ИПМ им.М.В.Келдыша РАН

Абрау-2017 • Труды конференции

Г.М. Михайлов, М.А. Жижченко,
А.М. Чернецов

**Обеспечение плавной перенумерации
сети при смене провайдера**

Рекомендуемая форма библиографической ссылки

Михайлов Г.М., Жижченко М.А., Чернецов А.М. Обеспечение плавной перенумерации сети при смене провайдера // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. — С. 351-355. — URL: <http://keldysh.ru/abrau/2017/44.pdf> doi:[10.20948/abrau-2017-44](https://doi.org/10.20948/abrau-2017-44)

Размещена также [презентация к докладу](#)

Обеспечение плавной перенумерации сети при смене провайдера

Г.М. Михайлов¹, М.А. Жижченко¹, А.М. Чернецов¹

1 Вычислительный центр им. А.А. Дородницына ФИЦ ИУ РАН

Аннотация. В данной статье представлены результаты решения проблем, связанных с переходом от схемы доступа в виде статических реальных IP-адресов к динамическим, («серым») в связи со сменой провайдера применительно к локальной компьютерной сети (ЛКС) Вычислительного центра им. А.А.Дородницына ФИЦ ИУ РАН. Решение о смене провайдера было принято в связи с реорганизацией ВЦ РАН. В основу реализации проекта перехода была положена концепция максимального сохранения инфраструктуры ЛКС ВЦ РАН, ее программно-аппаратной платформы на начало 2017 года. В работе изложены основные подходы и пути их реализации с учетом топологии, специфики и функциональных особенностей ЛКС на момент начала работ.

Ключевые слова: Ethernet, IP-адрес, DHCP, NAT, DNS, маршрутизация

Введение

Со времени создания ЛКС ВЦ РАН и полномасштабного выхода ее в Internet (октябрь 1995 г.) по 31 декабря 2016 г. сеть работала с провайдером FREENet [1,2]. В юридическом плане отношения с провайдером оформлялись договорами на оказание следующих услуг:

- подключение по протоколам IPv4 и IPv6;
- выделение адресного пространства IPv4 в сети Интернет объёмом 16 сетей класса C (по 256 адресов) с регистрацией его в уполномоченных международных и российских организациях;
- обеспечение полосы пропускания канала не менее 50 Мбит/с (дуплекс);
- обеспечение неограниченного объема входящего и исходящего трафика без уменьшения полосы пропускания канала;
- предоставление возможности использования публичного номера автономной системы (AS) для организации трёх BGP сессий между двумя пограничными маршрутизаторами Заказчика и тремя маршрутизаторами Оператора для повышения надежности предоставления услуг;
- доступ к трем центральным серверам Оператора для синхронизации системных часов;
- предоставление возможности самостоятельно управлять внешней маршрутизацией через BGP- community;
- предоставление возможности использовать на сети Оператора от 3 до 10 различных классов обслуживания трафика Заказчика (QoS);

- предоставление возможности использования технологии многоадресной рассылки (multicast-групповая передача).

Перечисленные выше услуги оказывались провайдером FREEnet в полном объеме вплоть до 26.12.2016 года включительно. Указанный жесткий срок отключения сети от FREEnet диктовался двумя неотложными условиями:

- сроком сдачи научных отчетов в рамках выполнения грантов РФФИ и других проектов (до 26.12.2016);
- переводом всей действующей сети ВЦ РАН на новую сетку провайдера АКАДЕМИНФОРМ по распоряжению дирекции ФИЦ ИУ РАН к 01.01. 2017 года.

План – график работ по плавному переводу ЛКС ВЦ РАН на сетку АКАДЕМИНФОРМа с учетом особенностей аппаратно-программной платформы действующей сети разрабатывался авторами данной работы в течение 2016 года. В основу была положена концепция максимального сохранения архитектуры сети при полном сохранении сервиса пользователям всех уровней института. Понятие «плавной перенумерации сети» в данном случае имеет отношение только к пользовательской среде, которая не должна была заметить какие-либо неудобства, связанные с проведением комплекса работ по смене провайдера. В обязанности разработчиков, одновременно и исполнителей этого проекта входила реализация именно этой выбранной концепции.

