Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК

Антанович
Антон Александрович

Мониторинг состояния сетевых узлов

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

Научный руководитель

Астровский Иван Иванович
кандидат технических наук, доцент

Минск 2015

ВВЕДЕНИЕ

Мониторинг состояния узлов сети является одной из важнейших задач в управлении сети связи либо сети передачи данных. Ключевыми задачами мониторинга являются : поиск медленных или неисправных подсистем(каналов связи) и информирование администратора либо обслуживающий персонал о аварии на сети передачи данных (далее СПД).

Тенденции развития рынка услуг в области передачи данных требуют от провайдеров услуг постоянно повышать качество предоставляемых услуг на своих сетях. . Так доступность сетей передачи данных для конечного пользователя заставляет все больше внимания уделять надежности .Так же крупные предприятия имеющие развитую инфраструктуру , и даже филиалы по всему миру могут зачастую сопоставить свою сеть по размерам сети небольшого провайдера , это напрямую связано с процессами автоматизации и внедрения информационных технологий во все сферы народного хозяйства. Так же сети передачи данных зачастую не являются статичными и имеют динамичную топологию, что так же предполагает постоянный мониторинг

Классические системы мониторинга обеспечивают непрерывный мониторинг текущего состояния узлов входящих в состав СПД, но в современных условиях все более усложняющихся распределенных систем и жестких требований к их отказоустойчивости и надежности, а так же защищенности и информационной безопасности , к системам мониторинга СПД так же предъявляются требования по обеспечению возможности прогнозирования и диагностики состояния обслуживаемых систем в краткосрочном и долгосрочном периодах. Процесс контроля работы сети обычно делят на два этапа — мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Актуальность данной работы связана с ростом уровня автоматизации , проникновения информационных технологий во все сферы дефтельности человека и значительное повышение требований отказоустойчивости и надежности информационных систем.

Целью данной работы является изучение сетевого анализатора Cisco NAM2304-RJ45-K9, исследование и анализ систем мониторинга состояния сетевых узлов на примере Cisco NAM2304-RJ45-K9.

Задачи исследования:

– Изучить задачи мониторинга сетевых узлов и сети в целом

– Провести анализ существующих протоколов SNMP и NetFlow

– Рассмотреть линейку продуктов Cisco Nam ,особоее внимание уделив объекту исследований Cisco NAM2304-RJ45-K9

– Смоделировать модель реальной сети и провести мониторинг узлов с помощью Cisco NAM2304-RJ45-K9

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Основной целью данной магистерской диссертации работы является исследование и анализ современных систем сетевого мониторинга на примере программно-аппаратного комплекса Cisco NAM 2304.

В первой главе проанализированы задачи мониторинга узлов в современном мире .Рассмотрены основные протоколы используемые для решения этих задач такие как SNMP и NetFlow

Во второй главе рассмотрели как осуществляется анализ активности приложений и их классификация .Показано как это реализуется контрль приложений и узлов с помощью Cisco NAM 2304.Так же рассматривается линейка продуктов Network Analysis Module компании Cisco.

Третья глава посвящена непосредственно объекту исследования Cisco NAM 2304. В ней рассмотрена аппаратная часть, возможности и фунцкионал который предоставляет данный продукт. Смоделирована сеть в которой произведен анализ узлов и сети в целом. Рассмотрена возможность оповещения администратора о настроенных событиях и записи их в журнал.Произведен анализ результатов полученных по технологии SPAN

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Мониторинг сетевых устройств включает в себя сбор системных сообщений, контроль доступности, телеметрию сетевого устройства, а также оповещение инженера об изменениях в сети.

На многих устройствах, в том числе выпускаемых Cisco, в качестве системных служат сообщения syslog. Сбор телеметрических данных производится с использованием протокола SNMP. Для передачи оповещения о происходящих изменениях на сетевом оборудовании должны быть настроены средства рассылки уведомлений. Мониторинг каналов связи организуется по протоколу Netflow или с помощью его аналогов.Для любого сетевого устройства системные сообщения являются главным, а в некоторых случаях и единственно доступным инструментом поиска проблем и неисправностей. Выполняя диагностику сетевой проблемы, сразу после проверки корректности конфигурации инженер должен посмотреть журналы событий сетевых устройств. Вероятность выявления причины при анализе системного журнала крайне велика.

