МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т G.7712/Y.1703

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2003)

СЕРИЯ G: СИСТЕМЫ И СРЕДА ПЕРЕДАЧИ, ЦИФРОВЫЕ СИСТЕМЫ И СЕТИ
Цифровое оконечное оборудование – Эксплуатация, управление и техническое обслуживание передающего оборудования
СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА И АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP)
Аспекты межсетевого протокола (IP) – Эксплуатация, управление и техническое обслуживание

Архитектура и спецификация сети передачи данных

Рекомендация МСЭ-Т G.7712/Y.1703

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 СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ ПО МЕТАЛЛИЧЕСКИМ ЛИНИЯМ	G.300–G.399
ОБЩИЕ ХАРАКТЕРИСТИКИ МЕЖДУНАРОДНЫХ СИСТЕМ ТЕЛЕФОННОЙ СВЯЗИ ПО РАДИОРЕЛЕЙНЫМ ИЛИ СПУТНИКОВЫМ ЛИНИЯМ И ИХ ВЗАИМНОЕ СОЕДИНЕНИЕ С МЕТАЛЛИЧЕСКИМИ ЛИНИЯМИ	G.400–G.449
КООРДИНАЦИЯ РАДИОТЕЛЕФОНИИ И ПРОВОДНОЙ ТЕЛЕФОНИИ	G.450–G.499
ИСПЫТАТЕЛЬНОЕ ОБОРУДОВАНИЕ	G.500–G.599
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ	G.600–G.699
ЦИФРОВОЕ ОКОНЕЧНОЕ ОБОРУДОВАНИЕ	G.700–G.799
ЦИФРОВЫЕ СЕТИ	G.800–G.899
ЦИФРОВЫЕ УЧАСТКИ И СИСТЕМА ЦИФРОВЫХ ЛИНИЙ	G.900–G.999
КАЧЕСТВО ОБСЛУЖИВАНИЯ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ	G.1000–G.1999
ХАРАКТЕРИСТИКИ СРЕДЫ ПЕРЕДАЧИ	G.6000–G.6999
ЦИФРОВОЕ ОКОНЕЧНОЕ ОБОРУДОВАНИЕ	G.7000–G.7999
Общие положения	G.7000–G.7099
Кодирование аналоговых сигналов с помощью импульсно-кодовой модуляции	G.7100–G.7199
Кодирование аналоговых сигналов с помощью методов, отличающихся от ИКМ	G.7200–G.7299
Основные характеристики первичного мультиплексного оборудования	G.7300–G.7399
Основные характеристики мультиплексного оборудования второго порядка	G.7400–G.7499
Основные характеристики мультиплексного оборудования высшего порядка	G.7500–G.7599
Основные характеристики оборудования транскодера и цифрового мультиплексирования	G.7600–G.7699
Эксплуатация, управление и техническое обслуживание передающего оборудования	**G.7700–G.7799**
Основные характеристики оборудования мультиплексирования для синхронной цифровой иерархии	G.7800–G.7899
Другое оконечное оборудование	G.7900–G.7999
ЦИФРОВЫЕ СЕТИ	G.8000–G.8999

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

Рекомендация МСЭ-Т G.7712/Y.1703

Архитектура и спецификация сети передачи данных

Резюме

В настоящей Рекомендации рассматриваются требования, предъявляемые к архитектуре сети передачи данных (DCN), которая может поддерживать линии связи с распределенным управлением, относящиеся к сети управления электросвязью (сеть TMN), линии связи с распределенной сигнализацией, относящихся к транспортной сети с автоматической коммутацией (сеть ASTN) и прочим распределенным линиям связи (например, передача служебной информации или телефонная передача, пересылка по линиям связи программного обеспечения). Архитектура сети DCN рассматривает сети как работающие в режимах только-IP, только-OSI, так и в режиме мультимедиа (т. е. поддерживает и режим IP, и режим OSI). Приводится также спецификация взаимодействия между частями сети DCN, поддерживающими работу в режиме только IP, частями, поддерживающими работу в режиме только OSI, и частями, поддерживающими работу в этих обоих режимах – IP и OSI.

С целью транспортировки информации между большим количеством разных компонентов для разных применений (например, сети TMN, ASTN и пр.) требуется сеть, осуществляющая передачу информации в пакетном режиме. Например, для работы сети TMN нужна такая сеть связи, которая является сетью управления передачей данных (сеть MCN) и позволяет осуществлять транспортировку управляющих сообщений между компонентами сети TMN (например, компонент NEF и компонент OSF). Для работы сети ASTN нужна такая сеть связи, которая является сетью передачи сигнализации (SCN) и позволяет осуществлять транспортировку сигнальных сообщений между компонентами сети ASTN (например, компонентами CC). В настоящей Рекомендации приводится спецификация функций передачи данных, которые могут использоваться для поддержки одной или нескольких сетей связи различного применения.

Функции передачи данных, рассмотренные в версии 11/2001 настоящей Рекомендации, поддерживают услуги сети без установления соединений. Настоящая версия Рекомендации дополнительно рассматривает поддержку услуг сети SCN, требующих установления соединений благодаря включению специального механизма, основанного на многопротокольной коммутации меток (MPLS). Настоящая Рекомендация является одной из семейства Рекомендаций, в которых рассматриваются транспортные сети.

Источник

Рекомендация МСЭ-Т G.7712/Y.1703 была пересмотрена 15-й Исследовательской комиссией МСЭ-Т (2001–2004 гг.) и утверждена 16 марта 2003 года согласно процедуре Резолюции 1 ВАСЭ.

История документа	
Выпуск	**Примечания**
1.0	Выпуск Вопроса Q 14/15 на собрании в октябре 2001 года
1.1	Выпуск Вопроса Q 14/15 на собрании в апреле 2002 года
1.2	Завершение работы над 1.1
1.3	Выпуск Вопроса Q 14/15 на собрании в октябре 2002 года
1.4	Завершение работы над версией 1.3: Изменение заголовков параграфов с 7.1.a и т. д. на 7.1.13 и т. д. Снятие редакционных замечаний
1.5	Выпуск на собрании Вопроса Q 14/15 и представление на одобрение

Ключевые слова

Сети передачи данных, межсетевой протокол (IP), интерфейс открытых систем (OSI).

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.

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.

Соответствие положениям данной Рекомендации является добровольным делом. Однако в Рекомендации могут содержаться определенные обязательные положения (для обеспечения, например, возможности взаимодействия или применимости), и тогда соответствие данной Рекомендации достигается в том случае, если выполняются все эти обязательные положения. Для выражения требований используются слова "shall" ("должен", "обязан") или некоторые другие обязывающие термины, такие как "must" ("должен"), а также их отрицательные эквиваленты. Использование таких слов не предполагает, что соответствие данной Рекомендации требуется от каждой стороны.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, 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 извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

СОДЕРЖАНИЕ

		Стр.
1	Область применения	1
2	Ссылки	1
3	Термины и определения	3
4	Сокращения	4
5	Соглашения	6
6	Характеристики сети DCN	7
6.1	Применение сети TMN	9
6.2	Применение сети ASTN	16
6.3	Прочие применения, для которых требуются сети передачи	23
6.4	Классификация различных применений	23
7	Функциональная архитектура сети DCN и предъявляемые к ней требования	23
7.1	Технические требования, предъявляемые к функциям передачи данных	24
7.2	Требования, предъявляемые к обеспечению	35
7.3	Требования, предъявляемые к безопасности	35
Приложение A – Требования, предъявляемые к трехстороннему взаимодействию		35
A.1	Параметры TLV трехсторонней смежности соединения "точка–точка"	35
A.2	Трехстороннее состояние смежности	36
Приложение B – Требования, предъявляемые к автоматической инкапсуляции		37
B.1	Введение	37
B.2	Область применения	37
B.3	Описание функции AE-DCF	37
B.4	Требования и ограничения	39
Добавление I – Ограничения, относящиеся к функциям взаимодействия в сети DCN		49
I.1	Общие допущения	49
I.2	Общее для всех алгоритмов	49
Добавление II – Пример реализации автоматической инкапсуляции		51
II.1	Введение	51
II.2	Модификации алгоритма Dijkstra	52
Добавление III – Руководство по введению в действие элементов SDH NE в сдвоенном режиме работы согласно RFC 1195 и по влиянию факультативной автоматической инкапсуляции		55
III.1	Введение	55
III.2	Система Integrated IS-IS без автоматической инкапсуляции	55
III.3	Интегральный IS-IS (Integrated IS-IS) с автоматической инкапсуляцией	59
Добавление IV – Иллюстрация примеров пакетного режима с защитой 1+1		62
IV.1	Общее описание пакетного режима с защитой 1+1	62
IV.2	Иллюстрация защиты 1+1 в пакетном режиме	63
IV.3	Работа алгоритма константы выбора при различных алгоритмах отказа	65
Добавление V – Литература		69

Рекомендация МСЭ-Т G.7712/Y.1703

Архитектура и спецификация сети передачи данных

1 Область применения

В настоящей Рекомендации рассматриваются требования, предъявляемые к архитектуре сети передачи данных (DCN), которая может поддерживать линии связи с распределенным управлением, относящиеся к сети управления электросвязью (сеть TMN), линии связи с распределенной сигнализацией, относящихся к транспортной сети с автоматической коммутацией (сеть ASTN) и прочим распределенным линиям связи (например, передача служебной информации или телефонная передача, пересылка по линиям связи программного обеспечения). Архитектура сети DCN рассматривает сети как работающие в режимах только-IP, только-OSI, так и в режиме мультимедиа (т. е. поддерживает и режим IP, и режим OSI). Приводится также спецификация взаимодействия между частями сети DCN, поддерживающими работу в режиме только IP, частями, поддерживающими работу в режиме только OSI, и частями, поддерживающими работу в этих обоих режимах – IP и OSI.

Сеть DCN обеспечивает функции уровня 1 (физический уровень), уровня 2 (уровень звена передачи данных) и уровень 3 (сетевой уровень) и включает функции маршрутизации/коммуникации, соединенные посредством линий. Эти линии могут быть реализованы с использованием различных интерфейсов, включая интерфейсы территориально-распределенной сети (WAN), локальной (вычислительной) сети (LAN) и каналы со встроенным управлением (ECC).

С целью транспортировки информации между большим количеством разных компонентов для разных применений (например, сети TMN, ASTN и пр.) требуется сеть, осуществляющая передачу информации в пакетном режиме. Например, для работы сети TMN нужна такая сеть связи, которая является сетью управления передачей данных (сеть MCN) и позволяет осуществлять транспортировку управляющих сообщений между компонентами сети TMN (например, компонент NEF и компонент OSF). Для работы сети ASTN нужна такая сеть связи, которая является сетью передачи сигнализации (SCN) и позволяет осуществлять транспортировку сигнальных сообщений между компонентами сети ASTN (например, компонентами CC). В настоящей Рекомендации приводится спецификация функций передачи данных, которые могут использоваться для поддержки одной или нескольких сетей связи различного применения.

Функции передачи данных, рассмотренные в настоящей Рекомендации, поддерживают услуги сети без установления соединений. В будущие версии данной Рекомендации могут быть включены дополнительные функции, поддерживающие услуги сетей с установлением соединений.

2 Ссылки

Положения настоящей Рекомендации опираются на положения приведенных ниже Рекомендаций МСЭ-Т и других источников, на которые имеются ссылки. Ко времени публикации настоящей Рекомендации все указанные ниже источники информации были действующими. Однако все Рекомендации и прочие цитируемые источники подлежат пересмотру. Поэтому всем пользователям настоящей Рекомендации желательно рассмотреть возможность использования последних изданий перечисленных ниже Рекомендаций. Перечень действующих на текущий момент Рекомендаций МСЭ-Т публикуются регулярно. Ссылка в данной Рекомендации на какой-либо документ не дает последнему статус Рекомендации как отдельному документу.

– ITU-T Recommendation G.707/Y.1322 (2000), *Network node interface for the synchronous digital hierarchy (SDH)*.
– ITU-T Recommendation G.709/Y.1331 (2003), *Interfaces for the Optical Transport Network (OTN)*.
– ITU-T Recommendation G.783 (2000), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*.
– ITU-T Recommendation G.784 (1999), *Synchronous digital hierarchy (SDH) management*.
– ITU-T Recommendation G.798 (2002), *Characteristics of optical transport network hierarchy equipment functional blocks*.

– ITU-T Recommendation G.807/Y.1302 (2001), *Requirements for automatically switched transport networks (ASTN)*.

– ITU-T Recommendation G.872 (2001), *Architecture of optical transport networks*.

– ITU-T Recommendation G.874 (2001), *Management aspects of the optical transport network element*.

– ITU-T Recommendation G.7710/Y.1701 (2001), *Common equipment management function requirements*.

– ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the automatically switched optical networks (ASON)*.

– ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

– ITU-T Recommendation M.3013 (2000), *Considerations for a telecommunications management network*.

– ITU-T Recommendation M.3016 (1998), *TMN security overview*.

– ITU-T Recommendation Q.811 (1997), *Lower layer protocol profiles for the Q3 and X interfaces*.

– ITU-T Recommendation X.263 (1998) | ISO/IEC TR 9577:1999, *Information technology – Protocol identification in the Network Layer*.

– ISO/IEC 9542:1988, *Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*.

– ISO/IEC 10589:2002, *Information technology – Telecommunications and information exchange between systems – Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*.

– IETF RFC 791 (1981), *Internet Protocol DARPA Internet Program Protocol Specification*.

– IETF RFC 792 (1981), *Internet Control Message Protocol*.

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol*.

– IETF RFC 894 (1984), *A Standard for the Transmission of IP Datagrams over Ethernet Networks*.

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

– IETF RFC 1172 (1990), *The Point-to-Point Protocol (PPP) Initial Configuration Options*.

– IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*.

– IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP)*.

– IETF RFC 1377 (1992), *The PPP OSI Network Layer Control Protocol (OSINLCP)*.

– IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)*.

– IETF RFC 1662 (1994), *PPP in HDLC-like Framing*.

– IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

– IETF RFC 2328 (1998), *OSPF Version 2*.

– IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

– IETF RFC 2463 (1998), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

– IETF RFC 2472 (1998), *IP Version 6 over PPP*.

– IETF RFC 2740 (1999), *OSPF for IPv6*.

– IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.

3 Термины и определения

3.1 Термины, определение которых приведено в Рекомендации МСЭ-T G.709/Y.1331:

a) Блок обработки данных в оптическом канале (ODUk)

b) Транспортный блок в оптическом канале (OTUk)

c) Служебный сигнал оптического транспортного модуля (OOS)

3.2 Термин, определение которого приведено в Рекомендации МСЭ-TG.784:

a) Канал передачи данных (DCC)

3.3 Термины, определение которых приведено в Рекомендации МСЭ-T G.807/Y.1302:

a) Транспортная сеть с автоматической коммутацией (ASTN)

b) Межсетевой интерфейс (NNI)

c) Сетевой интерфейс пользователя (UNI)

3.4 Термины, определение которых приведено в Рекомендации МСЭ-T G.8080/Y.1304:

a) Контроллер вызовов (CallC)

b) Контроллер соединений (CC)

c) Интерфейс контроллеров соединений (CCI)

d) Контроллер подсети (SNCr)

3.5 Термины, определение которых приведено в Рекомендации МСЭ-T G.874:

a) Общий канал передачи данных (GCC)

b) Общие служебные сигналы управления передачей данных (COMMS OH)

3.6 Термины, определение которых приведено в Рекомендации МСЭ-T G.7710/Y.1701:

a) Расширенная управляющая сеть (xMN)

b) Расширенная управляющая подсеть (xMS)

3.7 Термин, определение которого приведено в Рекомендации МСЭ-T G.872:

a) Оптическая транспортная сеть (OTN)

3.8 Термины, определение которых приведено в Рекомендации МСЭ-T M.3010:

a) Устройство адаптации (AD)

b) Функция передачи данных (DCF)

c) Устройство согласования со средой передачи данных (MD)

d) Сетевой элемент (NE)

e) Функция сетевого элемента (NEF)

f) Операционная система (OS)

g) Функция операционной системы (OSF)

h) Q-интерфейс

i) Функция трансляции (преобразования)

j) Функция рабочей станции (WSF)

3.9 Термин, определение которого приведено в Рекомендации МСЭ-Т M.3013:

a) Функция передачи сообщений (MCF)

3.10 В настоящей Рекомендации даются определения следующих терминов:

3.10.1 Сеть передачи данных (DCN): сеть DCN представляет собой сеть, которая поддерживает функциональные возможности Уровня 1 (физического), Уровня 2 (звена передачи данных) и Уровня 3 (сетевого). Сеть DCN может быть разработана таким образом, чтобы поддерживать транспортировку сообщений распределенного управления сети передачи данных, относящихся к сети TMN, распределенной передачи сигнализации, относящейся к сети ASTN, и прочие операции по передаче данных (например, передача служебной информации/телефонная передача, пересылка по линиям связи программного обеспечения и т. п.).

3.10.2 Встроенный канал управления (ECC): канал ECC обеспечивает логический операционный канал между сетевыми элементами NE. Физический канал, поддерживающий канал ECC, зависит от используемой технологии. Примерами физических каналов, поддерживающих канал ECC, могут служить канал DCC в системе с SDH, канал GCC в сети OTN с системами OTUk/ODUk или канал COMMS OH в системе OOS в сети OTN.

3.10.3 Функция взаимодействия IP-маршрутизации: функция взаимодействия IP-маршрутизации дает возможность осуществлять передачу IP-топологии или IP-маршрута из одного протокола IP-маршрутизации в другой, несовместимый протокол IP-маршрутизации. Например, функция взаимодействия IP-маршрутизации может организовать шлюз между интегрированной системой IS-IS, маршрутируемой от сети DCN, и протоколом OSPF, маршрутируемым по этой же сети DCN.

3.10.4 Функция взаимодействия на сетевом уровне: функция взаимодействия на сетевом уровне дает возможность осуществлять совместное функционирование между узлами, которые поддерживают несовместимые протоколы на сетевом уровне. Примерами функции взаимодействия на сетевом уровне служат статические туннели базовой инкапсуляции маршрутизации (туннели GRE) или функция AE-DCF.

3.10.5 Функция автоматической инкапсуляции передачи данных (AE-DCF): функция AE-DCF производит автоматически инкапсуляцию пакетов, когда это потребуется, таким образом, чтобы с помощью элементов NE могла быть осуществлена их маршрутизация, если их дальнейшую передачу нельзя выполнить никаким другим способом. Функция AE-DCF обладает, помимо вышесказанного, возможностью согласования функции деинкапсуляции для восстановления рассматриваемого пакета в его первоначальную форму, если он прошел через несовместимые элементы NE.

4 Сокращения

В настоящей Рекомендации применяются следующие сокращения:

AD	Устройство адаптации
AE-DCF	Функция автоматической инкапсуляции передачи данных
ARP	Протокол преобразования адресов
ASON	Волоконно-оптическая сеть с автоматической коммутацией
ASTN	Транспортная сеть с автоматической коммутацией
ATM	Асинхронный режим передачи данных
CallC	Контроллер вызовов
CC	Контроллер соединений
CCI	Интерфейс контроллеров соединений
CLNP	Сетевой протокол передачи без установления соединения
CLNS	Сетевая служба без установления соединения
COMMS OH	Общие служебные сигналы управления передачей данных
DCC	Канал передачи данных
DCF	Функция передачи данных

DCN	Сеть передачи данных
DF	Не фрагментировать
ECC	Встроенный канал управления
EMF	Функция управления оборудованием
ES	Конечная система
ESH	Приветственное сообщение конечной системы (ISO 9542)
ES-IS	Конечная система – промежуточная система
GCC	Общий канал передачи
GNE	Сетевой элемент шлюза
GRE	Базовая инкапсуляция маршрутизации
HDLC	Высокоуровневое управление каналом передачи данных
ICMP	Протокол управляющего сообщения в Интернете
ID	Идентификатор
IIH	Приветственное сообщение промежуточная система – промежуточная система
IntISIS	Интегральная промежуточная система – промежуточная система
IP	Межсетевой протокол
IPCP	Управляющий протокол для межсетевого протокола (IP)
IPv4	Межсетевой протокол, версия 4
IPv6	Межсетевой протокол, версия 6
IS	Промежуточная система
ISDN	Цифровая сеть с интеграцией служб (ЦСИС)
ISH	Приветственное сообщение промежуточной системы (ISO 9542)
IS-IS	Промежуточная система – промежуточная система
IWF	Функция взаимодействия
LAN	Локальная (вычислительная) сеть (ЛВС)
LAPD	Протокол доступа к звену связи на канале D
LCN	Местная сеть передачи данных
LSP	Протокольный блок данных о состоянии канала
MAC	Управление доступом к среде передачи данных
MCF	Функция передачи сообщения
MCN	Сеть управления передачей данных
MD	Устройство согласования со средой передачи данных (Устройство медиатора)
MTU	Максимальный размер передаваемого блока
NE	Сетевой элемент
NEF	Функция сетевого элемента
NLPID	Идентификатор протокола сетевого управления
NNI	Межсетевой интерфейс

NSAP	Точка доступа к сетевой службе
ODUk	Блок обработки данных в оптическом канале
OOS	Служебный сигнал оптического транспортного модуля
OS	Операционная система
OSC	Оптический контрольный канал
OSF	Функция операционной системы
OSI	Интерфейс открытых систем
OSINLCP	Протокол управления сетевым управлением системы OSI
OSPF	Открытый протокол маршрутизации с определением кратчайшего маршрута
OTM	Оптический транспортный модуль
OTN	Оптическая транспортная сеть
OTUk	Устройство передачи по оптическому каналу
PDU	Протокольный блок данных
PPP	Протокол соединения "точка–точка"
RFC	Запрос на комментарий
SCN	Сеть передачи сигнализации
SDH	Синхронная цифровая иерархия
SID	Идентификатор системы
SNCr	Контроллер подсети
SP	Разбиение потока данных на ячейки (сегментация) разрешается
SPF	"Первый самый короткий путь"
TCP	Протокол управления передачей
TF	Функция преобразования
TLV	Тип Длина Значение
TMN	Сеть управления электросвязью
TNE	Элемент транспортной сети
UNI	Интерфейс пользователь–сеть
WAN	Территориально-распределенная сеть (ТРС)
WS	Рабочая станция
WSF	Функция рабочей станции
xMS	Расширенная управляющая подсеть

5 Соглашения

В настоящей Рекомендации используются следующие соглашения:

Мультимедийная сеть DCN: мультимедийная сеть DCN поддерживает несколько протоколов сетевого уровня (например OSI и IPv4). Мультимедийная сеть DCN допускает возможность того, что путь между двумя взаимодействующими объектами (например, системой OS и управляемым элементом NE) будет пересекать несколько частей, которые поддерживают только один протокол сетевого уровня (например, OSI), а также другие части, которые поддерживают другой протокол сетевого уровня (например, IPv4). Для обеспечения связи между такими объектами один протокол

сетевого уровня должен быть инкапсулирован в другой протокол сетевого уровня на границе рассматриваемых частей, которые поддерживают разные протоколы сетевого уровня.

Сеть DCN только с OSI: сеть DCN только с OSI поддерживает только протокол CLNP в качестве протокола сетевого уровня. Таким образом, путь, обозначенный только конечными точками между двумя взаимодействующими объектами (например, системой OS и управляемым элементом NE), будет поддерживать протокол CLNP, так что для поддержания подобной связи инкапсуляция одного протокола сетевого уровня в другой протокол сетевого уровня не потребуется.

Сеть DCN только с IPv4: сеть DCN только с IPv4 поддерживает только протокол IPv4 в качестве протокола сетевого уровня. Таким образом, путь, обозначенный только конечными точками между двумя взаимодействующими объектами (например, системой OS и управляемым элементом NE), будет поддерживать протокол IPv4, так что для поддержания подобной связи инкапсуляция одного протокола сетевого уровня в другой протокол сетевого уровня не потребуется.

Сеть DCN только с IPv6: сеть DCN только с IPv6 поддерживает только протокол IPv6 в качестве протокола сетевого уровня. Таким образом, путь, обозначенный только конечными точками между двумя взаимодействующими объектами (например, системой OS и управляемым элементом NE), будет поддерживать протокол IPv6, так что для поддержания подобной связи инкапсуляция одного протокола сетевого уровня в другой протокол сетевого уровня не потребуется.

6 Характеристики сети DCN

Для различных случаев применения (например, сети TMN, ASTN и т. п.) для передачи информации между различными компонентами требуется сеть связи, работающая в пакетном режиме. Например, сеть TMN требует такой сети связи, которая рассматривается как сеть управления передачей данных (MCN) для транспортировки управляющей информации между компонентами сети TMN (например, между компонентом функция NEF и компонентом функция OSF). Для сети ASTN требуется такая сеть связи, которая рассматривается как сеть передачи сигнализации (SCN) для транспортировки сигнальной информации между компонентами сети ASTN (например, компонентами контроллер CC). В настоящей Рекомендации рассматривается определение функций передачи данных, которые могут применяться для поддержания сети связи, предназначенной для одного или нескольких применений.

На рисунке 6-1 рассматриваются примеры применений, которые могут поддерживаться с помощью сети DCN. В зависимости от проекта сети каждое применение может поддерживаться разными сетями DCN или одной и той же сетью DCN.

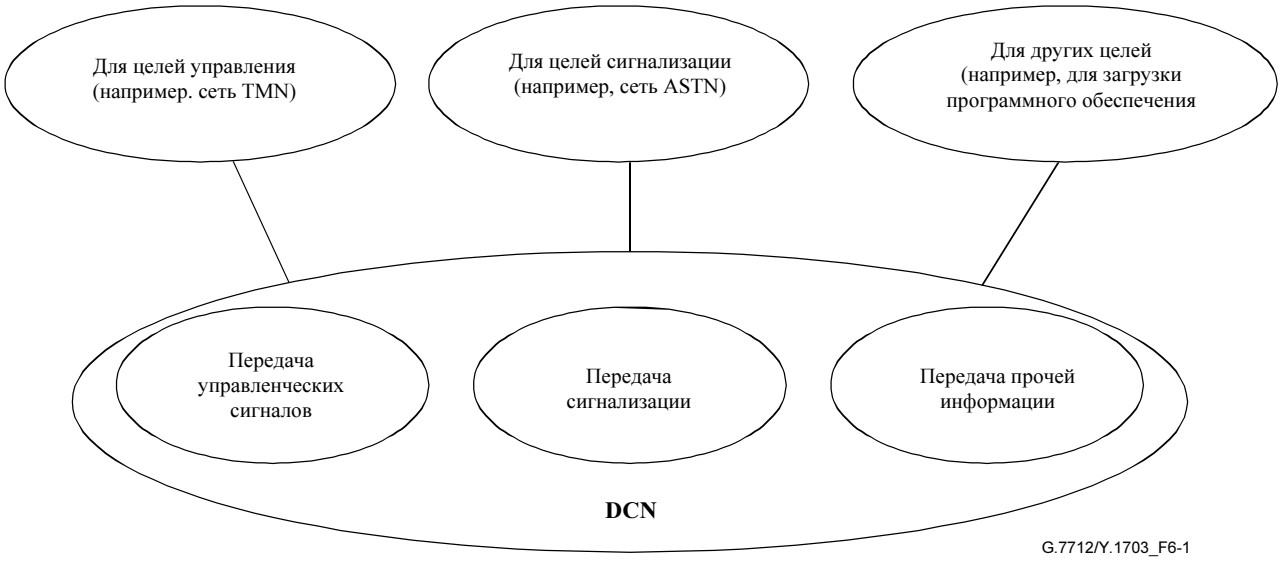


Рисунок 6-1/G.7712/Y.1703 – Примеры применений, поддерживаемых сетью DCN

Концептуально сеть DCN представляет собой совокупность ресурсов, предназначенных для поддержки передачи информации между распределенными компонентами. Как рассматривалось выше, примерами распределенной связи, которая может поддерживаться сетью DCN, являются распределенная передача сигналов управления, относящаяся к сети TMN, и распределенная передача

сигнализации, относящаяся к сети ASTN. В случае, когда сеть DCN поддерживает распределенную передачу сигналов управления, распределенными компонентами являются компоненты сети TMN (элементы NE, устройства AD, системы OS, устройства MD и рабочие станции WS, выполняющие такие функции сети TMN, как функции OSF, TF, NEF, WSF). В Рекомендациях МСЭ-Т M.3010 и M.3013 рассматриваются дальнейшие спецификации функций сети TMN. В случае, когда сеть DCN поддерживает распределенную передачу сигнализации, распределенными компонентами являются компоненты сети ASTN (элементы NE, выполняющие функции контроллеров SNCr в сети ASTN). В Рекомендациях МСЭ-Т G.807/Y.1302 и G.8080/Y.1304 рассматриваются дальнейшие спецификации функций сети ASTN.

Функции сети DCN, такие как коммутация каналов, пакетная коммутация, сеть LAN, режим ATM, иерархия SDH и сеть OTN, могут поддерживаться рядом технологий электросвязи. Важнейшими аспектами сети DCN являются качество обслуживания, скорость передачи информации и разнообразных методов маршрутизации для поддержания конкретных требований эксплуатации распределенной передачи, осуществляемой по сети DCN (например, распределенная передача управленческих сигналов, распределенная передачи сигнализации).

Целью спецификации интерфейса является обеспечение осмысленного взаимообмена данными между взаимосвязанными устройствами, с помощью которых по сети DCN выполняется передача заданной функции (например, работа сети TMN, работа сети ASTN). Интерфейс предназначен для обеспечения независимости типа устройства или поставщика. Для этого требуются совместимые протоколы обмена данными и совместимые представления данных для сообщений, в том числе совместимые видовые определения сообщений для управляющих функций сети TMN и управляющих функций сети ASTN.

Сеть DCN несет ответственность за обеспечение совместимой передачи на сетевом уровне (Уровень 3), уровне звена данных (Уровень 2) и физическом уровне (Уровень 1).

К рассмотрению интерфейсов необходимо подходить с точки зрения совместимости с наиболее эффективными устройствами транспортировки данных, которые имеются в каждом отдельно взятом сетевом элементе (например, арендованные каналы, соединение с коммутацией каналов, соединение с пакетной коммутацией, система сигнализации № 7, встроенные каналы управления с SDH, сети OTN и каналы D и B для доступа к сети ISDN).

В настоящей Рекомендации определяются три нижних уровня, предназначенные для передачи данных, и, следовательно, все взаимодействия между протоколами, действующими в рамках этих трех уровней. Эти взаимодействия обеспечиваются функцией передачи данных (DCF). Примеры подобного взаимодействия рассматриваются на рисунке 6-2. Необходимо отметить, что такое взаимодействие не завершает протоколы Уровня 3. Одним из примеров является взаимодействие между различными физическими уровнями, выполняемое с помощью общего протокола Уровня 2 (например, ретрансляция кадров MAC через интерфейс сети LAN в канал ECC). Другим примером может служить взаимодействие между различными протоколами уровня звена данных, выполняемое с помощью общего протокола Уровня 3 (например, маршрутизация IP-пакетов из интерфейса сети LAN в канал ECC). Третий пример, приведенный на рисунке 6-2, показывает взаимодействие между различными протоколами сетевого уровня, выполняемое с помощью функций туннелирования Уровня 3 (в этом примере интерфейс OSI инкапсулируется/туннелируется через IP; однако возможно также IP через инкапсулирование/туннелирование интерфейса OSI).

Тип информации, передаваемой между распределенными компонентами, зависит от типа интерфейсов, предусмотренных между этими компонентами. Сеть DCN, поддерживающая распределенную передачу управляющих сигналов, относящихся к сети TMN, требует реализации транспортировки информации, связанной с интерфейсами сети TMN, определение которых приводится в Рекомендации МСЭ-Т M.3010. Сеть DCN, поддерживающая распределенную передачу сигнализации, относящейся к сети ASTN, требует реализации транспортировки информации, связанной с интерфейсами сети ASTN, определение которых приводится в Рекомендации МСЭ-Т G.807/Y.1302.

Рисунок 6-2/G.7712/Y.1703 – Примеры взаимодействия на сети DCN

6.1 Применение сети TMN

Сеть TMN требует сети передачи, которая рассматривается как сеть управления передачей данных (MCN) для транспортировки управляющей информации между компонентами сети TMN (например, между компонентом функция NEF и компонентом функция OSF). На рисунке 6-3 представлен пример взаимосвязи сетей MCN и TMN. Представленные на рисунке 6-3 интерфейсы между различными элементами (например, системой OS, станцией WS, элементом NE) и сетью MCN являются логическими и могут быть реализованы через единственный физический интерфейс сети MCN или через несколько интерфейсов сети MCN.

На рисунке 6-4 представлен пример физической реализации сети MCN, поддерживающей распределенную передачу управляющих сигналов. В зависимости от выбора реализации сети MCN физические элементы могут предусматривать любую комбинацию интерфейсов канала ECC, интерфейсов сети LAN и интерфейсов сети WAN. На рисунке 6-4 представлены также типы функциональных блоков совокупности протоколов административного управления, которые могут быть реализованы в различных физических элементах. Подробные спецификации, относящиеся к этим функциональным блокам административного управления, изложены в Рекомендациях МСЭ-Т M.3010 и M.3013. Функция передачи данных (DCF) представляет собой часть каждого физического элемента и обеспечивает функции передачи данных.

