Средства анализа и управления сетями

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо тех, которые имеются в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критична для выполнения сетью своих основных функций. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляет эту информацию оператору сети. Обычно система управления работает в автоматизированном режиме, выполняя наиболее простые действия по управлению сетью автоматически, а сложные решения предоставляя принимать человеку на основе подготовленной системой информации. Система управления должна быть интегрированной. Это означает, что функции управления разнородными устройствами должны служить общей цели обслуживания конечных пользователей сети с заданным качеством.

Сами системы управления представляют собой сложные программно-аппаратные комплексы, поэтому существует граница целесообразности применения системы управления - она зависит от сложности сети, разнообразия применяемого коммуникационного оборудования и степени его распределенности по территории. 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.

7.1. Функции и архитектура систем управления сетями

7.1.1. Функциональные группы задач управления

Системы управления корпоративными сетями существуют не очень давно. Одной из первых систем такого назначения, получившей широкое распространение, был программный продукт SunNet Manager, выпущенный в 1989 году компанией SunSoft. SunNet Manager был ориентирован на управление коммуникационным оборудованием и контроль трафика сети. Именно эти функции имеют чаще всего в виду, когда говорят о

системе управления сетью. Кроме систем управления сетями существуют и системы управления другими элементами корпоративной сети: системы управления ОС, СУБД, корпоративными приложениями. Применяются также системы управления телекоммуникационными сетями: телефонными, а также первичными сетями технологий PDH и SDH.

Независимо от объекта управления, желательно, чтобы система управления выполняла ряд функций, которые определены международными стандартами, обобщающими опыт применения систем управления в различных областях. Существуют рекомендации ITU-T X.700 и близкий к ним стандарт ISO 7498-4, которые делят задачи системы управления на пять функциональных групп:

- управление конфигурацией сети и именованием;
- обработка ошибок;
- анализ производительности и надежности;
- управление безопасностью;
- учет работы сети.

Рассмотрим задачи этих функциональных областей управления применительно к системам управления сетями.

*Управление конфигурацией сети и именованием (Configuration Management).*Эти задачи заключаются в конфигурировании параметров как элементов сети (Network Element, NE), так и сети в целом. Для элементов сети, таких как маршрутизаторы, мультиплексоры и т. п., с помощью этой группы задач определяются сетевые адреса, идентификаторы (имена), географическое положение и пр.

Для сети в целом управление конфигурацией обычно начинается с построения карты сети, то есть отображении реальных связей между элементами сети и изменении связей между элементами сети - образование новых физических или логических каналов, изменение таблиц коммутации и маршрутизации.

Управление конфигурацией (как и другие задачи системы управления) могут выполняться в автоматическом, ручном или полуавтоматическом режимах. Например, карта сети может составляться автоматически, на основании зондирования реальной сети пакетами-исследователями, а может быть введена оператором системы управления вручную. Чаще всего применяются полуавтоматические методы, когда автоматически полученную карту оператор подправляет вручную. Методы автоматического построения топологической карты, как правило, являются фирменными разработками.

Более сложной задачей является настройка коммутаторов и маршрутизаторов на поддержку маршрутов и виртуальных путей между пользователями сети. Согласованная ручная настройка таблиц маршрутизации при полном или частичном отказе от использования протокола маршрутизации (а в некоторых глобальных сетях, например X.25, такого протокола просто не существует) представляет собой сложную задачу, Многие системы управления сетью общего назначения ее не выполняют, но существуют специализированные системы конкретных производителей, например система NetSys компании Cisco Systems, которая решает ее для маршрутизаторов этой же компании.

Обработка ошибок (Fault Management). Эта группа задач включает выявление, определение и устранение последствий сбоев и отказов в работе сети. На этом уровне

выполняется не только регистрация сообщений об ошибках, но и их фильтрация, маршрутизация и анализ на основе некоторой корреляционной модели, Фильтрация позволяет выделить из весьма интенсивного потока сообщений об ошибках, который обычно наблюдается в большой сети, только важные сообщения, маршрутизация обеспечивает их доставку нужному элементу системы управления, а корреляционный анализ позволяет найти причину, породившую поток взаимосвязанных сообщений (например, обрыв кабеля может быть причиной большого количества сообщений о недоступности сетей и серверов).

Устранение ошибок может быть как автоматическим, так и полуавтоматическим. В первом случае система непосредственно управляет оборудованием или программными комплексами и обходит отказавший элемент за счет резервных каналов и т. п. В полуавтоматическом режиме основные решения и действия по устранению неисправности выполняют люди, а система управления только помогает в организации этого процесса - оформляет квитанции на выполнение работ и отслеживает их поэтапное выполнение (подобно системам групповой работы).

В этой группе задач иногда выделяют подгруппу задач управления проблемами, подразумевая под проблемой сложную ситуацию, требующую для разрешения обязательного привлечения специалистов по обслуживанию сети.

Анализ производительности и надежности (Performance Management). Задачи этой группы связаны с оценкой на основе накопленной статистической информации таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи между двумя конечными абонентами сети, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети или ее определенной транспортной службы. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

Результаты анализа производительности и надежности позволяют контролировать *соглашение об уровне обслуживания (Service Level Agreement, SLA),* заключаемое между пользователем сети и ее администраторами (или компанией, продающей услуги). Обычно в SLA оговариваются такие параметры надежности, как коэффициент готовности службы в течение года и месяца, максимальное время устранения отказа, а также параметры производительности, например, средняя и максимальная пропускная способности при соединении двух точек подключения пользовательского оборудования, время реакции сети (если информационная служба, для которой определяется время реакции, поддерживается внутри сети), максимальная задержка пакетов при передаче через сеть (если сеть используется только как транзитный транспорт). Без средств анализа производительности и надежности поставщик услуг публичной сети или отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить нужный уровень обслуживания для конечных пользователей сети.

