Федеральное агентство связи

Государственное федеральное образовательное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Государственное образовательное учреждение высшего профессионального образования
«Поволжский государственный университет телекоммуникаций и информатики»

Кафедра МСИБ

Методические разработки к лабораторной работе

«Принципы управления и мониторинга в локальных сетях. Управление коммутатором Cisco Catalyst»

для студентов специальностей 210406, 210400, 210403, 210404

Составители:
к.т.н., доц. Киреева Н. В.
ст. преп. Буранова М.А.
инженер Малина М.А.

Редактор:
к.т.н., доц. Зайкин В.П.

Рецензент:
д.т.н., проф. Росляков А.В.

Самара 2011

Цель работы: Изучение принципов управление в локальных сетях. Использование различных методов управления коммутаторами Cisco Catalyst. Знакомство с интерфейсом командной строки операционной системы Cisco IOS коммутатора Catalyst.

1. Принципы построения систем управления сетями

Распределенная природа сетей обусловливает применение модели «менеджер-агент» для построения системы управления (Рис. 1). *Менеджер* представляет собой программно-аппаратные средства, собирающие информацию от агентов, выполняющие ее обработку для предоставления администратору сети. На основании этой информации администратор с помощью менеджера может осуществлять некоторые управляющие воздействия на объекты сети. Управление может быть в той или иной мере автоматизировано. *Агенты* располагаются в управляемых элементах сети. Они непосредственно взаимодействуют с управляемыми объектами и обслуживают базу данных управляемых (наблюдаемых) параметров. Информационные базы управления MIB (Management Information Base) содержат списки управляемых параметров и их значения, агенты отвечают за соответствие баз реальным состояниям объектов. Менеджер может в любой момент запросить информацию о состоянии объекта, выполняя операцию чтения, и агент в ответ на этот запрос обязан передать содержимое всей базы или ее части. Операция записи в базу, если она разрешена, заставляет агента выполнять управляющие воздействия на объект. Опросы состояния выполняются по инициативе менеджера регулярно или эпизодически, например, по запросу администратора.

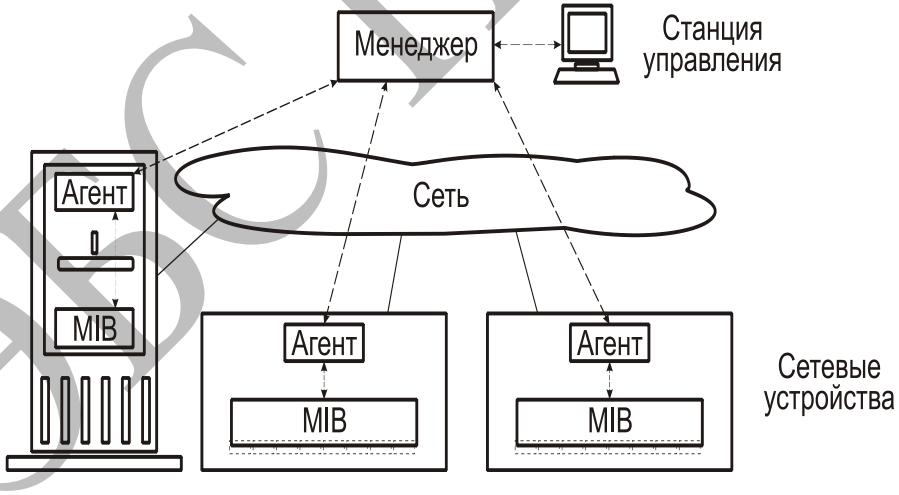


Рис. 1. Структура систем управления сетью

При создании системы управления обычно стремятся к максимальной централизации (в идеале — управление сетью из одной точки), но по разным причинам это не всегда удается. Агенты управления могут присутствовать как в сетевых коммуникационных устройствах (управляющие модули в повторителях, коммутаторах, маршрутизаторах), так и в конечных сетевых узлах (дополнительные аппаратные средства сетевых карт и загружаемые программные модули). Менеджер представляет собой программу, функционирующую, как правило, на компьютере общего назначения.

Всеобъемлющая система сетевого управления должна предоставлять администратору информацию о структуре сети со всеми связями, информацию о состоянии всех управляемых объектов (конечных узлов, линий связи, портов коммуникационной аппаратуры). Для решения этой задачи существуют специализированные и довольно дорогостоящие пакеты управляющего ПО, как правило, ориентированные на работу с оборудованием одного производителя.

Модель сетевого управления ISO рассматривает 5 концептуальных областей:

1. Производительность (performance management) — измерение параметров, определяющих пропускную способность, время отклика, загрузку линий и т. п. Система следит за значениями параметров, определяет их средние (нормальные) значения, а по достижении какими-либо критичными параметрами заданных порогов генерирует предупреждения или автоматически выполняет управляющие действия. Кроме наблюдения за сетью, в этой области управления возможно и активное воздействие на сеть с помощью симуляторов (генераторов трафика) для того, чтобы оценить поведение сети при повышении нагрузки (например, при грядущем расширении) и предпринять необходимые меры для обеспечения приемлемой производительности.

2. Конфигурирование (configuration management) — отслеживание информации об аппаратных и программных составляющих элементов узлов сети, включая сведения о типе и версии продуктов, их настройках и т. п. Сюда же относится управление функциями устройств в целом и конфигурирование их портов.

3. Использование ресурсов (accounting management) — учет трафика отдельных узлов и их групп, как для эффективного распределения ресурсов сети, так и с целью определения размера оплаты за предоставляемые услуги.

4. Обработка отказов (fault management) — обнаружение и регистрация отказов, уведомление администратора, восстановление работоспособности. При появлении симптомов отказа система должна по возможности изолировать проблемный участок, задействовать резервные элементы, запротоколировать события, восстановить исходную конфигурацию после устранения отказов.

