механизма обнаружения отказов. Один из них – механизм обнаружения отказа линии связи. Он работает на уровне канала и определяет состояние линии связи в режиме реального времени, периодически передавая служебные кадры. Другой механизм обнаруживает отказы трассы. Он работает на сетевом уровне и определяет наличие сквозного соединения в режиме реального времени, периодически передавая пакеты OAM.

6.6 Механизм запуска защитного переключения

Операция защитного переключения выполняется:

- 1) по инициативе оператора (ручное переключение, принудительное переключение и т. п.) в отсутствие более приоритетного действительного запроса на переключение;
- 2) при объявлении потери сигнала по рабочему, но не по защитному пути – после истечения времени таймера удержания; или
- 3) при истечении времени таймера ожидания восстановления (возвратный режим), когда потеря сигнала по рабочему пути не объявлена.

7 Защита линии связи

В PTDN для увеличения пропускной способности и надежности связи пара узлов может быть соединена несколькими физическими линиями. При расчете маршрута несколько физических линий объединяются в одну логическую линию, и трафик услуг распределяется между несколькими физическими линиями в соответствии с их пропускной способностью. При отказе одной или нескольких агрегированных линий трафик услуг, переносимый отказавшими линиями, перераспределяется по другим доступным линиям, а не переключается с рабочего пути на защитный, если только не отказал механизм защиты линии.

В PTDN отказ защиты линии происходит в следующих случаях:

- 1) вышли из строя все агрегированные физические линии;
- 2) при выходе из строя одной или нескольких агрегированных линий возможности оставшихся линий не удовлетворяют требования трафика.

При отказе защиты линии применяется механизм защиты трассы.

8 Защита трассы

В PTDN для защиты трассы используются три модели маршрутизации. Это двухпутевая модель маршрутизации, модель маршрутизации по кратчайшему пути и модель альтернативной маршрутизации.

В режиме связи без установления соединения узел PTDN определяет модель маршрутизации по значению поля защиты, которое состоит из двух битов в заголовке пакета [ITU-T Y.2613]. При отказе сети (линии или узла) или восстановлении рабочего пути значение поля защиты изменяется.

Значение поля защиты "00" означает, что применяется модель маршрутизации по кратчайшему пути. В этом случае при отказе сети (линии или узла) трафик услуг может прерываться, если только не применяется модель альтернативной маршрутизации – тогда значение поля защиты меняется с "00" на "10". При использовании модели альтернативной маршрутизации может быть гарантирована достигаемость сети, но QoS не гарантируется.

Если в поле защиты содержится код "11" или "01", это означает, что применяется двухпутевая модель маршрутизации. В этом случае при отказе сети (линии или узла) трафик услуг переключается с рабочего пути на защитный, а при восстановлении рабочего пути в процессе возвратной операции – с защитного пути на рабочий. Соответственно значение поля должно изменяться с "11" на "01" или с "01" на "11". Следует отметить, что QoS может быть гарантировано, только если сетевые ресурсы рабочего и защитного путей абсолютно одинаковы.

8.1 Двухпутевая модель маршрутизации

Двухпутевая модель маршрутизации предварительно рассчитывает два непересекающихся пути от исходного узла к узлу назначения на основе топологии сети и информации о ресурсах. Это рабочий путь и защитный путь. Все линии и узлы рабочего пути и защитного пути, за исключением исходного узла и узла назначения, – общие.

В топологии сети с двухпутевой моделью маршрутизации должны соблюдаться два условия:

- 1) каждый узел в PTDN связан как минимум с двумя другими узлами;
- 2) каждая линия связи в PTDN является двунаправленной.

С помощью алгоритма ушной декомпозиции можно получить две непересекающиеся направленные диаграммы (см. рисунок 8-1).

Более подробная информация по ушной декомпозиции приведена в Дополнении I.