Реализация плавной перенумерации сети при смене провайдера

Как было изложено выше, изначально доступ в Интернет обеспечивался за счет создания BGP-соединения (Border Gateway Protocol) двух пограничных маршрутизаторов ВЦ РАН с двумя маршрутизаторами FREEnet [3]. Как известно, BGP-протокол, будучи протоколом прикладного уровня, функционирующим поверх протокола транспортного уровня TCP, является основным протоколом динамической маршрутизации в сети Интернет и предназначен для обмена информацией о достижимости подсетей между автономными системами (АС). Контроль трафика, обеспечение безопасности, маршрутизация внутри ЛКС и другие функции реализовывались на указанных пограничных маршрутизаторах. В схеме подключения использовались два маршрутизатора, которые работали в режиме горячего резервирования с применением протоколов HSRP (Hot Standby Router Protocol) и OSPF (Open Shortest Path First).

Новая схема подключения к провайдеру АКАДЕМИНФОРМ основана на прямом соединении свитчей (уровень L2). При решении проблем, связанных со сменой провайдера, был произведён анализ ресурсов ЛВС на предмет того, какие ресурсы должны быть доступны извне и в каком объеме. Этим ресурсам должны быть сопоставлены прямые IP- адреса, выделенным новым провайдером. В качестве таких ресурсов в нашей сети выступают:

- DNS - сервера -3 адреса;

- MX - сервера – 2 адреса;
- Smtп-сервера – 3 адреса;
- Web - сервер (сайт ВЦ ФИЦ ИУ РАН) – 1 адрес;
- Ntp - сервера – 2 адреса;
- Сервер антивирусной защиты Drweb – 2 адреса для версий 6.0 и 10.0;
- Wifi - 3 адреса;
- Маршрутизаторы ВЦ ФИЦ ИУ РАН – 2 адреса;
- Сервер ПРНД – 1 адрес
- Персональные пользовательские сервера – 5 адресов.

С учетом вышеизложенного реализованы две взаимно дополняющие друг друга возможности для решения указанных проблем:

- 1) Создание DMZ (Demilitarized Zone) – демилитаризованной зоны, то есть сегмента, содержащего общедоступные сервисы, но при этом обеспечивающего дополнительный уровень безопасности локальных ресурсов. При этом устройству назначается реальный IP-адрес, и это устройство выходит в Интернет напрямую;
- 2) Переназначение («проброс») портов. Соответственно, для таких ресурсов необходимо зафиксировать отображения портов по принципу «порт на реальном адресе – порт на внутреннем адресе».

С учетом дефицита IP-адресов, выделенных провайдером для организации, все остальные ресурсы должны стать так называемыми «серыми», то есть «спрятанными» в адресном пространстве по методу трансляции сетевого адреса NAT (Network Address Translation) [4]. Как известно, для реализации подобных схем IANA (Internet Assigned Numbers Authority) выделила три диапазона частных IP-адресов:

10.0.0.0/8 – 10.255.255.255/8 (16 777 216 хостов);

172.16.0.0/12 – 172.31.255.255/12 (1 048 576 хостов);

192.168.0.0/16 – 192.168.255.255/16 (65 536 хостов).

Внедрение технологии NAT позволяет решить следующие задачи:

- Обеспечение корпоративных и частных локальных сетей большим количеством внутренних IP-адресов. При этом не возникает конфликтов между одинаковыми IP-адресами разных организаций.
- Обеспечение безопасности всех узлов локальной сети путем скрывания внутренних IP-адресов от внешней сети.
- Организация доступа к сети Интернет всем компьютерам одной локальной сети через единый шлюз, используя единственный IP-адрес.

В нашей схеме для реализации NAT- технологии выбран первый диапазон 10.0.0.0/8, как наиболее предпочтительный с учетом количества пользовательских точек. В качестве реального IP- адреса на выходе NAT-блока выделен один единственный IP-адрес, предоставленный провайдером. Такое решение получило название PAT-технологии (Port Address Translation, либо его называют Many-to-One NAT).

Для обеспечения «проброса» портов был установлен nginx-сервер, который, начиная с версии 1.11.5, поддерживает данный функционал [5]. В процессе выполнения работ выяснилось, что доступная бинарная версия была скомпилирована без его поддержки, поэтому пришлось компилировать выполняемый файл из исходного кода.

В результате проведенных преобразований в DMZ остались маршрутизаторы, DNS-сервера, сервера, обслуживающие электронную почту (POP3/IMAP/SMTP), и несколько других серверов.