Телеметрическая информация позволяет находить узкие места в сетевой топологии, предотвращать возможные отказы, отслеживать причины возникновения проблем, определять рабочие уровни (baseline) для показателей используемых устройств, выявлять аномалии в функционировании сети.

Среди этих показателей наиболее важными являются загрузка процессора устройства, загрузка оперативной памяти, параметры систем питания и охлаждения, температура устройства. Эти данные рекомендуется отслеживать на любом сетевом устройстве. Кроме того, в зависимости от возложенного функционала рекомендуется включать мониторинг дополнительных параметров.

Cisco Nam 2304 поддерживает SNMPv3 ,который обеспечивает следующие средства защиты :

- целостность сообщения — гарантирует, что в пакет не вмешались в пути
- аутентификация — определение сообщения из допустимого источника.
- шифрование — скремблирование содержания пакета препятствует тому, чтобы он был замечен несанкционированным источником.

Протокол NetFlow разработан компанией Cisco Systems. В контексте задачи управления сетью он является незаменимым инструментом для мониторинга загрузки каналов передачи данных.

Архитектура NetFlow крайне проста и состоит из двух компонентов: сетевого устройства, отправляющего информацию о проходящем через него трафике, и коллектора NetFlow. Последний собирает и анализирует информацию, передаваемую по протоколу NetFlow.

Принцип действия протокола заключается в следующем. При открытии очередного сеанса передачи данных на сетевом оборудовании формируется информация о данном сеансе, называемая поток (flow). Сведения о потоке включают количество передаваемых байтов, входной и выходной интерфейсы для сеанса, IP-адреса отправителя/получателя, порты отправителя/получателя, номер протокола IP, параметры QoS и т. д. Сведения о потоках аккумулируются на сетевом устройстве и отправляются коллектору NetFlow в датаграммах UDP.

Доставка приложений предполагает прохождение трафика через большое количество устройств в сети. При возникновении проблем с работой бизнес-критичных приложений и жалоб на их медленную работу от пользователей довольно трудно определить источник проблемы и “узкое место” в сети. Традиционные средства диагностики (команды ping, traceroute, анализ маршрутных таблиц, состояния интерфейсов устройств и т.д.) не позволяют сетевым администраторам понять, в чём суть проблемы (рисунок Причиной может быть проблема с WAN-каналом, проблема с сервером, проблема с приложением. Причина также может быть и на стороне самого пользователя.

Решение компании Cisco NAM 2304 представляет из себя набор аппаратно-программных инструментов идентификации, мониторинга и контроля работы приложений в сети и позволяют узнать о работающих в сети приложениях, трендах производительности, текущем времени отклика приложений для удаленных пользователей и т.д..

На базе полученной информации появляется возможность интеллектуально приоритезировать, контролировать и перенаправлять трафик бизнес-критичных приложений, что позволяет обеспечить более эффективную работу приложений и улучшить время их отклика для конечных пользователей.

Использование NAM позволяет :

- Дифференцировать критически важные для бизнеса рабочие нагрузки;
- Охарактеризовать производительность приложений и использование сетевых ресурсов;
- Ускорить решение проблем со скоростью доступа к критической сетевой информации;

- Проверить использование механизмов управления и оптимизации и измерение влияния операционных изменений, таких как консолидация сервера, миграция VM и WAN оптимизация;
- Производительность извлечения и аналитика использования, в режиме реального времени используя API REST/XML-based.

Основные функции программного обеспечения Cisco Prime NAM:

- Интерактивные инструментальные панели с разработанными потоками операций, контекстной навигацией, и захватом в один клик
- Всесторонняя статистика трафика, приложений, метрики производительности речи/видео
- Видимость overlay networks , таких как OTV, LISP и VXLAN
- Подробный поиск и устранение неисправностей с проницательными пакетными захватами, усовершенствованными фильтрами и ошибочным сканированием
- централизованное управление с помощью Cisco Prime Infrastructure.

