Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 10.09.2024 00:18:53
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«28» 08 2024 г.

СИНХРОНИЗАЦИЯ И УПРАВЛЕНИЕ В СЕТЯХ ДОСТУПА

Методические указания по выполнению лабораторной работы для студентов, обучающихся по направлению подготовки 11.04.02 «Информационные технологии и системы связи» направленность «Проектирование устройств, систем и сетей телекоммуникаций» по дисциплине «Проектирование оптических систем доступа»

Курск 2024

УДК 004.716

Составители: А. А. Гуламов

Рецензент

Доктор технических наук, старший научный сотрудник,
Зав. кафедры КПиСС *В.Г. Андронов*

Синхронизация и управление в сетях доступа: методические указания по выполнению лабораторной работы для студентов направления подготовки 11.04.02 направленность «Проектирование устройств, систем и сетей телекоммуникаций» / Юго-Зап. гос. ун-т; сост.: А.А. Гуламов. - Курск, 2024. – 56 с. табл. 9. – Библиогр.: с. 49.

Методические указания по выполнению лабораторной работы содержат теоретические сведения о тактовой синхронизации в сети с цифровой циклической передачи, в сети с передачей кадров, ячеек и пакетов, особенности синхронизации в PON, а так же данные об управлении оптической сетью доступа. Рассмотрены схема синхронизации сети доступа и схема управления сетью доступа. Представлен перечень контрольных вопросов.

Методические указания соответствуют учебному плану обучающихся по направлению подготовки 11.04.02 «Информационные технологии и системы связи» направленность «Проектирование устройств, систем и сетей телекоммуникаций» по дисциплине «Проектирование оптических систем доступа».

Предназначены для студентов, обучающихся по направлению подготовки 11.04.02 «Информационные технологии и системы связи» направленность «Проектирование устройств, систем и сетей телекоммуникаций»по дисциплине «Проектирование оптических систем доступа».

Текст печатается в авторской редакции

Подписано в печать. Формат 60x841/16.
Усл. печ. л..3,25 Уч.-изд. л.. 2,94 Тираж 100 экз. Заказ. 792 Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

Содержание

ИНСТРУКЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

Общие положения

Настоящая инструкция предназначена для студентов и работников, выполняющих работы на персональном компьютере и на сетевом оборудовании (коммутаторы, маршрутизаторы, межсетевые экраны и т.д.).

К выполнению работ допускаются лица:

- не моложе 16 лет;
- прошедшие медицинский осмотр;
- прошедшие вводный инструктаж по охране труда, а также инструктаж по охране труда на рабочем месте;
- прошедшие обучение безопасным приемам труда на рабочем месте по выполняемой работе.

Работник обязан:

- выполнять правила внутреннего трудового распорядка, установленные в положениях и инструкциях, утвержденных ректором ЮЗГУ, или его заместителями;
- выполнять требования настоящей инструкции;
- сообщать руководителю работ о неисправностях, при которых невозможно безопасное производство работ;
- не допускать присутствия на рабочем месте посторонних лиц;
- уметь оказывать первую помощь и при необходимости оказывать ее пострадавшим при несчастных случаях на производстве, по возможности сохранив обстановку на месте происшествия без изменения и сообщив о случившемся руководителю;
- выполнять требования противопожарной безопасности не разводить открытый огонь без специального на то разрешения руководителя работ;
- периодически проходить медицинский осмотр в сроки, предусмотренные для данной профессии.

Работник должен знать опасные и вредные производственные факторы, присутствующие на данном рабочем месте:

- возможность травмирования электрическим током при отсутствии или неисправности заземляющих устройств;

- вредное воздействие монитора компьютера при его неправильной установке или неисправности;

- возможность возникновения заболеваний при неправильном расположении монитора, клавиатуры, стула и стола;

- вредное воздействие паров, газов и аэрозолей, выделяющихся при работе копировальной и печатающей оргтехники в непроветриваемых помещениях.

Работник при выполнении любой работы должен обладать здоровым чувством опасности и руководствоваться здравым смыслом. При отсутствии данных качеств он к самостоятельной работе не допускается.

Требования охраны труда перед началом работы

Перед началом работы работник обязан:

- получить от руководителя работ инструктаж о безопасных методах, приемах и последовательности выполнения производственного задания;

- привести в порядок одежду, застегнуть на все пуговицы, чтобы не было свисающих концов, уложить волосы, чтобы они не закрывали лицо и глаза;

- привести рабочее место в безопасное состояние;

- запрещается носить обувь на чрезмерно высоких каблуках;

Перед включением компьютера или сетевого оборудования убедиться в исправности электрических проводов, штепсельных вилок и розеток. Вилки и розетки должны соответствовать Евростандарту. Отличительной особенностью этих вилок и розеток является наличие третьего провода, обеспечивающего заземление компьютера или другого прибора. При отсутствии третьего заземляющего провода заземление должно быть выполнено обычным способом с применением заземляющего проводника и контура заземления;

Убедиться, что корпус включаемого оборудования не поврежден, что на нем не находятся предметы, бумага и т.п. Вентиляционные отверстия в корпусе включаемого оборудования не должны быть закрыты занавесками, завалены бумагой, заклеены липкой лентой или перекрыты каким-либо другим способом.

Требования охраны труда во время работы

Запрещается во время работы пить какие-либо напитки, принимать пищу;

Запрещается ставить на рабочий стол любые жидкости в любой таре (упаковке или в чашках);

Помещения для эксплуатации компьютеров, сетевого оборудования должны иметь естественное и искусственное освещение, естественную вентиляцию и соответствовать требованиям действующих норм и правил. Запрещается размещать рабочие места вблизи силовых электрических кабелей и вводов трансформаторов, технологического оборудования, создающего помехи в работе и отрицательно влияющие на здоровье операторов;

Окна в помещениях, где установлены компьютеры должны быть ориентированы на север и северо-восток. Оконные проемы оборудуются регулируемыми устройствами типа жалюзи или занавесками;

Площадь на одно рабочее место пользователей компьютера должна составлять не менее 6 $м^2$ при рядном и центральном расположении, при расположении по периметру помещения – 4 $м^2$. При использовании компьютера без вспомогательных устройств (принтер, сканер и т.п.) с продолжительностью работы менее четырех часов в день допускается минимальная площадь на одно рабочее место 5 $м^2$;

Полимерные материалы, используемые для внутренней отделки интерьера помещений с ПК, должны подвергаться санитарно-эпидемиологической экспертизе. Поверхность пола должна обладать антистатическими свойствами, быть ровной. В помещениях ежедневно проводится влажная уборка. Запрещается использование удлинителей, фильтров, тройников и т.п., не имеющих специальных заземляющих контактов;

Экран видеомонитора должен находится от глаз оператора на расстоянии 600-700 мм, минимально допустимое расстояние 500 мм;

Продолжительность непрерывной работы с ПК должна быть не более 2 часов.

Требования охраны труда по окончании работы

По окончании работы работник обязан выполнить следующее:

- привести в порядок рабочее место;
- убрать инструмент и приспособления в специально отведенные для него места хранения;
- обо всех замеченных неисправностях и отклонениях от нормального состояния сообщить руководителю работ;
- привести рабочее место в соответствие с требованиями пожарной безопасности.

Действие при аварии, пожаре, травме

В случае возникновения аварии или ситуации, в которой возможно возникновение аварии немедленно прекратить работу, предпринять меры к собственной безопасности и безопасности других рабочих, сообщить о случившемся руководителю работ.

В случае возникновения пожара немедленно прекратить работу, сообщить в пожарную часть по телефону 01, своему руководителю работ и приступить к тушению огня имеющимися средствами.

В случае получения травмы обратиться в медпункт, сохранить по возможности место травмирования в том состоянии, в котором оно было на момент травмирования, доложить своему руководителю работ лично или через товарищей по работе.

Ответственность за нарушение инструкции

Каждый работник ЮЗГУ в зависимости от тяжести последствий несет дисциплинарную, административную или уголовную ответственность за несоблюдение настоящей инструкции, а также прочих положений и инструкций, утвержденных ректором ЮЗГУ или его заместителями.

Руководители подразделений, заведующий кафедрой, начальники отделов и служб несут ответственность за действия своих подчиненных, которые привели или могли привести к авариям и

травмам согласно действующему в РФ законодательству в зависимости от тяжести последствий в дисциплинарном, административном или уголовном порядке.

Администрация ЮЗГУ вправе взыскать с виновных убытки, понесенные предприятием в результате ликвидации аварии, при возмещении ущерба работникам по временной или постоянной утрате трудоспособности в соответствии с действующим законодательством.

1 Принципы тактовой синхронизации

Принципы тактовой синхронизации сетей доступа по своей сути не отличаются от принципов синхронизации транспортных сетей, однако подключение к тактовому синхронизму в сетях доступа производится в узле CDN от наиболее стабильного источника. Таким источником может служить транспортная сеть оператора на основе оборудования PDH, SDH, ATM и SyncEthernet (SyncE) и также коммутационное оборудование электронных АТС, коммутаторов ATM, Ethernet, подключенное к синхронизированной транспортной сети, где обеспечивается автоматический выбор наилучшего по качеству (стабильности, минимальным фазовым дрожаниям) синхросигнала.

Общие принципы тактовой синхронизации детально проработаны и закреплены в международных стандартах – рекомендациях ITU-T G.803, G.810, G.811, G.812, G.813, G.781, I.361 и других [1, 2, 3, 4]

Необходимо отметить, что помимо тактового синхронизма в сетях доступа применяются синхронизации по циклам, по сверхциклам, по кадрам, по ячейкам, по пакетам. Однако все эти виды синхронизации базируются на тактовом синхронизме физического уровня, и их проработка относится к каждой отдельной технологии мультиплексирования и передачи.

Тактовая синхронизация на физическом уровне во всех технология передачи едина и строится на принципе распределения тактов от ведущего генератора к ведомым генераторам, захватывающим такты от ведущего генератора и транслирующим эти такты другим генераторам (рис. 1). Такой способ распределения синхронизма получил в специальной литературе название «шинное распределение».

Ведущим генератором выступает первичный эталонный генератор ПЭГ - PRC (Primary Reference Clock) – высокостабильный атомный генератор, долговременное относительное отклонение частоты которого от номинального значения поддерживается не превышающим $1x10^{-11}$ при контроле по универсальному координированному времени.

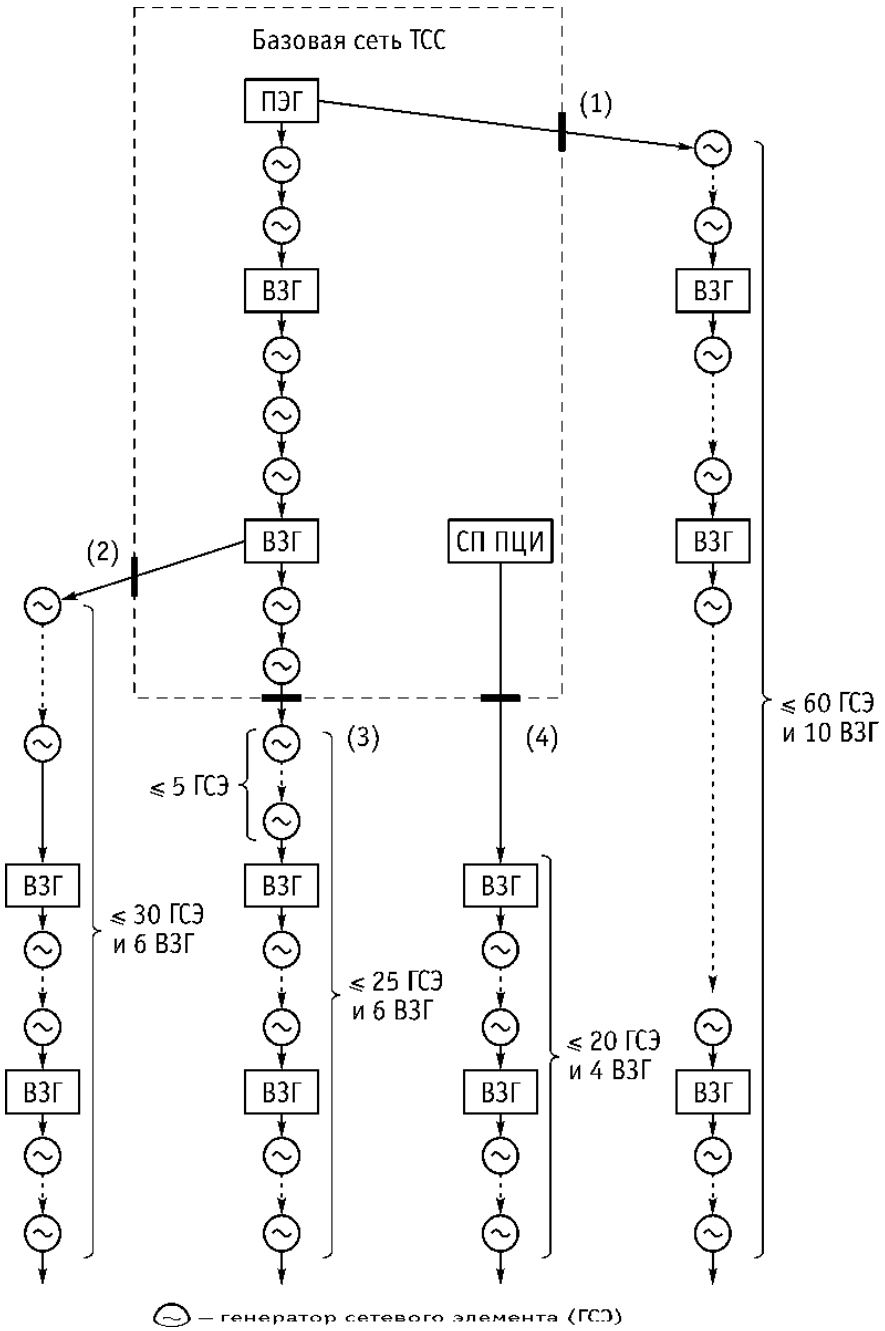


Рисунок 1- Схема присоединения сетей операторов к базовой сети синхронизации и классы подключения