5. Безопасность (security management) — управление доступом к сетевым ресурсам: авторизация пользователей, защита от несанкционированного доступа, предотвращение блокирования сети (намеренного и непреднамеренного).

В стеке протоколов ISO имеется общий протокол управляющей информации *CMIP* (Common Management Information Protocol). На основе этого протокола могут быть построены сложные системы управления (подразумевается большая интеллектуальность агентов, чем в SNMP, используется гарантированная доставка сообщений, имеются средства сокращения управляющего трафика). В локальных сетях управление по CMIP используется редко, здесь господствует SNMP.

Обмен сообщениями между агентами и менеджерами может происходить как по тем же каналам связи, по которым передаются «полезные» данные сети, так и по отдельным каналам. Первый способ называется *внутриполосным* (in band), его преимущество в отсутствии необходимости прокладывания

дополнительных коммуникаций. Расплатой за это является дополнительная загрузка сети служебным трафиком управления, проблемы авторизации управляющих воздействий (в принципе, любой клиент сети имеет физический доступ к каналу передачи управляющей информации) и некоторые ограничения на функции управления. Для того чтобы можно было устройством управлять, оно, естественно, должно иметь возможность обмениваться данными с менеджером. Но иногда возникают ситуации, когда для обеспечения возможности обмена требуется выполнить пока еще недоступные функции управления. Отдельные каналы для управляющей информации, требуемые для *внеполосного* управления (out of band), обеспечивают полную независимость функций управления от состояния управляемой сети. Большинство управляемых коммуникационных устройств поддерживает оба способа управления. Внутриполосное управление используется при регулярной работе, а подключение управляющей консоли по последовательному интерейсу — эпизодически, на этапе начального конфигурирования устройств и в некоторых особых случаях. Внутриполосное управление может быть основано на разных прикладных протоколах — SNMP, Telnet или Web-управление.

2. Управление коммуникационными устройствами

Каждое управляемое коммуникационное устройство — интеллектуальный хаб, коммутатор, маршрутизатор — должно иметь средство для обеспечения диалога с администратором в процессе конфигурирования и, если необходимо, средства связи его встроенных агентов управления с внешним менеджером. Для этих целей в большинстве устройств имеется консольный порт, в дополнение к которому могут поддерживаться протоколы Telnet, SNMP и Web-интерфейс. Во многих устройствах предусматривается возможность обновления встроенного ПО для расширения функциональных возможностей самого устройства и/или его системы управления. В старых устройствах для этого требовалась замена (перепрограммирование) ПЗУ с программным кодом, современные устройства допускают обновление ПО по протоколам BootP или TFTP.

2.1. Консольное управление

Консольное управление относится к внеполосному — к управляемому устройству подключают внешний терминал (консоль). Для подключения используют последовательный интерфейс RS-232C в асинхронном режиме, в ряде случаев с полным набором сигналов и возможностью коммуникаций через модемы по коммутируемым телефонным линиям связи. Чаше используют локальное подключение терминала по трехпроводному интерфейсу RS-232C. При подключении терминала должен быть выбран подходящий кабель — здесь встречается многообразие вариантов.

Терминал выполняет простейшие функции — пересылает коды символов клавиатурного ввода на вход приемника управляемого устройства и отображает символы, принятые с выхода передатчика устройства, на своем экране.

Форма диалога с устройством определяется его встроенным

программным обеспечением (firmware). Терминал должен поддерживать определенную систему команд (например, VT-52, VT-100), на которую рассчитано управляемое устройство. В противном случае не будут корректно обрабатываться управляющие коды (перемещение курсора, стирание символа и экрана) и вид диалогов будет сильно отличаться от приведенного в документации на устройство. В качестве терминала часто используют ПК с программной эмуляцией терминала (например, HyperTerminal в Windows), подключенный через COM-порт.

Консольное управление позволяет настраивать любые параметры устройства, независимо от состояния сети передачи данных. С его помощью настраивают параметры для внутриполосного управления (IP-адрес и маска, имя устройства, адрес маршрутизатора, параметры SNMP, Telnet, BootP, списки адресов узлов, которым разрешено управление данным устройством, пароль на доступ). Здесь же можно управлять и функциональными свойствами устройств (например, устанавливать режимы работы портов, разрешенные MAC-адреса подключаемых устройств, конфигурировать VLAN для коммутаторов, настраивать маршрутизаторы и т. п.). С консоли можно получать и статистические данные, если они собираются устройством. Установленные параметры конфигурирования могут быть сохранены в энергонезависимой памяти устройства, как правило, для этого выполняется явная команда. Если сохранение не выполнить, то после рестарта устройства (по аппаратному сбросу или включению питания) восстановятся прежние сохраненные значения параметров.

Недостатками консольного управления являются ограниченные возможности пользовательского интерфейса (любителей графических оконных интерфейсов он не устроит) и привязка консоли к устройству линией связи. Некоторые модели устройств (версии их управляющего ПО) позволяют использовать консольный порт для связи по протоколу SLIP.

2.2. Управление через Telnet

Управление через Telnet позволяет удаленно управлять устройствами по сети передачи данных (внутриполосное управление). По сути, это вариант консольного управления, но без специальных линий связи. Пользовательский интерфейс управления при этом выглядит так же и определяется встроенным ПО управляемого устройства. Управление через Telnet требует использования в сети передачи данных протокола IP. Для него на одном из компьютеров сети необходимо запустить приложение Telnet — эмуляцию терминала со связью через протокольный стек TCP/IP. В этом приложении необходимо установить связь с управляемым устройством, указав его IP-адрес или имя (если оно прописано в DNS) и введя пароль. После установления соединения компьютер будет играть роль удаленного терминала управляемого устройства, работа с которым аналогична вышеописанному консольному управлению.

