**Министерство образования Республики Беларусь**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Шишлянников Иван Викторович**

**Технология NANT.**

**Мини-коллоквиум**

Отчет по лабораторной работе № 13,

Вариант 39

( “Компьютерные сети”)

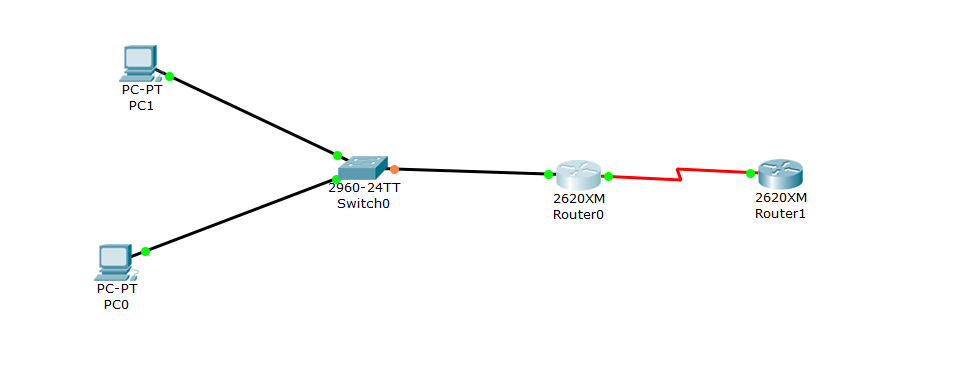
студента 2-го курса 12-ой группы

|  |  |  |
| --- | --- | --- |
|  |  | **Преподаватель** |
|  | **Горячкин В.В.** |
|  | | |
| **2020 г.** | | |

| **Вариант** | Адреса для узлов | Маршрутизатор 1 | Маршрутизатор  2 | IP-адрес  Loopback 1 |
| --- | --- | --- | --- | --- |
| 39 | 192.168.25.0/24 | 164.6.26.1/30 | 164.6.26.2/30 | 172.16.1.23/32 |

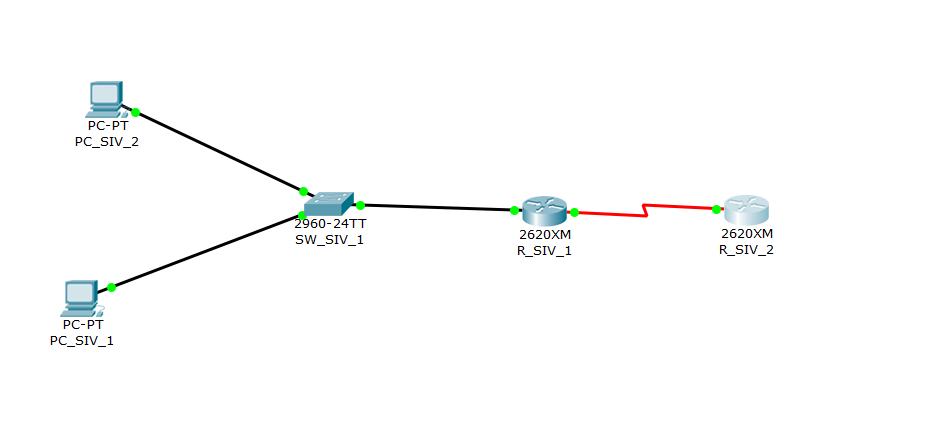
1. Реализовать по аналогии схему сети приведенной на рисунке 1.

Реализовали сеть как на рисунке.



1. Присвоить имена маршрутизаторам и хостам по уже принятым правилам..

Присвоил имена согласно правилам



1. Выполните пункты 1-13 методических указаний к лабораторной работе.  
   Адреса задавать согласно вашему варианту задания.

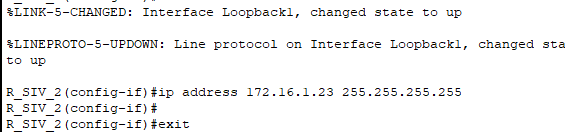
**Шаг 1. *Подсоединение устройств***

Выполнил в пунктах 2-3.

