

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНАЦИЙ
им. проф. М.А. БОНЧ-БРУЕВИЧА

Н. А. Апостолова, Б. С. Гольдштейн, В. Б. Кадыков

УНИВЕРСАЛЬНЫЙ ИНТЕРФЕЙС V5 СЕТИ АБОНЕНТСКОГО ДОСТУПА

Учебное пособие

по курсу

«СЕТИ АБОНЕНТСКОГО ДОСТУПА»

Рекомендовано Учебно-методическим объединением по образованию в области информатизации и связи в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности 200900 – Сети связи и системы коммутации и смежным специальностям

Санкт-Петербург
2005

Содержание

| | |
|---|-----------|
| Занятие 1 Общие принципы построения интерфейса V5 | 4 |
| 1.1 Введение | 4 |
| 1.2 Сетевые аспекты | 4 |
| 1.3 Опорная точка V | 5 |
| 1.4 Функциональное описание V5 | 6 |
| 1.5 Архитектура интерфейса | 7 |
| 1.5.1 Протоколы | 7 |
| 1.5.2 Типы данных, передаваемых через интерфейс V5 | 9 |
| 1.5.3 С-пути и С-каналы | 9 |
| 1.5.4 Канальные интервалы | 9 |
| 1.5.5 Размещение С-каналов в канальных интервалах | 9 |
| 1.5.6 Подуровни уровня 2 и мультиплексирование в С-каналах | 10 |
| 1.5.7 Связь между подуровнями уровня 2 | 10 |
| 1.5.8 Мультиплексирование на уровне 3 | 10 |
| 1.5.9 Резервирование С-каналов | 11 |
| Занятие 2 Структура кадров интерфейса V5 | 12 |
| 2.1 Структура кадров уровня 2 | 12 |
| 2.2 Формат сообщений уровня 3 | 14 |
| 2.2.1 Общее | 14 |
| 2.2.2 Дискриминатор протокола V5 | 14 |
| 2.2.3 Адрес уровня 3 | 14 |
| 2.2.4 Другие информационные элементы | 15 |
| 2.3 Способ передачи | 15 |
| Занятие 3 Протокол ТфОП (PSTN PROTOCOL) | 15 |
| 3.1 Основы протокола ТфОП | 15 |
| 3.2 Определение сигналов FE, сообщений и примитивов | 16 |
| 3.3. Состояния логических объектов протокола ТфОП | 18 |
| 3.3.1 Состояния FSM на стороне сети доступа (PSTN_AN) | 18 |
| 3.3.2 Состояния FSM на стороне АТС (PSTN_LE) | 18 |
| 3.4 Кодирование информационных элементов | 19 |
| Занятие 4 Информационные элементы сообщений протокола ТфОП | 20 |
| 4.1 Структура и кодирование информационных элементов | 20 |
| Занятие 5 Национальный мэппинг. Поточковые диаграммы | 22 |
| 5.1 Национальный мэппинг | 22 |
| 5.2 Поточковые диаграммы (Information flow diagrams) | 24 |
| Занятие 6 Протокол управления (CONTROL PROTOCOL) | 29 |
| 6.1 Основы протокола управления | 29 |
| 6.2 Спецификация сообщений | 29 |
| 6.3 Структура и кодирование информационных элементов | 30 |
| 6.4 FSM логических объектов протокола управления | 30 |
| 6.5 Семантика сообщений и процедуры | 31 |
| ЗАНЯТИЕ 7. Протокол управления трактами | 33 |
| 7.1 Общие положения | 33 |
| 7.2 События и сигналы FE, относящиеся к FSM управления трактом | 34 |
| 7.3 Спецификация сообщений протокола управления трактами | 34 |
| 7.4 FSM управления трактом | 35 |
| 7.5 FSM протокола управления трактами | 37 |
| 7.6 Таймеры протокола управления трактами | 37 |
| 7.7 Процедуры протокола управления трактами | 37 |
| Занятие 8 Протокол назначения несущих каналов (BCC PROTOCOL) | 39 |
| 8.1 Основы протокола BCC | 39 |
| 8.2 Сообщения протокола BCC | 41 |
| 8.3. Таймеры протокола BCC | 42 |
| 8.4 Описание состояний логического объекта протокола BCC | 42 |
| 8.5 Взаимодействие протоколов BCC и ТфОП/ISDN | 43 |
| Занятие 9 Протокол защиты (PROTECTION PROTOCOL) | 46 |

| | |
|---|-----------|
| 9.1 Основы протокола защиты..... | 46 |
| 9.2 Состояния логических объектов протокола защиты | 50 |
| 9.3 Спецификация сообщений протокола защиты..... | 50 |
| 9.4 Процедуры протокола защиты..... | 51 |
| Занятие 10 Тестирование протоколов интерфейса V5 | 52 |
| 10.1 Основные принципы..... | 52 |
| 10.2 Тестовые сценарии старта (категория А) интерфейса V5 | 52 |
| 10.3 Тестовые сценарии процедур управления конфигурацией (категория В)..... | 54 |
| 10.4 Тесты блокировки/разблокировки ИКМ-тракта (категория С) | 54 |
| 10.5 Тесты работы с отказами трактов (категория D) | 55 |
| 10.6 Тесты национального мэппинга ТфОП (категория E) | 55 |
| 10.7 Тесты доступа ISDN | 56 |
| 10.8 Услуги (категория G) | 57 |
| 10.9 Тесты стабильности (категория H)..... | 57 |
| 10.10 Протокол-тестеры SNT-7531 или SNT <i>lite</i> | 58 |
| Занятие 11 Преобразование протоколов интерфейса V5..... | 59 |
| 11.1 Вызов со стороны PRI E-DSS1 к стороне LE | 60 |
| 11.2 Вызов со стороны LE V5 к стороне PRI E-DSS1 | 61 |
| 11.3 Конвертер VSM..... | 61 |

Занятие 1 Общие принципы построения интерфейса V5

1.1 Введение

В недавнем прошлом интерфейсы между выносными абонентскими концентраторами и оборудованием АТС не подлежали стандартизации. Практически во всех установленных до недавнего времени цифровых АТС для этих интерфейсов на физическом уровне использовались цифровые тракты 2048 кбит/с, а на логическом - собственные «внутрифирменные» протоколы. Очевидным недостатком такого подхода является ограничение свободы выбора у операторов при установке дополнительного абонентского оборудования.

В последнее время существенно расширилась номенклатура оборудования абонентского доступа, широко распространяется оборудование беспроводного абонентского доступа WLL (Wireless Local Loop), подключаемое по оптическим линиям связи абонентское оборудование и т.п. В связи с этим возросла потребность в таком интерфейсе, который позволил бы совмещать в одной сети оборудование разных производителей, реализующее различные типы доступа: аналоговые абонентские линии, базовый и первичный доступ ISDN, цифровые абонентские линии DSL (Digital Subscriber Line). Именно для этих целей и был создан универсальный интерфейс V5, ориентированный на обслуживание трех источников сети доступа, соответствующих трем видам предоставляемых пользователям услуг связи:

- *передача речи* (телефонная связь, аудиоинформация, справочные услуги, речевая почта);
 - *передача данных* (электронная почта, Интернет, факсимильные сообщения, электронные платежи);
 - *передача видеoinформации* (видео по запросу, телеконференции),
- и взаимодействующий с тремя составными частями сети доступа:
- *металлический кабель* (*витая пара, коаксиальный кабель и др.*);
 - *волоконно-оптический кабель*;
 - *беспроводные средства* (WLL – Wireless Local Loop).

1.2 Сетевые аспекты

В качестве примера рассмотрим включение отечественных мультисервисных абонентских концентраторов МАК разработки НТЦ Протей, установленного в качестве лабораторной установки на кафедре СКИРИ СПбГУТ им.М.А.Бонч-Бруевича. Применение МАК в сельских и городских телефонных сетях традиционных операторов ТфОП с подключением его к опорным цифровым АТС через стандартный интерфейс V5.2 позволит снизить затраты на абонентскую кабельную сеть за счет концентрации абонентской нагрузки. В мультисервисных сетях следующего поколения подключение МАК к Softswitch выполняется по протоколу MGCP, рассмотрение которого выходит за рамки данного пособия.

Оборудование МАК работает с терминалами следующих типов:

- аналоговые телефонные аппараты, а также аппараты факсимильной связи и модемы;
- цифровые телефонные аппараты ISDN;
- интегрированные устройства доступа на основе технологии SHDSL, предусматривающие предоставление услуг как симметричной высокоскоростной передачи данных (до 2 Мбит/с), так и телефонии (VoDSL); электропитание таких устройств может быть дистанционным, что обеспечивает более высокую надежность;
- абонентские терминалы стандарта DECT.

Основной вариант включения МАК представлен на рис.1.1. Через интерфейс V5.2 концентратор подключается к опорной АТС, а с абонентской стороны в каждую кассету включается до 570 аналоговых абонентских линий, т.е. в одном стативе можно разместить оборудование, допускающее включение до 3420 таких линий. Другой вариант организации связи с помощью МАК иллюстрирует рис.1.2. Как и в первом варианте, через интерфейс V5.2 концентратор подключается к опорной АТС, а с другой его стороны, через интерфейс SHDSL, подключаются интегрированные абонентские устройства IAD, в которые, в свою очередь, могут включаться телефоны и другие аналоговые устройства, а также и персональные компьютеры. Последний вариант включения представлен на рис.1.3 и демонстрирует полный спектр возможностей МАК. Кроме названных ранее, показана возможность подключения концентратора к Softswitch по протоколу MGCP. При этом услуги телефонии для абонентских терминалов всех типов предоставляются, независимо от технологии доступа, с использованием единого плана нумерации.

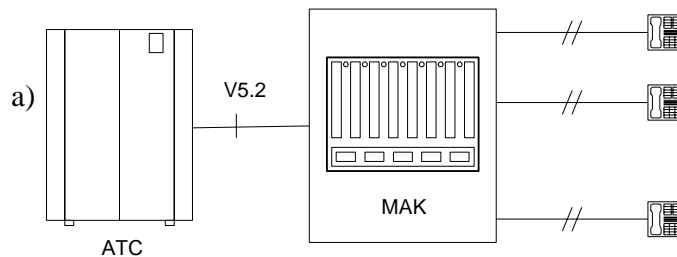


Рисунок 1.1 – Включение аналоговых абонентских линий в концентратор с V5

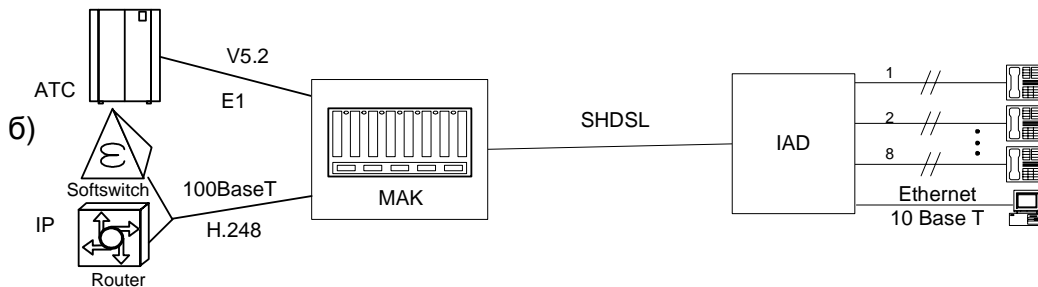


Рисунок 1.2 – Включение IAD в концентратор с V5

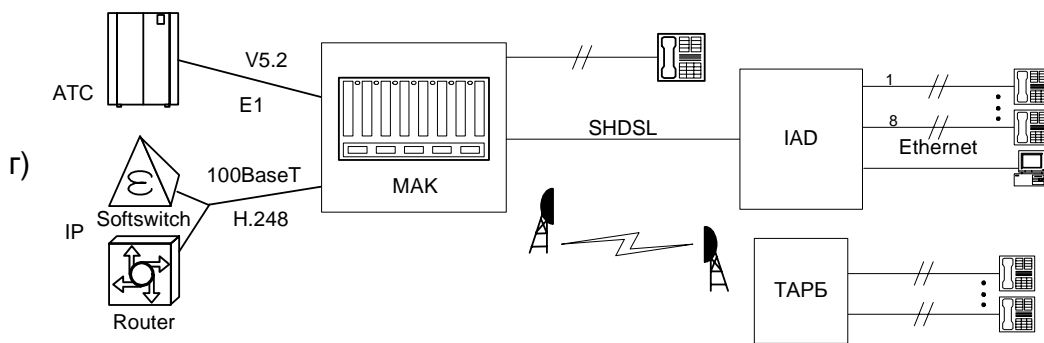


Рисунок 1.3 – Универсальный вариант включения MAK

1.3 Опорная точка V

Местоположение интерфейса сети доступа определено в опорной точке V, в которой рекомендацией ITU-T Q.512 определено пять вариантов интерфейса (рис.1). Интерфейс V1 предназначен для подключения к АТС пользователей ISDN с базовым доступом 2B+D, а интерфейсы V2, V3, V4 и V5 на физическом уровне представляют собой стандартные цифровые тракты 2048 Кбит/с.

Разработка спецификаций для интерфейса V5 была выполнена в девяностых годах Европейским институтом стандартизации ETSI. Национальные особенности в спецификациях интерфейса V5 определялись для каждой страны в отдельности, включая и российские национальные спецификации, описываемые отраслевыми стандартами ОСТ45.157-99 - "Сопряжение цифровой автоматической станции и сети доступа по интерфейсу V5. Сигнализация. Правила формализации информации" и ОСТ45.154-2001 - "Сопряжение цифровой автоматической станции и сети доступа по интерфейсу V5. Спецификация протокола передачи телефонной сигнализации".

Интерфейс V5.1 позволяет подключить оборудование сети доступа к АТС по цифровому тракту 2048 кбит/с. Это обеспечивает подключение (без концентрации нагрузки) до 30 аналоговых абонентских линий или до 15 линий ISDN с базовым доступом. Информация сигнализации передается по 16-му каналному интервалу (КИ16).

Интерфейс V5.2 ориентирован на группу до 16 трактов 2048 кбит/с и поддерживает концентрацию нагрузки. В каждом тракте предусмотрено несколько каналов сигнализации (КИ16, КИ15, КИ31).

Таким образом, один интерфейс V5.1 может поддерживать до 30 портов ТфОП (или до 15 портов базового доступа ISDN), а один интерфейс V5.2 может поддерживать (в зависимости от коэффициента концентрации) до двух тысяч портов ТфОП или до тысячи портов базового доступа ISDN.

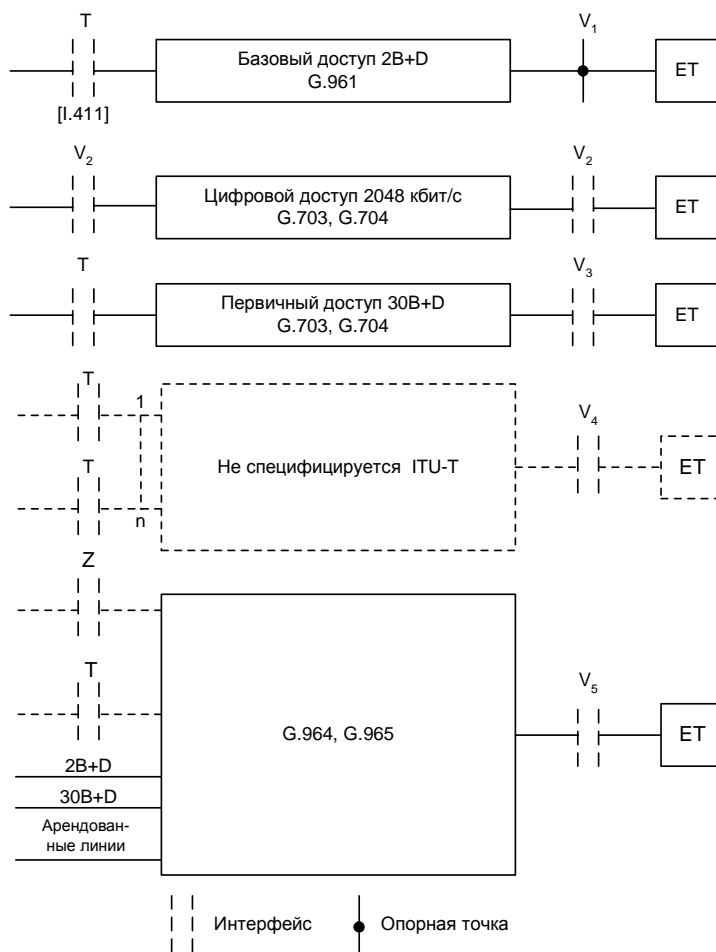


Рисунок 1.5 – Возможные варианты доступа в точке V

1.4 Функциональное описание V5

Итак, спецификации ETSI и Рекомендации ИТУ-Т определяют две разновидности интерфейса V5, различающиеся способами использования цифровых каналов, - это V5.1 и V5.2.

Интерфейс V5.1 содержит только один тракт ИКМ 2048 кбит/с. Кроме протокола, поддерживающего телефонную сигнализацию (протокола ТфОП) предусмотрен и протокол, обеспечивающий передачу между сетью доступа и станцией управляющей информации. С помощью этого протокола, в частности, занимаются и освобождаются порты ISDN с базовым доступом (BRA), а также производится их блокировка. Интерфейс V5.1 позволяет предоставлять услуги для клиентов сети в режиме по требованию (on-demand), а также, в режиме полупостоянной линии (Semi-permanent).

Интерфейс V5.2 предусматривает возможность концентрации абонентской нагрузки и имеет протокол назначения несущих каналов для портов, находящихся в активном состоянии. Интерфейс V5.2 может содержать от 1 до 16 трактов ИКМ со скоростью передачи 2048 кбит/с. Это позволяет кроме портов ISDN с BRA включать и порты ISDN с первичным доступом (PRA). Спецификации, касающиеся протокола поддержки телефонной сигнализации и протокола управления, не

отличаются от таковых для V5.1. Для обеспечения высокой надежности передачи сигнальных данных используется протокол защиты, а надежности при выходе из строя цифрового тракта – протокол управления трактами, включающий резервные тракты. Функциональная модель доступа через интерфейс V5.2 иллюстрируется на рисунке 1.2.

Оконечное оборудование абонента должно включаться в оборудование сети доступа, которое обеспечивает сигнальное взаимодействие с ответной частью оборудования, установленного на цифровой АТС, по каналам, организованным в КИ16, КИ15 или еще КИ31 ИКМ-трактов интерфейса V5.2.

Электрические параметры каждого ИКМ-тракта интерфейса V5 должны соответствовать рекомендациям ИТУ-Т G.703, G.704 и стандарту ETS 300 166.

В спецификациях определены следующие функции, которые должны быть реализованы в оборудовании интерфейса:

- *функции несущих (информационных) каналов*, обеспечивающие двухсторонний перенос через интерфейс информации В-каналов пользовательских портов ISDN или цифровых каналов 64 кбит/с портов пользователей ТфОП;
- *функции поддержки D-каналов ISDN*, обеспечивающие двухсторонний перенос через интерфейс информации D-каналов пользовательских портов ISDN (сигнальной информации, данных, передаваемых в пакетном режиме, и данных, передаваемых в режиме трансляции кадров);
- *функции поддержки сигнализации ТфОП*, обеспечивающие двухсторонний перенос через интерфейс сигнальной информации портов телефонной сети общего пользования;
- *функции управления пользовательскими портами*, обеспечивающие двухсторонний перенос через интерфейс контрольной и управляющей информации, которая связана с блокировкой и разблокировкой отдельных пользовательских портов ТфОП и ISDN, а также с рядом задач, специфических для портов ISDN (активизацией/деактивизацией доступа, индикацией ошибок, контролем рабочих характеристик, управлением потоком сигнальной информации);
- *функции общего управления*, обеспечивающие управление реконфигурацией интерфейса, временную блокировку D-каналов отдельных портов ISDN в условиях перегрузки, рестарт протокола ТфОП и проверку согласованности обеих сторон интерфейса;
- *функции управления трактами 2048 кбит/с* (только в интерфейсе V5.2), обеспечивающие проверку исправности трактов и соответствия их идентификаторов на разных сторонах интерфейса, блокировку/разблокировку трактов, а также цикловую и сверхцикловую синхронизацию;
- *функции управления звеньями уровня 2*, обеспечивающими надежный двухсторонний перенос информации разных протоколов;
- *функции защиты служебной информации* (только в интерфейсе V5.2), обеспечивающие переключение логических каналов сигнализации и управления на резервные физические каналы интерфейса при отказах ИКМ-трактов, а также контроль ошибок протокола и перезапуск средств нумерации сообщений;
- *функции назначения несущих каналов* (только в интерфейсе V5.2), обеспечивающие создание и разрушение физических соединений между пользовательскими портами сети доступа и несущими каналами интерфейса;
- *функции тактирования*, предоставляющие необходимую тактовую информацию для передачи битов, идентификации байтов и цикловой синхронизации.

1.5 Архитектура интерфейса

1.5.1 Протоколы

В интерфейсе V5 действуют различные протоколы, принадлежащие уровням 1, 2 и 3 семиуровневой модели OSI. На уровне 3 действуют следующие протоколы сетевого уровня:

- протокол поддержки телефонной сигнализации (протокол ТфОП);
- служебный протокол управления, реализующий функции управления пользовательскими портами (Port control) и функции общего управления (Common control);
- протокол назначения несущих каналов (BCC – Bearer Channel Connection);
- протокол управления трактами интерфейса (Link Control Protocol);
- протокол защиты (Protection Protocol).

Протокол ТфОП и протокол управления действуют в обоих интерфейсах V5.1 и V5.2, а

остальные протоколы – только в интерфейсе V5.2. На рисунке 1.7 представлена архитектура протоколов интерфейса V5.2.

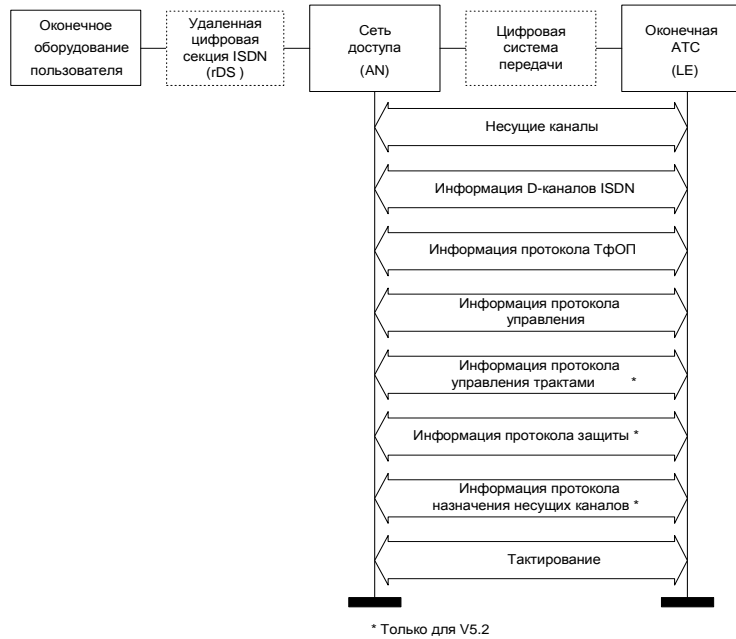
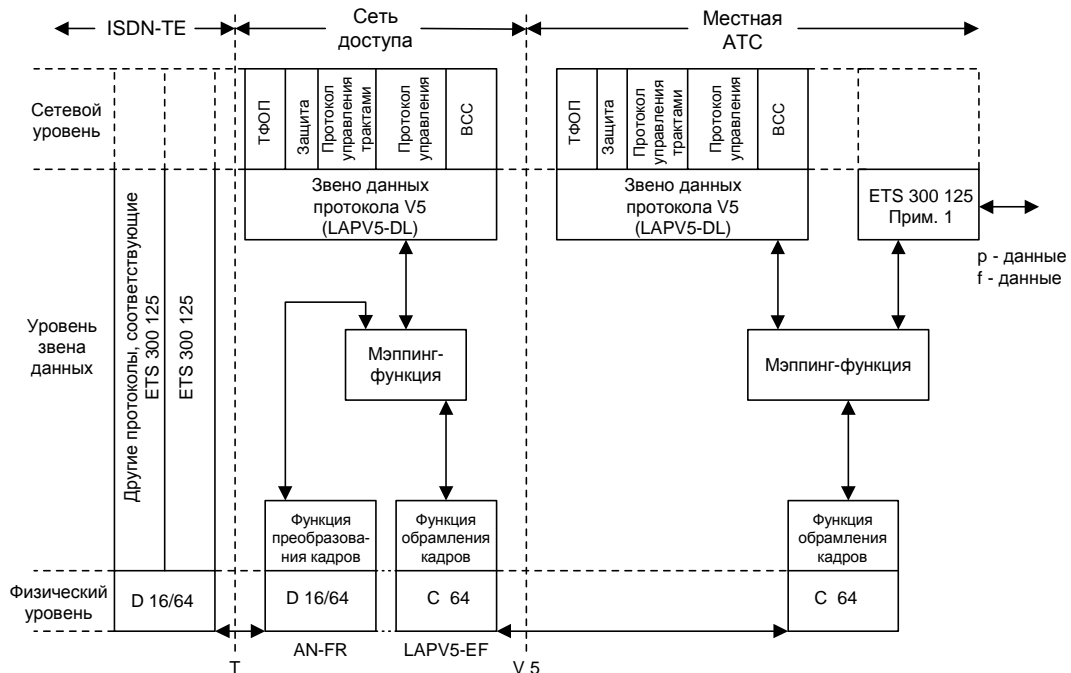


Рисунок 1.6 – Функциональная модель доступа через интерфейс V5.2



Примечания

1. Исключения составляют функции, оканчивающиеся в блоке “Функции преобразования кадров” стороны СД.
2. “Защита” – означает протокол защиты.
3. РНК – Протокол размещения несущих каналов.

Рисунок 1.7 - Архитектура протоколов интерфейса V5

Алгоритм функционирования любого протокола реализуется его логическим объектом, поведение которого описывается в терминах конечных автоматов. В данном контексте конечный автомат (Finite State Machine, FSM) – это система с конечным числом входных сигналов (событий), выходных сигналов (событий), состояний и с дискретным временем, в которой переход из одного состояния в другое может происходить только под воздействием входного сигнала. Этой моделью поведения описываются все логические объекты интерфейса V5.

1.5.2 Типы данных, передаваемых через интерфейс V5

Работа каждого из перечисленных протоколов сопровождается переносом через интерфейс V5 данных, типы которых перечислены ниже. Через интерфейс V5.2 проходят данные:

- р-типа - данные D-канала ISDN с SAPI=16 (коммутация пакетов) ;
- f-типа - данные D-канала ISDN с SAPI= 32-64 (трансляция кадров FR);
- Ds-типа - сигнальная информация D-канала ISDN (SAPI не равен ни одному из приведенных выше);
- сигнальная информация ТфОП;
- информация служебного протокола управления;
- информация служебного протокола управления трактами;
- информация служебного протокола назначения несущих каналов;
- информация служебного протокола защиты.

1.5.3 С-пути и С-каналы

Ресурс, выделяемый в интерфейсе V5 для передачи данных одного типа, называется С-путем. Группа из одного или нескольких С-путей разных типов, среди которых отсутствует С-путь для передачи информации протокола защиты, составляет логический С-канал. Канал 64 кбит/с в ИКМ-тракте интерфейса V5, предназначенный для передачи данных логического С-канала, называется физическим С-каналом.