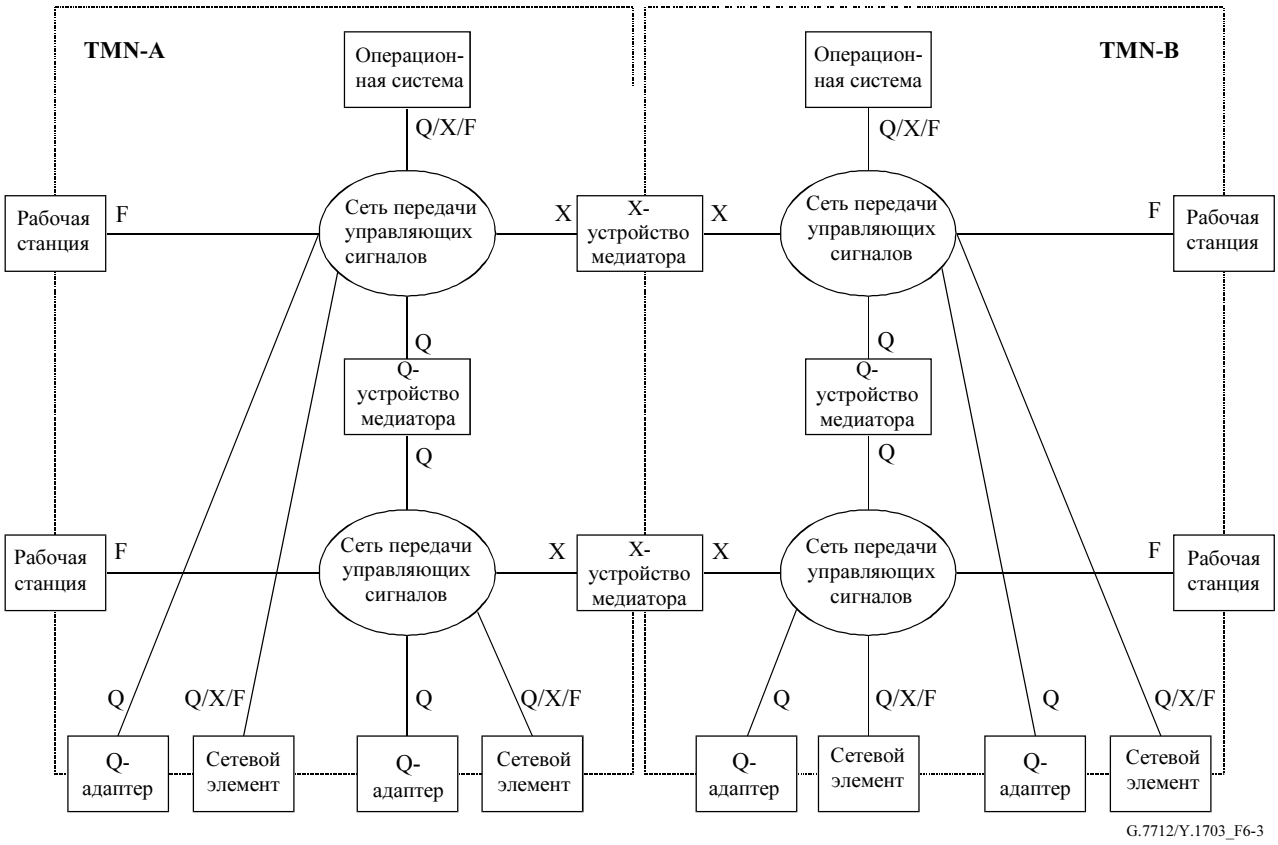


Рисунок 6-3/G.7712/Y.1703 – Пример взаимосвязи интерфейсов в сети TMN и сети MCN

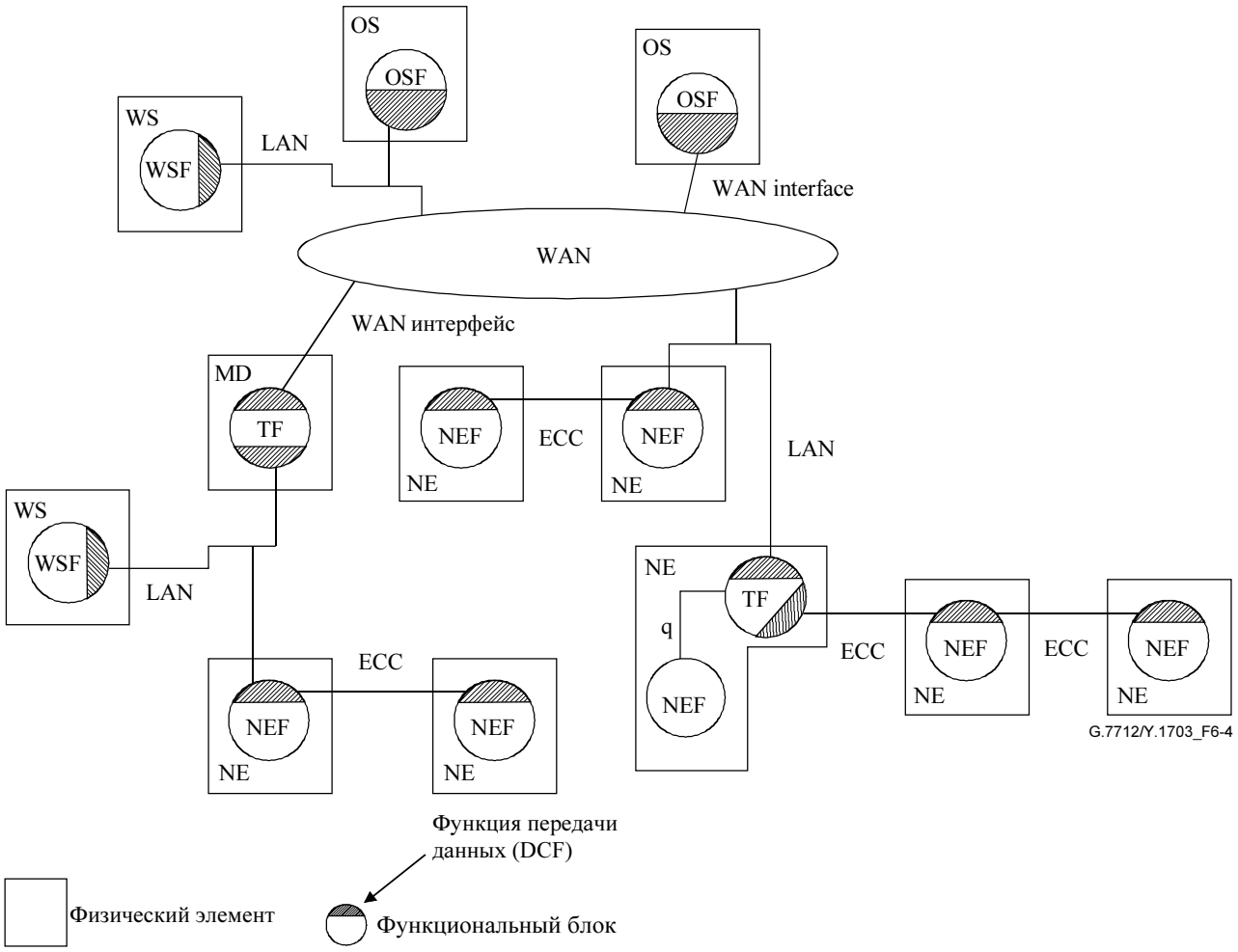


Рисунок 6-4/G.7712/Y.1703 – Пример физической реализации сети MCN, поддерживающей сеть TMN

6.1.1 Архитектура расширенной управляющей подсети

На рисунке 6-5 необходимо отметить несколько точек, относящихся к архитектуре расширенной управляющей подсети (xMS):

– *Большое число элементов NE в одном узле*

В любом заданном узле может появиться большое число имеющих адрес элементов NE с SDH или на сети OTN. Например, как представлено на рисунке 6-5, в одном узле оборудования могут быть одновременно размещены элементы NE_E и NE_G.

– *Элементы NE SDH/OTN и их функции взаимодействия*

Функция передачи сообщений элемента NE SDH и OTN завершает (с точки зрения более низких протокольных уровней) маршруты, а в других случаях производится обработка сообщений в канале ECC или подключения с помощью внешнего интерфейса.

i) Для окончания канала ECC требуются все элементы NE. Это означает, что каждый элемент NE должен быть в состоянии выполнять функции конечной системы интерфейса OSI или главного компьютера сети IP.

ii) Элементы NE могут потребоваться также для маршрутизации сообщений по каналу ECC между портами в соответствии с управляющей информацией маршрутизации, которая содержится в данном элементе NE. Это означает, что любой элемент NE также может потребовать выполнения функций промежуточной системы OSI или IP-маршрутизатора.

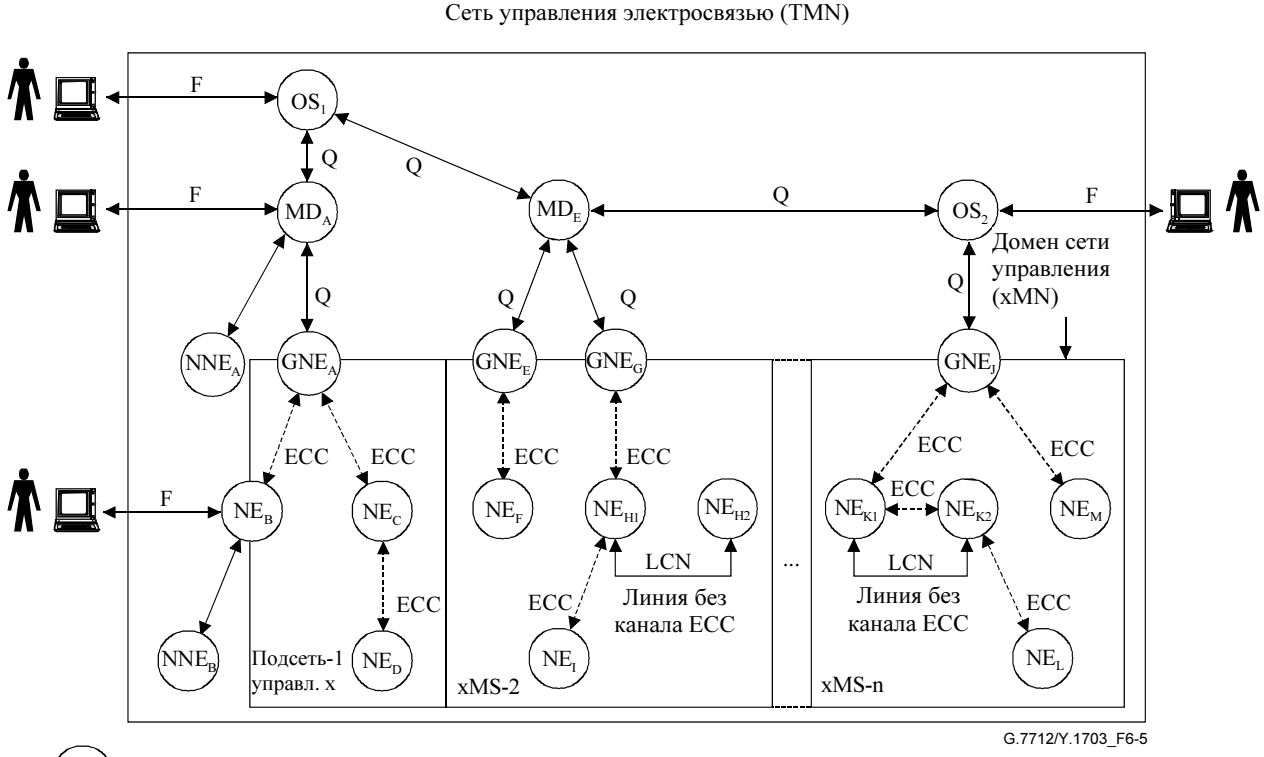
– *Межузловая передача SDH/OTN*

Межузловая или межстанционная линия связи между элементами NE SDH/OTN может быть организована каналами ECC SDH/OTN.

– *Передача SDH/OTN внутри узла*

В границах конкретного узла элементы NE SDH/OTN могут соединяться с помощью канала ECC внутри узла или с помощью местной сети передачи данных (сети LCN). На рисунке 6-5 представлены оба случая, относящихся к рассматриваемому интерфейсу.

ПРИМЕЧАНИЕ. – Стандартизированная сеть LCN для взаимосвязи между размещенными в одном узле сетевыми элементами была предложена в качестве альтернативы использованию канала ECC. Потенциально сеть LCN будет использоваться как общая сеть передачи, обслуживающая SDH, OTN и элементы NE без SDH/OTN (элементы NNE).



Блоки передачи (OS, MD, GNE, NE)

Линии передачи, использующей стандартный протокол Q-интерфейса

Канал ECC SDH/OTN

LCN Местная сеть связи

GNE Сетевой элемент шлюза

ПРИМЕЧАНИЕ. – Обозначение "Q" используется в значении видового определения.

Рисунок 6-5/G.7712/Y.1703 – Сеть TMN, сеть управления и модель подсети управления

6.1.1.1 Топология подсети управления

На рисунке 6-6 рассматриваются примеры топологий сети MCN, такие как линейная, кольцевая, с сеточной структурой и радиальная (звездообразная), использующие каналы ECC и/или местные сети передачи данных (LCN) (например, локальную сеть Ethernet LAN) в качестве физических каналов передачи данных, которые соединяют между собой сетевые элементы. На рисунке 6-7 рассматривается, каким образом с помощью каждой из перечисленных топологий можно осуществлять поддержку подсети управления. Общим для каждой топологии являются двухканальные шлюзы (GNE_1 и GNE_2), которые обеспечивают надежный доступ к элементам NE в границах подсети управления. Другим общим аспектом для каждой из приводимых в качестве примера топологий является тот факт, что каждая топология обеспечивает большое число различных путей между любыми элементами NE в границах подсети управления и операционной системы (OS).

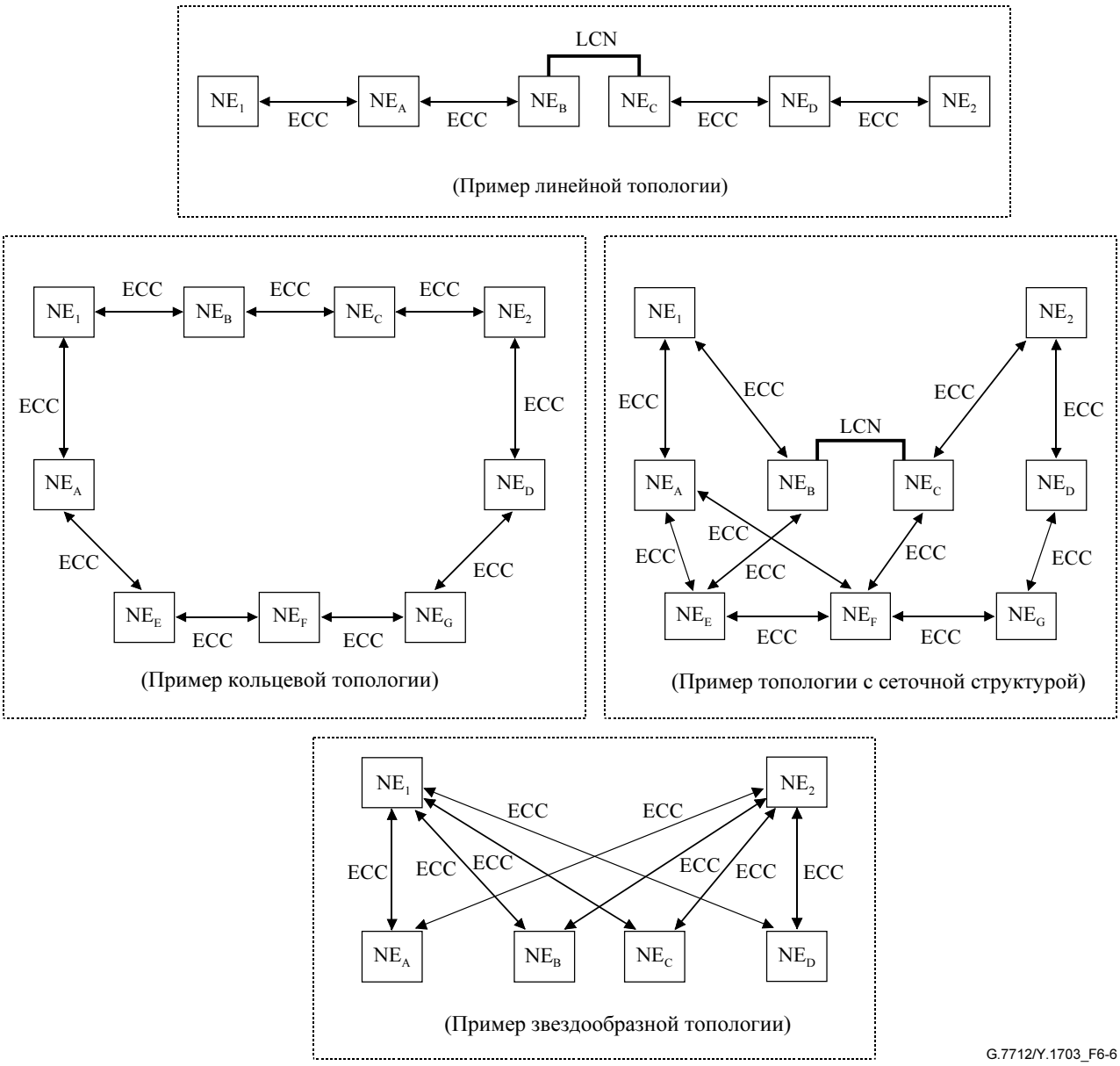


Рисунок 6-6/G.7712/Y.1703 – Примеры топологий

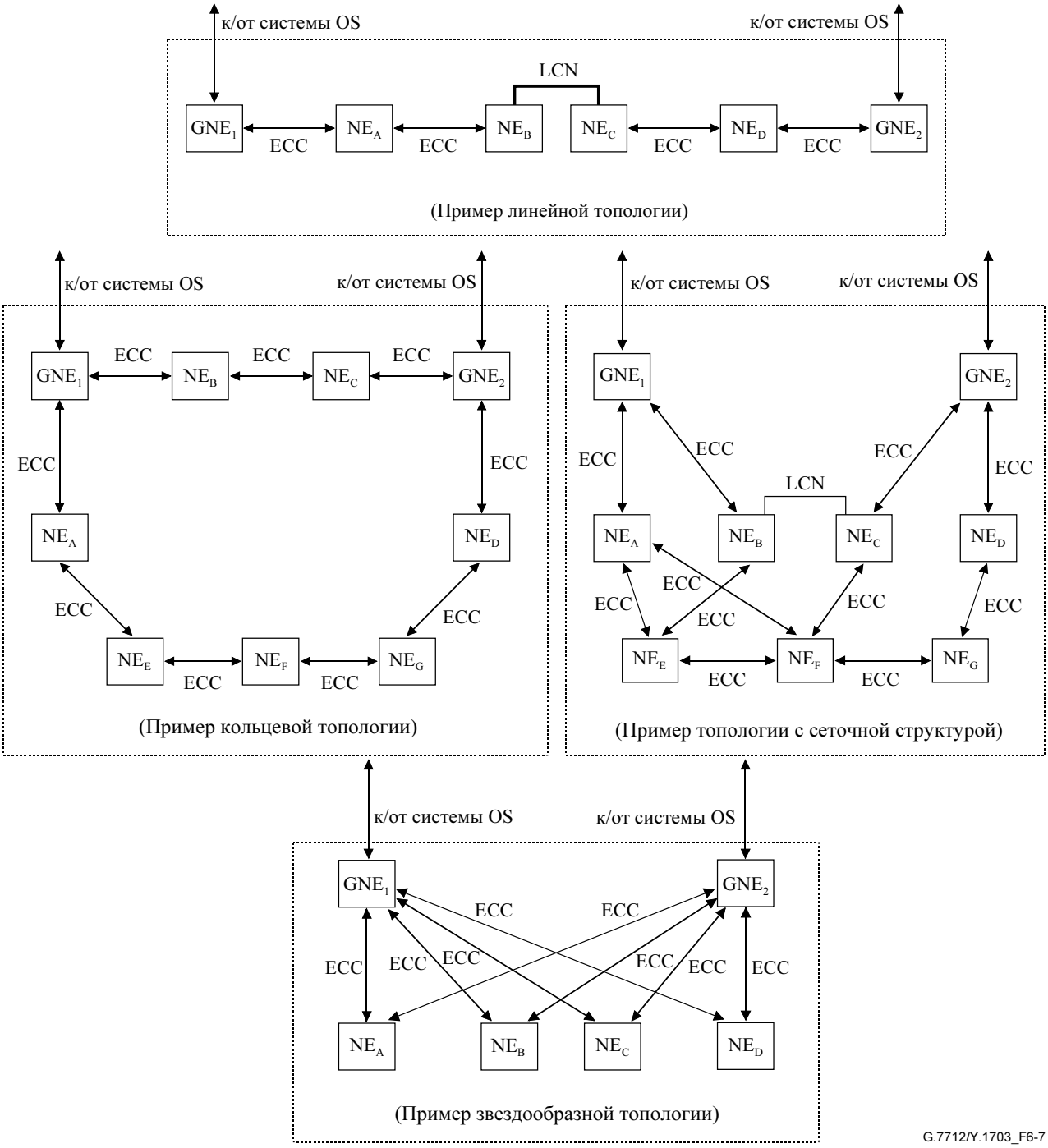


Рисунок 6-7/G.7712/Y.1703 – Поддержка подсистемы управления при использовании различных топологий

6.1.2 Надежность сети MCN

Сеть MCN должна быть спроектирована таким образом, чтобы помешать одиночной неисправности сделать невозможной передачу крайне важных сообщений, содержащих управленческую информацию.

Сеть MCN должна быть спроектирована таким образом, чтобы обеспечить положение, при котором перегрузка в сети MCN не служила бы причиной блокировки или чрезмерной задержки сообщений по управлению сетью, предназначенных для устранения отказа или неисправности.

Системы OS и элементы NE, которые обеспечивают функцию сообщения об аварийном состоянии, могут потребовать альтернативных или резервных (сдвоенных) каналов доступа к сети MCN для целей дублирования.

6.1.3 Безопасность сети MCN

Требования, предъявляемые к безопасности сети MCN, изложены в Рекомендации МСЭ-Т M.3016.

6.1.4 Функции передачи данных сети MCN

Функция DCF в объектах сети TMN должна поддерживать функциональные возможности конечной системы (ES) (в терминах OSI) или главного компьютера сети (в терминах IP).

- Когда функция DCF в объектах сети TMN поддерживает интерфейсы канала ECC, необходимо поддерживать следующие функции:
  - функцию доступа к каналу ECC (как определено в параграфе 7.1.1);
  - функцию завершения звена данных в канале ECC (как определено в параграфе 7.1.2);
  - функцию инкапсуляция "блока PDU сетевого уровня в уровень звена данных в канале ECC" (как определено в параграфе 7.1.3).
- Когда функция DCF в объектах сети TMN поддерживает интерфейсы сети Ethernet LAN, необходимо поддерживать следующие функции:
  - функцию завершения физического уровня сети Ethernet LAN (как определено в параграфе 7.1.4);
  - функцию инкапсуляции "блока PDU сетевого уровня в кадр Ethernet" (как определено в параграфе 7.1.5).

Функция DCF в объектах сети TMN может действовать как промежуточная система (IS) (в терминах OSI) или как маршрутизатор (в терминах IP). Функция DCF в объектах сети TMN, которая действует как IS/Routers, должна быть способна обеспечить маршрутизацию в своей зоне Уровня 1 и, следовательно, обеспечить функциональные возможности работы IS/Router на Уровне 1. Кроме того, функция DCF в объекте сети TMN может быть подготовлена к работе в качестве IS/Router на Уровне 2, благодаря чему обеспечивается способность выполнения маршрутизации из одной зоны в другую. Функциональные возможности IS/Router Уровня 2 необязательно должны проявляться в функции DCF всех объектов сети TMN. В качестве примера функции DCF, поддерживающей функциональные возможности IS/Router Уровня 2, можно считать функцию DCF в шлюзовом элементе NE.

- Когда функция DCF в объектах сети TMN действует как IS/Router, необходимо поддерживать следующие функции:
  - функцию продвижения данных блока PDU сетевого уровня (как определено в параграфе 7.1.6);
  - функцию маршрутизации на сетевом уровне (как определено в параграфе 7.1.10).

Функция DCF в объекте сети TMN, которая поддерживает протокол IP, может подключаться напрямую к функции DCF в соседнем объекте сети TMN, который может работать только с интерфейсом OSI.

- Когда функция DCF в объекте сети TMN поддерживает протокол IP, подключается напрямую к функции DCF в соседнем объекте сети TMN, который работает только с OSI, в функции DCF, поддерживающей протокол IP, необходимо поддерживать следующую функцию:
  - функцию взаимодействия блока PDU сетевого уровня (как определено в параграфе 7.1.7).

Функция DCF в объекте сети TMN может быть вынуждена осуществлять продвижение данных блока PDU сетевого уровня по сети, которая не работает с сетевым уровнем этого типа.

- Когда функция DCF в объекте сети TMN должна осуществлять продвижение данных блока PDU сетевого уровня по сети, которая не поддерживает сетевой уровень этого типа, необходимо поддерживать следующие функции:
  - функцию инкапсуляции блока PDU сетевого уровня (как определено в параграфе 7.1.8);
  - функцию туннелирования блока PDU сетевого уровня (как определено в параграфе 7.1.9).

Функция DCF в объекте сети TMN, которая поддерживает протокол IP, использующий маршрутизацию по протоколу OSPF, может быть подключена напрямую к функции DCF в соседнем объекте сети TMN, который поддерживает протокол IP, использующий систему IntISIS.

- Когда функция DCF в объекте сети TMN, который поддерживает протокол IP, использующий маршрутизацию по протоколу OSPF, подключается напрямую к функции DCF в соседнем объекте сети TMN, который поддерживает протокол IP, использующий системы IntISIS, необходимо, чтобы в функции DCF, поддерживающей протокол OSPF, поддерживалась следующая функция:
  - функция взаимодействия маршрутизации по протоколу IP (как определено в параграфе 7.1.11).

6.2 Применение сети ASTN

Сеть ASTN требует сети передачи, которая рассматривается как сеть передачи сигнализации (SCN) для транспортировки сигнальных сообщений между компонентами сети ASTN (например, между компонентами контроллера CC).

На рисунке 6-8 представлен пример взаимосвязи сетей SCN и ASTN. Представленные на рисунке 6-8 интерфейсы между различными элементами и сетью SCN являются логическими и могут быть реализованы через единственный физический интерфейс сети SCN или через несколько интерфейсов сети SCN.

На рисунке 6-9 представлен пример физической реализации сети SCN, поддерживающей распределенную передачу сигнализации. В зависимости от выбора реализации сети SCN физические элементы могут предусматривать любую комбинацию интерфейсов канала ECC, интерфейсов сети LAN и интерфейсов сети WAN. На рисунке 6-9 представлены также типы функциональных блоков совокупности протоколов управления, которые могут быть реализованы в различных физических элементах. Подробные спецификации, относящиеся к этим функциональным блокам управления, изложены в Рекомендациях МСЭ-Т G.807/Y.1302 и G.8080/Y.1304. Функция передачи данных (DCF) представляет собой часть каждого физического элемента и обеспечивает функциональные возможности передачи данных.

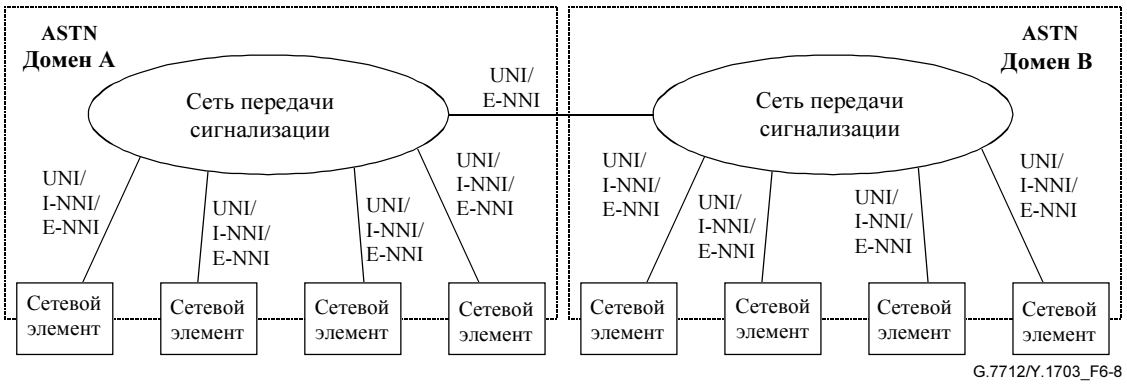


Рисунок 6-8/G.7712/Y.1703 – Пример взаимосвязи интерфейсов сети ASTN и сети SCN

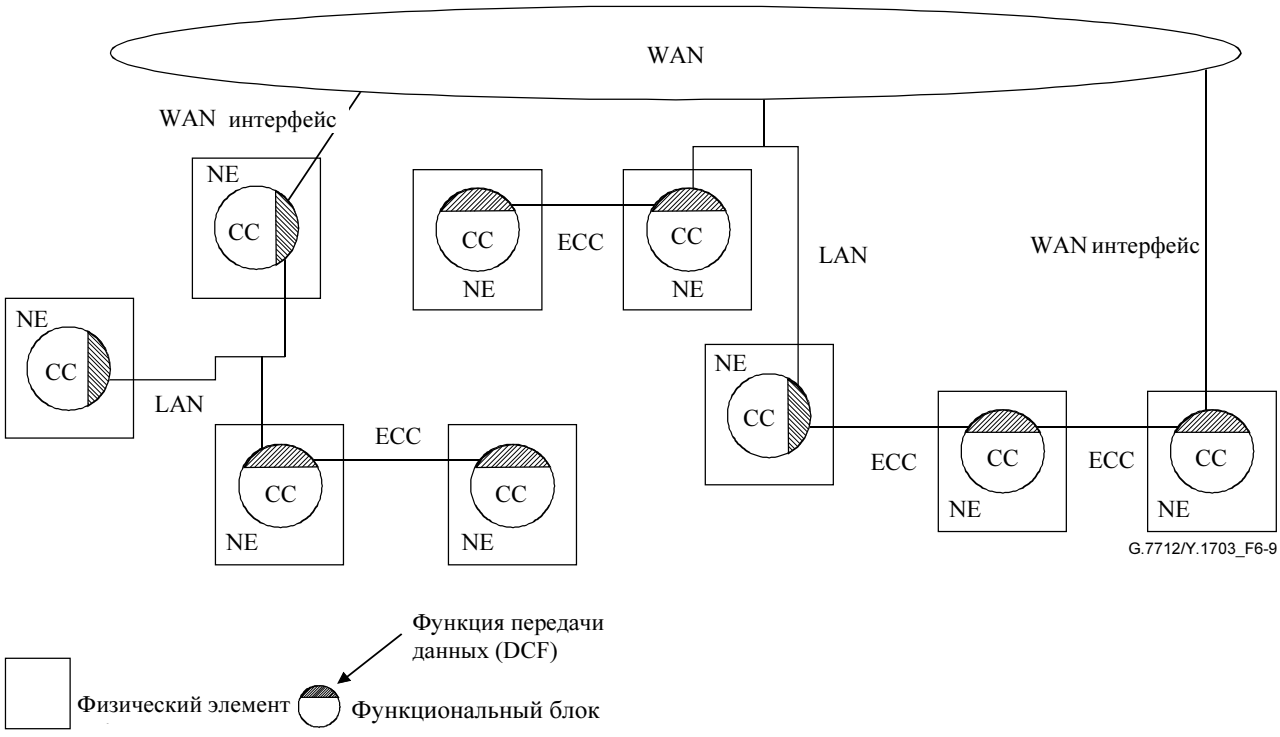


Рисунок 6-9/G.7712/Y.1703 – Пример физической реализации сети SCN, поддерживающей сеть ASTN

6.2.1 Топология сети SCN

На рисунке 6-10 рассматриваются примеры топологий сети SCN, такие как линейная, кольцевая, с сеточной структурой и радиальная (звездообразная), использующие каналы ECC и/или местные сети передачи (LCN) (например, локальную сеть Ethernet LAN), в качестве физических каналов передачи данных, которые соединяют между собой сетевые элементы. На рисунке 6-11 рассматривается, каким образом с помощью каждой из перечисленных топологий можно осуществлять поддержку сети сигнализации сети ASTN. Общим для каждой топологии является тот факт, что между объектами передачи (связи) (например, элементами NE сети ASTN) обеспечивается большое число различных путей. Следует отметить, что для поддержки различных альтернативных путей между взаимосвязанными элементами NE сети ASTN в случае использования линейной топологии может быть предоставлена внешняя линия WAN между краевыми элементами NE сети ASTN.