До использования Telnet управляемое устройство должно быть сконфигурировано, как правило, через консоль. Ему должен быть назначен IP-адрес, маска подсети и адрес маршрутизатора в соответствии с местом его

установки. В целях обеспечения безопасности на управляемом устройстве задают пароль доступа, причем могут быть заданы разные пароли для доступа только по чтению (read only) и с разрешением записи (read-write). Время предъявления пароля (login timeout) и количество попыток ввода (login retries) могут быть ограничены, и по срабатыванию ограничения соединение разрывается. Можно задавать и время неактивности оператора (inactivity timeout), после которого соединение разрывается. Также задается и список IP-адресов узлов (allowed source IP address), с которых разрешены сеансы Telnet.

Управление через Telnet позволяет с одного компьютера управлять множеством устройств, но при этом требует «живой» сети с протоколом IP. Как и консольный вариант Telnet-управление подразумевает непосредственный диалог с человеком-оператором, и не подходит для организации сложных систем управления, тем более автоматизированных. Протокол Telnet является небезопасным, поскольку данные в пределах сеанса связи передаются в незашифрованном виде и могут быть прочитаны при их перехвате (в том числе и пароли доступа). Для повышения безопасности необходимо позаботится о сохранности передаваемых данных (к примеру, весть трафик системы управления передавать в отдельной VLAN). Отдельные устройства поддерживают безопасный протокол SSH, в котором предусмотрено шифрование передаваемых данных.

2.3. Протокол управления SNMP

Протокол прикладного уровня SNMP (Simple Network Management Protocol — простой протокол сетевого управления) является частью протокольного стека TCP/IP, хотя его сообщения могут пересылаться и по протоколу IPX/SPX.

Протокол SNMP оперирует следующими понятиями:

- Управляемое устройство (managed devices) — узел управляемой сети (промежуточный или конечный), снабженный агентом. Управляемое устройство способно собирать и хранить управляющую информацию и обмениваться ею по протоколу SNMP.

- Агент (agent) — программный модуль, расположенный в управляемом устройстве, преобразующий локальную ему доступную управляющую информацию в формат сообщений SNMP и обратно.

- Система сетевого управления NMS (network-management system) — компьютер, на котором установлено программное обеспечение, взаимодействующее с управляемыми устройствами.

Протокол определяет набор базовых команд взаимодействия NMS с объектами:

- Get — получение значений объектов (наблюдение за устройством) по инициативе NMS.

- GetNext — вариант команды для последовательного обращения к однотипным объектам (например, элементам таблиц маршрутов или таблиц состояния портов).

- GetBulk — получение значений блока объектов (только в SNMP v.2).

- Set — установка значений объектов (управление устройством) по инициативе NMS.

- Trap — асинхронное сообщение (прерывание) от устройства к NMS о каком-либо событии.

- Inform — передача сообщений между двумя NMS (только в SNMP v.2).

Сообщения SNMP передаются с помощью протокола UDP (негарантированная доставка, без подтверждения), хотя возможна настройка и на гарантированный транспорт TCP, а также IPX. Сообщения имеют заголовок с идентификатором версии и строкой «общности» — *community* и блок протокольных данных (PDU). Строка *community* используется как идентификатор группы устройств, общающихся по SNMP. Это примитивное средство обеспечения безопасности: агент будет отвечать на запрос, если в нем указана та же строка (чувствительно к регистру), что и сконфигурированная у агента. NMS не будет воспринимать сообщение с «неправильной» строкой. Поскольку строки *community* передаются по сети в открытом виде, безопасность весьма условна. Протокольный блок (PDU) содержит идентификатор типа сообщения (код команды), несколько служебных полей и список имен и значений объектов.

Поскольку форматы сообщений и некоторые протокольные правила разных версий несовместимы, при использовании агентов с разными версиями система управления должна быть «двуязычной» либо использовать прокси-систему, транслирующую диалог между NMS одной версии и агентами другой версии.

Информационная база управления MIB (Management Information Base) SNMP представляет собой иерархически организованную систему объектов. Каждый объект MIB является одним из множества параметров управляемого устройства. Объекты могут быть двух типов. Скалярный (scalar) объект определяет единичный параметр. Табличный (tabular) объект описывает множество однотипных параметров, объединенных в таблицу. Каждый объект имеет *идентификатор,* однозначно определяющий его положение в иерархии.

Информационная база MIB I (RFC 1156, 1990 г.) была определена для маршрутизаторов TCP/IP. В нее входит 114 объектов, разделенных на 8 групп. База предоставляет общую системную информацию об устройстве (например, тип устройства, время непрерывной работы), параметры сетевых интерфейсов, таблицу трансляции адресов и основные данные по протоколам IP, ICMP, TCP, UDP, EGP. Предусматривалось только чтение данных. Эта база была расширена до 10 групп и 185 объектов в версии MIB II (RFC 1213, 1992 г.), и появилась возможность управления (команда записи). MIB II позволяет, например, собирать статистические данные по пакетам определенных типов (одноадресные, широковещательные), принятых и переданных интерфейсами.

В дереве стандартов определены места для MIB, специфичных для конкретных моделей оборудования. Их определяют производители оборудования, они должны быть известны и разработчикам систем управления.

Минимально необходимые программные средства взаимодействия с конкретными устройствами для популярных ОС (Windows, UNIX и т. д.), как

правило, поставляются вместе с управляющими модулями. Для универсальных систем управления к каждому типу устройств (или даже версий его управляющего ПО) должны быть соответствующие программные модули (или базы данных). Управление по SNMP может иметь графический интерфейс (вплоть до изображения лицевой панели устройства с правдивым отображением всех индикаторов). Результаты работы зондов могут отображаться в удобном графическом формате.