Ведомым или вторичным задающим генератором ВЗГ - SRC (Second Reference Clocks) является кварцевый дополнительно стабилизированный генератор, фаза которого подстраивается по входному сигналу, полученному от генератора более высокого или того же качества. ВЗГ обеспечивает, как правило, высокую кратковременную относительную стабильность частоты (около 10^{-}

^{9}...10^{-11}) и существенно более низкую относительно ПЭГ долговременную относительную стабильность (около 10^{-8}).

Генераторы сетевых элементов ГСЭ - ETS (Equipment Timing Source) – синхронизируемые внешними синхросигналами генераторы (обычный кварцевый), помещаются в мультиплексоры PDH, SDH, ATM, Ethernet, кроссовые коммутаторы и т. д. Такты ГСЭ так же подстраиваются под внешние такты, как и в ВЗГ, однако их собственная относительная долговременная стабильность не превышает 10^{-6}.

Указанные генераторы имеют следующие иерархические положения по значимости в сети синхронизации (ТСС).

1-й или высший уровень иерархии ТСС – ПЭГ (называемый нулевым).

1-й уровень иерархии ТСС-ПЭИ (первичный эталонный источник), не являющийся составной частью ТСС, например, навигационный спутник GPS/ГЛОНАСС или ПЭГ другой сети.

2-й уровень иерархии ТСС – ВЗГ, который представляют как транзитный или оконечный и совмещаемый с узлами автоматической коммутации (УАК) и автоматическими междугородными телефонными станциями (АМТС) или цифровыми АТС.

3-й уровень иерархии ТСС – ГСЭ, к которым относятся мультиплексоры SDH, кроссовые коммутаторы SDH, оконечные цифровые АТС, коммутаторы АТМ и Ethernet.

Для синхронизации сетей различных операторов предложено четыре класса присоединения к базовой сети синхронизации (рис. 1):

- 1-й класс – сеть оператора получает сигнал синхронизации через пассивные соединительные линии от ПЭГ базовой сети ТСС;
- 2-й класс – сеть оператора получает сигнал синхронизации от ВЗГ;
- 3-й и 4-й классы – сеть оператора получает сигнал синхронизации от ГСЭ.

Внутри каждого региона сеть принудительной синхронизации должна строиться по иерархическому принципу в виде древовидной схемы (радиально-узловой), исключающей возможность образования петель синхронизации в любой ситуации. В качестве ведомых генераторов на АМТС, АТС и т.д. могут использоваться

блоки, встроенные в аппаратуру коммутации. На узлах и станциях, на которых кроме АМТС, АТС и т.д. установлено другое оборудование, нуждающееся в синхронизации (аппаратура кроссирования, оперативного переключения и т.д.), в качестве ведомых генераторов, которые синхронизируют все оборудование на данном узле, должны использоваться выделенные ВЗГ, соответствующие рекомендации МСЭ-Т G.812. При этом каждый ВЗГ должен иметь альтернативные входы синхронизации.

Максимальное число ВЗГ в пределах региона в одной цепи синхронизации не должно превышать 10, что обусловлено накоплением фазовых дрожаний (джиттер и вандер). ВЗГ могут отличаться собственной стабильностью тактовой частоты и полосой частот захвата внешнего синхронизма. Число каскадно включаемых ГСЭ также нормировано, т.е. не более 20 между 2-мя ВЗГ.

Помимо общих принципов тактовой синхронизации в каждой из технологий мультиплексирования и передачи используются специфические решения по управлению тактовым синхронизмом.

2 Синхронизация в сети с цифровой циклической передачей

Тактовый синхронизм в цифровой сети с циклической передачей обеспечивается линейными сигналами. В сети доступа на основе гибких мультиплексоров передача тактового синхронизма может сопровождаться, согласно рекомендации ITU-T G.704, маркером синхронизации SSM (Synchronization Status Message) в нулевом канальном интервале нечётных циклов E1 на позициях 5,6,7,8 бит (табл. 1). Этот маркер используется для обозначения качества тактового синхронизма (стабильности источника тактов), что необходимо для автоматического выбора лучшего синхросигнала и запрета использования синхросигнала для исключения образования петель синхронизации, т.е. захвата ведущим генератором собственной частоты.

В случае использования в сети доступа сигналов цифровой передачи PDH E3, E4 формируемых на основе рекомендации G.832 с синхронной передачей циклов 125мкс, также используются биты SSM в байте MA (Maintenance and Adaptation) заголовка кадра.

Таблица 1 Значения маркера показателя качества

КИ0, МА и S1 (двоичный)	Маркер (десятичный)	Значение по рек. МСЭ-Т	Стабильность частоты	Уровень качества
xxxx 0010	2	ПЭГ (G.811)	1×10^{-11}	Q1(Q2)
xxxx 0100	4	ВЗГ (транзит) (G.812)	1×10^{-9} за сутки	Q2(Q4)
xxxx 1000	8	ВЗГ (местный) (G.812)	2×10^{-8} за сутки	Q3(Q8)
xxxx 1011	11	ГСЭ в режиме holdover (G.813)	4×10^{-6}	Q4(Q11)
xxxx 0000	0	Качество неизвестно	–	Q5(Q0)
xxxx 1111	15	Для синхронизации не использовать	–	Q6(Q15)

Применение в сети доступа оборудования SDH также предполагает организацию и сети синхронизации с передачей тактового синхронизма линейными сигналами STM-N и сигнала маркера SSM в байте S1 заголовка секции мультиплексирования MSOH. Функции, возлагаемые на SSM SDH, аналогичны для SSM PDH.

3 Синхронизация в сети с передачей кадров, ячеек и пакетов

В синхронном Ethernet тактовая частота передаётся линейным сигналом в виде непрерывной последовательности бит как в системах PDH (E1) так и SDH (STM-N) [5, 6]. Применяется древообразная структура с ведущим эталонным генератором ПЭГ (PRC), под такты которого подстраиваются генераторы оборудования Ethernet (EEC, Ethernet Equipment Clock), т.е. в структуре используется принцип «ведущий-ведомый» (рис. 2). Кроме того, в структуре распределения синхросигналов могут применяться ВЗГ (SRC). В сети SyncE используется канал обмена информацией о синхронизации ESMC (Ethernet Synchronization Messaging Channel), в котором сообщения маркера SSM передаются с помо-

щью специального низкоскоростного протокола Ethernet – OSSP (Organization Specific Slow Protocol).

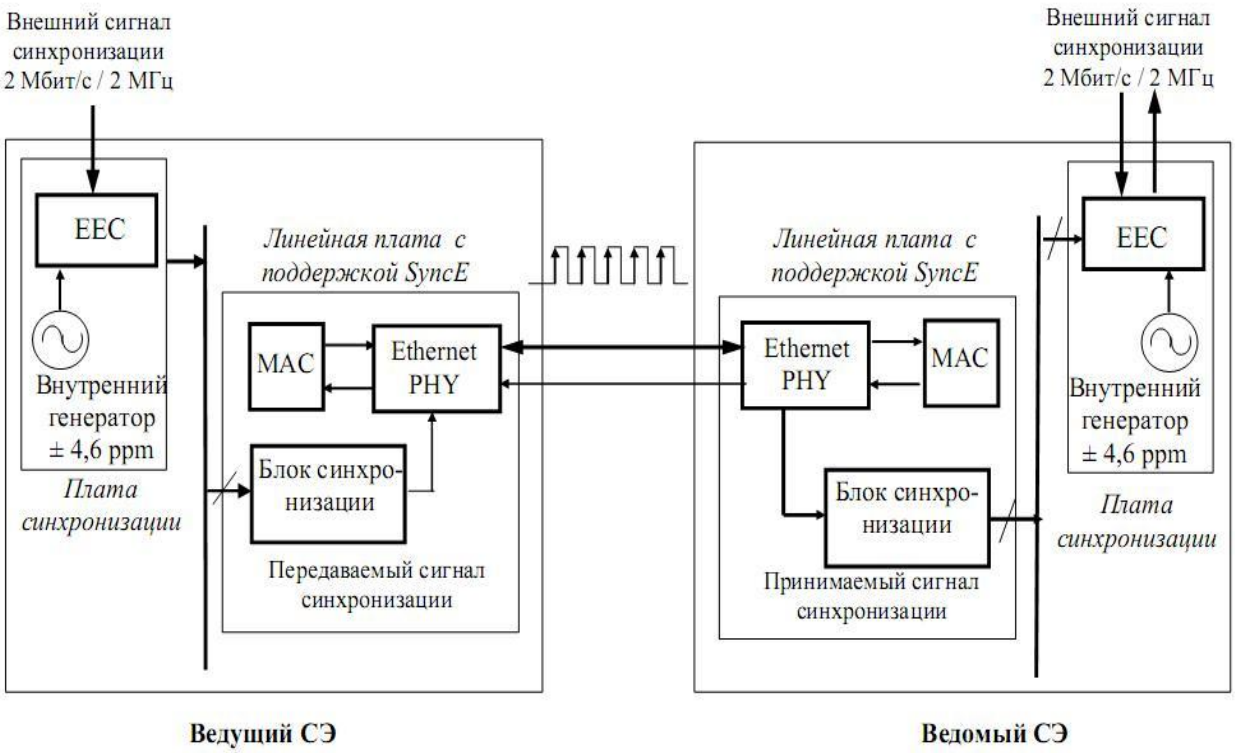


Рисунок 2 - Схема синхронизации СЭ в сети Ethernet

В канале ESMC различают два типа сообщений, переносящих коды SSM: один раз в секунду передаются информационные сообщения IM (Information Message), задающие периодичность и в случае изменения содержимого SSM сразу передаётся сообщение о событии EM (Event Message). Если в течение 5с по входящему каналу ESMC не поступило ни одного информационного сообщения, то оборудование EEC распознаёт как неисправность синхронизации. Структура кадра передачи протокола OSSP представлена в табл. 2. Упаковка поля данных и заполнение представлены в табл. 3.

Таблица 2 Структура кадра Ethernet для OSSP

Ёмкость (байт, бит)	Назначение поля	Содержание поля в 16-ричном формате
6 байт	Адрес места назначения	01-80-C2-00-00-02

6 байт	Адрес источника	MAC – адрес - порта
2 байта	Тип низкоскоростного протокола	88-09
1 байт	Подтип низкоскоростного протокола	0A
3 байта	Специальный идентификатор ITU-OUI	00-19-A7
2 байта	Подтип ITU	01
4 бита	Номер версии	01
1 бит	Флаг события	0- для PDU с информационным сообщением 1-для PDU с сообщением о событии
3 бита	Резерв	Резерв для будущего использования
3 байта	Резерв	
36-1400 байт	Данные и заполнение до минимальной ёмкости 64 байт	Табл. 5.3
4 байта	FCS	Проверочная последовательность

Таблица 3 Структура поля данных и заполнения

Ёмкость (байт, бит)		Назначение поля	Содержание поля в 16-ричном формате
1 байт		Тип	01
2 байта		Длина	04
1 байт	4 бита	Не используется	0
	4 бита	Маркер синхросигнала SSM	Код SSM

Учитывая, что сообщения байта SSM в сети Ethernet и в сети SDH одинаковы, сети синхронизации могут совмещаться. Таким образом существующие средства синхронизации для сетей SDH (ПЭГ, ВЗГ, системы распределения синхросигналов) пригодны для применения в сетях SyncE.

При передаче ячеек АТМ на уровне AAL-1 обрабатываются сигналы реального времени, чувствительные к задержкам передачи (например, речевые сообщения). Для поддержки услуг самого высокого класса (категории А) требуется выполнение условий синхронизации источника и приёмника сигнала. Сеть АТМ, являясь транспортной средой, как правило, имеет собственный высокостабильный синхронизм. Однако источник и приемник

информационных сигналов не всегда имеют общий синхронизм с АТМ. По этой причине может возникать большое расхождение тактовых механизмов источника и приемника сигналов. Таким образом сеть АТМ не будет полностью «прозрачной» транспортной средой для сигналов. Поскольку сеть АТМ основана на передаче ячеек, то характеристика частоты источника синхронизма на приемной стороне может зависеть от сегментации ячеек и задержки возможных случайных смешиваний.

Маршрут извлечения источника синхронизма принадлежит пользовательскому соединению типа «точка-точка», построенному по принципу буферизации FIFO (First in First Out – первый пришел первый вышел) в выходном буфере, например, для E1 с регулировкой частоты записи-считывания. Частота считывания не может быстро меняться и подстраиваться под дрожание фазы приходящих импульсов (под джиттер). При этом может быть нарушено требование по стабильности синхронизма, например, для E1 согласно рекомендации ITU-T G.703 требование стабильности составляет 50×10^{-6} (или ppm, part per million). Поэтому важнейшей функцией AAL-1 может быть восстановление с требуемой точностью тактовой частоты. Рекомендацией ITU-T I.363.1 определен метод введения SRTS (Synchronous Residual Time Stamps) – синхронной остаточной временной метки. Эта метка вводится в сегмент AAL-1 (рис. 3) в виде p-бита CSI.

Метка представляет собой четырех битовое слово, переносимое в восьми подряд следующих сегментах. Метка вычисляется на передаче как разность частот сигнала (например, E1) и тактовой частоты АТМ сети, которая вычисляется делением:

$$f_{\text{ATM}} = \frac{155{,}52}{2 \cdot x}, \text{ МГц},$$

где **x** выбирается таким образом, чтобы переносимая частота была выше частоты тактов компонентного сигнала. Для E1 значение x = 6 и частота тактирования в АТМ будет 2,43 МГц. Для E3 значение x = 4, частота тактирования АТМ будет 38,88 МГц.

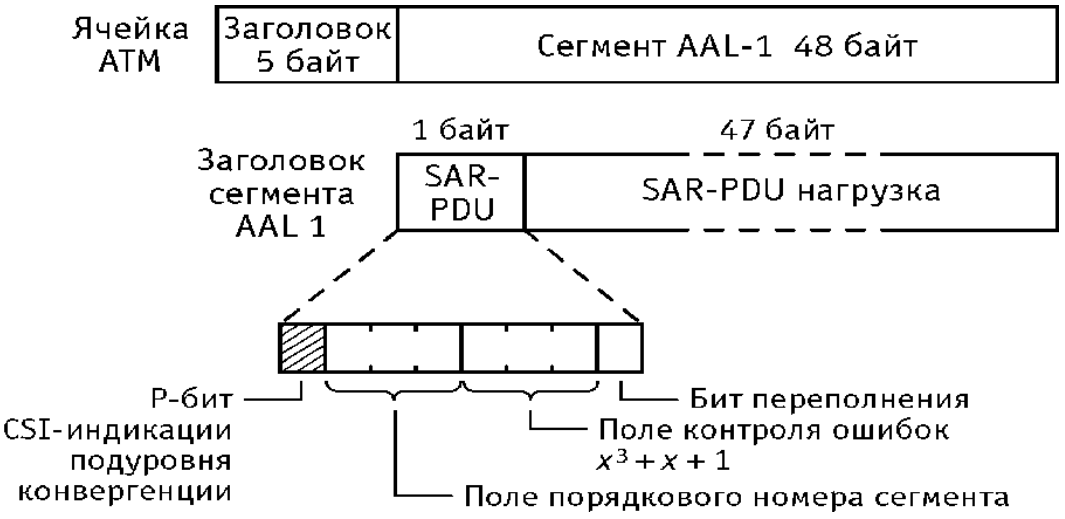


Рисунок 3 - Структура ячейки АТМ с сегментом AAL-1

При этом частота Е1 делится на число N = 3008 (общее число битов данных в восьми сегментах) и используется как затвор 4-х бит (р-бит) счетчика для частоты 2,43 МГц (рис. 4).

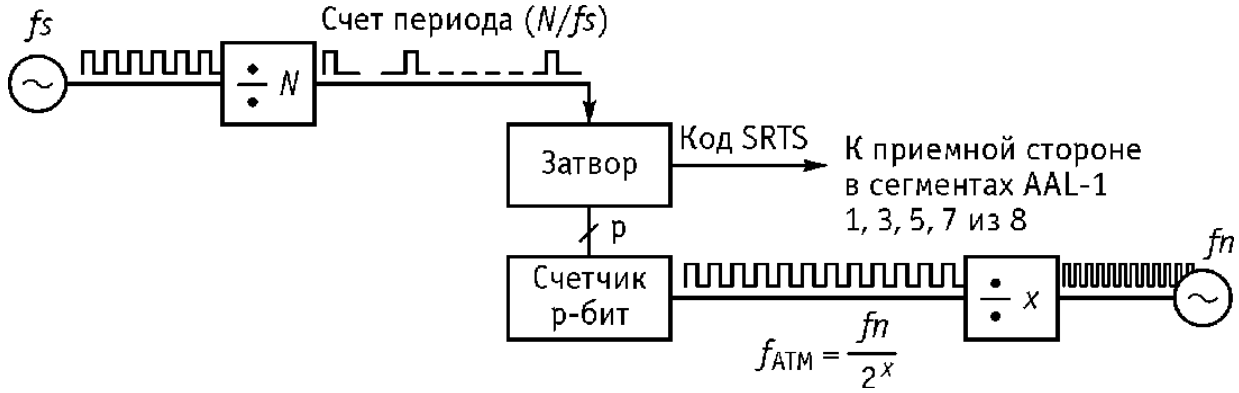


Рисунок 4. Формирование SRTS

На приемной стороне частота местного генератора кода SRTS сравнивается с частотой источника SRTS передающей стороны. Разность двух SRTS кодов используется для выравнивания локальной частоты синхронизации, с которой информационные данные из сети АТМ поставляются в сеть пользователя.

Следующей ступенью развития тактового синхронизма становится отдельная передача синхросигналов в сети с коммутацией пакетов с помощью специально разработанных IEEE протоколов: NTP (Network Time Protokol); PTP (Precision Time Protocol)

IEEE1588-2008 [6, 7]. Протокол NTP используется для синхронизации текущего времени на прикладном уровне модели ISO/OSI. В отличие от него, протокол «точного времени» PTP действует на втором (канальном) уровне модели ISO/OSI, т.е., например, в сети Ethernet.

Согласно стандарту IEEE1588-2008 протокол PTP представляет собой стандартный метод синхронизации устройств в сети с точностью до 10 нс. Этот протокол обеспечивает синхронизацию ведомых устройств от ведущего, удостоверяясь, что события и временные метки на всех устройствах используют одну и ту же временную базу. Протоколом предусмотрены две ступени для синхронизации устройств:

- определение ведущего устройства;
- коррекция расхождения во времени, вызванного смещением отсчёта часов в каждом устройстве и задержками в передаче данных по сети.

При активации системы синхронизации протокол PTP использует алгоритм «наилучших ведущих часов» для определения самого точного источника синхронизации в сети. Такой источник становится ведущим, а все остальные устройства (или сетевые элементы) ведомые и подстраивают свои такты по ведущему устройству. Разница во времени между ведущим и ведомыми устройствами представляет собой комбинацию смещения такта (нестабильности) и задержки передачи синхросигнала. Т.о. коррекция временного сдвига выполняется в два этапа (рис. 5):

- вычисление задержки передачи и сдвига;
- коррекция сдвига.

Ведущее устройство начинает коррекцию сдвига тактов, используя сообщения Sync и Follow-up. В сообщении Follow-up указывается время отправления сообщения Sync (T_{M1}), измеренное наиболее близко к среде передачи для минимизации ошибки во времени опорного источника (ПЭГ, ВЗГ). После того, как ведомое устройство получит первое сообщение Sync и Follow-up, оно использует свои часы для отметки времени прибытия сообщения Sync (T_{S1}) и сравнивает данную отметку с той, что пришла от ведущего устройства в сообщении Follow-up. Разница между этими

двумя метками отражает сдвиг тактов T_0 плюс задержку передачи сообщения от ведущего к ведомому: $\Delta T_{MS} = T_{S1}-T_{M1}=T_0+\Delta T_M$.

Для вычисления времени задержки передачи сообщения и сдвига отсчёта тактов ведомое устройство отправляет сообщение Delay-request со своим временем T_{S2}. Ведущее устройство отмечает прибытие данного сообщения и отправляет в ответ сообщение Delay-response меткой T_{M2}. Разница между двумя метками – это задержка передачи от ведомого к ведущему устройству ΔT_{SM} минус сдвиг в отсчёте ведомого устройства: $T_{M2}-T_{S2}= \Delta T_{SM}-T_0$.

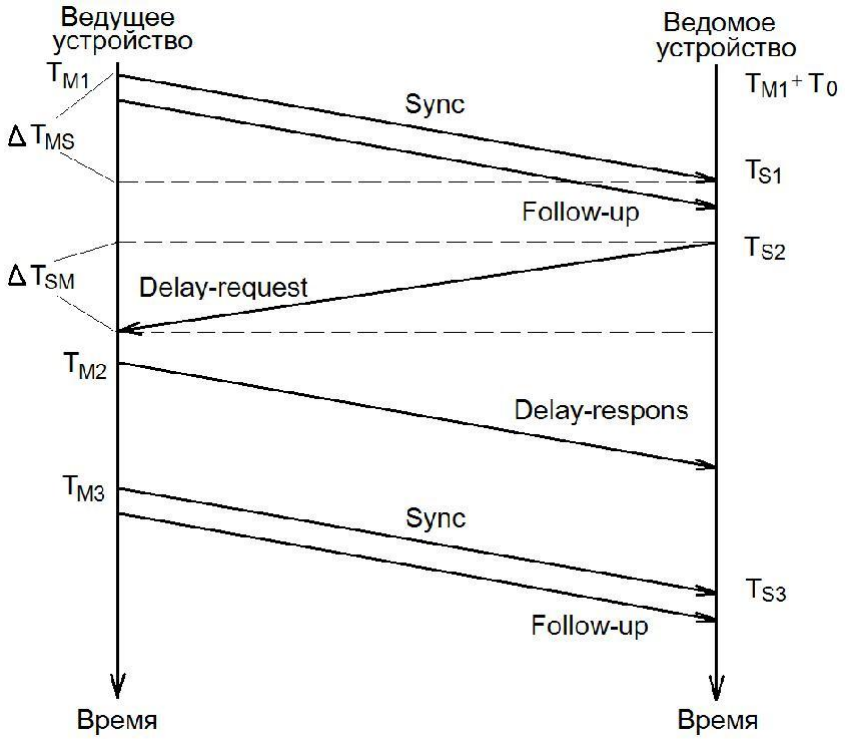


Рисунок 5 - Алгоритм протокола PTP

При вычислении задержки передачи сообщения принимается, что средняя задержка передачи данных в канале равна среднему арифметическому задержек распространения в разные стороны канала:

$$\Delta T = (T_{MS}+T_{SM})/2.$$

Зная времена T_{S1}, T_{M1}, T_{M2} и T_{S2} ведомое устройство вычисляет усреднённую задержку распространения в канале передачи данных:

$$\Delta T = [(T_{S1}-T_{M1})+(T_{M2}-T_{S2})]/2.$$

Финальная синхронизация тактов выполняется после отправки ведущим устройством второго набора сообщений Sync(T_{S3}) и Follow-up (T_{M3}). Ведомое устройство вычисляет сдвиг своих часов по формуле $T_0 = T_{M3} - \Delta T$. После этого ведомое устройство подстраивает свои такты в соответствии с вычисленными значениями. Поскольку опорные источники синхросигналов в каждом СЭ нестабильны и задержки в канале передачи данных могут меняться, должны производиться регулярные операции по коррекции тактов.

Реализация протокола PTP может иметь следующие решения: программное; программно-аппаратное; аппаратное. Наиболее высокую точность имеет аппаратная реализация. Наименьшую точность имеет программная реализация. Кроме того, на точность коррекции влияет частота тактов синхросигнала. Чем выше частота тактов, тем меньше точность. Кроме того, на качество синхронизации влияет топология сети и потоки трафика. Чем выше загрузка сети передачей данных, тем меньшая точность коррекции обеспечивается. По этим причинам для передачи синхросигналов предпочтительно использовать отдельную сеть передачи данных.

4 Особенности синхронизации в PON

Синхронизация PON на физическом уровне производится по тактам генератора OLT CDN, передаваемым к всем блокам ONU оптическими сигналами. Однако в каждой технологии PON (APON/BPON, GEPON/EPON и GPON) предусмотрены спецификации по синхронизации передачи данных, увязанные с механизмами регистрации ONU, предоставления временных ресурсов и т.д.

Синхронизация в сетях APON/BPON отличается принципом ранжирования (ranging), который определён для дистанций между OLT и ONU и для фазирования прямого и обратного потоков данных между OLT и n – количеством ONU. Ранжирование по дистанции (расстоянию) – это определение временной задержки, связанное с удалением на разные расстояния ONU от OLT, выполня-

ется на этапе регистрации абонентских узлов и требуется для бесконфликтного синхронизированного переноса пакетов в обратном направлении от ONU к OLT. Ранжирование по фазе необходимо для прямого и обратного направлений передачи. Суть этой синхронизации состоит в том, что абонентские узлы ONU синхронизируются в начале своей инициализации и затем всё время поддерживают синхронизацию, подстраиваясь под непрерывный поток трафика TDM. Это обеспечивает синхронный приём данных. Напротив, OLT синхронизируется каждый раз по преамбуле вновь приходящего пакета ATM от ONU. Метод приёма данных с синхронизацией по преамбуле называется асинхронным.

Синхронизация в сетях GEPON/EPON производится путём передачи служебных кадров от OLT к всем ONU в единой временной шкале. Т.е. отправка данных абонентскими узлами производится в разрешенные интервалы времени, которые называют «тайм-слоты». В «тайм-слот», длина которого определяется на OLT, может помещаться один или несколько кадров Ethernet. До поступления разрешения на передачу кадры хранятся в буферной памяти.

5 Схема синхронизации сети доступа

Схема синхронизации СД необходима для задания приоритетов использования синхросигналов, которые могут происходить от различных источников: коммутационного цифрового узла телефонной сети, коммутатора Ethernet или ATM, гибкого мультиплексора, включенного в транспортную сеть с арендой трактов, приёмника от навигационного спутника GPS или ГЛОНАСС и т.д. На схеме синхронизации показываются пути передачи тактового синхронизма и возможные схемы коррекции по известным протоколам NTP, PTP, SRTS. На рис. 6 представлен пример схемы прохождения синхросигналов в оптической СД, где в качестве ведущего узла синхронизации используется телефонная станция МС-240, которая включена через транспортную сеть в АМТС, имеющую ВЗГ, запитанный тактовым синхронизмом от ПЭГ ОАО РОСТЕЛЕКОМ.

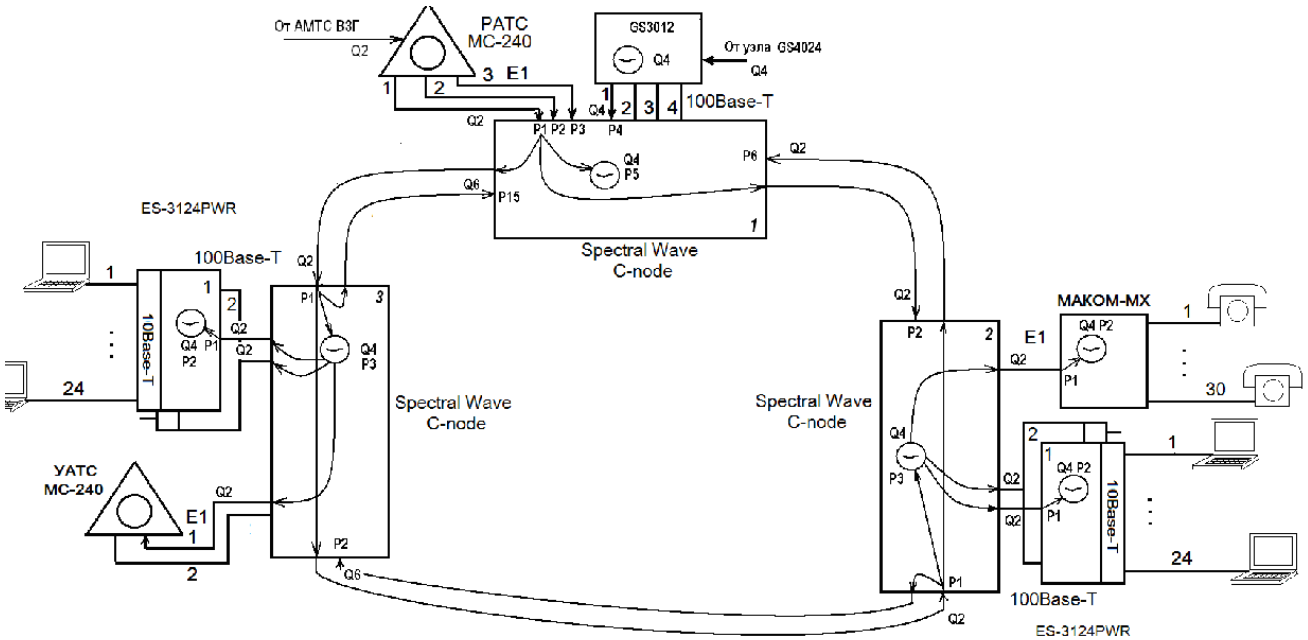


Рисунок 6 - Пример схемы синхронизации сети доступа

В схеме обозначены показатели качества Q2….Q6 и приоритеты P1….P15. Показатели качества распространяются в составе линейного сигнала STM1 в байте S1 заголовка секции мультиплексирования MSOH. В других схемах, например, с оборудованием коммутаторов Ethernet, показатели распространяются служебными пакетами имеют тот же смысл, что и в SDH. Приоритеты расставлены в каждом сетевом элементе из расчёта поддержки живучести синхронизации при различных аномальных состояниях на СД. При этом в сетевых элементах недопустимо использования хотя бы двух одинаковых приоритетов. Кольцо синхронизации может разрываться также установкой приоритета, как показано на рис.6 P6 в шлюзовом узле 1, где создаются интерфейсы в различные сети услуг. При составлении проектов сложных схем синхронизации необходимо все приоритеты и показатели качества представить отдельной таблицей (пример в табл. 4).

Таблица 4 - Распределение приоритетов и показателей качества синхронизации по сетевым элементам

Входные интерфейсы (Т – стандарты обозначений В аппаратуре)	1 сетевой элемент		2 сетевой элемент		3 сетевой элемент	
	P	Q	P	Q	P	Q
Внешний вход (Т3)	-	-	-	-	-	-
Линейный вход – запад (Т1)	P15	Q6	P2	Q6	P2	Q2
Линейный вход – восток (Т1)	P6	Q2	P1	Q2	P1	Q2
Компонентный вход Е1 (Т2) 1	P1	Q2	-	-	-	-
Компонентный вход Е1 (Т2) 2	P2	Q2	-	-	-	-
Компонентный вход Е1 (Т2) 3	P3	Q2	-	-	-	-
Компонентный вход 100Base-T (Т2) 4	P4	Q4	-	-	-	-
Внутренний генератор	P5	Q4	P3	Q4	P3	Q4

6 Управление оптической сетью доступа

Функционирование любой сети, в том числе сети доступа, невозможно без ее обслуживания на различных уровнях.

Обслуживание сети сводится в общем случае к автоматическому, полуавтоматическому или ручному управлению системой, ее тестированию и сбору статистики о прохождении сигнала и возникающих неординарных или аварийных ситуациях, а также менеджменту (административному управлению системой). Эти функции в свою очередь невозможно осуществить без сигнализации различного рода о состояниях системы, например сигнализации о возникновении аварийного состояния. Сигнализация должна осуществляться по специальным встроенным или зарезервированным для этого каналам, связывающим управляющие (оперирующие на сети) операционные системы OS и управляемые системы или сетевые элементы NE.

Управление сетью доступа осуществляется на физическом, логическом, информационном и административном уровнях. Информационный и административный уровни относятся к особой категории управления – менеджменту.

Функциональные группы задач управления системами определены в стандарте ITU-T X.700:

- управление конфигурацией (Configuration Management);
- обработка ошибок (Fault Management);
- анализ производительности и надёжности (Performance management);
- управление безопасностью (Security Management);
- учёт работы (Accounting Management).

Для решения задач управления на всех уровнях необходима модель сети и описание типов интерфейсов связи, необходимые для реализации функций управления на различных участках сети. Такую модель создал ITU-T, обозначенную как концепция TMN (Telecommunications Management Network) и подробно представленная в рекомендации М.3010. При этом для сети доступа возможны упрощения на всех уровнях управления, которые касаются набора функций управления, протоколов управления, интерфейсов управления, информационных баз данных управления и т.д.

Кроме ITU-T разработкой стандартов управления заняты следующие организации:

- IETF, Internet Engineering Task Force - специальная комиссия интернет-разработок — открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, созданное в 1986 году, которое занимается развитием протоколов и архитектуры Интернета, стандарты протоколов SNMP (Simple Network Management Protocol – простой протокол управления сетью), HTTP (HyperText Transfer Protocol - протокол передачи гипертекста), FTP (File Transfer Protocol - протокол передачи файлов), TELNET (протокол сетевых телекоммуникаций);
- ISO, International Standardization Organization — Международная организация по стандартизации, ИСО международная организация, занимающаяся выпуском стандартов, стандарты протоколов CMIP (Common Management Information Protocol – общий протокол информации управления), CMIS (Common management Information Service - информационная услуга общего управления);
- DMTF, Distributed Management Task Force – рабочая группа по управлению настольными системами, стандарты протоколов WBEM (Web-Based Enterprise Management – веб основанное управление предприятием) , CIM (Common Information Model – общая модель информации);

- OMG, Object Management Group – группа объектного управления, стандарты протоколов CORBA (Common Object Request Broker Architecture – общая архитектура брокера объектных запросов).

Наибольшее распространение в сетях доступа получили протоколы управления IETF, относящиеся к прикладному уровню семиуровневой и четырёхуровневой моделям (см. рис. 7) передачи данных.

При этом чаще всего функции нижних уровней (транспортного, сетевого, канального) выполняются основе модели TCP/IP. Т.е. используются протоколы транспортировки пакетов TCP и UDP, протокол сетевой маршрутизации IP, а на канальном уровне пакеты упаковываются в кадры Ethernet, ячейки ATM или другие структуры передачи данных. Использование в качестве транспортной сети для управления Internet указывает на вид управления Web – управление. В качестве физического уровня взаимодействия в сети управления может использоваться любая подходящая среда передачи (проводная и беспроводная) по скорости передачи данных и по количеству допустимых ошибок передачи. Например, такой средой может быть канальный интервал в цикле E1, который поддерживает скорость 64кбит/с, как в проводном, так и в беспроводном соединении, или другой вариант, выделенная сеть VLAN и т.п.

Уровни модели ISO/OSI				Уровни модели протоколов TCP/IP
7	**Прикладной** Интерфейс с прикладными процессами	4	**Прикладной** Формирование потока данных FTP, RSTP, HTTP, SNMP , ...	
6	**Представительский** Согласование форматов представления данных			
5	**Сеансовый** Поддержка диалога прикладных процессов Соединение и разъединение	3	**Транспортный** Формирование сегментов или дейтаграмм TCP, UDP	
4	**Транспортный** Сквозной обмен информацией между системами			
3	**Сетевой** Вид сервиса сетевой маршрутизации, сегментирование и объединение блоков данных, обнаружение ошибок	2	**Сетевой** Формирование пакетов IP или дейтаграмм	
2	**Канальный** Управление каналом передачи данных. передача данных по каналу , обнаружение и устранение ошибок	1	Нет спецификации (реализация вне протоколов TCP/IP)	
1	**Физический** Физический интерфейс с каналом передачи данных			

Рисунок 7 - Модели передачи данных

В сетях доступа применяют следующие виды управления:

- консольное, т.е. непосредственное введение команд управления в строке через подключенный к сетевому элементу персональный компьютер;
- управление через Web-узел или управление с использованием ресурсов любой подходящей сети передачи данных, чаще всего Internet, средствами протоколов Telnet, SNMP и др.;
- управление через специализированную систему управления фирменного производства с применением протоколов TCP/IP или ISO/OSI, встроенных каналов передачи данных, что характерно для платформенных систем Fast Link от Siemens или HONET от Huawei.

Каждый вид управления имеет свои особенности, достоинства и недостатки, оценки которых могут подсказать выбор наиболее подходящего решения при проектировании СД [8, 9].

Организация управления СД, как правило, централизованная, т.е. в структуре управления выделяются программы управления, которые называют в международной стандартизации Менеджером и Агентом открытых систем (рис.8).

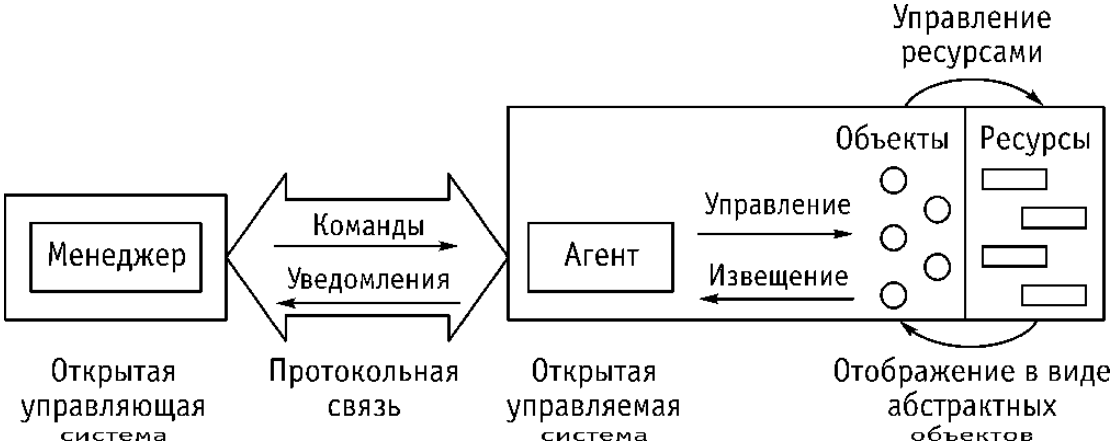


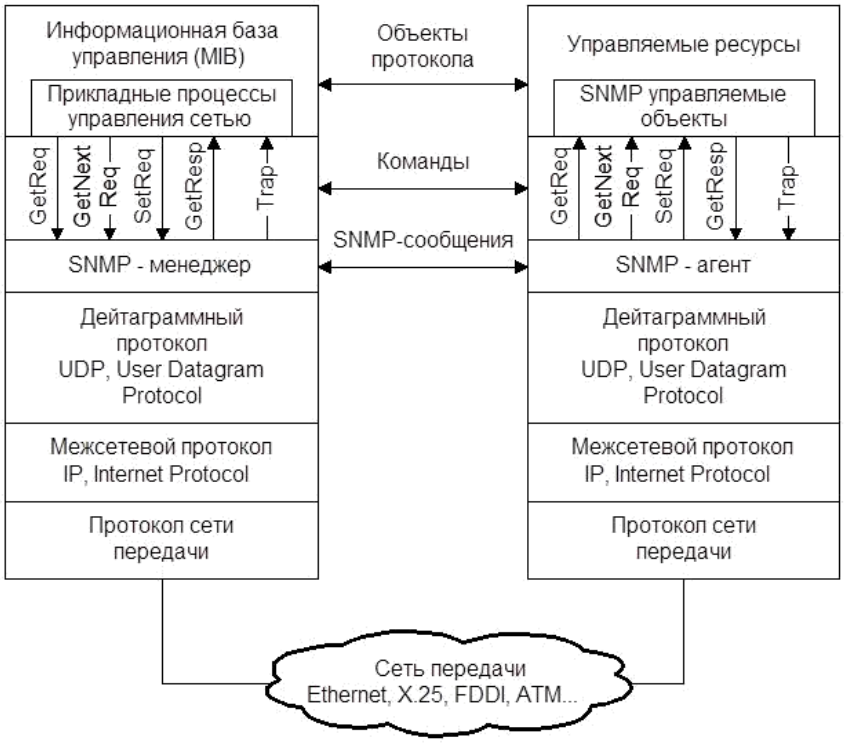
Рисунок 8 - Принцип взаимодействия в системе управления

«Менеджер» размещается на сервере в центре управления, а «Агенты» помещаются в операционные системы управляемых сетевых элементов (мультиплексоры, коммутаторы, сетевые терминалы у пользователей и т.д.). «Менеджер» и «Агенты» имеют базу данных управления MIB (Management Information Base), в которой

фиксируются все объекты управления и их состояния, отражающие состояния реальных ресурсов. «Менеджер» посылает команды управления «Агентам». «Агенты» уведомляют «Менеджера» и исполнении команд. При аномальных состояниях оборудования, соединений и т.д. «Агент» посылает запросы «Менеджеру» о необходимости обратить внимание (Trap - прерывание).

Пример общей структуры управления с использованием возможностей прикладных протоколов управления SNMP представлен на рис. 9.

Протоколы SNMP, HTTP, FTP и TELNET получили широкое применение в управлении сетевыми элементами и сетями доступа с различным оборудованием. Все эти протоколы имеют стандартное взаимодействие с протоколом TCP и UDP с определёнными по умолчанию номерами портов серверов, например, HTTP имеет порт TCP 80, а FTP имеет порт TCP 21, TELNET имеет порт TCP 23, SNMP имеет порты TCP 161 и 162 и т.д.[10].



Команды протокола SNMP:

GetReqest - менеджер запрашивает требуемый параметр о SNMP - агента управляемой станции;

GetNextReqest - менеджер запрашивает у агента очередной параметр;

SetReqest - менеджер устанавливает заданную величину параметра для управляемого объекта;

GetResponse - ответ агента на любой запрос с включением информации об ошибках в содержательной части ответа;

Trap - реакция агента на воздействие от ресурсов в сторону станции управления (прерывания).

Рисунок 9 - Взаимодействие в структуре «Агент-Менеджер» на основе SNMP

Протокол TELNET позволяет обслуживающему серверу рассматривать все удаленные терминалы как стандартные "сетевые виртуальные терминалы" строчного типа, работающие в коде ASCII (американский стандартный код для обмена информацией), а также обеспечивает возможность согласования более сложных функций (например, локальный или удаленный эхо-контроль, страничный режим, высота и ширина экрана и т.д.) TELNET работает на базе протокола TCP. На прикладном уровне над TELNET находится либо программа поддержки реального терминала (на стороне пользователя), либо прикладной процесс в обсуживающем сервере управления, к которому осуществляется доступ с терминала.

Работа с TELNET походит на набор телефонного номера. Пользователь набирает на клавиатуре что-то вроде telnet delta и получает на экране приглашение на вход в машину delta.

Протокол строится на базе протокола TCP и работает по дуплексному, многопользовательскому протоколу. Это значит, что один сервер может обслуживать одновременно несколько терминалов.

Протокол TELNET построен на трех основных принципах:

1 NVT - Network Virtual Terminal - принцип виртуальных сетевых терминалов. После установления соединения предполагается, что каждый участник работает как «Виртуальный сетевой терминал» - мнимое устройство, выполняющее стандартные сетевые промежуточные функции обычного терминала.
2 Принцип настраиваемых параметров. Если хост предоставляет дополнительный сервис помимо NVT, и клиент в состоянии его использовать, TELNET предоставляет возможность сделать это.
3 Принцип симметрии терминалов и процессов. Участники соединения равноправны.

NVT - устройство для ввода/вывода 7-и битных ASCII символов. Все преобразования и кодировки выполняются выше NVT и не рассматриваются как часть NVT. NVT имеет устройство ввода

«виртуальная клавиатура» и устройство вывода «виртуальный принтер», что выглядит как дисплей. Выводное устройство не имеет ограничений на ширину и выводит все печатаемые символы из диапазона 32 - 126. Управляющие коды ASCII (0-31, 127) имеют специальное значение. Коды 128-255 имеют также специальное назначение (табл. 5).

Таблица 5 - Управляющие коды ASC11

0	NULL	Пусто
10	LF	Перенос курсора на следующую строку с сохранением позиции.
13	CR	Перенос курсора на начало текущей строки.
7	BELL	Звонок
8	BS	Перенос курсора на одну позицию влево
9	HT	Перенос курсора на следующую позицию горизонтальной табуляции
11	VT	Перенос курсора на следующую позицию вертикальной табуляции
12	FF	Перенос курсора на начало след страницы с сохранением позиции в строке

Ввод и передача буферируются. Данные накапливаются в буфере пока не будет завершена строка или не будет выполнено форсирование передачи до завершения строки. Клавиатура должна генерировать все 128 кодов, соответствующих 128 ASCII символам. Кроме того, она должна генерировать управляющие коды от 244 до 255 (табл. 6).

Таблица 6 - Управляющие коды клавиатуры

244	IP	Interrupt Process - прервать процесс. Команда останавливает операции или процесс пользователя. Используется при зависании или ошибках.
245	AO	Abort Output - прервать вывод. Вывод прекращается и выводной буфер очищается.
246	AYT	Are You There - вы тут?
247	EC	Erase Char - Удалить символ из буфера.
248	EL	Erase Line - Удалить строку. Очищает текущую строку ввода.
249	GA	Go Ahead - Далее. Передача контроля над соединением без

		отправки каких либо данных.
250	SB	SubNegotiation, Параметры расширения. Указывает, что за этим последует передача дополнительных опций
240	SE	Subnegotiation End. Конец параметров расширения.
251	WILL	квитанция согласования.
252	WON'T	квитанция согласования.
253	DO	квитанция согласования.
253	DON'T	квитанция согласования.
255	IAC	Interpret As Command - Код команды. Следующий байт - команда telnet. Третий опциональный байт - код настраиваемой опции.

TELNET является универсальным клиентом и позволяет соединиться с большим количеством портов и общаться с различными приложениями.

FTP — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов (баз данных) и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами. Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов. Процесс нешифрованной авторизации проходит в несколько этапов (символы \r\n означают перевод строки): установка TCP-соединения с сервером (обычно на 21 порт); посылка команды USER ***логин***\r\n; посылка команды PASS ***пароль***\r\n.

Если к серверу разрешён анонимный доступ (как правило, лишь для загрузки данных с сервера), то в качестве логина используется ключевое слово «anonymous» или «ftp», а в качестве пароля

— адрес электронной почты: USER anonymous\r\n; PASS someone@email\r\n.

После успешной авторизации можно посылать на сервер другие команды.

- ABOR — Прервать передачу файла.
- CDUP — Сменить директорию на вышестоящую.
- CWD — Сменить директорию.
- DELE — Удалить файл (DELE filename).
- EPSV — Войти в расширенный пассивный режим. Применяется вместо PASV.
- HELP — Выводит список команд принимаемых сервером.
- LIST — Возвращает список файлов директории. Список передается через соединение данных.
- MDTM — Возвращает время модификации файла.
- MKD — Создать директорию.
- NLST — Возвращает список файлов директории в более кратком формате чем LIST. Список передается через соединение данных.
- NOOP — Пустая операция
- PASV — Войти в пассивный режим. Сервер вернет адрес и порт к которому нужно подключиться чтобы забрать данные. Передача начнется при введении следующих команд RETR, LIST и тд.
- PORT — Войти в активный режим. Например PORT 12,34,45,56,78,89. В отличие от пассивного режима для передачи данных сервер сам подключается к клиенту.
- PWD — Возвращает текущую директорию.
- QUIT — Отключиться
- REIN — Реинициализировать подключение.
- RETR — Скачать файл. Перед RETR должна быть команда PASV или PORT.
- RMD — Удалить директорию
- RNFR и RNTO — Переименовать файл. RNFR — что переименовывать, RNTO — во что
- SIZE — Возвращает размер файла

- STOR — Закачать файл. Перед STOR должна быть команда PASV или PORT
- STOU — Закачать файл. Перед STOR должна быть команда PASV или PORT
- SYST — Возвращает тип системы(UNIX, WIN, …)
- TYPE — Установить тип передачи файла(Бинарный, текстовый)
- USER — Имя пользователя для входа на сервер

HTTP (HyperText Transfer Protocol - протокол передачи гипертекста) был разработан как основа World Wide Web - всемирной паутины.

Основой протокола HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP в настоящее время повсеместно используется во всемирной паутине для получения информации с веб-сайтов. HTTP используется также в качестве «транспорта» для других протоколов прикладного уровня, таких как SOAP, XML-RPC, WebDAV.

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объекты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т. д. Именно благодаря возможности указания способа кодирования сообщения клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

HTTP — протокол прикладного уровня, аналогичными ему являются FTP и SMTP. Обмен сообщениями идёт по обыкновенной схеме «запрос-ответ». Для идентификации ресурсов HTTP использует глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-

ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами. Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

Работа по протоколу HTTP происходит следующим образом: программа-клиент устанавливает TCP-соединение с сервером (стандартный номер порта-80) и выдает ему HTTP-запрос. Сервер обрабатывает этот запрос и выдает HTTP-ответ клиенту. HTTP-запрос состоит из заголовка запроса и тела запроса, разделённых пустой строкой. Тело запроса может отсутствовать. Заголовок запроса состоит из главной (первой) строки запроса и последующих строк, уточняющих запрос в главной строке. Последующие строки также могут отсутствовать.

Команды HTTP:

GET - запрос документа. Наиболее часто употребляемый метод; в HTTP/0.9, говорят, он был единственным.

HEAD - запрос заголовка документа. Отличается от GET тем, что выдается только заголовок запроса с информацией о документе. Сам документ не выдается.

POST - этот метод применяется для передачи данных CGI-скриптам. Сами данные следуют в последующих строках запроса в виде параметров.

PUT - разместить документ на сервере. Насколько я знаю, используется редко. Запрос с этим методом имеет тело, в котором передается сам документ.

Ресурс - это путь к определенному файлу на сервере, который клиент хочет получить (или разместить - для метода PUT). Если ресурс - просто какой-либо файл для считывания, сервер должен по этому запросу выдать его в теле ответа. Если же это путь к какому-либо CGI-скрипту, то сервер запускает скрипт и возвращает результат его выполнения. Кстати, благодаря такой унификации ресурсов для клиента практически безразлично, что он представляет собой на сервере.

Версия протокола - версия протокола HTTP, с которой работает клиентская программа. Таким образом, простейший HTTP-запрос может выглядеть следующим образом:

GET / HTTP/1.0

Здесь запрашивается корневой файл из корневой директории web-сервера. Строки после главной строки запроса имеют следующий формат:

Параметр: значение.

Таким образом, задаются параметры запроса. Это является необязательным, все строки после главной строки запроса могут отсутствовать; в этом случае сервер принимает их значение по умолчанию или по результатам предыдущего запроса (при работе в режиме Keep-Alive).

Перечислю некоторые наиболее употребительные параметры HTTP-запроса:

Connection (соединение)- может принимать значения Keep-Alive и close. Keep-Alive ("оставить в живых") означает, что после выдачи данного документа соединение с сервером не разрывается, и можно выдавать еще запросы. Большинство браузеров работают именно в режиме Keep-Alive, так как он позволяет за одно соединение с сервером "скачать" html-страницу и рисунки к ней. Будучи однажды установленным, режим Keep-Alive сохраняется до первой ошибки или до явного указания в очередном запросе Connection: close. close ("закрыть") - соединение закрывается после ответа на данный запрос.

User-Agent - значением является "кодовое обозначение" браузера, например:

Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)

Accept - список поддерживаемых браузером типов содержимого в порядке их предпочтения данным браузером, например для IE5:

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, */*

Это, очевидно, нужно для случая, когда сервер может выдавать один и тот же документ в разных форматах.

Значение этого параметра используется в основном CGI-скриптами для формирования ответа, адаптированного для данного браузера.

Referer - URL, с которого перешли на этот ресурс.

Host - имя хоста, с которого запрашивается ресурс. Полезно, если на сервере имеется несколько виртуальных серверов под одним IP-адресом. В этом случае имя виртуального сервера определяется по этому полю.

Accept-Language - поддерживаемый язык. Имеет значение для сервера, который может выдавать один и тот же документ в разных языковых версиях.

Формат ответа очень похож на формат запроса: он также имеет заголовок и тело, разделенное пустой строкой.

Заголовок также состоит из основной строки и строк параметров, но формат основной строки отличается от таковой в заголовке запроса.

Основная строка запроса состоит из 3-х полей, разделенных пробелами:

Версия протокола - аналогична соответствующему параметру запроса.

Код ошибки - кодовое обозначение "успешности" выполнения запроса.

Код 200 означает "все нормально" (OK).

Словесное описание ошибки - "расшифровка" предыдущего кода.

Например для 200 это OK, для 500 - Internal Server Error.

Наиболее употребительные параметры http-ответа:

Connection - аналогичен соответствующему параметру запроса. Если сервер не поддерживает Keep-Alive (есть и такие), то значение Connection в ответе всегда close.

Протокол SNMP, представленный семейством протоколов разных версий, работает на базе транспортных возможностей UDP (возможны реализации и на основе TCP) и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении в сети Интернет. Протокол определяет формат данных, а их обработка и интерпретация остаются на усмотрение управляющих станций или

менеджера сети. SNMP-сообщения не имеют фиксированного формата и фиксированных полей. При своей работе SNMP использует управляющую базу данных MIB.

Семейство стандартов SNMP создано для решения задач обработки ошибок и анализа производительности и надёжности.

Обработка ошибок

выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне выполняется регистрация сообщений об ошибках, их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели.

Анализ производительности и надёжности оценка на основе статистической информации таких параметров, как время реакции системы, пропускная способность каналов связи, интенсивность трафика в отдельных сегментах сети, вероятность искажения данных, коэффициент готовности служб сети. Результаты такого анализа позволяют контролировать соглашение об уровне обслуживания SLA (Service Level Agreement).

Согласно идеологии SNMP, управление должно быть простым, пусть даже ценой потери мощности, масштабируемости и защищённости. Поэтому при разработке стандартов SNMP учитывались следующие условия:

- Повсеместность. Системы под управлением SNMP могут быть любыми и могут быть везде: от принтеров до коммутационных узлов, абонентских терминалов.
- Простота добавления управляющих функций. Управляемая система ограничена в функциональности управления, очень проста и не может контролировать себя. Вместо этого все управляемые системы контролирует сложная управляющая система, функциональность которой можно расширять.
- Устойчивость в критических ситуациях. Например, при перегрузке и проблемах в сети, т. е. при множественных ошибках.

Архитектуру системы управления на основе протокола SNMP можно описать в терминах обрабатывающих элементов (или компонентов), соединяющих элементов (или соединителей) и элементов данных. Составные элементы системы управления SNMP:

- компоненты

- Агент

- Менеджер

- соединители

- транспортный протокол

- протокольные блоки данных PDU (Protocol Data Units) и сообщения SNMP

- данные

-управляющая информация MIB.

Менеджер взаимодействует с агентами при помощи протокола SNMP с целью обмена управляющей информацией. В основном, это взаимодействие реализуется в виде периодического опроса менеджером множества агентов, т. к. агенты всего лишь предоставляют доступ к информации, но не знают, что им с ней делать. Видно, что система, построенная по таким принципам, теряет в масштабируемости, поскольку есть выделенный клиент, занимающийся опросом всех серверов. Зато такая схема обеспечивает простоту реализации систем под управлением SNMP.

Для повышения масштабируемости и административной управляемости вводится понятие прокси-агента, который может переправлять операции протокола SNMP, а также понятие менеджера промежуточного уровня, который скрывает несущественные подробности управляющей информации от систем управления сетями верхнего уровня, интегрируя получаемые от агентов данные. Это позволяет создавать многоуровневые системы управления, соответствующие архитектурному стилю «многоуровневый клиент-сервер» (рис. 10).

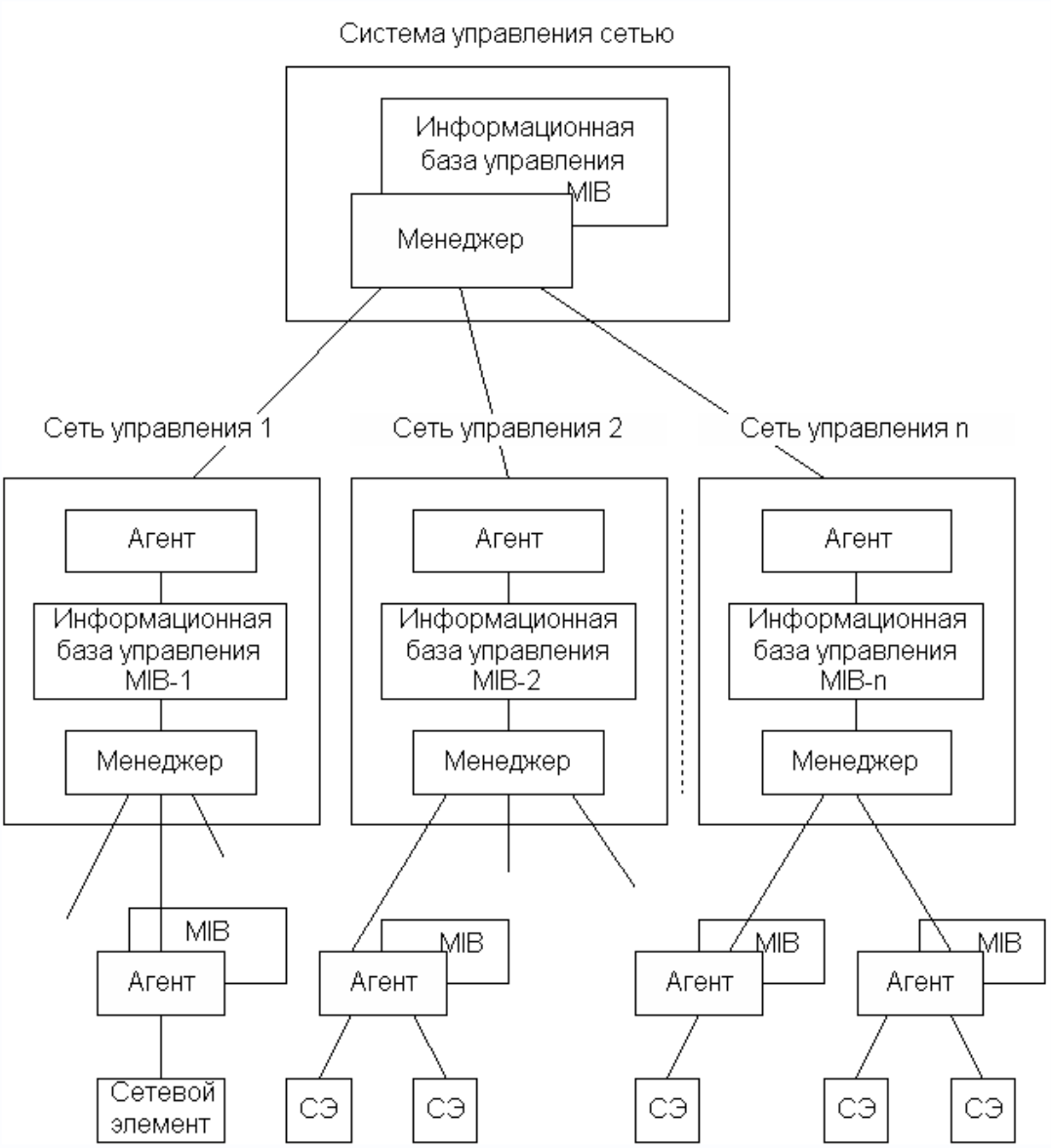


Рисунок 10 - Многоуровневое управление средствами SNMP

Более детальная классификация компонентов по ролям:

- Менеджер
- Менеджер промежуточного уровня
- Система управления сетями
- Агент
- Минимальный агент
- Прокси-агент
- Менеджер промежуточного уровня.

В SNMP каждое управляемое устройство, на котором расположен агент, представляет свою управляющую информацию в виде переменных. Такими переменными могут быть, например, имя системы, время с момента её перезапуска, записи в таблице мар-

шрутизации и т. д. В общем случае переменные можно разделить на скалярные переменные и таблицы переменных.

Схема данных описывается структурой управляющей информации SMI (Structure of Management Information). Схема данных определяет, как выглядит управляющая информация, т. е. описывает её синтаксис. SMI базируется на Abstract Syntax Notation One (ASN.1).

Конкретные наборы управляющей информации для разных типов устройств, протоколов и т. д. описываются базами управляющей информации MIBs (Management Information Bases). Базы MIB определяют, какая управляющая информация существует. Например, для устройства, поддерживающего IP, MIB описывает таблицу маршрутизации, флажок активации функции маршрутизации, число переданных и принятых пакетов, число ошибок различного характера и т. д.

Для протокола SNMP существует несколько стандартов баз данных управляющей информации: MIB-1, MIB-2, RMON MIB, которые могут быть задействованы в структуре управления. Кроме того, существуют другие специальные базы данных управления конкретного типа (концентраторов, модемов).

Спецификация MIB-1 определяет только операции чтения значений переменных. В MIB-1 определены 114 объектов, которые сгруппированы в 8 блоков:

System – общие данные об устройстве;

Interfaces – параметры сетевых интерфейсов устройства;

Address Translation Table – описание соответствия между сетевыми и физическими адресами;

Internet Protocol – данные, относящиеся к протоколу IP;

ICMP (Internet Control Message Protocol) – данные, относящиеся к протоколу обмена управляющими сообщениями;

TCP – данные, относящиеся к протоколу TCP; UDP – данные, относящиеся к протоколу UDP;

EGP (Exterior Gateway Protocol) – данные, относящиеся к протоколу обмена маршрутной информацией.

Спецификация RMON MIB содержит около 2000 объектов, сгруппированных в 10 блоках. RMON обеспечивает удаленное взаимодействие базой MIB. Объекту RMON присвоен номер 16 в

наборе объектов MIB, а сам объект RMON объединяет 10 блоков следующих объектов:

Statistics – текущие накопления статистических данных о характеристиках пакетов, количестве столкновений и т.п.;

History – статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений;

Alarms – пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру;

Hosts – данные о главных станциях сети;

Filter – условия фильтрации пакетов и так далее.

Таким образом, каждое устройство содержит набор значений переменных, определённых в некотором количестве MIB, описанных по правилам SMI. Этот набор переменных и является данными, управляющей информацией для протокола SNMP.

Важным вопросом является именование переменных. В SNMP каждой переменный присваивается уникальный идентификатор объекта OID (Object Identifier). Пространство имён OID является иерархическим и контролируется организацией по распределению номеров в Интернете IANA (Internet Assigned Numbers Authority). Каждый компонент имени является числом. В текстовом виде имена записываются как десятичные числа, разделённые точками, слева направо. Числам могут быть поставлены в соответствие текстовые строки для удобства восприятия. В целом, структура имени похожа на систему доменных имён Интернета DNS (Domain Name System).

Каждая MIB определяет набор переменных, т. е. определённую ветку дерева OID, описывающую управляющую информацию в определённой области. Например, ветка 1.3.6.1.2.1.1 (мнемонический эквивалент: iso.org.dod.internet.mgmt.mib-2.system) описывает общую информацию о системе. Опишем некоторые переменные из этой ветки:

- sysDescr (1.3.6.1.2.1.1.1) — краткое описание системы
- sysUpTime (1.3.6.1.2.1.1.3) — время с момента последнего перезапуска
- sysName (1.3.6.1.2.1.1.5) — имя системы.

Переменные и сведения об их типе определены также в MIB. А сами типы переменных — в SMI.

Помимо непосредственно данных, необходимо ввести операции над ними. Набор этих операций изменялся и расширялся по мере развития SNMP. Основными операциями являются:

- чтение переменной
- запись переменной
- чтение переменной, следующей за заданной переменной (требуется для просмотра таблиц переменных).

В целом, операции над данными в SNMP похожи на удалённую отладку некоторого приложения: состояние системы описывается неким набором переменных, которые можно просматривать и изменять.

Для обмена данными между компонентами используются соединители. В случае SNMP в качестве соединителя используется протокол прикладного уровня, обычно работающий поверх стека протоколов UDP/IP. Современные стандарты SNMP разрешают использование и других транспортных протоколов.

Стек протоколов с привязкой протоколов к Open Systems Interconnection Reference Model (OSI RM) приведён в табл. 7.

SNMP вводит свой протокол прикладного уровня. Имеются четыре версии данного протокола: SNMPv1, SNMPv2, SNMPv2c и SNMPv3. Во всех версиях предусмотрены базовые команды (табл. 8). В процессе развития SNMP расширялись возможные операции, т. е. типы протокольных блоков данных PDUs (Protocol Data Units), а также вводились новые форматы сообщений SNMP для обеспечения безопасности. Т.о. версии семейства протоколов отличаются степенью безопасности передачи информации управления.

Таблица 7 Наполнение стеков протоколов

Уровень	Протокол	Комментарий
7	SNMP	Сообщения, PDU, операции
6	ASN.1 BER	Кодирование данных
5	—	—
4	UDP	Транспорт между службами
3	IP	Связь между узлами сети

Таблица 8 Команды SNMP

Команда SNMP	Тип PDU	Назначение
Get - request	0	Получить значение указанной переменной или информацию о состоянии сетевого элемента
Get - next request	1	Получить значение переменной, не зная точного её имени (следующий логический индикатор на дереве MIB)
Set - request	2	Присвоить переменной соответствующее значение, используя для описания действия, которое должно быть выполнено
Get - respons	3	Отклик на Get – request, Get_next_request. Содержит также информацию о состоянии (коды ошибок и другие данные)
Trap	4	Отклик сетевого объекта на событие или на изменение состояния
Get Bulk Rquest	5	Запрос посылки больших объёмов данных, например, таблиц
Inform Request	6	Менеджер обращает внимание агента на определённую информацию в MIB
SNMPv3-Trap	7	Отклик на событие (расширение по отношению к v1, v2)
Report	8	Отчёт

У версии SNMPv1 вопрос безопасности не стоял во время его разработки, что оказалось уязвимым для сети управления. Версия 2, известная так же, как Party-based SNMPv2, или SNMPv2p, не получила широкого распространения из-за серьёзных разногласий по поводу инфраструктуры безопасности в стандарте. SNMPv2 улучшал версию 1 в области быстродействия, безопасности, конфиденциальности и взаимодействий «менеджер-менеджер». Он представил новый тип PDU Get-Bulk-Request, альтернативу Get-Next-Request для получения больших объёмов информации при помощи одного запроса. Тем не менее, новая система безопасности на основе сторон выглядела для многих как чересчур сложная и не была широко признана.

Community-based SNMPv2, или SNMPv2c, представил SNMPv2 без новой модели безопасности версии 2. Вместо неё предлагалось использовать старую модель безопасности версии 1 на основе сообществ. Соответствующее предложение RFC было принято только как черновик стандарта, однако стало де факто стандартом SNMPv2. Безопасность SNMP снова оказалась нерешённым вопросом. User-based SNMPv2, или SNMPv2u, является компромиссом между незащищённостью SNMPv1 и чрезмерной сложностью SNMPv2p. Предложенная модель безопасности на основе пользователей была положена в основу SNMPv3. SNMPv3 наконец-то решил проблемы с безопасностью способом, который многие посчитали приемлемым. Версия 3 SNMP принята IETF как стандарт Интернета (IETF STD 62). Почти все предыдущие RFC признаны устаревшими.

Сообщение SNMP содержит номер версии SNMP, информацию о безопасности и протокольный блок данных PDU, который характеризует выполняемую операцию и её параметры. Описанные PDU, как уже упоминалось, являются частью сообщения SNMP. Сообщения кодируются для передачи по сети при помощи ASN.1 Basic Encoding Rules (BER). Это функция шестого уровня (уровня представления) эталонной модели OSI. Далее закодированные сообщения отправляются одним компонентом SNMP другому при помощи транспортного протокола.

Как уже отмечалось, стандарт предусматривает использование различного транспорта для SNMP, но почти что всегда используется протокол пользовательских датаграмм UDP (User Datagram Protocol). Агенты используют хорошо известный порт UDP 161 (рис.11). Этот протокол предоставляет минимальные транспортные услуги (доставка сообщений от службы к службе и проверка контрольной суммы) и не предполагает организацию сеансов и потоковую передачу данных, как Transmission Control Protocol (TCP). За счёт этого удаётся добиться большой скорости реакции и быстродействия, что соответствует поставленным перед SNMP целям.

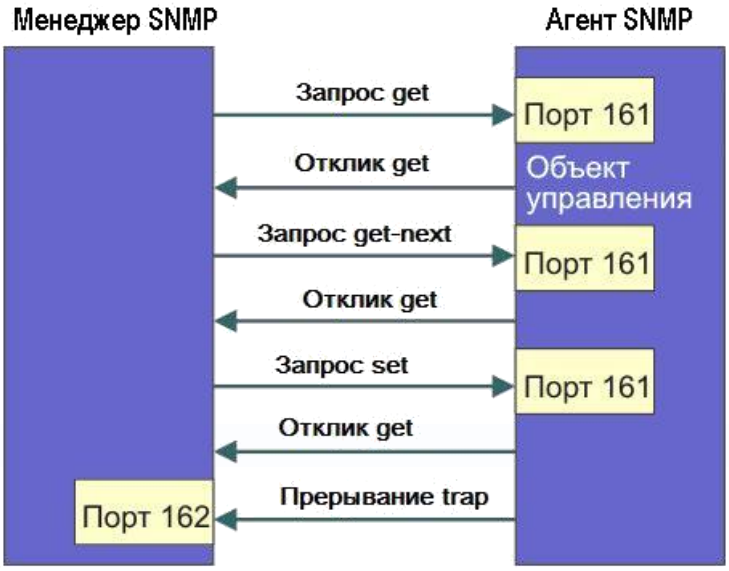


Рисунок 11 - Схема запросов/откликов SNMP

Для повышения скорости реакции менеджера на срочные события вводится специальный тип операции протокола SNMP, называемый «ловушка» (Trap). Он позволяет агентам асинхронно информировать менеджера (по собственной инициативе) о наступлении ограниченного числа значимых событий. В этом случае агент выступает в необычной для себя роли клиента, а менеджер — в роли сервера. В случае использования транспорта UDP для входящих соединений менеджер использует хорошо известный порт UDP 162 (табл. 9).

Таблица 9 Номера и назначения используемых портов

Назначение	Порт	Пояснение
SNMP	161/TCP	Simple Network Management Protocol
SNMP	162/TCP	Trap
SMUX	199/TCP	SNMP Unix Multiplexer
SMUX	199/UDP	SNMP Unix Multiplexer
Synoptics-relay	391/TCP	SynOptics SNMP Relay Port
Synoptics-relay	391/UDP	SynOptics SNMP Relay Port
agentx	705/TCP	AgentX
Snmp-tcp-port	1993/TCP	Cisco SNMP TCP port
Snmp-tcp-port	1993/UDP	Cisco SNMP TCP port

Необходимо отметить, что ни одна из этих операций не предполагает, что агент хранит информацию о сессии с менеджером. Для выполнения операции Trap такая информация хранится статически, т. е. сессия в таком случае статична и перманентна. Помимо этого операции SNMP определяют единые, унифицированные интерфейсы агентов и менеджеров SNMP. Таким образом, SNMP — это протокол без сохранения состояния, который соответствует архитектурному стилю «унифицированный многоуровневый клиент-сервер без сохранения состояния».

В качестве заключения необходимо отметить достоинства семейства протоколов SNMP:

- SNMP широко используется для управления сетями, особенно IP-сетями
- Успех SNMP по сравнению с другими стандартами управления показывает преимущества процесса стандартизации IETF
- История развития SNMP показывает важность задач защиты информации
- Архитектура SNMP интересна как пример для анализа архитектуры сетевого программного обеспечения; она соответствует поставленным перед SNMP целям
- Архитектура SNMP соответствует архитектурному стилю ULCSS сетевого программного обеспечения
- В SNMP для решения функций 6 уровня модели OSI RM используется ASN.1, что необычно для стандартов IETF и положительно сказывается на вопросах формализации протоколов, однозначности стандартов, удобства проектирования приложений
- Структура стандартов SNMP хорошо продумана и показательна как пример для изучения стандартов
- Лишь некоторые модели безопасности SNMP отвечают поставленным перед системой безопасности SNMP целям
- SNMP сравним со всеми объектами в мире, а в случае сетевых технологий 4-7 уровня OSI RM это к тому же имеет практический смысл и может иметь теоретический смысл

- Агенты и менеджеры SNMP просты в программной реализации, однако всегда нужно помнить об информационной безопасности

7 Схема управления сетью доступа

Схема управления сетью доступа составляется для обозначения всех интерфейсов управления, каналов передачи данных управления, технологий управления и оборудования управления. В конечном итоге средства управления, которые не относятся к базовой комплектации каждого сетевого элемента, должны быть внесены в таблицу комплектации, например, серверы управления, рабочие станции управления, соединительные кабели и т.д. Упрощенный пример схемы управления СД представлен на рис. 12.

В приведённом примере схемы управления каждый сетевой элемент включен в сеть управления через соответствующие каналы: АТС МС-240 и мультиплексор МАКОМ – МХ подключены в сеть через 31 канальный интервал потоков Е1; коммутаторы Ethernet включены в другую сеть управления через виртуальные каналы, задаваемые MAC-адресами при конфигурировании сети.

В каждом сетевом элементе устанавливается программа «Агент» управления (А), которая взаимодействует через протокол управления (Telnet или SNMP) с программой «Менеджером» управления (М), которая размещается в отдельном сервере управления. К серверу управления подключается рабочая станция (РС), с помощью которой оператор сети наблюдает за всеми состояниями, изменяет настройки и т.д. Шлюзовый сетевой элемент СД содержит интерфейс Qx для подключения сервера. Этот интерфейс поддерживает передачу данных в канале управления. В отличие от Qx интерфейс F (RJ-45) или RS-232 не поддерживают передачу данных по сетевым протоколам и обеспечивают только локальное управление сетевым элементом с персонального компьютера, содержащего программу управления. С деталями управления сетевыми элементами по отдельности и в составе сети необходимо знакомиться по техническим документам производителей

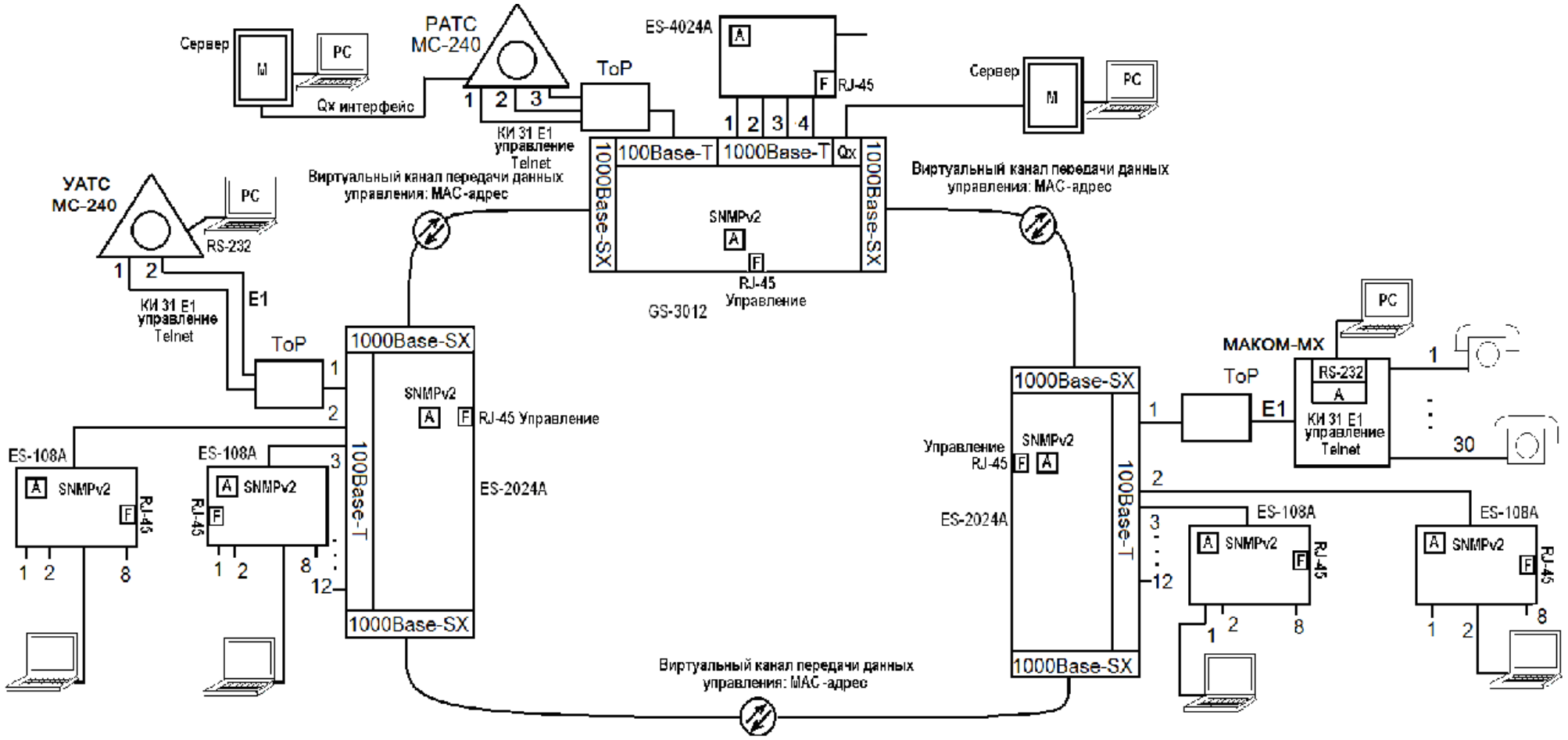


Рисунок 12 - Пример схемы управления

8 Контрольные вопросы

1 К чему может приводить отсутствие тактовой синхронизации в СД?
2 Что может служить источником тактового синхронизма в СД?
3 Чем определены принципы и нормативы тактовой синхронизации для СД?
4 По какому принципу распределяется тактовый синхронизм в СД?
5 Какие классы подключения к сети тактовой синхронизации предусмотрены?
6 Чем отличаются классы подключения к сети ТСС?
7 Что обозначает иерархический принцип подключения к сети ТСС?
8 Что используется для информирования о тактовом синхронизме в сети с циклической передачей?
9 В чём отличие сети синхронизации при пакетной передаче трафика?
10 В чём сущность протоколов NTP и PTP?
11 В чём особенности синхронизации PON?
12 С какой целью в сети доступа вводится управление?
13 Какие задачи управления решаются в сети доступа?
14 Какие организации разработали стандарты управления для СД?
15 Какие протоколы управления получили наибольшее применение в СД?
16 Какие виды управления предусмотрены для СД?
17 Что представляют собой агенты и менеджеры управления ?
18 В чём состоит принцип взаимодействия в системе управления?
19 Что необходимо для эффективного взаимодействия человека-оператора с системой управления?
20 Какие принципы положены в основу протокола Telnet?
21 Что предусмотрено командами протокола FTP?
22 Какие функции протокола HTTP можно применить для управления сетью доступа?
23 Какие функции управления заложены в семействе протоколов SNMP?
24 Чем отличаются версии протоколов SNMP?
25 Какие команды управления предусмотрены в SNMP?
26 Какое назначение в сети управления имеют MIB?

27 Чем отличаются различные MIB?
28 В чём состоят достоинства протокола SNMP?

Библиографический список

1. Фокин, В. Г. Проектирование оптической сети доступа : учебное пособие / В. Г. Фокин. - Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2012. - 311 с. - URL: http://biblioclub.ru/index.php?page=book&id=431523 (дата обращения 27.10.2023) . - Режим доступа : по подписке. - Текст : электронный

2. Скляров, О. К. Волоконно-оптические сети и системы связи : учебное пособие / О. К. Скляров. – Москва : СОЛОН-ПРЕСС, 2009. – 266 с. – URL: http://biblioclub.ru/index.php?page=book&id=117684 (дата обращения 27.10.2023). – Режим доступа : по подписке. – Текст : электронный.

3. Шарангович, С.Н. Многоволновые оптические системы связи : учебное пособие / С.Н. Шарангович. – Томск : ТУСУР, 2016. – 156 с. - URL: http://biblioclub.ru/index.php?page=book&id=492591 (дата обращения 27.10.2023) . - Режим доступа : по подписке. - Текст : электронный.

ЗАКЛЮЧЕНИЕ

По результатам выполнения лабораторных работ студент формирует следующие компетенции:

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-9/ основной, завершающий.	ПК-9.1. Применяет методы измерения показателей качества работы закрепленного оборудования, с учетом конструктивных особенностей, принципиальных и функциональных схем. ПК-9.2. Решает задачи по организации и контролю проведения измерений и проверке качества работы оборудования, планово-профилактических и ремонтно-восстановительных работ.	**Знать:** Основные методы проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации. **Уметь:** Применять основные методы проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих	**Знать:** Применяемые методы проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации. **Уметь:** Применять методы проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих	**Знать:** Современные эффективные методы выполнения проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации. **Уметь:** Применять современные эффективные методы проектирования, монтажа и эксплуатации систем, сетей

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	ПК-9.3. Контролирует выполняемые работы по синтезу радиоэлектронного средства, опираясь на научную методологию разработки приемопередающих инфокоммуникационных устройств и каналов связи (направляющих средств передачи).	сред передачи информации. **Владеть:** Навыками применения основных методов проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации.	сред передачи информации. **Владеть:** Навыками применения методов проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации.	и устройств инфокоммуникаций, а также направляющих сред передачи информации. **Владеть** Навыками применения современных эффективных методов проектирования, монтажа и эксплуатации систем, сетей и устройств инфокоммуникаций, а также направляющих сред передачи информации.
ПК-10/ завершающий.	ПК-10.1. Определяет назначение и принцип действия измерительных приборов, порядок их периодической	**Знать:** Основные методы эксплуатации оборудования, проведения измерений и про-	**Знать:** Методы эксплуатации оборудования, проведения измерений и провер-	**Знать:** Эффективные современные методы эксплуатации оборудования, проведе-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	поверки, процессы технического обслуживания, а также правила технической эксплуатации оборудования, каналов передачи, нормативные требования, определяющие порядок разработки технической документации по эксплуатации оборудования. ПК-10.2. Контролирует проведение измерений и проверку качества работы оборудования для последующего принятия управленческих решений в стандартных и нестандартных ситуациях, несет за них ответственность. ПК-10.3. Анали-	верки. **Уметь:** Применять основные методы эксплуатации оборудования, проведения измерений и проверки. **Владеть:** Навыками применения основных методов эксплуатации оборудования, проведения измерений и проверки.	ки. **Уметь:** Применять методы эксплуатации оборудования, проведения измерений и проверки. **Владеть:** Навыками применения методов эксплуатации оборудования, проведения измерений и проверки.	ния измерений и проверки. **Уметь:** Применять эффективные современные методы эксплуатации оборудования, проведения измерений и проверки. **Владеть:** Навыками применения эффективных современных методов эксплуатации оборудования, проведения измерений и проверки.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	зирует показатели качества работы, для регламентации проведения профилактических, ремонтно-восстановительных работ инфокоммуникационного оборудования.			
ПК-11/ завершающий.	ПК-11.1. Применяет методы оценки параметров работы сети, программно-технические средства диагностики и мониторинга. ПК-11.2. Выполняет работы по отслеживанию состояния сети, определяя необходимые параметры мониторинга и анализируя их значения. ПК-11.3. Формирует исходные	**Знать:** Основные методы расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации. **Уметь:** Применять основные мето-	**Знать:** Методы расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации. **Уметь:**	**Знать:** Эффективные современные методы расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств авто-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	данные для осуществления предварительных расчетов и последующего мониторинга состояния сетей с помощью автоматизированных средств мониторинга параметров инфокоммуникационных сетей.	ды расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации. **Владеть:** Навыками применения основных методов расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и	Применять методы расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации. **Владеть:** Навыками применения методов расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим	матизации. **Уметь:** Применять эффективные методы расчета по проектированию сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации. **Владеть:** Навыками применения эффективных методов расчета по проектированию сетей, сооружений и средств ин-

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		средств автоматизации.	заданием с использованием стандартных методов, приемов и средств автоматизации.	фокоммуникаций в соответствии с техническим заданием с использованием стандартных методов, приемов и средств автоматизации.

ПРИЛОЖЕНИЕ А

(обязательное)

Форма титульного листа отчета, обучающегося о выполненной лабораторной работе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»

Кафедра космического приборостроения и систем связи

ОТЧЕТ
о выполненной лабораторной работе по дисциплине
«Проектирование оптических сетей доступа»
на тему «_____»

Выполнил _____ /Фамилия, инициалы/
(подпись)

Проверил _____ /Фамилия, инициалы/
(подпись)

Курск 20___