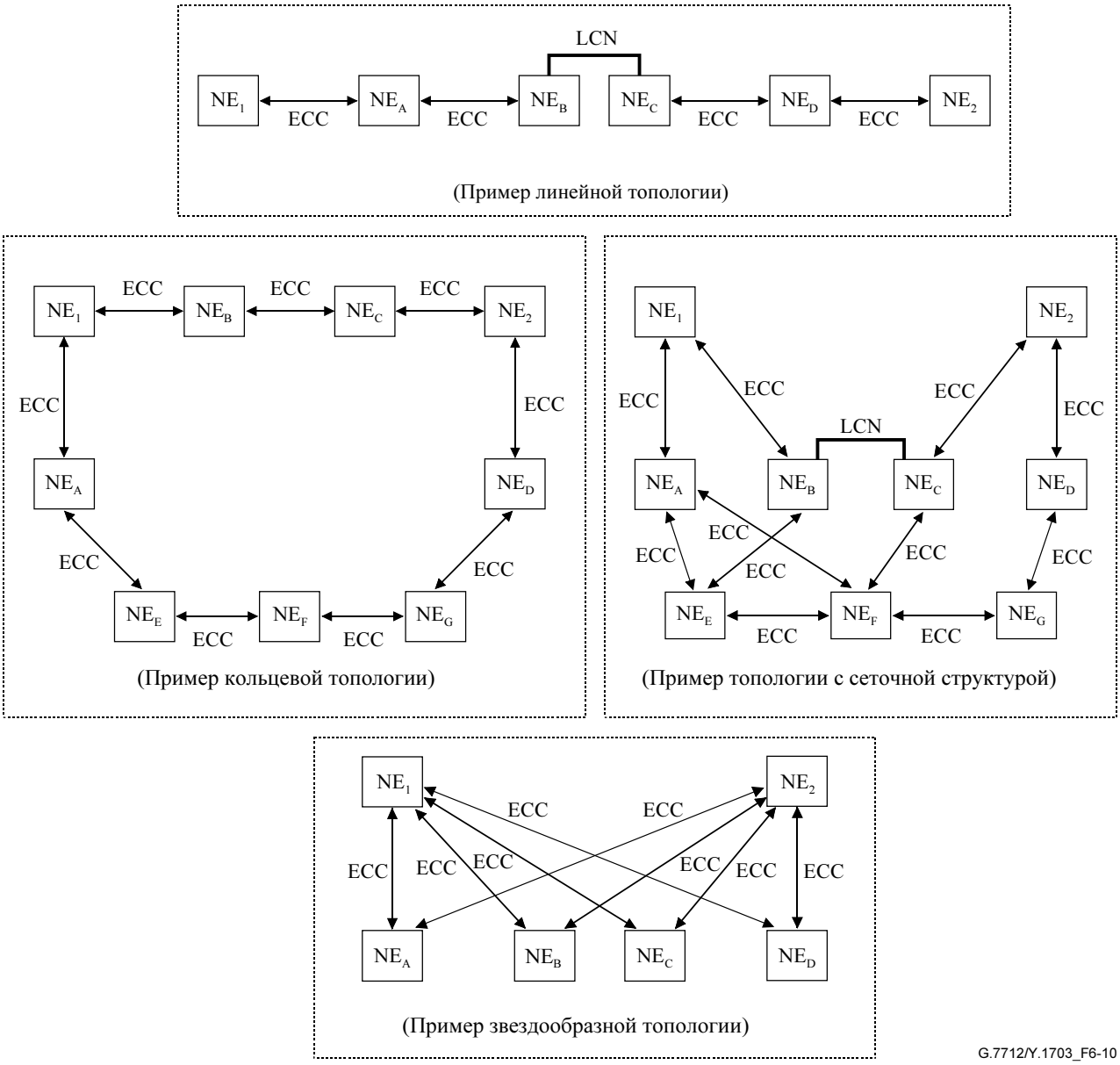


Рисунок 6-10/G.7712/Y.1703 – Примеры топологий

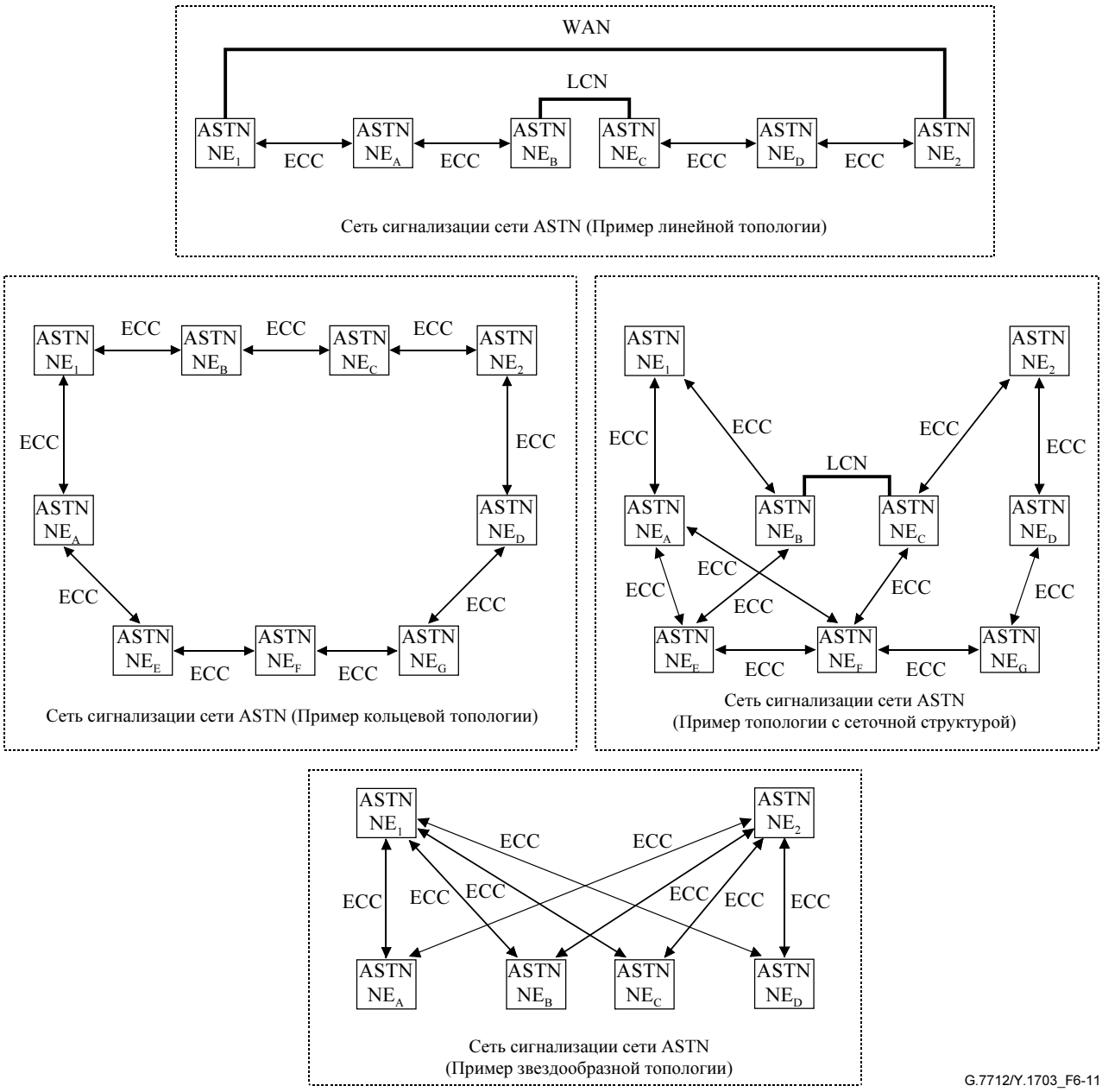


Рисунок 6-11/G.7712/Y.1703 – Поддержка сети сигнализации сети ASTN при использовании различных топологий

Ни рисунке 6-12 рассматривается возможность, при которой сеть сигнализации сети ASTN состоит из трех различных частей: потребитель–сеть, домен внутриадминистративного управления и домен межадминистративного управления. Этот пример показывает, что в качестве физических линий взаимосоединения элементов NE сети ASTN применяется технология с сетчатой структурой, использующая каналы ECC, местные сети передачи данных (например, сеть Ethernet LAN) и арендованные линии (например, DS1/E1, VC-3/4). Топология домена внутриадминистративного управления дает возможность осуществлять сигнализацию, располагая для этого альтернативными различными путями между двумя взаимосоединяемыми элементами NE сети ASTN. Топология домена межадминистративного управления зависит от того, какие соглашения были приняты Административными доменами A и B. Этот пример показывает точки доступа по двум направлениям между этими Административными доменами. Топология части потребитель–сеть зависит от того, какие соглашения были приняты между потребителем и поставщиком услуг. Этот пример показывает, что между потребителем и сетью существует только одна точка доступа.

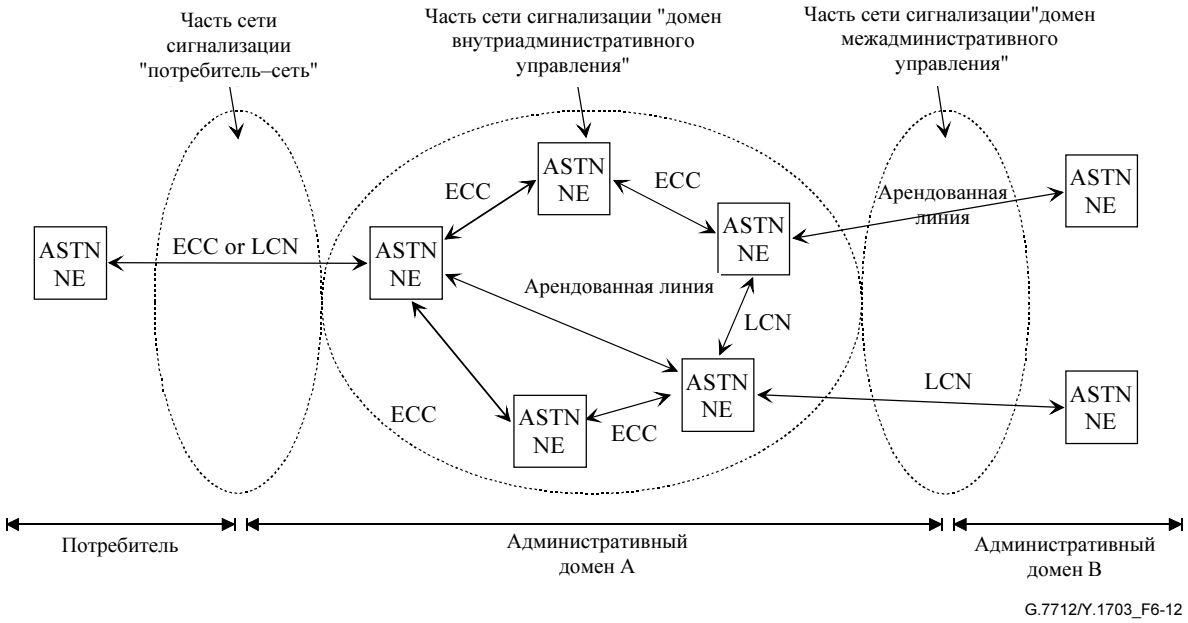


Рисунок 6-12/G.7712/Y.1703 – Пример сети SCN

6.2.2 Надежность сети SCN

На рисунке 6-13 рассматриваются управляющие сообщения сети ASTN, которые передаются по сети SCN. На рисунке представлены следующие логические интерфейсы:

UNI Интерфейс пользователь–сеть.

NNI Межсетевой интерфейс.

CCI Интерфейс контроллеров соединений.

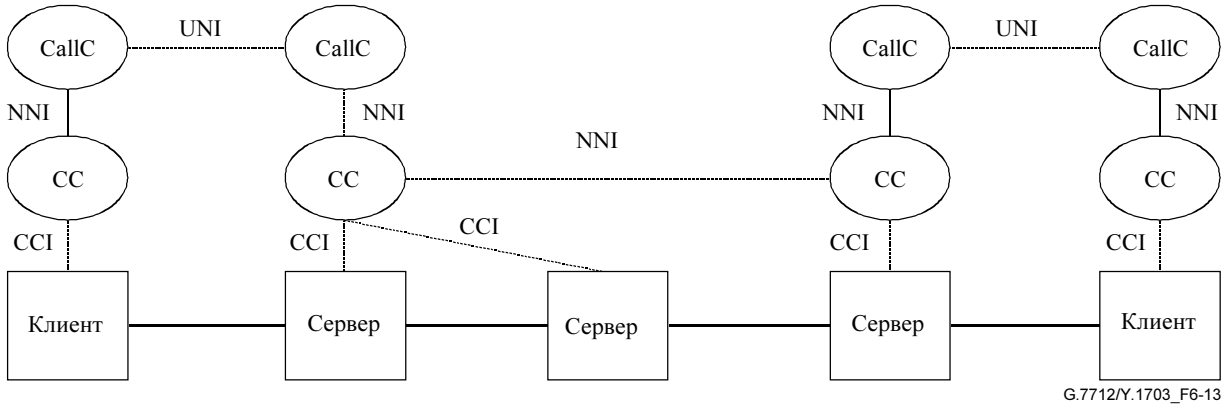


Рисунок 6-13/G.7712/Y.1703 – Интерфейсы сети ASTN, поддерживаемые сетью SCN

На приведенном примере показано, что логические интерфейсы UNI, NNI и CCI работают через сеть SCN. Сеть SCN может состоять из различных подсистем, а это приводит к тому, что логические каналы могут совместно использовать общие физические маршруты с транспортной сетью, но подобная конфигурация не требуется, но и не исключается.

Вполне возможна ситуация, когда в сети SCN возникает отказ, не зависящий от транспортной сети. Подобный сценарий представлен на рисунках 6-14 и 6-15. В этом примере, где основное внимание уделяется передаче сообщений сети ASTN по сети SCN, появление независимого отказа может оказать вредное влияние на запросы установить новое соединение и завершить соединение.

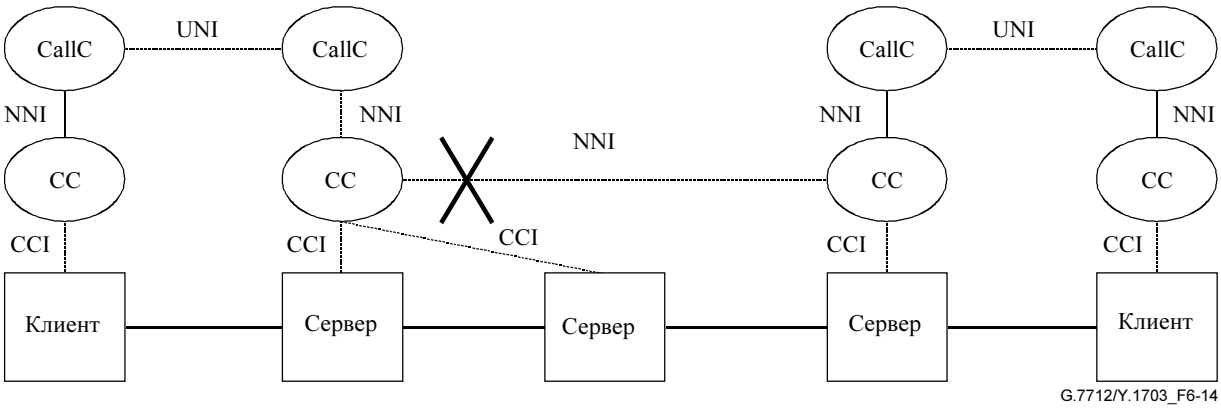


Рисунок 6-14/G.7712/Y.1703 – Отказ сети SCN, оказывающий влияние на интерфейс сигнализации

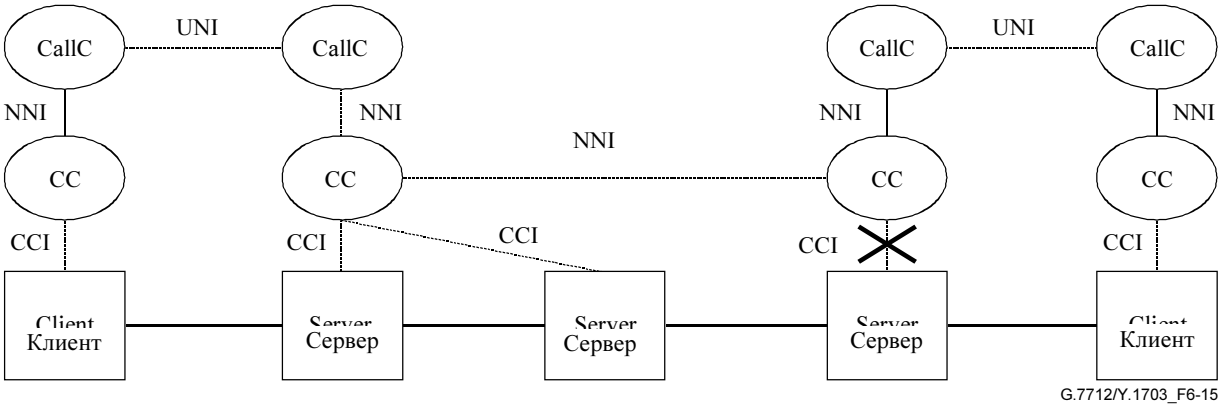


Рисунок 6-15/G.7712/Y.1703 – Отказ сети SCN, оказывающий влияние на интерфейс CCI

Как представлено на рисунке 6-15, некоторые логические каналы в сети SCN могут также совместно использовать общие физические маршруты в рассматриваемой транспортной сети. В подобном случае в сети SCN может возникнуть отказ, который вызывается транспортной сетью (т. е. отказ прерывает как трафик в сети SCN, так и трафик в транспортной сети), что иллюстрируется на рисунке 6-16. В этом примере, где основное внимание уделяется передаче сообщений сети ASTN по сети SCN, появление такого отказа может оказать вредное влияние на устранение его, когда сеть ASTN используется для восстановления существующих соединений. Следовательно, для сети SCN является крайне важным обеспечить способность противостоять отказам при передаче сообщений о восстановлении нормального состояния.

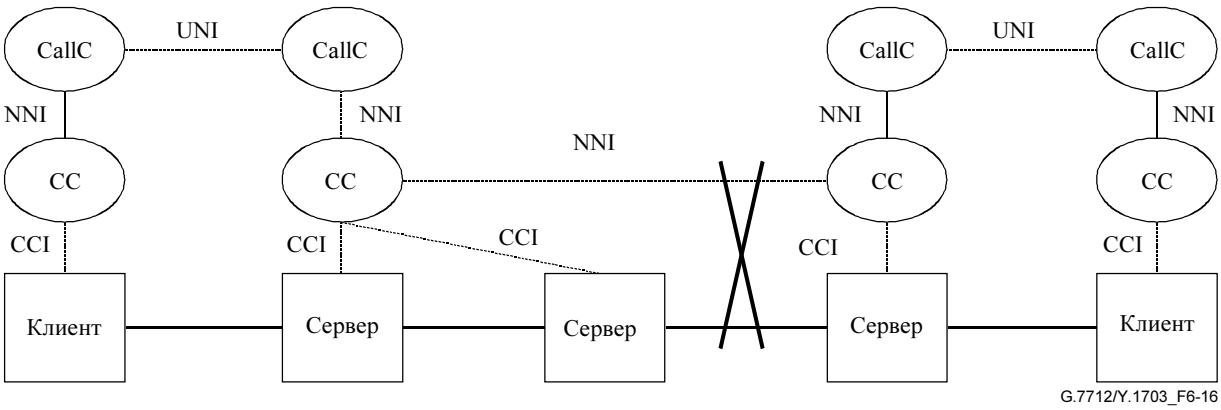


Рисунок 6-16/G.7712/Y.1703 – Отказ сети SCN, оказывающий влияние как на интерфейсы сигнализации, так и на интерфейсы передачи данных

Если применение сети ASTN используется только для обеспечения установления или завершения соединений, вполне достаточной будет сеть SCN без установления соединений. Однако, если сеть ASTN используется также и для восстановления, может потребоваться сеть SCN с установлением соединений. Для такой сети SCN потребуется спецификация дополнительных функций для поддержания услуг сети, ориентированной на установление соединений.

К сети SCN предъявляются следующие требования в отношении надежности:

Сеть SCN должна поддерживать различные уровни восстановления в зависимости от требований в отношении надежности, предъявляемым к передающим компонентам, для чего и производится транспортировка (т. е. восстановление может поддерживаться между этими передающими компонентами, требующими высоконадежной передачи без требования восстановления, которое должно поддерживаться всеми передающими компонентами).

Одним из способов достижения надежности сети SCN является применение пакетного режима с защитой 1+1 для протокола, ориентированного на установление соединений, например MPLS, как описано в параграфе 6.2.4.

Сеть SCN может обеспечить транспортировку сообщений о восстановлении. В подобном случае сеть SCN должна предусмотреть скорости восстановления, обеспечивающие надлежащую работу соединений, для которых осуществляется управление сообщениями о восстановлении.

6.2.3 Безопасность сети SCN

Сеть SCN, поддерживающая передачу сообщений сети ASTN, может обеспечивать способность к подключению между различными административными доменами. Когда сеть SCN обеспечивает способность к подключению между административными границами, необходимо предпринимать такие меры предосторожности, чтобы только те сообщения, которые получают разрешение проходить между этими двумя административными доменами, могли пересечь интерфейс, тогда как другие сообщения, которые не получают разрешения проходить между административными доменами, были не в состоянии пересечь этот интерфейс. Необходимо, чтобы сеть SCN обеспечивала положение, при котором только выбранному набору сообщений, имеющих разрешение административных сторон на любом конце интерфейса, фактически предоставлялась возможность осуществить переход через этот интерфейс.

6.2.4 Функции передачи данных сети SCN

Функция DCF в объектах сети ASTN должна поддерживать функциональные возможности конечной системы (ES) (в терминах OSI) или главного компьютера (в терминах IP).

- Когда функция DCF в объектах сети ASTN поддерживает интерфейсы канала ECC, необходимо поддерживать следующие функции:
  - функцию доступа к каналу ECC (как определено в параграфе 7.1.1);
  - функцию завершения звена данных в канале ECC (как определено в параграфе 7.1.2);
  - функцию инкапсуляции "блока PDU сетевого уровня в уровень звена данных в канале ECC" (как определено в параграфе 7.1.3).
- Когда функция DCF в объектах сети ASTN поддерживает интерфейсы сети Ethernet LAN, необходимо поддерживать следующие функции:
  - функцию завершения уровня сети Ethernet LAN (как определено в параграфе 7.1.4);
  - функцию инкапсуляции "блока PDU сетевого уровня в кадр Ethernet" (как определено в параграфе 7.1.5).

Функция DCF в объектах сети ASTN может действовать как промежуточная система (IS) (терминах OSI) или как маршрутизатор (в терминах IP). Функция DCF в объектах сети ASTN, которая действует как IS/Routers, должна быть способна обеспечить маршрутизацию в своей зоне Уровня 1 и, следовательно, обеспечить функциональные возможности работы IS/Router на Уровне 1. Кроме того, функция DCF в объекте сети ASTN может быть подготовлена к работе в качестве IS/Router Уровня 2, благодаря чему обеспечивается способность выполнения маршрутизации из одной зоны в другую. Функциональные возможности IS/Router Уровня 2 необязательно должны проявляться в функции DCF всех объектов сети ASTN.

- Когда функция DCF в объектах сети ASTN действует как IS/Router, необходимо поддерживать следующие функции:
  - функцию передачи данных блока PDU сетевого уровня (как определено в параграфе 7.1.6);
  - функцию маршрутизации на сетевом уровне (как определено в параграфе 7.1.10).

Функция DCF в объекте сети ASTN, которая поддерживает протокол IP, может подключиться напрямую к функции DCF в соседнем объекте сети ASTN, который может работать только с функцией OSI.

- Когда функция DCF в объекте сети ASTN, которая поддерживает протокол IP, может подключаться напрямую к функции DCF в соседнем объекте сети TMN, который работает только с OSI, в функции DCF, поддерживающей протокол IP, необходимо поддерживать следующую функцию:
  - функцию взаимодействия блока PDU сетевого уровня (как определено в параграфе 7.1.7).

Функция DCF в объекте сети ASTN может быть вынуждена осуществлять продвижение данных блока PDU сетевого уровня по сети, которая не работает с сетевым уровнем подобного типа.

- Когда функция DCF в объекте сети ASTN должна осуществлять продвижение данных блока PDU сетевого уровня по сети, которая не работает с сетевым уровнем подобного типа, необходимо поддерживать следующие функции:
  - функцию инкапсуляции блока PDU (как определено в параграфе 7.1.8);
  - функцию туннелирования блока PDU сетевого уровня (как определено в параграфе 7.1.9).

Функция DCF в объекте сети ASTN, которая поддерживает протокол IP, использующий маршрутизацию по протоколу DCF, может быть подключена напрямую к функции DCF в соседнем объекте ASTN, который поддерживает протокол IP, использующий систему IntISIS.

- Когда функция DCF в объекте сети ASTN, который поддерживает протокол IP, использующий маршрутизацию по протоколу OSPF, подключается напрямую к функции DCF в соседнем объекте сети ASTN, который поддерживает протокол IP, использующий систему IntISIS, необходимо, чтобы в функции DCF, поддерживающий протокол OSPF, поддерживалась следующая функция:
  - функция взаимодействия маршрутизации по протоколу IP (как определено в параграфе 7.1.11).

Функция DCF в объектах сети ASTN может работать как краевой маршрутизатор (LER).

Когда функция DCF в объектах сети ASTN работает как маршрутизатор LER, необходимо поддерживать следующие функции:

- если функция DCF поддерживает интерфейсы канала ECC, то это будет функция инкапсуляции "блока PDU коммутации MPLS в уровень звена данных канала ECC" (как определено в параграфе 7.1.13);
- если функция DCF поддерживает интерфейсы сети LAN, то это будет функция инкапсуляции "блока PDU коммутации MPLS в кадр Ethernet" (как определено в параграфе 7.1.14);
- функцию сигнализации блока LSP коммутации MPLS (как определено в параграфе 7.1.15);
- функцию продвижения данных блока LSP коммутации MPLS (как определено в параграфе 7.1.16);
- функцию вычисления пути блока LSP коммутации MPLS (как определено в параграфе 7.1.17).
- функцию инкапсуляции "блока PDU сетевого уровня в коммутацию MPLS" (как определено в параграфе 7.1.18).

Функция DCF в объектах сети ASTN может работать как коммутатор-маршрутизатор (LSR).

Когда функция DCF в объектах сети ASTN работает как коммутатор-маршрутизатор LSR, необходимо поддерживать следующие функции:

- если функция DCF поддерживает интерфейсы канала ECC, то это будет функция инкапсуляции "блока PDU коммутации MPLS в уровень звена данных канала ECC" (как определено в параграфе 7.1.13);
- если функция DCF поддерживает интерфейсы сети LAN, то это будет функция инкапсуляции "блока PDU коммутации MPLS в кадр Ethernet" (как определено в параграфе 7.1.14);
- функцию сигнализации блока LSP коммутации MPLS (как определено в параграфе 7.1.15);
- функцию продвижения данных блока LSP коммутации MPLS (как определено в параграфе 7.1.16).

Функция DCF в объектах сети ASTN может обеспечивать возможность применения пакетного режима с защитой 1+1.

Минимальными требованиями, предъявляемыми к обеспечению возможности применения пакетного режима с защитой 1+1, являются следующие:

- отсутствие добавочных возможностей, необходимых на внутренних узлах сети;
- сеть должна поддерживать возможность установления соединений по большому числу различных маршрутов.
- *Входной узел*
  - должен располагать возможностью связывать два соединения, которые используются для обеспечения применения пакетного режима с защитой 1+1 между двумя конечными узлами;
  - должен поддерживать перенос идентификатора в пакет, который будет служить для идентификации дублированных копий этого пакета в выходном узле;
  - должен располагать возможность спаренной подачи каждого пакета в эти два спаренные соединения.
- *Выходной узел*
  - должен располагать возможностью связывать два соединения, которые используются для обеспечения применения пакетного режима с защитой 1+1 между двумя конечными узлами;
  - должен располагать возможностью идентификации дублированных копий пакета спаренной подачи с использованием имеющегося идентификатора;
  - должен располагать возможностью выбора и передачи одной и только лишь одной копии пакета.

Механизм, используемый для связывания двух различных соединений, а также формат и местоположение идентификатора последовательности должны соответствовать определенным в параграфе 7.1.19.

6.3 Прочие применения, для которых требуются сети передачи

Помимо применения в сетях TMN и ASTN существуют и другие службы, такие как телефонная связь (например, передача служебной информации), пересылка по линиям связи программного обеспечения и связь для конкретного оператора, требующие наличия сети передачи для обеспечения транспортировки информации между компонентами.

6.4 Классификация различных применений

В зависимости от проекта сети, ее размера, пропускной способности каналов связи, требований, которые предъявляются к безопасности и эффективности, возможны различные уровни классификации большого количества применений (например, сети TMN, ASTN). Под уровнем классификации понимается выбор, который делается среди операторов и поставщиков на этапе выполнения проектирования сети. Ниже приводятся примеры различных уровней классификации.

Вариант A: Сеть DCN может быть спроектирована таким образом, что сети MCN, SCN и прочие применения (например, сеть связи, разработанная в соответствии с требованиями конкретного оператора) действуют в сетях уровня 3 (например, совместно используют одну и ту же сеть IP).

Вариант B: Сеть DCN может быть спроектирована таким образом, что сети MCN, SCN и прочие применения (например, сеть связи, разработанная в соответствии с требованиями конкретного оператора) действуют на разных сетях уровня 3, тем не менее, они не могут осуществлять совместную передачу по некоторым из имеющихся физических каналов.

Вариант C: Сеть DCN может быть спроектирована таким образом, что сети MCN, SCN и прочие применения (например, сеть связи, разработанная в соответствии с требованиями конкретного оператора) работают в разных физических сетях (т. е. в разных сетях уровня 3, в которых ни один физический канал не подлежит совместному использованию.

7 Функциональная архитектура сети DCN и предъявляемые к ней требования

Требования, предъявляемые в настоящем параграфе к архитектуре сети DCN, относятся только к доменам IP, только к доменам OSI и к смешанным доменам IP+OSI. Эти требования не зависят от применяемой технологии. В Рекомендациях, связанных с конкретной технологией, таких как Рекомендация МСЭ-T G.784, где рассматривается иерархия SDH, и в Рекомендации МСЭ-T G.874, где рассматривается сеть OTN, определяются, какие именно требования применимы для каждой конкретной технологии.

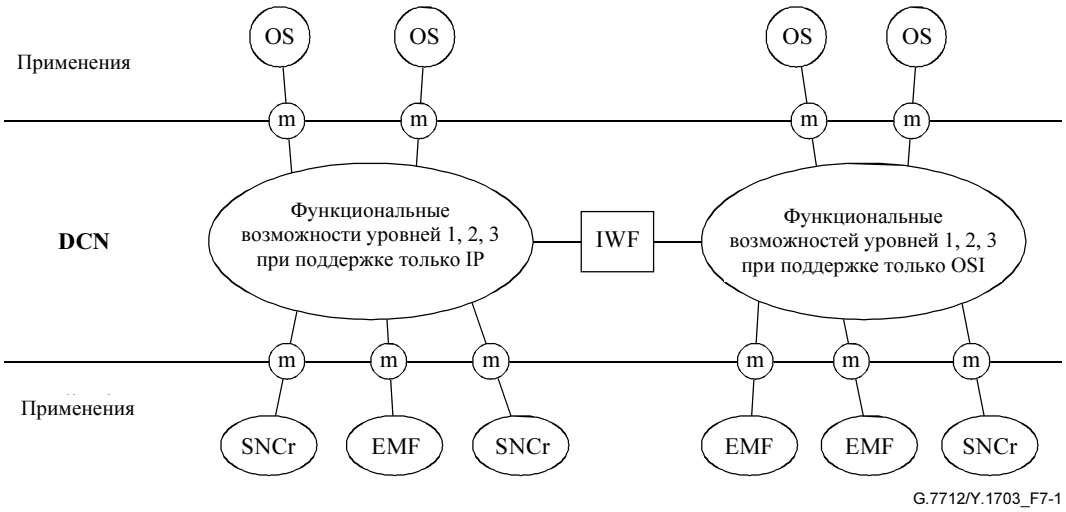
Сеть DCN известна протоколам Уровня 1, Уровня 2 и Уровня 3; кроме того, она является прозрачной для протоколов более высоких уровней, используемых в тех применениях, для которых эта сеть является транспортной.

Сеть DCN может быть спроектирована таким образом, что она может поддерживать только протокол IP. Сеть DCN, поддерживающая только протокол IP, может иметь в своем составе несколько различных подсетей, которые используют разные протоколы физического уровня и уровня звена данных; тем не менее, все эти подсети будут поддерживать протокол IP как протокол сетевого уровня.

Однако, поскольку встроенные сети DCN поддерживают интерфейс OSI, некоторые из них могут иметь в своем составе части, которые поддерживают только протокол IP, только интерфейс OSI и оба эти протокола IP и OSI.

Те части сети DCN, которые поддерживают протокол IP (т. е. либо те части, которые поддерживают только протокол IP, либо те части, которые поддерживают IP и OSI), могут состоять из функций DCF, которые поддерживают только протокол IP (т. е. функций DCF с одним набором только протоколов IP), и/или функций DCF, которые поддерживают IP+OSI (например, функция CDF с двоичным набором, который способен выполнять маршрутизацию как IP-пакетов, так и OSI-пакетов). Те части сети DCN, которые поддерживают только OSI, будут состоять из функций DCF, которые поддерживают только OSI (т. е. функция DCF с одним набором только OSI).

На рисунке 7-1 представлена функциональная архитектура сети DCN. Как уже указывалось ранее, сеть DCN может состоять из частей, которые поддерживают только протоколы IP, только OSI, а также поддерживают как протоколы IP, так и OSI. Рассматриваются также функция взаимодействия (функция IWF) между теми частями сети DCN, которые поддерживают только протокол IP, только OSI и IP+OSI, а также функции отображения, которые осуществляют отображение применений в IP-уровне. Для обеспечения подобной транспортировки сеть DCN поддерживает функциональные возможности Уровня 1 (физического), Уровня 2 (звена данных) и Уровня 3 (сетевого). Помимо этого рассматриваются требования, предъявляемые к архитектуре для тех частей сети DCN, которые поддерживают только IP, только OSI, а также требования, предъявляемые к взаимодействию тех частей сети DCN, которые поддерживают только IP, только OSI, а также IP+OSI. На рисунке 7-1 овал, представляющий часть сети DCN, в которой поддерживается только IP, соответствует абстрактному представлению этой сети DCN и вследствие этого может быть также применим к одиночному элементу NE IP, взаимосвязанному с элементами NE OSI с помощью функции IWF.



IWF Функция взаимодействия
SNCr Контроллер соединения в подсети
EMF Функция управления оборудованием
OS Операционная система
m отображение между применением и сетью DCN

Рисунок 7-1/G.7712/Y.1703 – Функциональная архитектура сети DCN

7.1 Технические требования, предъявляемые к функциям передачи данных

В настоящем параграфе рассматриваются технические требования, предъявляемые к различным функциям передачи данных, которые относятся к интерфейсам канала ECC, интерфейсам сети LAN Ethernet и возможностям сетевого уровня.

7.1.1 Функция доступа к каналу ECC

Функция доступа к каналу ECC обеспечивает доступ к битовому потоку, передаваемому по каналу ECC. Эта функция определяется в рекомендациях, рассматривающих оборудование, выполненное по конкретным технологиям (например, Рекомендациях МСЭ-Т G.783 и G.798). Скорости передачи данных и определения различных каналов ECC (например, DCC, GCC и общие служебные сигналы COMMS OH в канале OSC) рассматриваются в рекомендациях, рассматривающих конкретные технологии (например, Рекомендациях МСЭ-Т G.784 и G.874).

7.1.2 Функция завершения уровня звена данных в канале ECC

Функция завершения уровня звена данных в канале ECC обеспечивает общую обработку на уровне звена данных независимо от блока PDU сетевого уровня, инкапсулированного в кадр уровня звена данных. Отображение этого кадра уровня звена данных в канал ECC также обеспечивается этой функцией. Функция рассматривается в Рекомендациях, в которых речь идет о конкретных технологиях. Однако функция завершения уровня звена данных SDH канала ECC с точки зрения ее спецификации рассматривается ниже.

7.1.2.1 Функция завершения уровня звена данных SDH в канале ECC

7.1.2.1.1 Отображение кадра уровня звена данных SDH в канале ECC

Объединенный в кадр сигнал протокола HDLC представляет собой последовательный поток битов, в котором содержатся заполненные кадры, окруженные одной или несколькими последовательностями флагов. Формат такого объединенного в кадр сигнала протокола HDLC рассматривается в Рекомендации МСЭ-Т Q.921 в связи с протоколом LAPD и в RFC 1662 в связи с протоколом PPP в кадрировании протокола HDLC. Кадр протокола HDLC состоит из N октетов, как показано на рисунке 7-2. Этот кадр передается справа налево и сверху вниз. После всех последовательностей из пяти последовательных битов 1 в контенте кадра протокола HDLC (октеты с 2 до N-1) вставляется бит 0, гарантирующий, что в кадре не будет сымитирована последовательность флагов или аварийного завершения.

Отображение объединенного в кадр сигнала протокола HDLC в канал DCC синхронизируется по битам (а не по октетам), поскольку заполненный кадр протокола HDLC необязательно содержит целое число октетов как следствие процесса введения 0. Поэтому в канале DCC отсутствует прямое отображение заполненного кадра протокола HDLC в байты. Генератор сигналов протокола HDLC получает свою синхронизацию от функции ServerLayer/DCC_A (т. е. от сигнала DCC_CI_CK) для иерархии SDH. Следующие функции ServerLayer/DCC_A определяются в Рекомендации МСЭ-Т G.783; функция MSn/DCC_A, функция MS256/DCC_A и функция RSn/DCC_A.

Сигнал кадра протокола HDLC представляет собой поток последовательных битов и может быть введен в канал DCC таким образом, что биты будут передаваться через модуль STM-N в том же порядке, в каком они были приняты из генератора сигналов фрейма протокола HDLC.