До использования SNMP управляемое устройство должно быть сконфигурировано. Ему должен быть назначен IP-адрес, маска подсети и адрес маршрутизатора в соответствии с местом его установки (в случае использования не IP-протокола конфигурирование будет иным). Также должен быть задан адрес узла (список узлов), на который посылаются сообщения-прерывания по событиям, и, возможно, определен список событий, по которым посылаются прерывания. Необходимо также занести корректное значение строки *community,* помня о его чувствительности к регистру. Строка *community* может быть задана отдельно для доступа только по чтению *(SNMP read community,* по умолчанию часто используется слово *public),* для доступа с разрешенной записью *(SNMP read-write community,* по умолчанию слово *private)* и для прерываний *(SNMP trap community).*

2.4. Удаленный мониторинг — RMON и RMON2

С появлением интеллектуальных хабов и коммутаторов в них стали встраивать зонды для мониторинга —RMON (Remote MONitoring) Probe. Взаимодействие с этими зондами, как правило, ведется по протоколу SNMP. Для зондов, поначалу работавших только на MAC-уровне, был принят стандарт *RMON.* В нем определена база MIB из 9 групп объектов управления и наблюдения (RMON Groups). Первые 3 группы специфичны для технологии Ethernet с ее коллизиями, слишком короткими или длинными кадрами и т. п. Остальные группы не привязаны к конкретной реализации MAC-уровня, а для Token Ring выделена группа с номером 10. Впоследствии определили дополнительные 10 групп для наблюдений на более высоких уровнях — RMON2 (RFC 2074).

Группы, специфические для MAC-уровня Ethernet (RFC 1271):

- Statistics (статистика) — информация об активности сети (порта, сегмента): общее число переданных и принятых кадров и байт информации, количество нормальных кадров и кадров с разными типами ошибок (см. 6.1), количество коллизий, распределение кадров по размерам (64, 65-127, 128-255, 256-511, 512-1023, 1024-1518 байт), количество широковещательных и многоадресных кадров.

- History (история) — набор статистических данных (но без распределения по размерам пакетов), накапливаемых за заданные интервалы времени. Позволяют наблюдать за поведением сети, определять типовые нагрузки и определять тенденции их изменений.

- Alarm (тревоги) — установка порогов на измеряемые параметры (счетчики, измерители уровней), по достижении которых агент генерирует

сообщение-прерывание. На каждый параметр устанавливается два порога: один на превышение, другой — на возврат к норме.

MAC-независимые группы:

- Host (хосты) — статистические данные (аналогичные 1 группе), собираемые по каждому обнаруженному узлу (по MAC-адресам).

- HostTopN *(N* самых активных хостов) — определение списка хостов, выдающихся по определенным статистическим показателям. К примеру, определение пятерки узлов, генерирующих основной поток широковещательного трафика.

- Matrix (матрица трафика) — отслеживание диалогов между парами узлов (уровень трафика и ошибок в каждом направлении).

- Filter (фильтр) — установка специфических признаков фильтрации кадров для захвата.

- Packet Capture (захват пакетов) — определение условий начала захвата кадров (пакетов), удовлетворяющих критериям фильтра, и числа захватываемых кадров. Начало и окончание захватов является событиями для генерации прерываний.

- Event (события) — управление посылкой прерываний по событиям (превышение порогов и возврат, начало и окончание захвата и т. п.).

Группы RM0N2 (RFC 2021 и 2074) предназначены для мониторинга сетевого и прикладного уровней.

- Protocol Directory (каталог протоколов) — список протоколов, которые могут отслеживаться зондом.

- Protocol Distribution (распределение протоколов) — статистика (распределение и тенденции) трафика по протоколам (IP, IPX, DECnet, AppleTalk...).

- Address Mapping (карта адресов) — таблица соответствия сетевых и MAC-адресов узлов.

- Network-Layer Host (хосты на сетевом уровне) — статистика трафика (входного и выходного) по каждому обнаруженому в сети хосту.

- Network-Layer Matrix (матрица сетевого уровня) — статистика трафика диалогов между парами хостов.

- Application-Layer Host (хосты на прикладном уровне) — статистика трафика (входного и выходного) хоста по конкретному протоколу (вплоть до прикладного уровня). Позволяет определять трафик таких приложений, как Web, Telnet, Lotus Notes и т. п.

- Application-Layer Matrix (матрица прикладного уровня) — статистика трафика диалога хостов по конкретным протоколам вплоть до прикладного уровня.

- User History Collection (программируемый сбор истории) — периодическая выборка значений параметров по выбору пользователя (из списка группы статистики RMON1).

- Probe Configuration (конфигурация зонда) — стандартизованный способ задания таких параметров, как адрес назначения прерываний, и других параметров, обычно устанавливаемых внеполосным (консольным) управлением.

Зонды RMON во многих случаях позволяют отказаться от дорогостоящих внешних анализаторов.

2.5. Дистанционное конфигурирование и обновление встроенного программного обеспечения (BootP и TFTP)

Интеллект управляемого сетевого оборудования определяется его встроенным ПО (firmvare), и при появлении новых версий ПО возможно расширение возможностей (как функциональных, так и управленческих) эксплуатируемых устройств. Управляющие модули (NMM) современных коммуникационных устройств (Network Management Module) представляют собой микрокомпьютеры с иерархической системой памяти. В нее входит:

- Оперативная память. Используется для хранения данных, необходимых для функционирования управляющего ПО, хранения информации о текущей конфигурации устройства. В эту же память может загружаться и исполняемый код управляющего ПО.

- Энергонезависимая память для хранения управляющего ПО (firmware). Как правило, строится на микросхемах флэш-памяти, что позволяет осуществлять модернизацию управляющего ПО перезаписью через внешние интерфейсы устройства.

- Энергонезависимая память хранения параметров конфигурации.