Cisco NAM может собирать статистику с интерфейсов посредствам технологии RMON и анализировать полученные данные:

– Базовая статистика – утилизация канала, пакеты, ошибки, утилизация на основе протоколов и пакетов;
– Статистика хоста включает в себя количество принятых и переданных байт или пакетов на основе MAC адреса на канальном уровне, сетевого адреса на сетевом и прикладном уровне;
– Статистика сессии – количество байт и пакетов, переданных от одного хоста к другому;
– Захват пакетов – RMON может использоваться для захвата пакетов для последующего их анализа;
– Пороги и действия – RMON может учитывать установленные пороги по различным условиям (например, утилизация канала больше чем на 70% в течении 60 секунд) и отправить SNMP трап на систему управления по этому событию.

ЗАКЛЮЧЕНИЕ

В данной работе мы установили следующее :

1. Мониторинг сетевой инфраструктуры. Мониторинг сетевой инфраструктуры можно разбить па следующие составляющие:

– мониторинг сетевых устройств;

– мониторинг каналов передачи данных.

И свою очередь, задача мониторинга сетевых устройств может быть разделена на три подзадачи:

– сбор системных сообщений — журналов устройства;

– мониторинг доступности и телеметрии сетевого устройства;

– оповещение инженера об изменениях в сети.

2. Простой протокол управления сетью (Simple Network Management Protocol, SNMP) является стандартом для обмена управляющей информацией между сетевыми устройствами и системой управления сетью (Network Management System, NMS). С точки зрения мониторинга сети протокол SNMP служит незаменимым средством сбора телеметрической информации с сетевых устройств.

Телеметрическая информация позволяет находить узкие места в сетевой топологии, предотвращать возможные отказы, отслеживать причины возникновения проблем, определять рабочие уровни (baseline) для показателей используемых устройств, выявлять аномалии в функционировании сети.

Nam 2304 поддерживает SNMPv3 ,который обеспечивает следующие средства защиты :

- целостность сообщения — гарантирует, что в пакет не вмешались в пути
- аутентификация — определение сообщения из допустимого источника.
- шифрование — скремблирование содержания пакета препятствует тому, чтобы он был замечен несанкционированным источником.

3. Cisco Nam 2304 эффективно использует протокол NetFlow/Протокол NetFlow разработан компанией Cisco Systems. В контексте задачи управления сетью он является незаменимым инструментом для мониторинга загрузки каналов передачи данных.

Принцип действия протокола заключается в следующем. При открытии очередного сеанса передачи данных на сетевом оборудовании формируется информация о данном сеансе, называемая поток (flow). Сведения о потоке включают количество передаваемых байтов, входной и выходной интерфейсы для сеанса, IP-адреса отправителя/получателя, порты отправителя/получателя, номер протокола IP, параметры QoS и т. д. Сведения о потоках аккумулируются на сетевом устройстве и отправляются коллектору NetFlow в датаграммах UDP.

Коллектор NetFlow агрегирует полученную информацию, проводит анализ и формирует удобные для восприятия отчеты и графики.

4. Интеграция NBAR2 с технологией Flexible Netflow позволяет обеспечить IPv4/v6 мониторинг на уровнях L2-L7 для классифицированных приложений .

В отличие от традиционного Netflow, технология Flexible Netflow позволяет явно указать необходимые для мониторинга ключевые поля кэша потока данных (Netflow-записи) и передавать кэш на несколько различных коллекторов Netflow .

5. Использование NAM позволяет :

- Дифференцировать критически важные для бизнеса рабочие нагрузки;
- Охарактеризовать производительность приложений и использование сетевых ресурсов;
- Ускорить решение проблем со скоростью доступа к критической сетевой информации;
- Проверить использование механизмов управления и оптимизации и измерение влияния операционных изменений, таких как консолидация сервера, миграция VM и WAN оптимизация;
- Производительность извлечения и аналитика использования, в режиме реального времени используя API REST/XML-based.

Основываясь на доводах описанных выше можно твердо сказать что Cisco NAM 2304 является эффективным инструментов для мониторинга и анализа состояния сетевых узлов.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. Доля, Н.А. Захват и анализ сетевого трафика с помощью технологии SPAN на базе сетевого анализатора Cisco NAM 2304 /Н.А. Доля, А.А. Антонович, А.В. Артамонов, О.Ю. Минченко, М.Д.А. Аль-Джебнаве // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. научно-технич. семинара. Минск, апрель–декабрь 2014 г. – Мн.: БГУИР, 2014. – С. 21-25.