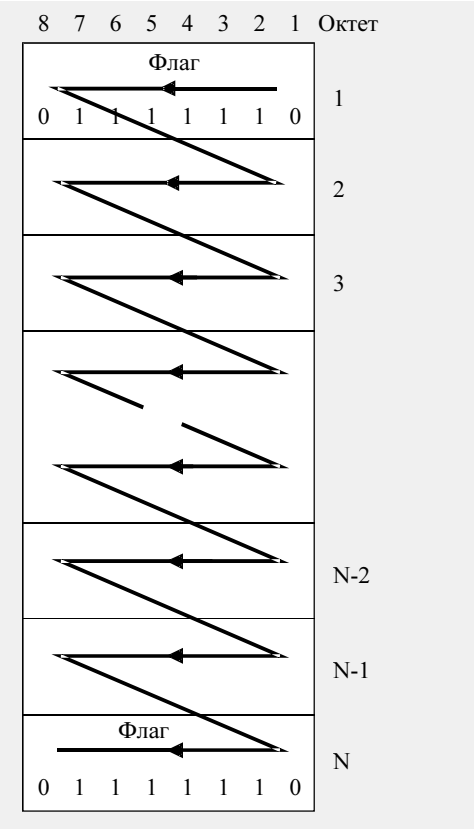


Рисунок 7-2/G.7712/Y.1703 – Формат кадра протокола HDLC

7.1.2.1.2 Спецификация протокола уровня звена данных SDH в канале ECC

В настоящем параграфе определяются три типа интерфейсов: интерфейсы только IP, интерфейсы только OSI и сдвоенные интерфейсы (сдвоенными интерфейсами называют такие интерфейсы, которые могут передавать как пакеты IP, так и пакеты OSI). Когда по каналу DCC передача ведется только через протокол IP, то в качестве протокола уровня звена данных следует использовать кадрирование PPPinHDLC. Поскольку сдвоенные интерфейсы могут работать и с IP, и с OSI, то такой интерфейс может подключаться либо к интерфейсу, действующему только по протоколу IP, либо к интерфейсу, действующему только как интерфейс OSI, либо к другому сдвоенному интерфейсу. Интерфейс, действующий только как OSI, существует в сетях, используемых в настоящее время; протокол уровня звена данных, применяемый для подобных интерфейсов, – это протокол LAPD, рассматриваемый в Рекомендации МСЭ-Т G.784. Чтобы обеспечить возможность сдвоенным интерфейсам подключаться либо к интерфейсам только IP, либо к интерфейсам только OSI, необходимо, чтобы протокол уровня звена данных, поддерживаемый в этом сдвоенном интерфейсе, располагал возможностью изменять конфигурацию для поддержки либо протокола PPPinHDLC, либо протокола LAPD. Исключение допускается для встроенных элементов сети NE SDH, поддерживающих протокол в аппаратном обеспечении, которое модернизируется для поддержки сдвоенных интерфейсов. Для ограничения объема работ по модернизации аппаратного обеспечения допускается модернизация элементов NE SDH, предназначенных только для поддержки протокола LAPD.

7.1.2.1.2.1 Интерфейс только IP-протокола

Интерфейсы только IP-протокола представлены на рисунке 7-3.

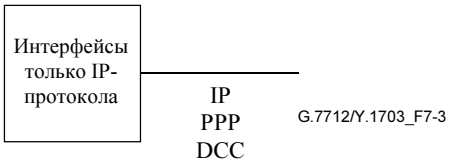


Рисунок 7-3/G.7712/Y.1703 – Интерфейс только IP-протокола

Интерфейсы только IP-протокола должны использовать протокол PPP (см. RFC 1661).

7.1.2.1.2.2 Интерфейс только OSI

Интерфейсы только OSI представлены на рисунке 7-4.

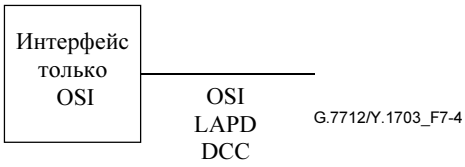


Рисунок 7-4/G.7712/Y.1703 – Интерфейс только OSI

Интерфейсы только OSI должны использовать протокол LAPD (см. Рекомендацию МСЭ-Т G.784).

7.1.2.1.2.3 Сдвоенный интерфейс (IP+OSI)

Сдвоенные интерфейсы (сдвоенными называются интерфейсы, которые могут передавать пакеты OSI и IP), могут подключаться к интерфейсам только IP, интерфейсам только OSI или к другим сдвоенным интерфейсам. Чтобы обеспечить возможность сдвоенным интерфейсам подключаться к другим интерфейсам только IP или к другим интерфейсам только OSI, необходимо, чтобы протокол уровня звена данных, поддерживаемый в этом сдвоенном интерфейсе, располагал возможностью изменять конфигурацию для переключения с протокола PPP при кадрировании в протоколе HDLC (см. RFC 1662) в протокол LAPD (см. Рекомнедацию МСЭ-Т G.784), как это представлено на рисунке 7-5. Необходимо отметить, что встроенные элементы NE SDH, поддерживающие протокол LAPD в аппаратном обеспечении и подлежащие модернизации для поддержки протокола IP, не требуются для поддержки протокола PPP при кадрировании в протоколе HDLC в этих рассматриваемых сдвоенных интерфейсах. Поэтому такие сдвоенные интерфейсы требуются только для поддержки протокола LAPD.

Рисунок 7-5/G.7712/Y.1703 – Сдвоенные интерфейсы

Сдвоенные интерфейсы, поддерживающие протокол PPP, должны использовать протокол PPP (см. RFC 1661).

Сдвоенные интерфейсы, поддерживающие протокол LAPD должны использовать протокол LAPD (см. Рек. МСЭ-Т G.784).

7.1.3 Функция инкапсуляции "блока PDU сетевого уровня в кадр канала ECC уровня звена данных"

Функция инкапсуляции "блока PDU сетевого уровня в кадр канала ECC уровня звена данных" осуществляет инкапсуляцию и декапсуляцию блока PDU сетевого уровня в кадр уровня звена данных. Эта функция также обрабатывает идентификатор протокола. Она рассматривается в Рекомендациях, о которых речь идет об использовании конкретных технологий. Тем не менее спецификация функции инкапсуляции "блока PDU сетевого уровня в кадр канала ECC SDH уровня звена данных" рассматривается ниже.

7.1.3.1 Функция инкапсуляции "блока PDU сетевого уровня в кадр канала ECC SDH звена данных"

Специализация функции инкапсуляции "блока PDU сетевого уровня в кадр канала ECC SDH звена данных" для интерфейсов только IP, интерфейсов только OSI и сдвоенных интерфейсов описывается ниже.

7.1.3.1.1 Интерфейсы только IP

Интерфейсы только IP должны использовать только протокол PPPinHDLC кадрирования/канал DCC (см. RFC 1662).

Интерфейс только IP определяется следующим образом:

Конец передачи

– должен ввести пакеты IS-IS непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении OSI (см. RFC 1377) в протокольное поле протокола PPP;

– должен ввести пакеты IPv4 непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении IPv4 (см. RFC 1332) в протокольное поле протокола PPP;

– должен ввести пакеты IP непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении IPv6 (см. RFC 2472) в протокольное поле протокола PPP.

Конец приема

– Пакет IS-IS идентифицирован, если протокольное поле протокола PPP имеет протокольное значение OSI (см. RFC 1377) и если этот пакет имеет идентификатор NLPID для IS-IS, как это определено в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577.

– Пакет IPv4 идентифицирован, если протокольное поле протокола PPP имеет протокольное значение IPv4 (см. RFC 1332).

– Пакет IPv6 идентифицирован, если протокольное поле протокола PPP имеет протокольное значение IPv6 (см. RFC 2472).

7.1.3.1.2 Интерфейс только OSI

Интерфейсы только OSI должны использовать только протокол LAPD/канал DCC (см. Рекомендацию МСЭ-Т G.784).

Интерфейс только OSI определяется следующим образом:

Конец передачи

– должен ввести пакеты CLNP, IS-IS и ES-IS непосредственно в полезную нагрузку протокола LAPD (см. Рекомендацию МСЭ-Т G.784).

Конец приема

– должен проверить идентификатор протокола, размещенный в первом октете полезной нагрузки протокола LAPD. Значение этого идентификатора совместимо со значением, указанным в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577. Если принятый блок PDU предназначен для протокола, не поддерживаемого приемником, то такой блок PDU следует отбросить.

7.1.3.1.3 Сдвоенный (IP+OSI) интерфейс

Сдвоенный интерфейс, поддерживающий протокол PPP в качестве протокола звена данных, определяется следующим образом:

Конец передачи

– должен ввести пакеты CLNP, IS-IS и ES-IS непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении OSI (см. RFC 1377) в протокольное поле протокола PPP;

– должен ввести пакеты IPv4 непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении IPv4 (см. RFC 1332) в протокольное поле протокола PPP;

– должен ввести пакеты IPv6 непосредственно в информационное поле протокола PPP (см. RFC 1661) при протокольном значении IPv6 (см. RFC 2472) в протокольное поле протокола PPP.

Конец приема

– Пакет OSI идентифицирован, если протокольное поле протокола PPP имеет протокольное значение OSI (см. RFC 1377).

– Пакет IPv4 идентифицирован, если протокольное поле протокола PPP имеет протокольное значение IPv4 (см. RFC 1332).

– Пакет IPv6 идентифицирован, если протокольное поле протокола PPP имеет протокольное значение IPv6 (см. RFC 2472).

Сдвоенный интерфейс, поддерживающий протокол LAPD в качестве протокола звена данных, определяется следующим образом:

Конец передачи

– должен ввести пакеты CLNP, IS-IS и ES-IS непосредственно в полезную нагрузку протокола LAPD (см. Рекомендацию МСЭ-Т G.784);
– должен ввести пакеты IP непосредственно в полезную нагрузку протокола LAPD, в начале которой добавлен состоящий из одного октета идентификатор протокола. Этот идентификатор совместим со значениями для IPv4 и IPv6, указанными в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577.

Конец приема

– должен проверить идентификатор протокола, размещенный в первом октете полезной нагрузки протокола LAPD. Значение этого идентификатора совместимо со значениями, указанными в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577. Если принятый блок PDU предназначен для протокола, не поддерживаемого приемником, то такой блок PDU следует отбросить.

7.1.4 Функция завершения физического уровня сети Ethernet LAN

Функция завершения физического уровня сети Ethernet LAN завершает физический интерфейс Ethernet.

Необходимо работать на одной или на нескольких из следующих скоростей передачи: 1 Мбит/с, 10 Мбит/с, 100 Мбит/с.

Доступ к прекратившим работу каналам ECC допускается с помощью сетевых элементов, поддерживающих интерфейсы сети Ethernet LAN. Не все сетевые элементы, поддерживающие каналы ECC, должны поддерживать порты сети Ethernet LAN, пока имеется путь канала ECC от сетевого элемента, завершающего канал ECC, до другого сетевого элемента, обеспечивающего порты сети Ethernet LAN.

7.1.5 Функция инкапсуляции "блока PDU в кадр Ethernet frame"

Эта функция осуществляет инкапсуляцию и декапсуляцию блока PDU сетевого уровня в кадр 802.3 или кадр Ethernet frame (версия 2).

С ее помощью должна выполняться инкапсуляция блоков PDU сетевого уровня в кадры 802.3 или Ethernet frame (версия 2) в соответствии со следующими правилами.

- Она должна инкапсулировать и декапсулировать блоки PDU для CLNP, IS-IS и ES-IS в кадры 802.3 (см. Рекомендацию МСЭ-Т Q.811).
- Она должна инкапсулировать и декапсулировать пакеты IP в кадры Ethernet frame (версия 2) (см. RFC 894).
- IP-адреса должны быть отображены в адреса Ethernet MAC с помощью протокола преобразования адресов (см. RFC 826).

Она должна определить тип принятого кадра (802.3 или Ethernet версия 2), как указано в разделе 2.3.3 (см. RFC 1122).

7.1.6 Функция передачи данных блока PDU сетевого уровня

Функция передачи данных блока PDU сетевого уровня осуществляет передачу пакетов сетевого уровня.

Если эта функция передает пакеты протокола CLNP, то она должна передавать пакеты протокола CLNP, как это описано в Рекомендации МСЭ-Т Q.811.

Если эта функция передает пакеты IPv4, то она должна передавать пакеты IPv4, как это описано в RFC 791.

Если эта функция передает пакеты IPv6, то она должна передавать пакеты IPv6, как это описано в RFC 2460.

Предпочтительным форматом адресации является IPv6. Протокол IP-маршрутизации должен располагать возможностью применения адресации IPv6 и IPv4.

7.1.7 Функция взаимодействия блока PDU сетевого уровня

Функция взаимодействия блока PDU сетевого уровня должна обеспечивать положение, при котором соседние функции DCF, действующие по различным протоколам сетевого уровня, могут взаимодействовать. Для поддержки OSI, допускающей связь с соседней функцией DCF, поддерживающей только OSI, требуется функция DCF, поддерживающая протокол IP.

7.1.8 Функция инкапсуляции блока PDU сетевого уровня

Функция инкапсуляции блока PDU сетевого уровня осуществляет инкапсуляцию и декапсуляцию одного блока PDU в другой блок PDU сетевого уровня.

Пакеты протокола CLNP должны инкапсулироваться по протоколу IP с помощью базовой инкапсуляции маршрутизации (GRE), как это описано в RFC 2784, в качестве полезной нагрузки в пакете протокола IP, используя протокол IP номер 47 (десятичный) и с неустановленным битом *Не фрагментировать* (DF). В соответствии с RFC 2784 инкапсуляция GRE должна иметь в своем составе Ethertype, который указывает, какой именно протокол сетевого уровня переводится в состояние инкапсуляции. При этом необходимо использовать промышленный стандарт OSI Ethertype, а именно 00FE (шестнадцатеричный).

Согласно RFC 2784 пакеты протокола IP должны инкапсулироваться по службе CLNS с применением инкапсуляции GRE в качестве полезной нагрузки блока PDU типа данных протокола CLNP, как это описано в документе ИСО/МЭК 8473-1, используя значение индикатора выбора точки NSAP, равное 47 (десятичный) и установление флага SP (сегментирование разрешено). Более подробную информацию можно найти в RFC 3147.

Пакеты протокола IP должны инкапсулироваться по протоколу IP с применением инкапсуляции GRE, как это описано в RFC 2784, в качестве полезной нагрузки в пакете протокола IP, используя номер протокола IP, равный 47 (десятичный) и с неустановленным битом *Не фрагментировать* (DF).

В качестве версии функция инкапсулирования блока PDU сетевого уровня может передавать блоки PDU через несовместимые узлы, используя для этого процедуру автоматической инкапсуляции, которая рассматривается в Приложении B. Необходимо отметить, что функция DCF, поддерживающая описанную в Приложении B процедуру автоматической инкапсуляции, совместима с ней и может использоваться в той же зоне, что и функция DCF, которая не поддерживает эту процедуру автоматической инкапсуляции.

7.1.9 Функция туннелирования блока PDU сетевого уровня

Функция туннелирования блока PDU сетевого уровня предусматривает статический туннель (соединение со средствами туннелирования) между двумя функциями DCF, поддерживающими один и тот же блок PDU сетевого уровня. Что касается туннелирования, сконфигурированного на размеры максимального передаваемого блока (блок MTU), то любой пакет протокола IP, передача которого по этому туннелю невозможна из-за того, что его размер превышает размер блока MTU, и для которого установлен относящийся к нему бит DF, должен быть отброшен; при этом отправителю такого пакета должно быть отослано сообщение об ошибке недоступности согласно протоколу ICMP (в частности, код "требуется фрагментировать и установить флаг DF").

7.1.10 Функция маршрутизации на сетевом уровне

Функция маршрутизации на сетевом уровне осуществляет рассылку по маршрутам пакетов сетевого уровня.

Согласно документу ИСО/МЭК 10589 функция DCF, поддерживающая маршрутизацию OSI, должна поддерживать также IS-IS.

Функция DCF, поддерживающая IP-маршрутизацию, должна поддерживать интегральные IS-IS (см. параграф 7.1.10.1, где изложены требования, предъявляемые к интегральным IS-IS), и, кроме того, может поддерживать протокол OSPF и прочие протоколы IP-маршрутизации.

7.1.10.1 Требования, предъявляемые к интегральным IS-IS

Функция DCF, поддерживающая интегральные IS-IS, должна соответствовать положениям RFC 1195.

Функция DCF, поддерживающая интегральные IS-IS, должна поддерживать трехстороннее взаимодействие на всех двухпунктовых звеньях данных (см. Приложение A, где изложены требования, предъявляемые к трехстороннему взаимодействию). Трехстороннее взаимодействие модифицирует создание смежности и характера изменения поддержки, что рассматривается в документе ИСО/МЭК 10589.

7.1.10.1.1 Создание смежности при поддержке протокола сетевого уровня

Функция DCF должна включать параметры TLV "поддерживаемых протоколов" во все блоки PDU сообщений IIH и ISH на всех интерфейсах и во все блоки LSP с блоком LSP числа 0, как об этом говорится в RFC 1195.

При поступлении в блок PDU сообщений IS-IS ISH или IIH PDU функция DCF должна произвести проверку этого блока PDU на предмет, содержит ли он параметры TLV "поддерживаемых протоколов". Это должно выполняться на всех интерфейсах, будь то сеть LAN, канал DCC или любые другие соединения. Если в блоке PDU сообщений ISH или IIH параметры TLV "поддерживаемых протоколов" не содержатся, то такой блок должен рассматриваться таким образом, как если бы он содержал параметры TLV "поддерживаемых протоколов", имеющие в своем составе только идентификатор NLPID для протокола CLNP.

Функция DCF должна выполнять сравнение идентификаторов NLPID, перечисленных в параметрах TLV "поддерживаемых протоколов" (при этом допускается, что если отсутствуют все другие протоколы, то присутствует хотя бы только протокол CLNP), с протоколами сетевого уровня, передавать которые может сама эта функция DCF.

Если отсутствует смежность с соседом, который посылает сообщения ISH или IIH, и если функция DCF не в состоянии передавать никакие из протоколов сетевого уровня, перечисленных в параметрах "поддерживаемых протоколов", принятых от соседа сообщений ISH или IIH, то такая функция DCF не должна организовывать состояние смежности с этим соседом.

Если же имеет место смежность с этим соседом, который посылает сообщения ISH или IIH, и если функция DCF не в состоянии осуществить передачу ни одного из протоколов сетевого уровня, перечисленных в параметрах TLV "поддерживаемых протоколов" сообщений ISH или IIH, принятых от соседа, то функция DCF должна исключить эту смежность с соседом и генерировать событие несоответствия поддерживаемых протоколов ProtocolsSupportedMismatch Event.

Если же сама функция DCF в состоянии осуществлять передачу одного или нескольких протоколов сетевого уровня, перечисленных в параметрах TLV "поддерживаемых протоколов" принятых сообщений ISH или IIH, то функция DCF будет обрабатывать эти сообщения ISH или IIH как нормальные.

Функция DCF не должна принимать в расчет значение параметров TLV "поддерживаемых протоколов" блоков LSP в течение всего этого процесса.

Функция DCF, которая не может передавать блоки PDU протокола CLNP, должна игнорировать блоки PDU сообщения ESH и, следовательно, не должна объявлять конечным системам OSI End Systems о возможности достижимости.

7.1.10.1.2 Распределение префиксов протокола IP в масштабах домена IS-IS

Функции DCF, поддерживающие интегральные IS-IS Уровня-1, Уровня-2, должны обеспечивать объявление о сконфигурированных префиксах пункта назначения в IP-протоколе, о которых они узнают из блоков LSP Уровня-2 в Уровень-1, а также о префиксах пункта назначения в IP-протоколе из блоков LSP Уровня-1 в Уровень-2. При режиме работы по умолчанию, когда не сконфигурированы никакие префиксы пункта назначения в IP-протоколе, не следует никакие префиксы Уровня-2 передавать в блоки LSP Уровня-1, поскольку все уже известные префиксы Уровня-1 должны быть переданы в блоки LSP Уровня-2.

7.1.10.1.2.1 Префиксы конфигурирования

Оператор должен предусмотреть две таблицы, которые служат для управления распространением префиксов. Одна таблица должна управлять распространением от Уровня-1 в Уровень-2, а другая – от Уровня-2 в Уровень-1.

7.1.10.1.2.2 Тегирование распространяемых префиксов

Поскольку распространение префиксов от Уровня-2 в Уровень-1 и, следовательно, от Уровня-1 обратно в Уровень-2, может вносить образование замкнутых контуров маршрутизации, то совершенно необходим тег, который позволяет идентифицировать источник этого префикса. Этот тег, называемый реверсивным битом, хранится в ранее неиспользованном старшем бите (бите 8) метрического поля по умолчанию в параметрах TLVдостижимости IP-протокола и в параметрах TLV внешней достижимости IP-протокола. Существующие реализации IS-IS (см. RFC 1195) не будут испытывать воздействия вследствие переопределения этого бита, поскольку RFC 1195 требует установить его на 0 при инициировании блоков LSP, а после приема – игнорировать. Дополнительную информацию можно найти в RFC 2966.

Параметры TLV достижимости IP-протокола и параметры TLV должны обрабатываться таким же способом. Тип принятого параметра TLV будет соответствовать типу, который используется, когда производится передача префикса производителя из зоны Уровня-2 в зону Уровня-1, а также из зоны Уровня-1 в зону Уровня-2.

Это отличается от указаний RFC 1195, которые ограничивают возможность передачи параметров TLV внешней достижимости IP-протоколов только в блоки LSP Уровня-2.

7.1.10.1.2.2.1 Передача блоков LSP с параметрами TLV достижимости IP-протокола и с параметрами TLV внешней достижимости IP-протокола

В соответствии с указаниями RFC 1195 значение реверсивного бита должно быть 0 для всех параметров TLV IP-протокола в блоках LSP Уровня-2. Значение реверсивного бита должно быть 0 для блоков LSP Уровня-1, формируемых в зоне Уровня-1.

Реверсивный бит должен быть установлен на 1 в параметрах TLV IP-протокола в блоке LSP Уровня-2, когда производится передача элементами NE интегральных IS-IS Уровня-1, Уровня-2 сконфигурированного префикса от Уровня-2 в Уровень-1.

7.1.10.1.2.2.2 Прием блоков LSP с параметрами TLV достижимости IP-протокола и с параметрами TLV внешней достижимости IP-протокола

Функция DCF, поддерживающая интегральный IS-IS, должна игнорировать значение реверсивного бита при разработке маршрутов, которые предназначены для применения в зоне Уровня-1 и для Уровня-2.

Функция DCF, поддерживающая интегральный IS-IS Уровня-1, Уровня-2, которая принимает блок LSP с параметрами TLV IP-протокола для префикса, согласующего ввод в таблицу передачи (распространения) от Уровня-1 в Уровень-2, должна объявить/указать надлежащий префикс от Уровня-1 в Уровень-2.

Функция DCF, поддерживающая игтегральный IS-IS Уровня-1, Уровня-2, которая принимает блок LSP с реверсивным битом, установленным на 1, никогда не должна применять префикс для передачи информации от Уровня-1 в Уровень-2.

7.1.10.1.2.2.3 Применение реверсивного бита в блоках LSP Уровня-2

Вопрос, касающийся применения реверсивного бита в блоках LSP Уровня-2, подлежат дальнейшему изучению.

7.1.10.1.2.3 Предпочтение маршрутам

При условии, что теперь префиксы могут передаваться от Уровня-2 в Уровень-1, то для учета этого нового источника необходимо обновить предпочтение маршрутам, которые рассматриваются в RFC 1195. В результате получается следующий порядок предпочтений маршрутам:

1) L1 внутризоновые маршруты с внутренней метрикой;

   L1 внешние маршруты с внутренней метрикой.

2) L2 внутризоновые маршруты с внутренней метрикой;

   L2 внешние маршруты с внутренней метрикой;

   межзоновые маршруты, поступающие от L1 в L2 с внутренней метрикой;

   межзоновые внешние маршруты, поступающие от L1 в L2 с внутренней метрикой.

3) Межзоновые маршруты, поступающие от L2 в L1 с внутренней метрикой;

   внешние маршруты, поступающие от L2 в L1 с внутренней метрикой.

4) L1 внешние маршруты с внешней метрикой.

5) L2 внешние маршруты с внешней метрикой;

   межзоновые внешние маршруты, поступающие от L1 в L2 с внешней метрикой.

6) Межзоновые внешние маршруты, поступающие от L2 в L1 с внешней метрикой.

7.1.11 Функция взаимодействия маршрутизации по IP-протоколу

Функция DCF, поддерживающая функцию взаимодействия маршрутизации по IP-протоколу, должна поддерживать механизмы фильтрации маршрутов в соответствии с указаниями, приведенными в разделах 7.5 и 7.6 RFC 1812, благодаря чему сети с двумя протоколами маршрутизации могут соединяться через несколько – а не только через один – пунктов передачи.

7.1.12 Функция отображения "применения на сетевом уровне"

Соединения при применении OSI, проходящие (частично) по сети DCN, которая поддерживает только IP, могут отображаться в IP-протокол, как это указано в параграфе 2.1.6/Q.811, работающий с профилем протоколов, как это указано в RFC 1006/TCP/IP. Такое отображение представляет собой решение Уровня 4, вследствие чего в рамках настоящей Рекомендации не рассматривается. В качестве другой версии передачи соединений при применении OSI (частично) по сети DCN, которая поддерживает только IP, необходимо предусмотреть инкапсуляцию OSI в IP-протокол Уровня 3, как это рассматривается в параграфе 7.1.8.

Отображение соединений при применении IP-протокола (частично) по сети DCN, которая поддерживает IP, должно соответствовать комплекту спецификаций IP-протокола.

7.1.13 Функция инкапсуляции "блока MPLS PDU в уровень звена данных канала ECC"

Эта функция осуществляет инкапсуляцию и декапсуляцию блока MPLS PDU в кадр канала ECC уровня звена данных.

Если протокол PPP поддерживается в интерфейсе канала ECC канальным протоколом, то необходимо:

– *На конце передачи*
  Ввести пакеты MPLS непосредственно в информационное поле протокола PPP, как это указано в RFC 1661, при протокольном значении MPLS, составляющим 0281 (шестнадцатеричный), в протокольное поле протокол PPP, как это указано в разделе 4.3 RFC 3032, где рассматривается коммутация MPLS по конкретному адресу (MPLS Unicast).
– *На конце приема*
  Пакет MPLS идентифицировать, если протокольное поле протокола PPP имеет протокольное значение коммутации MPLS, составляющее 0281 (шестнадцатеричный), как это указано в разделе 4.3 RFC 3032, где рассматривается коммутация MPLS по конкретному адресу.

7.1.14 Функция инкапсуляции "блока MPLS PDU в кадр Ethernet frame"

Эта функция осуществляет инкапсуляцию и декапсуляцию блока MPLS PDU в кадр Ethernet frame (версия 2).

Она должна инкапсулировать блоки MPLS PDU в кадры Ethernet frame (версия 2), как указано в RFC 894, в значение стандарт Ethertype 8847 (шестнадцатеричный), как указано в разделе 5 RFC 3032, где рассматривается коммутация MPLS по конкретному адресу.

7.1.15 Функция сигнализации блока MPLS LSP

Функция сигнализации блока MPLS LSP обеспечивает сигнализацию, необходимую для создания блока MPLS LSP.

Функция DCF, поддерживающая функцию сигнализации блока MPLS LSP, должна поддерживать следующую модель резервирования: четко определенный путь по строго установленному маршруту через простые узлы (32-битовый IP-адрес) для блока LSP по конкретному адресу точка-точка по стилю резервирования "FF" через протокол IPv4.

Сообщение Путь передается вперед к пункту назначения по пути, указанному перечнем IP-адресов в Объекте четко определенных маршрутов (Explicit Route Object – ERO). В этом ERO зарегистрирован каждый узел (LSR) указанного пути. С помощью объекта запроса метки упомянутые узлы LSR обеспечивают соединение меток в течение данного сеанса. (См. RFC 3209, разделы 2.2, 3.1, 4.2 и 4.3, где рассматривается Протокол резервирования ресурсов – эффективность информационного обмена – RSVP-TE.)

В ответ узел-пункт назначения отсылает сообщение Resv, которое направляет отправителю поток данных в направлении, обратном указанному в перечне узлов в объекте ERO. Метка в объекте метки (Label object) сообщения Resv используется в каждом промежуточном узле LSR с тем, чтобы связать исходящий обмен с его протоколом LSP. Если рассматриваемый узел не является отправителем, то он выделяет новую метку и размещает ее в объекте метки сообщения Resv, в результате чего выполняется передача обмена в направлении, обратном основному трафику, в PHOP. (См. RFC 3209, разделы 2.2, 3.2. и 4.1, где рассматривается протокол RSVP-TE.)

Если же узел не в состоянии выполнить этот запрос, он передает в узел-отправитель сообщение PathErr или ResvErr. (См. RFC 3209, раздел 4.5, где рассматривается протокол RSVP-TE.)

Процедура программно-управляемого состояния протокола RSVP подразумевает периодическую передачу полного представления информационных потоков состояния протокольного блока LSP в

сообщениях Resv и Path с целью поддержания этого блока LSP. Вместо такой периодической передачи стандартных сообщений Path и Resv используется сообщение Srefresh. Каждый идентификатор MessageID в сообщении Srefresh представляет полное сообщение Path или Resv, для которого состояние не меняется. (См. RFC 2961, раздел 5.5 – протокол RSVP-ORE.)

Объект MESSAGE_ID_NACK применяется для индикации того, что полученный идентификатор MessageID не соответствует нужному; вследствие этого требуется полное сообщение Path или Resv, чтобы восстановить протокол LSP. (См. RFC 2961, раздел 5.4 – протокол RSVP-ORE.)

Объект MESSAGE_ID_ACK применяется для подтверждения правильности приема сообщений, содержащих объект MESSAGE_ID, в результате чего устанавливается флаг ACK_Desired. Он является частью алгоритма повторной передачи сообщения Srefresh, как рассматривается в RFC 2961, раздел 6.3 – протокол RSVP-ORE.)

7.1.16 Функция передачи данных блока MPLS LSP

Функция передачи данных блока MPLS LSP отсылает входящий пакет MPLS в исходящий интерфейс, основываясь на метке этой коммутации MPLS и на записи о передаче метки следующего переприема (NHLFE), как указано в RFC 3031.

Последовательность пакетов должна поддерживаться в протоколе LSP.

7.1.17 Функция вычисления пути блока MPLS LSP

Функция вычисления пути блока MPLS LSP выполняет вычисление пути для однонаправленного блока LSP. Эта функция должна обеспечивать возможность вычисления путей и для двух однонаправленных блоков LSP к одному и тому же пункту назначения таким образом, чтобы их пути не пересекались в одном и том же узле или в одной и той же подсети.

7.1.18 Функция инкапсуляции "пакета сетевого уровня в коммутацию MPLS"

Функция инкапсуляции "пакета сетевого уровня в коммутацию MPLS" дополнительно вводит/удаляет запись набора меток в/из пакета сетевого уровня (см. RFC 3032).

7.1.19 Функция применения пакетного режима с защитой 1+1 для коммутации MPLS

7.1.19.1 Связывание двух блоков LSP

Входной и выходной узлы должны обеспечивать идентификацию и связывание двух блоков LSP, обеспечивающих пакетный режим с защитой 1+1. Такое связывание двух блоков LSP может быть выполнено с помощью либо интерфейса, либо сигнализации управления сетью.

Что касается сигнализации, то идентификатор должен передаваться через каждый из рассматриваемых разных блоков LSP. Такой идентификатор должен быть пригоден для каждого из этих разных блоков LSP, а также он должен быть единственным для блоков LSP, инициируемых во входном узле, и для блоков LSP, завершающихся в выходном узле.

Вопрос о конкретном механизме назначения такого идентификатора, а также о том, каким образом этот идентификатор будет транспортироваться в рамках протокола сигнализации, подлежит дальнейшему изучению. Этот механизм будет аналогичен требуемому для связывания блоков LSP для других механизмов защиты на базе коммутации MPLS, например, 1+1 или 1:1.

Для удовлетворения требования в отношении того, чтобы в данном случае не было необходимости в расширении сигнализации на промежуточные узлы, рассматриваемые Идентификатор и Тип услуг блока LSP (т. е. пакетный режим защиты 1+1) должны передаваться в непрозрачных объектах.

7.1.19.2 Формат идентификаторов с порядковыми номерами

Порядковый номер должен использоваться в качестве идентификатора для пакетного режима защиты 1+1. Каждая копия переданного дублированного пакета имеет один и тот же единственный порядковый номер, выделяемый входным узлом. Порядковый номер следующего пакета формируется посредством прибавления единицы к рассматриваемому порядковому номеру.

Выходной узел использует порядковый номер, чтобы удостовериться, что берется только первая принятая копия пакета, а вторая отбрасывается. Выходной узел удаляет порядковый номер из текста пакета сразу же после его отбора и до пропускания в верхний уровень используемого набора (стека). Необходимо отметить, что схема восстановления защиты 1+1 при работе в пакетном режиме не зависит от применений/протоколов, поддерживаемых коммутацией MPLS.

Порядковый номер должен передаваться в каждом пакете в виде первых четырех байтов внутри специального заголовка каждого из пакетов LSP, обеспечивающих пакетный режим защиты 1+1. Первый порядковый номер, который выделяется первому пакету на входном узле, должен быть использован по согласованию между входным и выходным узлами. Значением по умолчанию для этого первого порядкового номера является 0.

Порядковый номер размещается после заголовка инкапсуляции коммутации MPLS, состоящего из 4-х байтов, как показано на рисунке 7-6. Необходимо отметить, что пакетный режим защиты 1+1 может обеспечиваться на любом уровне иерархии вложенного пакета LSP.

Специальный заголовок из 4-х байтов	Порядковый номер из 4-х байтов
Заголовок инкапсуляции	Порядковый номер

Рисунок 7-6/G.7712/Y.1703 – Формат идентификаторов с порядковыми номерами

7.2 Требования, предъявляемые к обеспечению

Каждый элемент NE должен обеспечивать возможность создания интерфейса, который не имеет никакого физического внешнего вида. Такой интерфейс должен быть таким, чтобы его можно было обеспечить IP-адресом.

Необходимо сконфигурировать размер блока LSP.

Это позволит установить в рамках рассматриваемого домена размер MTU.

Для протокола OSPF требуется предусмотреть обеспечение зоны идентификатора ID для каждого интерфейса, включая каналы ECC и сеть LAN.

7.3 Требования, предъявляемые к безопасности

Необходимо предпринять меры для избежания нежелательных взаимодействий (адреса и т. п.) между IP-сетью общего пользования и сетью DCN, поддерживающей IP-протокол.

Приложение A[1]

Требования, предъявляемые к трехстороннему взаимодействию

Процедура трехстороннего взаимодействия основана и спроектирована на возможности совместимости с функцией трехстороннего взаимодействия Рабочей группы по системам IS-IS IETF (RFC 3373).

A.1 Параметры TLV трехсторонней смежности соединения "точка–точка"

Функция DCF, поддерживающая интегральные IS-IS, должна включать параметры TLV во все блоки IIH PDU двухточечных соединений. Структура параметра TLV должна быть такого вида:

Тип = 0xF0 (десятичный 240)
Длина = от 5 до 17 октетов
Значение:
Трехстороннее состояние смежности (один октет):
0 = вверх (Up)
1 = инициализация
2 = вниз (Down)
Расширенный идентификатор ID линии местной сети состоит из четырех октетов
Идентификатор ID соседней системы состоит из нуля до восьми октетов, если это известно
Расширенный идентификатор ID линии местной сети соседней системы состоит из четырех октетов, если это известно

[1] ПРИМЕЧАНИЕ. – Это новое Приложение A заменило Приложение A к Рекомендации МСЭ-T G.7712/Y.1703 в версии 2001 года.

Расширенный идентификатор ID линии местной сети должен выделяться функцией DCF при организации этой линии; функция DCF должна использовать разные значения для каждой двухточечной линии, которой она располагает.

Трехстороннее состояние смежности, о котором сообщается в параметре TLV, должно соответствовать спецификации, приведенной в параграфе A.2.

A.2 Трехстороннее состояние смежности

Функция DCF, поддерживающая интегральные IS-IS, должна иметь трехстороннее состояние смежности для каждой двухточечной линии. Это состояние отличается от состояния, которое рассматривается в документе ИСО/МЭК 10589.