При инициализации устройства (по включении питания, кнопки или команде рестарта) выполняется самотестирование, после чего в оперативную память загружается исполняемый код и параметры конфигурации устройства. В устройствах, не привязанных к системам управления сетью, загрузка производится только из локальной энергонезависимой памяти, после чего параметры конфигурации можно изменять вручную через консоль (через консольный порт или Telnet). Измененные настройки могут быть сохранены в энергонезависимой памяти, и тогда после следующей перезагрузки они окажутся параметрами, принятыми по умолчанию. Включение NMM-устройства в общую систему управления сетью NMS (Network Management System) позволяет выбирать различные варианты загрузки NMM. При этом можно вместо локально хранящихся программных модулей и параметров конфигурирования загружать эти компоненты по сети по протоколу TFTP (примитивный протокол файлового обмена). Файлы с *образами* программных модулей управляющего ПО (image file) и файлы *конфигурации* (configuration file) должны быть размещены на сервере сети, поддерживающем протокол TFTP. Сервис TFTP не является сервисом, предоставляемым по умолчанию, и в ОС типа Windows 9x/NT, UNIX его необходимо установить и сконфигурировать (определить доступные каталоги, в которых помещают файлы-образы, предоставить права доступа и т. п.). Управляемое устройство должно «знать», с какого сервера и какие файлы (образ и конфигурация) оно должно загрузить при инициализации. Эта информация заносится в локальную энергонезависимую память устройства при его конфигурировании (внеполосном) или принимается от специального сервера по протоколу BootP. Рассмотрим этапы загрузки и возможные варианты конфигурирования.

1. Для того чтобы можно было обратиться к серверу за файлами по TFTP, устройство должно иметь собственную IP-настройку (адрес и маску подсети, адрес, маршрутизатора), знать IP-адрес сервера, имена файлов (образа и конфигурации) и каталога, в котором они находятся. Если устройство поддерживает BootP, то конфигурация загрузки (boot configuration) может предлагать ряд вариантов:

- использовать только локальные данные из энергонезависимой памяти; D использовать только BootP (при неполучении ответа NMM не загрузится);

- пытаться использовать BootP, а при неудаче использовать локальные данные;

- пытаться использовать BootP, а при неудаче использовать данные, полученные при предыдущем успешном использовании BootP.

2. Если используется BootP, то при инициализации NMM после самотестирования устройство посылает широковещательный запрос BootP, на который должен ответить сервер. Посылая запрос, устройство о себе еще ничего не знает, а BootP-сервер опознает его по MAC-адресу («зашитому» в устройство изготовителем). На сервере в файле конфигурации BootP должна присутствовать запись, в которой указывается MAC-адрес NMM для каждого управляемого устройства, его параметры IP-конфигурации, имена файлов и каталогов. Формат файла конфигурации зависит от используемого «демона» BootP — части программного обеспечения NMS. В ответе на запрос устройство получает данные, необходимые для работы по TFTP.

3. Загрузка образа и конфигурации также может производиться по выбору, локально или по TFTP. Выбор источника загрузки для конфигурации и образа независим. Загруженный образ может быть автоматически записан в энергонезависимую память устройства по выбору: сохранять, если отличается (writeDiff); сохранять, если более новая версия (writeNewer); не сохранять (noWrite). Заметим, что адрес маршрутизатора, используемого при загрузке, может отличаться от адреса маршрутизатора, используемого в дальнейшей работе (хранящегося в локальной памяти или загруженного по TFTP).

4. Файлы с образом управляющего ПО и образцы файлов конфигурации получают в составе пакета NMS, в комплекте с устройством (или его NMM) или, например, на Web-сайте производителя. Обновление версии ПО можно выполнять не только в момент загрузки, но и в произвольное время по инициативе оператора. Для этого предусматривается специальная консольная команда.

5. Дистанционное конфигурирование устройств актуально для сложных сетей с развитой системой управления. Оно позволяет избегать диалогов администратора с каждым из устройств — одни и те же конфигурационные шаблоны могут использоваться группой однотипных устройств. При удобном пользовательском интерфейсе NMS вносить изменения в конфигурационные файлы удобнее, чем вести диалоги. Кроме того, устанавливаемые конфигурации автоматически документируются, что упорядочивает процесс управления.

2.6. Web-интерфейс управления

Повсеместное распространение Web-технологий захватило и сферу управления сетевыми устройствами. Общая идея Web-управления, или *WBM* (Web-Based Management), заключается в обеспечении возможности выполнения оператором (администратором) управляющих действий через графический интерфейс стандартного Web-браузера с любой станции сети. Web-управление может быть организовано двумя способами: через встроенные (embeded) Web-серверы или через прокси-системы.

При *встроенном WBM* в программное обеспечение управляемого устройства вводятся функции Web-сервера, динамически формирующего «странички» интерфейса управления. Эти страницы могут отображаться в графическом виде Web-браузером любого узла, с которого управляемое устройство доступно по протоколу HTTP стека TCP/IP. Вид интерфейса задается ПО управляемого узла (а также возможностями и настройками браузера). Использование графических элементов, гиперссылок и других разнообразных элементов языка HTML, а также Jawa-апплетов позволяет создавать наглядные интуитивно понятные образы панелей управления устройств. В отличие от графических оболочек управляющих программ, использующих SNMP, Web-управление не требует установки специализированного ПО на специальной станции управления, привязанного к конкретным управляемым устройствам. Для управления может использоваться любая станция сети со стандартным Web-браузером. С точки зрения сетевого управления встроенный WBM мало чем отличается от Telnet, хотя пользовательский интерфейс гораздо привлекательнее и нагляднее.

Для обеспечения Web-управления устройству должны быть указаны параметры его IP-подключения (IP-адрес и маска, адрес маршрутизатора). *Безопасность* (блокировка несанкционированного доступа) обеспечивается паролированием доступа, ограничением списка разрешенных узлов и, чего нет ни в SNMP, ни в Telnet, возможностью шифрования данных (data encryption) по требованию сервера (управляемого устройства).