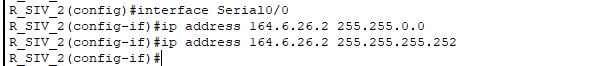
**Шаг 2. *Настройка основной конфигурации маршрутизатора 2***

Задайте в настройках конфигурации маршрутизатора 2 имя узла (ISP), задайте IP-адреса для интерфейсов согласно вашему варианту задания. Сохраните конфигурацию.

Настроил Lopback интерфейс маршрутизатора 2 согласно своему варианту:



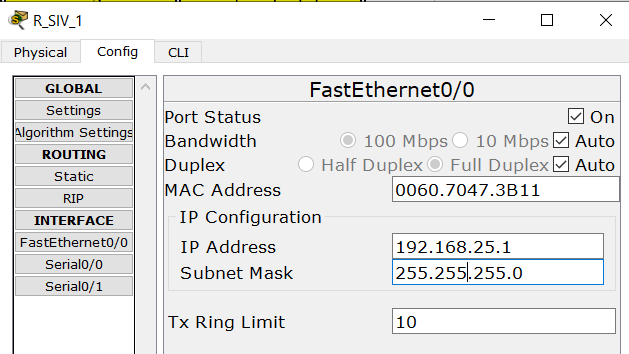
Настроил интерфейс Serial0/0 маршрутизатора 2 согласно своему варианту:



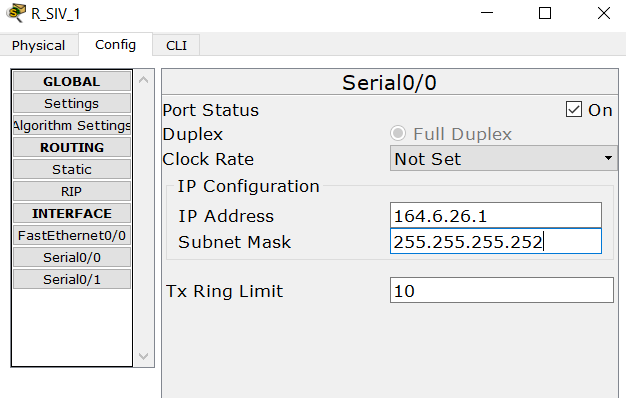
**Шаг 3*. Настройка маршрутизатора, используемого в качестве шлюза***

Задайте в настройках основной конфигурации маршрутизатора 1 имя узла (Gateway), задайте IP-адреса для интерфейсов. Сохраните конфигурацию.

Настроил интерфейс Fa0/0 маршрутизатора 1 согласно своему варианту:



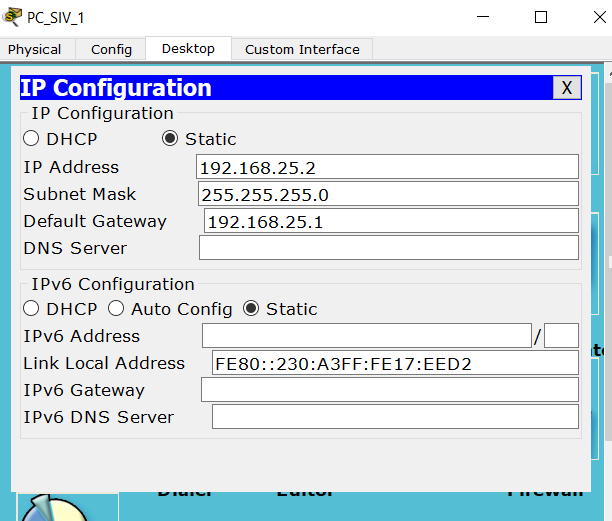
Настроил интерфейс Serail0/0 маршрутизатора 1 согласно своему варианту:



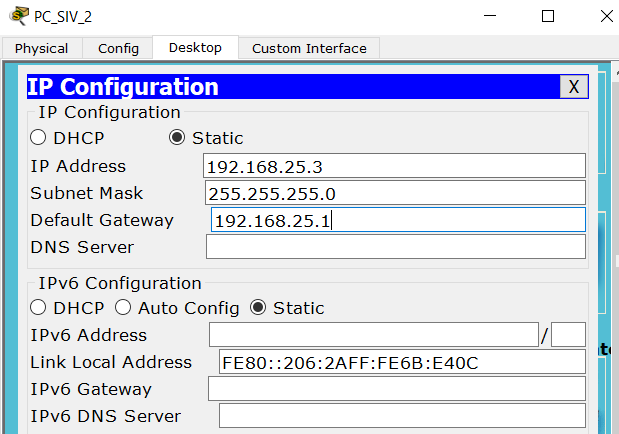
**Шаг 4*. Настройка правильного IP-адреса, маски подсети и шлюза по умолчанию для узлов.***

Присвойте каждому узлу соответствующий IP-адрес, маску подсети и шлюз по умолчанию. Оба узла должны получить внутренние частные IP-адреса в сети 10.10.10.0/24 (**вам необходимо задать адреса согласно вашему варианту задания**). Шлюзом по умолчанию должен быть IP-адрес интерфейса FastEthernet маршрутизатора с именем Gateway.

Настройка ПК1 согласно варианту:



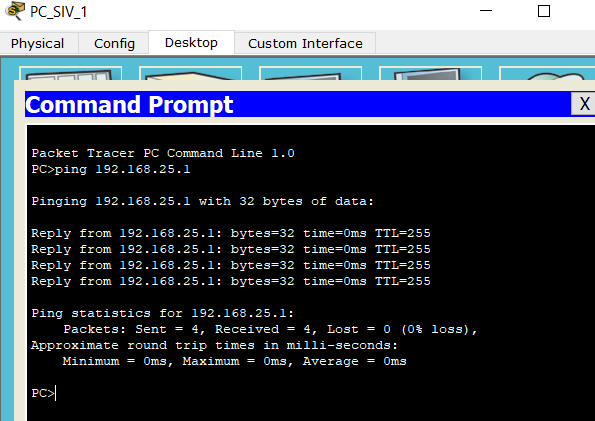
Настройка ПК2 согласно варианту:



**Шаг 5*. Проверка работоспособности сети.***

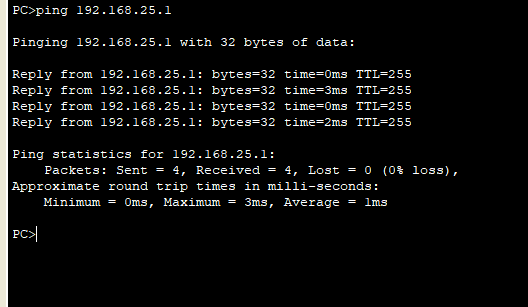
1. С присоединенных узлов отправьте эхо-запрос на интерфейс FastEthernet маршрутизатора, используемого в качестве шлюза по умолчанию. Ответьте на следующие вопросы.

Отправляем эхо-запрос с ПК1:



a). Успешно ли выполнен эхо-запрос с узла 1? \_\_\_\_\_\_Да\_\_\_\_\_\_

Отправляем эхо-запрос с ПК2:

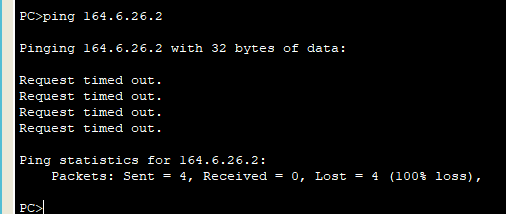


b) Успешно ли выполнен эхо-запрос с узла 2? \_\_\_\_Да\_\_\_\_\_\_\_\_

2. Если ответы на оба вопросы отрицательны, выполните поиск и устранение ошибок в конфигурации маршрутизатора и узлов. Тестируйте соединение до тех пор, пока эхо-запросы не будут успешными.

3. Отправьте эхо-запросы на IP-адрес маршрутизатора ISP. Какой получили результат. Поясните свой ответ.

