

Начинающему СІО

Построение ЛВС центрального офиса

Леонид КОЛПАЧЕВ,
руководитель отдела проектной
поддержки партнеров, CompTek

В последнее время получило распространение мнение, что построение ЛВС – дело простое. Действительно, совсем нетрудно найти в Интернете или в специализированных журналах типовую схему сети, которая, по сути, отражает структуру кабельной системы. А дальше в прайс-листах производителей достаточно выбрать коммутаторы подешевле, лишь бы они имели необходимое число портов 10/100 Ethernet, Gigabit или даже 10-Gigabit Ethernet, и все – дело в шляпе.

Хотим предостеречь читателей от подобного подхода. Нельзя упрощенно рассматривать сеть только как систему «перевоски» данных, самая главная, первичная задача сети – обеспечение должной работы приложений, которые, в свою очередь, обеспечивают поддержку бизнес-процессов. Именно эта задача определяет функциональное наполнение сети, на которое и следует обратить внимание в первую очередь. При этом идеальный вариант – чтобы сеть работала абсолютно «прозрачно» и сотрудники вообще забыли о ее существовании. Приложения работают как надо, и это самое главное.

Основные функциональные характеристики современных сетей можно свести в четыре ключевые группы:

- производительность;
- надежность;

В серии статей «Начинающему СІО» будут рассмотрены вопросы, связанные с построением и эксплуатацией относительно небольшой корпоративной сети (до 500 рабочих мест). Мы начнем с вопроса организации ЛВС центрального офиса и поговорим о телефонии, подключении филиалов и удаленных пользователей, обеспечении безопасности, внедрении беспроводных решений и т. д. Эти статьи предназначены для людей, которые отвечают за развитие информационных технологий на своих предприятиях. Прочитав статьи, они смогут больше узнать о возможностях, заложенных в современных сетевых технологиях.

- безопасность;
- управляемость.

Производительность

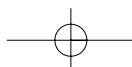
Когда мы говорим о производительности, то имеем в виду не столько битовую скорость интерфейсов, сколько должную производительность работы приложений. Для одних приложений самое важное – скорость отклика сервера, для других – качество речевого сигнала (телефония), для третьих – разрешение картинки (видеоконференцсвязь или ТВ-вещание). От того, какие приложения будут работать по сети, во многом зависят принципы ее построения и необходимая функциональность сетевых устройств. Можно сделать производительность гарантированно большой (например, закупив коммутаторы с 10-гигабитными портами), но это стоит больших денег и далеко не всегда является оптимальным решением. Есть и другие способы, которые помогут вам обеспечить необходимую работу приложения, не вкладывая огромные суммы в гигабиты или даже терабиты пропускной способности.

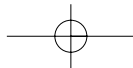
Наиболее известный и эффективный способ обеспечения

должной производительности – использование механизмов QoS. Однако часто считают, что механизмы QoS нужны только для телефонии. Но даже если нет телефонии, в сети всегда есть критичные и второстепенные приложения. Механизмы QoS способны обеспечить критичным приложениям гарантированную полосу пропускания в сети независимо от ее состояния. И сотрудники будут получать адекватный отклик системы.

Положительное влияние на производительность информационной системы в целом могут также оказывать технологии, которые изначально или напрямую не предназначены для решения именно этой проблемы. Одна из них – технология виртуальных ЛВС (VLAN). Существует мнение, что VLAN – это некая абстрактная модель для отображения административной структуры предприятия на сетевую топологию. На самом деле строить VLAN в соответствии со структурой компании – занятие малопродуктивное. VLAN – это в первую очередь эффективный механизм повышения производительности, надежности и безопасности сети.

Сетевые приложения и сервисы генерируют много широковещательного трафика, что приводит к





Красноярский край

щательного трафика, который снижает производительность сети в целом. Такой трафик не только перегружает каналы и коммутаторы, но и «заставляет отвлекаться» все конечные устройства, подключенные к сети. Как ограничить прохождение ненужного широковещательного трафика? Наиболее действенный способ – разбиением сети на L2-домены, т. е. на VLAN.

В корпоративных сетях довольно много и многоадресного (группового) трафика. Сетевые устройства должны поддерживать механизмы обработки такого трафика, в частности отслеживать запросы протокола IGMP. Если таких механизмов нет, то многоадресный трафик становится широковещательным со всеми негативными последствиями для работы сети.

Виртуальные ЛВС не являются абсолютно замкнутыми, трафик между ними, конечно, должен «ходить». Для обеспечения связности используют маршрутизи-

рующие коммутаторы (L3), которые гарантируют высокоскоростную, надежную и безопасную пересылку трафика между VLAN-сетями. Это очень важное устройство, поскольку через него проходит львиная доля трафика, поэтому, как правило, его дублируют.