Прокси-системы позволяют распространить Web-управление и на устройства с классическим SNMP-управлением. Для этого создается специализированное управляющее приложение, взаимодействующее с управляемыми устройствами по SNMP, включая поддержку RMON. Это приложение запускается на компьютере сети и связывается с серверным ПО, предоставляющим доступ к его данным по протоколу HTTP. Это приложение становится Web-представителем (proxy) управляемых устройств для Web-броузеров, и управление SNMP-объектами станет возможным с любой станции.

3. Конфигурирование коммутаторов Catalyst

3.1 Методы конфигурации коммутаторов Catalyst

При попытке войти в систему конфигурирования (log in) коммутатора Catalyst пользователю предлагается ввести пароль. При вводе правильного пароля пользователь попадает в режим конфигурации коммутатора Catalyst в

обычном режиме (NORMAL mode). Обычный режим эквивалентен режиму *пользовательских команд* (User EXEC), который используется в маршрутизаторах. В данном режиме пользователь имеет право просматривать большинство параметров конфигурации коммутатора Catalyst, однако у него нет авторизации для внесения изменений в конфигурацию. Если пользователю нужно внести изменения в конфигурацию, он должен войти в *привилегированный режим* (PRIVILEGED mode) работы с коммутатором Catalyst. Привилегированный режим работы с коммутатором Catalyst эквивалентен режиму *привилегированных команд* (PRIVILEGED EXEC mode) маршрутизаторов Cisco. В привилегированном режиме пользователь имеет право просматривать конфигурацию и вносить в нее изменения. Для входа в данный режим необходимо выполнить команду enable. Далее операционная система коммутатора Catalyst предложит пользователю ввести пароль.

Доступ к интерфейсу командной строки коммутатора Catalyst можно получить тремя основными способами: через консольный интерфейс, по сети с помощью протокола Telnet или через простейший протокол передачи файлов (Trivial File Transfer Protocol — TFTP).

3.2 Конфигурирование устройства через консольный интерфейс

Модуль управления коммутаторов Catalyst предоставляет возможность физического подключения к одному консольному интерфейсу.

Консольный интерфейс может работать в двух режимах: собственно в режиме консоли, а также в режиме поддержки протокола slip. При работе в режиме консоли к этому интерфейсу может быть подключен терминал или устройство эмуляции терминала, такое, как персональный компьютер, с установленным соответствующим программным обеспечением. Такой режим работы позволяет получить непосредственный доступ к интерфейсу командной строки независимо от конфигурации. Данный режим доступа используется в случае, если для коммутатора Catalyst не установлено значение IP-адреса. Без определенного значения IP-адреса нет возможности установить сессию с коммутатором Catalyst по сети, используя протокол Telnet. Данный режим также используется в случае необходимости восстановления пароля (password recovery). Процедура восстановления пароля описана в одном из следующих разделов. Данный метод доступа к коммутатору Catalyst может быть выбран в том случае, если администратор находится в непосредственной близости от коммутатора и у него в распоряжении есть свободный терминал.

Консольный порт может быть установлен в режим поддержки протокола SLIP (Serial Line Interface Protocol — межсетевой протокол для последовательного канала).

Данный протокол является предшественником протокола PPP**.** При использовании консоли в режиме SLIP пользователю предоставляется возможность входа по протоколу Telnet непосредственно на консольный порт. При таких настройках вероятнее всего к консольному порту подключается модем, что дает возможность непосредственного установления сессии по протоколу Telnet с коммутатором без необходимости использования сети.

Такой режим работы может быть очень полезен при устранении ошибок конфигурации в случаях, когда к коммутатору нет доступа по сети.

3.3 Конфигурирование устройства посредством службы Telnet

Доступ к интерфейсу командной строки может быть получен по сети с помощью протокола Telnet. Коммутатор Catalyst имеет внутренний *логический интерфейс,* которому можно присвоить IP-адрес. Данный адрес является адресом отправителя для пакетов, которые генерируются коммутатором, и адресом получателя для пакетов, которые должны быть получены коммутатором. Назначение IP-адреса такому интерфейсу приводит к тому, что коммутатор Catalyst становится станцией в сети, работающей по протоколу IP. Адрес может быть использован для работы с протоколами Telnet, TFTP, BOOTP, RARP, ICMP, а также для выполнения команд trace, host и других функций, свойственных сетевым станциям. По умолчанию этот интерфейс принадлежит виртуальной локальной сети VLAN 1, и IP-адрес ему не присвоен. Перед тем, как осуществлять конфигурацию коммутатора Catalyst по протоколу Telnet, необходимо назначить IP-адрес. Установить сеанс по протоколу Telnet с коммутатором Catalyst можно только в том случае, если устройство, с которого устанавливается сеанс, может отправлять пакеты в ту сеть VLAN и сеть IP, которым принадлежит интерфейс. Сеанс, установленный с коммутатором Catalyst по протоколу Telnet, позволяет пользователю выполнять команды так же, как если бы он имел доступ через консольный интерфейс. Однако для того, чтобы получить доступ, необходимо знать пароли для входа в обычный режим и режим привил

Средства контроля доступа коммутатора Catalyst позволяют пользователю указать список полномочий доступа (access list), в котором можно указать список станций, с которых пользователи имеют права доступа на коммутатор по протоколу Telnet или права управления по протоколу SNMP (Simple Network Management Protocol — простой протокол управления сетью).

