ИНФРАСТРУКТУРА ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ АКАДЕМИЧЕСКОГО УЧРЕЖДЕНИЯ И ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Г.М. Михайлов, Ю.П. Рогов, А.М. Чернецов

В докладе изложены вопросы развития, поддержки и администрирования инфраструктуры локальных компьютерных сетей (ЛКС) на примере Учреждения Российской академии наук Вычислительного центра им. А.А. Дородницына РАН (ВЦ РАН), одного из ведущих профильных институтов в области прикладной математики и информатики [1].

Функционирующая в настоящее время локальная компьютерная сеть (ЛКС), на базе которой развернута информационно-вычислительная система (ИВС), была спроектирована и выполнена ЗАО "АКАДЕМИНФОРМ" по заказу ВЦ РАН в течение 2004-2005 гг. с представлением заказчику всех необходимых проектно-сметных и исполнительных документаций, протоколов испытаний в соответствии с правилами и стандартами, регламентирующими проектирование и строительство объектов связи [2].

Спецификация кабельной сети соответствует ANSI/TIA/EIF-568-B.2 Category 5e. Топология сети включает в себя две площадки в виде двух зданий, интегрированных в единую сеть с точки зрения управления и функционирования. Заметим, что созданная структурированная кабельная сеть (СКС) включает в себя также всю телефонную сеть и систему пожарно-охранной сигнализации института.

В части активного коммуникационного оборудования было сформировано совершенно новое ядро компьютерной сети ВЦ РАН. В качестве ядра сети были выбраны коммутаторы Cisco Catalyst 3750, которые предназначены для сетей Ethernet с производительностью 10, 100 и 1000 Мб/сек. Эти коммутаторы просты в использовании и являются одними из самых надежных среди устройств со стековым подключением [2].

Для стекирования коммутаторов этой серии используется технология Cisco StackWise, поддерживающая быстродействие на уровне 32 Гб/сек. Технология стекирования коммутаторов позволяет использовать стек как один коммутатор с общим пространством MAC-адресов и одним IP-адресом управления. Стек коммутаторов включает в себя:

- Catalyst 3750-24TS-S (2 устройства) с 24 портами 10/100Мб/с и 2 портами Gigabit Ethernet;
- Catalyst 3750-48TS-S (7 устройств) с 48 портами 10/100Мб/с и 4 портами Gigabit Ethernet.

В трех узлах связи коммутаторы объединены по три в стек.

Новые модели Cisco Catalyst 3750 Series Switches, обеспечивая объединение в стек до девяти коммутаторов, позволяют получить в одном логическом устройстве до 432 портов 10/100 Fast Ethernet или до 468 портов 10/100/1000 Gigabit Ethernet. Каждый стек коммутаторов Catalyst 3750, с точки зрения системы управления, выглядит как единое логическое устройство, для управления которым используется один IP-адрес.

Одновременно с заменой сетевых коммутаторов в узлах связи была произведена и установка нового маршрутизатора Cisco2851 Internet Security Router. Главное отличие нового маршрутизатора от старого - наличие модуля Four port 10/100 Ethernet Switch Interface Card.

Этот модуль дает возможность работать в сети с четырьмя адресными интерфейсами (4 порта), один из которых отвечает за внешний канал связи (Интернет). Выход на этот канал осуществляется через трансивер и далее через оптоволоконный кабель до маршрутизатора провайдера.

Наличие большого адресного пространства (IP-addresses), выделенного ВЦ РАН провайдером, позволило очень гибко использовать этот ресурс для виртуальной сегментации нашей сети. Чтобы частично задействовать эти ресурсы, был установлен еще один дополнительный аналогичный модуль.

В 2009 г. силами организации IBS Platformix был проведен аудит сетевой инфраструктуры ВЦ РАН. Целью аудита ставилась апробация текущей конфигурации локальной вычислительной сети (ЛВС) и внешнего канала ВЦ РАН, выявление слабых мест в конфигурации и выдача рекомендаций по модернизации с учётом выявленных замечаний.

