Развитие корпоративной сети Межведомственного суперкомпьютерного центра

О.С. Аладышев, А.П. Овсянников, Б.М. Шабанов

Аннотация

В статье рассматриваются проблемы развития корпоративной вычислительной сети на примере локальной вычислительной сети Межведомственного суперкомпьютерного центра. Обсуждены вопросы организации высокоскоростного доступа к вычислительным и информационным ресурсам, мониторинга и управления, надежности и защищенности.

Кратко обсуждается работающая структура локальной вычислительной сети Суперкомпьютерного Центра, рассматриваются достоинства и недостатки, узкие места.

Вступление.

ГУ Межведомственный Суперкомпьютерный Центр – первый центр, созданный для поддержки высокопроизводительных расчетов научного сообщества России, существует относительно недолго. В Америке таких центров значительно больше, больше и их мощность. В России же зачастую полагают, что слово «суперкомпьютерный» просто новомодное слово, используемое организацией для саморекламы. Тем не менее, слово “суперкомпьютер” не означает “очень модный, дорогой и особенно котирующийся в среде подростков” персональный компьютер. Это общепринятое определение счетных систем на электронной базе, построенных лишь с одной целью - ускорить ход математических расчетов различных фундаментальных научных задач в различных областях: гидро- и газодинамики, сверхпроводимости, астрономии, генетики, биологии, разработки фармацевтических препаратов, материаловедения, разведки нефти и газа, прогнозирования погоды и многих других. Для решения таких задач требуются большие скорости вычислений, технологии распараллеливания расчетов, визуализации, ввода и хранения колоссальных объемов данных.. Вычислительные системы такого рода очень сложны, их построение и эксплуатация требует больших затрат. В Межведомственном суперкомпьютерном центре накоплен опыт по созданию таких систем и их обслуживанию. Этот опыт нашел отражение в данной статье.

Требования к построению сети центра.

В предыдущей статье, описывавшей локальную сеть Центра, подробно рассматривались принципы, по которым надо строить большие корпоративные сети [1]. Во главу угла ставится надежность работы. Простой сети из-за поломки почти всегда приводит к простою дорогостоящих суперкомпьютеров. И если минута простоя сети стоит десятки долларов, то простой 1-Терафлопного суперкомпьютера стоит десятки тысяч долларов. На втором месте по важности стоит защита информации, далее - гибкость, доступность, защита, эффективность, качество сервиса.

Заметим, что скорость передачи информации не рассматривается в качестве важнейшего

критерия в проекте развития сети центра, хотя и считается немаловажной. На пороге уже стоит технология 10 Gigabit Ethernet (10GigE), однако ее использование в центре пока не предусматривается. Причиной, прежде всего, является высокая стоимость оборудования 10GigE. Однако нельзя исключить применение этой технологии в будущем для объединения удаленных суперкомпьютеров в высокопроизводительную вычислительную сеть или для доступа суперкомпьютера к банкам данных.

Основными функциями сети вычислительного центра остаются:

- скоростная связь между узлами сети;
- скоростной доступ для удаленных пользователей;
- связь Центра с партнерами
- скоростной доступ в “TeraGrid” научного общества в Америке.

Составляющие:

- комплекс услуг сети Интернет (web-сервис, почта, news-сервис);
- сервис телеконференций;
- сервис доступа к ресурсам (NSF, FTP, SSH, …);
- службы управления (NIS и Active Directory для пользователей, управление доступом, пользователями, управление устройствами и доступом);
- Мониторинг и отчетность;

Локальная вычислительная сеть центра

Ресурсы центра

В настоящее время в Межведомственном Суперкомпьютерном центре эксплуатируются:

- высокопроизводительные вычислительные ресурсы:
  - сервер МВС1000М (768 CPU Alpha 21264, производительность – 1 Терафлоп);
  - сервер МВС1000/200 (96 CPU Alpha 21264);
  - кластер серверов HP V-класс (4 сервера V2250, каждый по 16 процессоров PA8200),
  - учебная вычислительная система МСЦ2000 – кластер на базе процессоров Pentium III;
  - 2-х процессорные графические станции HP J-класс: 3 станции J-2240 и станция J-5000

- рабочие станции C-класс C-240 (4 шт.);
- 2-х процессорная станция D-класс D380;

- хранилище данных - архивная система, построенная на базе двухпроцессорного сервера К-класса фирмы Hewlett Packard (K580) с 3-х уровневой иерархией внешней памяти емкостью 10 Тбайт с программной системой оптимизации размещения информации по уровням, в состав которой входят дисковые массивы: HP Model 30*9GB/FC Fiber Channel Disk Array (~210GB), HP SCSI-2 AutoRAID-5 (12*9.1GB), Jukebox HP SureStore 1200EX (5.2GB x 238 MO дисков).

- рабочие места: X-терминалы и персональные компьютеры, используемые как интеллектуальные терминалы (около 100 рабочих мест)

Локальная вычислительная сеть центра

Локальная вычислительная сеть МСЦ должна обеспечивать:

- высокоскоростной защищенный доступ локальных и удаленных абонентов центра к серверным комплексам;

- обмен информацией между серверами, осуществление резервного копирования и др. сервисных операций;

- бесперебойную связь внутренних абонентов центра с внешними сетями и доступ в Интернет;

- передачу всех видов информации, в том числе расширенную поддержку приложений мультимедиа.

ЛВС Центра разбита на сегменты. Сегментирование сети предназначено для оптимизации работы сети и служит для решения следующих основных задач:

- контроль и фильтрация сетевых потоков и распределение нагрузки между отдельными сетевыми сегментами, соответствующими внутренней структуре центра;

- обеспечение необходимой защиты сетевых ресурсов и сервисов;

- обеспечение требуемого качества сетевых сервисов;

- обеспечение удобства использования и администрирования сетевых ресурсов.

Управление сетью осуществляется с помощью интегрированной системы управления HP OpenView.

ЛВС МСЦ построена с использованием двух основных технологий Fast Ethernet и ATM.