Если на линии не существует никакой смежности, то трехстороннее состояние смежности должно быть установлено в положение "Down".

Если функция DCF принимает сообщение ISH по двухточечной линии, что приводит в результате к созданию новой смежности с состоянием "инициализация", то трехстороннее состояние смежности должно быть установлено в положение "Down".

Если функция DCF принимает сообщение IIH по двухточечной линии, в котором не содержится параметра трехсторонней смежности, то такая функция DCF должна вести себя, как указано в документе ИСО/МЭК 10589; однако она должна включать параметр TLV в блоки PDU сообщения IIH на этой линии, зарегистрировав трехстороннее состояние смежности в положении "Down".

Если функция DCF принимает блок PDU сообщения IIH по двухточечной линии и в нем содержится параметр TLV трехсторонней смежности, то такая функция DCF должна вести себя иначе, чем указано в документе ИСО/МЭК 10589, и обработка блока PDU сообщения IIH осуществляется следующим образом:

– Если представлены поля идентификатора ID соседней системы и расширенного идентификатора ID линии местной сети параметра TLV и если идентификатор ID соседней системы не соответствует идентификатору ID рассматриваемой функции DCF, или расширенный идентификатор ID линии местной сети не соответствует расширенному идентификатору ID рассматриваемой функции DCF, то этот блок PDU сообщения IIH должен быть отброшен и не подвергаться обработке.
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept" (ПРИНЯТ) и если принятое трехстороннее состояние смежности установлено в положение "Down", то рассматриваемая функция DCF изменяет установку своего трехстороннего состояния смежности в положение "Initializing".
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept", и если принятое трехстороннее состояние смежности установлено в положение "Initializing", то рассматриваемая функция DCF должна изменить свое трехстороннее состояние смежности из положения "Down" или "Initializing" в положение "Up" и получить результат "AdjacencyChangeState(Up)".
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept" и если принятое трехстороннее состояние смежности установлено в положение "Initializing", то если рассматриваемая функция DCF уже имеет трехстороннее состояние смежности в положении "Up", она должна поддерживать это трехстороннее состояние смежности в положении "Up".
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept" и если принятое трехстороннее состояние смежности установлено в положение "Up", то если рассматриваемая функция DCF уже имеет трехстороннее состояние смежности в положении "Down", она должна создавать результат "AdjacencyStateChange(Down)" на основании "Повторного включения соседнего узла" (Neighbour restarted) и смежность должна быть исключена без выполнения впоследствии обработки блока PDU сообщения IIH.
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept", и если принятое трехстороннее состояние смежности установлено в положение "Up", то если рассматриваемая функция DCF уже имеет трехстороннее состояние смежности в положении "Initializing", эта функция должна изменить свое трехстороннее состояние смежности на положение "Up" и создать результат "AdjacencyChangeState(Up)".
– Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept", и если принятое трехстороннее состояние смежности установлено в положение "Up", то если

рассматриваемая функция DCF уже имеет трехстороннее состояние смежности в положении "Up", эта функция должна поддерживать трехстороннее состояние смежности в положении "Up".

– После сравнения идентификатора ID источника от блока PDU с местной системой, идентификатор ID и обработка идентификатора ID канала выполняться не должны.

Если блок PDU сообщения IIH соответствует таблицам состояний, указанных в документе ИСО/МЭК 10589 и устанавливающихся в положение "Up" или "Accept", то функция DCF должна:

1) скопировать соседние записи адреса зоны смежности (areaAddressOfNeighbour entries) из поля адресов зоны (Area Addresses field) блока PDU;
2) установить значение таймера блокировки (holdingTimer value) поля времени блокировки от блока PDU; и
3) установить идентификатор соседней системы (neighbourSystemID) на значение идентификатора источника (Source ID) от блока PDU, как указано в документе ИСО/МЭК 10589.

Приложение B

Требования, предъявляемые к автоматической инкапсуляции

B.1 Введение

В настоящем приложении рассматривается спецификация дополнительной функции AE-DCF, которая позволяет узлам, поддерживающим маршрутизацию в соответствии с различными несовместимыми протоколами сетевого уровня, например протоколами CLNS, IPv4 или IPv6, которые должны присутствовать в единственной зоне IS-IS Уровня-1 или субдомене Уровня-2; автоматически производится инкапсуляция одного протокола сетевого уровня в другой по мере необходимости и при том условии, что все узлы поддерживают IS-IS или маршрутизацию интегральных IS-IS.

B.2 Область применения

Функция AE-DCF представляет собой факультативную функцию. Если она предусматривается, то она является такой функцией, которая рассматривается в настоящем приложении. Требования настоящего приложения применимы только к функциям, которые содержат дополнительные функциональные возможности функции AE-DCF. Эта функция AE-DCF требует от функций DCF определенных характеристик, которые не включены в состав функциональных возможностей AE-DCF, чтобы получить возможность взаимодействовать с ними. Требования, предъявляемые к функциям DCF и не включенные в функциональные возможности AE-DCF, можно найти в параграфе 7.1.10.1 для IP-узлов и сдвоенных узлов, а также в документе ИСО/МЭК 10589 для OSI-узлов.

B.3 Описание функции AE-DCF

B.3.1 Введение

Интегральная IS-IS, как указано в RFC 1195, первоначально была разработана для получения возможности маршрутирования IP и CLNS с помощью единого протокола маршрутизации и единого алгоритма SPF. С этой целью она представляет адрес IPv4 и маски подсети в качестве 64-битового числа, которое затем обрабатывается SPF-алгоритмом, как если бы это был адрес конечной системы OSI. Узлы интегральной IS-IS нужны для того, чтобы иметь адрес зоны IS-IS и идентификатор системы, который обрабатывается таким же образом, поскольку адрес NSAP относится только к узлу OSI. Затем узлы интегральной IS-IS образуют смежности и идентификаторы систем лавинной маршрутизации, а также метрические системы через свою зону Уровня-1 (маршрутизаторы Уровня-1) или свой субдомен Уровня-2 (маршрутизаторы Уровня-2) таким же образом, как узлы IS-IS только OSI.

Идентификаторы Систем (SID) и метрические системы других идентификаторов SID направляются лавиной через зону Уровня-1 или субдомен Уровня-2 с использованием блоков LSP (блоков PDU состояния линии), которые являются общими как для узлов IS-IS, так и для узлов интегральной IS-IS. В этом случае к рассматриваемым блокам LSP добавляется конкретная IP-информация, для чего используются расширенные параметры TLV, которые понимаются только способными на это IP-узлами. Маршрутизаторы только для OSI не могут выполнить расшифровку таких параметров TLV, но все еще производят их лавинную передачу во все свои пункты смежности. В подобном случае можно построить дерево SPF, для чего используется любой узел IS-IS или интегральной IS-IS, либо передача может маршрутизироваться по CLNS, IPv4 или IPv6. Узлы, пригодные для OSI, будут вычислять кратчайшие пути к конечным системам OSI, узлы, пригодные для IPv4, будут вычислять кратчайшие пути к адресам или префикесам IPv4, а узлы, пригодные для IPv6, будут вычислять кратчайшие пути к адресам или префиксам IPv6.

Одним из следствий такого положения дел является тот факт, что узел, работающий только с OSI, будет вычислять кратчайший путь к конечной системе OSI, который проходит через узел, работающий только с IP, несмотря на то, что такой узел только-IP не может передавать пакеты сетевой службы CLNS. Аналогично этому, узел только-IP будет вычислять кратчайший путь к IP-пункту назначения; такой путь проходит через узел только-OSI, даже если такой узел только-OSI не может передавать IP-пакеты. Таким образом, узел, способный работать только с OSI, не следует размещать в той части сети, где существует возможность, при которой такой узел окажется на кратчайшем пути к IP-пункту назначения, а узел, способный работать только с IP, не следует размещать в той части сети, где существует возможность, при которой такой узел окажется на кратчайшем пути к конечной системе OSI.

Алгоритм интегральной IS-IS может использовать только единственный алгоритм SPF для двух или более протоколов сетевого уровня благодаря допущению о том, что все протоколы сетевого уровня располагают доступом к одним и тем же ресурсам, другими словами, к подобной сети с подобной топологией. Таким образом, интегральная IS-IS требует, чтобы любой узел в зоне Уровня-1 или в субдомене Уровня-2 имел возможность осуществлять маршрутизацию любого протокола сетевого уровня, который представлен в рассматриваемых зоне или домене, соответственно.

Исходя из этих соображений, RFC 1195 устанавливает топологические ограничения для сетей, маршруты в которых определяются интегральной IS-IS, требуя при этом, чтобы все узлы поддерживали как IP, так и CLNS в зоне, где в них имеют место как CLNS-трафик, так и IP-трафик.

Следовательно, согласно RFC 1195, если один узел модифицируется и передает IP-пакеты, то и все другие узлы в зоне Уровня-1 или в субдомене Уровня-2 также должны быть модифицированы.

Предполагаемое здесь решение позволяет снять это топологическое ограничение, вследствие чего производится автоматическая инкапсуляция CLNS-пакетов в IP-пакеты для передачи данных, которая осуществляется через узлы, работающие только с IP, и автоматическая инкапсуляция IP-пакетов в CLNS-пакеты для передачи данных, которая осуществляется через узлы, работающие только с OSI. Предполагаемое решение полностью совместимо с существующими узлами только-OSI, для которых не требуется никакой модификации. Помимо требований, изложенных выше в RFC 1195, обсуждаемое решение требует для узлов, работающих только с IPv4 или IPv6, специальной функции создания смежности при поддержке протоколов сетевого уровня, рассматриваемой в параграфе 7.1.10.1.1.

B.3.2 Основная концепция

Эта концепция позволяет извлечь выгоду из того факта, что все узлы интегральной IS-IS и IS-IS совместно используют основную топологическую информацию совершенно одинаково, а также из той особенности поведения, что узлы, работающие только с OSI, будут делать попытки передачи пакета через узел, работающий только с IP, и наоборот, даже в том случае, если этот узел не располагает фактической возможностью передать данный пакет. Как правило, это заканчивается потерей пакета, однако функция AE-DCF производит инкапсуляцию пакетов до того, как они передаются через несовместимые узлы, так чтобы они не потерялись.

Когда два изолированных участка узлов с интегральной IS-IS, способных к работе с IP, соединяются между собой с помощью централизованной сети, которая поддерживает только OSI, и если эти узлы работают в одной и той же зоне (в случае узлов Уровня-1), то узлы, поддерживающие только IP, будут принимать блоки LSP от всех других узлов, поддерживающих только IP, даже от узлов, находящихся в другом изолированном участке, а также блоки LSP от всех узлов, работающих только с OSI в центре. Таким образом, они выполняют вычисления кратчайших путей через узлы только-OSI для всех IP-пунктов назначения на изолированном участке дальней стороны. Вычисление оказывается неверным только в том случае, когда узлы, способные работать только с IP, фактически осуществляют передачу IP-пакета в узел, работающий только с OSI, в результате чего происходит потеря пакета. Этим-то и обусловлены топологические ограничения, устанавливаемые в RFC 1195.

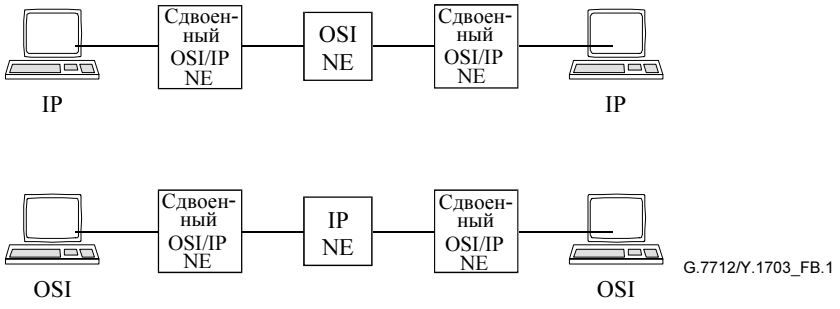


Рисунок B.1/G.7712/Y.1703 – Запрещенные топологии

В вышерассмотренном примере сети, представленные на рисунке B.1, согласно RFC 1195, имеют запрещенные топологии. В верхней сети IP-пакеты будут направляться с одной стороны сети на другую, но при поступлении в узел только-OSI они будут отбрасываться. Аналогично этому, в нижней сети CLNS-пакеты будут направляться с одной стороны сети на другую, но при поступлении в узел только-IP они будут отбрасываться. Функция AE-DCF, технические характеристики которой рассматриваются в данном параграфе, исправляет такое поведение.

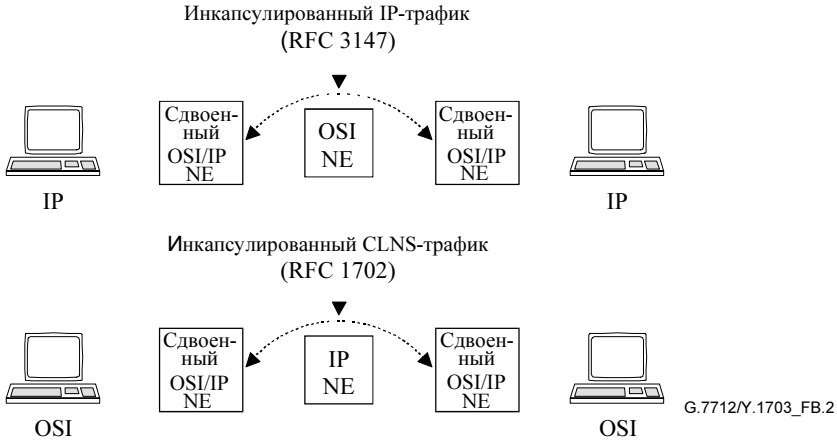


Рисунок B.2/G.7712/Y.1703 – "Устранение недостатков" посредством инкапсуляции

Функция AE-DCF размещается в сдвоенных узлах и дает им возможность распознавать, какой из конкретных соседних узлов будет отбрасывать определенный трафик, чтобы, таким образом, прибегнуть к инкапсуляции его в такую форму, в которой он отбрасываться не будет (см. рисунок B.2). Благодаря этому "устраняются недостатки" сети, так что часть сети между сдвоенными узлами работает таким образом, как если бы она состояла только из сдвоенных узлов, в то время как на деле один или более таких узлов не являются сдвоенными.

Функция AE-DCF не изменяет пути, по которому пакет должен пересечь всю сеть; любой отдельно взятый пакет все же пересечет эту сеть, используя кратчайший путь, который был вычислен по алгоритму нормального пути IS-IS SPF.

Специальная функция создания смежности при поддержке протоколов сетевого уровня, рассматриваемая в параграфе 7.1.10.1.1, заставляет трафик проходить через узлы, которые поддерживают и IP и OSI, всякий раз, когда по кратчайшему пути передается трафик через границу между частями зоны, которые способны к передаче IP-сообщений и к работе в режиме OSI. Таким образом, функция AE-DCF предоставляет этим сдвоенным узлам возможность выполнять инкапсуляцию пакета, если это окажется необходимым, так что он может быть передан через узлы, которые не поддерживают рассматриваемый протокол сетевого уровня. Подобная инкапсуляция имеет место только в случае необходимости и, следовательно, эти туннели создаются автоматически и носят динамический характер. Полученные в результате туннели никогда не поддерживаются ни в каком из направлений, а существуют только как входные данные в таблицах передачи. Когда речь идет о протоколе маршрутизации, эти туннели не появляются ни как каналы, ни как интерфейсы. Таким образом, пакеты все еще пересекают сеть по кратчайшему пути, который каждый узел вычисляет обычным способом; поэтому нет необходимости выполнять инкапсуляцию IS-IS-пакетов, а инкапсуляции подлежат только IP-трафик и CLNS-трафик.

B.4 Требования и ограничения

B.4.1 Требования, предъявляемые к узлам только-OSI

Для взаимодействия с функцией AE-DCF узлы только-OSI должны соответствовать документу ИСО/МЭК 10589.

B.4.2 Требования, предъявляемые к узлам только-IP

Для взаимодействия с функцией AE-DCF узлы только-IP должны соответствовать RFC 1195.

В частности, от узлов, способных работать с IP, требуется игнорировать параметр TLV "поддерживаемых протоколов" в блоках LSP тех узлов, которые рассматриваются как кандидаты на кратчайшие пути при выполнении алгоритма SPF.

Узел, способный работать с IP, который включает только узлы, способные работать с IP при вычислении его SPF, не будет соответствовать RFC 1195, где указано:

– на стр. 26 RFC 1195: "Вычисление Dijkstra не учитывает, является ли маршрутизатор только-IP, только-OSI или сдвоенным по своему характеру. Топологические ограничения, которые определены в разделе 1.4, гарантируют, что IP-пакеты будут переданы только через маршрутизаторы, способные действовать только через IP, а OSI-пакеты, будут переданы только через маршрутизаторы, способные действовать только через OSI".

Функция AE-DCF совместима с реализациями, изложенными в RFC 1195, которые соответствуют вышеприведенному утверждению. Реализация, которая только включает узлы, способные работать с IP, в вычисление блока SPF, не будет включать пути, проходящие только через узлы только-OSI, в качестве подходящего маршрута и не будет использовать преимущество этой функции AE-DCF.

Для взаимодействия с функцией AE-DCF IP-узлы должны соответствовать параграфу 7.1.10.1.1. Причиной этого являются следующие моменты:

– Это решение зависит от IP-пакетов, поступающих в узел только-OSI с первым прохождением через функцию AE-DCF, и от CLNS-пакетов, поступающих в узел только-IP с первым прохождением через функцию AE-DCF. После этого функция AE-DCF несет ответственность за инкапсуляцию этих пакетов таким образом, чтобы их можно было передавать.

– Следовательно, узел только-IP никогда не должен иметь смежности с узлом только-OSI.

– Если это решение используется для смешанного использования узлов IPv4 и IPv6 в одной и той же зоне Уровня-1 или в одном и том же субдомене Уровня-2, то по аналогии с этим узел только-IPv4 никогда не должен иметь смежности с узлом только-IPv6.

– Это требование удовлетворяется, если все узлы, способные работать с IP, соответствуют параграфу 7.1.10.1.1. Необходимо отметить, что это требование в RFC 1195 отсутствует.

В качестве альтернативы оператор может вручную обеспечить положение, при котором узлы, не поддерживающие в общем случае протокол сетевого уровня, не должны иметь смежностей.

B.4.3 Требования, предъявляемые к сдвоенным или использующим многие языки узлам с автоматической инкапсуляцией

Если это свойство должно применяться в зоне Уровня-1 или в субдомене Уровня-2, то узлы, которые поддерживают несколько протоколов сетевого уровня, но не поддерживают функцию AE-DCF, могут использоваться с предосторожностью. Более безопасная альтернатива заключается либо в соблюдении топологических ограничений, приведенных в RFC 1195, либо в использовании только сдвоенных или использующих многие языки узлов, которые поддерживают функцию AE-DCF.

B.4.3.1 Параметр возможности инкапсуляции TLV

Функция AE-DCF будет включать новый параметр TLV в блоках LSP с номером блока LSP, равным нулю. Новый параметр TLV имеет следующую структуру:

Код: 16 (десятичный)
Длина: Размерность значения
Значение: Переменная часть размерности, содержащей:
Тип подпараметра TLV: 1
Длина подпараметра TLV: Втрое превышает число режимов инкапсуляции в подпараметре TLV
Значение подпараметра TLV:
47, указывающее, что следующие два байта являются инкапсуляцией GRE;
идентификатор NLPID пакета, который может быть инкапсулирован (внутренний);
идентификатор NLPID пакета, который переносит инкапсулированный пакет (внешний);
байты 4,5,6: Режим второй инкапсуляции (в случае необходимости);
байты 7,8,9: Режим третьей инкапсуляции (в случае необходимости);
и т. д.

Применяемые идентификаторы NLPID должны соответствовать определенным в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577. Узлы, передающие этот параметр TLV, должны указывать форматы, которые узел может принимать, и передавать. Узлы должны располагать возможностью как автоматически инкапсулировать, так и автоматически декапсулировать те форматы, которые характеризуются этим параметром TLV, так что трафик может приниматься и возвращаться в обратном направлении.

Рекомендуется, чтобы сдвоенные узлы, поддерживающие функцию AE-DCF, располагали возможностью инкапсулировать/декапсулировать A в B и B в A (где A и B – это два поддерживаемых протокола сетевого уровня), создавая в типовом сдвоенном узле два режима инкапсуляции.

Например, содержимое рассматриваемого параметра TLV для типовой функции AE-DCF при OSI и IPv4 будет следующим:

16: код;
8: размерность значения (в данном примере);
1: подпараметр TLV типа 1;
6: длина подпараметра TLV (в данном примере);
47: следующие два байта составляют поддерживаемый режим инкапсуляции GRE;
129: интерфейс IPI для протокола CLNP, рассматриваемый в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577;
204: интерфейс IPI для IPv4, рассматриваемый в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577;
47: следующие два байта составляют поддерживаемый режим инкапсуляции GRE;
204: интерфейс IPI для IPv4, рассматриваемый в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577;
129: интерфейс IPI для протокола CLNP, рассматриваемый в Рекомендации МСЭ-Т X.263 | ИСО/МЭК 9577.

Функция AE-DCF при OSI, IPv4, IPv6 будет, таким образом, как правило, использовать шесть режимов инкапсуляции для индикации протокола CLNP в IPv4, CLNP в IPv6, IPv4 в CLNS, IPv4 в IPv6, IPv6 в CLNS и IPv6 в IPv4, давая значение длины порядка 20.

Подобный параметр TLV не будет включаться в протоколах LSP псевдо-узлов.

Функция AE-DCF, которая не располагает никакими адресами IPv4, не должна размещать никаких форматов инкапсуляции в своем параметре TLV типа, равного 16, который включает IPv4 как индикатор NLPID передачи инкапсуляции (внешней) до тех пор, пока не будет обеспечен и объявлен адрес IPv4.

Функция AE-DCF, которая не располагает никакими адресами IPv6, не должна размещать никаких форматов инкапсуляции в своем параметре TLV типа, равного 16, который включает IPv6 как индикатор NLPID передачи инкапсуляций (внешний) до тех пор, пока не будет обеспечен и объявлен адрес IPv6.

B.4.3.2 Процесс передачи (продвижения) данных

Поскольку функция AE-DCF не модифицирует путь, по которому следует пакет, такая функция AE-DCF может вычислить кратчайший путь для IP-пакета, который приводит к подключению к следующему узлу, представляющему собой узел только-OSI.

Когда это случается, функция AE-DCF должна не просто передавать пакет в соседний (смежный) узел, который не поддерживает протокол сетевого уровня такого типа. Вместо этого функция AE-DCF должна инкапсулировать этот пакет внутри нового пакета такого типа, который поддерживает следующий узел. Критерием того, поддерживает или не поддерживает смежный узел конкретный протокол сетевого уровня, является тот факт, указан ли этот протокол сетевого уровня в перечне "поддерживаемых протоколов" параметра TLV в блоках PDU сообщения IS-IS Hello, поступивших из этого узла по смежности, который является следующим узлом для указанного пункта назначения.

Для этого нового пакета требуется протокол сетевого уровня, адрес пункта назначения и адрес источника, чтобы выполнить инкапсуляцию исходного пакета:

– Протокол сетевого уровня этого нового пакета должен быть таким, который поддерживается следующим узлом, как это определено "поддерживаемыми протоколами" параметра TLV блоков сообщения Hello, принятых от следующего узла.

– Адрес пункта назначения этого нового пакета должен быть равен идентификатору следующего узла, который передается по кратчайшему пути первоначально указанного

пункта назначения и который был представлен в режиме инкапсуляции, имеющем как тип протокола сетевого уровня, где исходящий пакет представляет собой инкапсулированный (внутренний) идентификатор NLPID, а также как протокол сетевого уровня, который поддерживается следующим узлом (как это определяется параметрами TLV "поддерживаемых протоколов" блоков PDU сообщения Hello, поступивших из следующего узла) в качестве идентификатора NLPID транспортировки (внешней) инкапсуляции.

– Это должно достигаться посредством контроля рассматриваемого нового параметра TLV типа, равного 16 из блоков LSP, принятых от каждого узла в данном пути к нужному пункту назначения до тех пор, пока не обнаружится первый, который удовлетворяет вышеизложенному требованию.
– Когда контролируемые параметры TLV типа равны 16, функция AE-DCF должна игнорировать любой из подпараметров TLV, который она не понимает, и перейти к следующему подпараметру TLV; после этого она должна контролировать его либо до тех пор, пока она не найдет все режимы инкапсуляции, подходящие для него, либо пока она не достигнет конца этого параметра TLV.
– Адрес источника нового пакета должен быть равен идентификатору функции AE-DCF, которая создает новый пакет инкапсуляции.

Если функция AE-DCF может осуществлять передачу пакета, не прибегая к инкапсуляции, поскольку следующий узел поддерживает рассматриваемый тип пакета, то эта функция AE-DCF должна выполнить передачу данного пакета без его инкапсуляции.

Функция AE-DCF может передавать пакеты LSP, в которых содержится IP-достижимость от узла только-IP до узла с секционированным стеком, или наоборот; следовательно, в этом случае может потребоваться инкапсуляция пакетов, заглавных для узла с секционированным стеком, или декапсуляция пакетов, принятых от узла с секционированным стеком.

Таким образом, узел с секционированным стеком, инкапсулированный автоматически, должен, кроме этого, соблюдать тот же процесс контролирования пакетов LSP узлов между собой и пунктом назначения, отыскивая тот узел, который имеет подходящий формат инкапсуляции.

Необходимо отметить, что узел с секционированным стеком может располагать возможностью приема пакета IPv4 только инкапсулированного, например, внутри сетевой службы CLNS. В этом случае узел с секционированным стеком будет осуществлять передачу только "CLNS" в поле с "поддерживаемыми протоколами" своих пакетов Hello и включать только один режим инкапсуляции в своем параметре TLV типа, равного 16 в своих пакетах LSP. Этот единственный режим инкапсуляции будет определять IPv4 как инкапсулированный (внутренний) пакет NLPID и CLNS в качестве пакета NLPID транспортировки инкапсуляции (внешней).

B.4.3.3 Процесс приема

Когда функция AE-DCF принимает пакет, который предназначен непосредственно для нее, этот пакет необходимо проконтролировать с тем, чтобы установить, не содержится ли внутри него другой инкапсулированный пакет. При этом обнаруженный некапсулированный пакет CLNS, IPv4 или IPv6 должен передаваться как нормальный. Если же полученный в результате некапсулированный пакет содержит другой пакет, предназначенный для этого узла, то рассмотренный процесс повторяется; это обусловлено тем фактом, что при единственной функции AE-DCF может потребоваться декапсуляция нескольких уровней инкапсуляции.

Пакеты IS-IS не сравнимы с IP-пакетами и не могут передаваться по сетям Интернет общего пользования или по другим только-IP сетям. Это является большим достоинством безопасности, поскольку затрудняет злонамеренный элемент дистанционного запуска пакетов IS-IS в узлах IS-IS или интегральных IS-IS узлах по сети Интернет общего пользования. Для того чтобы не лишиться этого преимущества, при обнаружении поступления IS-IS или ES-IS пакета, инкапсулированного внутри другого пакета, предназначенного для функции AE-DCF, эта функция AE-DCF должна не принимать его в расчет, если только он не поступил от узла, с которым данная функция AE-DCF имеет вручную выполненный туннель с IS-IS, предназначенный для прохождения по нему. В другом же случае может быть составлено сообщение об ошибке, информирующее администратора сети о том, что пакет был принят и пропал после поступления, либо о том, что это является фактом потенциального злонамеренного акта.

Все пакеты должны быть инкапсулированы с помощью применения инкапсуляции GRE, как это рассматривается в параграфе 7.1.8.

B.4.3.4 Требования, предъявляемые к размеру блока MTU и его фрагментации

Инкапсуляция одного пакета внутри другого может привести к новому пакету, который имеет большую длину, чем размер блока MTU в линии, по которой этот новый пакет должен быть передан. Следовательно, этот новый пакет GRE отвергаться не должен; подобные пакеты не должны включать

бит "не фрагментировать" (Don't Fragment), обычно используемый, если эти пакеты являются пакетами IPv4, но должны включать флаг Сегментация разрешена (Segmentation Permitted flag), если эти пакеты являются пакетами CLNS, как описано в параграфе 7.1.8.

После этого полученные в результате пакеты инкапсуляции должны подвергнуться фрагментированию, прежде чем они будут передаваться, если длина такого пакета превысит предельное значение пакета MTU рассматриваемой линии.

Нет необходимости выполнять фрагментирование пакета до его инкапсулирования, поскольку в случае потребности фрагментированию будет подвергнут пакет, получаемый в результате.

B.4.3.5 Требования, предъявляемые к функции AE-DCF с широковещательными (LAN) интерфейсами

B.4.3.5.1 Процесс выбора псевдоузла

В соответствии с положениями параграфа 7.1.10.1.1 узлам только-IP не разрешается создавать смежность с узлами только-OSI, а узлам только-IPv4 не разрешается создавать смежность с узлами только-IPv6.

Поэтому когда узлы только-IP и узлы только-OSI подключаются к одной и той же сети LAN и в той же зоне Уровня-1 или субдомена Уровня-2, то узлы только-IP будут создавать смежности с любым другим узлом и выбирать псевдоузел, а узлы только-OSI будут создавать другие смежности и выбирать другой псевдоузел. Таким образом, будут иметь место два разных псевдоузла на одной сети LAN – один для узлов только-OSI и один для узлов только-IP.

Аналогичная ситуация может сложиться и в том случае, если узлы только для IPv4 и только для IPv6 окажутся подключенными к одной и той же сети LAN.

Поэтому функция AE-DCF должна принимать участие в процессах выбора этих разных псевдоузлов независимо от каждого поддерживаемого ею сетевого уровня. Функция AE-DCF Уровня-1/Уровня-2 должна участвовать в двух процессах выбора псевдоузла для каждого протокола сетевого уровня, который она поддерживает (один для Уровня-1 и один для Уровня-2).

Каждый псевдоузел в сети LAN, размещенный на узле протокола сетевого уровня и совместимый с функцией AE-DCF, будет располагать смежностью с этой функцией AE-DCF. Таким образом, на сети IP и OSI LAN эта функция AE-DCF по всем правилам будет той одной функцией, которая располагает обоснованными смежностями как с IP-псевдоузлом, так и с OSI-псевдоузлом (если в сети LAN имеется несколько псевдоузлов). Функция AE-DCF будет располагать смежностью с IP-псевдоузлом и с OSI-псевдоузлом, однако IP-псевдоузел не будет иметь непосредственной смежности с OSI-псевдоузлом, и наоборот, но вместо этого будет увеличивать возможности взаимодействия только через функцию AE-DCF, благодаря чему будет гарантироваться положение, при котором CLNS-пакеты инкапсулируются функцией AE-DCF перед тем, как они будут передаваться в узлы только-IP, а IP-пакеты будут инкапсулироваться функцией AE-DCF перед тем, как они будут передаваться в узлы только-OSI.

Функция AE-DCF, способная работать с IP и OSI, может быть выбрана в качестве назначенного маршрутизатора (Designated Router) узлами, способными работать с IP в сети LAN, но не узлами, способными работать с OSI; в этом случае функция AE-DCF должна создать псевдоузел, а этот псевдоузел должен назначить смежности в своих блоках LSP только при наличии узлов, способных работать с IP в сети LAN.

По аналогии с этим, функция AE-DCF, способная работать с IP и OSI, может быть выбрана в качестве маршрутизатора Designated Router, узлами, способными работать с OSI в сети LAN, но не узлами, способными работать с IP, в этом случае функция AE-DCF должна создать псевдоузел, а этот псевдоузел должен назначить смежности в своих блоках LSP только при наличии узлов, способных работать с OSI в сети LAN.

Функция AE-DCF, способная работать с IP и OSI, может быть выбрана в качестве маршрутизатора Designated Router, как узлами, способными работать с IP, так и с узлами, способными работать с OSI в сети LAN; в этом случае функция AE-DCF должна создать псевдоузел, который назначает смежность в своих блоках LSP для всех узлов в сети LAN.
По существу, функция AE-DCF принимает участие в отдельном процессе выбора для каждого протокола сетевого уровня, который она поддерживает; если же она выиграет любой из выборов, то она создает псевдоузел, а этот псевдоузел должен назначить смежности в своих блоках LSP только с набором или наборами узлов, которые его выбрали.

Следовательно, узлы только с OSI или только с IP могут получать пакеты LSP от псевдоузла, который описывает смежности для узлов в сети LAN, которые не имеют смежностей. Если необходимо, чтобы пакет направлялся через подобный узел, то необходимо его передать в обозначенный IS (Designated IS), как это указано в пункте "h" раздела C.2.5 в документе

ИСО/МЭК 10589 и в RFC 1195, раздел C.1.4, этап 0, пункт 8 на стр. 73. Необходимо отметить, что эти пункты в документах ИСО/МЭК 10589 и RFC 1195 не являются нормативными. Вполне возможно, что существуют реализации, которые не проявляют такого поведения. Такая реализация будет скорее сбрасывать пакеты, чем передавать трафик в функцию AE-DCF для автоматической инкапсуляции, если эта функция AE-DCF представляет собой маршрутизатор Designated Router и если на одном кратчайшем пути оказываются несовместимые друг с другом станции в одной и той же сети LAN.

Следовательно, разработчики и операторы имеют возможность сделать выбор, а именно:

1) Установить первоочередность функции AE-DCF на наибольшее значение. Это приводит к появлению в сети LAN единственного псевдоузла, поддерживаемого функцией AE-DCF. Недостаток этого метода заключается в том, что невелик шанс того, что в сети LAN существует традиционная реализация, при которой трафик не будет передаваться в функцию AE-DCF, если на кратчайшем пути в сети LAN будет существовать несовместимый узел;

или

2) установить первоочередность функции AE-DCF на наименьшее значение. Это приводит к появлению в сети LAN одного псевдоузла для каждого поддерживаемого протокола сетевого уровня, совершенно точно выполняющего передачу трафика в несовместимые узлы через функцию AE-DCF. Это улучшает функциональную совместимость, но удваивая при этом величину пакетов LSP, передаваемых в сеть LAN, что вполне может привести к снижению возможности расширения.

Рекомендуется, чтобы приоритетность функции AE-DCF могла конфигурироваться оператором.

B.4.3.5.2 Процесс обновления пакетов LSP

В разделе 7.3.15.1 документа ИСО/МЭК 10589 констатируется, что принятый пакет LSP, который поступил не из надлежащей смежности, должен быть отброшен. Поэтому точная реализация только-OSI будет отбрасывать пакеты LSP, которые поступают в интерфейс сети LAN от узла только-IP, поскольку узел только-IP отказался от смежности, рассматриваемой в параграфе 7.1.10.1.1. Следовательно, этот узел только-OSI может принять подобный пакет LSP только от функции AE-DCF. Если не выполнить необходимую модификацию, то сдвоенный узел будет передавать такой пакет LSP только в течение периодически выполняемой синхронизации базы данных пакетов LSP.

Следовательно, требуется функция AE-DCF, которая бы изменила характер лавинной маршрутизации пакетов LSP таким образом, чтобы узлам только-OSI или только-IP не было необходимости ожидать следующего процесса синхронизации базы данных пакетов LSP.