В процессе выполнения работ был также решен вопрос с работой и переносом DNS-серверов. В предыдущей конфигурации сети они были реализованы на основе BIND (Solaris 10, Solaris 8). В новой конфигурации сети с вводом в нее зоны DMZ пришлось для DNS-серверов вводить представления (views) public и internal. При этом в зоне internal обслуживаются все запросы для клиентов, входящих в адресное пространство «серых» адресов, а в зоне public обслуживаются все запросы для клиентов адресного пространства реальных адресов, в том числе находящихся вне ЛВС ВЦ ФИЦ ИУ РАН. Для таких клиентов DNS-сервера обслуживают только зону ccas.ru. Отметим также, что DNS-сервера на базе ОС Windows не позволяют работать с представлениями. Соответственно, при организации сетевого трафика на базе этой платформы пришлось бы создавать отдельные сервера (физические или виртуальные) для решения этой задачи [6].

Ещё одна проблема возникла при назначении IP-адресов в новой сети. За долгие годы работы при статической адресации устройствам было назначено несколько сотен статических IP-адресов [1,2]. Все эти адреса было необходимо заменить на новые. Эта задача решалась с применением протокола DHCP (Dynamic Host Configuration Protocol) на маршрутизаторах cisco 3925 и cisco 2851. Из-за необходимости внедрения технологии преобразования сетевых адресов NAT и с учетом того, что маршрутизацию выполняет NAT-сервер, пришлось перенести функции маршрутизатора на выделенный сервер под управлением Solaris 10. Для настройки NAT пришлось настраивать встроенный в ОС ipfilter.

Следует заметить, что при всей простоте и привлекательности внедрения NAT-технологии для компенсации нехватки IP-адресов подобное решение скорее вынужденное, чем оптимальное. Как описано в [4], NAT-технологии свойственны следующие недостатки:

- нарушение основного принципа уникальности каждого IP-адреса;
- нарушение «сквозного» принципа: каждый хост должен уметь отправлять пакет любому другому хосту в любой момент времени;
- нарушение (косвенное) принципа работы сети без установления соединения;
- нарушение одного из фундаментальных правил построения многоуровневых протоколов: уровень k не должен строить предположений о полезной нагрузке, поступающей от уровня $k+1$;

– нарушение принципа использования многоуровневых TCP/IP-соединений.

Несмотря на перечисленные недостатки, на данный момент это решение было единственно возможным как из-за временных ограничений сроков выполнения работ, так и в связи с резким ограничением ресурсов по IP-адресам.

В результате проведенных работ в январе 2017 г. был произведён успешный переход на новый провайдер, а время простоя было доведено до минимального значения без особого ущерба для пользователей сети.

В заключение заметим, что в процессе интеграции информационно-вычислительной системы (ИВС), развернутой на обновленной аппаратно-программной платформе ЛВС ВЦ РАН в общую инфраструктуру ФИЦ ИУ РАН, было обеспечено прямое физическое соединение между ИВС ВЦ РАН и ИПИ РАН, и соответственно, реализован доступ по протоколу TCP/IP из сети ВЦ РАН в внутреннюю сеть ИПИ РАН. Решение реализовано путем «проброски» соответствующих VLAN на коммутаторах в ВЦ РАН и ИПИ РАН.

Работа представлена в рамках выполнения темы: «Локальная информационно-коммуникационная сеть ВЦ ФИЦ ИУ РАН, как составная часть единой объединенной сети Центра».

Литература

1. И.В. Байкова, М.А. Копытов, М.В. Кулагин, Г.М. Михайлов, Ю.А. Привезенцев, Ю.П. Рогов. Распределенные информационно - вычислительные системы. Выпуск 1. Локальная сеть ВЦ РАН. — М.: ВЦ РАН, 1995, 111 с.
2. И.В. Байкова, М.А. Копытов, М.В.Кулагин, А.В. Метелкин, Г.М. Михайлов, П.Ю. Плечов, Ю.П. Рогов. Распределенные информационно - вычислительные системы. Выпуск 2. Инфраструктура и базовые средства локальной сети ВЦ РАН. — М.: ВЦ РАН, 1996, 99 с.
3. Рогов Ю.П., Чернецов А.М. Аппаратно-программные средства и развитие инфраструктуры ИВС ВЦ РАН. — М.: ВЦ РАН, 2010. 120 с.
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. 960 с. ISBN 978-5-459-00342-0Э.
5. <https://sheensey.ru/nginx>
6. Михайлов Г.М., Рогов Ю.П., Чернецов А.М. Опыт использования виртуальных ресурсов в ИВС ВЦ РАН // Научный сервис в сети Интернет: все грани параллелизма: Труды Международной суперкомпьютерной конференции (23-28 сентября 2013 г., г. Новороссийск). — М.: Изд-во МГУ, 2013 — С. 333-338. — 589 с.