Управление безопасностью (Security Management). Задачи этой группы включают в себя контроль доступа к ресурсам сети (данным и оборудованию) и сохранение целостности данных при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, распределение и поддержка ключей шифрования, управления полномочиями и т. п. Часто функции этой группы не включаются в системы управления сетями, а реализуются либо в виде специальных продуктов (например,

системы аутентификации и авторизации Kerberos, различных защитных экранов, систем шифрования данных), либо входят в состав операционных систем и системных приложений.

Учет работы сети (Accounting Management). Задачи этой группы занимаются регистрацией времени использования различных ресурсов сети - устройств, каналов и транспортных служб. Эти задачи имеют дело с такими понятиями, как время использования службы и плата за ресурсы - billing. Ввиду специфического характера оплаты услуг у различных поставщиков и различными формами соглашения об уровне услуг, эта группа функций обычно не включается в коммерческие системы и платформы управления типа HP Open View, а реализуется в заказных системах, разрабатываемых для конкретного заказчика.

Модель управления OSI не делает различий между управляемыми объектами - каналами, сегментами локальных сетей, мостами, коммутаторами и маршрутизаторами, модемами и мультиплексорами, аппаратным и программным обеспечением компьютеров, СУБД. Все эти объекты управления входят в общее понятие «система», и управляемая система взаимодействует с управляющей системой по открытым протоколам OSI.

Однако на практике деление систем управления по типам управляемых объектов широко распространено. Ставшими классическими системы управления сетями, такие как SunNet Manager, HP Open View или Cabletron Spectrum, управляют только коммуникационными объектами корпоративных сетей, то есть концентраторами и коммутаторами локальных сетей, а также маршрутизаторами и удаленными мостами, как устройствами доступа к глобальным сетям. Оборудованием территориальных сетей обычно управляют системы производителей телекоммуникационного оборудования, такие как RADView компании RAD Data Communications, MainStreetXpress 46020 компании Newbridge и т. п.

Рассмотрим, как преломляются общие функциональные задачи системы управления, определенные в стандартах X.700/ISO 7498-4, в задачи такого конкретного класса систем управления, как системы управления компьютерами и их системным и прикладным программным обеспечением. Их называют *системами управления системой (System Management System).*

Обычно система управления системой выполняет следующие функции.

- *Учет используемых аппаратных и программных средств (Configuration Management).* Система автоматически собирает информацию об установленных в сети компьютерах и создает записи в специальной базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, какими ресурсами он располагает и где тот или иной ресурс находится, например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие компьютеры обладают достаточным количеством памяти, дискового пространства и т. п.
- *Распределение и установка программного обеспечения (Configuration Management).* После завершения обследования администратор может создать пакеты рассылки нового программного обеспечения, которое нужно инсталлировать на всех компьютерах сети или на какой-либо группе компьютеров. В большой сети, где проявляются преимущества системы управления, такой способ инсталляции может существенно уменьшить трудоемкость этой процедуры. Система может также позволять централизованно устанавливать и администрировать приложения,

которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети.

- *Удаленный анализ производительности и возникающих проблем (Fault Management and Performance Management).* Эта группа функций позволяет удаленно измерять наиболее важные параметры компьютера, операционной системы, СУБД и т. д. (например, коэффициент использования процессора, интенсивность страничных прерываний, коэффициент использования физической памяти, интенсивность выполнения транзакций). Для разрешения проблем эта группа функций может давать администратору возможность брать на себя удаленное управление компьютером в режиме эмуляции графического интерфейса популярных операционных систем. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами систем управления системами являются Microsoft System Management Server (SMS), CA Unicenter, HP Operationscenter и многие другие.

Как видно из описания функций системы управления системами, они повторяют функции системы управления сетью, но только для других объектов. Действительно, функция учета используемых аппаратных и программных средств соответствует функции построения карты сети, функция распределения и установки программного обеспечения - функции управления конфигурацией коммутаторов и маршрутизаторов, а функция анализа производительности и возникающих проблем - функции производительности.

Эта близость функций систем управления сетями и систем управления системами позволила разработчикам стандартов OSI не делать различия между ними и разрабатывать общие стандарты управления.

На практике уже несколько лет также заметна отчетливая тенденция интеграции систем управления сетями и системами в единые интегрированные продукты управления корпоративными сетями, например CA Unicenter TNG или TME-10 IBM/Tivoli. Наблюдается также интеграция систем управления телекоммуникационными сетями с системами управления корпоративными сетями.

7.1.2. Многоуровневое представление задач управления

Кроме описанного выше разделения задач управления на несколько функциональных групп, полезно разделять задачи управления на уровни в соответствии с иерархической организацией корпоративной сети. Корпоративная сеть строится иерархически, отражая иерархию самого предприятия и его задач. Нижний уровень сети составляют элементы сети - отдельные компьютеры, коммуникационные устройства, каналы передачи данных. На следующем уровне иерархии эти элементы образуют сети разного масштаба - сеть рабочей группы, сеть отдела, сеть отделения и, наконец, сеть предприятия в целом.

Для построения интегрированной системы управления разнородными элементами сети естественно применить многоуровневый иерархический подход. Это, в принципе, стандартный подход для построения большой системы любого типа и назначения - от государства до автомобильного завода. Применительно к системам управления сетями наиболее проработанным и эффективным для создания многоуровневой иерархической системы является стандарт Telecommunication Management Network (TMN), разработанный совместными усилиями ITU-T, ISO, ANSI и ETSI. Хотя этот стандарт и

предназначался изначально для телекоммуникационных сетей, но ориентация на использование общих принципов делает его полезным для построения любой крупной интегрированной системы управления сетями. Стандарты TMN состоят из большого количества рекомендаций ITU-T (и стандартов других организаций), но основные принципы модели TMN описаны в рекомендации M.3010.

На каждом уровне иерархии модели TMN решаются задачи одних и тех же пяти функциональных групп, рассмотренных выше (то есть управления конфигурацией, производительностью, ошибками, безопасностью и учетом), однако на каждом уровне эти задачи имеют свою специфику. Чем выше уровень управления, тем более общий и агрегированный характер приобретает собираемая о сети информация, а сугубо технический характер собираемых данных начинает по мере повышения уровня меняться на производственный, финансовый и коммерческий.