Функция AE-DCF должна выполнять проверку входящих пакетов LSP, которые поступают на интерфейсы сети LAN, чтобы установить, поступили ли они с соседнего узла, поддерживающего все протоколы сетевого уровня, которыми располагает эта функция AE-DCF. Это должно достигаться посредством контроля параметра TLV "поддерживаемых протоколов" в пакете Hello, поступившем от соседнего узла.

Если данный пакет LSP получен от соседнего узла, который поддерживает все протоколы сетевого уровня, поддерживаемые функцией AE-DCF, то эта функция должна вести себя, как рассматривается в документе ИСО/МЭК 10589, и удалить флаг SRM для данного пакета LSP на этом интерфейсе сети LAN, если там уже имеется этот пакет LSP, либо передать его из всех других интерфейсов, если такого пакета LSP в нем уже не имеется.

Если данный пакет LSP получен от соседнего узла, который поддерживает не все протоколы сетевого уровня, поддерживаемые функцией AE-DCF, и если в этом узле уже не имеется данного пакета LSP, то функция AE-DCF должна установить флаг SRM для этого пакета на этом интерфейсе сети LAN, через который этот пакет был принят, в дополнение ко всем другим интерфейсам; это приводит к ситуации, когда функция AE-DCF осуществляет повторную передачу этого пакета LSP в сети LAN.

Следовательно, если пакет LSP передается по сети LAN узлом только-IP, то функция AE-DCF производит повторную передачу этого пакета LSP, что позволит принять его – исходя из обоснованной смежности – узлами только-OSI в данной сети LAN, и наоборот.

B.4.3.5.3 Переадресации

Если функция AE-DCF организует запрос переадресации протокола ICMP, то в этом случае не должна иметь место переадресация пакетов IPv4 из узла, способного работать в режиме IPv4, в узел, не способный работать в этом режиме. Аналогично этому, если функция AE-DCF организует переадресацию блоков PDU – в соответствии с документом ИСО/МЭК 9542, – то такая переадресация не должна касаться переадресации пакетов CLNS из узла, способного работать в режиме OSI, в узел, не способный работать в этом режиме.

B.4.3.5.4 Одновременное использование в сети LAN сдвоенных узлов, соответствующих только RFC 1195, и узлов с автоматической инкапсуляцией

Сдвоенный узел, совместимый с RFC 1195, но не поддерживающий функцию AE-DCF, не должен располагаться в сети LAN в той же зоне Уровня-1 или субдомене Уровня-2, что и узлы только-IP и только-OSI, поскольку он может передавать IP-трафик в узел только-OSI, либо трафик CLNS в узел только-IP, что приводит к потере пакетов. Этот факт является топологическим ограничением, свойственным RFC 1195.

Сдвоенный узел, совместимый с RFC 1195, но не поддерживающий функцию AE-DCF, может располагаться в сети LAN в той же зоне Уровня-1 или субдомене Уровня-2, что и функция AE-DCF.

Помимо этого, такой узел может располагаться в сети LAN с узлом только-OSI, если он в состоянии осуществлять передачу только трафика CLNS в этот узел, с узлом только-IPv4, если он в состоянии осуществлять передачу только IPv4 трафика в этот узел, либо с узлом только-IPv6, если он в состоянии осуществлять передачу только IPv6 трафика в этот узел.

B.4.4 Требования, предъявляемые к узлам с секционированным стеком и автоматической инкапсуляцией

Узел с секционированным стеком начинает и завершает передачу пакетов протокола сетевого уровня такого типа, который не может передаваться непосредственно в каналах DCC этого узла. Поэтому единственным способом, который подобный узел имеет возможность использовать для начала или завершения передачи таких пакетов, является их передача в инкапсулированной форме.

Это решение особенно полезно для дополнительного введения IP-карты в преимущественно OSI-узел, либо в узел, который, например, был организован в действующей OSI-сети. Кроме того, может быть легче выполнить модификацию элемента NE OSI-интерфейса в узле с секционированным стеком, чем в сдвоенном узле функции AE-DCF, таким образом, чтобы IP-трафик мог поступать в сеть и покидать сеть, для которой рассматриваемый узел является шлюзом.

Узел с секционированным стеком должен располагать возможностью внутренне выбирать маршрут для любых пакетов, которые он принимает и которые соответствуют протоколу сетевого уровня, одному из перечисленных в параметрах TLV "поддерживаемых протоколов" пакетов IS-IS LSP.

Узел с секционированным стеком должен использовать параметр TLV "поддерживаемых протоколов" в блоках IS-IS Hello PDU для индикации только тех протоколов сетевого уровня, которые он может принять и передать непосредственно на любом своем индивидуальном интерфейсе (либо не поддерживать этот параметр TLV, если он представляет собой интерфейс только-OSI).

Таким образом, узел IP-через-OSI может направлять услугу CLNS непосредственно по своим каналам DCC, а также направлять IP-трафик, поступающий в него в виде инкапсулированных пакетов элемента IP-через-OSI GRE или, что вполне возможно, в Ethernet-интерфейс.

Следовательно, узел с секционированным стеком может указывать один протокол сетевого уровня в параметре TLV "поддерживаемых протоколов" пакетов Hello на одном интерфейсе и совсем другой протокол сетевого уровня в параметре TLV "поддерживаемых протоколов" пакетов Hello на другом интерфейсе. Подобный узел вполне способен направлять эти оба протокола сетевого уровня в качестве внутренних и таким образом объявлять о них обоих в параметре TLV "поддерживаемых протоколов" своих пакетов LSP.

Узел с секционированным стеком должен использовать параметры TLV достижимости IP-протокола в пакетах IS-IS LSP для указания диапазона адресов инкапсулированных пакетов, которые он может завершить.

Узел с секционированным стеком может принимать расширения достижимости IP-протокола от узла только-IP через сдвоенную функцию AE-DCF. По этой причине такой узел с секционированным стеком должен обладать возможностью передавать трафик в пункт назначения через функцию AE-DCF, где и будут декапсулироваться его пакеты. Для достижения такого положения узел с секционированным стеком должен отыскать следующий узел на пути к каждому пункту назначения, который способен выполнить декапсуляцию, либо пункт назначения с секционированным стеком точно таким же образом, как это выполняет функция AE-DCF.

Узел с секционированным стеком и автоматически выполняемой инкапсуляцией должен объявить о том, какие режимы инкапсуляции он поддерживает, используя для этой цели параметр TLV, относящийся к возможности выполнения инкапсуляции в соответствии с параграфом B.4.3.1.

Когда узел с секционированным стеком принимает пакет, для которого он является пунктом назначения, он должен произвести контроль этого пакета с целью установить, нет ли внутри этого пакета другого инкапсулированного пакета. Если да, то этот пакет подлежит внутренней обработке, если он не является пакетом IS-IS или ES-IS, ибо в этом случае он должен быть отброшен (если не существует предусмотренного и вручную обеспечиваемого туннеля, по которому необходимо пропускать IS-IS) таким же образом, как это выполняет сдвоенная функция AE-DCF.

Таким же образом, как это выполняет сдвоенная функция AE-DCF, узел с секционированным стеком должен поддерживать инкапсуляцию GRE, рассматриваемую в параграфе 7.1.8.

B.4.5 Использование IP-узлов, которые не соответствуют положениям параграфа 7.1.10.1.1 в отношении функции AE-DCF

Узлы только-IPv4 или только-IPv6, которые соответствуют положениям RFC 1195, но не поддерживают функцию создания смежности при поддержке протокола, которая рассматривается в параграфе 7.1.10.1.1, могут использоваться в той же смешанной зоне Уровня-1 или субдомене Уровня-2, что и функция AE-DCF, однако администратор сети должен вручную удостовериться в том, что подобный узел не имеет никаких смежностей с другими узлами, которые могут передавать ему пакеты, им не поддерживаемые.

B.4.6 Использование сдвоенных узлов без функции AE-DCF и сдвоенных узлов с функцией AE-DCF в одной и той же IS-IS зоне

Сдвоенные узлы, которые соответствуют положениям RFC 1195, но не поддерживают функцию AE-DCF, могут использоваться в тех же смешанных зонах Уровня-1 или субдоменах Уровня-2 с функцией AE-DCF при нижеперечисленных ограничениях:

Интегральные IS-IS узлы (или группы узлов), которые поддерживают несколько протоколов сетевого уровня, но не поддерживают функцию AE-DCF, все еще подвержены топологическим ограничениям, рассматриваемым в RFC 1195. Это означает, что администратор сети должен удостовериться в том, что подобный узел не может пропускать пакеты в соседний узел, который не может передать данные о типе этого пакета.

Следовательно, слово "сдвоенный" обозначает сдвоенный интегральный IS-IS узел, который соответствует положениям RFC 1195, но не содержит функцию AE-DCF:

надежной комбинацией является OSI-AEDCF-сдвоенный-AEDCF-IP;

надежной комбинацией является OSI-AEDCF-сдвоенный-сдвоенный-сдвоенный-AEDCF-IP;

надежной комбинацией является IPv4-AEDCF-сдвоенный IPv4&IPv6-AEDCF-IPv6;

надежной комбинацией является сдвоенный-AEDCF-OSI-AEDCF-сдвоенный;

ненадежной комбинацией является OSI-IPv4&OSIAEDCF-сдвоенный IPv4&OSI-сдвоенный IPv4& IPv6-IPv4&IPv6 AEDCF-IPv6;
ненадежной комбинацией является OSI-IPv4&OSIAEDCF-сдвоенный IPv4&OSI-IPv4&IPv6&OSI-сдвоенный IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6.

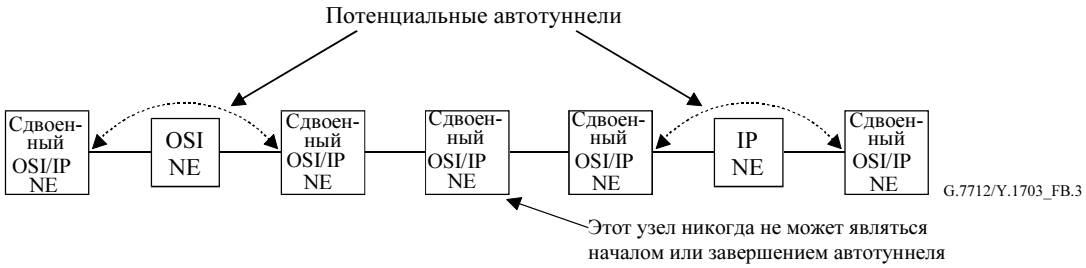


Рисунок B.3/G.7712/Y.1703 – Топологические требования, предъявляемые к сдвоенным узлам IS-IS зоны

B.4.7 Требования, предъявляемые к узлам Уровня-1 и Уровня-2

Рекомендуется, чтобы узлы, которые поддерживают как маршрутизацию Уровня-1, так и маршрутизацию Уровня-2 и располагаются в зоне, где используются эти функции AE-DCF, применялись:

– либо для поддержки всех протоколов сетевого уровня, которые имеют место как в субдомене Уровня-1, так и в субдомене Уровня-2, в котором работает этот узел и поддерживает функцию AE-DCF;

или

– для поддержки всех протоколов сетевого уровня, которые имеют место как в субдомене Уровня-1, так и в субдомене Уровня-2, в котором работает этот узел и соединяется либо напрямую, либо транзитом с непрерывными цепочками других узлов, которые поддерживают все протоколы сетевого уровня в рассматриваемой зоне, с узлом, который поддерживает функцию AE-DCF, а также все протоколы сетевого уровня в рассматриваемой зоне.

Следовательно, слово "сдвоенный" означает сдвоенный интегральный IS-IS узел, который соответствует положениям RFC 1195, но не поддерживает функцию AE-DCF:

надежно L2_subdomain-dual_L1/L2-non_dual (в соответствии с RFC 1195);

надежно L2_subdomain-dual_L1/L2-dual-dual-non_dual is safe (в соответствии с RFC 1195);

надежно L2_subdomain-dual_L1/L2-AE-DCF-mixted_network;

надежно L2_subdomain-dual_L1/L2-dual-dual-AE-DCF-mixted_network is safe;

ненадежно L2_subdomain-dual_L1/L2-non_dual-dual (если не применяются ограничения, указанные в RFC 1195);

ненадежно L2_subdomain-dual_L1/L2-non_dual-AE-DCF (если не применяются ограничения, указанные в RFC 1195).

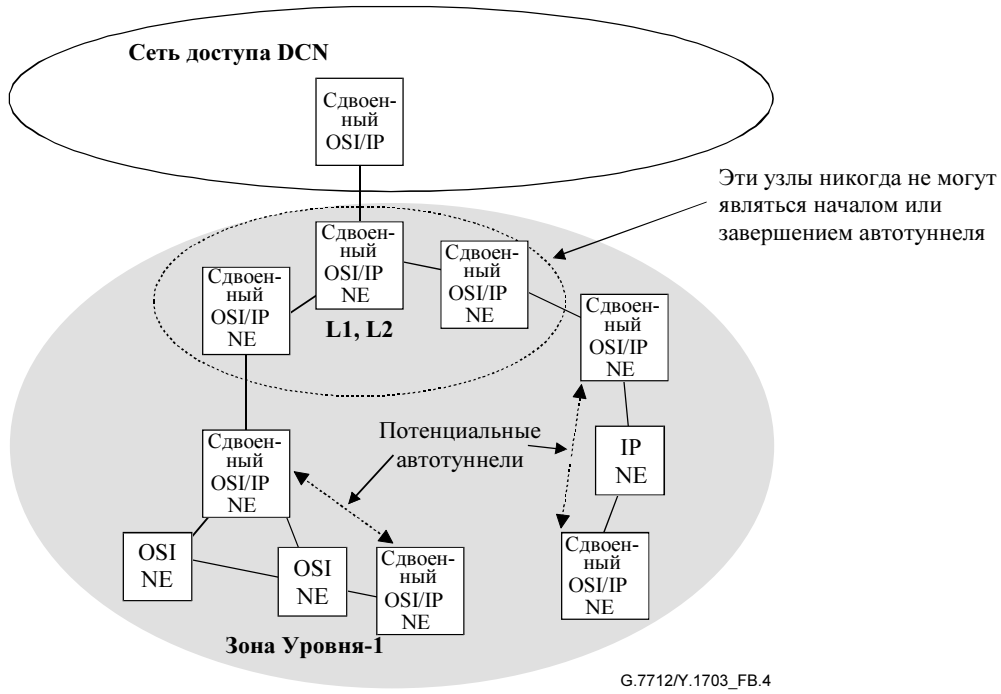


Рисунок B.4/G.7712/Y.1703 – Требования, предъявляемые к узлам Уровня-1 и Уровня-2

Однако вполне понятно, что шлюзовой элемент NE и, следовательно, маршрутизатор L1, L2 могут представлять собой устройство только-OSI. В этом случае вполне возможно иметь IP и автоматическую инкапсуляцию в рассматриваемой зоне благодаря следующему методу, пользоваться которым необходимо с осторожностью:

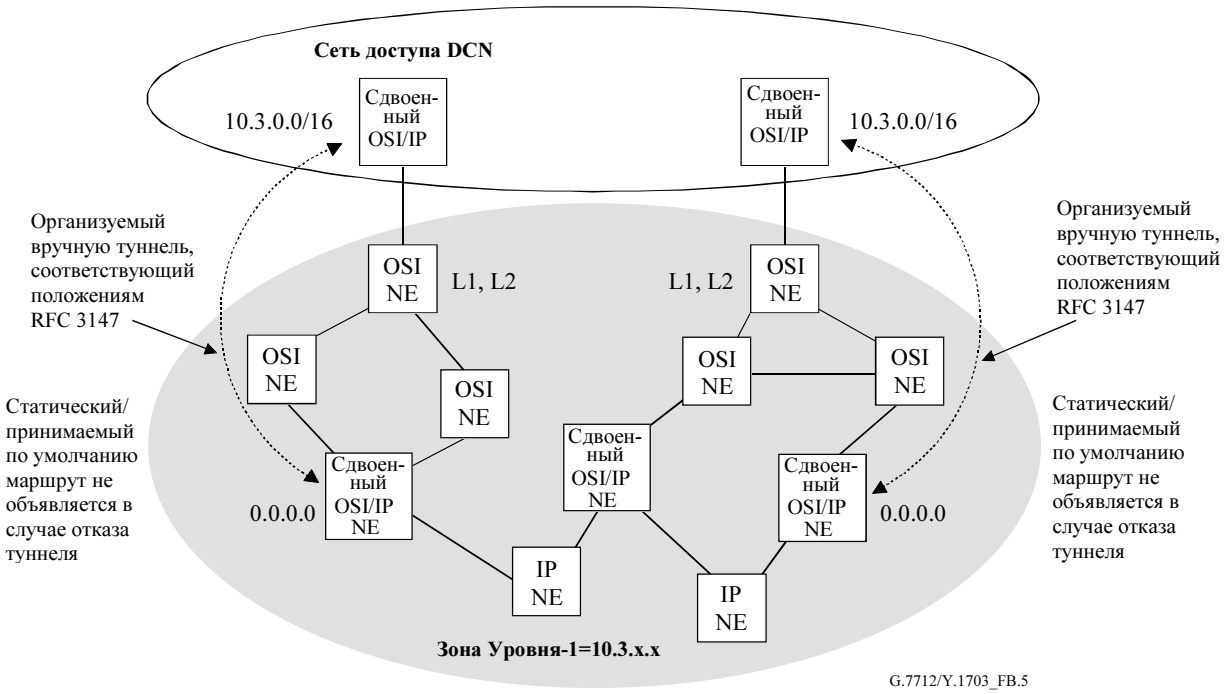


Рисунок B.5/G.7712/Y.1703 – Использование узла только-OSI в качестве шлюза

Один или несколько сдвоенных узлов в рассматриваемой зоне могут быть выбраны в качестве шлюзов для IP-пакетов. Эти узлы будут иметь конфигурацию, которая объявит о маршруте по умолчанию (0.0.0.0) в данной зоне с тем, чтобы привлечь весь IP-трафик, "передаваемый за ее пределами". Затем эти узлы будут передавать весь трафик "за пределами рассматриваемой зоны" по организованному вручную GRE туннелю, который проходит через узел только-OSI Уровня-1 и Уровня-2 в другой сдвоенный узел, размещенный за пределами зоны.

Этот сдвоенный узел, размещенный за пределами рассматриваемой зоны, должен иметь префикс, вручную вводимый в него, чтобы привлечь весь IP-трафик, связанный с ним для передачи в данной зоне и передать его в эту зону по имеющемуся туннелю. В другом случае такое устройство как протокол IP-маршрутизации может предусматриваться для передачи по туннелю таким образом, что с каждого конца можно видеть, подключен ли к источнику питания другой конец. Однако если используется интегральный IS-IS, то в этом случае должна использоваться другая маршрутизация, отличающаяся от обычно применяемой в рассматриваемой зоне, поскольку в данном случае фактически это будет уже маршрутизация, выполняемая в другом домене.

В случае применения подобного устройства сдвоенный узел в рамках рассматриваемой зоны, – если дальний конец "исчезает", – должен прекратить объявление маршрута, выбираемого по умолчанию, а сдвоенный узел, расположенный за пределами данной зоны, должен прекратить объявление префикса, который служит для определения узлов в этой зоне. Таким образом, могут быть предусмотрены резервные IP-шлюзы.

Необходимо отметить, что положения RFC 1195 утверждают, что в пакетах LSP Уровня-1 не должны объявляться маршруты, выбираемые по умолчанию. Данное решение требует, чтобы это правило было нарушено. Обычно RFC 1195 при рассмотрении узла Уровня-1 исходит из того, что узел Уровня-1, Уровня-2 представляет собой его маршрут по умолчанию. При подобном решении требуется, чтобы была выполнена перезапись этого режима работы после поступления в пакет LSP Уровня-1 объявления о маршруте по умолчанию. В случае невозможности выполнения такой перезаписи обходным маневром служит такая конфигурация IP-шлюзового узла, при которой производится выбор статических маршрутов, покрывающих все возможные пункты назначения "за пределами рассматриваемой зоны", что, по всей вероятности, будет сделана попытка достичь IP-стек в данной зоне.

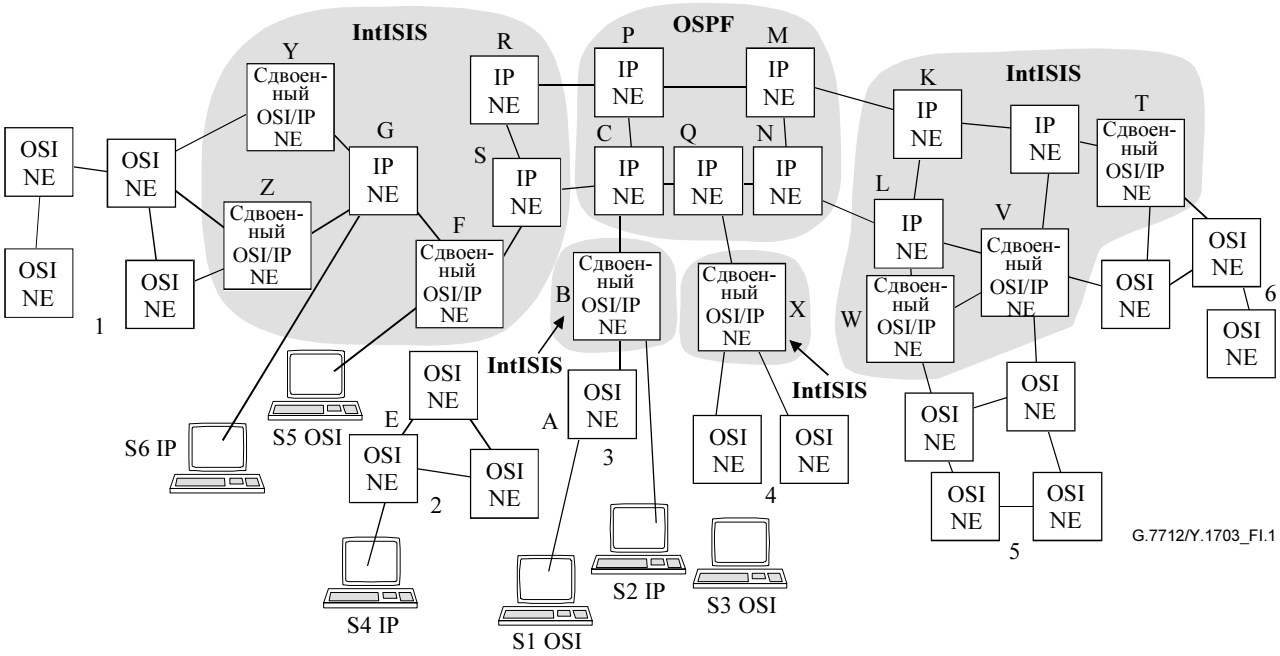
B.4.8 Требования, предъявляемые к субдомену Уровня-2

Вполне допустимо направлять по маршрутам все протоколы, изначально имеющие место в субдомене Уровня-2, – что соответствует положениям RFC 1195; в этом случае ни один из узлов Уровня-2 не должен поддерживать функцию AE-DCF, но все они должны поддерживать все имеющиеся протоколы сетевого уровня.

В другом случае также вполне допустимо использовать узлы Уровня-2, которые поддерживают не все имеющиеся в рассматриваемом домене протоколы сетевого уровня; в этом случае от сдвоенных или предназначенных для работы на многих языках узлов потребуется поддержка функции AE-DCF, так что пакеты могут автоматически инкапсулироваться, чтобы получить возможность пройти через подобные узлы.

Добавление I[2]

Ограничения, относящиеся к функциям взаимодействия в сети DCN



IntISIS Интегральная IS-IS

Рисунок I.1/G.7712/Y.1703 – Алгоритмы (сценарии) взаимодействия

I.1 Общие допущения

В сети DCN действует функция IWF для IP-OSI стеков Уровня 2-3. Механизмы взаимодействия, применяемые на других уровнях, в настоящей Рекомендации не рассматриваются (т. е. она носит лишь посреднический характер).

Определение взаимодействия рассматривается в параграфе 7.1.7.

Рассмотрение вопроса о туннелях основывается на положениях материалов RFC.

Элементы NE только-IP поддерживают IP-маршрутизацию и могут содержать повторное распределение между интегральными IS-IS и функцией OSPF.

I.2 Общее для всех алгоритмов

Динамическая маршрутизация выполняется посредством применения повторного распределения IP-адресной информации между функцией OSPF и элементами IS-IS NE. Повторное распределение производится на узлах OSPF между парами: (R,P), (S,C), (M,K), (N,L).

I.2.1 Алгоритм 1: Система управления на основе OSI, подключенная к узлу A

Должен существовать хотя бы один туннель, выполненный от B до одного или нескольких Y или Z.

Должен существовать туннель, выполненный от B до X.

Должен существовать туннель, выполненный от B до F.

Должен существовать хотя бы один туннель, выполненный от B до одного или нескольких W, V или T.

---

[2] ПРИМЕЧАНИЕ. – Это новое Добавление I заменяет собою Рекомендацию МСЭ-T G.7712/Y.1703 (версия 2001 года).

Вышеперечисленные туннели будут, по всей вероятности, допускать передачу IS-IS через них (внутри каждого туннеля); однако вполне возможна также маршрутизация между доменами. В случае подобных условий некоторые туннели могут в результате выбора маршрутизации оказаться перегруженными.

Система управления на основе OSI теперь имеет возможность взаимодействия CLNS с любым элементом NE только-OSI или со сдвоенным стеком в рассматриваемой сети, но не располагает возможностью взаимодействия с элементами NE только-IP. Хотя подсистема управления на основе OSI будет располагать возможностью передачи CLNS пакетов в элемент NE со сдвоенным стеком, она все же не сможет управлять им, если он не будет удобным в управлении на основе OSI.

I.2.2 Алгоритм 2: Системы управления на основе IP, подключенные к узлу B

В этой конкретной сети IP-трафик может передаваться с узла B во все элементы IP NE, не требуя при этом никаких туннелей. Элементы NE OSPF, а именно, P, C, M и N, должны поддерживать повторное распределение IP-маршрутов в интегральной IS-IS. Фильтры должны конфигурироваться по функции OSPF в узлах P, C, M и N с тем, чтобы воспрепятствовать образованию зацикливания при маршрутизации.

Система управления на основе IP теперь имеет возможность взаимодействия IP с любым элементом NE только-IP или со сдвоенным стеком в рассматриваемой сети, но не располагает возможностью взаимодействия с элементами NE только-OSI. Хотя подсистема управления на основе IP будет располагать возможностью передачи IP-пакетов в элемент NE со сдвоенным стеком, она все же не сможет управлять им, если он не будет удобным в управлении на основе IP.

I.2.3 Алгоритм 3: Системы управления на основе OSI, подключенные к узлу C

Сетевой элемент C (NE C) не сможет обеспечить возможность взаимодействия OSI, так что окажется невозможной передача CLNS-пакетов; вследствие этого система управления на основе OSI в данном узле функционировать не сможет.

I.2.4 Алгоритм 4: Системы управления на основе IP, подключенные к узлу E

Сетевой элемент E (NE E) не сможет обеспечить возможность взаимодействия IP, так что окажется невозможной передача IP-пакетов; вследствие этого система управления на основе IP в данном узле функционировать не сможет.

I.2.5 Алгоритм 5: Системы управления на основе OSI, подключенные к узлу F

CLNS-трафик может передаваться через элемент NE F в сеть 2 OSI, не требуя при этом никаких туннелей, поскольку элемент NE F сам в состоянии осуществлять передачу CLNS-пакетов.

Должен существовать туннель, выполненный от F до B.

Должен существовать хотя бы один туннель, выполненный от F до одного или нескольких Z или Y.

Должен существовать туннель, выполненный от F до X.

Должен существовать хотя бы один туннель, выполненный от F до одного или нескольких W, V или T.

Вышеперечисленные туннели будут, по всей вероятности, допускать передачу IS-IS через них (внутри каждого туннеля); однако вполне возможна также маршрутизация между доменами. В случае подобных условий некоторые туннели в результате выбора маршрутизации могут оказаться перегруженными.

Система управления на основе OSI теперь имеет возможность взаимодействия CLNS с любым элементом NE только-OSI или со сдвоенным стеком в рассматриваемой сети, но не располагает возможностью взаимодействия с элементами NE только-IP. Хотя подсистема управления на основе OSI будет располагать возможностью передачи CLNS-пакетов в элемент NE со сдвоенным стеком, она все же не сможет управлять им, если он не будет удобным в управлении на основе OSI.

I.2.6 Алгоритм 6: Системы управления на основе IP, подключенные к узлу G

В этой конкретной сети IP-трафик может передаваться с узла G во все элементы IP NE, не требуя при этом никаких туннелей. Элементы NE OSPF, а именно, P, C, M и N, должны поддерживать повторное распределение IP-маршрутов в интегральной IS-IS. Фильтры должны конфигурироваться по функции OSPF в узлах P, C, M и N с тем, чтобы воспрепятствовать образованию зацикливания при маршрутизации.

Система управления на основе IP теперь имеет возможность взаимодействия IP с любым элементом NE только-IP или со сдвоенным стеком в рассматриваемой сети, но не располагает возможностью взаимодействия с элементами NE только-OSI. Хотя подсистема управления на основе IP будет располагать возможностью передачи IP-пакетов в элемент NE со сдвоенным стеком, она все же не сможет управлять им, если он не будет удобным в управлении на основе IP.

Добавление II

Пример реализации автоматической инкапсуляции

II.1 Введение

Настоящее Добавление не является требованием, а служит кратким примером особенностей возможности реализации узла на базе одного аспекта, присущего обсуждаемой в настоящей Рекомендации характеристики.

Простейший (однако не единственный) способ для узла выполнить вычисление следующего узла на кратчайшем пути до оконечного пункта назначения, куда должен быть передан пакет, который может не подвергаться инкапсуляции, состоит в модификации способствующего этому алгоритма SPF.

Этот алгоритм может быть модифицирован таким образом, чтобы найти следующий узел на кратчайшем пути к пункту назначения, который принимает инкапсулированный трафик (IP через OSI), и следующий узел на кратчайшем пути к пункту назначения, который принимает инкапсулированный трафик (OSI через IP). Необходимо отметить, что эти два узла на практике могут представлять собой один и тот же узел, либо могут быть разными узлами. Ниже рассматривается модифицированный алгоритм Dijkstra, с помощью которого можно этого достичь.

Данный дополнительный процесс должен произойти только тогда, когда следующий переход не поддерживает протокол сетевого уровня такого типа, который соответствует адресу пункта назначения на рассматриваемом пути. Если же следующий переход поддерживает протокол сетевого уровня такого типа (как определено в параметре TLV "поддерживаемых протоколов" в блоках IS-IS Hello PDU, поступивших от подобного узла), то пакеты в этот пункт назначения могут быть просто переданы и забыты, вследствие чего нет необходимости выполнять поиск узла на этом пути, который может выполнить декапсуляцию.

Затем данный алгоритм должен идентифицировать IP-адрес для этого следующего узла с декапсуляцией, если в качестве пункта назначения на рассматриваемом пути выступает система OSI End System, а затем должен идентифицировать OSI-адрес для следующего узла с декапсуляцией, если IP-адрес соответствует пункту назначения пути (PATH).

Неблагоприятный исход процесса отыскания IP-адреса для следующего узла с декапсуляцией указывает, что в конфигурации этого узла имеет место ошибка (отсутствие IP-адреса); в некоторых случаях это может закончиться передачей администратору сети ошибочного сообщения. Может произойти потеря пакета, если для CLNS-пакета требуется передача по туннелю в этот узел через IP, поскольку при отсутствии IP-адреса пункта назначения невозможно выполнить инкапсуляцию, что и приведет к отбрасыванию данного пакета.

Неблагоприятный исход процесса отыскания узла, который может выполнить декапсуляцию, указывает на то, что при проектировании сети была допущена ошибка, говоря более конкретно, отказ в соответствии тем топологическим ограничениям, которые рассматриваются в настоящей Рекомендации. Это должно привести к передаче ошибочного сообщения "пункт назначения недоступен".

Для каждого IP-пункта назначения, который требует выполнения инкапсуляции после следующего перехода, этот узел может сделать отметку в IP-таблице передачи данных с указанием OSI-адреса пункта назначения, который должен использоваться для инкапсуляции всех IP-пакетов с пунктом назначения по этому адресу.

Для каждого OSI-пункта назначения, который требует выполнения инкапсуляции после следующего перехода, этот узел может сделать отметку в OSI-таблице передачи данных с указанием IP-адреса пункта назначения, который должен использоваться для инкапсуляции всех OSI-пакетов с пунктом назначения по этому адресу.

Узел, поддерживающий IPv4, IPv6 и OSI, может найти два адреса (например, адрес IPv4 и адрес IPv6), которые можно было бы использовать для выполнения инкапсуляции. В данном случае такой узел может выбирать, какой из них приведет к получению пакета, являющегося типом протокола сетевого уровня, который поддерживает следующий переход (как это рассматривается в параметре TLV "поддерживаемых протоколов", представленном в блоках IS-IS Hello PDU, которые поступили из этого узла).

II.2 Модификации алгоритма Dijkstra

В приводимых ниже параграфах содержится полный алгоритм Dijkstra, включая расширения для поддержки автотуннелирования. Он основан на алгоритме, рассматриваемом в RFC 1195. Этот алгоритм подходит для сдвоенного IPv4 и CLNS узла с автоматическим выполнением инкапсуляции. Изменения, внесенные в этот алгоритм, показаны ***жирным курсивом***.

С помощью этого алгоритма создается база данных PATHS; для каждого пункта назначения она содержит идентификацию первого узла от S до N, способного выполнить декапсуляцию IP через OSI, и идентификацию первого узла от S до N, способного выполнить декапсуляцию OSI через IP.

Для каждого IP-пункта назначения первый узел от S до N, способный выполнить декапсуляцию IP через OSI, может иметь свой OSI-адрес, загруженный в IP-таблицу передачи данных в качестве адреса пункта назначения, который должен использоваться в любом CLNP-пакете, применяемом для инкапсуляции IP через OSI в том случае, если следующий переход не поддерживает IP.

Для каждой системы OSI End System первый узел от S до N, способный выполнить декапсуляцию OSI через IP, может иметь один из своих IP-адресов, загруженных в OSI-таблицу передачи данных в качестве адреса пункта назначения, который должен использоваться в любом IP-пакете, применяемом для инкапсуляции OSI через IP в том случае, если следующий переход не поддерживает OSI.

II.2.1 Изменения, вносимые в базу данных

База данных PATHS и TENTS должна модифицироваться, чтобы содержать расширение до элемента {Adj(N)} этой triple. Элемент N смежности будет содержать две соответствующие записи поддержки сдвоенного протокола (IDP(N)-ODP(N)), которые будут представлять собой идентификатор System ID первого маршрутизатора Dual router на пути от S до N, способного выполнить декапсуляцию туннелированных пакетов IP через OSI (IDP(N)), а также идентификатор System ID первого маршрутизатора Dual Router на пути от S до N, способного выполнить декапсуляцию туннелированных пакетов OSI через IP (ODP(N). Если на пути PATH не имеется никакого маршрутизатора *DP(N), то это значение будет установлено на нуль. Если в базе данных либо TENTS, либо PATHS имеется несколько записей Adj(N), то каждая смежность будет иметь соответствующие записи *DP(N). Таким образом, каждая triple будет иметь формат <N,d(N),{Adj(N)-IDP(N)-ODP(N)}>

Если значение IDP(N) установлено на нуль, то это означает, что на пути к пункту назначения не имеется никакого маршрутизатора Dual Router, способного выполнить декапсуляцию и инкапсуляцию пакетов IP через OSI.

