Управление и мониторинг корпоративной вычислительной сети вуза

Крюков В.В., Майоров В.С., Шахгельдян К.И.

На физическом уровне корпоративной вычислительной сети (КВС) Владивостокского государственного университета экономики и сервиса (ВГУЭС) используются структурированная кабельная система (СКС). Применяется витая пара категории 5е (для связи этажных коммутаторов с коммутаторами рабочих групп) и оптоволоконные линии связи (магистральные каналы для соединения центрального маршрутизирующего коммутатора с этажными коммутаторами). Каждый магистральный канал выполнен в виде двух физических сегментов из многомодового кабеля. Объединение физических сегментов в магистральных каналах происходит с использованием технологии MultiLink Trunking. Реализация этой технологии компанией Nortel на данный момент является не совсем эффективной с точки зрения распределения нагрузки между физическими сегментами. Разброс в загруженности каналов может достигать 50% (т.е. на одном сегменте агрегированного канала нагрузка может быть меньше чем на другом более чем на 50%), что ведет к снижению производительности сети. Планом развития КВС предусмотрено перейти на более эффективное решение, основанное на переводе магистральных каналов на стандарт Gigabit Ethernet.

В качестве активного сетевого оборудования в корпоративной сети ВГУЭС используется маршрутизирующий коммутатор Nortel Networks Accelar 1100A и коммутаторы второго уровня BayStack 350/450. Использование в корпоративной сети оборудования одного производителя упрощает процесс сопряжения оборудования. Однако даже в этом случае проблемы возникают, так максимально допустимый размер кадра Ethernet (MTU) в Accelar равен 1500 байт, в то время как в этажных коммутаторах MTU равно 1516 байт. Как следствие, на портах Accelar, к которым подключены этажные коммутаторы, появлялись в большом количестве ошибки типа FrameTooLong. Ликвидировать ошибку удалось путем увеличения MTU на Accelar до 1750 байт (используется в Gigabit Ethernet), что обеспечило высокую производительность и безошибое функционирование оборудования.

Подход, используемый при проектировании и внедрении канального и сетевого уровня корпоративной сети ВГУЭС заключается в том, что на канальном уровне модели OSI сеть разбивается на относительно независимые друг от друга сегменты (подсети), а на более высоких уровнях (сетевой) происходит приведение разрозненных сегментов в единую систему.

Разделение корпоративной сети на канальном уровне повышает стабильность функционирования сетевой инфраструктуры в целом. Если возникают проблемы в одном из сегментов сети, то они незначительно влияют на функционирование остальных сегментов. Дополнительным преимуществом разбиения является более быстрая и точная локализация неисправности, в случае ее возникновения. Для создания КВС вуза на канальном уровне используется методология виртуальных сетей (VLAN - IEEE 802.1Q). Виртуальные сети выделяются по нескольким критериям: локализация трафика внутри групп, наиболее интенсивно обменивающихся информацией, безопасность передачи данных по сети. Большое количество виртуальных сетей затрудняет первоначальную регистрацию и администрирование сетью, однако чем больше подсетей, тем КВС является лучше управляемой и надежной. В корпоративной сети ВГУЭС было выделено 16 виртуальных сетей, при этом учитывалось достижение компромисса в плане производительности, управляемости и надежности КВС.

Виртуальные сети организованы с использованием адресов портов, т.е. принадлежность рабочей станции к определенной виртуальной сети определяется тем, к какому порту этажного коммутатора подключен компьютер. Реализация по портам позволяет использовать технологию виртуальных сетей без дополнительных материальных

вложений в сетевую инфраструктуру (по сравнению с реализацией основанной на идентификаторе сетевой карты, когда все рабочие станции должны иметь сетевые адаптеры с поддержкой IEEE 802.1Q). Методика использования адресов портов является более гибкой по сравнению с использованием идентификаторов на уровне протоколов обмена данными и более защищенной по сравнению с организацией VLAN по MAC-адресам (каждому MAC-адресу необходимо сопоставить идентификатор виртуальной сети, к которой он принадлежит). На канальном уровне в сети ВГУЭС используется DHCP-сервер, который раздает сетевые настройки (сетевой уровень OSI) всем узлам корпоративной сети.