С-пути для передачи информации протоколов управления, ВСС, управления ИКМ-трактами и защиты изначально всегда должны размещаться в КИ16 так называемого Первичного тракта интерфейса V5.2. С-пути для передачи данных р-, f- и Ds-типа могут размещаться в одном логическом С-канале или разделяться для передачи по разным логическим С-каналам.

Данные протокола ТфОП могут содержаться только в одном логическом С-канале.

Данные р-, f- или Ds-типа одного любого пользовательского порта ISDN не могут размещаться в разных логических С-каналах.

1.5.4 Канальные интервалы

В интерфейсе V5.1 имеется только один ИКМ-тракт, канальные интервалы (КИ) которого - КИ16, КИ15 и КИ31 используются для передачи данных протокола управления, данных телефонной (ТфОП) и ISDN (D-канал) сигнализации. Остальные КИ используются как несущие каналы портов ТфОП и ISDN.

В интерфейсе V5.2 может присутствовать до 16 ИКМ-трактов. Канальные интервалы КИ16, КИ15 и КИ31 каждого из ИКМ-трактов могут использоваться для передачи сигнальных данных и данных служебных протоколов. Если после размещения этой информации некоторые из названных КИ остаются не занятыми, они могут использоваться как несущие каналы.

1.5.5 Размещение С-каналов в канальных интервалах

Канальные интервалы КИ16, КИ15 и КИ31 каждого ИКМ-тракта 2048 кбит/с могут использоваться как физические С-каналы. В интерфейсе V5.1 эти КИ используются в приведенной выше последовательности. Информация протокола управления всегда размещается в КИ16.

Если интерфейс V5.2 содержит всего один тракт 2048 кбит/с, размещение С-путей в КИ должно совпадать с размещением, принятым для интерфейса V5.1; это необходимо, чтобы обеспечить совместимость V5.2 с V5.1. Если в интерфейсе имеется более одного тракта, необходимо использовать протокол защиты.

В этом случае КИ16 Первичного тракта должен использоваться для передачи информации протокола защиты и для организации С-путей, которые планировались для протокола управления, ВСС и протокола управления трактом. В КИ16 Вторичного тракта также должна передаваться информация протокола защиты.

Если возникает необходимость иметь дополнительные КИ, они должны выбираться в такой последовательности:

- КИ16 каждого из оставшихся трактов 2048 кбит/с; если этого недостаточно, то
- КИ15 Первичного ИКМ-тракта; если этого недостаточно, то
- КИ31 того же ИКМ-тракта; а если и этого недостаточно, то
- КИ15 и КИ31 следующего тракта, как описано выше.

Этот процесс может продолжаться до тех пор, пока не будут заняты КИ15 и КИ31 всех трактов интерфейса.

1.5.6 Подуровни уровня 2 и мультиплексирование в С-каналах

Согласно общим принципам семиуровневой модели OSI задача уровня 2 состоит в том, чтобы обеспечить надежную передачу сообщений уровня 3 с использованием тех средств, которые предоставляет уровень 1. Это достигается путем нумерации кадров уровня 2, вычисления и добавления в конец каждого кадра контрольной комбинации для обнаружения ошибок. Если проверка принятого кадра показывает, что он содержит ошибку, запрашивается повторная передача всех кадров, начиная с последнего правильно принятого.

Спецификация протокола и процедуры протокола уровня 2 основаны на протоколе LAPD и процедурах, определенных в Рекомендации МККТТ Q.921 для системы цифровой абонентской сигнализации DSS1.

Протокол LAPV5 уровня 2 содержит два подуровня, один из которых образуют функции обрамления кадров LAPD (подуровень LAPV5-EF), а второй – собственно функции поддержки звена данных в интерфейсе V5 (подуровень LAPV5-DL). Для переноса информации D-канала ISDN функции обрамления должны быть дополнены в сети доступа функциями преобразования кадров (AN-FR).

1.5.7 Связь между подуровнями уровня 2

Взаимодействие подуровней уровня 2 происходит под управлением т.н. функции мэппинга (mapping function).

Направление от LAPV5-EF к LAPV5-DL: Когда подуровень LAPV5-EF принимает кадр со стороны АТС, и при этом V5DL-адрес находится внутри диапазона, который отведен для адресов логических объектов протоколов V5, информационное поле обрамленного кадра передается к подуровню LAPV5-DL.

Направление от LAPV5-DL к LAPV5-EF: Подуровень LAPV5-DL запрашивает функцию обрамления сформировать обрамленный кадр с EF-адресом, равным адресу V5DL. Кадр подуровня LAPV5-DL помещается в информационное поле обрамленного кадра LAPV5-EF.

Направление от AN-FR к LAPV5-EF: Кадры D-канала, принимаемые от пользовательских портов ISDN, обрабатываются функциями преобразования кадров в сети доступа и поступают в LAPV5-EF для передачи интерфейс V5 к АТС. В качестве параметра передается EF-адрес, связанный с пользовательским портом, и обработанный кадр вводится в информационное поле обрамленного кадра LAPV5-EF.

Направление от LAPV5-EF к AN-FR: Когда подуровень LAPV5-EF принимает от АТС кадр с V5DL-адресом, который находится внутри диапазона, отведенного для идентификации портов пользователей ISDN, содержание информационного поля обрамленного кадра и EF-адрес поступают к функциям преобразования кадров в сети доступа для дополнительной обработки и передачи к пользовательскому порту ISDN.

1.5.8 Мультиплексирование на уровне 3

В интерфейсе V5.1 сигнальная информация пользовательских портов ТфОП объединяется на уровне 3 и передается по одному звену данных уровня 2 для протокола ТфОП.

Аналогично, управляющая информация объединяется на уровне 3 и передается по звену данных уровня 2 для протокола управления. Адресная информация портов содержится в сообщениях уровня 3 ТфОП и протокола управления.

Мультиплексирование на уровне 3 в интерфейсе V5.2 производится так же со следующими дополнениями.

Информация протокола управления трактами мультиплексируется на уровне 3 и переносится через интерфейс по звену уровня 2, предназначенному для информации управления трактами.

Информация протокола ВСС мультиплексируется на уровне 3 и передается по звену уровня 2, предназначенному для информации ВСС.

Информация протокола защиты мультиплексируется на уровне 3 и переносится через интерфейс по двум звеньям уровня 2, предназначенным для протокола защиты и организуемым в Первичном и Вторичный трактах 2048 кбит/с.

1.5.9 Резервирование С-каналов

В интерфейсе V5.2 предусмотрена возможность резервирования логических С-каналов, по которым передается сигнальная информация и данные всех служебных протоколов. Протокол защиты позволяет при отказе одного из трактов интерфейса V5.2 автоматически переключаться на другой тракт, разумеется, при условии, что интерфейс содержит, по меньшей мере, два таких тракта. Сообщения протокола защиты имеют приоритет относительно других сообщений, передаваемых в физическом С-канале. Протокол действует так, что все С-пути резервируемого логического С-канала переключаются на один резервный физический С-канал. Для резервируемых С-каналов организуется группа защиты 1 и, как правило, группа защиты 2.

Группа защиты 1 использует два физических С-канала, размещенных в КИ16 Первичного (основного) и Вторичного (резервного) трактов интерфейса V5.2.

При пуске системы логический С-канал, содержащий С-пути протокола управления, протокола управления трактом и протокола ВСС, размещается в КИ16 Первичного тракта, а при отказе этого тракта логический С-канал переключается на КИ16 Вторичного тракта. Потери сообщений при переключении (если они происходят) должны обнаруживаться процедурами уровня 3. Средства протокола защиты обеспечивают непрерывный мониторинг флагов всех (активных и резервных) физических С-каналов для защиты от отказов, которые еще не обнаружены средствами уровня 1,.

Если организуется группа защиты 2, то она, как правило, обеспечивает N2 логических каналов в соответствии с соотношением: $1 \leq N2 \leq (3 \times L - 2 - K2)$, где L - количество трактов в интерфейсе, K2 - количество резервных каналов ($1 \leq K2 \leq 3$).

Группа защиты 2 отличается от группы защиты 1 тем, что она не предусматривает резервного КИ для каждого логического С-канала. Данные протокола защиты в КИ группы защиты 2 и по резервным канальным интервалам для группы защиты 2 не передаются. Как и в случае группы защиты 1, все сообщения, поврежденные в результате переключения, передаются повторно в рамках обычного процесса исправления ошибок на уровне 3.

Контрольные вопросы

- 1 Составьте функциональное описание интерфейса V5.
- 2 Опишите типы оборудования сети доступа с V5.
- 3 Какие уровни протоколов существуют в интерфейсе V5 и каково их соответствие модели взаимодействия открытых систем OSI?
- 4 Какой моделью можно описать алгоритм работы протокола?
- 5 Назовите функции уровня 2, его подуровни и связь между подуровнями.
- 6 Дайте определение С-путей, С-каналов и типов данных, передаваемых через интерфейс V5.
- 7 Как производится размещение С-путей в логических С-каналах и в канальных интервалах (КИ) ИКМ-тракта; порядок размещения?
- 8 Как обеспечивается резервирование трактов и каналов; группа защиты 1 и группа защиты 2?

Контрольное задание

1. Составьте схемы возможных вариантов включения мультисервисного абонентского концентратора МАК в цифровую АТС в опорной точке "V" с использованием интерфейса V5.

Занятие 2 Структура кадров интерфейса V5

2.1 Структура кадров уровня 2

Структура кадров формируется функцией обрамления (Envelop function – EF), образующей один из подуровней уровня 2. Эта структура приведена на рисунке 2.1.

| | | | | | | | | |
|------------------------------------|---|---|---|---|---|---|---|------|
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Байт |
| Отрывающий флаг | | | | | | | | 1 |
| Адресная информация (старшие биты) | | | | | | | | 2 |
| Адресная информация (младшие биты) | | | | | | | | 3 |
| Информация кадра LAPD | | | | | | | | : |
| | | | | | | | | :: |
| | | | | | | | | : |
| Проверочный полином | | | | | | | | N-2 |
| | | | | | | | | N-1 |
| Закрывающий флаг | | | | | | | | N |

Рисунок 2.1 - Структура кадра, поддерживаемого функцией EF

Как видно из рисунка, кадр ограничен двумя флагами: “Отрывающим” и “Закрывающим”, которые имеют одну и ту же кодировку – “01111110”, совпадающую с кодировкой флагов в системах DSS-1 и ОКС7.

После “Отрывающего флага” размещаются два байта адресной информации. Формат адресного поля для “Адресной информации” приведен на рисунке 2.2.

| | | | | | | | | |
|----------------------------------|---|---|---|---|---|---|------|------|
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Байт |
| EF-Адрес уровня 2 (старшие биты) | | | | | | 0 | EA=0 | 2 |
| EF-Адрес уровня 2 (младшие биты) | | | | | | | EA=1 | 3 |

Рисунок 2.2 - Поле EF-адреса уровня 2

Бит “EA” – это бит расширения адресного поля (Address Extension). Значение бита EA=0 указывает, что это не последний байт адресного поля, а значение бита EA=1 указывает, что это последний байт адресного поля. Бит “2” второго байта всегда имеет фиксированное значение “0”. Таким образом, для кодировки адреса остается 13 битов. Эти 13 битов образуют общее адресное пространство для портов ТфОП, портов ISDN и каждого из служебных протоколов V5. 13-битовая последовательность позволяет присваивать внешнему адресу значения от 0 до 8191. Адреса от 0 до 8175 используются для идентификации портов ISDN, связанных с интерфейсом V5. Информацию с этими адресами EF-функция передает далее для обработки функцией мэппинга (mapping function), в задачу которой входит преобразование полученного формата в формат кадров LAPD. Это необходимо в связи с тем, что сообщения ISDN до передачи через интерфейс V5 уже были помещены в информационное поле кадров LAPD. Чтобы эти кадры могли транслироваться через сеть доступа, необходимо снабдить их адресом пользовательского порта ISDN.

Остающиеся адреса от 8176 до 8191 используются для идентификации (в соответствии с идеологией модели взаимодействия открытых систем) точек доступа к услугам (service access point – SAP) уровня 2 со стороны уровня 3 на любой стороне интерфейса V5. Из этого адресного пространства выбраны EF-адреса для протоколов интерфейса, которые приведены в таблице 2.1.

За полем EF-адреса помещается информационное поле кадра, где находится информация, которую EF-функция передает на подуровень звена данных.

В интерфейсе V5 для информационного поля кадра (рисунок 2.1) определены максимальная и минимальная длины – 531 и 3 байта, соответственно. Эти ограничения нуждаются в пояснении. Дело в том, что EF-функция не рассчитана на обработку “неограниченных” кадров, которые считаются недопустимыми и стираются при обработке. Такими являются кадры, у которых не обнаружен закрывающий флаг на протяжении удвоенной максимальной длины плюс два байта, т.е. (2 x 268 + 2) 538 байтов.

Кадр с максимальной длиной 537 байтов считается “слишком длинным”, но подлежит обработке. “Открывающий” и “Закрывающий” флаги, проверочный полином кадра и EF-адрес в сумме составляют 6 байтов, поэтому максимальная длина информационного поля кадра для EF-функции и составляет $537-6=531$ байтов. Минимальную длину информационное поле кадра имеет тогда, когда не передается информация и кадры не нумеруются. В этом случае передается 2 байта V5DL-адреса (рисунок 2.3) и 1 байт в поле “УПРАВЛЕНИЕ”, т.е. всего 3 байта.

Структуру информационного поля кадра определяют форматы кадров подуровня звена данных (LAPV5-DL), которые приведены на рисунке 2.3 (формат А – без информационного поля) и рисунке 2.4 (формат Б – с информационным полем).

Структура А должна использоваться при покадровой передаче без подтверждения. Структура В должна использоваться в режиме передачи нумерованных кадров с информацией уровня 3.

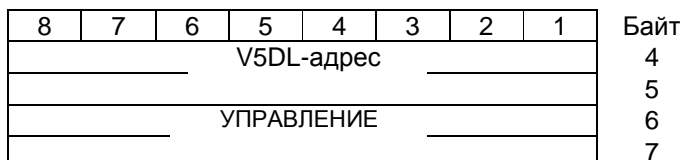


Рисунок 2.3 - Структура А кадра (без информационного поля)

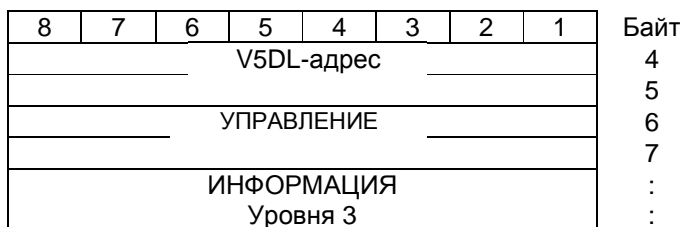


Рисунок 2.4 - Структура В кадра (с информационным полем)

Формат поля V5DL-адрес приведен на рисунке 2.5.

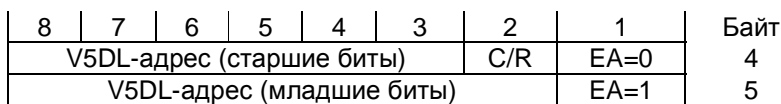


Рисунок 2.5 - Поле V5DL-адреса уровня 2

Бит идентификации команды/ответа (C/R) кадра ISDN указывает, является ли кадр командой или ответом. Принята разная кодировка для стороны пользователя и стороны сети, которая обеспечивает совместимость с системой DSS1.

Поле V5DL-адреса такое же, как и поле EF-адреса. Это сделано для того, чтобы протокол управления мог обращаться к пользовательским портам как ТфОП, так и ISDN с помощью адресов уровня 3, причем таких же, как адреса, используемые для управления соединением с базовым доступом ISDN как на уровне 2, так и на уровне 3. Аналогичная двухуровневая структура адресации кадра применяется и для сообщений других протоколов, что позволяет свободно специфицировать в дальнейшем внутреннюю часть кадра для новых протоколов сети доступа.

Адреса портов ISDN уровня 3 соответствуют адресам уровня 2, используемым для идентификации портов ISDN.

Завершают обрамление два байта проверочной комбинации FCS и закрывающий флаг.

Перед тем как инициировать какое-либо действие, связанное с сообщением, на приемной стороне кадры проверяются специальными процедурами. Неправильные кадры отбрасываются без уведомления об этом передающей стороны. К неправильным кадрам относятся те, которые:

- четко не ограничены двумя флагами, т.е. имеют длину более 533 байтов (531 байт плюс 2 байта EF-адреса);
- имеют длину менее 5 байтов;

- не содержат целое число байтов до введения ZERO-бита или после удаления ZERO-бита;
- содержат ошибочный проверочный полином кадра;
- содержат адресное поле длиной 1 байт.

2.2 Формат сообщений уровня 3

2.2.1 Общее

Логические объекты любого протокола уровня 3, находящиеся по разные стороны интерфейса V5, обмениваются через этот интерфейс информацией с помощью сообщений. Общая структура сообщения протоколов уровня 3 представлена на рисунке 2.6.

Каждое сообщение состоит из информационных элементов, три из которых являются обязательными для всех сообщений: дискриминатор протокола (1 байт), адрес уровня 3 (2 байта), тип сообщения (1 байт). Обязательность/необязательность каждого из других информационных элементов, как и его длина, зависит от типа сообщения.

| Биты | | | | | | | | Байт |
|--------------------------------|---------------|---|---|---|---|---|---|--------|
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
| Дискриминатор протокола | | | | | | | | 1 |
| Адрес уровня 3 | | | | | | | 1 | 2 |
| Адрес уровня 3 (младший байт) | | | | | | | | 3 |
| 0 | Тип сообщения | | | | | | | 4 |
| Другие информационные элементы | | | | | | | | 5 |
| | | | | | | | | 6 |
| | | | | | | | | и.т.д. |

Рисунок 2.6 - Общая структура сообщения протоколов уровня 3

Любой информационный элемент может присутствовать в сообщении только один раз. Это правило относится ко всем протоколам V5.

2.2.2 Дискриминатор протокола V5

Дискриминатор протокола занимает первый байт сообщения и имеет значение 01001000 (48 в шестнадцатеричной системе). Задача дискриминатора протокола – обеспечить возможность отличать сообщения протоколов V5 по ETS 300 324-1 и ETS 300 347-1 (протокола ТфОП, протокола управления, протокола управления трактами, ВСС-протокола и протокола защиты) от сообщений других протоколов, использующих то же соединение уровня 2, а также обеспечить структурную совместимость с другими протоколами (например, с ETS 300 102-1), в том числе, и с новыми протоколами уровня 3, которые находятся в стадии разработки.

2.2.3 Адрес уровня 3

Следом за дискриминатором протокола помещаются два байта адреса уровня 3. Назначение этого обязательного информационного элемента – идентификация логического объекта уровня 3 в интерфейсе V5.

Для протокола ТфОП адрес уровня 3 – это число, которое идентифицирует определенный пользовательский порт ТфОП. Бит с номером «1» в первом байте адреса имеет фиксированное значение «1», а оставшиеся 15 битов обеспечивают адресацию для 32768 портов ТфОП (п.13.4.3 ETS 300 324-1).

В протоколе управления адрес уровня 3 идентифицирует порт ТфОП или ISDN. а также функции общего управления. Для идентификации порта ТфОП в качестве адресов уровня 3 используются такие же значения, как и для протокола ТфОП.

Для идентификации порта ISDN и функции общего управления бит «1» первого байта адреса должен иметь значение «0». Бит «2» этого байта должен также иметь значение «0». Значение «Адрес уровня 3» должно быть копией адреса LAPV5-EF, используемого для порта ISDN (D-канал), которому предназначена информация булуправления, или адресом функции общего управления, который совпадает с адресом LAPV5-DL, т.е. равен 8177.

Протокол ВСС помещает в двухбайтовое поле адреса уровня 3 «ссылочный номер» (Reference Number), который для идентификации процесса, создаваемого протоколом тоже использует 13 битов.

Бит "8" первого байта ссылочного номера – это бит индикации логического объекта (сети доступа или оконечной АТС), создавшего процесс. Кодовое слово длиной 13 битов обеспечивает 8192 возможных значения "ссылочного номера" процесса ВСС, к которому относится сообщение.

В протоколе управления трактами старший байт адреса уровня 3 содержит только биты, имеющие значение "0". Восемь битов младшего байта определяют значения идентификаторов 16 трактов интерфейса V5.2 (п.16.3.2.1 ETS 300 347-1). Эти значения должны совпадать со значениями, записанными в поле идентификатора ИКМ-тракта протокола ВСС.

Протокол защиты помещает в двухбайтовое поле адреса уровня 3 идентификатор логического С-канала, к которому относится сообщение. Значения идентификатора – от 0 до 65535. Для одного интерфейса V5.2 могут быть идентифицированы 44 логических С-канала. Поясним это. Значение 44 соответствует максимальному числу логических С-каналов в интерфейсе V5.2. Оно равно максимальному числу физических С-каналов ($3 \times 16 = 48$) минус 1 резервный канал для группы защиты 1 и минус 3 резервных канала для группы защиты 2.

2.2.4 Другие информационные элементы

За обязательными информационными элементами в сообщениях могут следовать и необязательные. Их состав и структура зависят от протокола и от передаваемого сообщения.

2.3 Способ передачи

В каждом байте бит, обозначенный "бит 1", передается первым, в каждом информационном элементе байт, обозначенный "байт 1", передается первым; за ним передаются байты 2,3,4 и т.д.

Когда информационное поле состоит более чем из одного байта, "веса" битов уменьшаются с увеличением номера байта. Таким образом, самый маленький вес в составе информационного поля имеет младший бит байта с наибольшим номером.

Для размещения информации проверочного полинома кадра принят обратный порядок: первый бит первого байта имеет наибольший вес; восьмой бит второго байта проверочного полинома кадра имеет наименьший вес

Биты, не используемые в структуре информационного элемента, но потенциально возможные, рассматриваются как резервные и имеют значение "0". Тем не менее, прием сообщения со значениями битов резервного поля, отличными от "0", не приводит к ошибке протокола.

Контрольные вопросы

1. Какова общая структура сообщений протоколов интерфейса V5?
2. Какова структура сообщений протоколов интерфейса V5.1?
3. Какова структура сообщений служебных протоколов интерфейса V5.2?
4. Каковы признаки неправильных кадров?
5. Какие соглашения приняты относительно порядка размещения и передачи информации?

Занятие 3 Протокол ТфОП (PSTN PROTOCOL)

3.1 Основы протокола ТфОП

Протокол, обеспечивающий перенос через интерфейс V5 сигнальной информации при обслуживании вызовов абонентов ТфОП (протокол ТфОП), не управляет процедурами обработки вызова в сети доступа, а потому используется совместно с национальным протоколом сигнализации ТфОП, реализованным в АТС. Большинство линейных сигналов протоколом ТфОП не интерпретируется, а просто без изменения переносится им от пользовательского порта в АН к логическому объекту национального протокола АТС и в обратном направлении.

Главная функция протокола ТфОП – поддержка национального протокола управления соединениями в телефонной сети. С этой целью для каждого вызова абонента ТфОП (как исходящего, так и входящего) протокол ТфОП предусматривает создание в интерфейсе V5 логического соединения, использующего ресурс того С-пути, который предназначен для сигнализации ТфОП.

Кроме того, протокол ТфОП может использовать этот же С-путь и без создания в нем логического соединения, когда возникает необходимость в передаче информации, не связанной с управлением соединениями ТфОП (например, данных об абонентской линии – от сети доступа к АТС). Упомянутое логическое соединение называют сигнальным путем (signaling path). Сигнальный путь существует в течение всех фаз соединения ТфОП и обеспечивает прозрачный обмен сообщениями уровня 3 между логическими объектами протокола ТфОП, расположенными по разные стороны интерфейса.

Процедуры протокола обеспечивают создание сигнального пути, освобождение сигнального пути, разрешение конфликтов "встречных" вызовов и проблем, возникающих при перегрузке АТС.

С каждой стороны интерфейса V5 протокол ТфОП представлен одним или несколькими логическими объектами, функционирование которых описывается в терминах конечных автоматов. Конечный автомат (Finite State Machine, FSM) – это модель процесса с конечным число состояний, с конечным числом входных/выходных сигналов и с дискретным временем. Переход FSM из одного состояния в другое происходит только под воздействием входного сигнала. Выходными сигналами могут быть сообщения уровня 3, примитивы, обеспечивающие внутреннее взаимодействие FSM со средствами эксплуатационного управления, и сигналы (команды/ответы/извещения), связанные с управлением т.н. "элементарными функциями" (Function Elements, FE) логических объектов, а входными сигналами – также и срабатывания таймеров.

При исходящей связи информация телефонной сигнализации в виде сигналов FE, которые формируются блоком "Обработка примитивов и FE", передается к FSM на стороне сети доступа (рисунок 3.1).

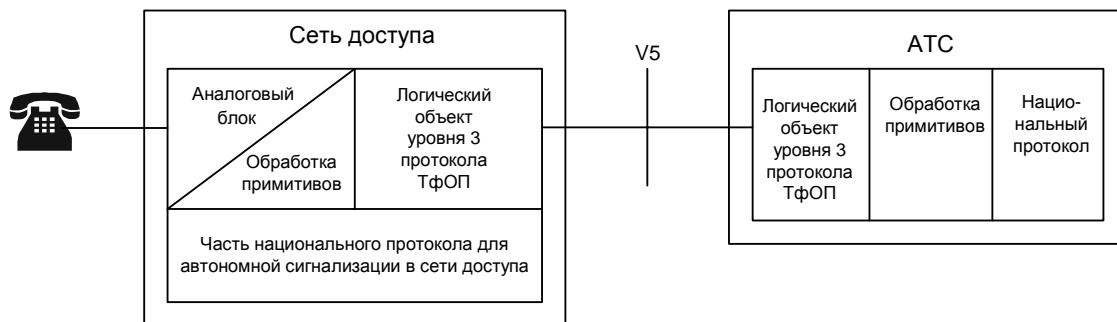


Рисунок 3.1. Функциональная модель пользовательского порта ТфОП

На основе этих сигналов логический объект уровня 3 на стороне сети доступа формирует сообщения и передает их через интерфейс V5 к логическому объекту уровня 3 на стороне АТС. Из этих сообщений последний формирует сигналы FE, и передает их к логическому объекту национального протокола ТфОП, который инициирует выполнение соответствующих действий или элементарных функций.

При входящей связи процесс происходит в обратном порядке

АТС, в отличие от сети доступа, имеет всю информацию о состоянии процесса обслуживания вызова и поэтому отвечает за обеспечение и поддержку услуг. Передатчики и приемники многочастотного набора (DTMF), генераторы тональных сигналов и автоинформаторы должны размещаться на АТС. Это означает, что информация об адресе в форме сигналов DTMF должна передаваться "прозрачно" между портом пользователя и АТС, тогда как линейные сигналы должны интерпретироваться в сети доступа и затем передаваться через интерфейс V5 с помощью сообщений уровня 3.

3.2 Определение сигналов FE, сообщений и примитивов

В таблице 3.1 приведены сигналы FE протокола ТфОП, которые должны использоваться либо внутри сети доступа между логическим объектом ТфОП и портом пользователя, либо внутри АТС между логическим объектом ТфОП и логическим объектом национального протокола.