Модель TMN упрощенно можно представить в виде двухмерной диаграммы (рис. 7.1).

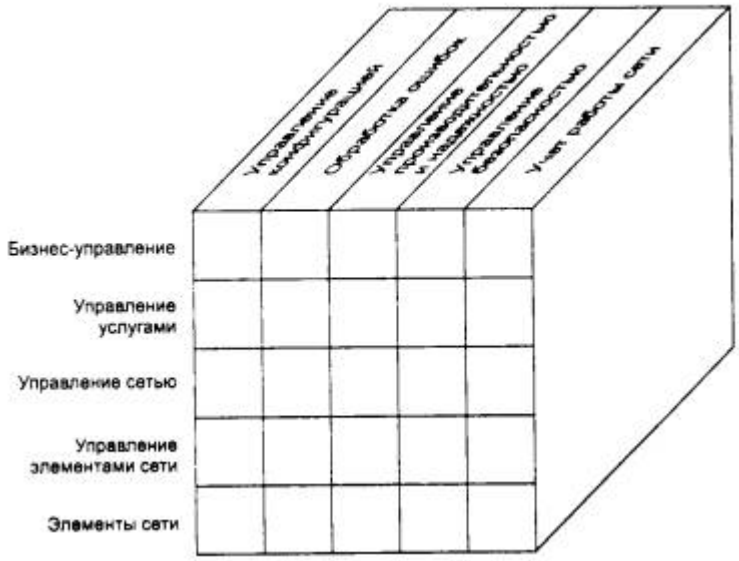

Рис. 7.1. Многоуровневое представление задач управления сетью

Нижний уровень - *уровень элементов сети (Network Element layer, NE)* - состоит из отдельных устройств сети: каналов, усилителей, оконечной аппаратуры, мультиплексоров, коммутаторов и т. п. Элементы могут содержать встроенные средства для поддержки управления - датчики, интерфейсы управления, а могут и представлять вещь в себе, требующую для связи с системой управления разработки специального оборудования - *устройств связи с объектом, УСО*. Современные технологии обычно имеют встроенные функции управления, которые позволяют выполнять хотя бы минимальные операции по контролю за состоянием устройства и за передаваемым устройством трафиком. Подобные функции встроены в технологии FDDI, ISDN, frame relay, SDH. В этом случае устройство всегда можно охватить системой управления, даже если оно не имеет специального блока управления, так как протокол технологии обязывает устройство поддерживать некоторые функции управления. Устройства, которые работают по протоколам, не имеющим встроенных функций контроля и управления, снабжаются отдельным блоком управления, который поддерживает один из двух наиболее распространенных протоколов управления - SNMP или CMIP. Эти протоколы относятся к прикладному уровню модели OSI.

Следующий уровень - *уровень управления элементами сети (network element management layer)* - представляет собой элементарные системы управления. Элементарные системы управления автономно управляют отдельными элементами сети - контролируют канал связи SDH, управляют коммутатором или мультиплексором. Уровень управления элементами изолирует верхние слои системы управления от деталей и особенностей управления конкретным оборудованием. Этот уровень ответственен за моделирование поведения оборудования и функциональных ресурсов нижележащей сети. Атрибуты этих моделей позволяют управлять различными аспектами поведения управляемых ресурсов. Обычно элементарные системы управления разрабатываются и поставляются производителями оборудования. Примерами таких систем могут служить системы управления CiscoView от Cisco Systems, Optivity от Bay Networks, RADView от RAD Data Communications и т. д.

Выше лежит *уровень управления сетью (Network management layer)*. Этот уровень координирует работу элементарных систем управления, позволяя контролировать конфигурацию составных каналов, согласовывать работу транспортных подсетей разных технологий и т. п. С помощью этого уровня сеть начинает работать как единое целое, передавая данные между своими абонентами.

Следующий уровень - *уровень управления услугами (Service management layer)* - занимается контролем и управлением за транспортными и информационными услугами, которые предоставляются конечным пользователям сети. В задачу этого уровня входит подготовка сети к предоставлению определенной услуги, ее активизация, обработка вызовов клиентов. Формирование услуги (service provisioning) заключается в фиксации в базе данных значений параметров услуги, например, требуемой средней пропускной способности, максимальных величин задержек пакетов, коэффициента готовности и т. п. В функции этого уровня входит также выдача уровню управления сетью задания на конфигурирование виртуального или физического канала связи для поддержания услуги. После формирования услуги данный уровень занимается контролем за качеством ее реализации, то есть за соблюдением сетью всех принятых на себя обязательств в отношении производительности и надежности транспортных услуг. Результаты контроля качества обслуживания нужны, в частности, для подсчета оплаты за пользование услугами клиентами сети. Например, в сети frame relay уровень управления услугами следит за заказанными пользователем значениями средней скорости CIR и согласованной пульсации Bc, фиксируя нарушения со стороны пользователя и сети.

Уровень бизнес-управления (Business management layer) занимается вопросами долговременного планирования сети с учетом финансовых аспектов деятельности организации, владеющей сетью. На этом уровне помесячно и поквартально подсчитываются доходы от эксплуатации сети и ее отдельных составляющих, учитываются расходы на эксплуатацию и модернизацию сети, принимаются решения о развитии сети с учетом финансовых возможностей. Уровень бизнес-управления обеспечивает для пользователей и поставщиков услуг возможность предоставления дополнительных услуг. Этот уровень является частным случаем уровня автоматизированной системы управления предприятием (АСУП), в то время как все нижележащие уровни соответствуют уровням автоматизированной системы управления технологическими процессами (АСУТП), для такого специфического типа предприятия, как телекоммуникационная или корпоративная сеть. Но если телекоммуникационная сеть действительно чаще всего является основой телекоммуникационной компании, то корпоративную сеть и обслуживающий ее персонал обычно трудно назвать предприятием. Тем не менее на некоторых западных фирмах корпоративная сеть выделена в автономное

производственное подразделение со своим бюджетом и со своими финансовыми договорами на обслуживание, которое данное подразделение заключает с основными производственными подразделениями предприятия.