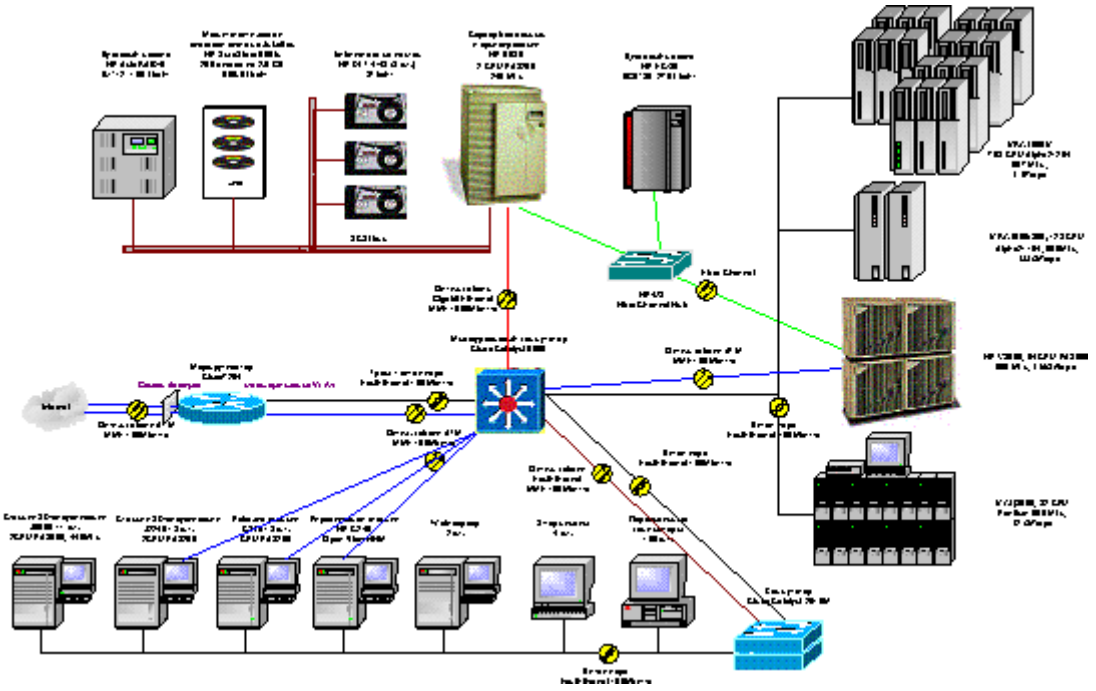

Рис.1. Схема существующей ЛВС

Основным активным сетевым элементом сети, является коммутатор Catalyst 5500 фирмы Cisco Systems. Этот коммутатор поддерживает используемые в сети технологии ATM 155Mbps, Fast Ethernet 100Mbps и обеспечивает поддержку коммутации сегментов внутренней сети МСЦ. Кроме того, через канал оптического Gigabit Ethernet к коммутатору подключен сервер распределенной файловой системы и баз данных – один из наиболее используемых ресурсов центра.

Межсегментная маршрутизация осуществляется через маршрутизатор Cisco 7204. Абоненты сети подключены по протоколам Ethernet и Fast Ethernet через коммутаторы уровня доступа Cisco Catalyst 2916M.

Удаленный доступ из внешних сетей к сети МСЦ осуществляется через маршрутизатор Cisco 7204.

Безопасность доступа к ресурсам МСЦ обеспечивается защитными экранами, расположенными в различных сегментах сети. В настоящее время используются списки доступа (access control lists) на наружном маршрутизаторе Cisco 7204, контролирующем основные каналы связи, и защитные экраны на базе операционной системы FreeBSD, на резервном канале.

Защитные экраны выполняют следующие функции:

- ограничение доступа только по IP протоколу;
- открытие и закрытие доступа из/к внутренней сети по конкретным портам TCP и UDP.

Необходимость развития ЛВС

Существующая локальная вычислительная сеть центра планировалась в 1998 году и

основывалась на передовых технологических решениях того времени. Сеть была сделана масштабируемой и гибкой, благодаря чему и в настоящее время сеть центра удовлетворительно справляется с возросшими информационными потоками.

Однако существует ряд причин, обуславливающих необходимость глубокой модернизации ЛВС.

Ресурсы центра постоянно подвергаются модернизации: в 2001 году был введен в эксплуатацию сервер МВС1000М производительностью 1 Терафлоп; в 2003 году в центре должна быть установлена система производительностью 5 Терафлоп, в 2005 году – 25 Терафлоп; осуществляется расширение системы хранения данных центра; внедряется система видеоконференций; планируется приобретение оборудования для визуализации.

Таким образом, рост и модернизация центра уже сами по себе требуют соответствующей модернизации локальной вычислительной сети.

Кроме того, в существующей топологии сети есть уязвимые места с точки зрения надежности и наращивания производительности.

В частности, узким местом сети, как с точки зрения надежности, так и производительности, является центральный коммутатор Catalyst 5500. В случае поломки или перегрузки коммутатора вся сеть теряет работоспособность.

Другим уязвимым местом сети является маршрутизатор Cisco 7204, который осуществляет и внешнюю маршрутизацию, и маршрутизацию VLAN, и контроль доступа. Это приводит к дополнительной потере производительности. Отказ маршрутизатора также приведет к потере работоспособности всей сети.

Так что, хотя в настоящее время, производительность сети и достаточна для имеющихся в центре ресурсов, ее предел уже достигнут. Кроме того, по мере роста производительности центра увеличивается число его пользователей, важность решаемых задач и, следовательно, возрастают требования к надежности сети и каналов доступа в центр.

Помимо увеличения объема и сложности решаемых задач, появились принципиально новые приложения, активно использующие аудио и видео информацию. Это различные мультимедийные и визуализационные приложения, системы видеоконференций и др. Такие приложения часто используют многопротокольные многоадресные (multicast) потоки данных. Для их использования необходимо повышать производительность сети и внедрять систему контроля качества обслуживания на уровне приложений.

Итак, основными причинами, требующими глубокой модернизации локальной вычислительной сети центра являются:

- расширение вычислительных мощностей и информационных ресурсов центра и достигнутый в настоящее время предел производительности сети;

- возросшие требования надежности и наличие уязвимых с точки зрения надежности мест в существующей конфигурации сети;

- увеличение объема и сложности решаемых задач и появление принципиально новых

сетевых приложений требующих контроля качества обслуживания.