Если значение ODP(N) установлено на нуль, то это означает, что на пути к пункту назначения не имеется никакого маршрутизатора Dual Router, способного выполнить декапсуляцию и инкапсуляцию пакетов OSI через IP.

II.2.2 Изменения, вносимые в алгоритм

Изменения, вносимые в SPF алгоритм, рассматриваемый в разделе C.1.4 RFC 1195, будут следующими:

```
Шаг 0: Инициализировать TENT и PATHS, чтобы они были свободными. Инициализировать длину
TENT(tentlength), чтобы она была [internalmetric=0, externalmetric=0].

    (длина tentlength соответствует длине пути (pathlength) элементов на базе данных
    TENT, которую мы в настоящий момент рассматриваем).

    1) Добавить <SELF,0,W-0-0> в базу данных PATHS, где W - это конкретное значение,
       включающее трафик, чтобы SELF пропускалось до внутренних процессов (а не
       передавалось).

    2) Теперь произведем предварительную загрузку базы TENT местной базой данных
       смежности (каждый ввод в TENT должен маркироваться либо как представляющий
       собой систему End System, либо как маршрутизатор, чтобы иметь возможность
       проверить правильность окончания Шага 2 - Следует отметить, что каждый местный
       ввод IP достижимости включается в качестве смежности и маркируется как
```

представляющий собой систему End System). Для каждой смежности Adj(N) (включая уровень 1 OSI Руководства по смежностям или уровень 2 OSI разрешаемых незаблокированных адресов и вводы IP достижимости) на незаблокированных каналах к системе N для SELF в состоянии "Up" вычисляют:

d(N) = стоимость родительского канала смежности (N),
полученную из metric.k, где k = это один из {default metric,
delay metric, monetary metric, error metric}

Adj(N)***-IDP(N)-ODP(N)*** = номер смежности в N,
SID маршрутизатора следующего транзитного участка по тракту до соседнего участка, способного декапсулировать IP по пакетам OSI и SID маршрутизатора следующего транзитного участка по тракту до соседнего участка, способного декапсулировать OSI по пакетам IP. В этом случае, т. е. во время инициализации оба значения DP будут устанавливаться на 0

3) Если triple <N,x,{Adj(M)-***IDP(N)-ODP(N)***}> размещается в TENT, то:

Если x = d(N), то {Adj(M)***-IDP(N)-ODP(N)***} <--- {Adj(M)***-IDP(M)-ODP(M)***}
U {Adj(N)***-IDP(N)-ODP(N)***}.

4) Если N представляет собой маршрутизатор или ввод OSI End System и теперь имеется большее число смежностей в {Adj(M)}, чем maximumPathSplits, то избыточные смежности удаляются, как это описано в п. 7.2.7 ИСО/МЭК 10589. Если N представляет собой ввод IP достижимости, то избыточные смежности могут удаляться по желанию. Это не окажет никакого влияния на правильность маршрутизации, однако может исключить определенность для IP маршрутов (т. е. IP пакеты в рамках зоны все еще будут передаваться по оптимальным маршрутам, но когда существуют несколько одинаково хороших маршрутов, эти IP пакеты необязательно будут передаваться точно по тому маршруту, который является одним конкретным ожидаемым маршрутом).

5) Если x < d(N), то не предпринимать никаких действий.

6) Если x > d(N), удалить <N,x,{Adj(M)***-IDP(M)-ODP(M)***}> из TENT и дополнительно ввести triple <N,d(N),{Adj(N) ***-IDP(N)-ODP(N)***}> в TENT.

7) Если triple <N,x,{Adj(M)***-IDP(M)-ODP(M)*** }> отсутствует в TENT, то дополнительно ввести в TENT <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}>.

8) Теперь дополнительно ввести системы, в которых местный маршрутизатор не имеет смежностей, но которые упоминаются в LSPs соседнего псевдоузла. Смежность в таких системах устанавливается для предназначенного маршрутизатора. Необходимо отметить. что это не включает вводы IP достижимости от LSP соседнего псевдоузла. В частности, LSP псевдоузла не включают вводы IP достижимости.

9) Для всех широковещательных каналов в состоянии "On" найти LSP псевдоузла для такого канала (в особенности LSP с номером 0 или с первыми 7 октетами LSPID, равными LnCircuitID для этого канала, где n равно 1 (для маршрутизации Уровня 1) или 2 (для маршрутизации Уровня 2)). Если такая ситуация имеет место, во все соседние N, указанные во всех LSP рассматриваемого псевдоузла, которые отсутствуют в TENT, дополнительно ввести в TENT запись <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}>, где:

d(N) = metric.k рассматриваемого канала.
Adj(N) = число смежностей в DR.

10) Перейти к Шагу 2.

Шаг 1: Рассмотреть состояние PDU нулевой линии в P, системы, только что размещенной в PATHS (т. е. LSP с такими же первыми 7 октетами LSPID, как в P, и нуль числа LSP).

1) Если присутствует эта LSP и понятен бит "Неопределенная стоимость Hippity", то для каждого Adj(*) – IDP(*) – ODP(*) имеется пара в базе данных PATHS для P. Если она не является LSP псевдоузла и если IDP(*) равен нулю, то необходимо проверить поле возможности декапусляции LSP, если она поддерживает IP в OSI, затем определить значение IDP(P) для этой смежности, которое должно быть системой ID в P. Если ODP(*) равен нулю, то необходимо проверить поле возможности декапсуляции LSP, если она поддерживает OSI и IP, затем определить значение IDP(P) для этой смежности, которое должно быть системой ID в P.

2) Если присутствует эта LSP и понятен бит "Неопределенная стоимость Hippity", то для каждой LSP в P (т. е. все LSP с одинаковыми первыми 7 октетами LSPID и P, независимо от значения числа SP) вычислить:

dist(P,N) = d(P) + metric.k(P,N)

для каждого соседнего N (как End System, так и маршрутизатора) этой системы P. Если установлен бит "Неопределенная стоимость Hippity", то необходимо рассматривать только соседние End System этой системы P.

Необходимо отметить, что соседние End Systems этой системы P включают вводы IP достижимых адресов, включенных в LSP из системы P. В данном случае d(P) представляет собой второй элемент рассматриваемой triple

<P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}>

и metric.k(P,N) представляет собой стоимость этой линии от P до N, как указано в PDU состояния линии P.

3) Если dist (P,N) > MaxPathMetric, то не предпринимать никаких действий.

4) Если <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> размещается в PATHS, то не предпринимать никаких действий.

ПРИМЕЧАНИЕ. – d(N) должно быть меньше, чем dist(P,N), или иначе N не будет включено в PATHS. В данном случае может быть выполнена дополнительная логическая проверка, позволяющая убедиться в том, что d(N) фактически будет меньше, чем dist(P,N).

5) Если в TENT размещается triple <N,x,{Adj(N)***-IDP(N)-ODP(N)***}>, то:

a) Если x = dist(P,N), то {Adj(N)***, IDP(N)-ODP(N)***} <--
{Adj(N)***-IDP(N)-ODP(N)***} U {Adj(P)***-IDP(P)-ODP(P)***}.
Необходимо отметить, что даже если значение Adj(N) равно значению Adj(P), но соответствующие значения либо IDP(P), либо ODP(P) и IDP(N) или ODP(N) различаются, то это должно рассматриваться как другая смежность и будет представлять собой другой путь к месту назначения.

b) Если N представляет собой маршрутизатор или OSI end system, и при этом в {Adj(N)} имеет место больше смежностей, чем maximumPath Splits, то следует удалить излишние смежности, как описано в п. 7.2.7 ИСО/МЭК 10589. Для вводов IP достижимости избыточные смежности могут удаляться по желанию. Это не оказывает никакого влияния на правильность маршрутизации, однако может исключить определенность для IP маршрутов (т.е. IP пакеты в рамках зоны все еще будут передаваться по оптимальным маршрутам, когда существуют несколько одинаково хороших маршрутов, эти IP пакеты необязательно будут передаваться точно по тому маршруту, который является одним конкретным ожидаемым маршрутом).

c) Если x < dist(P,N), то не предпринимать никаких действий.

d) Если x > dist(P,N), то удалить из TENT <N,x,{Adj(N)***-IDP(N)-ODP(N)***}> и дополнительно ввести туда <N,dist(P,N),{Adj(P)***-IDP(P)-ODP(P)***}>

6) Если triple <N,x,{Adj(N)}> отсутствует в TENT, то дополнительно ввести в TENT <N,dist(P,N),{Adj(P)}>.

Шаг 2: Если TENT свободен, необходимо остановиться. Кроме того:

1) Найти элемент <P,x,{Adj(P)***-IDP(P)-ODP(P)***}> с минимальным x следующим образом:

a) Если элемент <*,tentlength,*> остается в TENT в перечне длины пути (tentlength), то выбрать этот элемент. Если в перечне длины пути указаны не один элемент, а несколько, то выбрать один из этих элементов (если таковой существует) для системы, которая представляет собой псевдоузел, отдавая предпочтение перед системой, не являющейся псевдоузлом. Если в рассматриваемом перечне длины пути не имеется других элементов, то увеличить длину пути и повторить Шаг 2.

b) Удалить из TENT <P,tentlength,{Adj(P)***-IDP(P)-ODP(P)***}>.

c) Дополнительно ввести в PATHS <P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}>.

d) Если он представляет собой выполнение процесса решения Уровня 2 и эта система только что введена дополнительно в PATHS с указанием в перечне как промежуточной системы сегмента Уровня 2, то дополнительно ввести в PATHS <AREA.P,d(P),{Adj(P)}>, где AREA.P представляет собой название элемента сети другого конца виртуальной линии, полученное посредством использования первой AREA, включенной в перечень LSP в P, и присоединением ID в P.

e) Если рассматриваемая система, только что дополнительно включенная в PATHS, была End System, то следует перейти к Шагу 2. Кроме того, перейти к Шагу 1.

ПРИМЕЧАНИЕ. – В контексте Уровня 2 "End Systems" представляют собой набор Префиксов достижимых адресов (Reachable Address Prefixes) (для OSI), набор адресов зоны (Area addresses) с нулевой стоимостью (опять же для OSI) и набор вводов IP достижимости (включая как внутренние, так и внешние).

Добавление III

Руководство по введению в действие элементов SDH NE в сдвоенном режиме работы согласно RFC 1195 и по влиянию факультативной автоматической инкапсуляции

III.1 Введение

В настоящем добавлении рассматривается руководство по вводу в действие узлов Integrated IS-IS в сети двухрежимной передачи IPv4 и OSI, а также по вопросу о том, каким образом использовать описанную в Приложении B функцию факультативной автоматической инкапсуляции.

III.2 Система Integrated IS-IS без автоматической инкапсуляции

III.2.1 Введение и правила, изложенные в RFC 1195

Система Integrated IS-IS, как это рассматривается в RFC 1195, первоначально была записана как протокол сдвоенной маршрутизации. Конкретно она была записана как имеющая возможность осуществлять маршрутизацию как IPv4, так и CLNP с помощью выполнения единственного вычисления SPF, единственного набора количественных величин как для IP, так и для CLNP, а также единственного набора сообщений Hello и блоков LSP.

Говоря еще более конкретно, маршрутизаторы Integrated IS-IS, соответствующие положениям RFC 1195, производят расчет кратчайших путей в зоне Уровня-1 или субдомене Уровня-2 без учета того факта, будет ли какой-либо кандидат-маршрутизатор фактически иметь возможность передавать пакеты любого конкретного типа.

Это четко изложено в разделе 3.10 в RFC 1195:

– "При выполнении вычислений Dijkstra не принимается в расчет тот факт, будет ли маршрутизатор типа IP-only, OSI-only или двойного типа. Топологические ограничения, рассматриваемые в разделе 1.4, обеспечивают, что IP-пакеты будут передаваться только через IP-маршрутизаторы, а OSI-пакеты – только через OSI-маршрутизаторы".

Что касается маршрутизатора Integrated IS-IS, то маршрутизатор является просто маршрутизатором. Предположение состоит в том, что любой маршрутизатор в рассматриваемой сети может обрабатывать пакет любого типа, который в нее поступает.

Следовательно, маршрутизаторы Integrated IS-IS выполняют расчет маршрутов и пересылают пакеты, в основе которых лежит вышеупомянутое предположение; оператор несет ответственность за обеспечение того факта, что данное предположение является на самом деле правильным.

Таким образом, в RFC 1195 изложены топологические ограничения. Отказ в реализации этих топологических ограничений RFC 1195 может привести к потере пакетов, поскольку пакеты исчезают в "черной дыре" маршрутизатора, который просто отбрасывает пакеты, не пригодные для передачи, ибо он не поддерживает их.

В простой сети с единственной зоной Уровня-1 эти правила совершенно просты. Эти правила таковы:

1) Если IPv4-пакеты должны передаваться в какой-либо зоне, то все эти маршрутизаторы этой зоны должны быть в состоянии передавать IPv4-пакеты.

2) Если CLNP-пакеты должны передаваться в какой-либо зоне, то все эти маршрутизаторы этой зоны должны быть в состоянии передавать CLNP-пакеты.

3) Если и IPv4-пакеты, и CLNP-пакеты должны передаваться в какой-либо зоне, то все маршрутизаторы этой зоны должны быть сдвоенными, т. е. быть в состоянии передавать оба вида пакетов.

Таким образом, достаточно легко выполнить классификацию зон IS-IS Уровня-1 на классы "зона только-OSI", "зона только-IP" и "Сдвоенная зона". Это представлено на рисунке III.1.

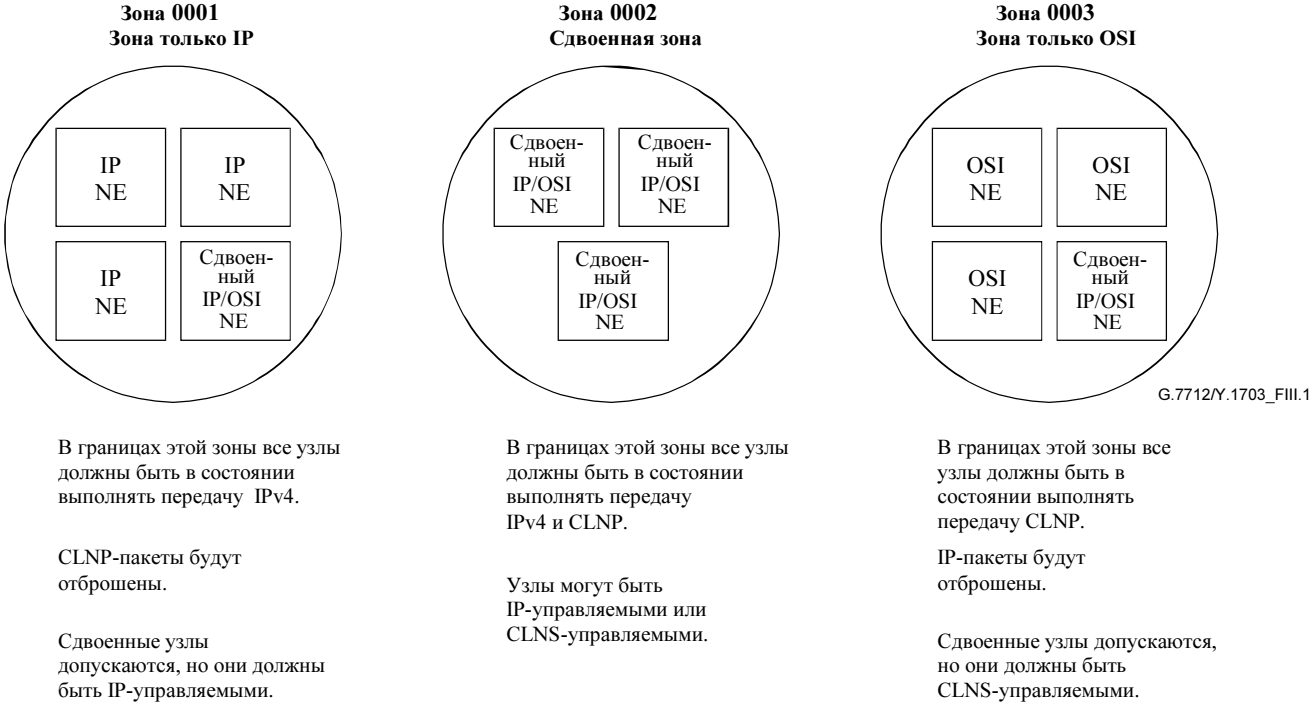


Рисунок III.1/G.7712/Y.1703 – Классификация зон IS-IS Уровня-1

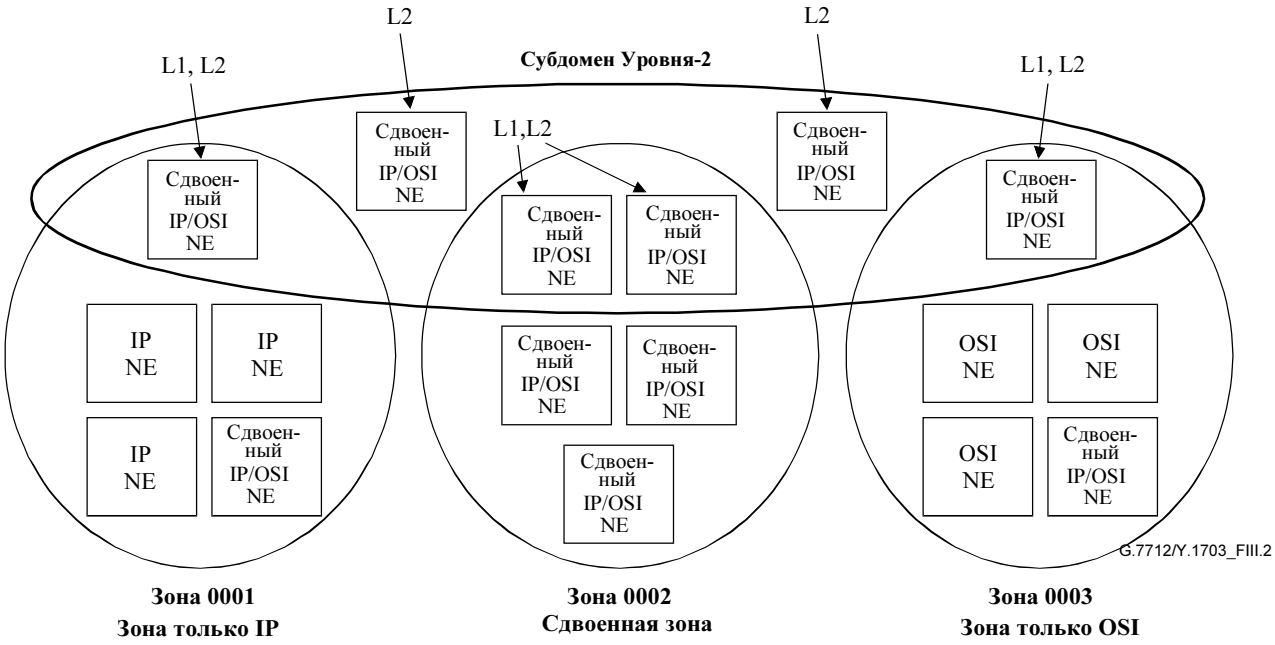
III.2.2 Субдомен Уровня-2

Если требуется сеть больших размеров, в которой необходима маршрутизация Уровня-2, то субдомен Уровня-2 передает пакеты между зонами Уровня-1 и, следовательно, должен поддерживать все типы пакетов, которые присутствуют во всех таких зонах Уровня-1. Правила для субдомена Уровня-2 таковы:

1) Если IPv4-пакеты передаются в любой из этих зон (зоны только-IP или сдвоенные зоны), то все маршрутизаторы в субдомене Уровня-2 должны быть в состоянии передавать IPv4.

2) Если CLNP-пакеты передаются в любой из этих зон (зоны только-OSI или сдвоенные зоны), то все маршрутизаторы в субдомене Уровня-2 должны быть в состоянии передавать CLNP.

Следовательно, если любая из этих зон является сдвоенной или если существуют и зоны только-OSI, и зоны только-IP, то маршрутизаторы в субдомене Уровня-2 должны быть сдвоенными. Это представлено на рисунке III.2.



Поскольку и IPv4, и CLNP передаются в границах зон Уровня-1, все узлы в субдомене Уровня-2 должны быть сдвоенными, даже те, которые имеются в зонах только-IP или только-OSI.

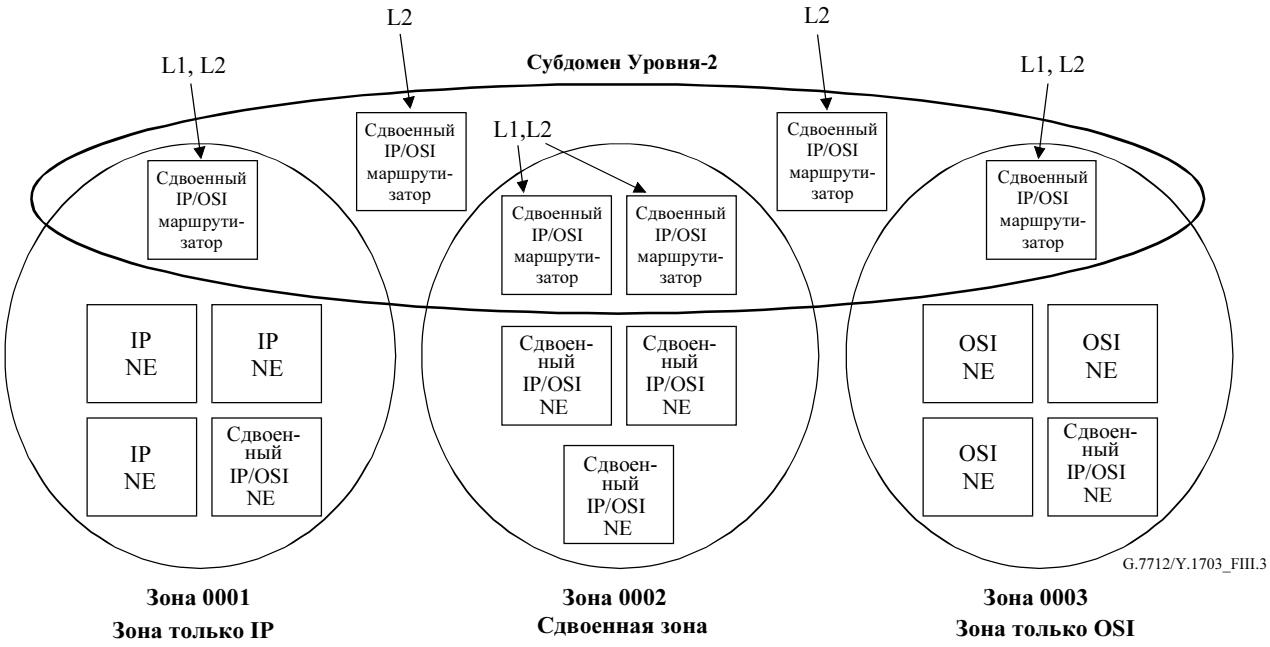
Узел представлен в субдомене Уровня-2, если он работает, используя маршрутизацию Уровня-2.

Рисунок III.2/G.7712/Y.1703 – Субдомен Уровня-2

III.2.3 Субдомен Уровня-2 с внешними маршрутизаторами, работающими в интегральной IS-IS

В настоящее время многие операторы используют маршрутизацию IS-IS Уровня-1 в своих элементах SDH NE только-OSI, а затем подключают несколько зон с помощью маршрутизации IS-IS Уровня-2 в маршрутизаторе внешней сети.

Если оператор намерен использовать аналогичную модель для сдвоенной сети, то он может работать в каждой зоне, применяя Integrated IS-IS Уровня-1, а в каждой внешней зоне маршрутизатор Integrated IS-IS Уровня-2. Это позволяет получить сеть, очень похожую на предыдущую, как показано на рисунке III.3.



Поскольку и IPv4, и CLNP передаются в границах зон Уровня-1, все маршрутизаторы в субдомене Уровня-2 должны быть сдвоенными, даже те, которые имеются в зонах только-IP или только-OSI.

Рисунок III.3/G.7712/Y.1703 – Маршрутизация IS-IS Уровня-2 в маршрутизаторе внешней сети

III.2.4 Внешние маршрутизаторы, работающие по протоколу OSPF или другим протоколам IP-маршрутизации

В настоящее время многие операторы используют IS-IS Уровня-2 в своих внешних маршрутизаторах, а также протокол OSPF или другие протоколы маршрутизации для IP. В этом случае внешний маршрутизатор должен оставаться маршрутизатором Уровня-2, используемым для элементов SDH NE, и, следовательно, в сдвоенной зоне должен действовать как сдвоенный Integrated IS-IS маршрутизатор. Однако его можно сконфигурировать для маршрутизации всех IP-пакетов, использующих протокол OSPF, посредством конфигурирования повторного распределения IP-маршрутов между IS-IS и протоколом OSPF. Благодаря этому все IP-пакеты будут маршрутизироваться по протоколу OSPF, тогда как CLNP-пакеты будут продолжать маршрутизироваться по IS-IS Уровня-2. Это показано на рисунке III.4.

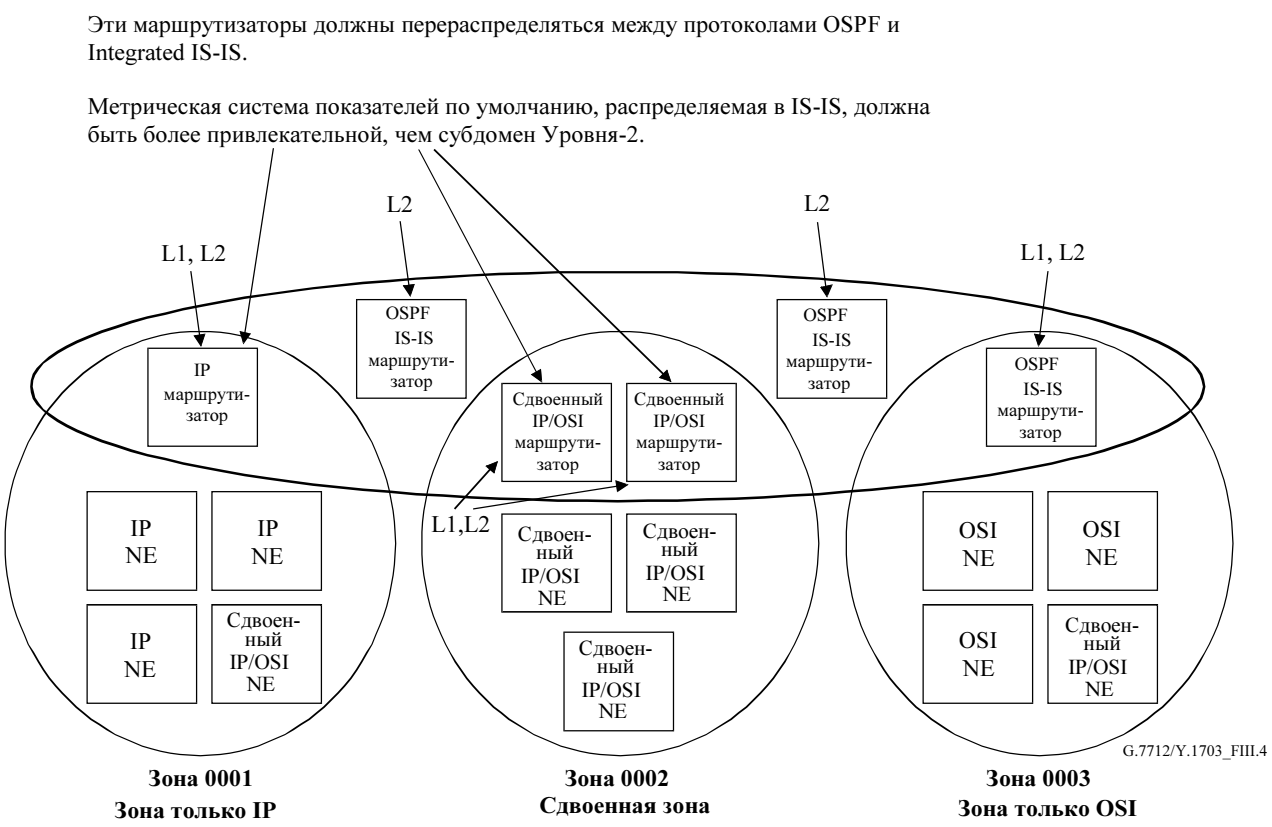


Рисунок III.4/G.7712/Y.1703 – Внешние маршрутизаторы, работающие по протоколу OSPF

Необходимо отметить, что стек Integrated IS-IS во внешних маршрутизаторах не будет ощущать, что субдомен Уровня-2 имеет значение только для CLNP-пакетов. Следовательно, рассматриваемые маршруты по протоколу OSPF должны перераспределяться в Integrated IS-IS с низким метрическим показателем по умолчанию, что сделает их более привлекательными для IP-пакетов, чем субдомен Уровня-2.

III.3 Интегральный IS-IS (Integrated IS-IS) с автоматической инкапсуляцией

III.3.1 Введение и влияние на топологические ограничения

Факультативная автоматическая инкапсуляция дает возможность нарушить топологические правила, рассматриваемые в RFC 1195. Автоматическая инкапсуляция в реальности приводит к созданию узла или группы узлов, которые обладают возможностью передавать пакеты, чего без этого сделать они не могут.

Процесс автоматической инкапсуляции представлен на рисунке III.5.

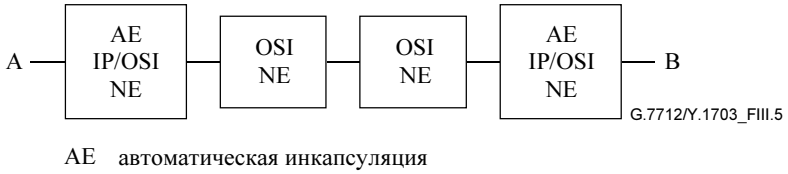
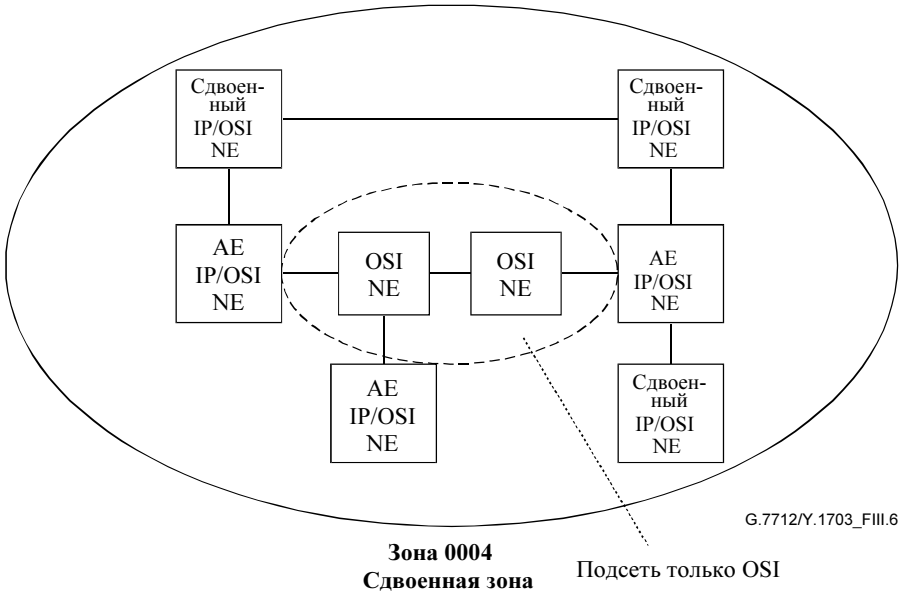


Рисунок III.5/G.7712/Y.1703 – Группа узлов с автоматической инкапсуляцией

Теперь эта группа узлов передает и IPv4-пакеты, и CLNP-пакеты, как только они поступят в пункт A или B от одного из узлов, где осуществляется автоматическая инкапсуляция.

Теперь эта группа узлов может безопасно размещаться в сдвоенной зоне, либо в сдвоенном субдомене Уровня-2, поскольку пара из узлов, осуществляющих автоматическую инкапсуляцию, будет передавать IPv4-пакеты посредством их инкапсуляции внутри CLNP-пакетов таким образом, что они будут передаваться элементами NE только-OSI, а не отбрасываться.

Теперь годная к работе сдвоенная зона может выглядеть внешне таким образом, как показано на рисунке III.6.

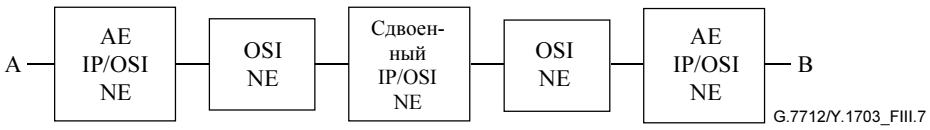


AE автоматическая инкапсуляция

Рисунок III.6/G.7712/Y.1703 – Пример действующей сдвоенной зоны

Необходимо отметить, что узлы только-OSI не должны напрямую подключаться к одному из сдвоенных узлов, в которых отсутствует возможность осуществления автоматической инкапсуляции. Лишь только наличие узлов с автоматической инкапсуляцией препятствует пересылке IPv4-пакетов в узел только-OSI.

Сдвоенный узел может напрямую подсоединяться к узлу только-OSI, если он также рассматривается как узел только-OSI, что можно видеть на рисунке III.7.



