РАЗВИТИЕ ИНФРАСТРУКТУРЫ КОМПЬЮТЕРНОЙ СЕТИ ВЦ РАН. НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ

И.В. Байкова, Г.М. Михайлов, Ю.П. Рогов, А.М. Чернецов

Проблемы обеспечения надежности работы и безопасности компьютерной сети постоянно находятся под контролем системных администраторов: бесперебойное питание, антивирусная защита, резервирование служб сети и каналов связи и многое другое [1].

Параллельно с вышеперечисленными проблемами решаются вопросы повышения производительности функционирующих систем путем изменения конфигурации сетей и внедрения новых активных элементов и соответствующего программного обеспечения (ПО). Одним из важных составляющих элементов при этом является внедрение технологии агрегирования каналов, которая позволяет объединить несколько физических каналов в один логический. С учетом ввода дополнительных высокоскоростных оптических соединений между узлами связи и сетевыми серверами, а также базируясь на технологии EtherChannel, поддерживаемой платформой Cisco, нам удалось значительно повысить качество функционирования локальной сети, ее защиту, безопасность и производительность.

Рассмотрим более подробно перечисленные выше этапы усовершенствования компьютерной сети ВЦ РАН.

Технология EtherChannel.

Эта технология агрегирования каналов может быть применена как для настройки статических агрегированных каналов, так и для использования протоколов:

- LACP (Link Aggregation Control Protocol) – стандартизированный протокол;
- PAgP (Port Aggregation Protocol) – фирменное решение корпорации Cisco.

В нашем случае мы связываем узлы связи между собой посредством соединения соответствующих стеков коммутаторов Cisco Catalyst. Следует отметить, что PAgP-протокол не может использоваться на межстековых каналах EtherChannel, в то время как LACP-протокол реализует эту поддержку [2]. В настоящее время в нашей схеме используется статическая настройка для объединения несколько физических каналов в один логический. В дальнейшем мы планируем использовать и другие настройки агрегированных каналов для оптимизации пропускной способности линий связи.

При объединении порты Fast Ethernet формируют порт Fast EtherChannel, соответственно объединение гигабитных портов образует порт Gigabit EtherChannel. Рекомендуемая последовательность настройки такова. Сначала создается интерфейс канала - interface PortChannel N - на одном из узлов. Таких интерфейсов может быть несколько. Такой же интерфейс должен быть создан и на узле, который будет соединяться с первым. После этого производится конфигурирование портов, которые будут входить в состав агрегированного канала (каналов).

Можно сначала соответствующим образом сконфигурировать порты, выполнив команду channel-group N mode on, которая создает интерфейс канала N-го порта. Любые команды, которые выполняются на этих интерфейсах после выполнения команды channel-group, автоматически добавляются к интерфейсу канала порта. Если команда channel-group применяется после остальных команд настройки, то интерфейс канала порта создается, не имея при этом необходимой настройки. В таких случаях настройка интерфейса канала порта выполняется вручную.

При создании агрегированного канала необходимо выполнить следующие действия:

- оставить интерфейсы, которые должны использоваться при объединении портов в канал, в состоянии административного выключения;
- создать канал порта (группу каналов) на 1-м стеке коммутаторов; убедиться, что для режима канала задано значение on, например channel-group 1 mode on;
- создать канал порта на 2-м стеке коммутаторов; убедиться, что для режима канала задано значение on;
- снова включить интерфейсы, которые были отключены ранее, на обоих стеках с помощью команды no shut.

Выполненная последовательность действий позволяет избежать проблем с протоколом STP (Spanning Tree Protocol) в процессе настройки. Протокол STP может блокировать некоторые порты в состоянии "отключенный из-за ошибки" (err-disable), если одна сторона настроена как канал до того, как аналогичным образом может быть настроена другая сторона.

Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов [3].

Таким образом, при выходе из строя одного из портов (линков), который входит в состав агрегированного канала, в работу включается второй порт того же канала.

Чтобы проверить канал порта на коммутаторах, можно выполнить команды:

- show interfaces port-channel номер-группы-каналов;
- show etherchannel номер-группы-каналов summary.

Для проверки состояния протокола STP на коммутаторах, необходимо выполнить команду:

- show spanning-tree vlan номер-VLAN detail.

Электронная почта.

Проблемы, связанные с работой электронной почты и описанные в работе [1], в большей степени нами решены. Механизм антиспама работает на всех наших почтовых (MX) серверах.

За счет использования black-листов, ограничений на различные тайм-ауты и количество процессов удалось снизить поток “почтового мусора” в 10 раз (90 %). Мы не стали увеличивать степень фильтрации на этом уровне (серверном), так как при этом оказалось, что потери полезной информации значительны.

Оставшийся спам отфильтровывается на почтовых клиентах пользователя за счет использования антивирусной программы ДоктарВеб (Dr.Web), ее серверной версии “Dr.Web Enterprise Suite и компоненты SpIDer Mail.

В результате использования указанных средств дополнительно отфильтровывается еще 90% от оставшейся части спама с помощью специальной маркировки писем. Среди данных сообщений изредка попадаются полезные. В этом случае они не теряются и могут быть прочитаны пользователем. Таким образом, благодаря этим замечательным средствам мы избавляемся почти от 99% “почтового мусора”, хотя общее количество спама прогрессирует.

Основная масса наших пользователей использует на своих компьютерах антивирусную программу, упомянутую выше, и после соответствующих настроек почтовых клиентских программ этот последний спам легко отсеивается.

Для остальных мы рекомендуем пользоваться другими “антиспам-программами”, либо переходить на наши штатные средства.

Другой удобный способ работы с почтой - это использование web-интерфейса, когда пользователь имеет возможность работать с собственным почтовым ящиком через интернет-браузер, что позволяет избежать процедуры настройки почтовых клиентов, так как все системные настройки доступа через web-интерфейс выполняются администраторами.

В компьютерной сети ВЦ РАН реализован вариант свободно распространяемого web-интерфейса производства (авторства) IlohaMail [4]. Среда написана на PHP 4. Авторами были произведены соответствующие индивидуальные настройки для работы в сети ВЦ РАН. Этот интерфейс находится в опытной эксплуатации.

ЛИТЕРАТУРА:

1. Рогов Ю.П., Чернецов А.М. Аппаратно-программные средства и развитие инфраструктуры ИВС ВЦ РАН (монография), М.: ВЦ РАН, 2010.
2. Михайлов Г.М., Рогов Ю.П., Чернецов А.М. Инфраструктура локальной компьютерной сети академического учреждения и вопросы обеспечения безопасности и защиты информации. Тезисы доклада в трудах Международной суперкомпьютерной конференции "Научный сервис в сети Интернет: суперкомпьютерные центры и задачи" (г. Новороссийск, 20-25 сентября 2010 г.). – М.: МГУ, 2010. С. 98-101.
3. http://ciscosetup.blogspot.com/2009/06/etherchannel-catalyst-3750.html
4. http:// ilohamail.org