Эти устройства должны не только обеспечивать маршрутизацию сетевого трафика, но они также должны обладать дополнительным интеллектом, который бы позволил корректно организовать такие востребованные в корпоративной сети сервисы, как DHCP, WINS и другие. Примером такого интеллекта может служить DHCP relay agent в устройствах компании Cisco Systems.

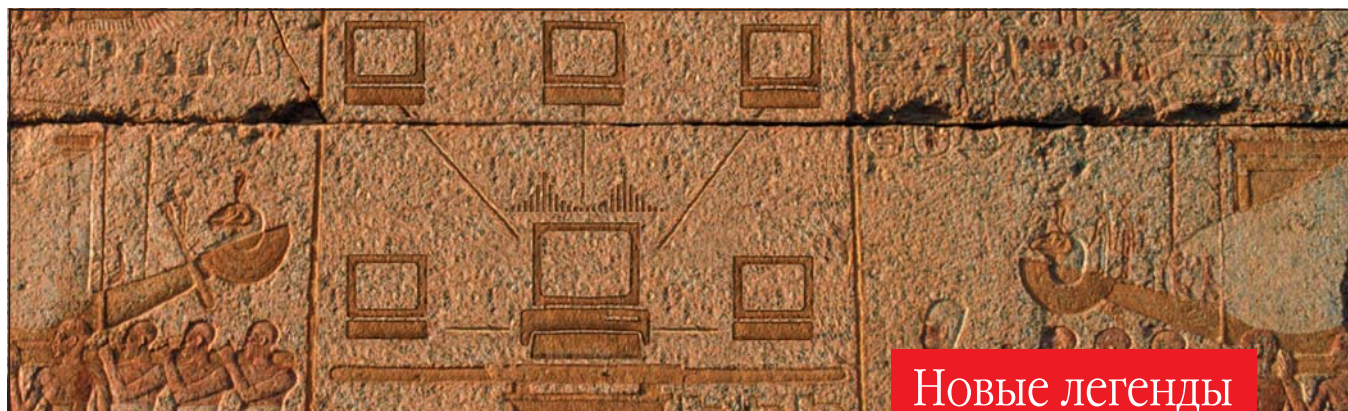
Выбор протокола маршрутизации также достаточно важен. Так, например, если для простых небольших сетей может подойти RIP v.2, то для более сложных инфраструктур требуется протокол с меньшим временем сходимости, например OSPF. Однако до-

статочно часто оптимальным вариантом является применение EIGRP – фирменного протокола компании Cisco Systems.

Производительность, надежность, безопасность и управляемость – вещи очень связанные и во многом взаимозависимые. Приведем в качестве примера «побочный эффект» от применения механизмов QoS. Используя знания обо всех приложениях в сети, мы можем классифицировать весь полезный и служебный трафик, а оставшийся трафик загнать в «мусорный класс» с жестким ограничением по полосе пропускания. В этом случае заражение одного или нескольких хостов в сети неизвестным червем или вирусом не породит большой рост паразитного трафика, что сохранит ее работоспособность.

Надежность

Надежность функционирования сетевой инфраструктуры скла-



Новые легенды
века «железа»

Дистрибуция – это наш бизнес. Профессионализм, проверенный временем.

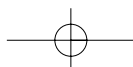
Что такое Value Add Distributor? Это – быстрые прямые поставки; собственный склад; развитая служба техподдержки, работающая в режиме 24x7; лаборатория компетенции, тестирования и проектирования; он-лайн конференции и доступ к складу; информационная поддержка.

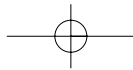
CompTek – Value Add Distributor оборудования и решений Cisco Systems, из года в год обеспечивающий своим партнерам лучшие условия поставки и поддержки. Стратегия CompTek – создание благоприятной атмосферы для развития партнерами своего бизнеса.

COMP **TEK**

142784, МО, Ленинский р-н,
"Бизнес-парк "Румянцево", стр. 1, подъезд 5, этаж 8
Тел. (495) 785-2525, Факс (495) 785-2526
www.comptek.ru. e-mail: sales@comptek.ru


CISCO





дывается из двух основных составляющих: это средства повышения надежности сетевых узлов (резервирование различных подсистем коммутаторов/маршрутизаторов, «горячая» замена их плат и т. п.) и алгоритмы резервирования и восстановления связи между сетевыми узлами. Как известно, классические сети Ethernet основаны на протоколе остоного дерева (STP), который обеспечивает переключение на резервные маршруты (в случае аварии), но делает это медленно – его время сходимости составляет от 30 до 60 с. Для снижения этого времени был разработан протокол остоного дерева с ускоренной сходимостью (Rapid STP – RSTP), который стандартизирован институтом IEEE в документе 802.1w.