Направления развития сетевой инфраструктуры центра

Направления развития сетевой инфраструктуры напрямую вытекают из целей стоящих перед информационной системой МСЦ.

В связи с увеличением объема и сложности решаемых задач и с появлением принципиально новых приложений, активно использующих аудио и видео информацию, необходимо повышать производительность сети и внедрять систему контроля качества обслуживания на уровне приложений.

С другой стороны увеличения количества приложений предъявляет повышенные требования к надежности сети.

Повышенные требования к надежности неизбежно влекут повышения внимания к защите сети от несанкционированного доступа.

Кроме того, мощнейшим инструментом для решения проблем производительности, качества обслуживания, надежности и защиты является эффективная система управления сетью.

Таким образом, основными приоритетами при развитии сети МСЦ становятся:

- повышение производительности и масштабируемости сети;
- внедрение интеллектуальных сервисов для приложений;
- повышение надежности сетевой инфраструктуры;
- усиление защиты сети;
- внедрение эффективной системы управления сетью.

Возможные решения

Повышение производительности сети может быть обеспечено как расширением общей пропускной способности сети, так и расширением полосы пропускания отдельных сегментов.

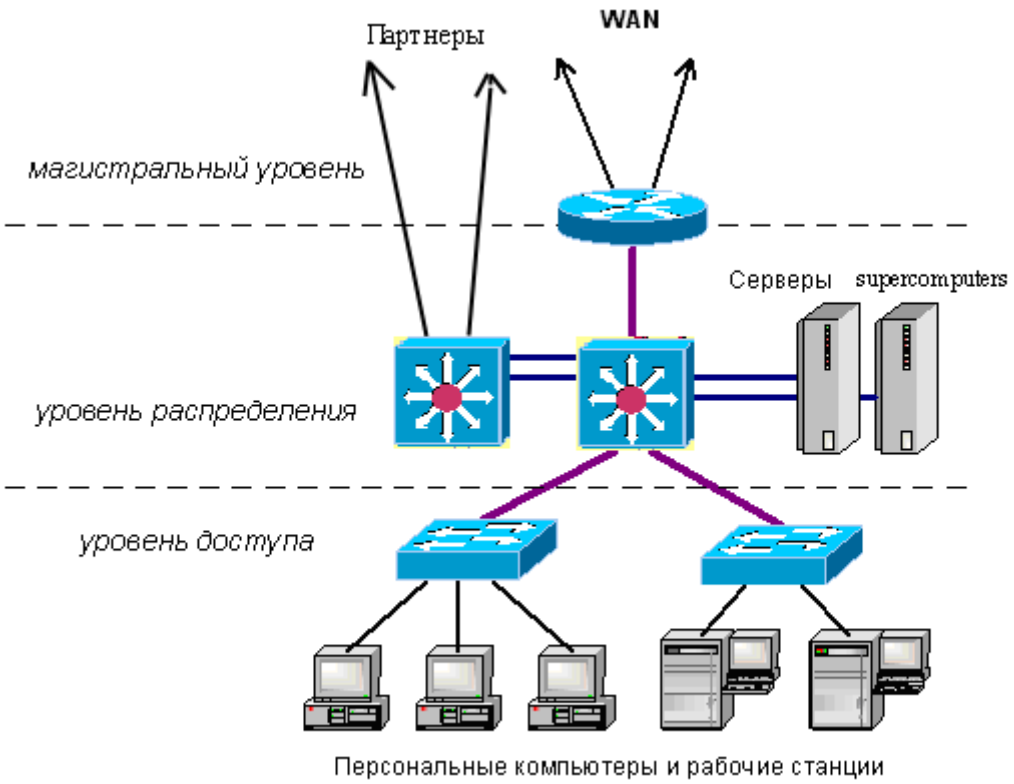

Рис.2. Иерархия сети

Анализ информационных потоков в локальной сети центра показывает, что основные информационные потоки – это потоки между серверным и пользовательским сегментами. Обычно, в корпоративной сети можно снизить информационные потоки, распределив сервера между рабочими группами. Но в локальной сети вычислительного центра это практически невозможно сделать, так как все сервера, имеют общее «вычислительное» назначение; пользовательские рабочие места универсальны, а, следовательно, равноправны; общая файловая система должна быть доступна с любого рабочего места, с любого сервера. И хотя деление на рабочие группы существует и в какой-то мере влияет на дифференциацию информационных потоков, установить такое деление на группы, при котором межгрупповое взаимодействие будет ограничено, не представляется возможным.

Следовательно, для повышения производительности сети необходимо увеличить пропускную способность каналов, соединяющих коммутаторы уровня доступа и уровня распределения; увеличить производительность коммутаторов уровня распределения.

Кроме того, для обеспечения межсегментной маршрутизации на уровне распределения целесообразно использовать коммутаторы третьего уровня.

Поскольку одним из главных требований к модернизируемой сети является требование поддержки управления качеством обслуживания на уровне приложений, все используемые в ЛВС центра коммутаторы и маршрутизаторы всех уровней доступа должны поддерживать стандартный протокол группового управления в Интернет Internet Group Management Protocol (IGMP). Для обеспечения требуемого качества сервиса (QoS), необходимого для передачи критичных к задержке приложений маршрутизаторы и маршрутизирующие коммутаторы должны поддерживать эффективные алгоритмы построения очередей с учетом приоритетов, а

также возможность резервирования полосы пропускания. Кроме того, маршрутизаторы (и маршрутизирующие коммутаторы) должны поддерживать необходимые для передачи видео и аудиотрафика протоколы Protocol Independent Multicast (PIM) и протокол резервирования ресурсов Resource Reservation Protocol (RSVP).

Кстати, эффективное групповое управление позволяет снизить объем непроизводительного трафика, уменьшает нагрузку на коммутаторы и оптимизирует использование полосы пропускания. Таким образом, сеть используется более эффективно, а, следовательно, повышается ее производительность (в широком смысле).

Повышение надежности сети может быть достигнуто за счет обеспечения отказоустойчивости работы ключевых сетевых элементов и узлов сети. Для этого наиболее ответственное активное оборудование и каналы могут дублироваться или резервироваться. Кроме того, может использоваться перенаправление трафика по альтернативным путям.