Обеспечить безопасность доступа к коммутатору Catalyst также можно с помощью системы TACACS+ (Terminal Access Controller Access Control System Plus — система управления доступом к контроллеру терминального доступа) и ее службы аутентификации. Система TACACS+ устанавливает коммуникационный протокол между коммутатором Catalyst и сервером системы TACACS+. Сервер осуществляет аутентификацию пользователей на основании имени пользователя и пароля, которые вводятся при попытке доступа к коммутатору Catalyst через консоль. Обычно в коммутаторах Catalyst применяется аутентификация на основании локальных параметров, таких, как пароли для входа в обычный режим и режим привилегированных команд. Если пользователь знает эти пароли, он получает право входа в соответствующий режим.

Система TACACS+ требует не только пароль, но также и имя пользователя. Если пользователь хочет войти в систему коммутатора Catalyst в то время, когда используется служба TACACS+, коммутатор посылает запрос на сервер системы TACACS+ для информации по аутентификации

пользователя. Сервер отвечает подтверждением аутентификации пользователя или отказом в доступе.

Для активизации системы доступа TACACS+ необходимо, чтобы в сети работал сервер системы TACACS+. Детали конфигурации службы TACACS+ выходят за рамки данной книги. За более подробной информацией по вопросу последовательности конфигурирования следует обратиться к документации по коммутаторам Catalyst.

3.4 Конфигурирование устройства по протоколу TFTP

Коммутаторы Catalyst имеют встроенный TFTP-клиент, который позволяет принимать и отправлять конфигурационные файлы с TFTP-сервера или на него. Синтаксис команд для передачи конфигурационных файлов по протоколу TFTP зависит от версии управляющего модуля, установленного на коммутаторе Catalyst.

3.5 Использование интерфейса командной строки коммутаторов Catalyst

При вводе команда коммутатора Catalyst запоминается в специальном командном буфере, который называется *буфером истории выполненных команд* (history buffer). Буфер истории может содержать до 20 команд, доступных для повторного вызова и редактирования. Для извлечения команд из буфера в строку ввода используются клавиши <↑>, <↓>.

При работе с маршрутизаторами Cisco доступ к системе подсказок (help) осуществляется с помощью ввода команды <?> в командной строке. В результате выполнения данной команды маршрутизатор выводит список всех возможных вариантов для следующего параметра. При вводе значения следующего параметра и вводе символа <?> маршрутизатор выводит новый список для выбора новых возможных вариантов параметров командной строки. Таким образом, маршрутизатор отображает подсказки по принципу следующих друг за другом параметров. Вывод подсказки маршрутизатором заканчивается отображением в командной строке уже введенной части команды. Такой интерфейс дает возможность продолжать введение команды без необходимости снова вводить уже набранную ранее часть.

Тем не менее, принцип функционирования системы подсказок коммутатора Catalyst отличается от того, что используется в маршрутизаторах. Доступ к системе подсказок осуществляется так же, как в случае маршрутизатора, однако результаты вывода отличаются. Например, в случае, когда маршрутизатор выдает приглашение для ввода следующего параметра, коммутатор Catalyst выводит все возможные опции по использованию команды, если введенная команда не настолько уникальна, что коммутатор Catalyst в состоянии определить, какая команда требуется пользователю.

С другой стороны, если введено достаточно информации для того, чтобы коммутатор Catalyst мог определить, какую команду необходимо выполнить, то будет выведен список всех возможных значений параметров для введенной команды.

Следует заметить, что когда на консоли отображается подсказка, то после ее вывода командная строка отображается пустой. Командная строка, которая только что была введена, не отображается. Для вывода только что набранной командной строки необходимо воспользоваться повторным вызовом только что набранной команды.

Коммутатор Catalyst также выводит подсказку, если ввести вопросительный знак в конце команды. Подсказка также выдается при вводе неоконченной команды, которая завершается символом **<возврат каретки>** (<ENTER>).

4. Конфигурирование коммутатора Catalyst 2940

Catalyst 2940 –управляемый коммутатор небольшой емкости с восемью портами Fast Ethernet и отдельным интегрированным uplink-интерфейсом Fast Ethernet или Gigabit Ethernet. Подробно технические характеристики коммутатора Catalyst 2940 приведены в Приложении 1.

4.1 Командные режимы Cisco IOS

Интерфейс командной строки (CLI) предоставляет возможность работы в различных режимах. Набор команд в различных режимах различается.

При открытии сессии на коммутаторе запускается режим пользователя EXEC. В этом режиме доступен ограниченный набор команд. Для получения доступа ко всему набору команд необходимо войти в привилегированный режим EXEC, который может быть защищен отдельным паролем.

Для изменения конфигурации необходимо перейти в режим конфигурации. Сохраненная в энергонезависимую память конфигурация будет доступна после перезагрузки устройства.

В Таблице 2 представлены основные командные режимы, способ получения доступа к режиму, вид запроса командной строки и порядок выхода из режима.

Таблица 2. Основные командные режимы

Режим	Метод доступа	Запрос CLI	Метод выхода	Описание
Пользовательский EXEC	При установлении соединения с коммутатором	Switch>	Команды **logout** или **quit**.	Доступно:- просмотр системной информации, - изменение настроек терминала, - базовые тесты.

Привилегированный EXEC	В пользовательском EXEC команда **enable**	Switch #	Команда **disable**	Режим защищен отдельным паролем. Доступны все команды
Глобальной конфигурации	В привилегированном EXEC команда **configure**	Switch(config) #	Команды **exit** или **end**. Комбинация клавиш **Ctrl+Z**.	Основной режим конфигурации.
Конфигурирования интерфейса	В режиме глобальной конфигурации команда **interface** с указанием интерфейса.	Switch(config-if)#	Для выхода в режим глобальной конфигурации – **exit**, в привилегированный EXEC – **end** или **Ctrl+Z**.	Настройка параметров интерфейса.
Конфигурирования VLAN	В привилегирован	Switch(vlan)#	в привилеги	Конфигурирование параметров

	ном EXEC команда **vlan database**		рован ный EXE C – **exit**.	VLAN с номерами от 1 до 1005

4.3 Параметры терминала

Для управления коммутатором через консольный порт необходимо настроить программу эмуляции терминала со следующими параметрами:

- Скорость - 9600 бит/с.
- Биты данных - 8.
- Стоповые биты - 1.
- Четность - нет.