7.1.3. Архитектуры систем управления сетями

Выделение в системах управления типовых групп функций и разбиение этих функций на уровни еще не дает ответа на вопрос, каким же образом устроены системы управления, из каких элементов они состоят и какие архитектуры связей этих элементов используются на практике.

Схема менеджер - агент

В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа.

Схема «менеджер - агент» представлена на рис. 7.2.

Рис. 7.2. Взаимодействие агента, менеджера и управляемого ресурса

Агент является посредником между управляемым ресурсом и основной управляющей программой-менеджером. Чтобы один и тот же менеджер мог управлять различными реальными ресурсами, создается некоторая модель управляемого ресурса, которая отражает только те характеристики ресурса, которые нужны для его контроля и управления. Например, модель маршрутизатора обычно включает такие характеристики, как количество портов, их тип, таблицу маршрутизации, количество кадров и пакетов протоколов канального, сетевого и транспортного уровней, прошедших через эти порты.

Менеджер получает от агента только те данные, которые описываются моделью ресурса. Агент же является некоторым экраном, освобождающим менеджера от ненужной информации о деталях реализации ресурса. Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например, строит зависимость загрузки порта от времени.

Для получения требуемых данных от объекта, а также для выдачи на него управляющих воздействий агент взаимодействует с реальным ресурсом некоторым нестандартным способом. Когда агенты встраиваются в коммуникационное оборудование, то разработчик

оборудования предусматривает точки и способы взаимодействия внутренних узлов устройства с агентом. При разработке агента для операционной системы разработчик агента пользуется теми интерфейсами, которые существуют в этой ОС, например интерфейсами ядра, драйверов и приложений. Агент может снабжаться специальными датчиками для получения информации, например датчиками релейных контактов или датчиками температуры.

Менеджер и агент должны располагать одной и той же моделью управляемого ресурса, иначе они не смогут понять друг друга. Однако в использовании этой модели агентом и менеджером имеется существенное различие. Агент наполняет модель управляемого ресурса текущими значениями характеристик данного ресурса, и в связи с этим модель агента называют базой данных управляющей информации - Management Information Base, MIB. Менеджер использует модель, чтобы знать о том, чем характеризуется ресурс, какие характеристики он может запросить у агента и какими параметрами можно управлять.

Менеджер взаимодействует с агентами по стандартному протоколу. Этот протокол должен позволять менеджеру запрашивать значения параметров, хранящихся в базе MIB, а также передавать агенту управляющую информацию, на основе которой тот должен управлять устройством. Различают управление inband, то есть по тому же каналу, по которому передаются пользовательские данные, и управление out-of-band, то есть вне канала, по которому передаются пользовательские данные. Например, если менеджер взаимодействует с агентом, встроенным в маршрутизатор, по протоколу SNMP, передаваемому по той же локальной сети, что и пользовательские данные, то это будет управление inband. Если же менеджер контролирует коммутатор первичной сети, работающий по технологии частотного уплотнения FDM, с помощью отдельной сети X.25, к которой подключен агент, то это будет управление out-of-band. Управление по тому же каналу, по которому работает сеть, более экономично, так как не требует создания отдельной инфраструктуры передачи управляющих данных. Однако способ out-of-band более надежен, так как он предоставляет возможность управлять оборудованием сети и тогда, когда какие-то элементы сети вышли из строя и по основным каналам оборудование недоступно. Стандарт многоуровневой системы управления TMN имеет в своем названии слово Network, подчеркивающее, что в общем случае для управления телекоммуникационной сетью создается отдельная управляющая сеть, которая обеспечивает режим out-of-band.

Обычно менеджер работает с несколькими агентами, обрабатывая получаемые от них данные и выдавая на них управляющие воздействия. Агенты могут встраиваться в управляемое оборудование, а могут и работать на отдельном компьютере, связанном с управляемым оборудованием по какому-либо интерфейсу. Менеджер обычно работает на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы.

Модель менеджер - агент лежит в основе таких популярных стандартов управления, как стандарты Internet на основе протокола SNMP и стандарты управления ISO/OSI на основе протокола CMIP.

Агенты могут отличаться различным уровнем интеллекта - они могут обладать как самым минимальным интеллектом, необходимым для подсчета проходящих через оборудование кадров и пакетов, так и весьма высоким, достаточным для выполнения самостоятельных действий по выполнению последовательности управляющих действий в аварийных

ситуациях, построению временных зависимостей, фильтрации аварийных сообщений и т. п.

Структуры распределенных систем управления

В крупной корпоративной сети полностью централизованная система управления, построенная на базе единственного менеджера, вряд ли будет работать хорошо по нескольким причинам. Во-первых, такой вариант не обеспечивает необходимой масштабируемости по производительности, так как единственный менеджер вынужден будет обрабатывать весь поток сообщений от всех агентов, что при нескольких тысячах управляемых объектов потребует очень высокопроизводительной платформы для работы менеджера и перегрузит служебной управляющей информацией каналы передачи данных в той сети, где будет расположен менеджер. Во-вторых, такое решение не обеспечит необходимого уровня надежности, так как при отказе единственного менеджера будет потеряно управление сетью. В-третьих, в большой распределенной сети целесообразно располагать в каждом географическом пункте отдельным оператором или администратором, управляющим своей частью сети, а это удобнее реализовать с помощью отдельных менеджеров для каждого оператора.

Схема «менеджер - агент» позволяет строить достаточно сложные в структурном отношении распределенные системы управления.

Обычно распределенная система управления включает большое количество связок менеджер - агент, которые дополняются рабочими станциями операторов сети, с помощью которых они получают доступ к менеджерам (рис. 7.3).