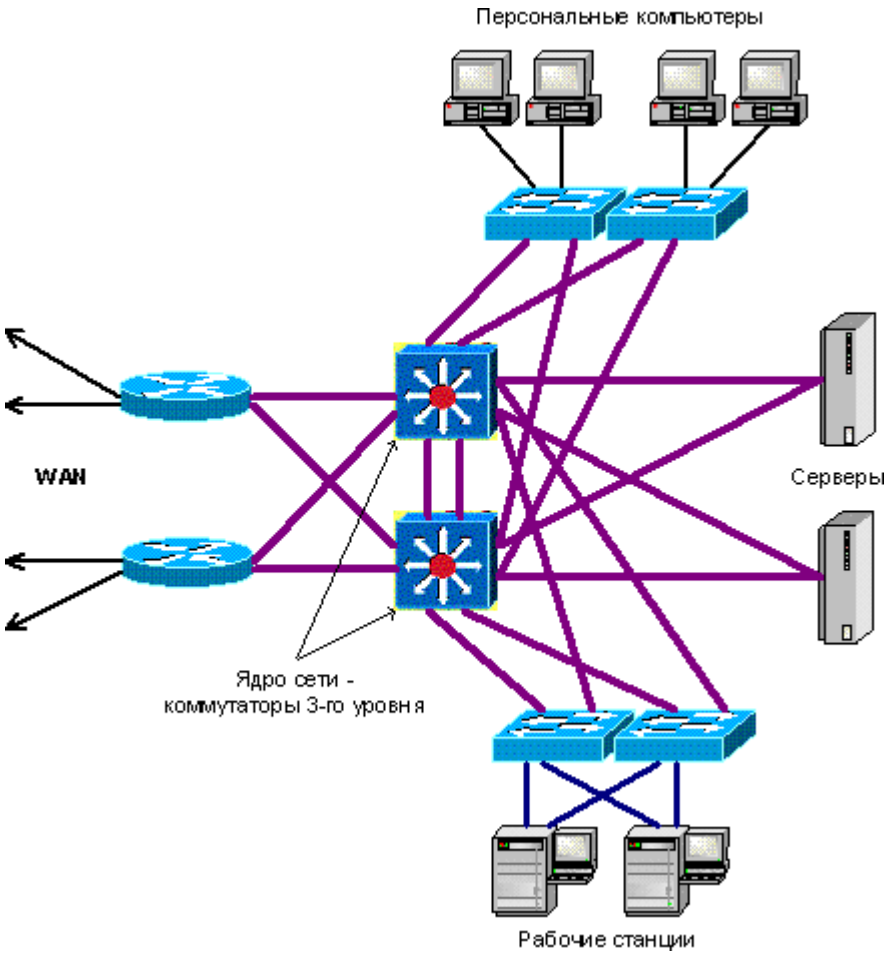

Рис.3. Дублирование ключевых элементов сети.

В ЛВС суперкомпьютерного центра дублирование наружных маршрутизаторов и коммутаторов ядра сети представляется совершенно оправданным. Естественно, коммутаторы уровня доступа

должны подключаться двумя каналами к разным коммутаторам. Сервера также должны присоединяться к сети как минимум двумя каналами.

Возможно, оправданным является и резервирование коммутаторов уровня доступа, хотя подключение каждого рабочего места к двум коммутаторам вряд ли экономически целесообразно.

Защита сети центра может быть усовершенствована за счет установки отказоустойчивой системы защитных экранов, обеспечивающих бесперебойный доступ к внешним ресурсам из сети МСЦ и контролируемый доступ к ресурсам МСЦ извне.

Кроме того, защищенный удаленный доступ в сеть МСЦ может быть расширен за счет установки сервера удаленного доступа.

Как уже упоминалось, эффективные средства управления сетью способны помочь решению проблем повышения производительности, надежности и защиты сети. Система управления сетью должна решать следующие задачи:

- управление конфигурацией сети;
    - управление ошибками;
    - управление производительностью;
    - управление безопасностью;
    - учет работы сетевых устройств.

Система управления сетью должна иметь возможность интеграции с используемой в центре системой управления информационными ресурсами и технологиями предприятия – HP Open View.

Безусловно, модернизация сети должна проводится, по возможности, с сохранением уже имеющейся сетевой инфраструктуры и технологий.