При указанной организации канального уровня КВС возможны три проблемы. Первая связана с возможностью подключения к сети не учтенного узла (некорректно настроенная рабочая станция, несанкционированное сетевое устройство). Вторая связана с возможным изменением идентификатора виртуальной сети пользователем самостоятельно (если сетевой адаптер поддерживает стандарт IEEE 802.1Q). Третья – возможность установки и использования неавторизованного DHCP-сервера. Первая проблема может стать причиной ошибочных состояний в рамках виртуальных сегментов КВС и влиять на работоспособность всех узлов сегмента. Для ее ликвидации используется механизм MAC-Security, который блокирует сетевые пакеты с неизвестных MAC-адресов на уровне этажного коммутатора (механизм активизирован на всех этажных коммутаторах). Использование этого механизма также позволяет устранить возможность подмены MAC-адреса на узле, что крайне важно для обеспечения безопасности и конфиденциальности в корпоративной сети. Вторая проблема (самостоятельная установка идентификатора виртуальной сети) вызывает ошибочные состояния только на том узле, на котором произошла установка, на остальные рабочие станции сети эта ошибка не влияет. Для устранения второй проблемы используется механизм отсечения маркированных фреймов (канальный уровень модели OSI) на портах этажных коммутаторов. Третья проблема может вызвать ошибочные состояния для всей КВС. Несмотря на то, что принят целый ряд мер против этой уязвимости, на данный момент удалось лишь частично ликвидировать эту проблему. Во-первых, используется механизм настройки DHCP в ядре корпоративной сети (маршрутизирующий коммутатор Accelar 1100A), в котором сопоставляется номер виртуальной сети и DHCP-сервер. Это позволяет устранить влияние неавторизированного DHCP сервера из одной виртуальной сети на рабочие станции другой виртуальной сети. Во-вторых, используются стандартные средства Active Directory (AD), позволяющие блокировать DHCP-серверы на рабочих станциях, подключенных к доменам AD. Это позволяет полностью ликвидировать проблему в виртуальных сетях, в которых все рабочие станции подключены к домену AD. Есть надежда, что полностью проблема будет снята после ввода распределенной системы мониторинга сети. В системе распределенного мониторинга КВС, которая разрабатывается в данный момент во ВГУЭС, предполагается использовать модуль для мониторинга канального уровня корпоративной сети, которые рассчитан на выявление неавторизированных DHCP-серверов и блокирование их путем задания правил на активном сетевом оборудовании КВС.

К физическому и канальному уровням КВС предъявляются повышенные требования по надежности, т.к. ликвидация ошибок, возникающие на этих уровнях, требует непосредственного участия администратора.

Основными задачами третьего (сетевого) уровня КВС являются объединение разрозненных сегментов сети в единую систему согласно принятой политики администрирования и регламентами доступа к корпоративным ресурсам. Формирование сети как единой информационной среды значительно упрощает работу администраторов, обслуживающих сервисы высокого уровня, а также представляет пользователям более удобные средства доступа к данным, приложениям и сервисам.

Во ВГУЭС каждой виртуальной сети сопоставляется IP-сеть. Путем задания правил устанавливаются маршруты между виртуальными сетями, что позволяет производить обмен данными между определенными виртуальными сетями. В идеальном варианте правила маршрутизации устанавливаются таким образом, чтобы узлы подсетей имели возможность взаимодействия лишь с централизованными корпоративными серверами, но не между собой. Взаимодействие узлов внутри КВС реализованы через корпоративные серверы (файловые серверы, web-серверы, ftp-серверы, серверы приложений, серверы СУБД и т.п.). Однако на практике реализация столь строгой политики объединения приводит к дополнительным неудобствам пользователей и накладывает ограничение на используемое программное обеспечение (невозможно использовать электронные ключи в нескольких виртуальных сетях одновременно). На данный момент для корпоративной сети ВГУЭС актуальным является выделение компьютеров общего пользования (учебные аудитории, библиотека и т.п.) с принятием политики, запрещающей данным узлам взаимодействовать напрямую с рабочими станциями сотрудников и большинством корпоративных серверов. Это обусловлено необходимостью защиты от несанкционированного доступа к корпоративным информационным ресурсам сети. Соответствующие правила реализованы в ядре сети (маршрутизирующий коммутатор Accelar 1100A). Более тонкие настройки, регламентирующие доступ к информационным ресурсам, реализуются с использованием сервисов высокого уровня, таких как: служба LDAP-каталогов (Active Directory), сервер доступа к глобальной сети (proxy-сервер Squid) и т.п.

Сколь бы не была надежно построена сетевая инфраструктура организации, возникновение ошибок в ходе ее функционирования миновать вряд ли удастся. Ошибки могут возникать как из-за некорректной работы пользователей, так и в результате выхода из строя аппаратного обеспечения. В связи с этим актуальным становится вопрос о мониторинге сетевой инфраструктуры организации. Системы мониторинга можно разделить на три типа: системы мониторинга канального и сетевого уровня, системы мониторинга доступности корпоративных сервисов, системы мониторинга производительности различных компонентов сетевой инфраструктуры.