Отправили эхо-запрос с ПК 1 на маршрутизатор 2 (ISP):



Результат отрицательный, так как мы еще не задали маршрут от шлюза по умолчанию до маршрутизатора 2.

**Шаг 6*. Создание маршрута по умолчанию***

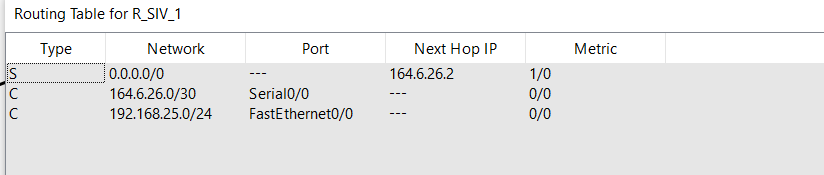
* С маршрутизатора, использующегося в качестве шлюза по умолчанию, создайте статический маршрут к маршрутизатору поставщика услуг Интернета в сети 0.0.0.0 0.0.0.0 с помощью команды ***ip route***. Это вызовет трафик к любому неизвестному адресу назначения через поставщика услуг Интернета путем настройки шлюза «последней надежды» на маршрутизаторе, использующемся в качестве шлюза по умолчанию.

Создали маршрут по умолчанию с маршрутизатора 1:



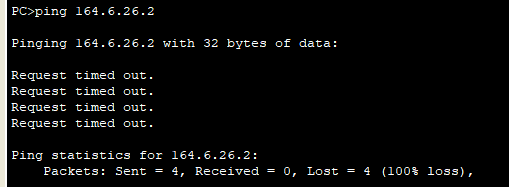
* Проверьте маршрут по умолчанию по таблице маршрутизации маршрутизатора Gateway. Находится ли статический маршрут в таблице маршрутизации?

Таблица маршрутизатора gateway :



* Попробуйте отправить эхо-запрос с одной с рабочих станций на IP-адрес последовательного интерфейса маршрутизатора поставщика услуг Интернета.

Пробуем отправить эхо-запрос повторно:



Успешно ли выполнен эхо-запрос?

Нет. Результат снова отрицательный, так как мы еще не создали статического маршрута от маршрутизатора 1 к маршрутизатору 2.

**Шаг 7*. Создание статического маршрута***

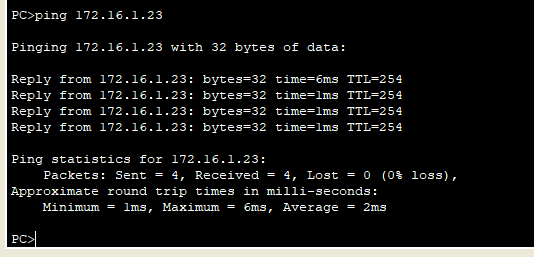
Создайте статический маршрут от маршрутизатора ISP к частной сети, присоединенной к маршрутизатору Gateway. Создайте статический маршрут с помощью команды ***ip route***.

Настроил статический маршрут на маршрутизаторе 2 (ISP):



* Отправьте эхо-запрос с узла 1 на адрес интерфейса loopback маршрутизатора ISP.

Отправил запрос на loopback интерфейс маршрутизатора ISP с ПК1:



Успешно ли выполнен эхо-запрос?

Да. Запрос выполнен успешно.

* Если эхо-запрос не выполнен, проверьте правильность конфигурации маршрутизатора и узла и повторите тестирование связи.

**Шаг 8*. Определение пула используемых публичных IP-адресов.***

Для определения пула используемых публичных IP-адресов используйте команду **ip nat pool.**

Определили пул используемых публичных адресов:



**Шаг 9*. Определение списка доступа, соответствующего внутренним частным IP-адресам.***

Для определения списка доступа, соответствующего внутренним частным адресам используйте команду **access-list**.

Определили список доступа, соответствующего внутренним частным адресам:



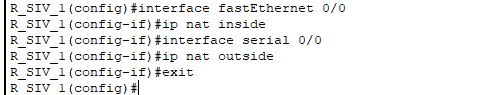
**Шаг 10. *Определение NAT из списка внутренних адресов в пул внешних адресов***

Для определения NAT используйте команду **ip nat inside source**.