Предлагаемое программно-аппаратное решение

Локальная Вычислительная Сеть МСЦ

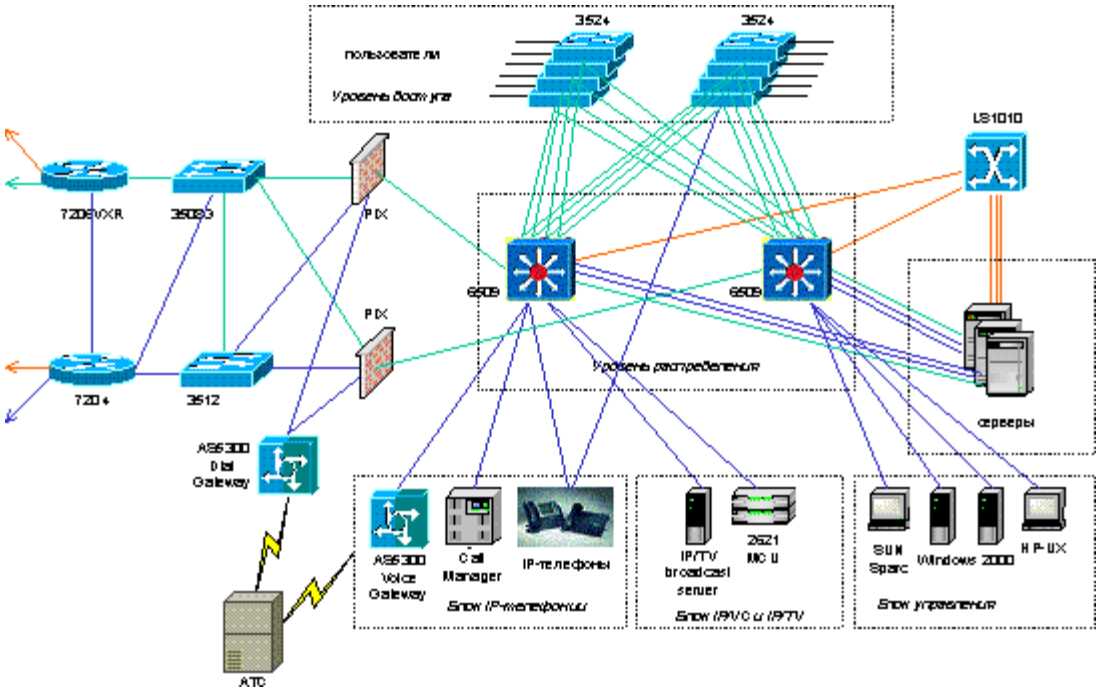

Рис.4. Планируемая конфигурация сети МСЦ

Ядро сети

Ядро сети предлагается построить на базе двух высокопроизводительных многоуровневых коммутаторов Cisco Catalyst 6509. Пропускная способность шины этих коммутаторов составляет 256 Гбит/с, а скорость коммутации достигает 150 миллионов пакетов в секунду. Коммутаторы будут оборудованы картами маршрутизации в комбинации с модулем управления, что позволит им работать в режиме коммутации третьего уровня (маршрутизации).

Эти коммутаторы будут выполнять задачи высокоскоростной коммутации фреймов Ethernet, маршрутизации пакетов между виртуальными подсетями (VLAN), объединения ATM и Ethernet сетей (LANE) и обеспечения качества сервиса для приложений.

Коммутаторы подключены таким образом, что в случае выхода из строя любого из них, оставшийся автоматически берет на себя выполнение всех функций неисправного коммутатора. Это позволяет обеспечить непрерывное функционирование ядра сети.

Доступ абонентов

Внутренние абоненты должны подключаться к коммутаторам уровня доступа Cisco Catalyst 3524. Каждый такой коммутатор обеспечивает 24 порта Ethernet 10/100Мбит/сек. и 2 порта Gigabit Ethernet.

Для обеспечения бесперебойной работы сети каждый из коммутаторов доступа соединяется с каждым из коммутаторов ядра каналами Gigabit Ethernet. В случае обрыва любого из каналов связи или выхода из строя одного из коммутаторов ядра сети связь Catalyst 3524 с ядром будет осуществляться по резервному каналу.

На уровне доступа не будет осуществляться никакой маршрутизации. Главными задачами

коммутаторов доступа являются: коммутация фреймов и поддержание независимости виртуальных подсетей (VLAN) друг от друга.

Подключение серверов

Подключение каждого сервера будет осуществляться как минимум по двум каналам, что позволит обеспечить большую надежность связи. Для обеспечения связности сети при выходе одного из каналов из строя предполагается использовать протоколы динамической маршрутизации.

Одним из каналов будет канал существующей ATM-сети, другим - канал FastEthernet или GigabitEthernet для высоко загруженных каналов.

Каналы Fast и Gigabit Ethernet от серверов подключаются непосредственно к коммутаторам ядра сети, каналы ATM OC-3c 155Мбит/сек подключаются к LightStream 1010, который в свою очередь подключается каналами ATM OC-12c 622Мбит/сек к коммутаторам ядра сети.

Удаленный доступ к ресурсам МСЦ

Удаленный доступ к ресурсам МСЦ возможен двумя способами: через маршрутизаторы доступа из внешних сетей и по коммутируемым каналам связи (Dial-Up).

Оба этих пути планируется контролировать устройствами защиты информации Cisco PIX Firewall. Эти брандмауэры сертифицированы ГТК при президенте РФ по третьему классу защиты и позволяют значительно снизить риск несанкционированного доступа.

Доступ из внешних сетей

Доступ из внешних сетей будет осуществляться через два маршрутизатора доступа. Одним из маршрутизаторов будет используемый в настоящее время Cisco 7204, другим – Cisco 7206VXR, обладающий достаточной производительностью для обслуживания подключения через гигабитный канал к строящейся сети РАН. Данные маршрутизаторы обладают достаточными возможностями для проведения первичной обработки информации и благодаря этому могут использоваться вместе с PIX Firewall для обеспечения защиты информации.

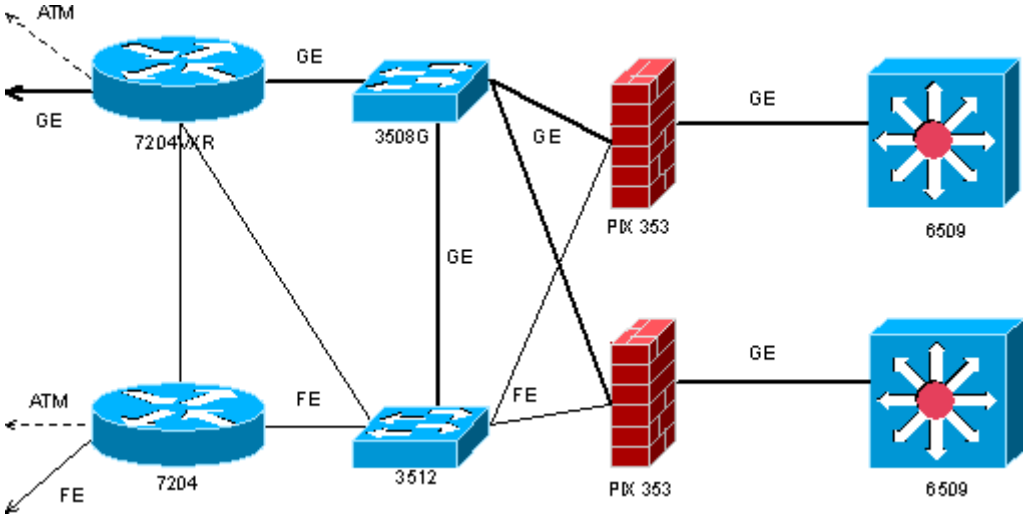

Рис.5. Доступ из внешних сетей в ЛВС МСЦ

В отличие от ядра сети, данная система не является симметричной. Тем не менее, она является достаточно отказоустойчивой по отношению к отказу маршрутизаторов/коммутаторов или разрыву внутренних каналов, хотя при этом и не гарантируется сохранение исходной пропускной способности.