Таблица 3.1 – Сигналы FE протокола ТфОП

| Имя | Направление | Описание |
|---|-------------|---|
| Сигналы, используемые FSM на стороне сети доступа | | |
| FE-line_information | PSTN_AN←SUB | Состояние абонентской линии изменилось |
| FE-line_signal | PSTN_AN←SUB | Электрический сигнал к/от порта ТфОП |
| FE-subscriber_seizure | PSTN_AN←SUB | Абонент требует создать сигнальный путь |
| FE-subscriber_release | PSTN_AN←SUB | Отбой абонента до создания сигнального пути |
| Сигналы, используемые FSM на стороне АТС | | |
| FE-disconnect_request | PSTN_LE←NAT | Нац. протокол требует освободить сигнальный путь |
| FE-disconnect_complete_request | PSTN_LE←NAT | Нац. протокол требует передать в сеть доступа подтверждение освобождения сигнального пути |
| FE-establish_acknowledge | PSTN_LE←NAT | Нац. протокол положительно подтверждает запрос создать сигнальный путь |
| FE-establish_request | PSTN_LE←NAT | Нац. протокол требует создать сигнальный путь |
| FE-line_signal_request | PSTN_LE←NAT | Нац. протокол требует передать сигнал к порту пользователя в сети доступа |
| FE-protocol_parameter_request | PSTN_LE←NAT | Нац. протокол требует изменить параметры протокола ТфОП |
| FE-disconnect_complete_indication | PSTN_LE←NAT | Индикация освобождения сигнального пути |
| FE-establish_indication | PSTN_LE←NAT | Индикация запроса создать сигнальный путь |
| FE-establish_acknowledge_ind. | PSTN_LE←NAT | Индикация подтверждение запроса создать сигнальный путь |
| FE-line_signal_indication | PSTN_LE←NAT | Индикация приема линейного сигнала |
| PSTN_AN – FSM протокола ТфОП на стороне сети доступа SUB – Пользовательский порт PSTN_LE – FSM протокола ТфОП на стороне АТС NAT – Национальный протокол | | |

В таблице 3.2 приведены сообщения (тип, функциональное назначение, направление передачи) протокола ТфОП, которые должны использоваться между логическими объектами ТфОП на стороне AN и стороне LE.

Таблица 3.2 - Сообщения протокола ТфОП

| Тип сообщения | Функциональное назначение сообщения | Направление |
|---|---|-------------------|
| | | передачи AN LE |
| 1 | 2 | 3 |
| Сообщения создания сигнального пути | | |
| ESTABLISH (создать сигнальный путь) | Передается, когда имеется запрос исходящей или входящей связи) | ←→ |
| ESTABLISH ACK (подтверждение создания сигнального пути) | Передается, когда логический объект выполнил действия, необходимые для создания сигнального пути | ←→ |
| SIGNAL (сигнал) | Передаёт в АТС сведения о режиме, в котором находится АЛ, а в сеть доступа – указания установить нужный режим | ←→ |
| SIGNAL ACK (подтверждение приема сообщения SIGNAL) | Подтверждает прием сообщения SIGNAL и сообщения PROTOCOL PARAMETER | ←→ |
| Сообщения освобождения сигнального пути | | |
| DISCONNECT (освободить сигнальный путь) | При передаче от АТС извещает, что обслуживание вызова завершено и что FSM на стороне сети доступа может вернуться в нулевое состояние, а при передаче к АТС – о том, что сигнальный путь должен быть освобожден | ←→ |
| DISCONNECT COMPLETE (сигнальный путь освобожден) | Извещает, что логический объект выполнил действия, предписанные сообщением DISCONNECT | ←→ |

Окончание таблицы 3.2

| 1 | 2 | 3 |
|--|--|---|
| Другие сообщения | | |
| STATUS ENQUIRY (запрос сведений о состоянии) | Передается для запроса сведений о состоянии FSM протокола ТфОП на стороне сети доступа | ← |
| STATUS (состояние) | Передается в ответ на сообщение STATUS ENQUIRY для индикации состояния FSM, или когда сеть доступа принимает от АТС непредвиденное сообщение | → |
| PROTOCOL PARAMETER (параметр протокола) | Передается от АТС для того, чтобы изменить параметр протокола в сети доступа | ← |

Обмен примитивами между логическим объектом протокола и системой эксплуатационного управления (как на стороне сети доступа, так и на стороне АТС) производится при управлении портами ТфОП, при перезапуске логического объекта и для индикации ошибок.

3.3. Состояния логических объектов протокола ТфОП

3.3.1 Состояния FSM на стороне сети доступа (PSTN_AN)

"Вне обслуживания" (AN0)

В этом состоянии FSM пребывает, когда системой эксплуатационного управления инициирована процедура перезапуска. Все порты ТфОП выведены из обслуживания.

"Нулевое" (AN1).

В этом состоянии порт ТфОП не занят обслуживанием вызова, но способен обнаружить занятие абонентской линии (возможно, уже существующее).

"Сеть доступа инициирует создание сигнального пути" (AN2)

В это состояние FSM переходит, когда в порту ТфОП обнаружен сигнал "занятие". К АТС передается сообщение ESTABLISH и от нее ожидается подтверждающее сообщение ESTABLISH ACK. Если подтверждение не поступает (например, при перегрузке LE), сообщение ESTABLISH периодически повторяется с частотой, определяемой таймером T1.

В этом состоянии может возникнуть необходимость разрешения конфликта со встречным вызовом.

"Отмена создания сигнального пути" (AN3)

В это состояние FSM переходит, если абонент дает отбой, когда сообщение ESTABLISH уже передано к АТС, а сообщение ESTABLISH ACK еще не получено. При повторном занятии порта это состояние позволяет ограничить количество сообщений ESTABLISH, которые будут переданы к АТС без получения подтверждения (возможно, из-за перегрузки АТС). По истечении интервала времени, определяемого таймером T1 (или T2), FSM возвращается в нулевое состояние AN1.

"Обработка данных о линии" (AN4)

В это состояние FSM переходит, когда сеть доступа передала данные об абонентской линии на АТС, и та ведет их обработку. В состоянии AN4 можно перейти только из состояния AN1, и перейти из AN4 можно только в AN1.

"Путь активен" (AN5)

Это – состояние, в котором для данного порта активны нормальные функции сигнализации ТфОП. В состоянии AN5 пользователь может устанавливать нужное ему соединение, участвовать в сеансе связи и прекратить эту связь.

"Порт заблокирован" (AN6)

В это состояние FSM может перейти из любого состояния, а выход из него возможен только в состояние AN1. Работа порта прекращается, и его можно деактивизировать.

"Сеть доступа требует освободить сигнальный путь" (AN7)

В это состояние FSM переходит, когда сеть доступа передает к АТС сообщение DISCONNECT, и выходит из него при приеме от АТС сообщения DISCONNECT COMPLETE. Если такого сообщения нет, в систему эксплуатационного управления передается соответствующее извещение.

3.3.2 Состояния FSM на стороне АТС (PSTN_LE)

"Вне обслуживания" (LE0)

В этом состоянии FSM пребывает, когда системой эксплуатационного управления инициирована

процедура перезапуска. Все порты ТфОП выведены из обслуживания.

"Нулевое" (LE1)

В этом состоянии порт неактивен – он не занят обслуживанием вызова.

"АТС инициирует создание сигнального пути" (LE2)

В это состояние FSM переходит, когда АТС, обслуживая входящий вызов, занимает порт и передает к сети доступа сообщение ESTABLISH. В состоянии LE2 может возникнуть необходимость разрешения конфликта со встречным вызовом.

"Сеть доступа инициирует создание сигнального пути" (LE3)

В это состояние FSM переходит, когда сеть доступа передала к АТС сообщение ESTABLISH и ожидает от нее подтверждающее сообщение ESTABLISH ACK. В этом состоянии тоже возможна ситуация, требующая разрешения конфликта со встречным вызовом.

"Путь активен " (LE4)

Это – состояние, в котором для данного порта активны нормальные функции сигнализации ТфОП. Пользователь может устанавливать нужное ему соединение, участвовать в сеансе связи и прекратить эту связь.

"АТС требует освободить сигнальный путь" (LE5)

В это состояние FSM переходит, когда АТС передает к сети доступа сообщение DISCONNECT, а выходит из него, приняв ответное сообщение DISCONNECT COMPLETE. Если такого сообщения не поступает, в систему эксплуатационного управления передается соответствующее извещение.

"Порт заблокирован " (LE6)

В это состояние FSM может перейти из любого состояния, а выход из него возможен только в состоянии AN1. Работа порта прекращается, и его можно деактивизировать.

3.4 Кодирование информационных элементов

“Дискриминатор протокола” является первым информационным элементом любого сообщения. Далее следует “Адрес уровня 3”, который идентифицирует пользовательский порт ТфОП, к которому относится данное сообщение. Формат этого информационного элемента рассмотрен на Занятии 2. “Адрес уровня 3” кодируется двоичным кодом; все значения от 0 до 32767 должны быть доступны. Информационный элемент “Тип сообщения” идентифицирует протокол, которому принадлежит сообщение, и назначение этого сообщения.

Контрольные вопросы

1. Дайте определение С-пути и С-канала.
2. Опишите функциональную модель протокола ТфОП, отражающую взаимодействие сети доступа и опорной АТС.
3. Составьте описание логического объекта протокола ТфОП.
4. Назовите сообщения, примитивы, сигналы (команды/ответы/извещения), связанные с управлением элементарными функциями FE логических объектов, и таймеры протокола ТфОП.
5. Дайте определение конечного автомата FSM. Поясните содержание и использование таблиц, описывающих поведение FSM
6. Поясните функциональное назначение сообщений, сигналов FE, примитивов и таймеров FSM логического объекта протокола ТфОП.
7. Поясните назначение, порядок использования и структуру сообщений протокола ТфОП.

Занятие 4 Информационные элементы сообщений протокола ТфОП

4.1 Структура и кодирование информационных элементов

Как уже указывалось (Занятие 3), любое сообщение содержит обязательные для каждого протокола информационные элементы “Дискриминатор протокола”, “Адрес уровня 3”, “Тип сообщения”. Кроме того, имеются и элементы, специфические для того или иного протокола. Их число в сообщении, как и обязательность или необязательность, зависит от типа сообщения. В таблице 4.1 приведен перечень и кодирование (в соответствии с правилами, определенными в ETS 300 102-1) идентификаторов информационных элементов, специфических для протокола ТфОП.

Таблица 4.1 - Кодирование идентификаторов информационных элементов

| Биты | | | | | | | | Информационные элементы | Длина |
|------|---|---|---|---|---|---|---|---|-------|
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | |
| 1 | - | - | - | x | x | x | x | ОДНОБАЙТОВЫЕ | |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | Импульсный сигнал передан (Pulse_notification) | 1 |
| 1 | 0 | 0 | 0 | x | x | x | x | Данные о линии (Line_information) | 1 |
| 1 | 0 | 0 | 1 | x | x | x | x | Состояние (State) | 1 |
| 1 | 0 | 1 | 0 | x | x | x | x | Автономная сигнализация (Autonomus_signaling_sequence) | 1 |
| 1 | 0 | 1 | 1 | x | x | x | x | Результат автономной сигнализации (Sequence-response) | 1 |
| 0 | - | - | - | - | - | - | - | МНОГОБАЙТОВЫЕ, ПОСТОЯННОЙ ДЛИНЫ | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Порядковый номер (Sequence_number) | 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | Модулированный вызов (Cadenced_ringing) | 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | Непрерывный сигнал (Steady_signal) | 3 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | Цифра (Digit_signal) | 3 |
| 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | Отмена автономной реакции на сигнал (Disable_autonomous_ack.) | 3 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | Время распознавания (Recognition_time) | 4 |
| 0 | - | - | - | - | - | - | - | МНОГОБАЙТОВЫЕ, ПЕРЕМЕННОЙ ДЛИНЫ | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | Импульсный сигнал (Pulsed_signal) | 3-5 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | Автономная реакция на сигнал (Enable_autonomous_acknowledge) | 4-6 |
| 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | Причина (Cause) | 3-5 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | Ресурс недоступен (Resource_unavailable) | 3-8 |

Примечание - Все остальные коды – резервные

Однобайтовые информационные элементы

Импульсный сигнал передан (Pulse_notification). Цель этого информационного элемента – сообщить АТС, что затребованная ею передача из пользовательского порта ТфОП в терминал абонента импульсного сигнала закончена. Сам элемент не содержит информации о том, какой именно импульсный сигнал был передан. Имеется в виду тот импульсный сигнал (или цифра), запрос передачи которого был последним.

Данные о линии (Line_information). Цель этого информационного элемента – при отсутствии сигнального пути передать от сети доступа к АТС сведения о состоянии абонентской линии.

Состояние (State). Этот информационный элемент предназначен для передачи к АТС, по ее запросу, сведений о состоянии FSM на стороне сети доступа.

Автономная сигнализация (Autonomus_signalling_sequence). С помощью этого информационного элемента АТС предписывает сети доступа начать автономный обмен с терминалом абонента определенной последовательностью сигналов, номер которой задается в поле “Тип последовательности”.

Результат автономной сигнализации (Sequence_response). В этом информационном элементе сеть доступа сообщает АТС результат предписанного ей автономного обмена последовательностью сигналов. В битах 1÷4 указывается соответствующее (из заранее определенных) значение ответа.

Многобайтовые информационные элементы постоянной длины

Порядковый номер (Sequence_number). Этот информационный элемент может передаваться в обоих направлениях. Его присутствие обязательно в сообщениях SIGNAL, PROTOCOL PARAMETER и SIGNAL ACKNOWLEDGE, а в других сообщениях – запрещено. Длина этого элемента всегда равна 3 байтам. В сообщениях SIGNAL и PROTOCOL PARAMETER информационный элемент "Порядковый номер" содержит номер сообщения в передаваемой последовательности M(S), а в сообщениях SIGNAL ACKNOWLEDGE – номер сообщения в принимаемой последовательности M(R).

Модулированный вызов (Cadenced_ringing). С помощью информационного элемента "Модулированный вызов", длина которого всегда равна 3 байтам, АТС информирует сеть доступа о том, что пользовательский порт должен начать передачу в терминал абонента вызывного сигнала, тип которого заранее определен. Этот элемент передается только в сообщениях от АТС к сети доступа.

Непрерывный сигнал (Steady_signal). С помощью этого информационного элемента АТС сообщает сети доступа о том, что пользовательский порт ТфОП должен начать передачу в терминал абонента определенного непрерывного сигнала, тип которого заранее определен, а сеть доступа информирует АТС о том, что определенный непрерывный сигнал, переданный абонентским оборудованием, был обнаружен в пользовательском порту ТфОП. Информационный элемент "Непрерывный сигнал" всегда имеет длину 3 байта.

Цифра (Digit_signal). Длина информационного элемента "Цифра" всегда равна 3 байтам. В битах 1 - 4 двоичным кодом передается одна цифра номера, принятая сетью доступа от абонента, или цифра, которую АТС передает в сеть доступа. Нулевое значение всех битов 1÷4 не имеет смысла, это – ошибка. Поле "Индикатор_запроса_подтверждения" (бит "7") позволяет АТС потребовать, чтобы сеть доступа указала порту пользователя конец цифры. В направлении от сети доступа к АТС этот бит должен всегда иметь значение "0". Биты 5 и 6 третьего байта должны иметь значение "0".

Время распознавания (Recognition_time). С помощью информационного элемента "Время распознавания" АТС может дать указание сети доступа изменить время существования определенного сигнала, чтобы оно было достаточным (но не чрезмерно долгим) для распознавания этого сигнала. Длина элемента всегда составляет 4 байта, а передается он только в сообщении от АТС к сети доступа. Поле "Указатель_длительности" содержит индекс той строки предварительно определенной в сети доступа таблицы, где указано время, в течение которого сигнал должен оставаться активным. Бит 7 четвертого байта всегда имеет значение "0".

Отмена автономной реакции на сигнал (Disable_autonomous_acknowledge). Этот информационный элемент передается в сообщении от АТС и указывает сети доступа, что предшествовавшее предписание автономно реагировать на сигнал от абонента отменяется. Длина элемента всегда составляет 3 байта.

Многобайтовые информационные элементы переменной длины

Импульсный сигнал (Pulsed_signal). При передаче от АТС к сети доступа этот информационный элемент указывает на то, что в пользовательском порту ТфОП должен быть сформирован импульсный сигнал. Передача такого элемента от сети доступа к АТС означает, что порт ТфОП получил сигнал от абонента или от УАТС. Длительность импульсного сигнала указывается в поле "Тип_длительности_импульса". Каждому типу длительности соответствует предварительно определенный набор характеристик импульсов и пауз между ними. Поле "Индикатор_подавления" (биты 6 и 7 в байте 4) дает АТС возможность сообщить сети доступа, должен ли быть подавлен входящий импульсный сигнал. Поле "Индикатор_запроса_подтверждения" (биты 6 и 7 в байте 4а) позволяет АТС запросить подтверждение исполнения требования передать импульсный сигнал: началась передача сигнала, закончилась передачи сигнала или передача одной из серий импульсов. Поле "Число_импульсов" содержит двоичное число, показывающее, сколько импульсов должно быть передано (значение "0" – неправильное). Длина данного информационного элемента может составлять от 3 до 5 байтов.

Активизировать автономную реакцию на сигнал (Enable_autonomous_acknowledge). Вводя этот информационный элемент в сообщение, передаваемое к сети доступа, АТС дает ей указание самостоятельно отвечать на определенный линейный сигнал, получаемый от абонентского оборудования. Это делается для того, чтобы ускорить реакцию на сигнал со стороны абонента.

Если реакция должна быть в форме непрерывного сигнала, информационный элемент и его поле "Сигнал" кодируется одним образом, а если реакция должна быть в форме импульсного сигнала, кодирование полей "Тип_длительности_импульса", "Индикатор_подавления", "Индикатор_запроса_подтверждения" и "Число_импульсов" производится по тем же правилам, что и в информационном элементе "Импульсный сигнал". Длина рассматриваемого элемента составляет 4 байта при активизации реакции в форме «Непрерывный сигнал» и от 4 до 6 байтов – в форме «Импульсный сигнал».

Причина (Cause). Информационный элемент "Причина" может присутствовать только в сообщениях, передаваемых от сети доступа к АТС. Цель этого элемента – сообщить о причине возникновения ошибки в сети доступа. Его длина может составлять 3, 4 или 5 байтов.

При ошибках некоторых типов в элементе "Причина" присутствует поле диагностики, куда помещается дополнительная информация, относящаяся к этим ошибкам. Поле диагностики содержит один или два байта, где помещается копия идентификатора типа принятого сообщения, вызвавшего передачу ответного сообщения с информационным элементом "Причина", и, если нужно, идентификатор соответствующего информационного элемента в принятом сообщении.

При отсутствии поля диагностики длина информационного элемента составляет 3 байта. Если в поле диагностики указывается только идентификатор типа сообщения, вызвавшего передачу сообщения о причине ошибки, длина элемента составляет 4 байта. Если же в поле диагностики указываются и идентификатор типа сообщения, и идентификатор информационного элемента, вызвавшего передачу сообщения о причине ошибки, то элемент "Причина" имеет длину 5 байтов.

Ресурс недоступен (Resource_unavailable). С помощью этого информационного элемента сеть доступа извещает АТС, что затребованный ею ресурс в данный момент недоступен. Элемент передается от сети доступа к АТС только в сообщении SIGNAL и содержит поле, в которое помещается копия того информационного элемента сообщения, принятого от АТС, в котором содержится требование действия, невыполнимого из-за отсутствия нужного ресурса. Длина элемента "Ресурс недоступен" зависит от длины этой копии и составляет от 3 до 8 байтов.

Контрольные вопросы

1. Назовите группы информационных элементов в зависимости от их длины.
2. Какие существуют однобайтовые информационные элементы и каково их функциональное назначение?
3. Какие существуют многобайтовые информационные элементы постоянной длины; каковы структура их информационных полей и их функциональное назначение?
4. Какие существуют многобайтовые информационные элементы переменной длины; каковы структура их информационных полей и их функциональное назначение?

Занятие 5 Национальный мэппинг. Потокные диаграммы

5.1 Национальный мэппинг

Национальный мэппинг – это документ, в котором отражены особенности использования сообщений и сигналов в протоколе ТфОП, принятые для национальной сети связи. Российские национальные спецификации базируются на стандартах ETSI и на рекомендациях ITU-T, но взаимосвязь протокола ТфОП с национальными системами сигнализации по абонентским линиям специфицируется национальной администрацией связи (практика, существующая во всех странах). В этом плане в ТфОП России, в отличие от большинства европейских и американских сетей связи, сложилась более удачная ситуация. Отсутствие интерфейсов "пред-ISDN" и простота абонентских систем сигнализации привели к тому, что национальные спецификации протокола ТфОП России являются подмножеством спецификаций, стандартизованных ETSI.

Набор сообщений и параметров, которые применяются в России, приведен в таблице 5.1.

Таблица 5.1 - Сообщения и параметры протокола ТфОП

| Сообщение | Информационные элементы | Содержание информационных элементов | Направление передачи |
|---------------------|-------------------------------|--|-------------------------------|
| ESTABLISH | Steady_signal | Off_hook | AN → LE |
| | Line_information | Любое допустимое | AN → LE |
| | Cadenced_ringing | Cadenced_ringing_type (1, 2, 3) | LE → AN |
| | Pulsed_signal | Initial_ring (Примечание 1) Suppression_indication (11), Pulse_duration_type (1), Acknowledge_request_indicator (10), Number_of_pulses (1) | LE → AN |
| ESTABLISH ACK | | | AN → LE; LE → AN |
| SIGNAL | Sequence_number | Порядковый номер | AN → LE; LE → AN |
| | Pulse_notification | Кодируется 7-битовой двоичной комбинацией (1000000) | AN → LE (Примечание 2) |
| | Autonomous_signaling_sequence | Sequence_type (1) | LE → AN (Примечание 3) |
| | Sequence_response | | AN → LE (Примечание 4) |
| | Cadenced_ringing | Cadenced_ringing_type (1, 2, 3) | LE → AN |
| | Steady_signal | Off_hook; On_hook Reversed_polarity (Примечание 5) Normal_polarity (Примечание 5) | AN → LE LE → AN LE → AN |
| | Digit_signal | | AN → LE; LE → AN |
| SIGNAL ACK | Sequence_number | Порядковый номер | AN → LE; LE → AN |
| STATUS ENQUIRY | | | LE → AN |
| STATUS | State | Состояние FSM протокола ТфОП (Примечание 6) | AN → LE |
| | Cause | Причина передачи сетью доступа сообщения STATUS (Примечание 7) | AN → LE |
| DISCONNECT | Steady_signal | Stop_ringing | AN → LE; LE → AN LE → AN |
| DISCONNECT COMPLETE | | | AN → LE; LE → AN |
| PROTOCOL PARAMETER | Recognition_time | Duration type (1) Pulsed_signal=register_recall | LE → AN (Примечание 8) |

Примечания к таблице 5.1.

1. Этот информационный элемент используется для идентификации номера вызывающего абонента по алгоритму, принятому в ряде зарубежных стран (с использованием кода DTMF). В России он практически не используется, и включение его в национальные спецификации несколько условно. Идентификация номера вызывающего абонента (АОН) обеспечивается передачей частоты 500 Гц по разговорному каналу. Для такой процедуры интерфейс V5 является прозрачным.

2. Этот информационный элемент имеет только одно значение (кодовая комбинация со старшим битом, имеющим значение "1"). Он используется для индикации того, что передача импульсного сигнала, который по требованию АТС должен быть передан из порта сети доступа в терминал абонента, либо началась, либо закончилась.

3. Этот информационный элемент передается только в сторону сети доступа и содержит указание передать в сторону абонента сигнальную последовательность определенного типа. Это бывает необходимо в тех случаях, когда нецелесообразно перегружать АТС передачей абоненту повторяющихся сигналов или обработкой длительных событий (например, при плохо положенной трубке). Тип последовательности кодируется 4-битовой комбинацией. Код "0001" соответствует сигналу блокировки абонентской линии.

4. Этот информационный элемент передается в ответ на сигнал блокировки абонентской линии.

5. Эти информационные элементы служат для управления кассированием монет в таксофонах. После ответа вызываемого абонента АТС производит переполюсовку напряжения на проводах абонентской линии, что вызывает кассирование монеты. В случае таксофона с централизованным управлением после кассирования монеты АТС восстанавливает полярность, чтобы обеспечить кассирование следующей монеты (если необходимо). Таксофон с автономным управлением сам вырабатывает сигналы кассирования.

6. Состояние FSM протокола ТфОП кодируется 4-битовой комбинацией. Комбинации от "0000" до "0111" используются для состояний от AN0 до AN7 соответственно. Комбинация "1111" – резервируется; остальные комбинации не используются.

7. Для кодирования этого информационного элемента используется 7 битов (см. таблицу 4.9).

8. Этот информационный элемент используется для переноса в сторону АТС запроса дополнительных услуг. Он передается при нажатии абонентом кнопки R (калиброванный разрыв шлейфа) или наборе цифры "1" в разговорной фазе телефонного соединения.

5.2 Потокосые диаграммы (Information flow diagrams)

При разработке сценариев сигнализации в соответствии с национальным мэппингом используются потокосые диаграммы. Они отображают информационные потоки, образующиеся при обмене информацией между функциональными (логическими) объектами. В соответствии с концепцией основных методов моделирования, описанной в Рекомендации I. 130 "Характеристики услуг сети ISDN и сетевые возможности ISDN", потокосые диаграммы соответствуют средствам описания Стадии 2. Эта стадия предназначена для определения функциональных и сигнальных требований и детально рассмотрена в Рекомендации Q.65. В основу Стадии 2 положено описание Стадии 1, выполненное в соответствии с правилами Рекомендаций серии I.200.

В рамках требований Стадии 2 взаимодействие "пользователь-сеть" Стадии 1 представлено на рисунке 5.1.



Рисунок 5.1 - Соотношение Стадии 1 и Стадии 2

Стадия 2 определяет функциональные возможности и информационные потоки, которые обеспечивают услугу, описанную на Стадии 1. Выходные описания Стадии 2 используются в качестве входных данных для разработки системы сигнализации и требований к узлу коммутации.

Этапы создания потокосых диаграмм

Создание функциональной модели

Первым этапом создания потокосой диаграммы является создание функциональной модели, которая, в свою очередь, основывается на требованиях к услугам. Полное множество функций делится на подмножества, которые соответствуют описанным в Рекомендации Q.65 (пункт 2.1.1) и называются функциональными объектами (ФО). Каждому ФО дается номер (или уникальное имя) и, в соответствии с Рекомендацией Q.65 (пункт 2.1.2), устанавливается связь между разными ФО.

На рисунке 5.2 показана элементарная модель, необходимая для описания базового соединения в ISDN (r_1 , r_2 , r_3 - типы связей между взаимодействующими парами ФО).

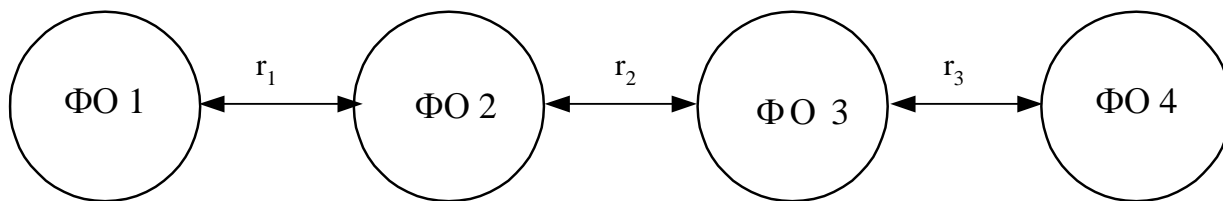


Рисунок 5.2 - Пример функциональной модели

В этой модели ФО1 и ФО4 могут быть представлены в качестве объектов, взаимодействующих с пользователем, а ФО2, ФО3 – в качестве объектов, обеспечивающих управление соединением.

После идентификации функциональной модели, могут быть определены требования к информационным потокам между ФО.

