

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

УДК 004.77_____

Шантарович
Виталий Дмитриевич

Система контроля состояния компонентов локальной сети

АВТОРЕФЕРАТ

на соискание степени магистра информатики и вычислительной техники
по специальности 1-40 81 02

Научный руководитель
Ганжа Виктор Александрович
канд. физ.-мат. наук, доцент

Минск 2019

Нормоконтроль

Введение

Работа «Система контроля состояния компонентов локальной сети» объемом стр. содержит введение, основную часть, состоящую из двух глав, заключения, приложений, 21 рисунок, 31 источник библиографического списка литературы.

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна.

Протокол SNMP (Simple Network Management Protocol) предназначен для удаленного управления сетевыми элементами: коммутаторами, маршрутизаторами, шлюзами, серверами. Он позволяет сетевым специалистам или автоматизированным системам получать информацию о работе сетевых элементов и изменять их конфигурацию. Протокол позволяет унифицировано управлять оборудованием разных производителей, работающем под различными ОС и на разных уровнях модели OSI.

Общая характеристика работы

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо имеющихся в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критически важна для выполнения сетью своих основных функций.

Распределенный характер крупной сети делает невозможным поддержание ее работы без централизованной системы управления сетью (Network Management System, NMS), призванной в автоматическом режиме контролировать сетевой трафик и управлять коммуникационным оборудованием сети.

Системы управления сетью работают, как правило, в автоматизированном режиме, выполняя наиболее простые действия автоматически и оставляя сложные решения для принятия человеку на основе подготовленной системой информации.

Системы управления сетью представляют собой сложные программно-аппаратные комплексы, поэтому существует граница целесообразности их применения.

В небольшой сети можно применять отдельные программы управления наиболее сложными устройствами, например, коммутатором, поддерживающим технику VLAN. Обычно каждое устройство, которое требует достаточно сложного конфигурирования, производитель сопровождает автономной программой конфигурирования и управления. Однако при росте сети может возникнуть проблема объединения разрозненных программ управления устройствами в единую систему управления, и для решения этой проблемы придется, возможно, отказаться от этих программ и заменить их интегрированной системой управления сетью.

Ставшими классическими системы управления сетями, такие как HP OpenView, Cabletron Spectrum или Zabbix, управляют только коммуникационными объектами корпоративных сетей, такими как маршрутизаторы и коммутаторы.

Краткое содержание работы

SNMP представляет собой протокол семейства TCP / IP (протокол Интернет), и, следовательно, могут быть использованы все типы интернет-сети. Он эксплуатирует возможности UDP транспортного протокола (Рисунок 1).

	Modèle OSI	Modèle TCP/IP (protocole)
7	Application	SNMP
6	Présentation	
5	Session	
4	Transport	UDP
3	Réseau	IP
2	Liaison	Interface réseau
1	Physique	

Рисунок 1 – Инкапсуляция протокола SNMP на протокол TCP / IP

Каждый кадр имеет адрес источника и адрес назначения, который позволит более высокие протоколы уровня, такие как SNMP может адресовать свои запросы.

UDP может использовать дополнительную контрольную сумму покрытия заголовков и кадр данных. В случае ошибки, принятый кадр UDP игнорируется гарантия надежности.

Протокол SNMP обслуживает передачу данных между агентами и станцией, управляющей сетью. SNMP использует дейтаграммный транспортный протокол UDP, не обеспечивающий надежной доставки сообщений.

Применение протокола SNMP определяет достаточно высокий начальный уровень сложности системы управления, так как для его работы необходимо реализовать ряд вспомогательных служб, объектов и баз данных объектов. Уведомления агента SNMP всегда передаются с помощью надежного транспортного протокола и в случае потери будут переданы повторно. Протокол SNMP рассчитан на агентов, которые могут по одной простой команде от менеджера выполнить сложную последовательность действий.

Протокол SNMP существенно лучше масштабируется, так как может воздействовать сразу на несколько объектов, а ответы от агентов проходят через фильтры, которые ограничивают передачу управляющей информации только определенным агентам и менеджерам. Протокол SNMP, который является протоколом взаимодействия между агентами и менеджерами системы управления OSI, позволяет с помощью одной команды воздействовать сразу на группу агентов, применив такие опции, как обзор и фильтрация.

Агенты SNMP выполняют, как правило, более сложные функции, чем агенты SNMP. Из-за этого операции, которые менеджеру можно выполнить над агентом SNMP, носят атомарный характер, что приводит к многочисленным обменам между менеджером и агентом.

Уведомления (traps) агента SNMP посылаются менеджеру без ожидания подтверждения, что может привести к тому, что важные сетевые проблемы останутся незамеченными, так как соответствующее уведомление окажется потерянным, в то время как уведомления агента SNMP всегда передаются с помощью надежного транспортного протокола и в случае потери будут переданы повторно.

Протокол NETCONF определяет механизм управления сетевым устройством путем задания или изменения текущего состояния оборудования. Протокол позволяет реализовать «формальный интерфейс прикладного программирования» (API) устройства. Для представления данных о конфигурации устройства в NETCONF используется язык моделирования данных YANG. В настоящее время многие производители сетевого оборудования (Cisco, Brocade, Juniper) переходят на использование NETCONF в качестве протокола сетевого конфигурирования выпускаемых ими устройств. Немаловажной частью механизма управления любым сетевым устройством является определение способа аутентификации – процедуры проверки подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных пользователей. Когда речь идет об обширных сетях, доступ к которым должен быть разрешен большому числу людей, возникает потребность создания единой базы данных учетных записей, которую могли бы единообразно использовать все сетевые устройства, решающие задачу аутентификации.

Заключение

В современной комплексной сети из маршрутизаторов, коммутаторов и серверов задача управления всеми устройствами и обеспечения того, чтобы они не просто функционировали, а работали оптимально, может показаться обескураживающей. Именно здесь нам может помочь SNMP (Simple Network Management Protocol) – простой протокол управления сетью, предоставляющий пользователям «простой» набор операций, позволяющий управлять этими устройствами удалённо.

В тексте выше обращено внимание на серьёзные «огрехи» безопасности протокола SNMP, который передаёт свои сообщения по протоколу UDP открытым незашифрованным текстом, в отличие от протокола CMIP. Но здесь мы забываем об одной вещи. Предполагаемое поле деятельности протокола SNMP – работа в крупной компьютерной сети, порядка 1000 узлов. Протокол SNMP не будут устанавливать в маленькую сеть меньше 200 узлов, потому что обслуживание и настройка SNMP – дорогое удовольствие. А в большой сети для управления сетью посредством SNMP скорее всего организуют внеполосное управление и проложат отдельные кабели, закрыв таким образом доступ посторонних лиц и обычных пользователей к передаваемым сигналам и данным протокола SNMP.

Проведен анализ протокола SNMP для мониторинга устройств. В настоящее время основная задача при подключении бытовых устройств возможность мониторинга состояния для решения аварийных ситуаций. В основном данные устройства используют протокол SNMP. Поэтому тестирование протокола SNMP в сетях Интернет является очень актуальной задачей.

Опубликованы 3 научные статьи:

- 1) Система контроля состояния компонентов локальной сети;
- 2) Контроль состояния компонентов локальной сети: проблемы безопасности;
- 3) Контроль состояния компонентов локальной сети компьютерной сети.