При анализе работы ЛВС рассматривались используемая модель VLAN (виртуальные локальные сети), состояние протокола STP, а также защищённость сети от внутрисетевых атак и несанкционированного доступа к ресурсам. При анализе работы маршрутизатора, обеспечивающего связь с оборудованием провайдера, исследовался настроенный функционал маршрутизации, а также количественные показатели качества работ Интернет-канала: скорость, потери, задержки.

В общей корпоративной сети было определено разделение на несколько подсетей посредством VLAN. В каждой из VLAN для пользователей, серверов и интерфейсов сетевых устройств используется собственная адресация. Маршрутизация между подсетями происходит на маршрутизаторе Cisco2851. Для связи с ресурсами Интернета и объявления в глобальную сеть собственного диапазона глобально значимых IP-адресов используется протокол "внешней" маршрутизации BGP.

Несколько слов о производительности локальной компьютерной сети ВЦ РАН. Как уже было представлено, ЛКС ВЦ РАН состоит из высокопроизводительных коммутаторов серии Cisco Catalyst 3700. Соединения рабочих станций организации с коммутаторами организованы по стандарту FastEthernet, способному поддерживать скорость до 100 Мб/сек. Соединения коммутаторов между собой организованы по стандарту GigabitEthernet, способному поддерживать скорость до 1 Гб/сек.

В существующей конфигурации сеть отвечает требованиям приложений, использующих её для передачи данных. Негативное влияние на производительность локальной сети мог бы оказать паразитный широковещательный трафик, образующийся при существовании колец на канальном уровне модели OSI. Но в нашем случае этой проблемы нет. Во-первых, в топологии сети нет замкнутых магистралей. Во-вторых, протокол STP по умолчанию включен на всех коммутаторах Cisco, и остовые деревья для каждой из VLAN строит верно.

Загрузка каналов коммутаторов сети в рабочее время не превышает 10%, а загрузка их ОЗУ не превышает 20%. Таким образом, запас по производительности в текущей сетевой конфигурации велик.

Что особенно нас интересовало, так это производительность внешнего канала (Интернет).

Доступ пользователей и серверных приложений из локальной сети в Интернет осуществляется через канал, организованный между маршрутизатором Cisco2851 и маршрутизаторами Интернет-провайдера. Единовременно в работе находится только одно из установленных соединений - в соответствии с результатом работы протокола BGP.

На физическом уровне подключение производится на скорости 100Мб/сек. В действительности скорость обмена информацией ресурсов локальной сети и ресурсов Интернета ниже из-за ограничений, вводимых администраторами Интернет-ресурсов, а также возможными задержками, вносимыми оборудованием Интернет-провайдеров.

Тестирование производительности Интернет-канала проводилось с использованием двух инструментов: IP SLA UDP Jitter и NetFlow Anayzer. В соответствии с технологией IP SLA маршрутизатор Cisco2851 выступал в качестве клиента - устройства, отправляющего тестовые пакеты. В качестве "респондера" - устройства, принимающего тестовые пакеты от клиента и высылающего пакеты клиенту в ответ - выступал маршрутизатор Cisco2821, расположенный в Москве на расстоянии около 15 км от здания ВЦ РАН. Также был проведён тест с использованием в качестве "респондера" маршрутизатора провайдера, подключенного к сети ВЦ РАН непосредственно.

Для снятия статистики в соответствии с технологией NetFlow на маршрутизаторе Cisco2851 была включена функция анализа всех IP-пакетов, входящих через интерфейс, обращённый в Интернет, и формирования записей, содержащих информацию о значениях заголовков проходящих IP-пакетов и, если имеются, заголовков протоколов транспортного уровня.

Полученная статистика говорит о хороших качественных показателях канала, а пропускная его способность пока внутренние потребности не ограничивает.

Общая локальная сеть разбита на несколько VLAN, что увеличивает количество широковещательных доменов и, таким образом, уменьшает объём широковещательного трафика, передаваемого по сети. Поэтому возможное расширение пользовательского пула не должно привести к перегрузкам в сети.

Проведенный аудит позволил выработать некоторое количество рекомендаций по улучшению эксплуатационных характеристик существующей сети ВЦ РАН. В настоящее время многие из этих рекомендаций реализованы, часть находится в процессе реализации. Заметим, к такой реализации нужно подходить очень осторожно.