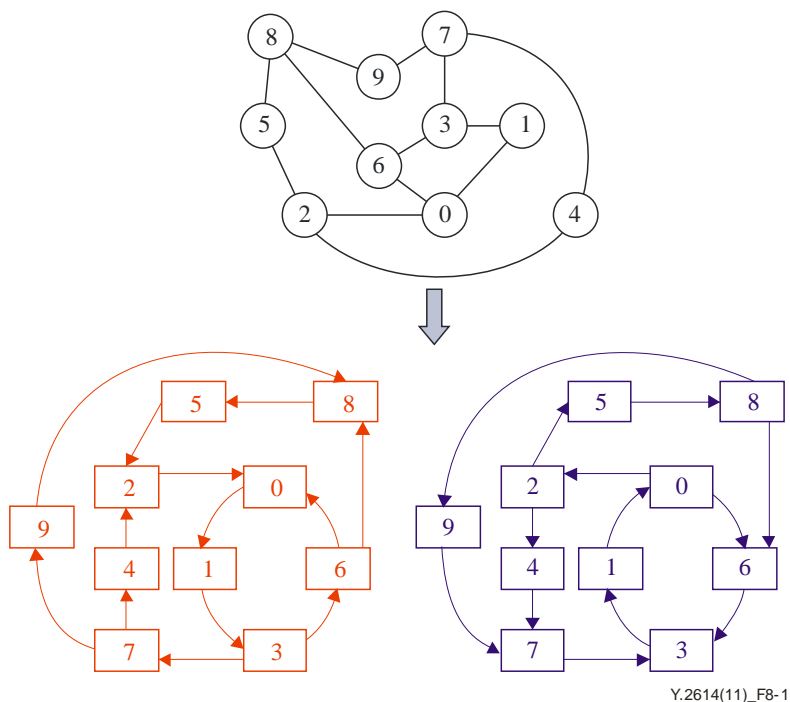


Рисунок 8-1 – Ушная декомпозиция в двухпутевой модели маршрутизации

Как показано на рисунке 8-1, между любыми двумя узлами имеются два непересекающихся пути. Например, имеются два непересекающихся пути из узла 1 к узлу 7. Один – это рабочий путь через узлы 1, 3 и 7. Другой – защитный путь через узлы 1, 0, 2, 4 и 7.

В случае отказа рабочего пути узел, ближайший к этой точке отказа, передает уведомление об отказе сети в исходный узел. Получив это уведомление, исходный узел переключает трафик с рабочего пути на защитный. Значение поля защиты в заголовке пакета изменено с "11" на "01".

При возвратной операции, если рабочий путь восстанавливается, трафик услуг возвращается на рабочий путь, а значение поля защиты в заголовке пакета должно быть изменено с "01" на "11".

При невозвратной операции трафик услуг не возвращается на рабочий путь даже после его восстановления, если только не произошел отказ защитного пути.

При двухпутевой модели маршрутизации QoS может быть гарантировано при переключении с рабочего пути на защитный или с защитного пути на рабочий, если сетевые ресурсы по этим двум путям одинаковы.

8.2 Модель маршрутизации по кратчайшему пути

Модель маршрутизации по кратчайшему пути обеспечивает детерминированный и уникальный кратчайший путь из исходного узла РТДН до узла назначения. В этой модели путь передачи и путь приема должен быть одним и тем же. При наличии нескольких соединений между доменами РТДН на границе домена активным является только одно соединение с наивысшим приоритетом.

При передаче пакета с использованием модели маршрутизации по кратчайшему пути значение поля защиты в заголовке пакета устанавливается в "00".

Для обеспечения досягаемости сети в случае отказа модели маршрутизации по кратчайшему пути применяется модель альтернативной маршрутизации. В этом случае значение поля защиты в заголовке пакета должно быть изменено с "00" на "10".

8.3 Модель альтернативной маршрутизации

В модели альтернативной маршрутизации предварительно рассчитываются несколько путей, которые сохраняются в таблице маршрутизации; один из этих путей – рабочий. В случае отказа рабочего пути активным становится второй маршрут из таблицы маршрутизации. Эти пути могут не быть кратчайшими, и не требуется, чтобы пути передачи и приема содержали одни и те же узлы и линии связи. Модель альтернативной маршрутизации может применяться в двух случаях.

- 1) Рабочим является кратчайший путь; модель альтернативной маршрутизации обеспечивает защитный путь (пути).

Отказ узла или линии связи или изменение топологии могут привести к отказу рабочего пути. В этой ситуации модель альтернативной маршрутизации обеспечивает защитный путь (пути). Значение поля защиты в заголовке пакета должно быть изменено с "00" на "01".

- 2) Рабочий путь и защитный путь (пути) выбраны по модели альтернативной маршрутизации.

При использовании модели альтернативной маршрутизации значение поля защиты в заголовке пакета устанавливается в "01". Предварительно рассчитываются и сохраняются в таблице маршрутизации несколько путей от исходного узла до узла назначения; один из этих путей используется в качестве рабочего. При отказе рабочего пути из таблицы маршрутизации выбирается защитный путь. В этом случае значение поля защиты в заголовке пакета не изменяется.

При модели альтернативной маршрутизации может быть гарантирована достижимость сети, но QoS не гарантируется.

9 Механизм координирования защиты

Если узлы соединены несколькими агрегированными линиями, то в случае отказа одной или нескольких линий сначала применяется защита линии, а в случае ее отказа – защита трассы.

Кроме того, во избежание переключения в обоих направлениях между уровнями защиты вводится время удержания. Например, если RTDN основана на транспортной сети (например, СЦИ, WDM), то защитное переключение RTDN инициируется только после истечения времени таймера удержания при условии, что состояние отказа (например, линии связи или узла транспортной уровневой сети) в этой точке все еще присутствует.

10 Вопросы безопасности

В настоящей Рекомендации определены механизмы создания одного или нескольких защитных путей для защиты рабочего пути. Эти механизмы способствуют повышению безопасности RTDN. Механизмы повышения надежности, описанные в настоящей Рекомендации, предполагают, что рабочий и защитный пути устанавливаются в одно и то же время и одинаковым образом. С учетом того, что настройка любого пути выполняется обычными процедурами RTDN, никаких дополнительных рисков для безопасности, специфичных для механизмов повышения надежности, описанных в этой Рекомендации, не выявлено.