**Шаг 11. *Назначение интерфейсов***

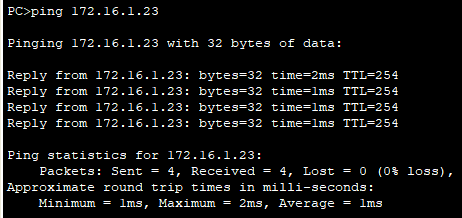
Активные интерфейсы маршрутизатора следует определить в качестве внутреннего или внешнего интерфейса в отношении к NAT. Для этого используйте команду ***ip nat inside*** или ***ip nat outside***.



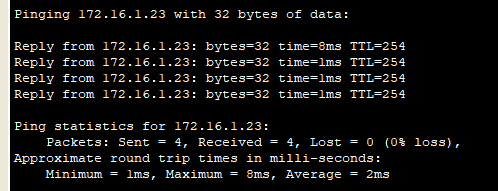
**Шаг 12. *Генерация трафика с маршрутизатора Gateway к маршрутизатору ISP***

Отправьте эхо-запросы с узлов 1 и 2 на адрес 172.16.1.1.

Отправляем эхо-запрос с ПК1:



Отправляем эхо-запрос с ПК2:

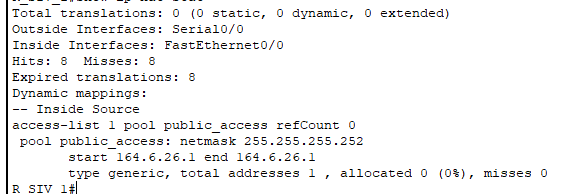


Все запросы прошли успешно.

**Шаг 13. *Проверьте работоспособность NAPT***

Для отображения статистики NAРT введите в приглашение привилегированного режима EXEC маршрутизатора Gateway команду ***show ip nat statistics***..

Выполнил команду **show ip nat statistic** на маршрутизаторе 1:



Проанализируйте полученную информацию и дать ответ на следующие вопросы.

1. Сколько активных преобразований выполнено?

Total transactions: 0;

0

1. Сколько адресов имеется в пуле?

Total addresses: 1;

1

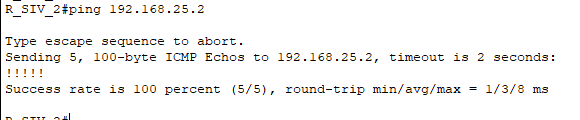
1. Сколько адресов уже выделено?

Allocated: 0;

0

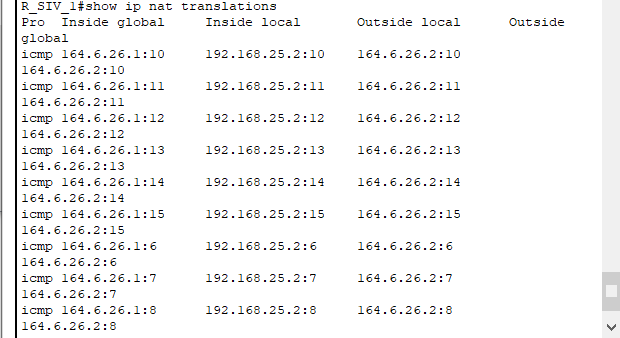
Если эхо-запрос выполнился успешно, отобразите преобразование NAT на маршрутизаторе Gateway с помощью команды **show ip nat translations**.

Выполняем эхо – запрос от маршрутизатора 2 (ISP) к PC1:

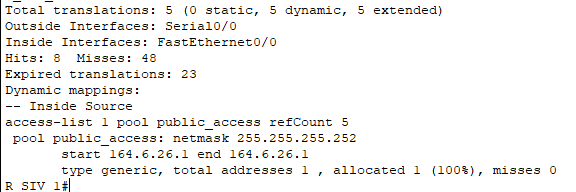


Запрос выполнился успешно.