Каждый агент собирает данные и управляет определенным элементом сети. Менеджеры, иногда также называемые серверами системы управления, собирают данные от своих агентов, обобщают их и хранят в базе данных. Операторы, работающие за рабочими станциями, могут соединиться с любым из менеджеров и с помощью графического интерфейса просмотреть данные об управляемой сети, а также выдать менеджеру некоторые директивы по управлению сетью или ее элементами.

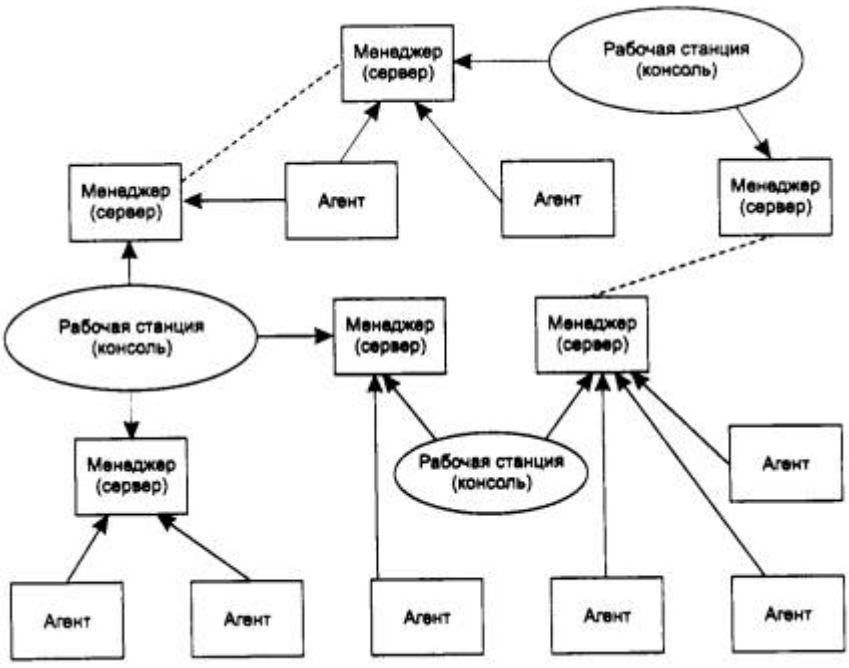

Рис. 7.3. Распределенная система управления на основе нескольких менеджеров и рабочих станций

Наличие нескольких менеджеров позволяет распределить между ними нагрузку по обработке данных управления, обеспечивая масштабируемость системы.

Как правило, связи между агентами и менеджерами носят более упорядоченный характер, чем тот, который показан на рис. 7.3. Чаще всего используются два подхода к их соединению - одноранговый (рис. 7.4) и иерархический (рис. 7.5).

Рис. 7.4. Одноранговые связи между менеджерами

Рис. 7.5. Иерархические связи между менеджерами

В случае одноранговых связей каждый менеджер управляет своей частью сети на основе информации, получаемой от нижележащих агентов. Центральный менеджер отсутствует. Координация работы менеджеров достигается за счет обмена информацией между базами данных каждого менеджера.

Одноранговое построение системы управления сегодня считается неэффективным и устаревшим. Обычно оно вызвано тем обстоятельством, что элементарные системы управления построены как монолитные системы, которые первоначально не были ориентированы на модульность системы (например, многие системы управления, разработанные производителями оборудования, не поддерживают стандартные интерфейсы для взаимодействия с другими системами управления). Затем эти менеджеры

нижнего уровня стали объединяться для создания интегрированной системы управления сетью, но связи между ними оказалось возможным создавать только на уровне обмена между базами данных, что достаточно медленно. Кроме того, в базах данных таких менеджеров накапливается слишком детальная информация об управляемых элементах сети (так как первоначально эти менеджеры разрабатывались как менеджеры нижнего уровня), вследствие чего такая информация малопригодна для координации работы всей сети в целом. Такой подход к построению системы управления называется подходом «снизу вверх».

Гораздо более гибким является иерархическое построение связей между менеджерами. Каждый менеджер нижнего уровня выполняет также функции агента для менеджера верхнего уровня. Такой агент работает уже с гораздо более укрупненной моделью (MIB) своей части сети, в которой собирается именно та информация, которая нужна менеджеру верхнего уровня для управления сетью в целом. Обычно для разработки моделей сети на разных уровнях проектирование начинают с верхнего уровня, на котором определяется состав информации, требуемой от менеджеров-агентов более низкого уровня, поэтому такой подход назван подходом «сверху вниз». Он сокращает объемы информации, циркулирующей между уровнями системы управления, и приводит к гораздо более эффективной системе управления.

Модель TMN в наибольшей степени соответствует иерархической архитектуре связей между менеджерами, хотя известны реализации принципов TMN и в одноуровневых архитектурах.

Платформенный подход

При построении систем управления крупными локальными и корпоративными сетями обычно используется платформенный подход, когда индивидуальные программы управления разрабатываются не «с нуля», а используют службы и примитивы, предоставляемые специально разработанным для этих целей программным продуктом - платформой. Примерами платформ для систем управления являются такие известные продукты, как *HP OpenView, SunNet Manager и Sun Soltice, Cdbletron Spectrum, IMB/Tivoli TMN10.*

Эти платформы создают общую операционную среду для приложений системы управления точно так же, как универсальные операционные системы, такие как Unix или Windows NT, создают операционную среду для приложений любого типа, таких как MS Word, Oracle и т. п. Платформа обычно включает поддержку протоколов взаимодействия менеджера с агентами - SNMP и реже CMIP, набор базовых средств для построения менеджеров и агентов, а также средства графического интерфейса для создания консоли управления. В набор базовых средств обычно входят функции, необходимые для построения карты сети, средства фильтрации сообщений от агентов, средства ведения базы данных. Набор интерфейсных функций платформы образует интерфейс прикладного программирования (API) системы управления. Пользуясь этим API, разработчики из третьих фирм создают законченные системы управления, которые могут управлять специфическим оборудованием в соответствии с пятью основными группами функций.