Распределение функций требует взаимодействия между ФО. Каждое взаимодействие рассматривается как "информационный поток" и носит свое имя.

Предполагается, что когда ФО принимает информацию, он выполняет действие или серию действий, результатом чего является формирование информации для других ФО, обеспечивающей продолжение процесса обслуживания. Поточковая диаграмма включает в себя описание всех информационных потоков, необходимых для успешного выполнения процесса обслуживания. Правила вычерчивания потоковых диаграмм для интерфейса V5

Существует несколько основных правил, которые приведены ниже, разработанных с учетом удобства пользования потоковыми диаграммами:

- Прием и передача информации от/к пользователю и информационные потоки изображены горизонтальными стрелками между вертикальными линиями, соответствующими ФО. Отсутствие линии означает отсутствие приема или передачи.

- Информационные потоки поименованы. Имя потока записывается прописными буквами над соответствующей стрелкой; под стрелкой в скобках строчными буквами могут быть записаны важные для понимания потоковых диаграмм пояснения, касающиеся информационного содержания диаграмм (например, имя сигнала, информационного элемента, примитива).

В дополнение к изложенным, существует еще несколько правил, определенных в Рекомендации G.964 (Приложение В, пункт 12):

- На потоковых диаграммах шкала времени направлена вниз и не масштабирована.
- Вертикальные линии соответствуют ФО, в качестве которых используются логические объекты интерфейса V5, обозначаемые следующим образом:

| | |
|-----------|---|
| Порт ТфОП | - национальный интерфейс между терминалом (оборудованием) пользователя ТфОП и сетью доступа |
| ЛОВ5AN | - логический объект ТфОП на стороне сети доступа |
| ЛОВ5LE | - логический объект ТфОП на стороне АТС |
| ЛОНПР | - логический объект национального протокола на стороне АТС |

- Краткое описание физического состояния абонентской линии дается в скобках под стрелкой.
- Диаграммы дают упрощенную информацию о таймерах, участвующих в обмене сообщениями через интерфейс V5.

- Пуск таймера обозначается пунктирной линией, начинающейся от стрелки с описательным именем сообщения. Пересечение пунктирной линии стрелкой обозначает перезапуск таймера. Перечеркнутая окружность, которой заканчивается пунктирная линия, обозначает остановку таймера. Пунктирная линия, заканчивающаяся стрелкой и горизонтальной линией в конце этой стрелки, обозначает срабатывание таймера. Имя таймера пишется заглавными буквами справа от пунктирной линии (примеры условных обозначений работы таймеров представлены ниже на рисунке 5.3).

Линейные сигналы, которые детектируются стороной AN, и примитивы, формируемые логическим объектом национального протокола в LE, преобразуются в сигналы FE, которые передаются в ЛОВ5.

Состояния логических объектов показаны в разрывах вертикальных линий, причем только в тех случаях, когда имеет место изменение состояния ФО

Сообщение SIGNAL ACK, используемое для подтверждения принятого сообщения SIGNAL, может передаваться в любой момент времени, когда ФО находится в состоянии "Путь активен" (но до истечения выдержки времени таймера Tr), и его положение на временной шкале произвольно. Поэтому сообщение SIGNAL ACK на диаграммах, как правило, не показывается.

Существуют две группы таймеров. К первой группе относятся таймеры собственно протоколов, которые определяют временные рамки обработки разных сообщений, передаваемых при создании и разрушении В-соединений. На диаграммах работа этих таймеров иллюстрируется изображениями, размещенными между вертикальными линиями, относящимися к логическому объекту "Порт ТфОП" и LOV5AN на стороне AN, и изображениями, размещаемыми правее линии LOV5LE.

Вторая группа состоит из таймеров общего назначения. Эти таймеры предназначены для контроля выдержек времени национального протокола ТфОП и имеют следующие обозначения:

- Ттс – выдержка времени, необходимая для фильтрации сигнала "трубка снята";
- Ттп – выдержка времени, необходимая для фильтрации сигнала "трубка положена";
- Тво – выдержка времени, необходимая для контроля продолжительности сигнала "ответ АТС";
- Твз – выдержка времени, необходимая для контроля продолжительности сигнала "занято";
- Тпв – выдержка времени, необходимая для контроля продолжительности сигнала "посылка вызова";
- Ткас – выдержка времени, необходимая для управления кассированием монеты.

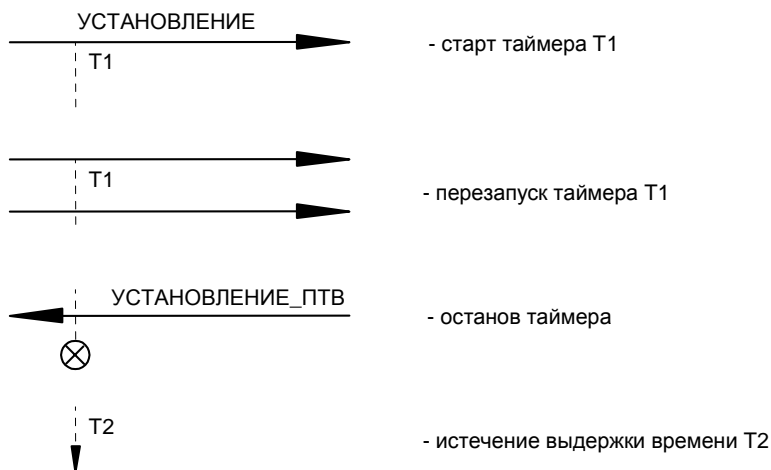


Рисунок 5.3 - Условные обозначения работы таймеров

Построение сценариев сигнализации

Разные сценарии сигнализации при использовании интерфейса V5 строятся на базе алгоритмов национального протокола телефонной сигнализации на абонентском участке (NAT). Необходимо иметь в виду, что абонент не должен чувствовать, как ему обеспечивается доступ к АТС: непосредственным включением или включением через интерфейс V5. В последнем случае должны быть сохранены все сигналы, которые передает и получает абонент, а также все алгоритмы взаимодействия абонента и АТС при установлении и разрушении соединения, включая и возможные нестандартные ситуации, которые предусмотрены в спецификации NAT. Описание сценариев выполняется в форме потоковых диаграмм как для стороны сети доступа (исходящие соединения), так и для стороны АТС (входящие соединения). Пример таких описаний приведен на рисунке 5.4.

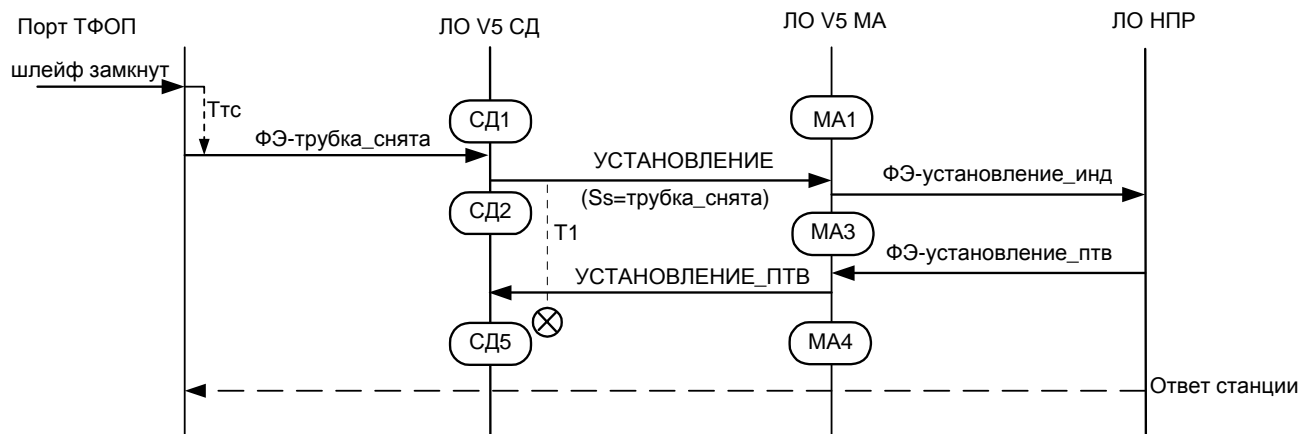


Рисунок 5.4 - Передача сообщений и сигналов FE. Исходящий вызов

Поясним, как строится потоковая диаграмма на примере, приведенном на рисунке 5.4.

1 Вначале определяются логические объекты, взаимодействие которых подлежит описанию. Для нашего примера – это логические объекты: “Порт ТфОП”, “ЛО V5 AN”, “ЛО V5 LE”, “ЛО NAT”.

2 Затем, в соответствии с национальным протоколом, выбирается то действие, которое должен произвести абонент, чтобы установить соединение. В нашем примере абонент снял трубку и поэтому логический объект “Порт ТфОП” сформировал сигнал “FE-subscriber_seizure”, который поступил на вход FSM ТфОП стороны AN.

3 Теперь необходимо воспользоваться таблицей поведения FSM, помещенной в Приложении, и найти в ней в столбце “Входной сигнал” клетку с “FE- subscriber_seizure”. Затем найти столбец с обозначением нулевого состояния FSM. В клетке таблицы на пересечении столбца “AN1” и строки “FE- subscriber_seizure” записаны действия, которые должен произвести FSM, находящийся в нулевом состоянии, при приеме входного сигнала “FE- subscriber_seizure”.

4 Действия: “пуск T1”, передача сообщения ESTABLISH и переход FSM в состояние AN2 отражены на диаграмме.

5 Действия по пунктам 1 – 4 происходят на стороне сети доступа и завершаются передачей сообщения в сторону местной АТС. Для того, чтобы продолжить построение диаграммы, необходимо перейти к таблице поведения FSM на стороне станции. Для этого FSM входным сигналом будет сообщение ESTABLISH, а состоянием – LE1. На пересечении строки с входным сигналом ESTABLISH и столбца LE1 находим перечисление действий FSM. Этими действиями являются передача логическому объекту NAT сигнала “FE-establish_ind” и переход в состояние LE3.

6 После того, как на станции будут успешно выполнены соответствующие процедуры, ЛО NAT передает “FE-establish_ack”, что и показано на диаграмме. Обращаясь к таблице поведения FSM стороны LE, находим на пересечении строки с входным сигналом “FE- establish_ack” и столбца с состоянием LE3, что FSM должен передать в сторону сети доступа сообщение ESTABLISH ACK и перейти в состояние LE4.

7 На стороне сети доступа прием сообщения ESTABLISH ACK в соответствии с таблицей поведения вызывает остановку таймера T1 и переход FSM в состояние AN5 (Путь активен). При этом вызывающий абонент слышит акустический сигнал “Ответ станции”.

Контрольные вопросы

1. Поясните назначение национального мэппинга. Особенности использования сообщений.
2. Метод потоковых диаграмм. Способ описания сценариев вызовов
3. Привести примеры описаний различных сценариев для исходящих и входящих вызовов в соответствии с вариантом задания.

Контрольные задания

Таблица – Варианты заданий

| Сценарий | Номер варианта | | | | | | | | | |
|--|----------------|---|---|---|---|---|---|---|---|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Исходящее соединение | | | | | | | | | | |
| Абонент А кладет трубку до получения стороной AN сообщения ESTABLISH ACK | + | | + | | + | | + | | + | |
| Занятие со стороны А; передача сообщения ESTABLISH несколько раз до получения сигнала “Ответ станции”; отбой А | | + | | + | | + | | + | | + |
| Многократная передача сообщений ESTABLISH (не поступило сообщение ESTABLISH ACK). Отбой А | + | | + | | + | | + | | + | |
| Абонент А при наборе цифры превысил допустимый Межсерийный интервал | | + | | + | | + | | + | | + |
| Срабатывание таймера для прослушивания сигналов “Ответ станции” и “Занято” (абонент А долго не набирает номер) | + | | + | | + | | + | | + | |
| Установление соединения (декадный набор номера). Разговор. Отбой Б. Отбой А | | + | | + | | + | | + | | + |
| Набор номера абонентом А. Получение сигнала “Занято” во время набора; принудительное разъединение со стороны АТС. Абонент А кладет трубку | + | + | | + | | + | | + | | + |
| Абонент А использует таксофон с централизованным управлением кассированием монет (однократная переполюсовка напряжения станционной батареи при ответе Б, однократное восстановление исходной полярности). Сигнал “Занято” в сторону А. Отбой А | | + | + | + | + | + | + | + | + | + |
| Абонент А использует таксофон с централизованным управлением кассированием монет (многократная переполюсовка напряжения при начислении платы) Отбой Б. Отбой А | | + | | | + | | + | | + | |
| Разговорное состояние; абонент А использует кнопку R или набирает цифру “1” | + | | + | | | + | | + | | + |
| Входящее соединение | | | | | | | | | | |
| Ответ абонента после приема вызывного сигнала | + | | | | + | | + | | + | |
| Вызывающий абонент кладет трубку до ответа вызываемого абонента | | + | | + | | | | | | + |
| Передача сообщения ESTABLISH при встречном занятии с преимуществом входящего (междугородного) вызова | + | | + | | + | | | + | | |
| Входящий вызов от АМТС при полуавтоматическом соединении (вызов абонента Б производит оператор АМТС) | | | + | + | | + | + | | + | |

Занятие 6 Протокол управления (CONTROL PROTOCOL)

6.1 Основы протокола управления

Протокол управления является единственным служебным протоколом, который должен присутствовать в обоих интерфейсах V5.1 и V5.2 и который управляет как пользовательскими портами, так и некоторыми общими функциями. Протокол управления позволяет:

- передавать в обе стороны информацию управления, относящуюся к индивидуальным пользовательским портам ТфОП и ISDN (блокировка и разблокировка портов, активизация, деактивизация портов, блокировка и разблокировка D-канала)
- проверять идентификацию и конфигурацию интерфейса V5
- управлять поддержкой общих функций (конфигурацией и реконфигурацией интерфейса)
- производить рестарт протокола ТфОП после отказа.

Протокол управления симметричен, т.е. его процедуры одинаково применимы для обеих сторон интерфейса.

6.2 Спецификация сообщений

В таблице 6.1 приведены сообщения управления портами ТфОП и ISDN, а также сообщения общего управления.

Таблица 6.1 - Сообщения протокола управления

| Тип сообщения |
|--|
| PORT CONTROL (управление портом) |
| PORT CONTROL ACKNOWLEDGE (подтверждение приема сообщения PORT CONTROL) |
| COMMON CONTROL (общее управление) |
| COMMON CONTROL ACKNOWLEDGE (подтверждение приема сообщения COMMON CONTROL) |

Сообщения протокола управления определяются по уже известной схеме (см. Занятие 3).

Каждое сообщение протокола управления содержит:

- обязательные информационные элементы “Дискриминатор протокола”, “Адрес уровня 3”, “Тип сообщения” и
- необязательные информационные элементы, количество которых зависит от типа сообщения.

Адрес уровня 3, предназначен для идентификации порта ISDN/ТфОП или логического объекта, работающего с протоколом управления.

Сообщения протокола идентифицируются информационным элементом “Тип сообщения” в общем заголовке. Предусматривается четыре типа сообщений. Два из них, PORT CONTROL и COMMON CONTROL, являются управляющими сообщениями для портов и общих функций, соответственно. Два других – PORT CONTROL ACKNOWLEDGE и COMMON CONTROL ACKNOWLEDGE – являются подтверждающими. Для сообщений общего управления адрес берется из общего адресного пространства V5. Для сообщений управления портом адрес определяется соответствующим портом ТфОП или ISDN. В заголовке сообщений управления имеет место дублирование информации, поскольку как адрес уровня 3, так и информационный элемент “Тип сообщения” указывают, ориентировано ли сообщение на порт или оно является сообщением общего управления.

Сообщение PORT CONTROL (управление портом). Это сообщение используется сетью доступа или АТС с целью передать встречной стороне информацию управления, которая содержится в информационном элементе “FE управления”.

Сообщение PORT CONTROL ACKNOWLEDGE (подтверждение приема сообщения PORT CONTROL). Это сообщение используется сетью доступа или АТС с целью подтвердить прием сообщения PORT CONTROL и не должно расцениваться как сообщение о выполнении действия, им предписанного.

Сообщение COMMON CONTROL (общее управление). Этим сообщением сеть доступа или АТС передает встречной стороне информацию, необходимую для выполнения общих, не предназначенных для управления портом, функций.

Сообщение COMMON CONTROL ACKNOWLEDGE (подтверждение приема сообщения COMMON CONTROL). Это сообщение используется сетью доступа или АТС с целью подтвердить прием сообщения COMMON CONTROL и не должно расцениваться как сообщение о выполнении действия, им предписанного.

6.3 Структура и кодирование информационных элементов

Дискриминатор протокола

Информационный элемент "Дискриминатор протокола" определен в Занятии 3.

Адрес уровня 3

Цель этого информационного элемента – идентификация порта ISDN или ТфОП, или индикация функции общего управления V5. Он является вторым информационным элементом каждого сообщения и кодируется следующим образом: первый бит 1-ого байта обозначает принадлежность полей адресов либо порту ISDN или функции общего управления V5 (значение "0"), либо порту ТфОП (значение "1"). Значение в поле "Адрес_уровня_3" должно быть либо копией адреса LAPV5-EF, используемого для записи данных сигнализации по D-каналу пользовательского порта ISDN, для которого предназначена информация управления, либо адресом для функции общего управления, который должен быть таким же, как адрес LAPV5-DL для протокола управления, и потому должен иметь десятичное значение 8177.

Тип сообщения

Информационный элемент "Тип сообщения" идентифицирует и протокол, к которому относится сообщение, и функцию этого сообщения. Он является третьим элементом каждого сообщения.

Другие информационные элементы

Как уже указывалось, каждое сообщение содержит обязательные для любого протокола информационные элементы "Дискриминатор протокола", "Адрес уровня 3", "Тип сообщения". Кроме того, в сообщениях присутствуют и информационные элементы, специфические для того или другого протокола, число которых зависит от типа сообщения:

Оценка характеристик работы (Performance_grading)

Причина отказа (Rejection_cause), указывает причину отказа выполнить действие согласно идентификатору функции управления "Верифицировать конфигурацию" или "Перейти на новый вариант".

FE управления (Control_function_element) идентифицирует состояние пользовательского порта ISDN или ТфОП и FE, который нужно передать в сообщении.

Идентификатор функции управления (Control_function_ID) идентифицирует ту функцию общего управления, о которой информирует сообщение.

Вариант (Variant) идентифицирует вариант конфигурации при спецификации значения "Верифицировать_реконфигурацию" в содержимом информационного элемента "Идентификатор функции управления". Элемент "Вариант" идентифицирует для элемента "Идентификатор функции управления" также и вариант текущего набора данных при спецификации значения поля "Вариант_и_идентификатор_интерфейса".

Идентификатор интерфейса (Interface_ID) идентифицирует интерфейс V5.1, через который получен идентификатор функции управления "Запрос_варианта_и_идентификатора_интерфейса".

6.4 FSM логических объектов протокола управления

Логический объект протокола управления представлен следующими FSM:

- FSM управления портами (по одному FSM для каждого порта ТфОП и ISDN);
- FSM общего управления (один FSM).

Процедуры протокола одинаковы для стороны сети доступа и для стороны АТС.

Для **FSM управления портом** по обе стороны интерфейса определены следующие состояния.

"Вне обслуживания" (AN0/LE0). В этом состоянии FSM оказывается при запуске системы, или переходит в него из другого состояния, когда от системы эксплуатационного управления получен MDU-stop_traffic. Вне обслуживания находятся одновременно все FSM управления портами.

"В обслуживании" (AN1/LE1). В это состояние FSM переходит из состояния "Вне обслуживания" при приеме от системы эксплуатационного управления примитива MDU-start_traffic.

"Ожидание подтверждения" (AN2/LE2). В это состояние FSM переходит, когда по звену уровня 2 CONTROL_DL передано сообщение PORT CONTROL.

Для **FSM общего управления** по обе стороны интерфейса определены следующие состояния.

"Вне обслуживания" (AN0/LE0). В этом состоянии FSM оказывается при запуске системы, или переходит в него из другого состояния, когда от системы эксплуатационного управления получен MDU-stop_traffic.

"Обслуживается" (AN1/LE1). В это состояние FSM переходит из состояния "Вне обслуживания" при приеме от системы эксплуатационного управления примитива MDU-start_traffic.

“Ожидание подтверждения” (AN2/LE2). В это состояние FSM переходит, когда по звену уровня 2 CONTROL_DL передано сообщение COMMON CONTROL.

6.5 Семантика сообщений и процедуры

Сообщения PORT CONTROL поддерживают блокировку и разблокировку всех портов ТфОП, ISDN и портов, связанных с арендованными линиями, а также ряд функций, специфических для портов ISDN: активизацию и деактивизацию, индикацию ошибок и рабочих характеристик, блокировку/разблокировку D-канала. В связи с этим в сообщения могут вводиться соответствующие необязательные информационные элементы. Например, сообщение PORT CONTROL содержит информационный элемент “Оценка характеристик работы” (Performance_grading).

Возможна ситуация, когда порт поврежден или находится на техническом обслуживании и, следовательно, должен быть заблокирован. Алгоритм блокировки порта зависит от того, какая сторона интерфейса V5 является ее инициатором.

Сеть доступа не всегда осведомлена о том, занят или нет пользовательский порт, поскольку сигнализация ISDN не интерпретируется и поскольку некоторые порты ISDN могут быть активными, даже когда отсутствует сигнализация или нагрузка. Исчерпывающие сведения о состоянии портов имеются только на АТС. Поэтому когда инициатором блокировки порта является сеть доступа, она запрашивает об этом АТС, передавая свой запрос в сообщении AN/PORT CONTROL: block_request. АТС может, либо немедленно, либо сразу же после освобождения порта, ответить сообщением LE/PORT CONTROL: block, указывающим, что она заблокировала порт. Сеть доступа может затем передать свое сообщение AN/PORT CONTROL: block без опасности нарушить обслуживание вызовов.

Если АТС не отвечает на сообщение AN/PORT CONTROL: block_request в течение некоторого времени, сеть доступа может передать сообщение AN/PORT CONTROL: block с риском нарушить текущие связи пользователей.

АТС не должна передавать запрос блокировки в сеть доступа, поскольку она может блокировать порт без нарушения текущих связей, т.к. она знает об их состоянии. Иницируя блокировку порта, АТС сразу передает сообщение PORT CONTROL: block.

Чтобы разблокировать порт, обе стороны должны передать и принять сообщение PORT CONTROL: unblock. Разблокировка отменяется, если с любой стороны передается сообщение PORT CONTROL: block, или если сеть доступа, приняв сообщение PORT CONTROL: unblock, передает сообщение AN/PORT CONTROL: block_request.

Чтобы предотвратить перегрузку С-канала, содержащего С-пути типа Ds, нужно, чтобы станция могла запросить в сети доступа блокировку сигналов по D-каналу определенного пользовательского порта ISDN. С этой целью АТС передает сообщение LE/PORT CONTROL: D-channel_block (блокировать D-канал), а по окончании перегрузки – сообщение LE/PORT CONTROL: D-channel_unblock (разблокировать D-канал).

Для активизации и деактивизации портов базового доступа ISDN предусматриваются следующие сообщения. Если активизация происходит по инициативе пользователя, то к АТС от сети доступа передается сообщение AN/PORT CONTROL: activation_initiated_by_user (активизация инициирована пользователем). Как правило, АТС отвечает сообщением LE/PORT CONTROL: activate_access (активизировать доступ), которое приводит к передаче соответствующего сигнала от сети к пользователю. Пользователь получает и тактовый синхросигнал, после чего к АТС передается сообщение AN/PORT CONTROL: access_activated (доступ активизирован). Если активизация производится по инициативе АТС, то от нее к сети доступа передается сообщение LE/PORT CONTROL: activate_access.

Деактивизацию доступа АТС запрашивает сообщением LE/PORT CONTROL: deactivate_access (деактивизировать доступ). В ответ к АТС передается сообщение AN/PORT CONTROL: access_deactivated (доступ деактивизирован).

Сообщения COMMON CONTROL обеспечивают проверку согласованности наборов данных по обе стороны интерфейса V5, рестарт протокола ТфОП, а также внесение изменений в конфигурацию на любой стороне интерфейса.

В ряде случаев может понадобиться принудительно вернуть протокол ТфОП в исходное состояние. Для самого протокола ТфОП это более сложная проблема, чем для других протоколов V5, поскольку сообщения этого протокола содержат информацию пользовательских портов, которые не предусматривают общего рестарта самого протокола. Если любая сторона интерфейса инициирует перезапуск протокола ТфОП, она передает сообщение COMMON CONTROL: restart_request. Принимающая сторона должна подтвердить его прием передачей в обратном направлении сообщения COMMON CONTROL ACK: restart_request (т.е. с тем же информационным элементом) и передать системе эксплуатационного управления MDU с тем же информационным элементом. Такая избыточность подтверждений (на уровне 2 плюс квитирование на уровне 3) обусловлена тем, что рестарт протокола ТфОП может повлиять на обслуживание нескольких тысяч пользователей.

Сообщения общего управления, связанные с реконфигурацией интерфейса, содержат информационный элемент "Вариант", в котором указывается номер предлагаемого варианта конфигурации. Сообщения COMMON CONTROL: not_ready_for_reprovisioning (к реконфигурации не готов) и COMMON CONTROL: cannot_reprovision (реконфигурация невозможна) содержат также информационный элемент Rejection_cause (причина отказа). Сообщения COMMON CONTROL: variant_and_interface_ID (вариант и идентификатор интерфейса) содержат информационный элемент "Идентификатор интерфейса".

Для протокола управления определены процедуры двух типов:

- процедуры, относящиеся к порту – для каждого порта ТфОП и ISDN существует свой логический объект протокола управления;
- процедуры общего управления – существует только один логический объект, работающий с этими процедурами.

В дополнение к названным процедурам, предусмотрены процедуры обработки ошибочных ситуаций, применяемые к каждому сообщению, которое получает логический объект протокола управления, перед тем, как будет продолжена его дальнейшая обработка. Эти процедуры, количество которых равно десяти, проверяют структуру, наличие (или отсутствие), и порядок следования информационных элементов в сообщениях. Вначале проверяется присутствие и семантическая корректность дискриминатора протокола, адреса уровня 3, типа сообщения. После этого инициируются (в указанном ниже порядке) процедуры, проверяющие:

- отсутствие повторяющихся обязательных/необязательных информационных элементов;
- факты пропуска обязательных информационных элементов;
- наличие неопознанных (не специфицированных) информационных элементов;
- наличие ошибок в содержании обязательных и необязательных информационных элементов;
- наличие необязательных информационных элементов в количестве, большем, чем это определено для данного сообщения;
- отсутствие таких необязательных информационных элементов, которые в данном сообщении должны присутствовать.

Об обнаруженных ошибках сообщается системе эксплуатационного управления, которая принимает решение о целесообразности дальнейшей обработки сообщения.

Контрольные вопросы

1. Опишите логический объект протокола управления уровня 3.
2. Поясните назначение, использование и структуру сообщений общего управления.
3. Поясните назначение, использование и структуру сообщений управления портами.
4. Назовите сообщения, примитивы и таймеры FSM общего управления и поясните их функциональное назначение.
5. Назовите сообщения, сигналы FE, примитивы и таймеры FSM управления портами и поясните их функциональное назначение.
6. Дайте характеристику процедур протокола. Типы процедур. Процедуры обработки ошибочных ситуаций

ЗАНЯТИЕ 7. Протокол управления трактами (LINK CONTROL PROTOCOL)

7.1 Общие положения

Функциональная модель управления одним ИКМ-трактом представлена на рисунке 7.1.