Отображаем преобразование NAT на маршрутизаторе gateway после выполнения нескольких повторных эхо - запросов:



Так же, проверив командой show ip nat stat:



можно заметить, что Total translations выросло до 5, а allocated стало равно 1.

# Небольшой реферат о технологии NAT.

**Введение:**

В 1994-м году группой разработчиков сетевых технологий Network Working Group был предложен метод, с помощью которого решалась задача экономии IP-адресов. В этом документе участники группы NWG опубликовали описание, как актуальности, так и возможного решения проблемы с помощью объединения отдельных IP-адресов в группы.  
В том же году была разработана технология NAT (Network Address Translation - преобразование сетевых адресов). Подробное описание принципов работы NAT вы найдете по этому адресу. И хотя разработчики заявили, что NAT временное решение проблемы, технология прижилась, не смотря на некоторые свои недостатки.  
Внедрение NAT позволяет решить следующие вопросы.

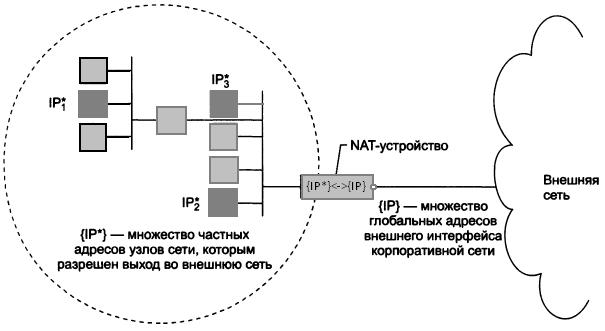
\* Обеспечение корпоративных и частных локальных сетей большим количеством внутренних IP-адресов.

\* Обеспечение безопасности всех узлов локальной сети, путем скрытия внутренних IP-адресов от внешней сети. Своего рода FireWall.

\* Организация доступа к Интернету всем компьютерам локальной сети через единый шлюз, используя единственный IP-адрес.

Необходимость преобразования (трансляции) адресов IP возникает в тех случаях, когда используемые внутри сети адреса IP невозможно использовать за пределами сети из соображений сохранения тайны или по той причине, что эти адреса корректны только внутри сети.  
Сетевая топология за пределами локального домена может изменяться по разным причинам. Абоненты могут менятьпровайдеров, опорные сети компаний могут реорганизоваться, а провайдеры могут делиться или объединяться. Всякий раз при изменении внешней топологии выделение адресов внутри локального домена также требуется соответствующим образом изменять. Эти изменения могут оставаться незаметными для пользователей внутри домена при централизованном изменении на одном маршрутизаторе, обеспечивающем трансляцию адресов.

**Основы NAT**

Идея технологии NAT состоит в следующем. Пусть сеть предприятия образует тупиковый домен, узлам которого присвоены частные адреса (рис. 1). На маршрутизаторе, связывающем сеть предприятия с внешней сетью, установлено программное обеспечение NAT. Это NAT-устройство динамически отображает набор частных адресов {IP\*} на набор глобальных адресов {IP}, полученных предприятием от поставщика услуг и присвоенных внешнему интерфейсу маршрутизатора предприятия.

*Рисунок 1.*

Важным для работы NAT-устройства является правило распространения маршрутных объявлений через границы частных сетей. Объявления протоколов маршрутизации о внешних сетях «пропускаются» пограничными маршрутизаторами во внутренние сети и обрабатываются внутренними маршрутизаторами. Обратное утверждение неверно — маршрутизаторы внешних сетей не получают объявлений o внутренних сетях, объявления о них отфильтровываются при передаче на внешние интерфейсы. Поэтому внутренние маршрутизаторы «знают» маршруты ко всем внешним сетям, а внешним маршрутизаторам ничего не известно о существовании частных сетей.

Традиционная технология NAT подразделяется на технологии базовой трансляции сетевых адресов (Basic Network Address Translation, Basic NAT) и трансляции сетевых адресов и портов (Network Address Port Translation, NAPT). В технологии Basic NAT для отображения используются только IP-адреса, а в технологии NAPT — еще и так называемые транспортные идентификаторы, в качестве которых чаще всего выступают TCP- и UDP-порты.