AE автоматическая инкапсуляция

Рисунок III.7/G.7712/Y.1703 – Подсоединение сдвоенного узла к узлу только-OSI

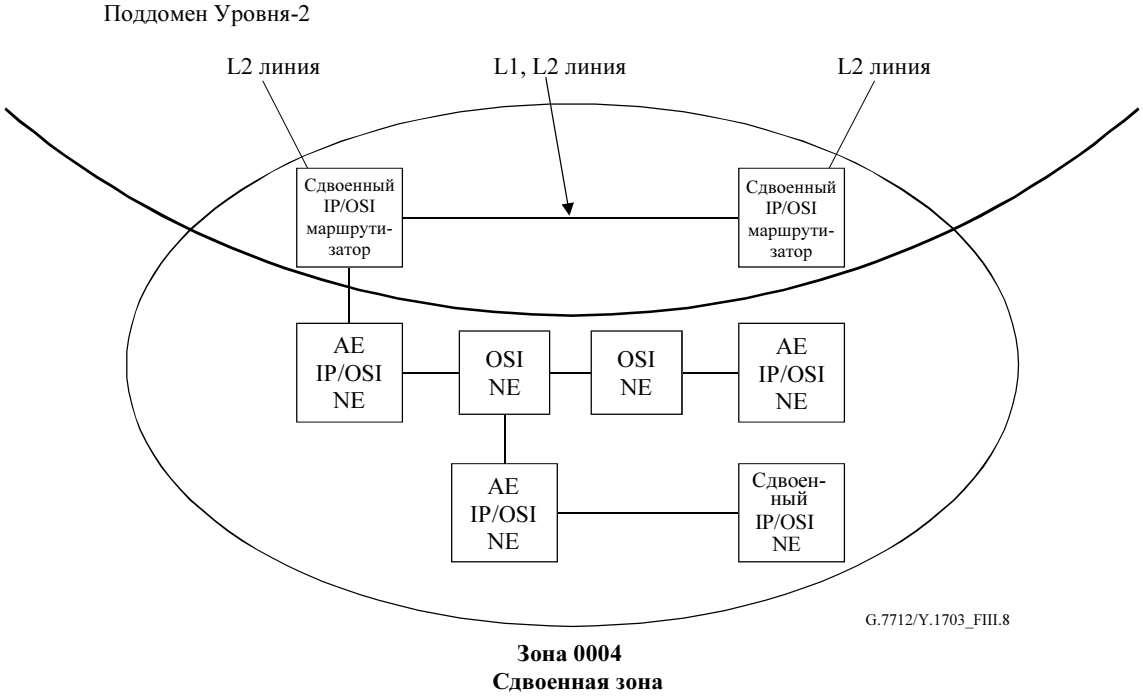
В этом случае сеть работает как сдвоенная сеть для пакетов, передаваемых из пункта A в пункт B; однако IPv4-пакеты дойти до центрального сдвоенного узла не в состоянии. Такой сдвоенный узел размещается внутри подсети только-OSI. Этот сдвоенный узел будет располагать возможностью передачи только CLNP-пакетов и должен управляться службой CLNS. Никаких других соединений к центральному сдвоенному узлу существовать не должно, поскольку, если IPv4-пакеты будут вводиться в этот центральный узел, они могут быть переданы в узел только-OSI и отброшены.

III.3.2 Поступление IP трафика в SDH сеть со встроенными средствами поддержки или из нее

III.3.2.1 Межсетевой элемент (шлюз) NE, способный к работе с IP-пакетами

И IP-пакеты, и CLNP-пакеты должны располагать возможностью войти в сдвоенную зону и покинуть ее независимо от того, используется ли автоматическая инкапсуляция. Как правило, трафик поступает в IS-IS зону или покидает ее через маршрутизаторы Уровня-1, Уровня-2. Эти маршрутизаторы работают как в зоне Уровня-1, так и в субдомене Уровня-2.

В этом случае самым простым способом построения такой схемы является обеспечение положения, при котором любые маршрутизаторы Уровня-1, Уровня-2 будут сдвоенными, как представлено на рисунке III.8.

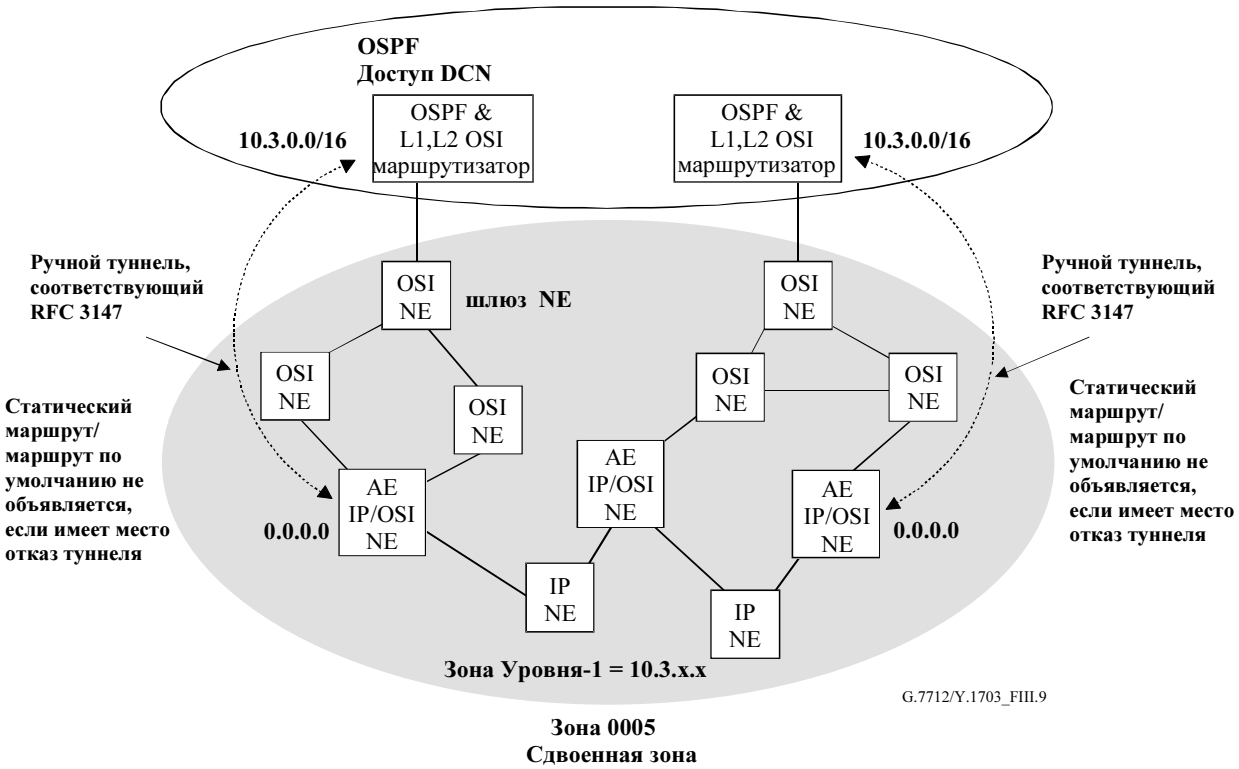


AE автоматическая инкапсуляция

Рисунок III.8/G.7712/Y.1703 – Сдвоенный шлюз

III.3.2.2 Шлюз NE, способный к работе по принципу только-OSI

В некоторых случаях узлы с автоматической инкапсуляцией будут применяться для модификации существующей зоны только-OSI, чтобы преобразовать ее фактически в сдвоенную зону. В этом случае данные шлюзовые узлы могут оставаться узлами только-OSI. При этом сеть можно сформировать, как показано на рисунке III.9.



AE автоматическая инкапсуляция

Рисунок III.9/G.7712/Y.1703 – Шлюз, работающий по принципу "только-OSI"

В этой сети CLNP-пакеты, которые должны покинуть зону Уровня-1, продолжают передаваться в OSI-маршрутизатор Уровня-1, Уровня-2. Узлы, которые располагают ручным туннелем, ведущим из зоны Уровня-1, объявляют об этом, как о маршруте по умолчанию. Следовательно, все узлы, способные работать по IP-протоколу, будут вносить добавление к записи внизу своих таблиц маршрутизации, вынуждая их к передаче всех IPv4-пакетов в один из узлов, который располагает ручным туннелем, если они не имеют какого-либо более конкретного маршрута. Таким образом, IPv4-пакет никогда не будет передан в узел Уровня-1, Уровня-2, а всегда будет передаваться через один из этих ручных туннелей.

Маршрутизатор в сети DCN доступа, которая заканчивается ручным туннелем, не нужен для прохождения Integrated IS-IS. Он будет работать с любым IP-протоколом маршрутизации, которые захочет применить оператор. Таким образом, действующая сеть, которая пользуется протоколом OSPF и IS-IS Уровня-2 в сети DCN доступа и IS-IS Уровня-1 в элементах SDH NE, может иметь зоны Уровня-1, модифицированные в сдвоенные зоны с незначительным влиянием на действующие элементы SDH NE только с OSI или на сеть DCN доступа.

Добавление IV

Иллюстрация примеров пакетного режима с защитой 1+1

IV.1 Общее описание пакетного режима с защитой 1+1

Защита 1+1 в пакетном режиме обеспечивает услугу защиты пакетного уровня, в некотором отношении аналогичную услуге защиты на уровне традиционного соединения, однако с некоторыми весьма важными различиями. Защита 1+1 пакетного уровня позволяет выполнять выбор входящих пакетов из любого соединения, независимо от соединения, из которого был выбран последний пакет. Таким образом, пакетный режим защиты 1+1 рассматривает оба эти соединения в качестве рабочих, в отличие от обозначения одного соединения в качестве работающего, а другого – в качестве защитного. В последнем случае выборка пакетов из работающего соединения производится до тех пор, пока отказ, возникший в этом рабочем соединении, не заставит осуществить переключение на защитное соединение. В отличие от этого случая, защита 1+1 в пакетном режиме не требует точного установления факта отказа и выполнения защитного переключения. Это дает возможность схеме

защиты 1+1 пакетного уровня немедленно и прозрачно устранять любой отказ. Аналогично защите 1+1 на уровне соединения, должны быть известны только краевые (концевые) узлы услуги, что позволяет существенно облегчить возможность взаимодействия.

Чтобы обеспечить службу защиты 1+1 в пакетном режиме между двумя краевыми узлами сети, ориентированной на соединения, вдоль непересекающихся путей организуется пара соединений. Пакеты от блок-схемы прикладной программы, предписанные к этой службе, должны выступать в качестве спаренных во входном узле на эти два соединения. В простейшем случае непересекающиеся пути могут рассматриваться как непересекающиеся линия или узел, но, как правило, могут потребовать более усложненного представления, например, как совместно используемые группы риска. На выходном краевом узле одна из двух копий пакетов выбирается, а затем передается на основе двух возможных принятых копий, каждая из которых пересекает (т. е. проходит) по непересекающемуся пути. В подобной ситуации любой единичный отказ в данной сети, не являющийся сам по себе ни входящим, ни выходящим узлом, может оказать серьезное воздействие на одну из копий каждого пакета. Это дает возможность рассматриваемой услуге прозрачно противостоять одному-единственномк отказу. С точки зрения времени восстановления она может характеризоваться как мгновенное устранение отказа, поскольку необходимость в обнаружении, уведомлении и переключении на защитное соединение отсутствует. Эту схему можно без каких-либо затруднений расширить для защиты от нескольких отказов посредством использования более чем двух непересекающихся путей.

IV.2 Иллюстрация защиты 1+1 в пакетном режиме

На рисунке IV.1 представлена реализация рассматриваемой услуги с использованием порядковых номеров в качестве идентификаторов. После прохождения через классификатор каждому пакету, который должен быть передан спаренными блоками LSP, присваивается свой порядковый номер исходящим краевым узлом, которому известно об этой услуге. Этот пакет со своей конкретной идентификацией затем дублируется и передается по двум непересекающимся блокам LSP. Выходящий узел должен выбрать только одну копию этого дублированного пакета. Для надлежащего выбора этого пакета только один раз пункт назначения должен располагать возможностью идентифицировать эти дублированные пакеты, в результате чего будет выбрана одна версия, но обработаны все возможные версии. Этот процесс выбора на пакетном уровне является нетривиальным, поскольку эти дублированные пакеты могут поступать неодновременно (вследствие задержки при распространении и нахождении в буферном запоминающем устройстве), и, кроме того, эти пакеты могут оказаться потерянными (вследствие ошибок при передаче и перегрузок буферного запоминающего устройства).

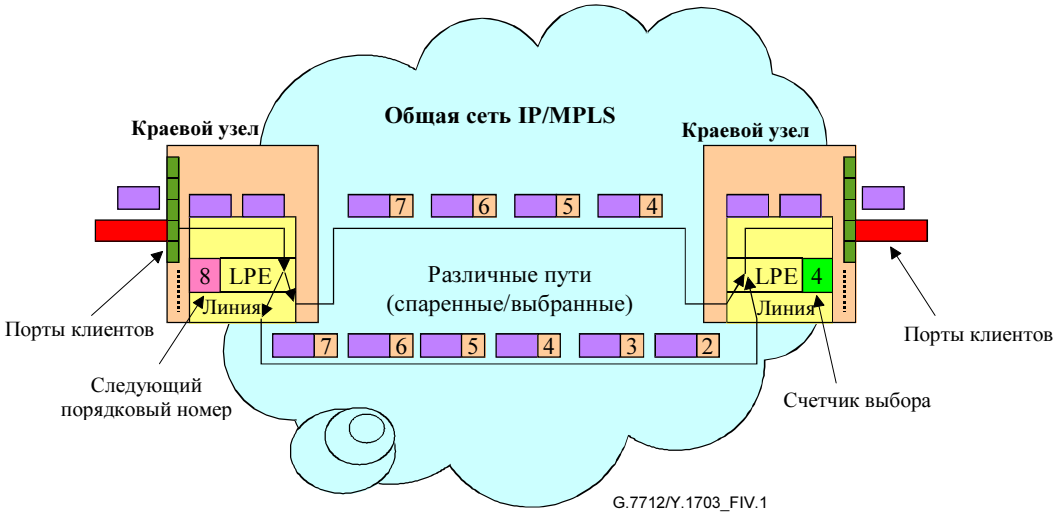


Рисунок IV.1/G.7712/Y.1703 – Схема защиты 1+1

Входной узел вводит порядковый номер, как рассматривается в параграфе 7.1.19.2. В этом случае данный пакет дублируется и транспортируется по различным пакетам LSP. Вследствие этого различия в пакетах LSP существуют ведущий (первый) пакет LSP и замыкающий (последний) пакет LSP. Ведущий пакет LSP доставляет пакеты в выходной узел быстрее, чем замыкающий пакет LSP. Поэтому в условиях отсутствия отказа выходной узел будет выбирать эти пакеты из ведущего пакета LSP. Пакеты, принятые с замыкающим пакетом LSP, будут представлять собой дублированные пакеты и, следовательно, будет отбрасываться.

Решение о принятии или отбрасывании поступившего пакета основывается на его порядковом номере и на счетчике со скользящим окном или рамкой (Sliding window) на выходящем узле. Счетчик показывает порядковый номер следующего пакета, поступление которого ожидается. Счетчик со скользящей рамкой обеспечивает рамку, где указываются допустимые к приему порядковые номера. Скользящая рамка необходима для правильного выполнения приема и отбрасывания пакетов. Если поступивший пакет попадает в эту рамку, то он считается обоснованным и может быть принят. В противном же случае этот пакет отбрасывается. По размерам рамка должна быть больше, чем максимальное количество поступивших друг за другом пакетов, которое может быть потеряно рабочим (находящимся под напряжением) блоком LSP.

Скользящая рамка используется для решения проблемы потери пакетов в ведущем пакете LSP, когда порядковый номер этого пакета оказывается очень близко от точки циклического возврата. На рисунке IV.2 представлен ведущий пакет LSP (LSP 1), который переносит пакет с порядковым номером 29. Этот пакет принимается, а показание счетчика увеличивается до 30. Если допустить, что потеряны 2 последовательно переданных пакета (т. е. пакеты с порядковыми номерами 30 и 31), то следующий поступивший пакет будет иметь в пакете LSP 1 порядковый номер 0. Без использования скользящей рамки выходящий узел отбросит этот пакет, поскольку $0 < 30$. Использование скользящей рамки, превышающей максимальное количество последовательных пакетов, которое рабочий (находящийся под напряжением) пакет LSP может потерять, как раз и может служит решением рассматриваемой проблемы. Если, например, максимальное количество последовательных пакетов, которое может потерять рабочий пакет LSP, составляет 5, то можно сделать расчет скользящей рамки на 6. Однако исходя из вышеприведенного примера, теперь посредством использования скользящей рамки выходной узел будет принимать пакеты в диапазоне значений {30, 31, 0, 1, 2, 3, 4}. Следовательно, даже если потеряются 5 пакетов (т. е. максимальное количество последовательных пакетов, которое может быть потеряно в рабочем пакете LSP), то следующий поступивший пакет будет иметь порядковый номер 3, благодаря чему этот пакет и будет принят.

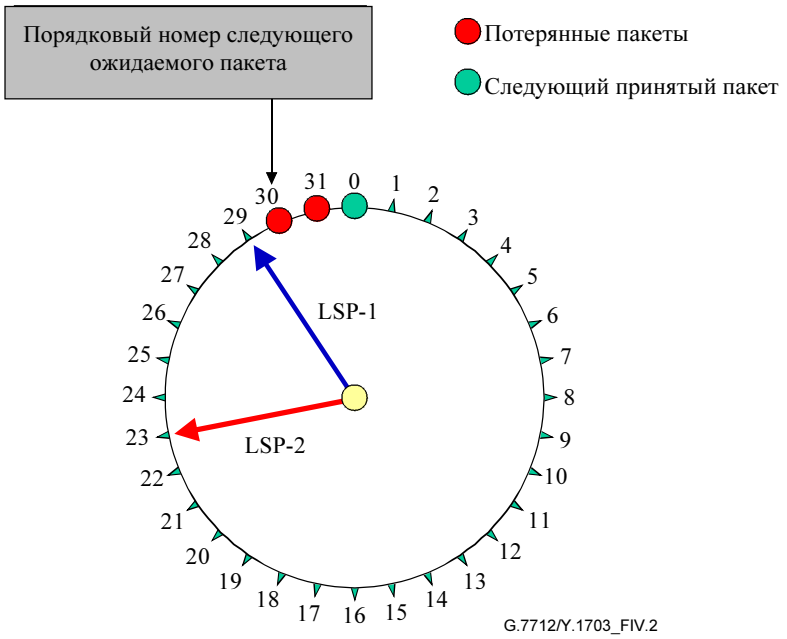


Рисунок IV.2/G.7712/Y.1703 – Механизм работы скользящей рамки

Необходимо отметить, что эта идея скользящей рамки работает только в случае, если выход за пределы пакета LSP не позволяет вернуть его обратно в пределы скользящей рамки. Если пакет с порядковым номером в пределах скользящей рамки принят за пределами пакета LSP, то он окажется принятым по ошибке. При подобной ситуации может быть принят только пакет с порядковым номером в пределах скользящей рамки, если он возвращается в исходный режим более чем на (2^N – размер скользящей рамки). Вследствие этого количество битов "N", применяемое для порядкового номера, должно соответствовать следующему равенству:

$$2^N > \text{скользящая рамка} + \text{рамка задержки},$$

где

скользящая рамка > максимального количества последовательных пакетов, которое может быть потеряно в пакете LSP,

а также

рамка задержки = максимальному количеству пакетов, на которое замыкающий пакет LSP может отставать от ведущего пакета LSP.

Необходимо отметить, что в параграфе 7.1.19.2 рассматривается 4-байтовое поле для размещения порядкового номера. Такое 4-байтовое поле обеспечивает последовательность более чем 4 миллиардов номеров, которая достаточно велика, чтобы вместить наихудший случай, связанный с потерями последовательных пакетов и дифференциальными уравнениями с запаздывающими аргументами.

Одним из целесообразных методов расчета размеров скользящей рамки и рамки задержки является уравнивание размеров этих рамок. (Необходимо отметить, что предполагается, что размер рамки задержки, как правило, превышает размер скользящей рамки.) Благодаря этому гарантируется выбор пакетов из ведущего пакета LSP во всех алгоритмах после устранения отказа в пакете LSP. Этот вопрос будет более подробно обсуждаться в следующем параграфе, где рассматриваются различные алгоритмы отказа.

IV.3 Работа алгоритма константы выбора при различных алгоритмах отказа

Один из методов, представленных для обсуждения работы алгоритма константы выбора, можно изобразить в виде часов с интервалами 2^N. На рисунке IV.3 в качестве примера рассматривается случай, где N = 4 (т. е. порядковый номер из 4 битов) и, следовательно, диапазон для порядковых номеров будет составлять от 0 до 15.

В приводимом примере скользящая рамка устанавливается равной рамке задержки, величина которой будет равна 5.

На рисунке IV.3 представлен ведущий пакет LSP впереди замыкающего пакета LSP на 3 порядковых номера. Ведущий пакет LSP доставляет пакет с порядковым номером = 1, после чего счетчик устанавливается на 2.

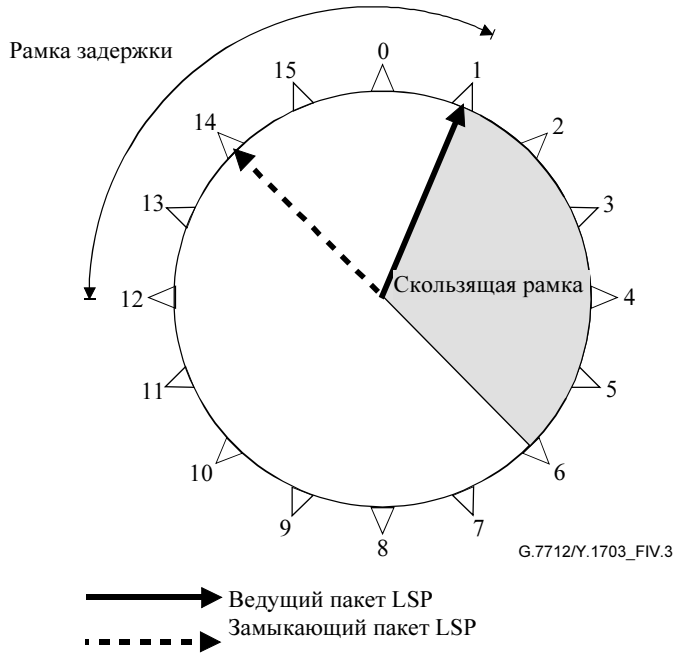


Рисунок IV.3/G.7712/Y.1703 – Работа алгоритма константы выбора

На рисунке IV.4 показано, что до приема пакета с порядковым номером 2 в ведущем пакете LSP этот последний нарушается. До тех пор пока пакет с порядковым номером 2 не будет доставлен из замыкающего пакета LSP, узел выхода не будет осуществлять выбор никаких пакетов, в результате чего счетчик останется на показании 2.

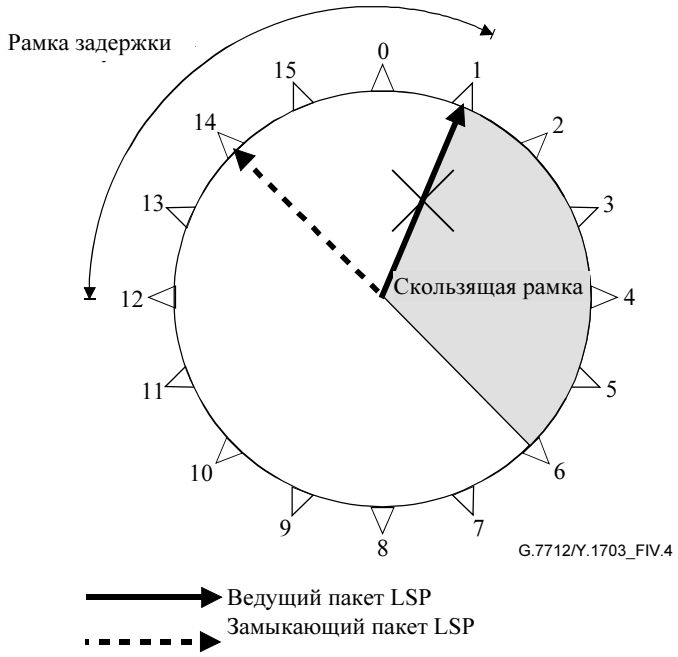


Рисунок IV.4/G.7712/Y.1703 – Отказ ведущего пакета LSP

На рисунке IV.5 показано, что когда пакет с порядковым номером 2 принят в замыкающем пакете LSP, узел выхода увеличивает показание счетчика до 3, а скользящая рамка смещается таким образом, что может быть принят пакет с порядковым номером в диапазоне от 3 до 7.

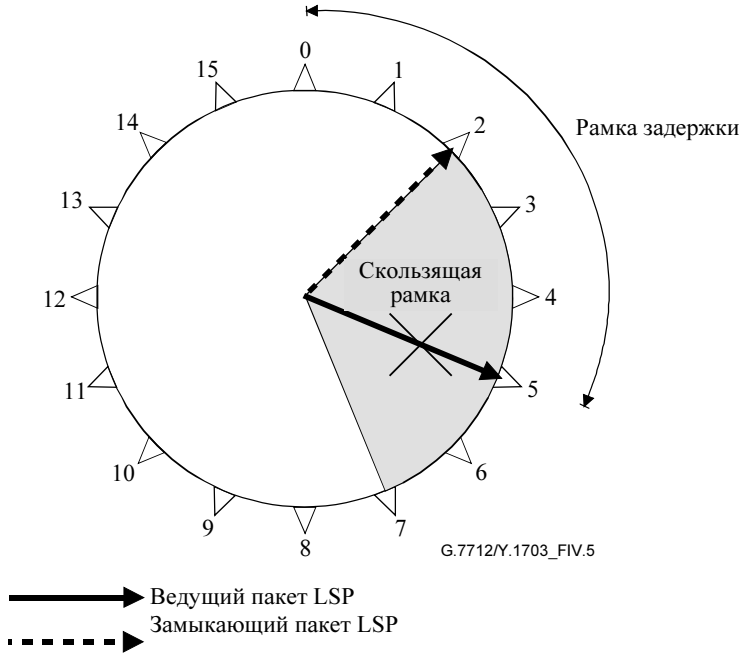


Рисунок IV.5/G.7712/Y.1703 – Прием пакета в замыкающем пакете LSP

На рисунке IV.6 показано, что до приема пакета с порядковым номером 3 из замыкающего пакета LSP ведущий пакет LSP восстанавливается и от этого последнего принимается пакет с порядковым номером 6. Поскольку цифра 6 попадает в диапазон скользящей рамки, этот пакет принимается. Следует отметить, что крайне важно, чтобы в течение всего времени работы ведущего пакета LSP из него поступали пакеты. Следовательно, чтобы обеспечить положение, при котором после восстановления ведущего пакета LSP он будет доставлять пакет, значение порядкового номера

которого находится в пределах диапазона скользящей рамки, эта скользящая рамка должна быть равной или превышать рамку задержки; в качестве примера на рисунке приведен именно этот случай.

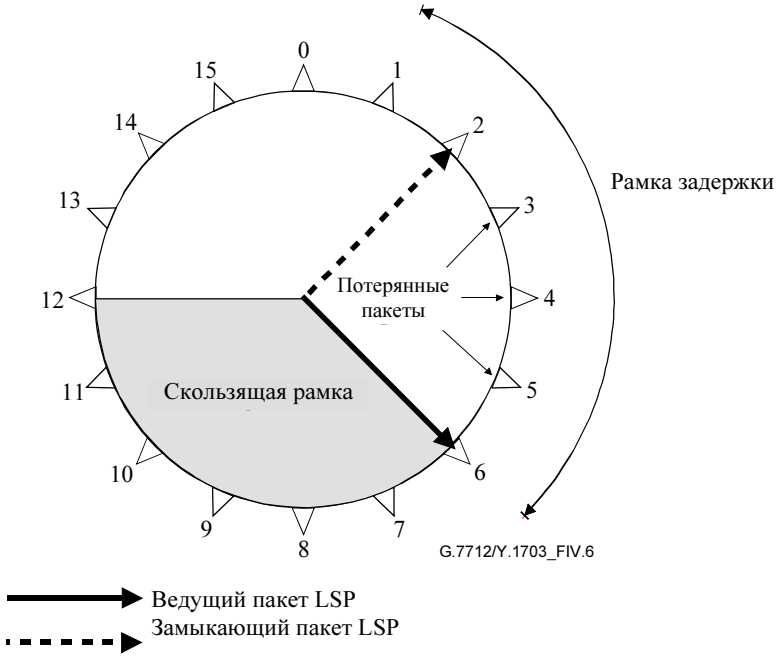


Рисунок IV.6/G.7712/Y.1703 – Ведущий пакет LSP восстановлен

На рисунках IV.7, IV.8 и IV.9 показано, каким образом складывается ситуация, если скользящая рамка устанавливается на размер меньше, чем рамка задержки. В этом случае вполне возможно, что когда ведущий пакет LSP окажется восстановленным, он доставляет пакеты с порядковыми номерами, выходящими за пределы скользящей рамки, и, следовательно, выходной узел продолжает принимать пакеты от замыкающего пакета LSP. Если позже замыкающий протокол LSP откажет, то существует возможность потерять большое количество пакетов (наихудший случай будет $2^N - size\_of\_sliding\_window$, где N – это количество битов, применяемое в качестве порядкового номера).

На рисунке IV.7 приводится пример, когда скользящая рамка устанавливается на 3, тогда как рамка задержки может быть установлена на любое число до 7. В этом примере замыкающий пакет LSP отстает от ведущего протокола LSP на 4 порядковых номера. Поскольку ведущий пакет LSP отказывает, необходимые пакеты выбираются из замыкающего пакета LSP.

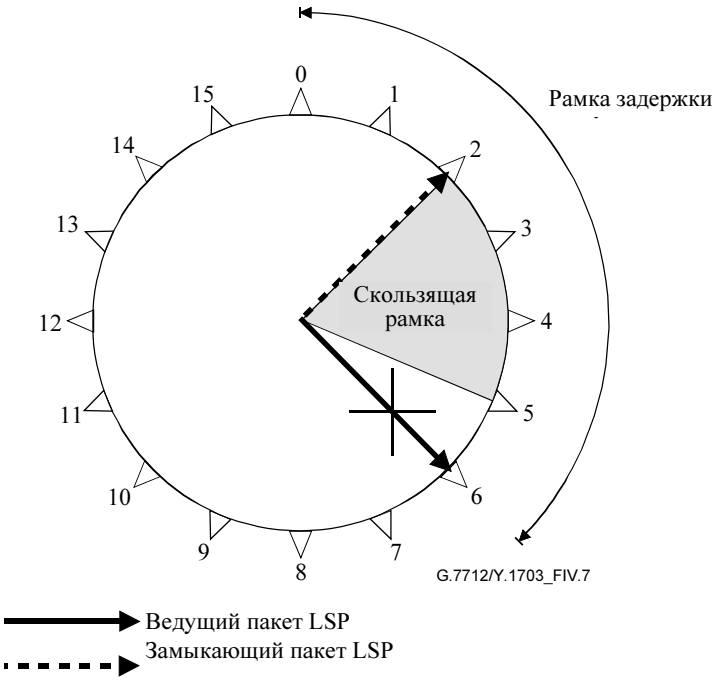


Рисунок IV.7/G.7712/Y.1703 – Скользящая рамка слишком мала: пакеты, выбранные из замыкающего пакета LSP

На рисунке IV.8 представлено, что в то время, когда ведущий пакет LSP находится в восстановленном состоянии, он доставляет пакет с порядковым номером, равным 7, который находится за пределами скользящей рамки и, следовательно, отбрасывается. Выборка пакетов продолжается из замыкающего пакета LSP.

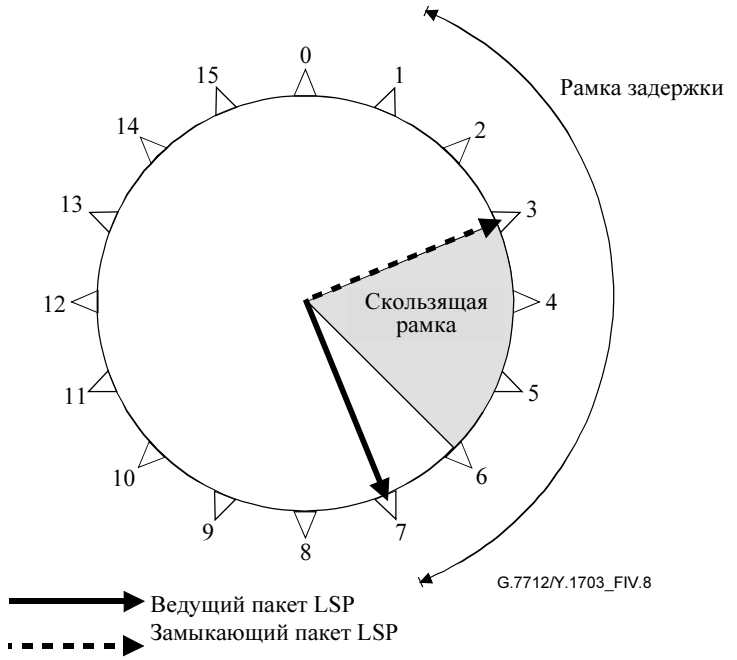


Рисунок IV.8/G.7712/Y.1703 – Скользящая рамка слишком мала: отбрасывание пакетов, доставленных восстановленным ведущим пакетом LSP

На рисунке IV.9 представлен отказ для замыкающего пакета LSP. Поскольку ведущий пакет LSP доставляет пакеты вне скользящей рамки и, следовательно, эти пакеты отбрасываются, выходящий узел не начнет принимать пакеты до тех пор, пока ведущий пакет LSP не пройдет весь путь, имеющий вид круга, и не начнет доставлять пакеты с порядковыми номерами, которые попадают в пределы скользящей рамки. Это может привести к потере значительного количества пакетов. Следовательно, чтобы воспрепятствовать этой ситуации, рекомендуется, чтобы этот тип алгоритма константы выбора был установлен в скользящей рамке, равной рамке задержки.

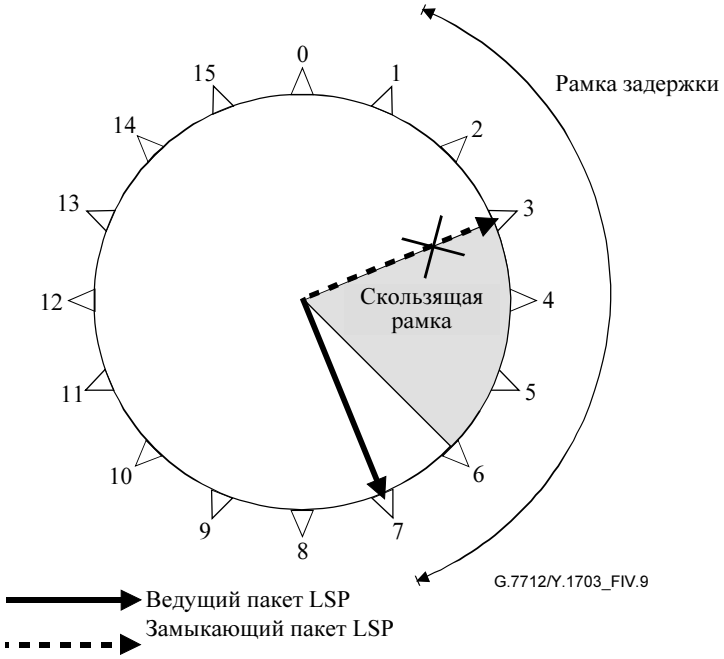


Рисунок IV.9/G.7712/Y.1703 – Скользящая рамка слишком мала: влияние отказа на замыкающий пакет LSP

Добавление V

Литература

– IETF RFC 1006 (1997), *ISO Transport Service on top of the TCP Version 3*.

– IETF RFC 2966 (2000), *Domain-wide Prefix Distribution with Two-Level IS-IS.*

– IETF RFC 3147 (2001), *Generic Routing Encapsulation of CLNS Networks*.

– IETF RFC 3373 (2002), *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*.

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА И АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP)

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 обозначение	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Показатели качества	Y.800–Y.899
АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА (IP)	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, сетевые возможности и управление ресурсом	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 оплаты	Y.1800–Y.1899

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

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 принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	**Системы и среда передачи, цифровые системы и сети**
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
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 и взаимосвязь открытых систем
Серия Y	**Глобальная информационная инфраструктура и аспекты межсетевого протокола (IP)**
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2004 г.