Протокол управления трактами присутствует только в интерфейсе V5.2, где для каждого ИКМ-тракта (общее число которых может достигать 16) должны обеспечиваться:

- идентификация тракта и определение его состояния на уровне 1;
- блокировка уровня 1 и координированная разблокировка этого уровня средствами эксплуатационного управления;
- верификация непрерывности тракта при его идентификации;
- координации этих функций управления трактом;
- связь между сторонами AN и LE для координации этих функций на обеих сторонах интерфейса V5.2.

Из приведенной модели видно, что FSM уровня 1 ИКМ-тракта, непосредственно связанный с сигналами в интерфейсе, автономно взаимодействует с FSM управления трактом и посредством примитивов MPH-DI и MPH-AI идентифицирует для этого FSM состояние уровня 1. FSM управления трактом координирует процедуры уровня 1, уровня 2 и уровня 3 управления трактом с тем, чтобы в системе эксплуатационного управления всегда была информация о состоянии этого тракта.

Состояние Уровня 1 определяется по обе стороны интерфейса по результатам проверки непрерывности тракта. Из-за того, что значения таймеров, предварительно задаваемые на стороне AN и LE, могут не совпадать, индикация состояния тракта в FSM управления трактом по разные стороны интерфейса может происходить в разное время. Проблемы, возникающие из-за этого, должны учитываться при определении поведения FSM управления трактом.

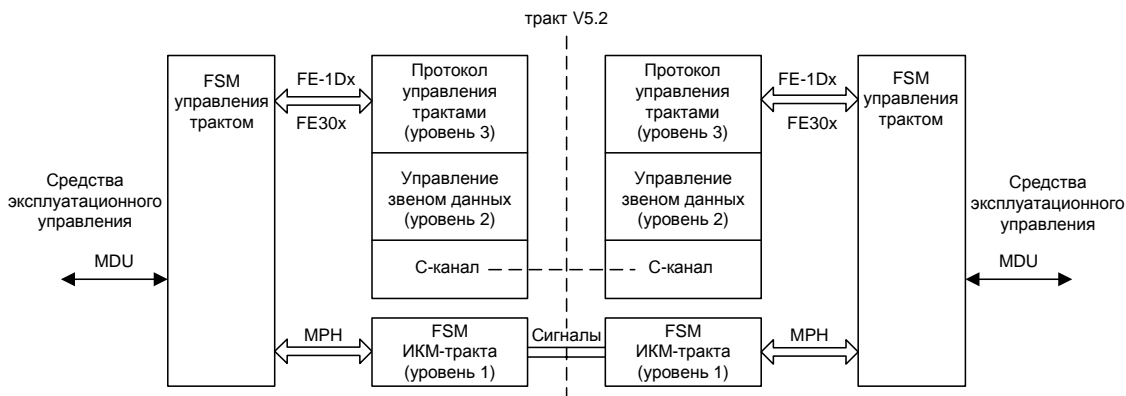


Рисунок 7.1 - Функциональная модель управления трактом интерфейса V5.2

Информационный обмен каждого из FSM управления трактом (на стороне AN и LE) со своим FSM уровня 1 ведется посредством примитивов MPH, а со средствами эксплуатационного управления – с помощью блоков данных MDU. Для связи с FSM управления трактом на другой стороне интерфейса используются сигналы FE, которые транспортируются протоколом уровня 3. Кроме этого, логический объект протокола управления трактом передает MDU к средствам эксплуатационного управления для поддержки процедур обработки ошибок протокола.

В связи с тем, что интерфейс V5.2 содержит несколько ИКМ-трактов, необходима проверка соответствия идентификаторов любого тракта на обеих сторонах интерфейса, для чего предусматривается специальная процедура (рисунок 7.2). Любая из сторон может передать запросить у другой стороны идентификатор тракта. Другая сторона передает в нулевом канальном интервале тракта с адресом, указанным в сообщении, специальный сигнал (биту Sa7 присвоено значение "0"). В случае коллизии запрос идентификации тракта со стороны LE имеет приоритет перед запросом со стороны AN. Эта процедура применима ко всем трактам, включая Первичный и Вторичный тракты протокола защиты. Идентификация тракта может проводиться, в частности, и после реконфигурации интерфейса.

Ее инициатором могут стать и средства эксплуатационного управления. При пуске интерфейса система управления ресурсами или средства эксплуатационного управления могут принять решение не проводить процедуру идентификации тракта.

7.2 События и сигналы FE, относящиеся к FSM управления трактом

Списки FE, относящихся к процедурам управления трактом, приведены в таблице 7.1.

Таблица 7.1 - Сигналы FE управления трактом

| ФЭ | Название | AN | LE | Описание |
|----------|----------------------|----|----|-------------------------------|
| ФЭ-IDReq | идентификация тракта | ←→ | | запрос |
| ФЭ-IDAck | идентификация тракта | ←→ | | подтверждение |
| ФЭ-IDRel | идентификация тракта | ←→ | | запрос освобождения |
| ФЭ-IDRej | идентификация тракта | ←→ | | индикация отказа |
| ФЭ301 | разблокировка тракта | ← | | запрос или индикация |
| ФЭ302 | разблокировка тракта | → | | запрос или индикация |
| ФЭ303 | блокировка тракта | ← | | индикация |
| ФЭ304 | блокировка тракта | → | | индикация |
| ФЭ305 | блокировка тракта | → | | запрос блокировки с задержкой |
| ФЭ306 | блокировка тракта | → | | запрос немедленной блокировки |

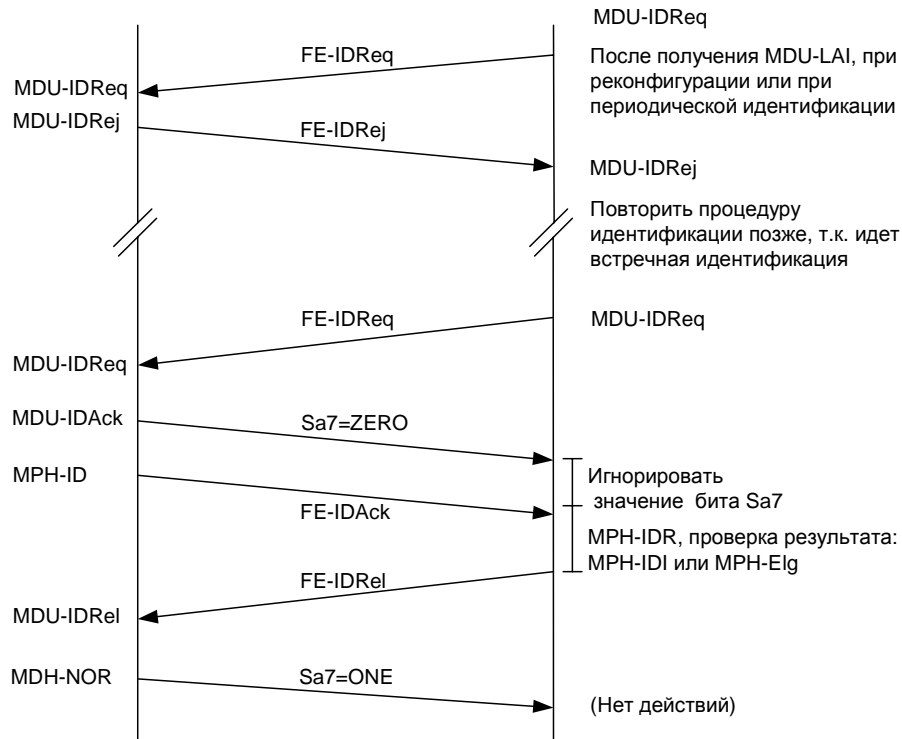


Рисунок 7.2 – Диаграмма процедуры идентификации трактов

7.3 Спецификация сообщений протокола управления трактами

Формат сообщений протокола управления трактами должен соответствовать общей структуре сообщений интерфейса V5 (Занятие 2). Список сообщений приведен в таблице 7.2, а затем описывается структура каждого сообщения.

Таблица 7.2 - Сообщения протокола управления трактами интерфейса V5.2

| Биты | | | | | | | Тип сообщения |
|--|---|---|---|---|---|---|------------------|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
| Кодирование информационного элемента "Тип сообщения" | | | | | | | |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | LINK CONTROL |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | LINK CONTROL ACK |

Сообщение *LINK CONTROL* передает либо AN, либо LE информацию, необходимую для управления одним трактом интерфейса, а сообщение *LINK CONTROL ACK* информирует AN или LE о необходимости немедленно подтвердить прием сообщения *LINK CONTROL*.

Сообщения протокола управления трактами имеют структуру, соответствующую общей структуре сообщений интерфейса V5, но не содержат необязательных информационных элементов. Среди обязательных информационных элементов протокола присутствуют уже описанные в предыдущих занятиях "Дискриминатор протокола", "Адрес уровня 3" и "Тип сообщения". Четвертым обязательным информационным элементом является 3-х байтовый элемент "Функция управления трактом".

Информационный элемент "Адрес уровня 3" используется для идентификации того тракта 2048 кбит/с, которому предназначается сообщение. Он является вторым информационным элементом сообщения. Для любого тракта поле "Адрес_Уровня_3" должно иметь то же самое значение, что и поле идентификатора тракта в информационном элементе идентификации канального интервала, используемом протоколом ВСС.

Информационный элемент "Функция управления трактом" идентифицирует функцию управления трактом, которую активизирует сообщение.

7.4 FSM управления трактом

Состояния FSM протокола управления трактами на сторонах AN и LE можно разделить на две группы: *Рабочее* и *Нерабочее*.

В группу *Нерабочее* входят 5 следующих состояний:

- отказ тракта (0.1)
- отказ тракта и блокировка (0.2)
- блокировка тракта (1.0)
- местная разблокировка тракта (1.1)
- дистанционная разблокировка тракта (1.2)

Это разделение на состояния позволяет упростить координацию двух FSM управления трактом в процессе разблокировки и гарантировать подтверждение разблокировки обеими сторонами перед переходом в рабочее состояние.

Блоки данных MDU-LUBI и MDU-LBI используются обоими FSM управления трактом для передачи средствам эксплуатационного управления информации о переходе тракта в рабочее и в нерабочее состояние, соответственно.

На стороне AN разблокировка тракта, как и его отложенная блокировка, требует подтверждения. Немедленная блокировка производится без подтверждения.

В группу *Рабочее* входят 3 следующих состояния:

- тракт в работе (2.0)
- дистанционная идентификация тракта (2.1)
- местная идентификация тракта (2.2)

Все три состояния с точки зрения управления трактом рассматриваются как рабочие. За инициирование любого действия, зависящего от состояния тракта, несут ответственность средства эксплуатационного управления.

FSM на стороне AN и на стороне LE отражает состояния только одного тракта интерфейса V5.2. Для адекватного отображения условий с отказом уровня 1 тракта и с блокировкой тракта введено состояние "комбинированных условий" 0.2. Если при наличии отказа на уровне 1 от средств эксплуатационного управления поступает запрос блокировки, то на встречную сторону дается соответствующая индикация, и происходит переход FSM в состояние 0.2. После восстановления уровня 1 тракта FSM управления трактом переходит в состояние блокировки, при этом средствами эксплуатационного управления передается MDU-LBI для координации разблокировки, если это потребуется.

Эта же процедура используется и для координированного восстановления после нарушения работы средств эксплуатационного управления, например, из-за утраты возможности передавать управляющие данные вследствие отказа уровня 1 или потери данных о статусе этих средств после перезапуска.

При наличии отказа уровня 1 запрос разблокировки любой стороной рассматривается как нарушение работы средств эксплуатационного управления, и FSM управления трактом должен в этом случае перейти в состояние 0.2, чтобы начать координированную разблокировку после восстановления уровня 1. То же самое рекомендуется для случая, когда в условиях отказа уровня 1 FSM принимает FE-IDReq.

Начнем рассмотрение с состояний FSM управления трактом на стороне AN

Нерабочее (AN_Link0 и AN_Link1): тракт находится в состоянии отказа на уровне 1 или в состоянии блокировки. Следовательно, физические C-каналы этого тракта не могут использоваться для организации в них логических C-каналов или находиться в резерве. Ни один канальный интервал не может использоваться как несущий канал для обслуживания вызова. Запрос идентификации такого тракта отклоняется.

“Отказ тракта” (AN0.1)

FSM уровня 1 дал индикацию устойчивой потери работоспособности уровня 1 (с помощью примитива MPH-DI).

“Отказ тракта и блокировка” (AN0.2)

FSM уровня 1 дал индикацию (примитив MPH-DI) устойчивой утраты работоспособности уровня 1 из-за блокировки тракта, или из-за действий, инициированных средствами эксплуатационного управления или стороной LE и связанных с нарушением согласованной работы FSM управления трактом на разных сторонах интерфейса.

“Блокировка тракта” (AN1.0)

Тракт находится в нерабочем состоянии, и ни одна из сторон не начала разблокировку.

“Местная разблокировка тракта” (AN1.1)

AN инициировала разблокировку тракта, передав FE302, и ожидает подтверждения от LE.

“Дистанционная разблокировка тракта” (AN1.2)

LE инициировала разблокировку тракта, передав FE301, и ожидает подтверждения от AN.

Примечание: Состояния AN1.1 и AN1.2 обеспечивают возможность синхронизации разблокировки трактов. Сторона AN может находиться в этих состояниях неопределенно долго.

“Тракт в работе” (AN2.0)

С точки зрения функций управления трактом и функций уровня 1, тракт готов выполнять свои функции. Может потребоваться проведение процедуры идентификации с целью верифицировать непрерывность тракта.

“Дистанционная идентификация тракта” (AN2.1)

Сторона LE инициировала идентификацию тракта и FSM уровня 1 (после подтверждения средствами эксплуатационного управления) получил указание присвоить значение “0” биту идентификации тракта Sa7. AN ожидает сигнал FE об окончании идентификации.

“Местная идентификация тракта” (AN2.2)

Средства эксплуатационного управления AN инициировали идентификацию тракта и ожидают либо FE-IDAck от LE, либо, если он уже был принят, индикацию идентификации тракта или невозможности идентификации тракта (в ответ на MPH-IDR). Прием FE-IDAck или результата попытки идентифицировать тракт ведет к передаче соответствующей информации средствами эксплуатационного управления и к окончанию процедуры идентификации.

Теперь рассмотрим состояния FSM управления трактом на стороне LE.

Нерабочее (LE_Link0 и LE_Link1): тракт находится в состоянии отказа на уровне 1 или в состоянии блокировки. Следовательно, физические C-каналы этого тракта не могут быть использованы для организации в них логических C-каналов или в качестве резервных. Ни один канальный интервал этого тракта не может использоваться как несущий канал для обслуживания вызова. Запрос идентификации этого тракта отклоняется.

“Отказ тракта” (LE0.1)

FSM уровня 1 дал индикацию устойчивой потери работоспособности уровня 1 (с помощью примитива MPH-DI).

“Отказ тракта и блокировка” (LE0.2)

FSM уровня 1 дал индикацию (примитив MPH-DI) устойчивой утраты работоспособности уровня 1 из-за блокировки тракта, или из-за действий, инициированных средствами эксплуатационного управления или стороной LE и связанных с нарушением согласованной работы FSM управления трактом на разных сторонах интерфейса.

“Блокировка тракта” (LE1.0)

Тракт находится в нерабочем состоянии, и ни одна из сторон не начала разблокировку.

“Местная разблокировка тракта” (LEk1.1)

LE инициировала разблокировку, передав FE301, и ожидает подтверждения от AN.

“Дистанционная разблокировка тракта” (LE1.2)

AN инициировала разблокировку, передав FE302, и ожидает подтверждения от LE. Причем состояния LE1.1 и LE1.2 обеспечивают возможность синхронизации разблокировки. Сторона LE может находиться в этих состояниях неопределенно долго.

“Тракт в работе” (LE2.0)

С точки зрения функций управления трактом и функций уровня 1, тракт готов выполнять свои функции. Может потребоваться проведение идентификации с целью верифицировать непрерывность тракта. Решения об этом принимают средства эксплуатационного управления.

“Дистанционная идентификация тракта” (LE2.1)

Сторона AN инициировала идентификацию тракта и, после подтверждения средствами эксплуатационного управления, FSM уровня 1 получил указание присвоить значение “0” биту идентификации тракта Sa7. Сторона LE ожидает сигнал FE об окончании идентификации.

“Местная идентификация тракта” (LE2.2)

Средства эксплуатационного управления LE инициировали идентификацию тракта и ожидают либо сигнал FE-IDAck от AN, либо, если он уже был принят, индикацию идентификации (или невозможности идентификации) тракта. Прием FE-IDAck или результата идентификации тракта влечет за собой передачу соответствующей информации средствам эксплуатационного управления и окончание процедуры идентификации.

7.5 FSM протокола управления трактами

В связи с тем, что протокол управления трактами является симметричным, FSM сторон AN и LE имеют одинаковое число и семантику состояний и процедуры, которые можно применять как со стороны AN, так и со стороны LE. Определены следующие состояния.

“Вне обслуживания” (AN0/LE0)

В это состояние FSM переходит сразу после запуска или после приема MDU-stop_traffic от средств эксплуатационного управления.

“В обслуживании” (AN1/LE1)

Переход в это состояние происходит тогда, когда FSM протокола управления, находясь в состоянии “Вне обслуживания”, принимает от средств эксплуатационного управления примитив MDU-start_traffic.

“Ожидание LINK CONTROL ACK” (AN2/LE2)

Переход в это состояние происходит тогда, когда сообщение LINK CONTROL было передано на 2-ой уровень для передачи на другую сторону интерфейса.

7.6 Таймеры протокола управления трактами

Таймер протокола управления трактами на сторонах AN и LE всего один и составляет 1 секунду. Причина пуска таймера - передача сообщения LINK CONTROL, а его остановка при приеме сообщения LINK CONTROL ACK.

7.7 Процедуры протокола управления трактами

Протокол управления трактами симметричен, т.е. его процедуры в равной степени применимы к сторонам AN и LE. Логический объект протокола управления трактами существует для каждого ИКМ-тракта.

Поскольку процедуры в один и тот же момент времени могут обрабатывать только одно сообщение, сигнал FE или примитив MDU-CTRL, необходимо предусмотреть для логического объекта каждого тракта в AN и LE память для хранения дальнейших сообщений (сигналов, примитивов) для передачи их на противоположную сторону в порядке их приема от FSM. Они будут передаваться, когда соответствующий FSM перейдет в состояние 1.

Каждое сообщение, принятое логическим объектом, перед его дальнейшей обработкой обязательно проходит процедуры проверки ошибок в структуре (защиты от ошибочных ситуаций). К этим процедурам относятся следующие семь процедур:

- проверка наличия/отсутствия ошибок в обязательных информационных элементах “Дискриминатор протокола”, “Адрес уровня 3” и “Тип сообщения”;

- проверка присутствия повторяющихся информационных элементов;
- проверка отсутствия обязательного информационного элемента;
- проверка наличия неопознанных информационных элементов;
- проверка наличия ошибок в содержании обязательных информационных элементах.

При обнаружении ошибки или несоответствия в информационных элементах, логический объект протокола управления трактами во всех случаях должен передать примитив MDU-link_control (protocol_error_indication) средствам эксплуатационного управления. Все сообщения, содержащие обнаруженные ошибки или несоответствия, игнорируются. Исключением является наличие неопознанных информационных элементов. В этом случае после передачи примитива MDU-link_control (protocol_error_indication) из сообщения удаляются неопознанные элементы, и продолжается его дальнейшая обработка.

После прохождения названных проверок могут выполняться остальные процедуры, перечисляемые ниже.

Процедура индикации начала обслуживания трафика должна выполняться, когда логический объект, находясь в состоянии **“Вне обслуживания” (AN0)**, получает от средств эксплуатационного управления примитив MDU-start_traffic. При этом логический объект должен перейти в состояние **“В обслуживании” (AN1)**.

Процедура индикации окончания обслуживания трафика должна выполняться, когда логический объект, находясь в состоянии **“В обслуживании” (AN1)** или в состоянии **“Ожидание LINK CONTROL ACK” (AN2)**, получает от средств эксплуатационного управления примитив MDU-stop_traffic. При этом логический объект должен перейти в состояние **“Вне обслуживания” (AN0)**.

Процедуры, обеспечивающие взаимодействие логических объектов по обе стороны интерфейса между собой и со средствами эксплуатационного управления должны подчиняться следующим общим правилам.

Когда логический объект протокола управления трактами находится в состоянии **“В обслуживании”** (или в состоянии **“Ожидание LINK CONTROL ACK”**) и получает сообщение LINK CONTROL, он должен передать сообщение LINK CONTROL ACK на противоположную сторону, а также FE с адресом уровня 3 в FSM протокола управления, содержащие то же значение информационного поля **“Функция_управления_трактом”**, что и в сообщении LINK CONTROL.

Когда логический объект протокола управления трактами находится в состоянии **“В обслуживании”** и получает сигнал FE от FSM протокола управления, он должен передать на противоположную сторону сообщение LINK CONTROL с информацией этого сигнала и с адресом уровня 3, запустить таймер и перейти в состояние **“Ожидание LINK CONTROL ACK”**.

Взаимодействие со средствами эксплуатационного управления на обеих сторонах интерфейса происходит только через FSM управления трактом. Таковы общие правила взаимодействия логических объектов интерфейса между собой и с названными средствами при помощи процедур протокола.

Процедуры блокировки и разблокировки трактов имеют некоторые особенности: блокировка может выполняться либо немедленно, либо с задержкой, а разблокировка должна быть координированной.

Процедура немедленной блокировки тракта запрашивается стороной AN, а сторона LE дает (или не дает) разрешение. При этом, если в тракте имеются активные C-каналы, средства эксплуатационного управления стороны LE должны, используя протокол защиты, перевести логические C-каналы в резервные физические C-каналы, затем освободить все коммутируемые соединения в этом тракте, перевести полупостоянные и некоммутируемые соединения на другие тракты этого же V5.2-интерфейса и передать FE303 (Link bloc indication) стороне AN. Если сторона LE не дает разрешения, она передает стороне AN сигнал FE301 (Link unbloc indication).

Сторона LE может инициировать немедленную блокировку (выполнив все необходимые действия), передав стороне AN сигнал FE303 (Link bloc indication).

Если сторона LE не дала разрешения, а стороне AN это совершенно необходимо (например, произошел отказ), то она может немедленно заблокировать тракт, передав при этом стороне LE сигнал FE306 (Link bloc non-deferred).

Процедуру отложенной блокировки тракта сторона AN запрашивает путем передачи стороне LE сигнала FE305 (Link bloc deferred). В этом случае средства эксплуатационного управления стороны LE не должны занимать свободные канальные интервалы этого тракта и должны дождаться освобождения занятых канальных интервалов. После этого необходимо обеспечить защиту логических C-каналов и всех полупостоянных и некоммутируемых соединений (если это требуется) и передать стороне AN сигнал FE303 (Link bloc indication).

Если обеспечить защиту логических С-каналов невозможно, то LE не дает разрешения и передает стороне AN сигнал FE301 (Link unblock indication).

Процедура координированной разблокировки является полностью симметричной. Запрос разблокировки всегда требует подтверждения от противоположной стороны. Для гарантии координированной разблокировки в FSM управления трактом обеих сторон введены два состояния: **“Местная разблокировка тракта”** (AN/LE 1.1) и **“Удаленная разблокировка тракта”** (AN/LE 1.2).

Если сторона LE начинает разблокировку, то FSM управления трактом передает стороне AN сигнал FE301 (Link unblock request) и переходит в состояние LE 1.1. Получив этот сигнал, FSM управления трактом на стороне AN переходит в состояние AN1.2 и передает соответствующий примитив средствам эксплуатационного управления AN.

Если указанные средства согласны, они сообщают об этом FSM, который передает запрос FE302 (Link unblock request) стороне LE и примитив индикации средствам эксплуатационного управления, после чего переходит в состояние **“Тракт в работе”** (AN2.0). FSM стороны LE, получив этот FE в состоянии LE1.1, переходит в состояние **“Тракт в работе”** (LE2.0) и передает примитив индикации в средствам эксплуатационного управления LE.

Инициатива разблокировки может исходить и от средств эксплуатационного управления стороны AN, но если те же средства на стороне LE не дают согласия на разблокировку, они передают примитив “Link block indication”, и разблокировка не происходит.

Принципы функционирования *процедуры идентификации трактов* иллюстрирует рисунок 7.2.

Контрольные вопросы

1. Опишите функциональную модель протокола управления трактами.
2. Составьте описание логического объекта протокола управления трактами.
3. Назовите сообщения, сигналы FE, примитивы и таймеры FSM управления трактом.
4. Назовите сообщения, сигналы FE и таймеры конечного автомата FSM протокола управления трактами.
5. Поясните функциональное назначение FE, примитивов и таймеров FSM протокола управления трактами.
6. Дайте характеристику процедур протокола. Типы процедур. Процедуры обработки ошибочных ситуаций.

Занятие 8 Протокол назначения несущих каналов (BCC PROTOCOL)

8.1 Основы протокола BCC

Протокол назначения несущих каналов (BCC – Bearer Channel Connection) предоставляет АТС средства, позволяющие ей запрашивать у сети доступа создание и разрушение соединений между определенными пользовательскими портами и определенными канальными интервалами ИКМ-трактов интерфейса V5.2. Иными словами, протокол BCC обеспечивает управление соединениями между пользовательскими портами сети доступа и несущими каналами интерфейса V5.2. Такие соединения удобно называть *В-соединениями*.

Протокол реализует функции назначения/отмены назначения несущих каналов интерфейса V5.2 и функции проверки В-соединений, выполняемые независимыми процессами. Один пользовательский порт может обслуживаться одновременно более чем одним процессом.

Процесс назначения. Это – процедура протокола BCC, определяющая действия сети доступа и АТС с целью назначить определенное количество несущих каналов в интерфейсе V5.2 для определенного пользовательского порта. Процесс имеет ограниченное время жизни и завершается либо по окончании назначения, либо если попытка назначения оказалась неудачной. В последнем случае соответствующая информация передается менеджеру ресурсов в АТС.

Процесс отмены назначения. Это – процедура протокола BCC, определяющая действия сети доступа и АТС с целью отменить назначение определенного количества несущих каналов в интерфейсе V5.2 для определенного пользовательского порта. Процесс имеет ограниченное время жизни и завершается либо после отмены назначения, либо если попытка отменить назначение оказалась неудачной. В последнем случае соответствующая информация передается менеджеру ресурсов в АТС.

Процесс проверки. Это – процедура протокола ВСС, определяющая действия сети доступа и АТС с целью проверить идентификацию несущего канала в интерфейсе V5.2 и его подключение к пользовательскому порту (т.е. наличие В-соединения). Процесс завершается после приема результатов проверки со стороны АН. Результаты проверки передаются менеджеру ресурсов в LE.

Для идентификации процесса ВСС ему присваивается ссылочный номер, кодируемый двоичным кодом.

Типы В-соединений

Протокол ВСС поддерживает В-соединения трех типов:

а) соединения в АТС и в интерфейсе V5.2, создаваемые оперативно для обслуживания каждого вызова ТфОП и ISDN с концентрацией трафика на стороне сети доступа;

б) соединения, создаваемые в АТС оперативно для каждого вызова, но использующие в сети доступа постоянные соединения, которые закрепляются в интерфейсе V5.2 за линиями ТфОП и ISDN с высокой нагрузкой (например, линиями УАТС) и за такими линиями, блокировка которых в сети доступа или в интерфейсе V5.2 недопустима (например, за линиями охранной сигнализации);

в) полупостоянные соединения, устанавливаемые в сети доступа и в АТС для поддержки услуг полупостоянных арендованных линий.