Dial-Up доступ

Для обеспечения удаленного доступа по коммутируемым каналам планируется установить специализированный сервер доступа Cisco AS5300 с 60 модемами. Cisco AS5300 должен подключиться к АТС двумя каналами E1 PRI и каналами Fast Ethernet к Cisco PIX Firewall.

Для обеспечения авторизации и тарификации будет использован сервер авторизации Cisco Secure, взаимодействующий с AS5300 по протоколу TACACS+.

Подсистема видеоконференций и передачи видеоинформации

Данная подсистема предназначена для организации видеоконференций, презентаций, визуализации информации и других приложений, работающих с видеоинформацией. Эта система, реализованная на базе продуктов Cisco IP/VC и Cisco IP/TV, должна заменить эксплуатируемую в центре экспериментальную систему видеоконференций на базе сервера под управлением Windows.

Подсистема IP телефонии

Рассматривается вопрос внедрения подсистемы IP телефонии, предназначенной для обеспечения телефонной связью абонентов ЛВС, для связи с внешними сетями IP и традиционной телефонии.

Подсистема будет включать в себя IP телефоны, модули для коммутаторов Catalyst 6509, и коммутаторов Catalyst 3524 с возможностью подключения IP телефонов, шлюз в сеть традиционной телефонии и программное обеспечение для маршрутизации голосового трафика.

Система управления сетью

Управление сетевыми устройствами

Управление вычислительными ресурсами Центра в основном осуществляет пакет HP OpenView, а сетью составляющая OpenView, NNM (Network Node Manager). Управление сетевыми устройствами планируется выполнять с помощью пакета CiscoWorks и интегрировать его в OpenView.

Рис.6. Структура пакета CiscoWorks.

Этот пакет программных средств управления является основой создаваемой системы управления, позволяет выполнять все базовые задачи по администрированию локальных и глобальных сетей и может интегрироваться в существующую систему управления информационными ресурсами предприятия.

В соответствии с моделью OSI выделяются пять базовых функций управления сетью.

1. **Управление конфигурацией сети** - включает в себя регистрацию устройств, работающих в сети, их месторасположение, сетевые адреса и идентификаторы, поддержание логической схемы сети.

2. **Управление ошибками** - это выявление, определение и разрешение проблем в работе сети. Эти проблемы могут вызываться отказами оборудования или отклонениями от заданных характеристик, различных аппаратных и программных компонентов сети.

3. **Управление производительностью** - подразумевает оценку на основе накопленной статистической информации производительности системы в целом и ее отдельных частей. Данная оценка позволяет выявлять узкие места в сети и предотвращать их появление.

4. **Управление безопасностью** - включает в себя контроль и разграничение доступа, сохранение целостности данных. В функции данной компоненты управления входят: процедура авторизации доступа к сетевым ресурсам, проверка и управление полномочиями, поддержка ключей шифрования, управление паролями, управление внешним доступом и межсетевым взаимодействием.

5. **Учет работы сетевых устройств** - регистрация использования ресурсов и устройств сети.

Все эти базовые функции выполняются пакетом CiscoWorks. Кроме того, существует ряд

специализированных приложений, интегрируемых с этой системой, в частности Cisco Voice Manager, который будет использован для управления передачей голосовой информации по сети.

Система управлением доступом абонентов

Система управления доступом абонентов должна решать следующие основные задачи:

- обеспечение фильтрации входящего трафика;
- обеспечение надежной системы авторизации;
- обеспечение активного отслеживания попыток несанкционированных действий в сети.

Для авторизации доступа планируется установка комплекса программного обеспечения (ПО) Cisco Secure. Это ПО взаимодействует с серверами доступа, брандмауэрами и другими устройствами, обеспечивающими авторизацию абонентов, по протоколам TACACS+ и RADIUS. Все запросы на авторизацию передаются в сервер Cisco Secure, который принимает решение об авторизации на основе анализа множества параметров абонента. Таким образом, будет обеспечен централизованный контроль доступа ко всем ресурсам МСЦ.

Система управления регистрацией и IP адресацией внутренних абонентов сети

Для регистрации внутренних абонентов и динамической раздачи IP адресов предусмотрено использование продукта Cisco Network Registrar (CNR). Этот продукт предоставляет интегрированные сервисы Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP), DHCP Safe Failover Protocol, управление адресным пространством IP для обеспечения сервисов по идентификации, авторизации и регистрации пользователей, упрощения и сокращения затрат на перемещения и добавления устройств.

Система управления качеством обслуживания

В качестве системы управления качеством обслуживания, предназначенной для обеспечения приоритезации трафика и преимущественного доступа к сетевым ресурсам соответствующих приложений, предлагается использовать ПО Cisco QoS Policy Manager. Это ПО обеспечивает централизованное управление всеми устройствами сети, позволяя, таким образом, быстро настраивать всю сеть на приоритетную работу выбранных приложений, а также контролировать работу механизмов QoS всей сети.

Система управления защитой информации

Помимо контроля доступа планируется также применение активных средств защиты информации, в частности системы обнаружения несанкционированного доступа Cisco Secure Intrusion Detection System. Система Cisco Secure IDS состоит из двух компонентов – Cisco Secure IDS Sensor и Cisco Secure IDS Director. Устройства Cisco Secure IDS Sensor являются высокоскоростными сетевыми детекторами устанавливаемыми в ключевых точках сети. Они анализируют содержание и контекст проходящих пакетов с целью обнаружения попыток хакерских атак. При обнаружении признаков атаки, система выполняет запрограммированную администратором последовательность действий. Например, блокирует или завершает соединение, или блокирует узел-источник атаки, или информирует администратора.

Таким образом, можно создать гибкую систему безопасности, позволяющую немедленно реагировать на подозрительную активность и блокировать хакерские атаки, не нанося ущерба функционированию всей сети.