Обычно платформа управления поставляется с каким-либо универсальным менеджером, который может выполнять некоторые базовые функции управления без программирования. Чаще всего к этим функциям относятся функции построения карты сети (группа Configuration Management), а также функции отображения состояния

управляемых устройств и функции фильтрации сообщений об ошибках (группа Fault Management). Например, одна из наиболее популярных платформ HP OpenView поставляется с менеджером Network Node Manager, который выполняет перечисленные функции.

Чем больше функций выполняет платформа, тем лучше. В том числе и таких, которые нужны для разработки любых аспектов работы приложений, прямо не связанных со спецификой управления. В конце концов, приложения системы управления - это прежде всего приложения, а потом уже приложения системы управления. Поэтому полезны любые средства, предоставляемые платформой, которые ускоряют разработку приложений вообще и распределенных приложений в частности.

Компании, которые производят коммуникационное оборудование, разрабатывают дополнительные менеджеры для популярных платформ, которые выполняют функции управления оборудованием данного производителя более полно. Примерами таких менеджеров могут служить менеджеры системы Optivity компании Bay Networks и менеджеры системы Trancsend компании 3Com, которые могут работать в среде платформ HP OpenView и SunNet Manager.

Выводы

- Желательно, чтобы системы управления сетями выполняли все пять групп функций, определенных стандартами ISO/ITU-T для систем управления объектами любого типа.
- Система управления большой сетью должна иметь многоуровневую иерархическую структуру в соответствии со стандартами Telecommunication Management Network (TMN), позволяющую объединить разрозненные системы управления элементами сети в единую интегрированную систему.
- В основе всех систем управления сетями лежит схема «агент - менеджер». Эта схема использует абстрактную модель управляемого ресурса, называемую базой управляющей информации - Management Information Base, MIB.
- Агент взаимодействует с управляемым ресурсом по нестандартному интерфейсу, а с менеджером - по стандартному протоколу через сеть.
- В больших системах управления используется несколько менеджеров, которые взаимодействуют друг с другом по одной из двух схем - одноранговой и иерархической.
- Иерархическая схема взаимодействия менеджеров соответствует стандартам TMN и является более перспективной.
- При построении систем управления активно используется платформенный подход. Платформа системы управления выполняет для менеджеров роль операционной системы для обычных приложений, так как обеспечивает разработчика менеджеров набором полезных системных вызовов общего для любой системы управления назначения.

7.2. Стандарты систем управления

7.2.1. Стандартизуемые элементы системы управления

При формализации схемы «менеджер - агент» могут быть стандартизованы следующие аспекты ее функционирования:

- протокол взаимодействия агента и менеджера;
- интерфейс «агент - управляемый ресурс»;
- интерфейс «агент - модель управляемого ресурса»;
- интерфейс «менеджер - модель управляемого ресурса»;
- справочная система о наличии и местоположении агентов и менеджеров, упрощающая построение распределенной системы управления;
- язык описания моделей управляемых ресурсов, то есть язык описания MIB;
- схема наследования классов моделей объектов (дерево наследования), которая позволяет строить модели новых объектов на основе моделей более общих объектов, например, модели маршрутизаторов на основе модели обобщенного коммуникационного устройства;
- схема иерархических отношений моделей управляемых объектов (дерево включения), которая позволяет отразить взаимоотношения между отдельными элементами реальной системы, например, принадлежность модулей коммутации определенному коммутатору или отдельных коммутаторов и концентраторов определенной подсети.

Существующие стандарты на системы управления отличаются тем, что в них может быть стандартизованы не все перечисленные выше аспекты схемы «менеджер - агент».

В стандартах систем управления как минимум стандартизуется некоторый способ формального описания моделей управляемых объектов, а также определяется протокол взаимодействия между менеджером и агентом.

Сегодня на практике применяются два семейства стандартов управления сетями - стандарты Internet, построенные на основе протокола SNMP (Simple Network Management Protocol), и международные стандарты ISO/ITU-T, использующие в качестве протокола взаимодействия агентов и менеджеров протокол CMIP (Common Management Information Protocol).

Стандарты систем управления, основанных на протоколе SNMP, формализуют минимум аспектов системы управления, а стандарты ISO/ITU-T - максимум аспектов, как и большинство стандартов, разработанных ITU-T. Традиционно, в локальных и корпоративных сетях применяются в основном системы управления на основе SNMP, а стандарты ISO/ITU-T и протокол CMIP находят применение в телекоммуникационных сетях.

7.2.2. Стандарты систем управления на основе протокола SNMP

Концепции SNMP-управления

В системах управления, построенных на основе протокола SNMP, стандартизуются следующие элементы:

- протокол взаимодействия агента и менеджера;
- язык описания моделей MIB и сообщений SNMP - язык абстрактной синтаксической нотации ASN.1 (стандарт ISO 8824:1987, рекомендации ITU-T X.208);
- несколько конкретных моделей MIB (MIB-I, MIB-II, RMON, RMON 2), имена объектов которых регистрируются в дереве стандартов ISO. Все остальное отдается на откуп разработчику системы управления. Протокол SNMP и тесно связанная с

ним концепция SNMP MIB были разработаны для управления маршрутизаторами Internet как временное решение. Но, как это часто бывает со всем временным, простота и эффективность решения обеспечили успех этого протокола, и сегодня он используется при управлении практически любыми видами оборудования и программного обеспечения вычислительных сетей. И хотя в области управления телекоммуникационными сетями наблюдается устойчивая тенденция применения стандартов ITU-T, в которые входит протокол CMIP, и здесь имеется достаточно много примеров успешного использования SNMP-управления. Агенты SNMP встраиваются в аналоговые модемы, модемы ADSL, коммутаторы ATM и т. д.