Для В-соединений типа (а) протокол ВСС используется в начале и в конце обслуживания каждого вызова, а управление соединением абонента ТфОП или ISDN производится со стороны АТС. Для В-соединений типов (б) и (в) процедуры протокола ВСС проводятся под контролем системы эксплуатационного управления АТС (например, через интерфейс Q_{LE}), которая не назначает для линий канальных интервалов или ИКМ-трактов интерфейса V5, но должна получать об этом информацию. Для В-соединений этих типов система эксплуатационного управления АТС специфицирует пользовательский порт ТфОП или канал порта ISDN.

Интерфейс V5.2 имеет возможность создавать и разрушать многоканальные В-соединения $n \times 64$ кбит/с (n может иметь значение от 1 до 30) для поддержки услуг с использованием каналов Н0 и Н12 и будущих широкополосных услуг. Такие В-соединения могут быть всех трех типов. Каналы Н0 и Н11 DSS1 должны быть “невидимы” для интерфейса V5 и поддерживаться прозрачно как n соединений каналов 64 кбит/с. Мультимедийные соединения также должны быть “невидимы” для интерфейса V5 и обрабатываться прозрачно как несколько независимых соединений.

Протокол ВСС поддерживает только соединения между пользовательскими портами сети доступа (или канальными интервалами портов ISDN) и канальными интервалами интерфейса V5.2. Соединения “порт АН – порт АН” протоколом не поддерживаются. (Это не исключает возможность устанавливать такие соединения полностью под управлением сети доступа, например, когда эта сеть изолирована от АТС в результате отказа интерфейса V5.2.)

Функциональная модель протокола ВСС приведена на рисунке 4.1

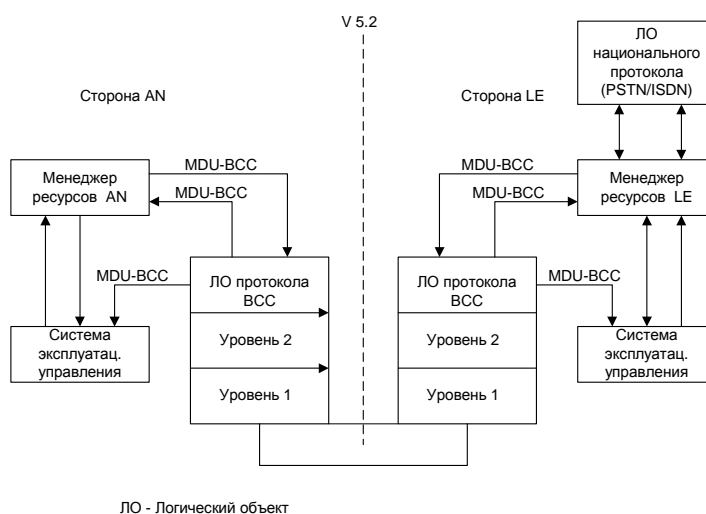


Рисунок 8.1 - Функциональная модель интерфейса протокола ВСС

8.2 Сообщения протокола ВСС

Полная спецификация каждого сообщения содержит:

- а) краткое описание сообщения;
- б) таблицу, отражающую содержание сообщения, где перечислены информационные элементы в порядке их появления в сообщении (этот порядок используется для сообщений всех типов).

Для каждого информационного элемента в таблице указывается:

- направление, в котором этот элемент может быть передан, т.е. от сети доступа к АТС, от АТС к сети доступа или оба направления;
- обязательность ("М") или необязательность ("О") присутствия элемента в сообщении;
- длина информационного элемента в байтах.

Ниже приводятся краткие описания сообщений протокола ВСС.

ALLOCATION (назначение).

Это сообщение используется стороной LE для того, чтобы назначить для определенного пользовательского порта один или несколько несущих каналов интерфейса V5.2. Если назначение несущих каналов производится для одного В-канала порта ISDN, LE должна указать тот канальный интервал в интерфейсе, который будет использоваться этим В-каналом. Для поддержки ISDN-услуг "nх64 кбит/с" сообщение ALLOCATION позволяет для n В-каналов порта ISDN назначить соответствующего размера блок канальных интервалов интерфейса V5.2.

ALLOCATION COMPLETE (назначение выполнено)

Это сообщение используется стороной AN для индикации стороне LE успешного назначения несущих каналов для пользовательского порта.

ALLOCATION REJECT (в назначении отказано)

Это сообщение используется стороной AN для индикации стороне LE отказа в назначении несущих каналов для пользовательского порта.

DE-ALLOCATION (отмена назначения)

Это сообщение используется стороной LE для запроса отменить на стороне AN назначение пользовательскому порту одного или нескольких несущих каналов интерфейса V5.2. Это сообщение позволяет также отменить назначение блока несущих каналов для поддержки высокоскоростных (nх64 кбит/с) услуг.

DE-ALLOCATION COMPLETE (назначение отменено)

Это сообщение используется стороной AN для передачи стороне LE информации о том, что отмена назначения несущих каналов пользовательскому порту успешно завершена.

DE-ALLOCATION REJECT (в отмене назначения отказано)

Это сообщение используется стороной AN для индикации стороне LE того, что отмена назначения несущих каналов пользовательскому порту не выполнена.

AUDIT (проверка)

Это сообщение используется стороной LE, чтобы запросить у стороны AN информацию, которой не достаёт для идентификации В-соединения 64 кбит/с. Сообщение позволяет запросить такую информацию, как идентификация пользовательского порта вместе с идентификацией канала порта ISDN, или проверить такую имеющуюся на стороне AN информацию, как идентификация канального интервала интерфейса V5.2.

AUDIT COMPLETE (проверка выполнена)

С помощью этого сообщения AN передает LE результат проверки В-соединения на основе частичных данных о нем, полученных в сообщении AUDIT, то есть либо информацию, идентифицирующую В-соединение полностью, либо сведения о том, что такого В-соединения не существует.

AN FAULT (неисправность в сети доступа)

Этим сообщением AN информирует LE о том, что из-за внутреннего отказа в AN нарушено одно определенное В-соединение 64 кбит/с, и обеспечивает LE информацией, необходимой ей для идентификации всех данных об этом соединении.

AN FAULT ACKNOWLEDGE (подтверждение приема AN FAULT)

Передача со стороны LE этого сообщения только подтверждает, что было получено сообщение AN FAULT, но не означает, что были предприняты какие-либо действия.

PROTOCOL ERROR (ошибка протокола)

Этим сообщением AN информирует LE о том, что в принятом сообщении содержится ошибка.

8.3. Таймеры протокола BCC

Характеристики и условия работы таймеров протокола BCC приведены в таблице 8.1. Таймеры используются логическими объектами протокола на стороне AN или LE.

Таблица 8.1 – Параметры и условия работы таймеров протокола BCC

| Таймер | Выдержка времени | Состояние | Причина пуска | Нормальная остановка | Первое срабатывание | Второе срабатывание |
|--|---------------------------|------------------|----------------------------------|--|---|--|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Tbcc1 | От 500 до 1500 мс (Прим.) | LEBcc0 LEBcc1 | Передача сообщения ALLOCATION | Прием сообщения ALLOCATION COMPLETE, ALLOCATION REJECT или MDU-BCC (De-allocation request) | Повторная передача ALLOCATION и перезапуск таймера Tbcc1 | Окончание процесса назначения и извещение системы управления ресурсами в LE |
| Tbcc2 | 2 с | LEBcc1 LEBcc2 | Передача сообщения DE-ALLOCATION | Прием сообщения DE-ALLOCATION COMPLETE, DE-ALLOCATION REJECT | Повторная передача DE-ALLOCATION и перезапуск таймера Tbcc2 | Окончание процесса отмены назначения и извещение системы управления ресурсами в LE |
| Tbcc3 | 2 с | LEBcc0 LEBcc3 | Передача сообщения DE-ALLOCATION | Прием сообщения DE-ALLOCATION COMPLETE, DE-ALLOCATION REJECT | Повторная передача DE-ALLOCATION и перезапуск таймера Tbcc3 | Окончание процесса отмены назначения и извещение системы управления ресурсами в LE |
| Tbcc4 | От 500 до 1500 мс (Прим.) | LEBcc0 LEBcc4 | Передача сообщения AUDIT | Прием сообщения AUDIT COMPLETE | Повторная передача AUDIT и перезапуск таймера Tbcc4 | Окончание процесса проверки и извещение системы управления ресурсами в LE |
| Tbcc5 | От 500 до 1500 мс (Прим.) | ANBcc0 ANBcc1 | Передача сообщения AN FAULT | Прием сообщения AN FAULT ACKNOWLEDGE | Повторная передача AN FAULT и перезапуск таймера Tbcc5 | Окончание процесса, вызванного сбоем AN, и извещение системы управления ресурсами в LE |
| Примечание – Эти значения могут заранее переопределяться с шагом 100 мс, но должны быть одинаковы у всех трех таймеров | | | | | | |

8.4 Описание состояний логического объекта протокола BCC

Состояния логического объекта BCC на стороне AN

РАБОЧЕЕ (ANBcc0). Протокол BCC на стороне AN является ведомым со стороны LE, т.е. процессы протокола BCC (назначение, отмена назначения и проверка) инициируются стороной LE. Для всех этих процессов существует только одно состояние логического объекта BCC на стороне AN – “Рабочее”.

ОТКАЗ В AN (ANBcc1). Логический объект протокола BCC переходит в это состояние после передачи сообщения AN FAULT. Сторона AN ожидает сообщение AN FAULT ACKNOWLEDGE до тех пор, пока не сработает таймер Tbcc5.

Состояния логического объекта BCC на стороне LE

“НУЛЕВОЕ” (LEBcc0). Логический объект находится в этом состоянии, когда еще не были запущены процедуры назначения или отмены назначения несущих каналов.

“ОЖИДАНИЕ НАЗНАЧЕНИЯ” (LEBcc1). Логический объект переходит в это состояние после передачи сообщения ALLOCATION. Сторона LE ожидает приема сообщения ALLOCATION COMPLETE или сообщения ALLOCATION REJECT до срабатывания таймера Tbcc1. В этом состоянии возможно получение внутреннего запроса отмены назначения.

“ОТМЕНА НАЗНАЧЕНИЯ” (LEBcc2). Логический объект переходит в это состояние после передачи сообщения DE-ALLOCATION в состоянии “ОЖИДАНИЕ НАЗНАЧЕНИЯ” (LEBcc1) и ожидает приема сообщения DE-ALLOCATION COMPLETE или DE-ALLOCATION REJECT до срабатывания таймера Tbcc2.

“ОЖИДАНИЕ ОТМЕНЫ НАЗНАЧЕНИЯ” (LEBcc3). Логический объект переходит в это состояние после передачи сообщения DE-ALLOCATION и ожидает приема сообщения DE-ALLOCATION COMPLETE или DE-ALLOCATION REJECT до срабатывания таймера Tbcc3.

“ОЖИДАНИЕ РЕЗУЛЬТАТА ПРОВЕРКИ” (LEBcc4). Логический объект переходит в это состояние после передачи сообщения AUDIT. Сторона LE ожидает приема сообщения AUDIT COMPLETE до срабатывания таймера Tbcc4.

8.5 Взаимодействие протоколов BCC и ТфОП/ISDN

Сценарии взаимодействия протоколов BCC и ТфОП могут быть описаны при помощи потоковых диаграмм. На рисунках 8.2, 8.3, 8.4, 8.5 такие диаграммы представлены для нормальных процедур обработки вызова и отбоя.

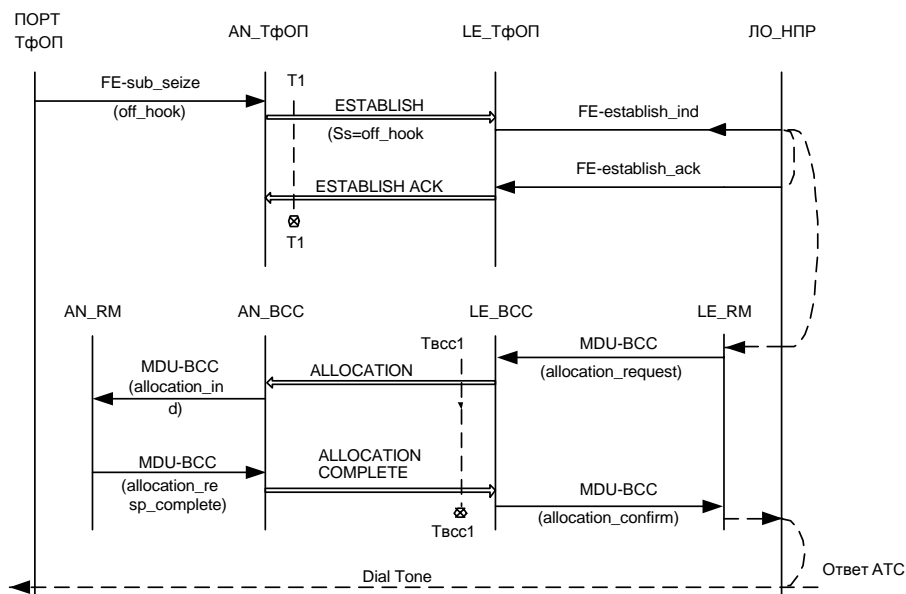


Рис. 8.2. Исходящий вызов. Нормальная процедура

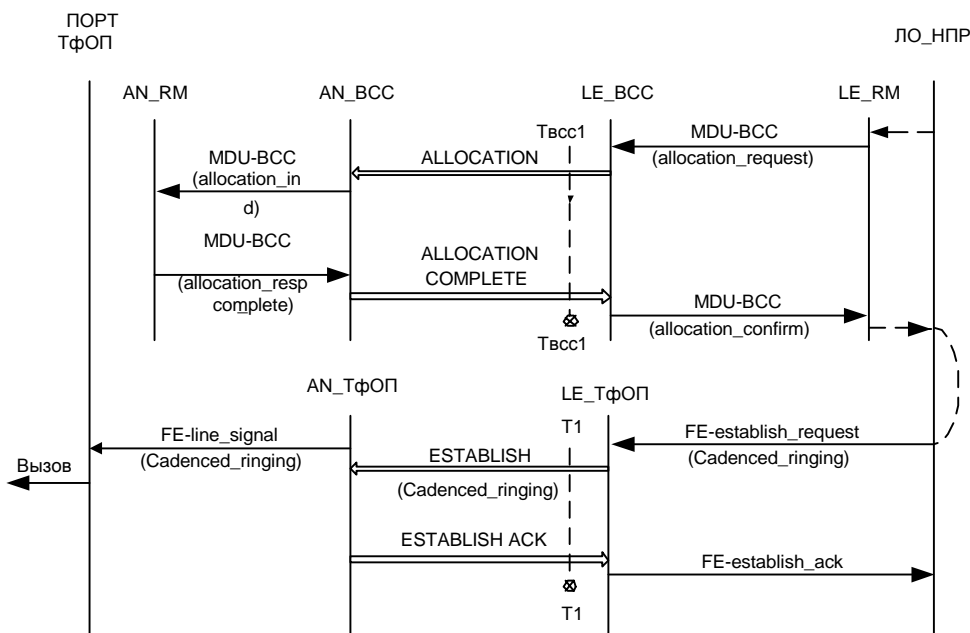


Рис. 8.3. Входящий вызов. Нормальная процедура

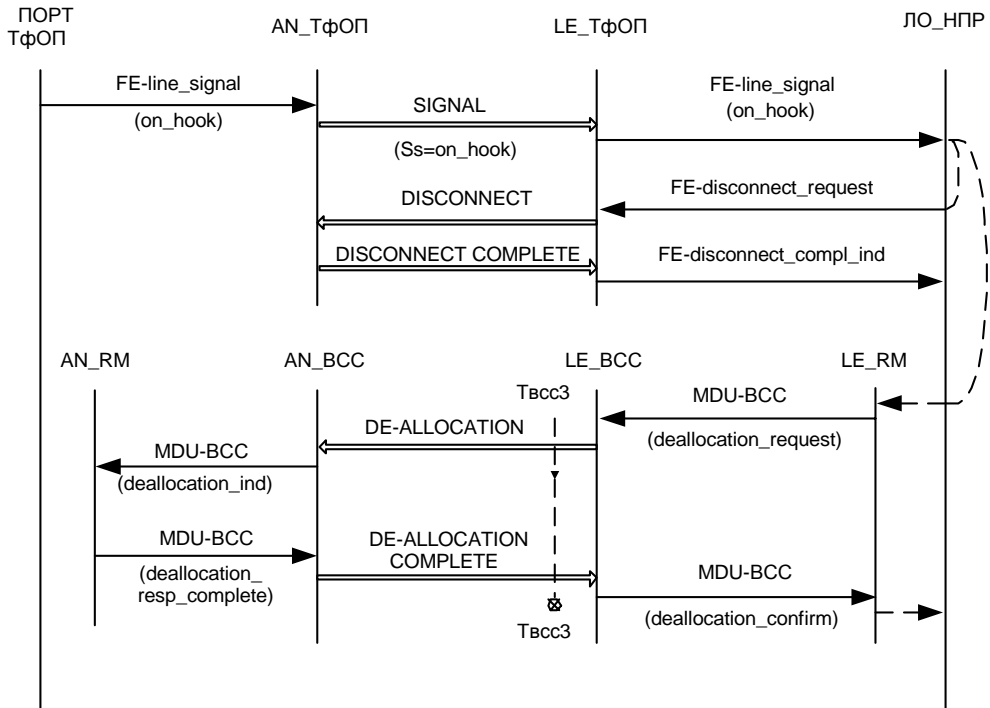


Рис. 8.4. Отбой абонента А. Нормальная процедура

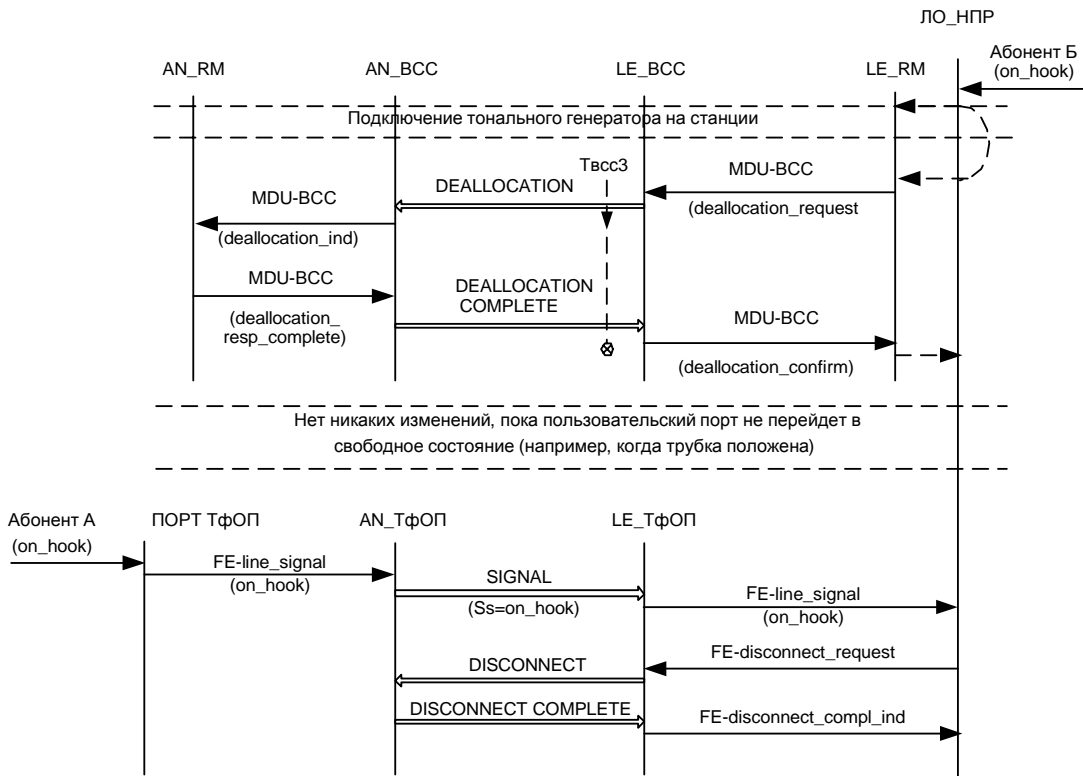


Рис. 8.5. Отбой со стороны абонента Б. Нормальная процедура

На рисунке 8.7 приведена диаграмма для случая встречного занятия, когда приоритет имеет станция. Это, как правило, делается с той целью, чтобы не препятствовать успешному завершению обслуживания вызова, который является междугородним и поэтому уже использовал значительный ресурс сети связи.

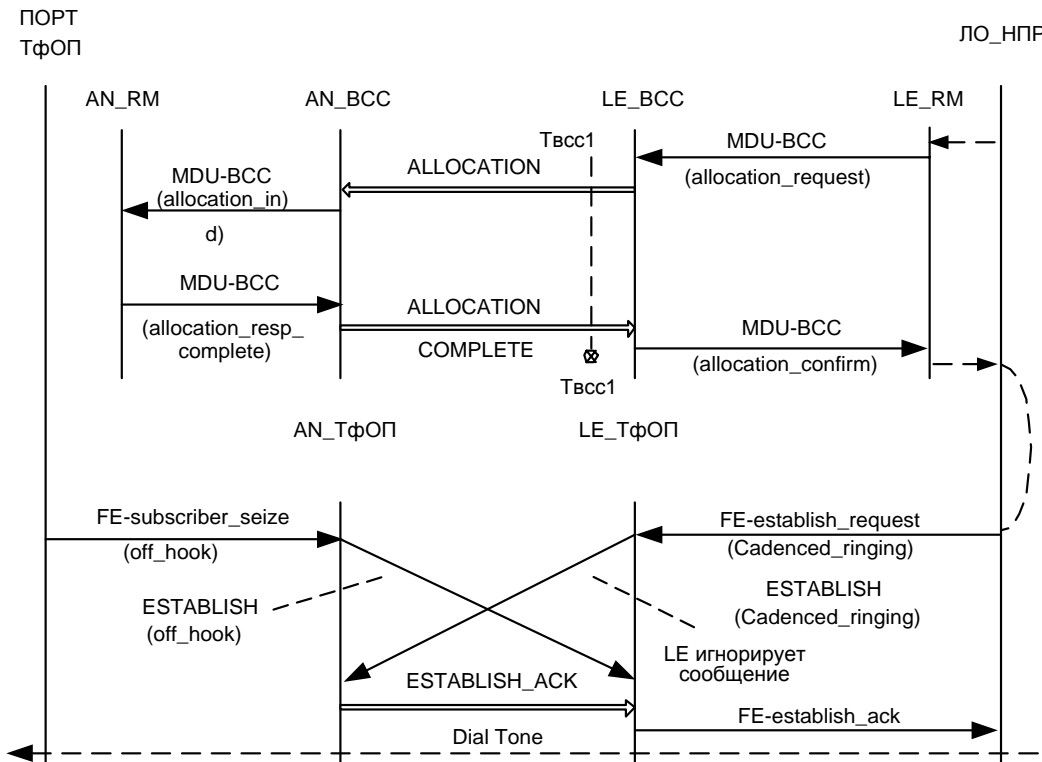


Рис. 8.6. Встречное занятие. Приоритет входящего вызова, LE_ISDN порт

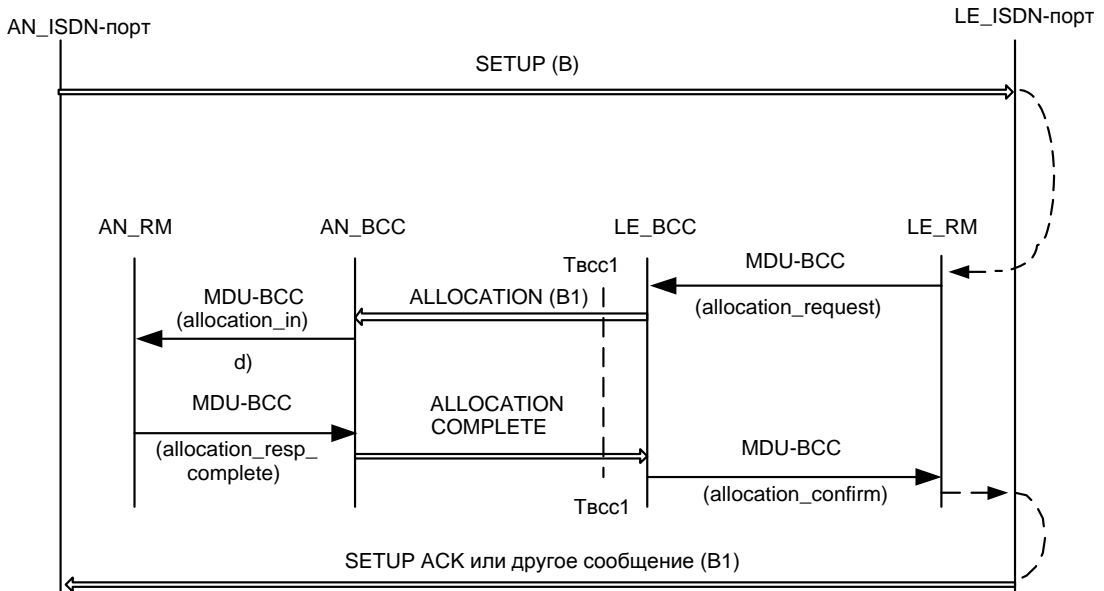


Рис. 8.7. Исходящий ISDN – вызов. Нормальная процедура

На рисунках 8.8, 8.9, 8.10 приведены диаграммы взаимодействия для нормальных процедур. Подобным образом можно описать взаимодействие и для других, более сложных ситуаций.

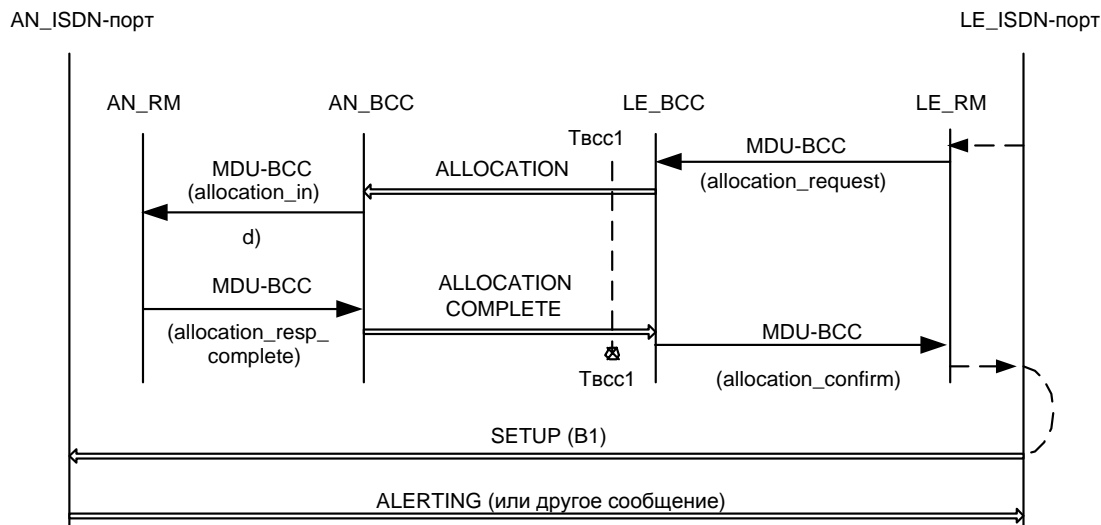


Рис. 8.8. Входящий вызов. Невозможен согласованный выбор В-канала (например, в случае пассивной конфигурации с общей шиной)

Контрольные вопросы

- 1 Опишите функциональную модель и охарактеризуйте основные процессы протокола BCC.
- 2 Составьте описание логического объекта протокола BCC.
- 3 Назовите сообщения, FE, примитивы и таймеры FSM протокола BCC и дайте его определение.
- 4 Поясните функциональное назначение FE, примитивов и таймеров FSM логического объекта протокола BCC. Поясните содержание и использование таблиц, описывающих поведение FSM.
- 5 Поясните назначение, порядок использования и структуру сообщений протокола BCC.
- 6 Дайте характеристику процедур протокола. Типы процедур. Процедуры обработки ошибочных ситуаций .
- 7 Дайте характеристику процедур назначения и отмены назначения несущих каналов интерфейса V5.2 (нормальная и исключительные процедуры).
- 8 Опишите взаимодействие протокола BCC и протокола ТфОП (потокные диаграммы).
- 9 Опишите взаимодействие протокола BCC и протокола DSS1 (потокные диаграммы).