Коммутатор поставляется с этими значениями. Значения можно изменить по необходимости. К примеру, при загрузке программного обеспечения Cisco IOS для обновления через консольный порт потребуется увеличить скорость передачи.

Ход работы:

Внимание!!! Не сохраняйте файл конфигурации в энергонезависимую память коммутатора. В работе это необходимо сделать на сервер TFTP. В следующей работе данный файл будет использоваться.

Часть I. Подключение коммутатора через консольный порт.

1. Визуально определите порт на ПК, к которому подключен коммутатор.
2. Запустите программу HyperTerminal (Пуск\Программы\Стандартные\Связь).
3. Настройте программу для работы с коммутатором.

Часть II. Сбор информации о аппаратно-программной конфигурации устройства.

1. В пользовательском режиме EXEC с помощью команды **show version** определите программно-аппаратную конфигурацию коммутатора (версия загрузчика, IOS, платформы, состав интерфейсов).
2. Просмотрите состояние и настройки интерфейсов с помощью команд show **interfaces status, show interfaces, show interfaces** [наименование интерфейса].

Часть III. Настройка IP адреса

IP адрес коммутатора может быть настроен автоматически по протоколу DHCP или вручную. Произведем настройку вручную.

1. Получите номера IP адреса и шлюза у преподавателя.
2. Перейдите в режим глобальной конфигурации.
3. Перейдите в режим конфигурации интерфейса **Vlan 1**, применив следующую команду:

Switch#vlan data
Switch(vlan)#vlan 1
Switch#exit

(По умолчанию все интерфейсы Fast Ethernet и Gigabit Ethernet находятся в VLAN с номером 1).

Входим в режим глобальной конфигурации, присваиваем интерфейс fa 0/3 к VLAN 1 с помощью команд:

Switch(config)#int fa 0/3
Switch(config-if)#switchport access vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#exit

4. Настройте IP адрес на виртуальном интерфейсе Vlan 1. (команда **ip address** [параметры]).

Switch(config)#int vlan 1
Switch(config-if)#ip address
Switch(config-if)#no shutdown
Switch2(config-if)#exit

5. Вернитесь в привилегированный EXEC.
6. Проверьте произведенные настройки (команды **show interfaces vlan 1, show ip redirects**)

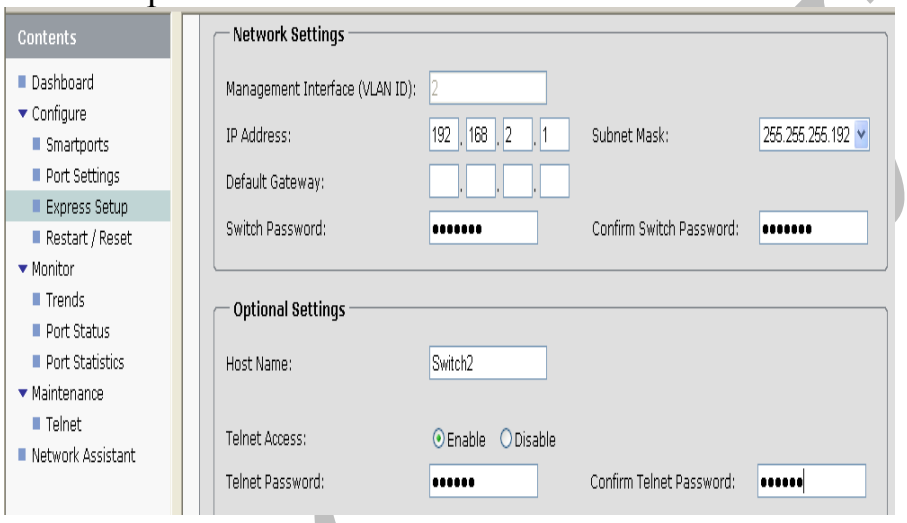
Теперь можно настраивать коммутатор по протоколу Telnet или через WEB-интерфейс.

Часть IV. Использование WEB-интерфейса.

1. Запустите Internet Explorer.
2. В строке адреса введите ip-адрес коммутатора.
3. Используя меню просмотрите настройки коммутатора, которые были определены в предыдущих частях.

Часть V. Подключение к коммутатору по протоколу Telnet.

1. Через WEB-интерфейс производим необходимые настройки для работы с Telnet.



2. Откройте командную строку Windows (Пуск\Выполнить\[cmd]).
3. введите команду **telnet** [ip адрес сконфигурированный на коммутаторе].
4. Используйте команды show из предыдущих частей для проверки конфигурации.

Часть VI. Подготовьте отчет по работе. Сохраните файл конфигурации на сервер TFTP используя команду **copy**.

Отчет по работе

Отчет должен содержать:

1. Информацию об программно-аппаратном обеспечении коммутатора.
2. Информацию об интерфейсах коммутатора.
3. Сохраненный файл конфигурации на сервере TFTP.

Контрольные вопросы

1. Что собой представляет модель «Менеджер-агент»?
2. Какие области рассматривает модель сетевого управления ISO?
3. Что собой представляет протокол управления SNMP?
4. Что представляет собой информационная база управления?
5. Что входит в иерархическую систему памяти?
6. Назовите параметры, необходимые для настройки программы эмуляции терминала?
7. В каком режиме происходит настройка IP-адреса на виртуальном интерфейсе Vlan?
8. Назовите достоинства и недостатки использования протокола Telnet.
9. Недостатком какого из видов управления являются ограниченные возможности пользовательского интерфейса? Расскажите о данном виде управления.
10. Расскажите о способах обмена сообщениями между агентами и менеджерами.