Обеспечение бесперебойной работы сети

Резервирование на уровне ядра сети

Как уже упоминалось выше, ядро модернизированной сети будет состоять из двух коммутаторов 3-го уровня Catalyst 6509. Топология сети обеспечивает в случае поломки полную передачу всех функций неисправного коммутатора к работающему устройству. Сами коммутаторы Catalyst 6509 представляют собой очень надежные устройства. Надежность коммутаторов обеспечивается резервированием блоков питания и процессорных модулей, а также пассивной шиной.

Для обеспечения бесперебойной маршрутизации между виртуальными подсетями (VLAN) используется Hot Standby Routing Protocol (HSRP), который позволяет в случае поломки одного из маршрутизаторов мгновенно переключиться на резервный.

Резервирование уровня доступа абонентов

Каждый коммутатор доступа будет подключен к двум разным коммутаторам ядра ЛВС по каналам Gigabit Ethernet. В случае сбоя в одном из каналов или отключения одного из коммутаторов ядра связь с ядром сети не пропадает.

Отключение абонента от сети возможно только в случае поломки ближайшего к нему коммутатора доступа. Однако при этом отключатся не более 24-х абонентов, вся остальная сеть не пострадает. Кроме того, предусматривается наличие резервных коммутаторов, что позволяет сократить время вынужденного простоя абонентов до минимума, требующегося на подключение резервного коммутатора.

Резервирование доступа к серверам

Резервирование доступа к серверам уже было описано выше. Сетевое оборудование Cisco, которое планируется использовать в сети, позволяет обеспечить и балансирование нагрузки на двух разных каналах доступа, и использование одного из каналов в режиме горячего резерва. Однако программное обеспечение большинства серверов не позволяет воспользоваться этой возможностью и вынуждает использовать динамическую маршрутизацию с запуском на каждом сервере соответствующего демона.

Обеспечение защиты информации

Система защиты информации теснейшим образом связана с системой управления сетью и в значительной мере уже была рассмотрена выше. Правильно выстроенная система управления позволяет оперативно реагировать на сигналы от оборудования и программных агентов и препятствовать попыткам несанкционированных действий. Но помимо системы управления имеются и аппаратные средства обеспечения защиты информации.

Защита информации от НСД из внешних сетей

Основным элементом технических средств защиты от НСД из внешних сетей являются

брандмауэры, которые обеспечивает фильтрацию IP пакетов по заданным правилам. С их помощью можно защищаться от попыток получения доступа к закрытой информации и определять источник атак во внешних сетях. С их же помощью можно проводить политику по ограничению возможности доступа к различным внешним сервисам со стороны соответствующих групп абонентов сети МСЦ.

Сеть МСЦ делится брандмауэрами на несколько сегментов:

- Внутренняя сеть,
- Внешний сегмент,
- «Демилитаризованная зона» (ДМЗ)

ДМЗ предназначена для размещения сервисов, к которым необходимо предоставлять доступ извне. Обычно в ДМЗ размещают сервера WWW, электронной почты, DNS и т.п. Благодаря этому, внешние абоненты не получают непосредственного доступа во внутреннюю сеть. Сами сервера в ДМЗ могут получать информацию из внутренней сети, но ограничены в ее изменении. Например, WWW сервер может получать информацию из внутренних баз данных. Такая организация взаимодействия позволяет внешним абонентам использовать ресурсы МСЦ, но не иметь при этом доступа во внутреннюю сеть. При этом сервера в ДМЗ играют роль посредников.

Весь обмен трафиком между всеми созданными сегментами обязательно проходит через брандмауэры, которые анализируют трафик на предмет обнаружения попыток атак и следят за выполнением установленных для информационных потоков правил.

ПО системы управления позволяет скоординировать работу брандмауэров с настройкой остальных сетевых устройств, задействованных в обеспечении защиты информации. К таким устройствам относятся: внешний маршрутизатор, коммутаторы ядра и уровня доступа.

Разграничение информационных потоков во внутренней сети

Для обеспечения безопасности информации информационные потоки различных подразделений МСЦ разделяются. Это организовано посредством использования технологии виртуальных подсетей (VLAN). Каждое подразделение имеет собственный VLAN, а обмен информацией между ними будет возможен только через коммутатор 3-го уровня в ядре сети.

Таким образом, весь обмен информацией между различными отделами осуществляется в одной точке, в которой настраиваются соответствующие правила обмена информацией между VLAN и производится постоянный мониторинг трафика с целью отслеживания попыток несанкционированных действий. Мониторинг будет осуществляться модулем Intrusion Detection System в коммутаторе ядра сети.

Этапы строительства сети

Первый этап

Первый этап строительства призван создать законченную и полностью работоспособную сетевую инфраструктуру передачи данных. Он заключается в установке двух коммутаторов 3-го

уровня для ядра сети, коммутаторы доступа для подключения абонентов, маршрутизатора Cisco 7206VXR и промежуточных коммутаторов Cisco Catalyst 3208G и Catalyst 3212.

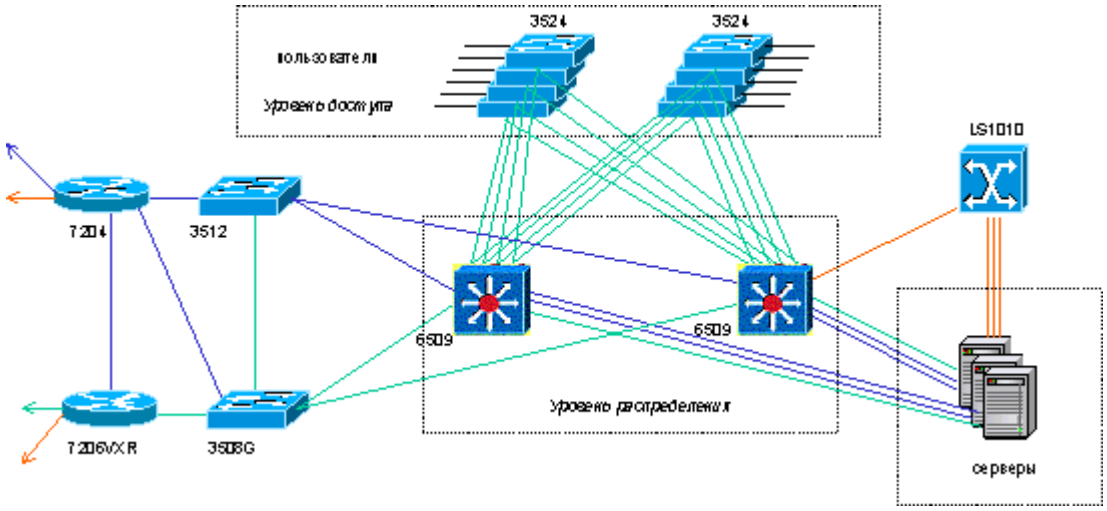

Рис.7. Структура сети МСЦ по завершению первого этапа.