SNMP - это протокол прикладного уровня, разработанный для стека TCP/IP, хотя имеются его реализации и для других стеков, например IPX/SPX. Протокол SNMP используется для получения от сетевых устройств информации об их статусе, производительности и других характеристиках, которые хранятся в базе данных управляющей информации MIB (Management Information Base). Простота SNMP во многом определяется простотой MIB SNMP, особенно их первых версий MIB I и MIB II. Кроме того, сам протокол SNMP также весьма несложен.

Существуют стандарты, определяющие структуру MIB, в том числе набор типов ее объектов, их имена и допустимые операции над этими объектами (например, считать»).

Древовидная структура MIB содержит обязательные (стандартные) поддеревья, а также в ней могут находиться частные (private) поддеревья, позволяющие изготовителю интеллектуальных устройств управлять какими-либо специфическими функциями устройства на основе специфических объектов MIB.

Агент в протоколе SNMP - это обрабатывающий элемент, который обеспечивает менеджерам, размещенным на управляющих станциях сети, доступ к значениям переменных MIB и тем самым дает им возможность реализовывать функции по управлению и наблюдению за устройством.

Основные операции по управлению вынесены в менеджер, а агент SNMP выполняет чаще всего пассивную роль, передавая в менеджер по его запросу значения накопленных статистических переменных. При этом устройство работает с минимальными издержками на поддержание управляющего протокола. Оно использует почти всю свою вычислительную мощность для выполнения своих основных функций маршрутизатора, моста или концентратора, а агент занимается сбором статистики и значений переменных состояния устройства и передачей их менеджеру системы управления.

Примитивы протокола SNMP

SNMP - это протокол типа «запрос-ответ», то есть на каждый запрос, поступивший от менеджера, агент должен передать ответ. Особенностью протокола является его чрезвычайная простота - он включает в себя всего несколько команд.

- Команда Get-request используется менеджером для получения от агента значения какого-либо объекта по его имени.
- Команда GetNext-request используется менеджером для извлечения значения следующего объекта (без указания его имени) при последовательном просмотре таблицы объектов.

- С помощью команды Get-response агент SNMP передает менеджеру ответ на команды Get-request или GetNext-request.
- Команда Set используется менеджером для изменения значения какого-либо объекта. С помощью команды Set происходит собственно управление устройством. Агент должен понимать смысл значений объекта, который используется для управления устройством, и на основании этих значений выполнять реальное управляющее воздействие - отключить порт, приписать порт определенной VLAN и т. п. Команда Set пригодна также для установки условия, при выполнении которого агент SNMP должен послать менеджеру соответствующее сообщение. Может быть определена реакция на такие события, как инициализация агента, рестарт агента, обрыв связи, восстановление связи, неверная аутентификация и потеря ближайшего маршрутизатора. Если происходит любое из этих событий, то агент инициализирует прерывание.
- Команда Trap используется агентом для сообщения менеджеру о возникновении особой ситуации.
- Версия SNMP v.2 добавляет к этому набору команду GetBulk, которая позволяет менеджеру получить несколько значений переменных за один запрос.

Структура SNMP MIB

На сегодня существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основными являются стандарты MIB-I и MIB-II, а также версия базы данных для удаленного управления RMON MIB. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Первоначальная спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II.

Версия MIB-I (RFC 1156) определяет 114 объектов, которые подразделяются на 8 групп.

- *System* - общие данные об устройстве (например, идентификатор поставщика, время последней инициализации системы).
- *Interfaces* - параметры сетевых интерфейсов устройства (например, их количество, типы, скорости обмена, максимальный размер пакета).
- *Address Translation Table* - описание соответствия между сетевыми и физическими адресами (например, по протоколу ARP).
- *Internet Protocol* - данные, относящиеся к протоколу IP (адреса IP-шлюзов, хостов, статистика о IP-пакетах).
- *ICMP* - данные, относящиеся к протоколу обмена управляющими сообщениями ICMP.
- *TCP* - данные, относящиеся к протоколу TCP (например, о TCP-соединениях)
- *UDP* - данные, относящиеся к протоколу UDP (число переданных, принятых и ошибочных UPD-дейтаграмм).
- *EGP* - данные, относящиеся к протоколу обмена маршрутной информацией Exterior Gateway Protocol, используемому в Internet (число принятых с ошибками и без ошибок сообщений).

Из этого перечня групп переменных видно, что стандарт MIB-I разрабатывался с жесткой ориентацией на управление маршрутизаторами, поддерживающими протоколы стека TCP/IP.

В версии MIB-II (RFC 1213), принятой в 1992 году, был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до 10.На рис. 7.6 приведен пример древовидной структуры базы объектов MIB-II. На нем показаны две из 10 возможных групп объектов - System (имена объектов начинаются с префикса Sys) и Interfaces (префикс if). Объект SysUpTimeсодержит значение продолжительности времени работы системы с момента последней перезагрузки, объект SysObjectID - идентификатор устройства (например, маршрутизатора).

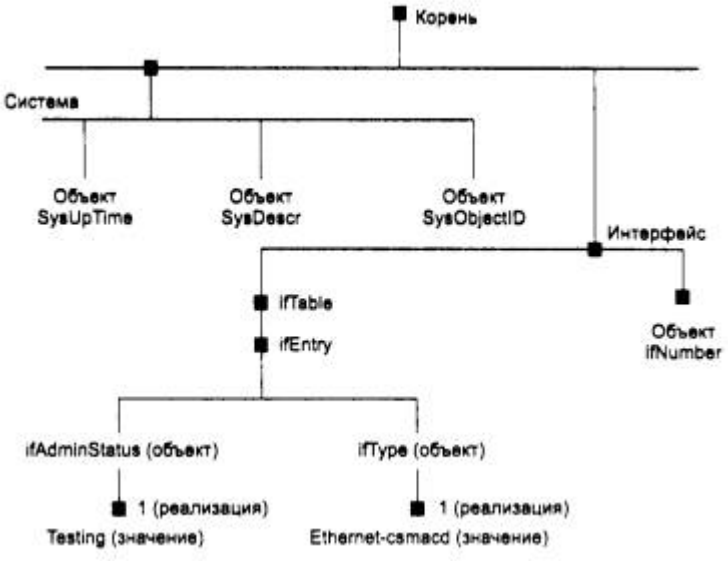

Рис. 7.6. Стандартное дерево MIB-II (фрагмент)

Объект ifNumber определяет количество сетевых интерфейсов устройства, а объект ifEntry является вершиной поддерева, описывающего один из конкретных интерфейсов устройства. Входящие в это поддерево объекты ifType и ifAdminStatus определяют соответственно тип и состояние одного из интерфейсов, в данном случае интерфейса Ethernet.

