АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ В КОРПОРАТИВНОЙ СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Алисеенко М.А.

Цветков В.Ю. – д.т.н., профессор

Сегодня все более популярными становятся видеоконференции с абонентами любой сети, что обеспечивает независимость от городских сетей связи, позволяет повысить эффективность управления компанией, сэкономить время и расходы на командировки. Остро стоит проблема выбора оптимальной системы видеоконференцсвязи, которая обеспечит хорошее качество, надежность и безопасность связи.

Видеоконференцсвязь (ВКС) – это телекоммуникационная технология интерактивного взаимодействия двух и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном времени, с учётом передачи управляющих данных. Для общения в режиме видеоконференции абонент должен иметь терминал ВКС. Для подключения к сети передачи данных используются протоколы IP или ISDN.

Существуют следующие виды систем ВКС:

11) Аппаратные – это системы видеоконференцсвязи, в которых алгоритмы передачи видеосигнала реализуются исключительно на аппаратном уровне с помощью специального оборудования. Это могут быть как видеотелефоны, так и разнообразные групповые ВКС системы, включая системы телеприсутствия. Аппаратная система видеоконференцсвязи базируется на кодеках, средствах отображения видео, средствах воспроизведения и захвата звука, MCU-сервере и дополнительных модулях.

12) Программные – представляют собой программное обеспечение для персональных компьютеров или смартфонов, которые выступают как в роли серверов, так и в роли терминальных устройств видеосвязи. В качестве периферии для захвата и воспроизведения видео и звука могут использоваться, как встроенные в устройство камера, микрофон или динамик, так и внешние устройства [1].

Чтобы выбрать более эффективную систему ВКС, следует прибегнуть к анализу ее входящего и исходящего трафика. Мониторинг и анализ трафика также необходимы для более эффективной диагностики и решения проблем, чтобы не доводить сетевые сервисы до простоя.

Можно выделить следующие методы мониторинга сети:

а) ориентированные на маршрутизаторы;

б) не ориентированные на маршрутизаторы (активные и пассивные);

в) комбинированный метод.

Методы мониторинга, основанные на маршрутизаторе – жёстко заданы (вшиты) в маршрутизаторах и, следовательно, имеют низкую гибкость. SNMP − протокол прикладного уровня, который собирает статистику по трафику до конечного хоста через пассивные датчики, которые реализуются вместе с маршрутизатором. Хотя, SNMP может быть полезным инструментом, но он создаёт возможность для угрозы безопасности, потому что он лишён возможности аутентификации. Расширение RMON включает в себя различные сетевые мониторы и консольные системы для изменения данных, полученных в ходе мониторинга сети и позволяет настраивать сигналы, которые будут мониторить сеть, основанную на определённом критерии. Еще одно расширение – Netflow, которое было представлено в маршрутизаторах Cisco, позволяет собирать IP сетевой трафик, если это задано в интерфейсе. Анализируя данные, которые предоставляются Netflow, сетевой администратор может определить такие вещи как: источник и приёмник трафика, класс сервиса, причины переполненности [2].

Технологии, не встроенные в маршрутизатор всё же ограничены в своих возможностях, они предлагают большую гибкость, чем технологии, встроенные в маршрутизаторы. Эти методы классифицируются как активные и пассивные.

Активный мониторинг сообщает проблемы в сети, собирая измерения между двумя конечными точками. Система активного измерения имеет дело с такими метриками, как: полезность, маршрутизаторы/маршруты, задержка пакетов, повтор пакетов, потери пакетов, неустойчивая синхронизация между прибытием, измерение пропускной способности. Проблема, которая существует с активным мониторингом, – это то, что представленные пробы в сети могут вмешиваться в нормальный трафик.

Пассивный мониторинг не добавляет трафик в сеть и не изменяет трафик, который уже существует в сети. Также в отличии от активного мониторинга, пассивный собирает информацию только об одной точке в сети. Пассивные измерения имеют дело с такой информацией, как: трафик и смесь протоколов, количество битов (битрейт), синхронизация пакетов и время между прибытием. Пассивный мониторинг может быть осуществлён, при помощи любой программы, вытягивающей пакеты. С пассивным мониторингом, измерения могут быть проанализированы только офф-лайн, что создаёт проблему, связанную с обработкой больших наборов данных.

Комбинированные технологии используют лучшие стороны и пассивного, и активного мониторинга сред – это «Просмотр ресурсов на концах сети» (WREN) и «Монитор сети с собственной конфигурацией» (SCNM) [3].

Основными параметрами анализа трафика, для определения эффективности системы ВКС с помощью сетевого анализатора, являются:

– распределение сетевого трафика по ip-адресам и протоколам;

– распределение пропускной способности по ip-адресам и протоколам;

– распределение пиков нагрузки в реальном времени;

– временные параметры узлов.

Сетевой анализатор позволяет выделять из общего потока данных сеансы обмена данными между конечными узлами. Применительно к видеоконференцсвязи возможно выделение конкретного RTP сеанса, для оценки качества и параметров сеанса видеоконференцсвязи. Таким образом, на основе данных о загрузке различных оконечных устройств систем ВКС можно прогнозировать отказ в обслуживании или понижение качества передаваемой мультимедийной информации.

Список использованных источников:

1. Alisha Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques.
2. Амато, В. Основы организации сетей Cisco : учебное издание. В 2 т. / В. Амато. – М. : Вильямс, 2004. – 464 с.
3. M. Uma, G. Padmavathi, An Efficient Network Traffic Monitoring for Wireless Networks.