Системы мониторинга канального уровня взаимодействуют непосредственно с активным аппаратным обеспечением, анализируя таблицы MAC-адресов, и в случае возникновения ошибок могут либо в экстренном режиме оповестить администратора, либо сгенерировать управляющие воздействия на активное сетевое оборудование для ликвидации ошибочной ситуации. Программы этого типа могут содержать модули принятия решений, которые позволяют более точно распознать и локализовать место неисправности и тип ошибки, после чего принять решение об управляющем воздействии.

Системы мониторинга доступности корпоративных сервисов предоставляют возможность администратору внести все корпоративные сервисы и указать способ проверки работоспособности этих сервисов. Программа мониторинга будет с заданным администратором интервалом проверять доступность сервисов и в случае возникновения ошибочной ситуации информировать об этом администратора. Как правило, в системах такого типа существует возможность задания зависимостей между сервисами - в случае возникновения ошибочной ситуации генерируется сообщение только от сервиса, на котором произошел сбой, а все зависимые от него сервисы переходят в состояние ожидания. Таким образом, даже в случае большого количества корпоративных сервисов при корректной и точной настройке системы мониторинга система самостоятельно локализует неисправность и выдает информационное сообщение. Для более точной локализации неисправности программы мониторинга распределены по различным сегментам КВС, но управление всеми программами мониторинга и способ хранения данных централизованы.

Система мониторинга производительности узлов КВС периодически собирает статистическую информацию с активного сетевого оборудования и серверов. Основываясь на собранной информации можно выявить узкие места в инфраструктуре.

Все три типа систем мониторинга могут быть реализованы как самостоятельные программы (например, HostMonitor, SNMPc и т.п.), однако большей эффективности можно добиться в случае, когда программы мониторинга реализованы в виде модулей одной системы. Примером такого подхода является программный комплекс IBM Tivoli. В его состав входят модули: IBM Tivoli Switch Analyzer – мониторинг канального уровня сети, IBM Tivoli NetView – мониторинг корпоративных сервисов, IBM Tivoli Enterprise Console – управление потоками сообщений поступающими от других модулей системы, ряд модулей для мониторинга СУБД и т.п. В настоящее время во ВГУЭС ведется работа по созданию программного продукта, обеспечивающего распределенный мониторинг КВС в соответствии с установленными регламентами и правилами доступа к корпоративным информационным ресурсам и сервисам.

Системы мониторинга, как правило, могут выявить и локализовать неисправность в сети, но этого недостаточно. Для экстренной ликвидации неисправностей в корпоративной сети должна быть налажена система удаленного администрирования ресурсов сети. Для удобства администрирования система удаленного управления должна иметь унифицированный интерфейс управления всеми ресурсами корпоративной сети. Т.е. управление любым ресурсом сети должно выполняться с использованием одной системы. На данный момент наиболее удобным решением являться подход, реализуемый корпорацией Microsoft. Ядром системы управления ресурсами является продукт – Microsoft Management Console(MMC). Его основной задачей является предоставление унифицированного интерфейса для администрирования любого сервиса. Управление самими сервисами происходит с использованием дополнительных модулей, которые могут быть разработаны как самой корпорацией Microsoft, так и независимыми поставщиками. Для того чтобы разработать определенный модуль для MMC достаточно реализовать строго определенный интерфейс, с помощью которого консоль взаимодействует с модулем. На данный момент реализованы модули для управления рабочими станциями и серверами под управлением ОС Windows 2000 и выше, модули управления DHCP-, DNS-, WINS-, файловыми серверами (клиентскими сеансами связи, квотами), web-сервером Internet Information Server (IIS), proxy-сервером Internet Security/Acceleration Server (ISA), MS SQL серверами, серверами и доменами Active Directory. Во ВГУЭС помимо стандартных модулей используется модуль управления proxy-сервером Squid (UNIX-платформа), который был разработан в университете и который позволяет регламентировать доступ к ресурсам Интернет (квоты на объем получаемой информации и расписание доступности Интернет) на уровне учетных записей пользователей.

Таким образом, правильно подобранные средства мониторинга и управления сетью способны повысить надежность функционирования корпоративной сети и минимизировать время устранения неполадок. Это в свою очередь улучшает качество предоставляемых сервисов пользователям корпоративной сети.