Занятие 9 Протокол защиты (PROTECTION PROTOCOL)

9.1 Основы протокола защиты

Один интерфейс V5.2 может содержать до 16 трактов 2048 кбит/с. В соответствии с архитектурой протокола и структурой мультиплексирования один С-путь может нести информацию, относящуюся к нескольким ИКМ-трактам (несвязанный режим переноса). Поэтому, отказ С-пути может нарушить предоставление услуг большому количеству пользователей. Это в особенности относится к информации протокола BCC, протокола управления и протокола управления трактами – в случае отказа С-пути будет нарушено обслуживание всех пользовательских портов.

Чтобы повысить надежность интерфейса V5.2, предусмотрены процедуры защиты С-путей, обеспечивающие их переключение из отказавшего тракта в другой тракт. Процедуры используются для защиты всех активных С-каналов. Это относится также и к С-пути самого протокола защиты.

Протокол не защищает несущие каналы и не предусматривает реконфигурацию интерфейса при отказе ИКМ-трактов, которым они принадлежат. Соединения пользователей, проходящие по каналам отказавшего тракта, будут разрушены. Поскольку вероятность таких отказов невелика, это считается допустимым.

Первое, что вызывает необходимость защиты С-путей, это отказ тракта 2048 кбит/с. Протокол защищает также от устойчивых отказов в любом из звеньев данных, организованных для протокола управления, протокола управления трактами, ВСС, ТфОП или протокола защиты. Кроме того, постоянно контролируются флаги во всех физических С-каналах (активных и резервных) для защиты от ошибок, которые не всегда обнаруживаются уровнем 1. Если отказ обнаружен в резервном С-канале, об этом уведомляются средства эксплуатационного управления, и, следовательно, логический С-канал не будет переключен на неисправный физический С-канал.

При наличии в интерфейсе V5.2 всего одного ИКМ-тракта протокол защиты не может быть реализован, и защита логического С-канала не обеспечивается.

После переключения на резерв все звенья данных LAPV5, на которые повлиял отказ, за исключением звеньев данных протокола защиты (16-й канальный интервал Первичного и Вторичного трактов), должны быть организованы заново.

В результате процедуры переключения на резерв, кадры уровня 2 и/или сообщения уровня 3 могут быть потеряны. Обработка такой ситуации возлагается на логические объекты соответствующего протокола уровня 3.

Организация физических и логических С-каналов

Размещение С-путей в логических С-каналах, а также первоначальное размещение логических С-каналов в физических С-каналах, должно обеспечиваться как стороной LE, так и стороной AN.

Два С-пути протокола защиты всегда организуются в 16-м канальном интервале Первичного и Вторичного ИКМ-трактов и не должны переключаться процедурой защиты.

С-пути протокола ВСС, протокола управления и протокола управления трактами сначала создаются в 16-м канальном интервале Первичного тракта, а тот же интервал Вторичного тракта используется как резервный для их защиты.

В одном и том же физическом С-канале при размещении в кадрах сообщений протокола защиты им дается более высокий приоритет, чем сообщениям других протоколов. Решение принимается на основании адреса функции обрамления, который для сообщений протокола защиты является уникальным (EFaddr = 8179).

Каждый интерфейс V5.2, содержащий более одного тракта 2048 кбит/с, должен иметь группу защиты 1 и, если это возможно, группу защиты 2. Группу защиты 1 всегда образуют 16-е канальные интервалы Первичного и Вторичного ИКМ-трактов. Таким образом, в группе защиты 1 используются:

$N_1 = 1$ (логический С-канал)

$K_1 = 1$ (резервный С-канал).

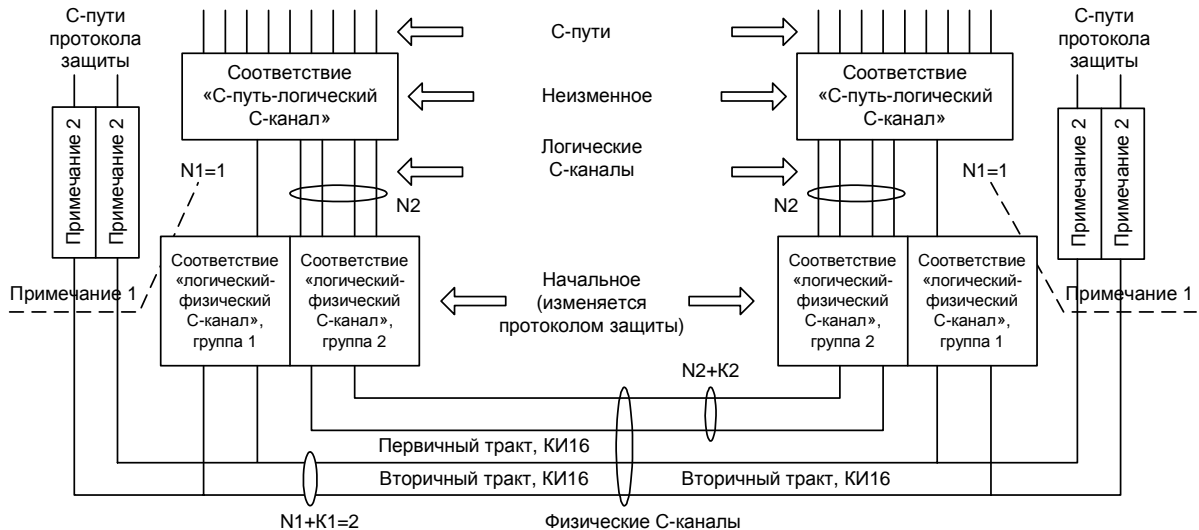
Если предусматривается группа защиты 2, то ее образуют N_2 логических С-каналов (и организованные в них С-пути) и группа, содержащая K_2 резервных С-каналов:

$$1 \leq K_2 \leq 3,$$

$$1 \leq N_2 \leq (3 \times L - 2 - K_2),$$

где L – количество ИКМ-трактов в интерфейсе V5.2. Значение K_2 должно быть не меньше максимального числа физических С-каналов в любом из трактов интерфейса без учета 16-х канальных интервалов Первичного и Вторичного трактов. Применение этого правила гарантирует, что в случае отказа одного ИКМ-тракта все активные С-каналы будут защищены.

Размещение С-путей в логических и физических С-каналах показано на рисунке 9.1.



Примечания

1. С-пути протокола управления, протокола управления трактами и протокола ВСС плюс (опционально) другие С-пути.
2. Размещение С-путей по физическим С-каналам.

Рисунок 9.1 - Размещение С-путей в логических и физических С-каналах

Переключение на резерв

Переключение на резерв может быть инициировано либо средствами эксплуатационного управления LE или AN автономно при обнаружения отказа или при блокировке тракта, либо оператором через интерфейсы Q_{LE} и Q_{AN} . Для группы защиты 1 средства эксплуатационного управления не должны допускать переключения, инициированного оператором.

Ведущей при переключении на резерв является сторона LE, и именно она должна назначить для логического С-канала другой физический С-канал.

Сторона AN может запросить переключение любого логического С-канала в любое время. Если переключение инициировал оператор AN через интерфейс Q_{AN} , то он может запросить, чтобы оно было произведено на предпочтительный для AN физический С-канал. Сторона LE должна дать на это разрешение. Если стороной AN определен канал не указан (это происходит всегда, когда обнаружен отказ в AN, и переключение инициируют ее средства эксплуатационного управления), то резервный С-канал выбирают средства эксплуатационного управления стороны LE.

Сторона AN может отклонить команду переключения, переданную со стороны LE, если по какой-то причине не может ее выполнить. Если AN или LE не могут выполнить переключение, уведомление об этом передается через интерфейсы Q_{LE} и Q_{AN} с указанием причины.

Переключение на резерв выполняется на уровне логического С-канала, т.е. размещение С-путей в логическом С-канале при переключении не изменяется. Поэтому все С-пути, размещенные в этом логическом С-канале, переключаются на один и тот же резервный физический С-канал.

Управление ресурсами С-канала после отказа

В отношении управления имеющимися ресурсами должны выполняться следующие правила.

Если переключение инициируется средствами эксплуатационного управления LE или AN автономно при обнаружении неисправности, то активные С-каналы не должны использоваться для защиты переключаемого логического С-канала. Этот же принцип должен применяться и при переключении, инициированном через интерфейс Q_{AN} .

Запрос поместить отказавший логический С-канал в активном С-канале может дать только оператор LE (через интерфейс Q_{LE}). В этом случае стороне AN должна быть передана специальная команда, получив которую, AN должна отменить прежнее размещение логических С-каналов в физическом канале и поместить в него логический С-канал, который должен быть защищен. К «изъятому» из физического С-канала логическому С-каналу применяется обычная процедура защиты, и так делается до тех пор, пока имеются доступные ресурсы.

Этот способ позволяет оператору LE вручную защитить протокол с более высоким приоритетом (например, протокол ТфОП) при множественных отказах трактов интерфейса даже в тех ситуациях, когда автономная процедура защиты оказалась неуспешной из-за недостатка ресурсов.

Для защиты логического С-канала выбирается и используется доступный резервный С-канал в той же группе защиты. Если доступно более одного резервного С-канала, менеджер ресурсов должен действовать по следующим правилам. В первую очередь используются все доступные резервные С-каналы, организованные в 16-м канальном интервале, затем – в 15-м, и, наконец, – в 31-м. Как только тракт восстанавливается, все физические С-каналы этого тракта становятся резервными С-каналами (переключение необратимо).

Для сохранения ресурсов протокола защиты при отказе тракта 2048 Кбит/с менеджер ресурсов должен пользоваться теми же правилами. Если не все логические С-каналы могут быть размещены в физических С-каналах, оператор сети извещается об этом через интерфейсы Q_{LE} и Q_{AN} .

В случае серьезной неисправности (например, при отказе и Первичного, и Вторичного трактов) имеется возможность изменить приоритеты вручную при помощи процедур реконфигурации интерфейса. Приоритеты, установленные вручную в начальной конфигурации, могут быть изменены после переключения на резерв.

Потеря С-путей протокола защиты, протоколов ВСС, управления и управления трактами из-за отказов и Первичного, и Вторичного трактов интерфейса V5.2 может быть восстановлена только реконфигурацией с переводом их на другой тракт.

Все переключения на резерв должны выполняться последовательно: любое переключение может быть начато только после того, как будет завершено переключение, начатое ранее.

Одно сообщение протокола защиты должно вызывать только одно действие (например, перевод логического С-канала X в резервный физический С-канал Y).

Запрос защитного переключения от AN или команда переключения со стороны LE могут быть подтверждены или отклонены только логическим объектом того же ранга. Сообщение о том, что запрос отклоняется, не должно содержать никакого альтернативного предложения. После того как запрос переключения отклонен, любая сторона может инициировать новое переключение.

Функции контроля и обнаружения ошибок

Главное событие, от которого требуется защита, – это отказ ИКМ-тракта. После приема от FSM протокола управления трактами в AN или LE примитива MDU-DI средства эксплуатационного управления AN или LE должны произвести автономное переключение на резерв всех активных С-каналов отказавшего тракта (ITU-T G.965 п.16.1). Чтобы обнаружить отказ С-канала и инициировать автономное переключение на резерв, в дополнение к контролю уровня 1 используются две другие функции. Это функции мониторинга флагов и мониторинга звена данных (уровень 2).

Флаги должны непрерывно контролироваться и в активном, и в резервном С-каналах. Если в физическом С-канале за одну секунду не было принято ни одного флага, этот канал считается не работающим, а средствам эксплуатационного управления дается индикация ошибки (error indication). Эта индикация означает то же, что прием примитива MDL-RELEASE-INDICATION от FSM звена данных (LAPV5-DL.). Пока флаги отсутствуют, такая индикация дается периодически с интервалом в одну секунду. Если в течение одной секунды в физическом С-канале будет обнаружен хотя бы один флаг, этот канал будет считаться работающим.

Контроль звена данных производится AN и LE для логических С-каналов, содержащих все С-пути (т.е. протокола защиты, управления, управления трактами, ВСС и ТфОП), общее звено данных которых оканчивается в AN.

Если от одного из звеньев LAPV5-DL средствами эксплуатационного управления принят примитив MDL-RELEASE-INDICATION, то физический С-канал, содержащий данный С-путь, считается не работающим, и названные средства должны запустить процедуру переключения на резерв организованного в нем логического С-канала.

Если средствами эксплуатационного управления снова получен примитив MDU-RELEASE-INDICATION из-за отказа того С-пути, который уже был причиной переключения на резерв, то названные средства не должны инициировать новое переключение, не получив до этого примитив MDL-ESTABLISH-INDICATION или MDL-ESTABLISH-CONFIRM. Это означает, что FSM звена данных, в котором находится отказавший С-путь, должен сначала (хотя бы раз) перейти в состояние, соответствующее режиму передачи кадров с подтверждением. Отсутствие такого перехода означает, что произошел внутренний отказ, после которого восстановление звена с помощью механизма защиты V5 невозможно, и средства эксплуатационного управления должны предпринять соответствующие действия.

Функциональная модель протокола защиты

Функциональная модель протокола защиты показана на рисунке 9.2. Для обмена информацией между логическими объектами протокола защиты в AN и LE используются два звена данных, организованных в 16-х канальных интервалах Первичного и Вторичного трактов. Любое сообщение уровня 3 должно передаваться по обоим звеньям. Объект уровня 3, принявший сообщения по обоим звеньям, должен обработать то из них, которое он принял первым, и игнорировать такое же сообщение, принятое вторым. Для того чтобы отличить сообщение, которое принято впервые, от сообщения, которое уже было принято по другому звену данных, всем сообщениям присваиваются порядковые номера.

Адреса EFaddr и соответствующий DLaddr для протокола защиты в 16-х канальных интервалах Первичного и Вторичного тракта должны иметь одинаковое значение.

Обнаружив отказ, требующий перехода на резерв, средства эксплуатационного управления LE или AN инициируют переключение, используя блоки управляющих данных MDU.

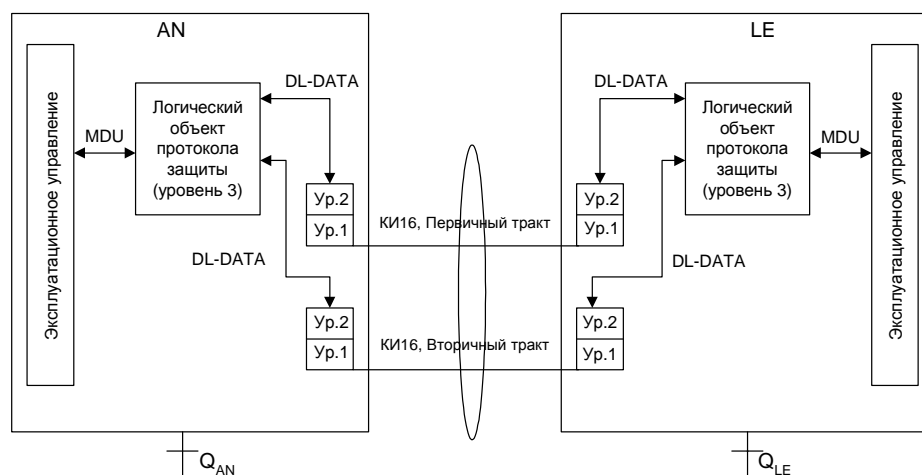


Рисунок 9.2 - Функциональная модель протокола защиты

9.2 Состояния логических объектов протокола защиты

Состояния в AN

“Нулевое” (SOAN0). Переключение не было инициировано ни стороной AN, ни стороной LE.

“Переключение запрошено AN” (SOAN1). Средства эксплуатационного управления AN запросили переключение предназначенным для этого примитивом MDU.

“Переключение инициировано LE” (SOAN2). Со стороны LE получено сообщение SWITCH-OVER COM или OS-SWITCH-OVER COM. Средства эксплуатационного управления AN должны решить, возможно ли переключение.

Состояния в LE.

“Нулевое” (SOLE0) Переключение не было инициировано ни стороной AN, ни стороной LE.

“Переключение инициировано LE” (SOLE1) Средства эксплуатационного управления LE запросили переключение предназначенным для этого примитивом MDU.

“Переключение запрошено AN” (SOLE2) Со стороны AN было получено сообщение SWITCH-OVER_REQ. Средства эксплуатационного управления LE должны решить, возможно ли это переключение.

9.3 Спецификация сообщений протокола защиты

Сообщения протокола защиты определяются по уже известной схеме (см. Занятие 3).

Сообщение SWITCH-OVER REQ используется стороной AN для запроса переключить логический C-канал на определенный физический C-канал. Сообщение содержит предложение поместить отказавший логический C-канал в указанный физический C-канал.

Сообщение SWITCH-OVER COM используется стороной LE для того, чтобы инициировать переключение логического C-канала на определенный физический C-канал. Сообщение содержит команду поместить указанный логический C-канал в указанный резервный физический C-канал.

Сообщение OS-SWITCH-OVER COM используется стороной LE для того, чтобы инициировать переключение логического C-канала на определенный физический C-канал по запросу оператора через интерфейс Q_{LE} . Сообщение несет команду поместить указанный логический C-канал в указанный физический C-канал.

Сообщение SWITCH-OVER ACK на стороне AN подтверждает переключение логического C-канала на указанный физический C-канал в результате выполнения команды переключения от LE.

Сообщение SWITCH-OVER REJECT информирует встречный логический объект о том, что переключение не может быть выполнено.

Сообщение PROTOCOL ERROR информирует сторону LE об обнаружении в принятом сообщении ошибки протокола и указывает ее причину.

Сообщение RESET SN COM информирует встречный логический объект о том, что имеет место несогласованность переменных (номеров сообщений) на передающей и принимающей сторонах, и что всем этим переменным должно быть присвоено значение "0".

Сообщение RESET SN ACK информирует встречный логический объект о присвоении всем переменным значения "0".

9.4 Процедуры протокола защиты

Протокол защиты – функциональный протокол. Запрос переключения от AN и команду переключения от LE встречный логический объект явно подтверждает сообщениями SWITCH-OVER COM или SWITCH-OVER ACK соответственно. Получение подтверждения контролируется таймерами. После первого срабатывания таймера при отсутствии подтверждения сообщение, которое должно быть подтверждено, передается повторно. При вторичном срабатывании таймера средствами эксплуатационного управления дается индикация ошибки, и FSM протокола защиты переходит в состояние "NULL", не передавая сообщение еще раз. Далее ответственность за необходимые действия по техобслуживанию несут средства эксплуатационного управления.

На стороне LE эти средства контролируют, в какой физический C-канал защиты поместил логический C-канал, получая информацию либо самостоятельно от менеджера ресурсов протокола защиты (если отказ обнаружила LE), либо через интерфейс Q_{LE} от оператора LE.

Средства эксплуатационного управления стороны AN могут инициировать переключение, обнаружив внутренний отказ, или по запросу оператора OS через интерфейс Q_{AN} . Оператор может указать, какой резервный C-канал предпочтительно использовать.

Получив примитив MDU-Protection (switch-over com) или MDU-Protection (OS-switch-over com), названные средства AN проверяют наличие доступных ресурсов, необходимых для переключения. При положительном результате этой проверки к LE передается сообщение SWITCH-OVER ACK, а при отрицательном – сообщение SWITCH-OVER REJECT. Если проблемы с переключением будут обнаружены позже какой-либо из сторон, должно быть инициировано новое переключение.

Если переключение на резерв инициировано оператором через интерфейс Q_{LE} , и оператор решил, что требуется перехват активного C-канала, средства эксплуатационного управления LE должны известить об этом логический объект протокола защиты с помощью примитива MDU-Protection (OS-switch-over com). Перехват не применяется в группе защиты 1.

Контрольные вопросы

1. Опишите функциональную модель протокола защиты.
2. Составьте описание логического объекта протокола защиты.
3. Назовите сообщения, сигналы FE, примитивы и таймеры FSM протокола защиты и дайте его определение.
4. Поясните функциональное назначение сигналов FE, примитивов и таймеров FSM логического объекта протокола защиты. Поясните содержание и использование таблиц, описывающих поведение FSM.
5. Поясните назначение, порядок использования и структуру сообщений протокола защиты.
6. Дайте характеристику процедур протокола. Типы процедур. Процедуры обработки ошибочных ситуаций

Занятие 10 Тестирование протоколов интерфейса V5

10.1 Основные принципы

Тестируемая конфигурация сети доступа приведена на рисунке 10.1. Оборудование сети доступа (AN) подключается к цифровой АТС (LE) посредством нескольких (более 3-х) ИКМ-трактов.

Со стороны AN подключается несколько телефонных аппаратов, как с многочастотным, так и с импульсным способом передачи сигналов набора номера, а также аппараты ISDN.

Для организации тестирования приведенной на рис.10.1 конфигурации интерфейса V5 необходимо задать некоторые начальные установки.

Поскольку число тестируемых абонентских портов невелико, для поддержки сигнализации можно задействовать общий С-путь, использующий КИ16. Так как спецификации V5 предусматривают возможность помещать С-пути для поддержки сигнализации ТфОП и сигнализации ISDN в разных КИ тракта, некоторые тестовые сценарии могут использовать для этих целей КИ15 и КИ31. Размещение С-путей в канальных интервалах указывается в соответствующей таблице.

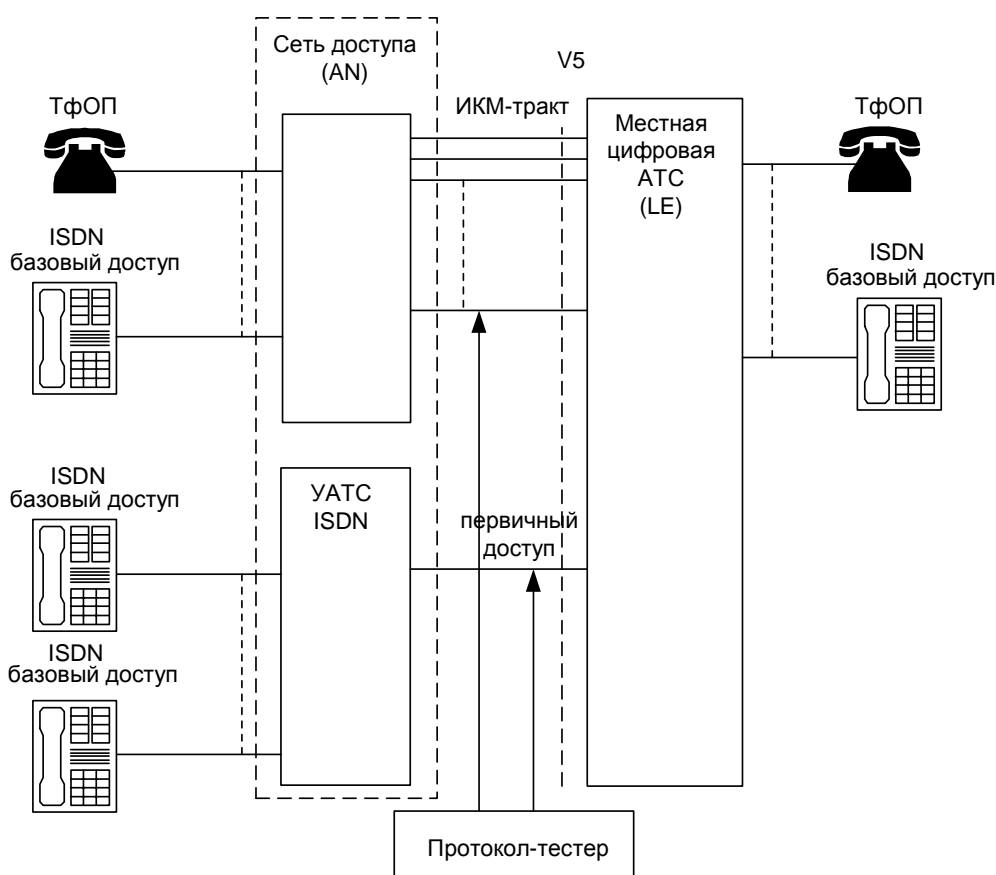


Рисунок 10.1 - Тестируемая конфигурация

10.2 Тестовые сценарии старта (категория А) интерфейса V5

При старте интерфейса V5 выполняются следующие действия:

- звенья данных для протокола защиты организуются в КИ16 Первичного и Вторичного трактов интерфейса (только в случае интерфейса V5.2);
- в Первичном тракте организуются звенья данных для протокола управления, протокола управления трактами, протокола ВСС и протокола ТфОП (для протокола управления трактами и протокола ВСС – только в случае интерфейса V5.2);

- проверяются “Variant” и “Interface_ID”;
- стартует процедура идентификации тракта (V5.2);
- инициируется процедура рестарта протокола ТфОП;
- инициируется процедура разблокировки пользовательских портов.

В связи с тем, что оборудование на одной стороне интерфейса стартует независимо от оборудования на другой его стороне, запросы логических объектов одного ранга, а также последовательности действий при выполнении стартовых процедур производятся параллельно. Поэтому на рисунках 10.2 - 10.4 указано «AN или LE».



Рисунок 10.2 – Организация звена данных (уровень2)

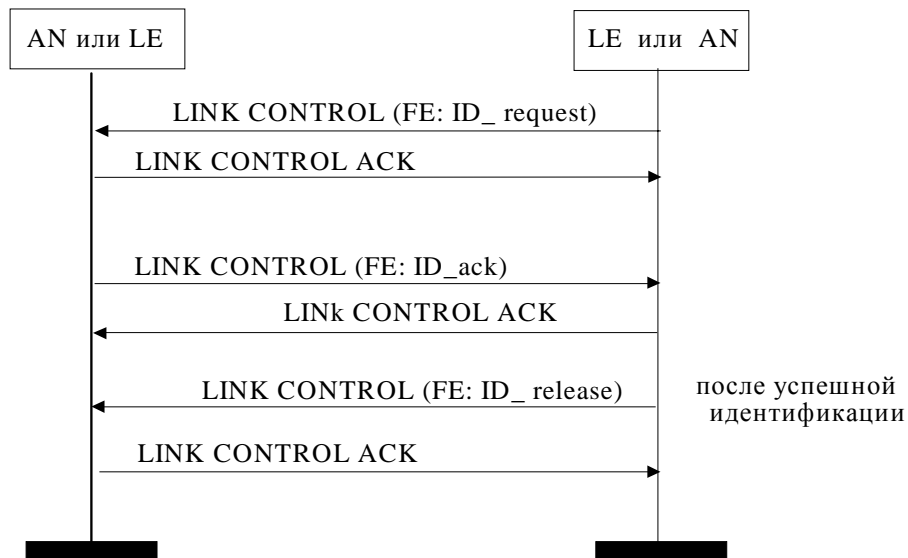


Рисунок 10.3 - Проверка : “Variant ” и “Interface_ID”

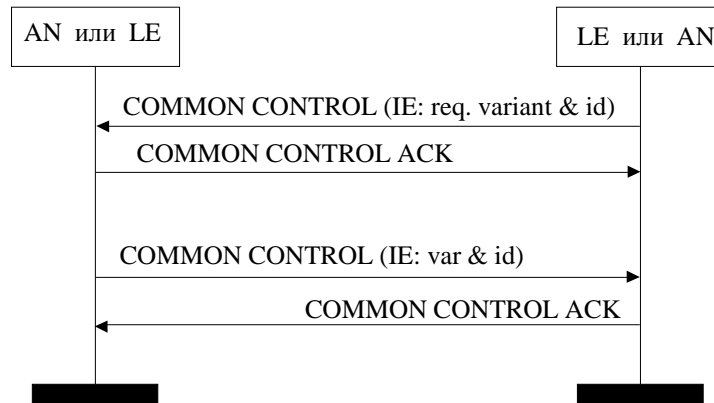


Рисунок 10.4 - Процедура идентификации тракта

10.3 Тестовые сценарии процедур управления конфигурацией (категория В)

В процессе тестирования оборудованием AN управляет местная система управления. После каждого изменения конфигурации интерфейс V5 активизируется, и производится проверка его функциональных возможностей с помощью контрольных вызовов.