В любом случае, эта процедура (аудит) оказалась на редкость полезной, и мы рекомендуем всем "держателям" таких сетевых инфраструктур провести аналогичные работы.

Важной задачей системного администрирования является обеспечение надежности работы и безопасности компьютерной сети. Многолетний опыт администрирования компьютерной сети ВЦ РАН позволил нам накопить некоторый опыт в этих вопросах. Следует отметить, что круг этих вопросов - очень широк. Для их описания необходимо отдельное издание, к тому же эти проблемы многократно, в том числе и специалистами ВЦ РАН, подробно освещались, например в [3]. Здесь мы остановимся лишь на одном из этих вопросов.

Актуальность антивирусной защиты - это отдельная тема, требующая решения проблемы на всех без исключения уровнях работы на современных компьютерах. В рамках обеспечения защиты в корпоративных сетях она становится задачей первостепенной важности. С учетом опыта работы с программой "Dr.Web" компании "Доктор Веб" [4] в течение многих лет, в 2008 году была принята новая концепция - реализация интегрированного варианта на базе сервера "Dr.Web Enterprise suite".

В 2009 г. эта работа была завершена, и практически все компьютеры переключены на новый режим работы антивирусной программы. Комплекс "Dr.Web Enterprise Suite" позволяет:

- предельно упростить процесс установки антивирусного программного обеспечения на защищаемые компьютеры, причем в большинстве случаев установка может производиться централизованно, без физического доступа к компьютеру;

- централизованно настраивать антивирусное программное обеспечение и производить его обновления с минимальными трудозатратами;
- централизованно обновлять вирусные базы и программное обеспечение на защищаемых компьютерах;
- отслеживать состояние антивирусной защиты;
- при необходимости централизованно запускать или прерывать задания антивирусного программного обеспечения на компьютерах;
- собирать и изучать информацию о вирусных событиях на всех защищаемых компьютерах;
- осуществлять управление антивирусной сетью и получение информации о ней администратором антивирусной защиты как с рабочих мест в сети, так и удаленно через Интернет.

Этот программный комплекс имеет архитектуру "клиент-сервер".

Его компоненты устанавливаются на компьютеры локальной сети и обмениваются информацией, используя сетевые протоколы. Совокупность компьютеров, на которых установлены взаимодействующие компоненты Dr.Web Enterprise Suite, называется антивирусной сетью.

В состав антивирусной сети входят компоненты, перечисленные ниже.

- антивирусный агент устанавливается на защищаемом компьютере, производит установку, обновление и управление антивирусным пакетом в соответствии с инструкциями, получаемыми с антивирусного сервера, передает на антивирусный сервер информацию о вирусных событиях и другие необходимые сведения о защищаемом компьютере;
- антивирусный сервер устанавливается на одном из компьютеров локальной сети, хранит дистрибутивы антивирусных пакетов для различных ОС защищаемых компьютеров, обновления вирусных баз, антивирусных пакетов и антивирусных агентов, пользовательские ключи и настройки пакетов защищаемых компьютеров, передает их по запросу агентов на соответствующие компьютеры, ведет единый журнал событий антивирусной сети и журналы по отдельным защищаемым компьютерам;
- антивирусная консоль используется для удаленного управления антивирусной сетью путем редактирования настроек антивирусного сервера, а также настроек защищаемых компьютеров, хранящихся на антивирусном сервере.

Закупаемые нами лицензии за период 2008 - 2010 гг. составили от 200 до 250. Максимальное количество одновременно работающих клиентов - 70.В перспективе планируется перевести большинство компьютеров института на корпоративную версию "Dr.Web Enterprise Suite" (более 300 ПК), с возможностью использования и других вариантов этой антивирусной программы.

Одна из актуальнейших наших задач - это полномасштабный перевод программного обеспечения (ПО) всех уровней ЛКС ВЦ РАН,в том числе и для параллельных вычислений,на прозрачный лицензионный уровень. Заметим, что статья расходов на такое ПО при ее исполнении оказывается весьма затратной по причине исключительной динамичности ПО и многочисленных поставляемых версий. Кроме того, многие лицензионные программы (даже в единственном экземпляре!) имеют очень большую стоимость.