**Теоретический мини коллоквиум**

Согласно варианту задания ответить на теоретический вопрос ( можно ***письменно, главное чтобы текст был читабельным) и вставить*** в отчет (Своего рода реферат).

Вариант 39.

**Мобильные сети**

Ответ:

Отдельные элементы системы сотовой связи существовали и раньше. В частности, некоторое подобие сотовой системы использовалось в 1949 г. в Детройте (США) диспетчерской службой такси — с повторным использованием частот в разных ячейках при ручном переключении каналов пользователями в оговорённых заранее местах. Однако архитектура той системы, которая сегодня известна как система **сотовой связи**, была изложена только в техническом докладе компании Bell System, представленном в Федеральную комиссию связи США в декабре 1971 года. С этого времени начинается развитие собственно сотовой связи.



*Рисунок 1. Сотовые панельные антенны на башне*

В 1974 г. Федеральная комиссия связи США приняла решение о выделении для сотовой связи полосы частот в 40 МГц в диапазоне 800 МГц; в 1986 г. к ней было добавлено ещё 10 МГц в том же диапазоне. В 1978 г. в Чикаго начались испытания первой опытной системы сотовой связи на 2 тыс. абонентов. Поэтому 1978 год можно считать годом начала практического применения сотовой связи. Первая автоматическая коммерческая система сотовой связи была введена в эксплуатацию также в Чикаго в октябре 1983 г. компанией American Telephone and Telegraph (AT&T). В Канаде сотовая связь используется с 1978 г., в Японии — с 1979 г., в североевропейских странах (Дания, Норвегия, Швеция, Финляндия) — с 1981 г., в Испании и Англии — с 1982 г. По состоянию на июль 1997 г. сотовая связь работала более чем в 140 странах всех континентов, обслуживая более 150 млн абонентов.

Первой коммерчески успешной сотовой сетью была финская сеть Autoradiopuhelin (ARP). Это название переводится на русский как «Автомобильный радиотелефон». Запущенная в 1971 г., она достигла 100%-го покрытия территории Финляндии в 1978 году, а в 1986 году в ней было более 30 тыс. абонентов. Работала сеть на частоте 150 МГц, размер соты — около 30 км.

Принцип действия сотовой связи



*Рисунок 2. Сотовая вышка CDMA*

Сотовые панельные антенны на башне

Основные составляющие сотовой сети — это сотовые телефоны и базовые станции, которые обычно располагают на крышах зданий и вышках. Будучи включённым, сотовый телефон прослушивает эфир, находя сигнал базовой станции. После этого телефон посылает станции свой уникальный идентификационный код. Телефон и станция поддерживают постоянный радиоконтакт, периодически обмениваясь пакетами. Связь телефона со станцией может идти по аналоговому протоколу (AMPS, NAMPS, NMT-450) или по цифровому (DAMPS, CDMA, GSM, UMTS). Если телефон выходит из поля действия базовой станции (или качество радиосигнала сервисной соты ухудшается), он налаживает связь с другой (англ. *handover*).

Сотовые сети могут состоять из базовых станций разного стандарта, что позволяет оптимизировать работу сети и улучшить её покрытие.

Сотовые сети разных операторов соединены друг с другом, а также со стационарной телефонной сетью. Это позволяет абонентам одного оператора делать звонки абонентам другого оператора, с мобильных телефонов на стационарные и со стационарных на мобильные.

Операторы могут заключать между собой договоры роуминга. Благодаря таким договорам абонент, находясь вне зоны покрытия своей сети, может совершать и принимать звонки через сеть другого оператора. Как правило, это осуществляется по повышенным тарифам. Возможность автоматического роуминга появилась лишь в стандартах 2G и является одним из главных отличий от сетей 1G.

Операторы могут совместно использовать инфраструктуру сети, сокращая затраты на развертывание сети и текущие издержки.