Рассмотрим менеджмент интерфейса V5.2

Следующие тестовые сценарии описывают примеры того, как может быть сконфигурирован интерфейс V5.2 (каждая строка – это отдельный сценарий).

После каждой операции конфигурирования интерфейс V5.2 активизируется с помощью процедур реконфигурации, и выполняются контрольные вызовы.

Тестовые сценарии для менеджмента интерфейса V5.2:

- создать интерфейс V5.2 только с одним ИКМ-трактом (1);
- создать интерфейс V5.2 с четырьмя ИКМ-трактами (2);
- подключить еще несколько абонентов к интерфейсу V5.2 (3);
- подключить еще один ИКМ-тракт к интерфейсу V5.2 (4);
- отключить ИКМ-тракт от интерфейса V5.2 (5).

Ожидаемые результаты:

- старт интерфейса V5.2 успешен,
- для каждого сценария (1-5) контрольные вызовы выполнены успешно.

10.4 Тесты блокировки/разблокировки ИКМ-тракта (категория С)

Рассмотрим блокировку Первичного тракта, инициируемую LE для интерфейса V5.2

Начальное состояние:

- AN и LE функционируют нормально;
- интерфейс V5 активен, все тракты доступны;
- звено данных для протокола ТфОП организовано в КИ16 тракта 3 (не Первичного и не Вторичного).

Тестовая процедура:

- выполнить контрольные вызовы по Первичному и по какому-либо другому тракту;
- выполнить блокировку Первичного тракта со стороны LE;
- выполнить контрольные вызовы для проверки интерфейса V5.

Ожидаемые результаты:

- вызовы по Первичному тракту не обслуживаются, а вызовы по другим трактам обслуживаются;
- звенья данных, размещенные в КИ16 Первичного тракта, протокол защиты переводит в КИ16 Вторичного тракта;

- первичный тракт блокируется;
- новые контрольные вызовы обрабатываются нормально.

10.5 Тесты работы с отказами трактов (категория D)

Начальное состояние:

- звено данных для протокола ТфОП организовано в КИ16 Первичного тракта;
- интерфейс V5.2 функционирует нормально, все тракты доступны;
- не было переключений на резерв.

Тестовая процедура

- установить соединения по каждому тракту;
- физически отключить Первичный тракт;
- выполнить контрольные вызовы для проверки работы интерфейса V5.2.

Ожидаемые результаты:

- успешное функционирование "Группы защиты 1";
- обслуживание вызовов Первичным трактом прекращено, вызовы по другим трактам обслуживаются нормально;
- новые контрольные вызовы успешны.

10.6 Тесты национального мэппинга ТфОП (категория E)

Сценарии соответствуют национальной спецификации мэппинга ТфОП. План, предлагаемый в этом параграфе, содержит только сценарии для основных случаев.

Занятие со стороны AN

Начальное состояние:

- интерфейс V5.2 функционирует нормально;
- возможно установление соединений.

Занятие без набора номера

Тестовая процедура:

- снять трубку;
- не набирать номер;
- положить трубку после получения сигнала "Занято".

Ожидаемый результат

- получение сигнала "Занято" по истечении выдержки времени, определяющей длительность передачи сигнала "Ответ станции" ($T_{OC} = 20 \div 30$ с).

Отбой после получения сигнала "Ответ станции"

Тестовая процедура:

- снять трубку;
- после получения сигнала "Ответ станции" положить трубку.

Ожидаемый результат

- разрушение соединения со станцией.

Превышение выдержки времени, ограничивающей длительность прослушивания сигнала "Занято"

Тестовая процедура

- снять трубку;
- слушать сигнал "Ответ станции" в течение времени T_{OC} ($T_{OC} = 20 \div 30$ с).
- слушать сигнал "Занято" в течение времени, превышающего T_3 ($T_3 = 20 \div 30$ с).

Ожидаемый результат

- блокировка линии вызывающего абонента по истечении времени T_3 .

10.7 Тесты доступа ISDN

Базовый доступ ISDN (категория F)

Активизация, инициируемая стороной AN

Начальное состояние:

- интерфейс V5 функционирует нормально;
- состояние пользовательского порта: "Рабочее деактивизированное".

Тестовая процедура:

- снять трубку и набирать номер.

Ожидаемые результаты:

- пользовательский порт активизирован со стороны AN;
- контрольные вызовы обслуживаются нормально.

Активизация, инициируемая стороной LE

Начальное состояние:

- интерфейс V5 функционирует нормально;
- состояние пользовательского порта: "Рабочее деактивизированное".

Тестовая процедура:

- выполнить контрольный вызов со стороны LE.

Ожидаемые результаты:

- пользовательский порт активизирован со стороны LE;
- контрольный вызов успешен.

Деактивизация со стороны LE

Начальное состояние:

- интерфейс V5 функционирует нормально;
- обслуживается контрольный вызов от AN к LE.

Тестовая процедура:

- дать отбой.

Ожидаемый результат:

- через 10 с после отбоя пользовательский порт деактивизируется со стороны LE.

Новый вызов до деактивизации порта

Начальное состояние:

- интерфейс V5 функционирует нормально;
- обслуживается контрольный вызов от AN к LE.

Тестовая процедура:

- дать отбой;
- менее чем через 10 с после отбоя выполнить новый вызов со стороны AN.

Ожидаемый результат:

- новый вызов успешен.

Несколько вызовов из одного порта

Начальное состояние:

- интерфейс V5 функционирует нормально;
- состояние пользовательского порта: "Рабочее деактивизированное";
- к одному порту в AN подключено несколько (больше двух) терминалов ISDN.

Тестовая процедура:

- выполнить контрольные вызовы одновременно со всех терминалов.

Ожидаемый результат:

- получают обслуживание только два вызова.
- Несколько вызовов к одному порту

Начальное состояние:

- интерфейс V5 функционирует нормально;
- состояние пользовательского порта: “Рабочее деактивизированное”;
- к одному порту в AN подключено несколько (больше двух) терминалов ISDN.

Тестовая процедура:

- выполнить одновременно несколько контрольных вызовов к этому порту AN.

Ожидаемый результат:

- получают обслуживание только два вызова.

10.8 Услуги (категория G)

Цель тестирования – убедиться в том, что абоненты AN, подключенные к LE через интерфейс V5, могут пользоваться теми же услугами, что и абоненты, подключенные к ней непосредственно. Поскольку интерфейс V5 по отношению к услугам является прозрачным, то здесь возможно использование тех же планов тестирования, что и для абонентов LE.

10.9 Тесты стабильности (категория H)

Стабильность функционирования проверяется путем генерации (с помощью специального оборудования) массовых контрольных вызовов, а также контролем устойчивости динамического назначения каналов интерфейса.

Массовые контрольные вызовы

Начальное состояние:

- интерфейс V5 функционирует нормально;
- на сторонах AN и LE подключено специальное оборудование для генерации массовых контрольных вызовов.

Тестовая процедура:

Методика проверки с помощью массовых контрольных вызовов, как правило, не отличается от типовых методик, используемых на городских АТС.

Ожидаемый результат:

- число неуспешных вызовов удовлетворяет норме потерь.

Тестирование динамического назначения каналов (интерфейс V5.2)

Начальное состояние:

- интерфейс V5.2 функционирует нормально;
- пользовательских портов больше, чем несущих каналов в интерфейсе V5.2.

Тестовая процедура:

- выполнить несколько контрольных вызовов из AN;
- вести мониторинг поведения протокола ВСС в интерфейсе V5.2.

Ожидаемые результаты:

- вызовы успешны, если имеются свободные несущие каналы в трактах V5.2;
- процедура назначения каналов работает удовлетворительно;
- вызовы неуспешны, когда все несущие каналы в интерфейсе V5.2 заняты, и в этих случаях абонентам передается сигнал “Занято при перегрузке”.

10.10 Протокол-тестеры SNT-7531 или SNT/lite

Внешний вид протокол-тестеров SNT-7531 и SNT/lite интерфейса V5 представлен на рисунке 10.5.



Рисунок 10.5 Внешний вид протокол-тестера SNT-7531 и SNT/lite

В контексте представленных выше тестовых сценариев рассмотрим возможности мониторинга и симуляции протоколов интерфейса V5. Пользовательский интерфейс содержит следующие конфигурируемые экранные элементы:

- окно режима мониторинга (основное и вспомогательное),
- окно режима симуляции,
- окна настройки

Окно режима мониторинга (рисунок 10.6) служит для отображения принимаемых и передаваемых сообщений. Оно разделено на два окна:

- основное окно,
- вспомогательное окно.

Основное окно (верхнее) используется для вывода декодированных сообщений в полном виде: каждое поле представлено в форме "номер байта – битовая маска – имя поля – значение поля". Степень детализации просматриваемой информации можно изменять посредством подменю "Детализация" с помощью левой клавиши манипулятора "мышь" или кнопками управления детализацией.

Вспомогательное окно (нижнее) предназначено для мониторинга входящих сообщений и просмотра основных полей сообщения. Каждое сообщение представляется в виде одной строки, где отображается время, пучок, направление, протокол (PSTN, BCC, LAPV5 и т.д.), имя сообщения (SIGNAL, DISCONNECT COMPLETE и т.д.) и дополнительная информация.

В режиме мониторинга можно провести анализ протоколов интерфейса V5.1 и V5.2 в соответствии с Рекомендациями ITU-T G.964 (для V5.1) и G.965 (для V5.5) и стандартами ETS 300 324-1 (для V5.1), ETS 300 347-1 (для V5.2). Анализируются следующие протоколы интерфейса V5:

- протокол ТфОП,
- протокол управления,
- протокол назначения несущих каналов (BCC),
- протокол управления трактами,
- протокол защиты.

Использование протокол-тестера дает возможность:

- проверки (подтверждения) существующей конфигурации трактов интерфейса V5.1/V5.2, используя опцию автоматического сканирования;
- одновременного наблюдения С-каналов Первичного и Вторичного тракта интерфейса V5.2; в двухпортовом режиме тестер SNT-7531 имеет возможность одновременно отображать работу С-каналов и Первичного, и Вторичного трактов; пользователь видит информацию о работе интерфейса;
- синхронного декодирования протоколов; протокол-тестер имеет возможность синхронно декодировать до 5 протоколов V5.2 в одном, двух или трех физических С-каналах; размещение этой информации в одном окне в течение всего сеанса облегчает поиск несоответствий в протоколах.

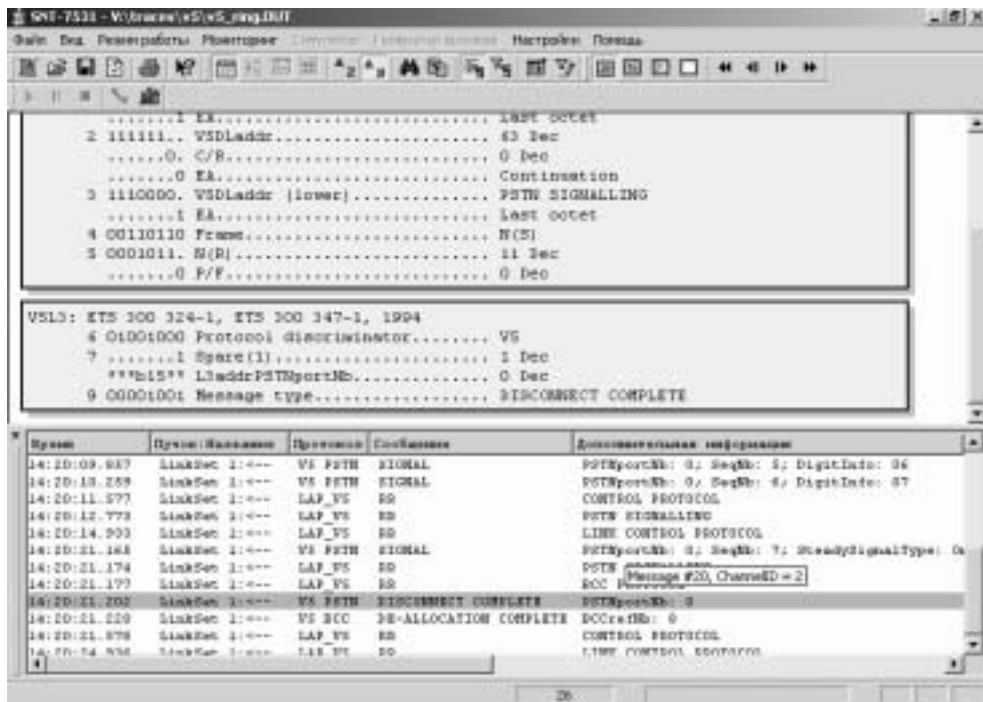


Рисунок 10.6 - Окно режима мониторинга

Окно режима симуляции предназначено для ввода информации, относящейся к имитации действий абонента (снятие трубки, набор номера и т.п.) и к блокировке/разблокировке портов или трактов, и для отображения состояний протоколов интерфейса V5.

Контрольные вопросы

1. Перечислить действия, которые выполняются при старте интерфейса V5.
2. Опишите тестируемую конфигурацию сети доступа.
3. Какие начальные установки необходимо задать для организации тестирования приведенной конфигурации интерфейса V5?
4. Перечислите категории тестовых сценариев и поясните их целевое назначение.
5. Каковы функциональные возможности протокол-тестеров SNT-7531 и SNT/ite?
6. Опишите пользовательский интерфейс протокол-тестеров?

Занятие 11 Преобразование протоколов интерфейса V5

Применение конвертеров позволяет решить проблему включения оборудования абонентского доступа с интерфейсами V5.1 и V5.2 в те АТС сетей России и стран СНГ, которые не содержат средств формирования этих интерфейсов. Применение конвертеров возможно и как временное решение, улучшающее экономические показатели отдельных этапов развития сети доступа. Например, при установке оборудования беспроводного доступа WLL, мультисервисных концентраторов Протей-МАК или BroadAccess ADC, рассмотренных на Занятии 1, можно временно включить его в АТС с помощью конвертера VSM, а после установки в этой АТС новой версии программного обеспечения исключить конвертер и использовать интерфейс V5 непосредственно.

Рассматриваются конвертеры типа VSM, которые преобразуют протоколы интерфейса V5 в протокол DSS1 (PRI, версия ETSI) или в протокол другой системы сигнализации, поддерживаемой данной АТС. Сценарии взаимодействия этих систем сигнализации рассматриваются на этом занятии.

11.1 Вызов со стороны PRI E-DSS1 к стороне LE

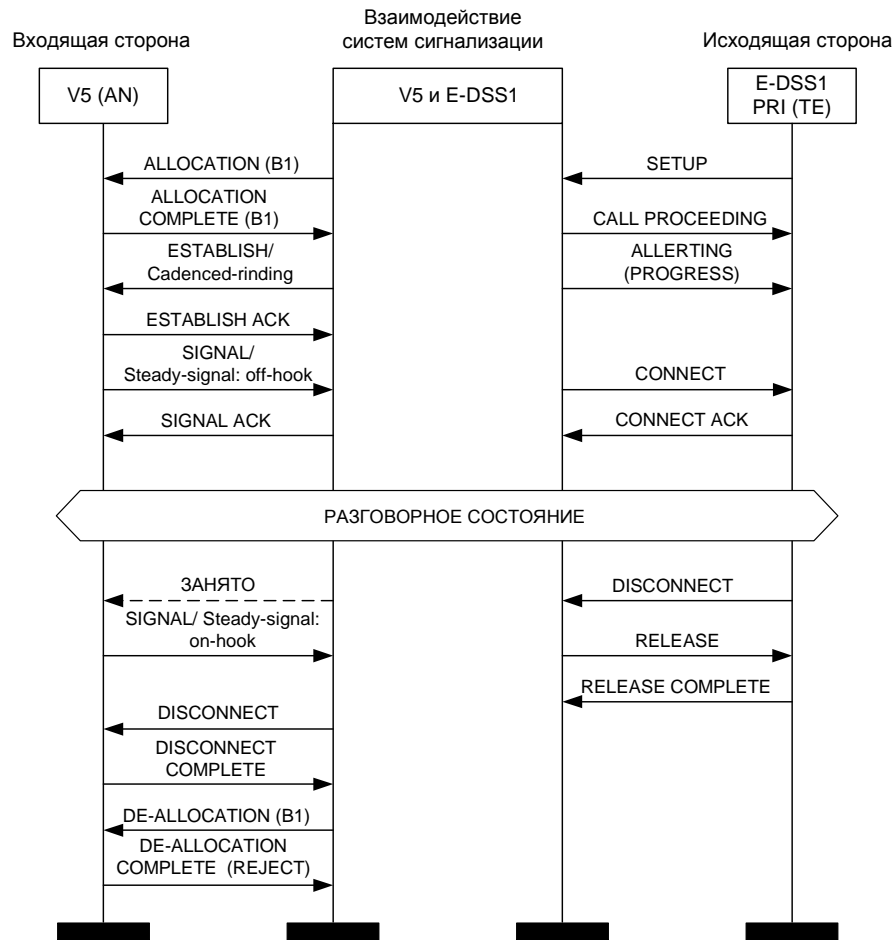


Рисунок 11.1 Вызов к свободному абоненту. Отбой абонента А

11.2 Вызов со стороны LE V5 к стороне PRI E-DSS1

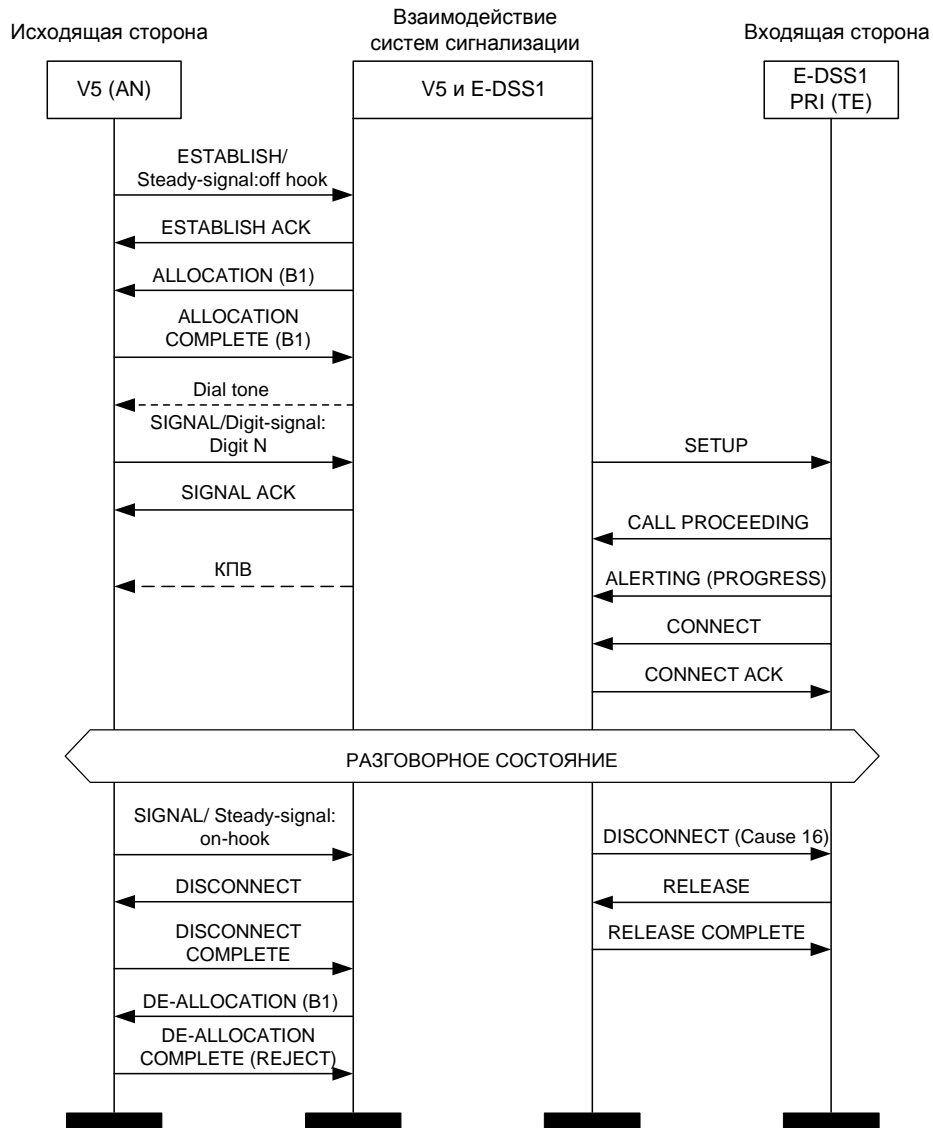


Рисунок 11.2. Вызов к свободному абоненту. Декадный код. Отбой абонента А

11.3 Конвертер VSM

Конвертер протоколов сигнализации VSM представляет собой модуль, который преобразует протоколы интерфейса V5, используемого для подключения к опорным АТС оборудования сети доступа, в протокол первичного доступа ISDN версии ETSI (а также других версий) с системой сигнализации DSS1, используемый при подключении к опорным АТС терминального оборудования первичного доступа ISDN и УПАТС. Конвертер позволяет подключить к АТС, поддерживающей систему сигнализации DSS1-PRI, оборудование сети доступа (концентраторы, системы WLL, системы CDMA), имеющее один или несколько интерфейсов V5.2 или V5.1.

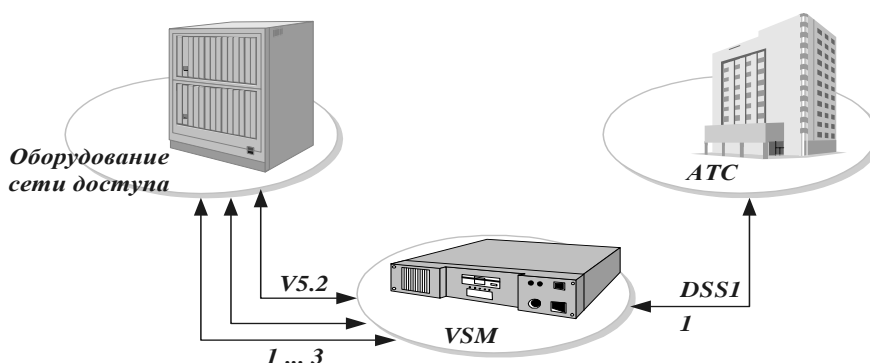
Конвертер сигнализации VSM организует взаимодействие АТС и оборудования сети доступа при установлении соединений всех типов.

Использование VSM обеспечивает концентрацию абонентской нагрузки, что позволяет эффективнее использовать абонентскую емкость АТС, а также уменьшить длины аналоговых участков абонентских линий и тем самым улучшить качество связи для пользователей, подключаемых к сети доступа по двухпроводным аналоговым абонентским линиям. Конвертер обеспечивает также возможность подключения любого оборудования доступа, имеющего порты ТФОП.

К функциональным возможностям конвертеров VSM относятся:

- Преобразование протоколов сигнализации V5<->DSS1 и DSS1<->V5
- Контроль состояния уровня 1 трактов ИКМ со стороны V5
- Контроль состояния уровня 1 трактов ИКМ со стороны DSS1
- Прием и обработка команд уровня 2 интерфейса V5 (LAPV5) – организация и поддержание рабочего состояния звена уровня 2 LAPV5
- Прием и обработка команд уровня 2 DSS1 – организация и поддержание рабочего состояния звена LAPD
- Прием и обработка сообщений уровня 3 стороны LE интерфейса V5, необходимых для управления базовым соединением, и преобразование их в соответствующие команды уровня 3 DSS1
- Прием и обработка сообщений уровня 3 DSS1, необходимых для управления базовым соединением, и преобразование их в соответствующие команды уровня 3 стороны LE интерфейса V5
- Обеспечение доступа внешнего терминала эксплуатационного управления – локально (через интерфейс RS-232), через модем (встроенный, внешний), или по сети Ethernet (TCP/IP).

Дополнительной возможностью конвертера VSM является обработка внутренних вызовов в сети доступа (коммутация V5 – V5), что снижает нагрузку управляющих устройств АТС.



На рисунке 11-3 представлен простейший вариант включения конвертера, при котором в сети доступа имеется три ИКМ-тракта с интерфейсами V5.1, которые преобразуются в один тракт с сигнализацией DSS1.

Рисунок 11 - 3. Включение конвертера

Контрольные вопросы

1. Какие задачи позволяет решить применение конвертеров?
2. Каковы функциональные возможности конвертера VSM?
3. Нарисуйте диаграммы преобразования протоколов сигнализации для сценариев использования конвертера VSM при взаимодействии системы сигнализации DSS1 и оборудования сети доступа с интерфейсом V5.

ЛИТЕРАТУРА

- 1 Гольдштейн Б.С., Ехриель И.М., Кадыков В.Б., Рерле Р.Д. Протоколы V5.1 и V5.2. Справочник//СПб.: BHV-2003.
- 2 Гольдштейн Б.С. Протоколы сети доступа. Том 2. — М.: Радио и связь, 2001.- 292 с.: ил.
- 3 ОСТ45.154-2001 Местная телефонная сеть. Сопряжение цифровой автоматической телефонной станции и сети доступа по интерфейсу V5. Спецификация протокола передачи телефонной сигнализации (Уровень 3).
- 4 ОСТ45.155-1999 Местная телефонная сеть. Сопряжение цифровой автоматической телефонной станции и сети доступа по интерфейсу V5. Сигнализация. Правила формализации информации.
- 5 ОТТ к цифровым АТС с функциями интерфейса V5 при взаимодействии с абонентской сетью доступа. Утв. Минсвязи России, 1996.
- 6 ETSI EN 300 324-1 (V.1.2). V-interfaces at the digital Local Exchange (LE); V5.1 interface for the support of Access Network (AN), Part 1: V5 interface specification.
- 7 ETSI EN 300 347-1. V-interfaces at the digital Local Exchange (LE); V5.2 interface for the support of Access Network (AN), Part 1: V5.2 interface specification.
- 8 ETSI ETR 150. V5 interface. Public Switched Telephone Network (PSTN) mappings, 1994.
- 9 ITU-T Recommendation G.964. V-interfaces at the digital Local Exchange (LE) — V5.1 interface (based on 2048 kbit/s) for the support of Access Network (AN).
- 10 ITU-T Recommendation G.965. V-interfaces at the digital Local Exchange (LE) — V5.2 interface (based on 2048 kbit/s) for the support of Access Network (AN).
- 11 ITU-T Recommendation Q.512. Digital exchange interfaces for subscriber access.