Как известно, лицензии на ПО бывают нескольких типов:

- по стоимости: бесплатные, условно-бесплатные, с ограничением функционала, коммерческие;
- по объекту лицензирования: лицензия на процессор, лицензия на пользователя,лицензия на компьютер;
- по сроку действия: неограниченные, с заданным сроком действия, полный функционал, пробные (trial);
- с точки зрения установки: на рабочее место, на сервер (запуск с сервера), на сервер (запуск с клиента);
- по типу ключевой информации: аппаратный ключ, лицензионный код, ключевой файл;
- по типам: сетевые (многопользовательские), concurrent, персональные, на 1 рабочее место, single;
- с точки зрения надежности: concurrent лицензии: с резервированием, без резервирования;
- по объекту лицензирования: лицензия на процессор, лицензия на пользователя, лицензия на компьютер.

Таким образом, при приобретении лицензионного программного обеспечения постоянно приходится решать сложные задачи по оптимальному выбору, как объектов лицензирования, так и самих программных продуктов.

Заключение.

Срок старения структурированной кабельной системы составляет согласно технической документации 8-10 лет. Компьютерная техника стареет значительно быстрее.

По сравнению с этими "долгожителями" программное обеспечение - "бабочка-однодневка" - постоянно видоизменяется, устаревает, отмирает. Тем не менее, установка обновлений, новых версий программного обеспечения - важная часть системного администрирования.

То же самое касается и модернизации ПК и серверов: увеличение размеров оперативной памяти, объема дисковой памяти, обновление комплектующих, наконец, замена устаревшей техники на более новую.

Наша задача - по возможности не отставать, а может быть даже и предвидеть грядущие изменения. Все зависит от квалификации специалистов, возможностей организации, финансирующей эту деятельность, наконец, от желания или степени энтузиазма тех же специалистов.

Во многом благодаря этим обстоятельствам в ВЦ РАН появилась новая СКС, было установлено и запущено современное сетевое оборудование в 3-х узлах связи, приобретено большое количество мощных серверов, ИБП различных конфигураций.

В ВЦ РАН успешно функционируют вычислительные кластеры (16-ти процессорный, SMP(4)),к подготовке к запуску находится новая система на базе HP Blade C3000. Кроме этого, были оборудованы и обустроены помимо узлов связи и две серверные (стойки, шкафы, кондиционеры, видеокамеры).

Для размещения лицензионного программного обеспечения и ключей к нему в ИВС ВЦ РАН было запущено несколько специальных серверов.

Важнейшей работой, выполненной за эти годы, является создание локальной компьютерной сети доменной структуры, что революционным образом повлияло не только на упорядочение работы компьютеров в сети, но и на психологию тех, кто за ними работает. Приходится до сих пор преодолевать неприятие многих нововведений, направленных и на то, чтобы все программное обеспечение было лицензионным.

Но постепенно отношение ко всему происходящему становится терпимей, не в последнюю очередь за счет развертывания в ЛКС дорогостоящего программного обеспечения на серверах сети. Количество пользователей ЛКС растет, число желающих иметь лицензионные операционные системы, другие сопутствующие программные продукты не уменьшается.

И пока это будет продолжаться, компьютерная техника совершенствоваться, новое программное обеспечение создаваться, а старое - поддерживаться, до тех пор будут существовать разные СКС, ЛКС, ИВС.

ЛИТЕРАТУРА:

1. Евтушенко Ю.Г., Михайлов Г.М., Копытов М.А., Рогов Ю.П. 50 лет истории вычислительной техники: от "Стрелы" до кластерных решений. В сборнике: 50 лет ВЦ РАН: история, люди, достижения, М.: ВЦ РАН, 2005.
2. Михайлов Г.М., Байкова И.В., Ващенко В.Ф., Ковалева Г.И.., Рогов Ю.П. Отчет: "Структурированная кабельная система ВЦ РАН" (СКС-2005 ВЦ РАН), М.: ВЦ РАН, 2005.
3. Копытов М.А., Рогов Ю.П. Системное администрирование компьютерной сети. Надежность и безопасность. Тезисы доклада в сборнике Всероссийской научной конференции "Научный сервис в сети Интернет" (г.Новоросийск, 18-23 сентября 2000 г.). - М.: МГУ, 2000.
4. http://www.drweb.com