Компания Cisco разработала ряд дополнений к STP, в частности протокол Flexlink, который обеспечивает время сходимости менее 50 мс. Здесь же следует упомянуть механизм PVST+/PVRST+ (Per-VLAN Spanning Tree Plus/ Per-VLAN Rapid Spanning Tree Plus), служащий для балансировки нагрузки между двумя дублирующими линками. При его использовании производительность сети повышается, поскольку задействуется канал, который в обычном случае был бы заблокирован средствами STP. Конечно же, устройства Cisco Systems поддерживают и стандартный чуть более громоздкий протокол MSTP (IEEE 802.1s).

Как видите, отказоустойчивость и производительность «идут» бок о бок. Еще один пример – технология EtherChannel, позволяющая объединять каналы между сетевыми устройствами в группы с увеличенной пропускной способностью. Скажем, если между коммутаторами имеется четыре канала Gigabit Ethernet, они могут быть объединены в единый канал со скоростью 4 Гбит/с. В случае аварии на одном из каналов группы, трафик будет перераспределен между другими. Таким образом, мы получаем отказоустойчивость с нулевым временем сходимости. Для автоматизи-

зации процесса создания подобных транков компания Cisco разработала протокол PAgP (Port Aggregation Protocol), который появился на свет значительно раньше стандарта LACP (802.3ad). Нам кажется излишним упоминать, что этот стандарт также поддерживается коммутаторами и маршрутизаторами Cisco Systems.

Управляемость

В современной корпоративной сети не должно быть неуправляемых устройств. Это аксиома. Причем управление должно быть максимально наглядным. Чтобы не тратить огромные деньги на зарплату технического гуру, который умеет на полуптичьем языке командной строки конфигурировать маршрутизатор, необходимы визуализированные графические интерфейсы управления, пользоваться которыми может и «рядовой» системный администратор. И дело здесь не только в экономии на зарплате; удобные графические системы управления позволяют тратить меньше времени на конфигурацию устройств и снижают вероятность человеческих ошибок, следовательно, повышают надежность сети.

Классическая система управления строится по схеме «клиент-сервер». Это значит, что есть централизованная станция управления, которое по определенному протоколу опрашивает сетевые устройства. Трафик управления должен быть защищен шифрованием, как это сделано, например, в протоколе SNMP версии 3.

В последнее время приобретают все большую популярность средства управления на основе веб-технологий: в сетевое устройство встраивается веб-сервер, доступ к которому возможен с обычного браузера. Такой подход имеет свои преимущества, однако он не оставляет единой картины сети. Поэтому когда в сети много устройств, лучше использовать классические системы сетевого управления.

Желательно трафик управления отделить от общего трафика.

И здесь мы опять приходим к технологии VLAN. Выделение для трафика управления отдельной VLAN гарантирует предсказуемую работу системы управления, а значит, удобство обслуживания сети, снижение времени на выявление, локализацию и устранение неисправностей.

Реализация

Выше мы рассмотрели лишь основные моменты, важные для поддержания высокого уровня производительности, надежности и управляемости сети (теме безопасности будет посвящена отдельная статья). Безусловно, множество важных протоколов и технологий осталось за рамками данной статьи.

Теперь пару слов о выборе производителя. Возможно мы выразим крамольную мысль, но на наш взгляд, моновендорность в корпоративной сети имеет большее количество плюсов, чем минусов, которые в конечном итоге выливаются в повышение надежности, производительности, управляемости и даже безопасности, при снижении затрат на эксплуатацию.

Выше уже упоминались некоторые отличительные характеристики сетевого оборудования Cisco. Назовем еще протоколы VTP и CDP, которые помогают в диагностике и автоматизации механизмов подстройки сети под меняющийся состав оборудования в сети. Кроме того, технические решения Cisco имеют развитые функции обеспечения качества обслуживания и безопасности, гибкие средства управления.

Безусловно, на рынке работают и другие уважаемые производители. Главное, при выборе сетевого оборудования обращать внимание не только на его стоимость, число Ethernet-портов и их скорость, но и на его функциональность. И если вы «проморгаете» какую-то важную функцию, то можете поставить под угрозу бизнес своего предприятия, а значит и свое будущее. Сеть на современном предприятии – это очень серьезно. ■