Что касается нестабильности при применении защиты, то в настоящей Рекомендации уже рассмотрены время задержки и механизм координирования защиты.

Дополнение I

Ушная декомпозиция

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Ушная декомпозиция $D = \{P_0; P_1; \dots; P_r - 1\}$ неориентированного графа $G = (V, E)$ представляет собой разбиение E на упорядоченную совокупность непересекающихся ребер простых путей $P_0; P_1; \dots; P_r - 1$, называемых ушами, таких, что:

- P_0 – это простой цикл.
- P_i ($i > 0$) – это простой путь, конечные точки которого принадлежат ушам с меньшим номером и ни одна из внутренних вершин не принадлежит ушам с меньшим номером;
- P_i ($i > 0$) также может быть простым циклом. Цикл, состоящий из единственного ребра, называют тривиальным ухом.

Ушная декомпозиция называется открытой тогда и только тогда, когда нет ни одного цикла P_i ($i > 0$).

На рисунке I.1 топология сети, показанная слева, разбита на четыре уха, как показано в правой части рисунка I.1. Из них P_0 – простой цикл, состоящий из узлов 0, 1, 3 и 6; P_1 состоит из узлов 2, 4 и 7, причем конечные точки 3 и 0 принадлежат уху P_0 , которое является ухом с меньшим номером по сравнению с P_1 ; P_2 состоит из узлов 5 и 8, причем конечные точки 2 и 6 принадлежат соответственно ушам P_1 и P_0 , которые являются ушами с меньшим номером по сравнению с P_2 ; P_3 состоит из узла 9 с конечными точками 7 и 8, принадлежащими соответственно ушам P_1 и P_2 , которые являются ушами с меньшим номером по сравнению с P_3 .

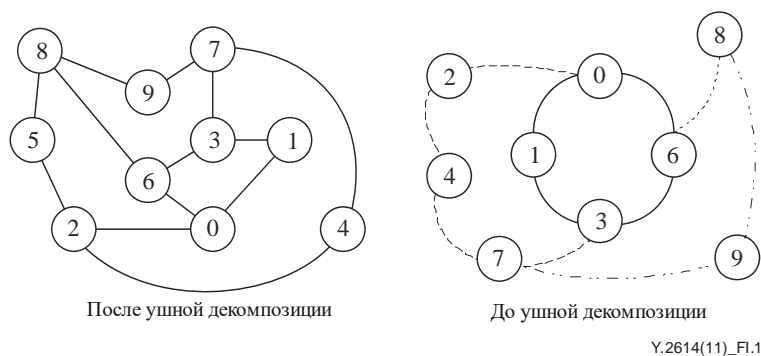


Рисунок I.1 – Ушная декомпозиция

Ушная декомпозиция существует тогда и только тогда, когда граф двухреберно связный. В сети РТДН двухреберно связный граф может обеспечить защиту от отказов линий связи и узлов.

Библиография

- [b-ITU-T G.780] Recommendation ITU-T G.780/Y.1351 (2010), *Terms and definitions for synchronous digital hierarchy (SDH) networks.*
- [b-ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2010), *Terms and definitions for optical transport networks (OTN).*
- [b-ITU-T G.8131] Recommendation ITU-T G.8131/Y.1382 (2007), *Linear protection switching for transport MPLS (T-MPLS) networks.*
- [b-ITU-T I.322] Recommendation ITU-T I.322 (1999), *Generic protocol reference model for telecommunication networks.*
- [b-ITU-T I.630] Recommendation ITU-T I.630 (1999), *ATM protection switching.*
- [b-ITU-T M.2102] Recommendation ITU-T M.2102 (2000), *Maintenance thresholds and procedures for recovery mechanisms (protection and restoration) of international SDH VC trails (paths) and multiplex sections.*
- [b-ITU-T X.25] Recommendation ITU-T X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*
- [b-ITU-T X.121] Recommendation ITU-T X.121 (2000), *International numbering plan for public data networks.*
- [b-ITU-T X.136] Recommendation ITU-T X.136 (1997), *Accuracy and dependability performance values for public data networks when providing international packet-switched services.*
- [b-ITU-T X.137] Recommendation ITU-T X.137 (1997), *Availability performance values for public data networks when providing international packet-switched services.*
- [b-ITU-T X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*
- [b-ITU-T X.212] Recommendation ITU-T X.212 (1995) | ISO/IEC 8886:1996, *Information technology – Open Systems Interconnection – Data Link service definition.*
- [b-ITU-T X.323] Recommendation ITU-T X.323 (1988), *General arrangements for interworking between Packet-Switched Public Data Networks (PSPDNs).*
- [b-ITU-T X.371] Recommendation ITU-T X.371/Y.1402 (2001), *General arrangements for interworking between Public Data Networks and the Internet.*
- [b-ITU-T Y.1001] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies.*
- [b-ITU-T Y.1251] Recommendation ITU-T Y.1251 (2002), *General architectural model for interworking.*
- [b-ITU-T Y.1720] Recommendation ITU-T Y.1720 (2006), *Protection switching for MPLS networks.*
- [b-ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СИП.*
- [b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; 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, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи