Администрирование информационных систем

ПОДКЛЮЧЕНИЕ ИС К УЗЛУ ОПЕРАТОРА СВЯЗИ.

Практически любая ИС имеет потребность в получении информации извне.

Эта информация может поступать от подразделений компании, находящихся на определенном расстоянии друг от друга, от контрагентов (клиентов или поставщиков компании) либо от удаленных пользователей. Источником информации может быть так же Интернет. Для ее получения администратор системы должен воспользоваться услугами операторов связи, что, в свою очередь, требует подключения ИС к узлу какого-либо оператора. При этом администратор системы должен учитывать, что пользователям ИС необходимы современные аппаратные средства передачи данных и современные каналы связи.

Операторы связи используют для передачи данных (ПД) специализированные и неспециализированные сети ПД, в частности телефонные сети общего пользования (ТФОП).

Несмотря на то что сеть ТФОП предназначена для передачи аналоговых сообщений, с помощью технологий ISDN и xDSL ее линии можно использовать для цифровой передачи данных. Для подключения ИС к узлу связи оператора, предпочтительно использовать выделенные линии, поскольку они обладают необходимыми для передачи данных характеристиками.

Основным вопросом при подключении ИС к узлу оператора связи является организация связи на участке от ИС до узла связи оператора.

Средства, необходимые для подключения абонента (в данном случае корпоративной ИС) к узлу оператора связи, называют «последней милей».

Они включают в себя кабельные системы (медные или современные оптоволоконные), аппаратные средства (мультиплексоры, модемы, конвертеры и другие устройства) на узле оператора связи и на стороне ИС, беспроводные средства передачи данных на отрезке от узла оператора связи до узла ИС. Основным «потребителем» медных пар на участке от абонента до узла связи является ТФОП.

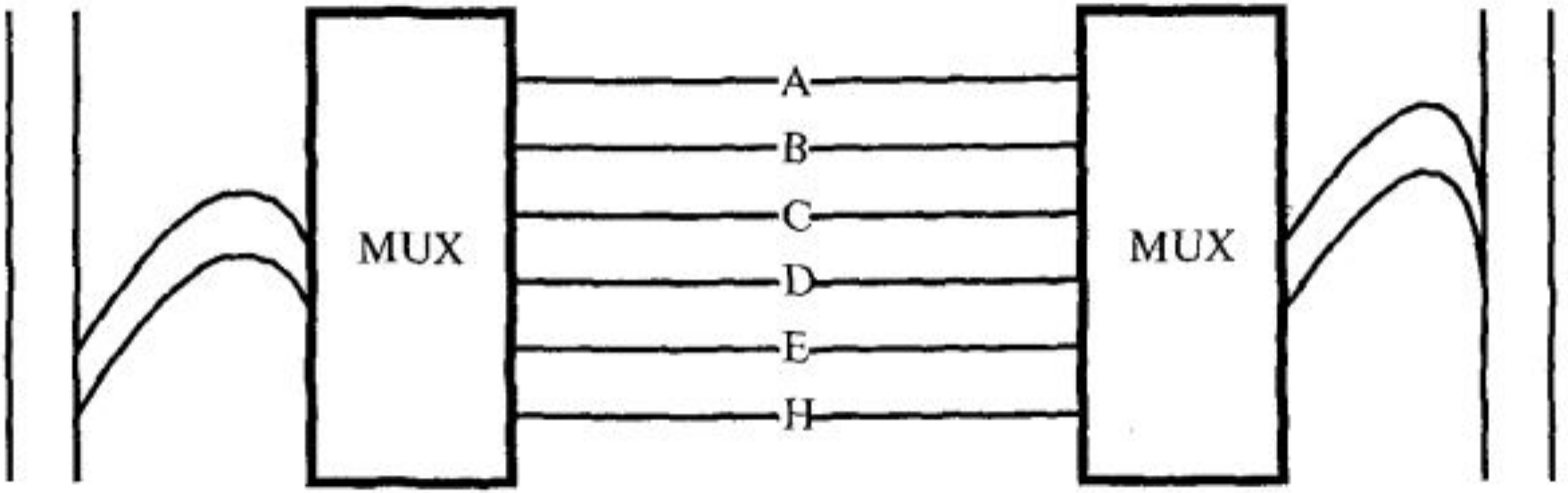
Организация последней мили на базе медных кабелей

Для передачи данных по ТФОП (PSTN) и превращения ее в цифровую сеть используют серию стандартов ISDN (Integrated Services Digital Network — цифровая сеть с интеграцией служб), которые стандартизируют объединение терминалов, компьютеров, телефонов, видео, голоса. Фактически в узлах операторов связи установлены мультиплексоры, а у абонентов — ISDN-терминалы или ISDN-телефоны. Между ними организованы каналы передачи данных. Пользователям предоставляется канал ISDN (ISDN-pipe) для передачи информации в режиме коммутации каналов или коммутации пакетов. Канал ISDN может передавать несколько стандартных комбинаций мультиплексированных каналов для получения различной пропускной способности.

Стандарты ISDN отличаются реализациями в различных странах. До сих пор разработка стандартов не завершена и завершена не будет из-за появления новых технологий. Запрос администратором системы у оператора связи ISDN-канала может вызывать затруднение из-за того, что современные операторы связи не всегда предоставляют такую услугу.

Характеристика комбинаций каналов в ISDN

- Канал MUX A — 4КГц, аналоговая телефония
- Канал MUX B — 64 Кбит/с, цифровые данные
- Канал MUX C — 8 или 16 Кбит/с, передача управляющего цифрового сигнала
- Канал MUX D — 16 или 64 Кбит/с, передача управляющего цифрового сигнала
- Канал MUX E — 64 Кбит/с, цифровой канал с сигнализацией ISDN
- Канал MUX H — 384 или 1536 или 1920 Кбит/с



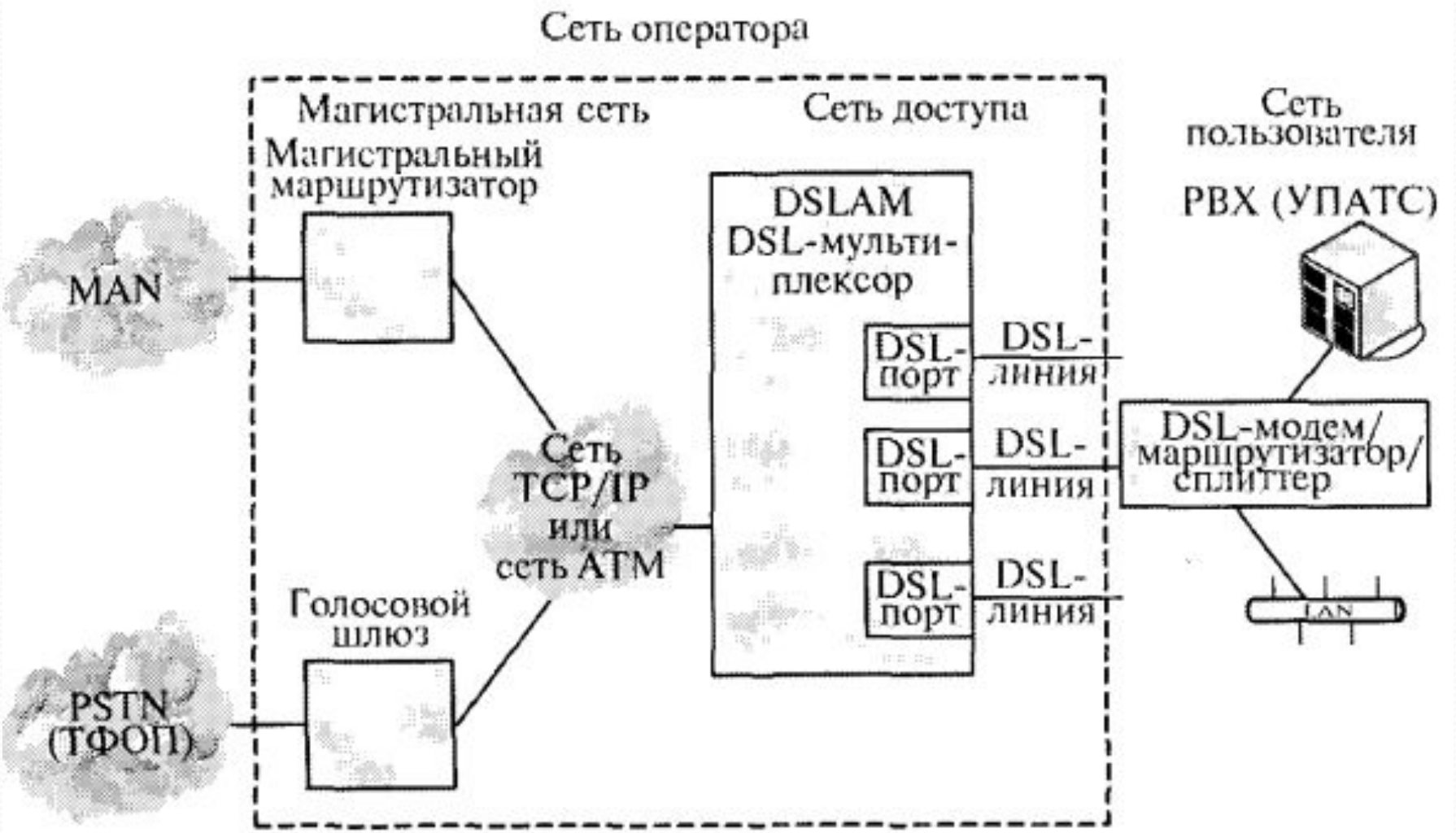
ITU-T стандартизировал три комбинации каналов для предоставления в качестве сервиса абонентам. Укажем две из них, получившие широкое распространение:

- BRI — базовый доступ (basic rate). Комбинация из двух каналов типа B и одного канала типа D (16 Кбит/с). Эта комбинация каналов обозначается 2B + D, используется, например, для расширения услуг, предоставляемых городской АТС (переадресация вызовов, конференц-связь и пр.).
- PRI — первичный доступ (primary rate). Комбинация из 30 B-каналов (Европа) и одного D-канала (64 Кбит/с) — ЗО B + D. Или комбинация из 23 B-каналов (США, Япония) и одного D-канала (64 Кбит/с) — 23B + D.

Соответственно в Европе —это линия со скоростью 2048 Кбит/с (El-канал), а в США —1544 Кбит/с (T1-канал). Каналы с такой пропускной способностью используют, например, для подключения корпоративных АТС (PBX) к городским. Многие современные офисные АТС имеют интегрированные устройства сопряжения с оборудованием ISDN.

Технология xDSL(Digital Subscriber Line)

В узле связи оператора устанавливается DSLAM-цифровой мультиплексор, а у пользователей ИС — xDSL - модемы (или маршрутизатор с xDSL-модемом, если присоединяется сеть пользователей). В xDSL-устройстве на стороне пользователя может находиться фильтр (splitter), который позволяет выделить голосовой сигнал и передать его на телефон или небольшую телефонную станцию (УПАТС, PBX). Соединение пользовательского оборудования с оборудованием оператора связи производится по обычным медным телефонным линиям. Мультиплексор преобразует полученный сигнал 1-го уровня OSI в пакет IP, ATM или SDH и отправляет его устройству уровня 3/4 (маршрутизатору, коммутатору или шлюзу). Далее информация передается, например, в городскую сеть передачи данных (MAN).


Сеть оператора
Магистральная сеть
Сеть доступа
Сеть пользователя
Магистральный маршрутизатор
DSLAM DSL-мульти-плексор
PBX (УПАТС)
MAN
DSL-порт
DSL-линия
DSL-порт
DSL-линия
DSL-порт
DSL-линия
DSL-модем/ маршрутизатор/ сплиттер
Сеть TCP/IP или сеть ATM
Голосовой шлюз
PSTN (ТФОП)
LAN

Проблемы xDSL.

В США, где разрабатывались первые виды DSL, существует три обычно определяемых длины «последней мили», которые различаются сопротивлением и диаметром кабеля, и, соответственно, три вида соглашений о сервисе, предоставляемом операторами связи. Согласно этим правилам длина линии от абонента до узла связи может быть

- в пределах 2 км (зона DA),
- 3—4 км (зона CSA),
- 6 км (зона RRD).

Различные виды DSL разрабатывались для предоставления высокоскоростного доступа в различных зонах.

В связи с тем, что передача сигнала ведется на высоких частотах, возникает межсимвольная интерференция, практически стирающая разницу между уровнями сигнала.

Существуют два способа борьбы с этой проблемой (без понижения скорости передачи), которые в комбинации применяются в действующих системах:

— передача на единичном интервале цифрового сигнала нескольких бит при допустимой с точки зрения помехоустойчивости скорости (специальные виды кодирования сигнала);

— использование эквалайзеров, исправляющих импульсы сигнала по шаблону.

Организация последней мили с использованием неограниченных сред

В тех случаях, когда отсутствует техническая или финансовая возможность организовать последнюю милю с помощью медных или оптоволоконных систем, администратору системы следует использовать неограниченные среды и различные беспроводные средства передачи.

- Микроволновая передача данных.
- Лазерная передача данных.
- Радиопередача данных.
- Беспроводные сети (wireless).

Микроволновая передача данных. Микроволновые системы передачи данных существуют в двух вариантах — спутниковые и наземные. Последние организуются, например, с помощью двух параболических антенн на крыше зданий, работают в нижней части гигагерцового диапазона и в условиях прямой видимости. Микроволновые системы являются дешевыми и высокоскоростными. Но они чувствительны к интерференциям, прослушиваниям, атмосферным явлениям.

Лазерная передача данных. Лазерная передача осуществляется с помощью узкого пучка света, генерируемого лазером. Система работает на более высоких частотах, чем микроволновая передача, и является более узконаправленной. В качестве излучателей используют лазеры, а в качестве приемников — фотодиоды. Лазерная передача устойчива к интерференциям, прослушиваниям, но сильно зависит от атмосферных явлений и работает на коротких расстояниях в условиях прямой видимости.

Инфракрасная передача данных. Для передачи используются инфракрасные диоды и фотодиоды с частотой выше1000 ГГц. Скорости передачи данных близки к оптоволоконным системам, но перекрываемое расстояние не превышает 25м при прямой видимости.

Радиопередача данных. Под радиопередачей понимают передачу данных в диапазоне частот от 3 МГц до 3 ГГц. Радиосистемы широко распространены, имеют низкую стоимость и применяются для:

- мобильных технологических приложений,
- радио (FM-передаваемый диапазон частот до 15 кГц),
- телевидения (передаваемый диапазон частот до 6 МГц).

Скорости передачи данных относительно невысокие, и передача чувствительна к помехам и прослушиваниям.

Беспроводные сети (wireless). Этот вид передачи данных осуществляется в ISM-диапазоне. ISM-диапазон (ISM — Industrial, Scientific and Medical) — это частоты, которые были зарезервированы разработчиками (правительственными органами США в 1985 г. в гражданских целях и в 1950 г. в военных целях) для решения:

- индустриальных задач (диапазон 902—928 МГц),
- научных задач (диапазон 2400—2483 МГц)
- и медицинских (диапазон5725—5850 МГц) задач.

Передача данных осуществляется с помощью широкополосного сигнала. В каждой сети свой уникальный код такого сигнала (реализуется с помощью чипа), позволяющий работать в данном регионе только тем, кто имеет такой же чип. Этот код добавляется к любому сообщению.

К факторам, которые надо учесть администратору системы вместе с оператором связи при применении беспроводных технологий, относятся:

- потери в атмосфере,
- дальность прямой видимости,
- зона Френеля,
- кривизна поверхности Земли
- и ряд других…

Величина потери в свободном пространстве (FSL) является оценкой потерь мощности сигнала на пути к принимающей станции.

Это теоретическая величина, при вычислении которой предполагается, что отсутствуют дифракция, рефракция и на пути перемещения волн нет препятствий или рассеивания.

Эта величина отражает лишь потери, которые испытывает сигнал при удалении от источника вследствие дивергенции лучей.

Расстояние прямой видимости (LOS). Для прямой видимости необходимо, чтобы в так называемой зоне Френеля не было никаких объектов, таких как деревья, дома или поверхность земли.

Под зоной Френеля понимается область, прилегающая к зоне прямой видимости, в которой распространяются электромагнитные волны после излучения передающей антенной. Эту область надо определить точно, так как вне ее качество сигнала резко падает из-за дополнительного ослабления.

Действия администратора системы по подключению к узлу оператора связи

Для подключения ИС к узлу оператора связи администратор системы должен осуществить следующие основные мероприятия:

- определить наличие различных операторов фиксированной связи на ближайшем к ИС узле связи ГТС;
- выявить возможности передачи данных и наличие свободных каналов последней мили от узла оператора до узла ИС;
- установить возможности какого-либо из операторов, находящегося на ближайшем узле связи; необходимо получить от данного оператора технические условия на подключение(либо соответствующую проектную документацию) и согласовать схемы организации связи;
- если последней мили не существует, а другие условия устраивают администратора системы, необходимо выявить вместе с оператором связи возможность и стоимость организации последней мили;

- если организация последней мили невозможна по техническим причинам или нерентабельна, администратор системы должен обратиться к другим операторам, имеющим свои точки присутствия в данном регионе, и выявить перечисленные выше условия у них; организация последней мили в беспроводном варианте должна осуществляться в случае невозможности ее реализации по медным или оптоволоконным линиям связи;
- после получения технических условий от оператора на присоединение и организации последней мили необходима установка и настройка аппаратуры и программного обеспечения на узле ИС согласно требованиям оператора, *например установка соответствующих требованиям оператора модемов и маршрутизаторов и настройка программного обеспечения маршрутизаторов.*

задача подключения и настройки оконечного оборудования

Из перечисленных мероприятий эта проблема в большей степени требует самостоятельных действий администратора ИС, например при установке и настройке маршрутизатора ИС, использующего в качестве сетевого протокола передачи данных протокол IP.

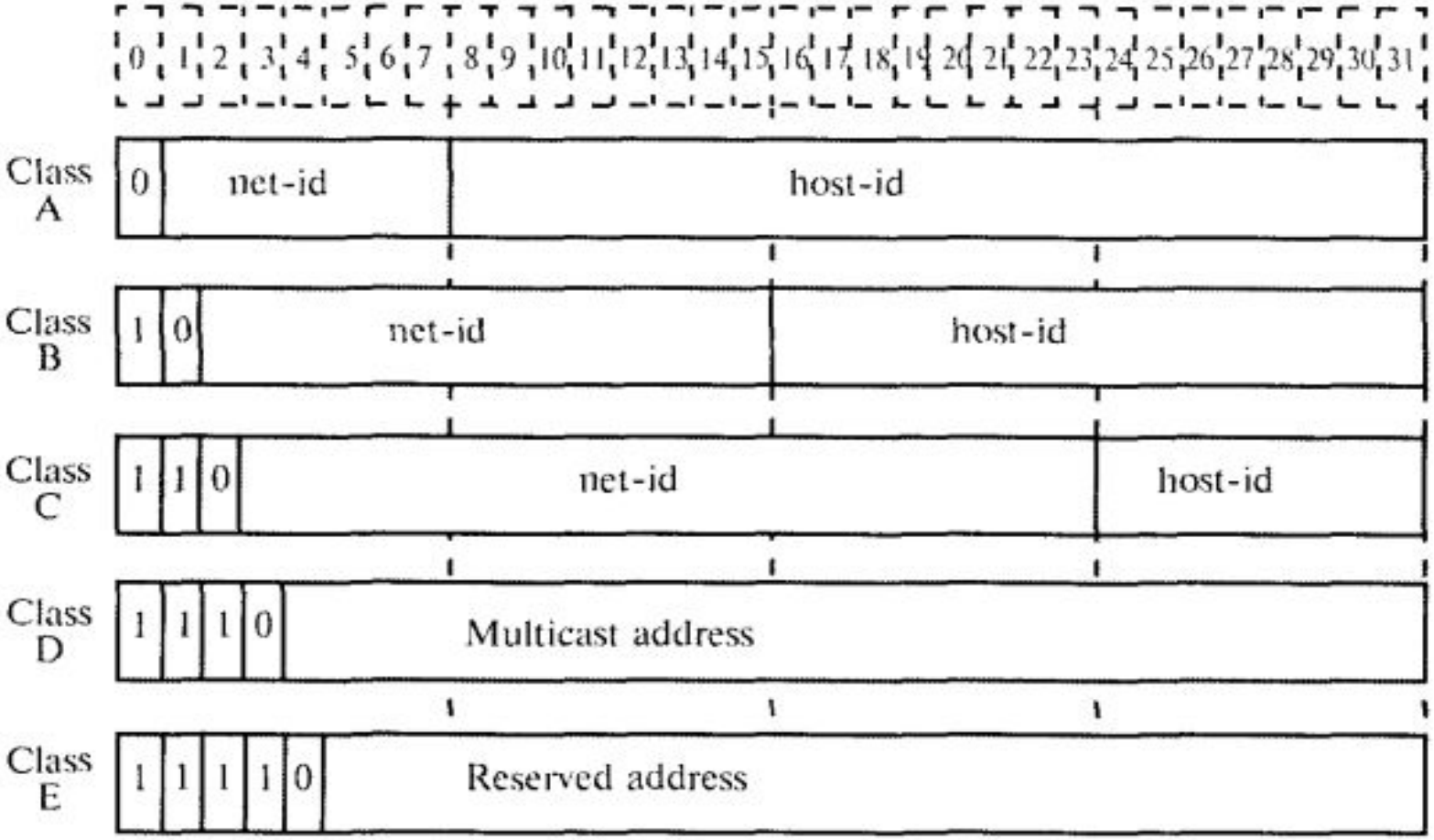
Для этого необходимо:

1. Подключить маршрутизатор ИС к обшей сети передачи данных оператора связи.
2. Получить от оператора связи пул IP-адресов, которые администратор системы сможет использовать в своей системе и распределить IP-адреса между пользователями (создать план адресации).
3. Загрузить, например, DHCP-сервер для подключаемого подразделения, если необходим выход во внешней мир каждого пользователя с использованием индивидуального IP-адреса.
4. Выполнить соответствующие настройки ОС на рабочих станциях пользователей ИС.

Классы IP-адресов (версия IP v.4)

- Адресация Class A нужна, если в сети много хостов. *Примером может служить сеть ARPANET.*
- Адресация Class B используется при среднем количестве хостов в сети,
- Адресация Class C при небольшом числе хостов в сети.
- Class D — адреса зарезервированы для специальных широковещательных сообщений (broadcast),
- Class E вообще зарезервированы для дальнейшего использования.

Поэтому для обычного использования остаются адреса Class C.



Классы сетей:

net-id — идентификатор сети; host-id — идентификатор хоста;
multicast address — мультипользовательский адрес;
Reserved address — резервные адреса

Маски подсетей

Чтобы наиболее эффективно использовать имеющийся запас IP-адресов, каждая сеть может быть разделена на подсети меньшего размера согласно стандарта RFC 950. Подсети дают адрес подсети внутри сети и адрес хоста внутри подсети. Адрес подсети выделяется администратором из области адресации хостов.

Механизм, с помощью которого выделяются подсети, называет маской подсети — это битовая маска, определяющая, какая часть адреса относится к адресу сети, а какая —к адресу хоста в этой сети.

Для того чтобы ее определить, все биты адреса сети устанавливаются в «1», а все биты адреса оставшиеся для хоста в «О». Строка бит переводится потом в десятичные значения с точкой, а результат и есть маска подсети.

IP-класс сети	Диапазон адресов Первый байт	Маска по умолчанию	Максимальное количество хостов
Class A	0—127	255.0.0.0	16 777 216
Class B	128—191	255.255.0.0	65 536
Class C	192—223	255.255.255.0	256

По адресам есть определенные соглашения:

- биты адреса хоста никогда не устанавливаются во все«0» или все «1». Эти адреса зарезервированы;
- если на месте адреса хоста установлены нули, то это —обращение ко всем хостам в сети, *например для сети Class B это выглядит как 145.32.0.0;*
- если нули установлены на месте адреса сети, то это —обращение к хосту в сети, например к хосту *с адресом 2.3 для сети Class B это выглядит как 0.0.2.3;*
- адрес 127.0.0.0 Class A зарезервирован для тестирования. Данные с таким адресом вернутся обратно к передающему устройству. Маршрутизатор или хост не пошлет их в другой сегмент;
- адрес из всех 32 нулей используется хостами при присоединении к сети и инициализации. Он никогда не является адресом назначения. В таблицах маршрутизации устройств он рассматривается как маршрут по умолчанию;
- адрес из всех 32 единиц (255.255.255.255) означает, что это широковещательный пакет для рассылки всем устройствам в сети;
- адрес хоста из всех единиц означает, что этот пакет будет передаваться всем хостам в подсети.

Изначально маски подсетей были фиксированной длины — FLSM (Fixed Length Subnet Masking). Это означало, что в одной сети все подсети были одинакового размера.

Однако фиксированная длина маски подсети неудобна с точки зрения эффективного распределения адресного пространства. Поэтому для более эффективного использования адресного пространства была разработана технология маски подсети переменной длины — VLSM (Variable Length Subnet Masking).

Маски подсети переменной длины обеспечивают возможность:

— создания более одной маски подсети в переделах одной сети;
— разбиения на подсети, уже разбитые на подсети группы1Р-адресов;
— использования суммированных маршрутов.

Например, подсеть 172.16.12.0/22 суммирует все адреса, которые входят в нее, включая подсети 172.16.13.0/24, 172.16.14.0/24 и172.16.15.0/24.

пример создания адресного плана

Администратором системы или оператором связи для подразделения А был выделен диапазон адресов 172.16.12.0 /22.

Данное подразделение имеет две крупные локальные сети примерно по 200 пользователей каждая, а также три удаленных сети примерно по 20 пользователей, для каналов связи до маршрутизаторов удаленных узлов тоже должны быть выделены IP-адреса.

Создание иерархического адресного плана подразделения содержит следующие шаги:

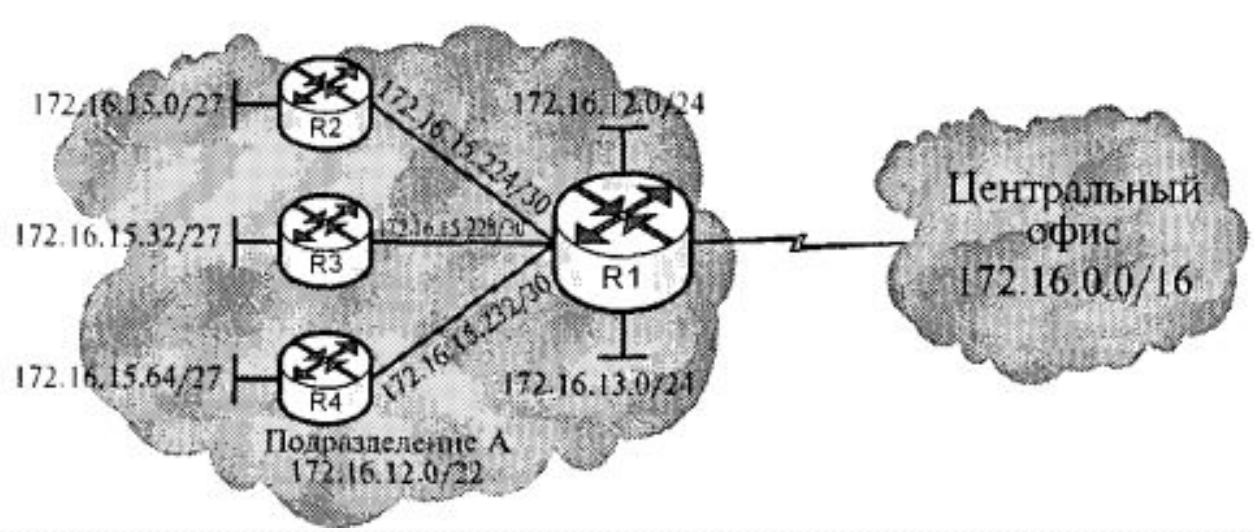
1) Выделение из выделенного адресного пространства адресов для двух локальных сетей на 200 пользователей.

2) Перераспределение оставшегося адресного пространства между тремя сетями по 20 пользователей.

3) Перераспределение оставшегося адресного пространства для адресации каналов связи между маршрутизаторами.

Проведем разделение адресного пространства 172.16.12.0/22.

1. *Так как у нас есть две локальные сети по 200 пользователей нам необходимо два блока по 256 адресов. Под локальные сети выделяем подсети 172.16.12.0/24 и 172.16.13.0/24.*
2. *Берем последний из оставшихся блоков адресов172.16.15.0/24 и делим его на блоки по 32 адреса. Получаем подсети для удаленных офисов 172.16.15.0/27, 172.16.15.32/27 и172.16.15.64/27.*
3. *Берем последний блок из оставшихся блоков адресов172.16.15.224/27 и делим его на блоки по 4 адреса для присвоения адресов интерфейсам маршрутизаторов 172.16.15.224/30,172.16.15.228/30, 172.16.15.232/30.*



Технология NAT

При получении пула адресов от оператора связи администратор системы может столкнуться с проблемой нехватки их для своей сети.

Для максимально эффективного использования зарегистрированных IP-адресов программное обеспечение маршрутизаторов использует службу преобразования адресов NAT (Network Address Translation).

Соответствующая служба программного обеспечения представляет собой реализацию рекомендаций RFC 1631. Она представляет собой способ использования одних и тех же IP-адресов в нескольких внутренних подсетях, уменьшая тем самым потребность в зарегистрированных IP-адресах.

Технология NAT позволяет корпоративным IP сетям, которые используют незарегистрированные IP-адреса (частные), подсоединяться к открытой сети передачи данных, такой как Internet.

Трансляция, выполняемая NAT, может быть статической либо динамической.

- Статическая трансляция осуществляется при ручной конфигурации таблицы преобразования адресов. Определенные внутренние адреса преобразуются в указанные внешние адреса. Внутренняя часть таблицы адресов однозначно отображается во внешнюю часть таблицы.
- Динамическое преобразование происходит, когда на граничном маршрутизаторе сконфигурирован пул внешних адресов, в которые можно транслировать внутренние адреса. Может применяться несколько пулов внешних адресов.

Внутренние и внешние IP-адреса определяют физическое расположение хостов относительно устройства NAT.

Локальные и глобальные IP-адреса определяют положение пользователя относительно устройства NAT.

Службам администратора системы необходимо выполнить следующие шаги.

1. В качестве подготовительного этапа сконфигурировать на маршрутизаторе IP-маршрутизацию и указать соответствующие IP адреса.

2. Далее необходимо задать стандартный IP список доступа с помощью команды access-list.

3. Указать пул адресов для службы NAT протокола IPс помощью команды ip nat pool.

4. Выполнить привязку списка доступа к пулу службы NAT с помощью команды ip nat inside source list.

5. Включить службу NAT, по крайней мере, на одном внутреннем и на одном внешнем интерфейсе с помощью команды ip nat {inside | outside}.

Администратор системы должен проверить результаты. Для этого в ОС IOS можно использовать специальные команды show ip nat translation show.

Сервисы NAT могут быть использованы и в целях защиты от несанкционированного доступа ИС.

Пример вывода информации для статической конфигурации адресов.

```
r1#show ip nat translation
Pro  Inside global   Inside local Outside local Outside global
---     92.2.2.1      10.1.1.1       ----           ----
---     192.2.2.2     10.1.1.2       ----           ----
r1#
```

Пример конфигурации перегрузки внутренних глобальных адресов

Шаг 1. В качестве подготовительного этапа сконфигурировать на маршрутизаторе IP—маршрутизацию и указать соответствующие IP-адреса.

Шаг 2. Сконфигурировать службу динамического преобразования адресов.

Шаг 3. После того, как сконфигурирован список доступа для пула адресов службы NAT, необходимо ввести команду ipnat inside source list

Шаг 4. Включить службу NAT на соответствующих интерфейсах с помощью команды ip nat {inside | outside}.