Дальнейшее строительство

Законченная сетевая инфраструктура будет создана в рамках следующих этапов строительства, при этом предполагается следующая последовательность действий.

После выполнения первого этапа следующими обязательными шагами должны стать завершение строительства системы резервной связи с серверами через сеть ATM и внедрение системы управления ЛВС. Иначе невозможно будет обеспечивать бесперебойное функционирование сети, отслеживать возникновение узких мест и прогнозировать развитие системы.

Следующим шагом необходимо будет настроить систему защиты информации и удаленного доступа к ресурсам МСЦ. Данный этап включает в себя развертывание как программных, так и аппаратных средств защиты. Результатом выполнения данного этапа должна стать система защиты данных как от несанкционированного доступа извне, так и от некорректных действий внутренних абонентов.

После внедрения системы безопасности необходимо будет установить систему управления качеством сервиса для приложений. Установка данной системы является необходимым условием для полномасштабного развертывания приложений передачи видео- и аудиоинформации.

Следующими этапами внедряются подсистемы видеоконференций и передачи видеоинформации и подсистемы IP телефонии.

Таким образом, предполагается следующая последовательность шагов:

1. Резервирование связи с серверами через ATM сеть и инсталляция системы управления ЛВС,

2. Инсталляция и настройка систем защиты информации и удаленного доступа,

3. Инсталляция и настройка системы управления качеством сервиса,

4. Развертывание систем передачи видеоинформации и IP телефонии.

Заключение

В настоящее время быстрое развитие современных сетевых технологий требует постоянного их отслеживания и учета возможностей. Новые технологии появляются, когда проект уже написан и начинает осуществляться. Технологии, которые кажутся перспективными на стадии подготовки проекта, могут оказаться не самым эффективным или не самыми удачными с точки зрения их стоимости. Многое удается исправить на стадии реализации, однако идеал часто остается недостижим. Накопленный центром опыт показывает, что идея, ядро проекта должна базироваться на самых передовых технологиях и должна иметь значительный запас для возможности маневра. Практика показывает, что локальная сеть любого предприятия подвергается постоянной модернизации и улучшению. Сеть всегда в движении как живой организм. Прекрати движение –и сеть из невидимого помощника, связующей нити, превратиться в тормоз, останавливающий все развитие предприятия.

Описанный проект не претендует на то, чтобы считаться идеальным, и достаточно часто обновляется. Однако он воплощает достаточно специфичный опыт, выработанный в уникальном в России своим масштабом суперкомпьютерном центре.

Литература

1. О.С. Аладышев, А.А. Мохнатюк, Б.М. Шабанов. Локальная сеть вычислительного комплекса.

2. Julia H. Allen. The CERT® Guide to System and Network Security Practices, Addison-Wesley, USA, 2001

3. Matthew Birkner. Cisco Internetwork Design. Cisco Press, 1999

4. Building Cisco Remote Access Networks. Edited by Catherine Paquet. CiscoPress, USA, 1999.

5. Earl Carter. □ Cisco Secure Intrusion Detection System. Cisco Press, USA, 2001

6. David Chapman, Andy Fox. Cisco® Secure PIX® Firewalls, Cisco Press, USA, 2001

7. CIM Voice Internetworking, VoIP Quality of Service. Cisco Press, USA, 2001

8. Merike Kaeo. Designing Network Security. Cisco Press, USA, 1999

9. Scott Keagy. Integrating Voice and Data Networks. Cisco Press, USA, 2000

10. Donald Lee, Enhanced IP Services for Cisco Networks, Cisco Press, 1999

11. Thomas A. Limoncelli and Christine Hogan. The Practice of System and Network Administration. Addison-Wesley, USA, 2002

12. Managing Cisco Network Security. Cisco Press, USA, 2001

13. Andrew Mason. Cisco® Secure Virtual Private Networks. Cisco Press, USA, 2001

14. Mark Newcomb, Andrew Mason. Cisco Secure Internet Security Solutions. Cisco Press, USA, 2001

15. Chris Oggerino. High Availability Network Fundamentals. Cisco Press, USA, 2001

16. Priscilla Oppenheimer. Top-Down Network Design. Cisco Press, USA, 1998

17. Radia Perlman. Interconnections: Bridges & Routers. Addison-Wesley, USA, 1992

18. Galina Pildush, Cisco ATM Solutions, Cisco Press, USA, 2000

19. Diane Teare. Designing Cisco Networks. Cisco Press, USA 1999

20. Srinivas Vegesna. IP Quality of Service. Cisco Press, USA, 2001

21. Karen Webb. Building Cisco Multilayer Switched Networks. Cisco Press. 2000.

22. Michael Wynstone. Cisco Enterprise Management Solutions, Volume I, Cisco Prwess, USA, 2001

Шабанов Борис Михайлович. Родился в 1954году. Окончил Московский энергетический институт в 1977 году. Кандидат технических наук. Область научных интересов: высокопроизводительные вычислительные системы. Автор более 20 научных работ. Заместитель директора ГУ Межведомственный суперкомпьютерный центр.

Овсянников Алексей Павлович. Родился в 1962 году. Окончил Московский физико-технический институт в 1985 году. Область научных интересов: телекоммуникации. Заведующий лабораторией ГУ Межведомственного суперкомпьютерного центра.

Аладышев Олег Сергеевич. Родился в 1970 году. Окончил факультет вычислительной математики и кибернетики Московский государственный университет имени М.В. Ломоносова. В 1992 году. Область научных интересов: проектирование, мониторинг и администрирование вычислительных и телекоммуникационных систем. Заведующий лабораторией Межведомственного суперкомпьютерного центра.