В число объектов, описывающих каждый конкретный интерфейс устройства, включены следующие.

- ifType - тип протокола, который поддерживает интерфейс. Этот объект принимает значения всех стандартных протоколов канального уровня, например rfc877-x25, ethemet-csmacd, iso88023-csmacd, iso88024-tokenBus, iso88025-tokenRlng и т. д.
- ifMtu - максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
- ifSpeed - пропускная способность интерфейса в битах в секунду (100 для Fast Ethernet).
- ifPhysAddress - физический адрес порта, для Fast Ethernet им будет MAC - адрес.
- ifAdminStatus - желаемый статус порта.
- up - готов передавать пакеты.
- down - не готов передавать пакеты.
- testing - находится в тестовом режиме.

- ifOperStatus - фактический текущий статус порта, имеет те же значения, что и ifAdminStatus.
- ifInOctets - общее количество байт, принятое данным портом, включая служебные, с момента последней инициализации SNMP-агента.
- ifInUcastPkts - количество пакетов с индивидуальным адресом интерфейса, доставленных протоколу верхнего уровня.
- IfInNUcastPkts - количество пакетов с широковещательным или мультивещательным адресом интерфейса, доставленных протоколу верхнего уровня.
- ifInDiscards - количество пакетов, которые были приняты интерфейсом, оказались корректными, но не были доставлены протоколу верхнего уровня, скорее всего из-за переполнения буфера пакетов или же по иной причине.
- ifin Errors - количество пришедших пакетов, которые не были переданы протоколу верхнего уровня из-за обнаружения в них ошибок.

Кроме объектов, описывающих статистику по входным пакетам, имеются аналогичные объекты, но относящиеся к выходным пакетам.

Как видно из описания объектов MIB-II, эта база данных не дает детальной статистики по характерным ошибкам кадров Ethernet, кроме этого, она не отражает изменение характеристик во времени, что часто интересует сетевого администратора.

Эти ограничения были впоследствии сняты новым стандартом на MIB - RMON MIB, который специально ориентирован на сбор детальной статистики по протоколу Ethernet, к тому же с поддержкой такой важной функции, как построение агентом зависимостей статистических характеристик от времени.

Форматы и имена объектов SNMP MIB

Для именования переменных базы MIB и однозначного определения их форматов используется дополнительная спецификация, называемая SMI - Structure of Management Information. Например, спецификация SMI включает в качестве стандартного имя IpAddress и определяет его формат как строку из 4 байт. Другой пример - имя Counter, для которого определен формат в виде целого числа в диапазоне от 0 до 2^{32}-1.

При описании переменных MIB и форматов протокола SNMP спецификация SMI опирается на формальный язык ASN.1, принятый ISO в качестве нотации для описания терминов коммуникационных протоколов (правда, многие коммуникационные протоколы, например IP, PPP или Ethernet, обходятся без этой нотации). Нотация ASN. 1 служит для установления однозначного соответствия между терминами, взятыми из стандартов, предназначенных для человеческого использования, и теми данными, которые передаются в коммуникационных протоколах аппаратурой. Достигаемая однозначность очень важна для гетерогенной среды, характерной для корпоративных сетей. Так, вместо того чтобы указать, что некоторая переменная протокола представляет собой целое число, разработчик протокола, использующий нотацию ASN.1, должен точно определить формат и допустимый диапазон переменной. В результате документация на MIB, написанная с помощью нотации ASN.1, может точно и механически транслироваться в форму кодов, характерных для сообщений протоколов.

Нотация ASN.1 похожа на другие метаязыки, например нормальную Бэкусову форму, используемую при описании языков программирования, в частности Алгола. Нотация

ASN.1 поддерживает базовый набор различных типов данных, таких как целое число, строка и т. п., а также позволяет конструировать из этих базовых типов составные данные - массивы, перечисления, структуры.

Существуют правила трансляции структур данных, описанных на ASN.1, в структуры данных языков программирования, например C++. Соответственно, имеются трансляторы, выполняющие эту работу. Примера описаний данных с помощью ASN.1 приведены ниже при описании протокольных блоков данных SNMP.

Нотация ASN.1 широко используется при описании многих стандартов OSI, в частности моделей управляемых объектов и структуры сообщений протокола CMIP.

Имена переменных MIB могут быть записаны как в символьном, так и в числовом форматах. Символьный формат используется для представления переменных в текстовых документах и на экране дисплея, а числовые имена - в сообщениях протокола SNMP. Например, символьному имени SysDescr соответствует числовое имя 1, а более точно 1.3.6.1.2.1.1.1.

Составное числовое имя объекта SNMP MIB соответствует полному имени этого объекта в дереве регистрации объектов стандартизации ISO. Разработчики протокола SNMP не стали использовать традиционный для стандартов Internet способ фиксации численных параметров протокола в специальном RFC, называемом «Assigned Numbers» (там описываются, например, численные значения, которые может принимать поле Protocol пакета IP, и т. п.). Вместо этого они зарегистрировали объекты баз MIB SNMP во всемирном дереве регистрации стандартов ISO, показанном на рис. 7.7.

Как и в любых сложных системах, пространство имен объектов ISO имеет древовидную иерархическую структуру, причем на рис. 7.7 показана только его верхняя часть. От корня этого дерева отходят три ветви, соответствующие стандартам, контролируемым ISO, ITU и совместно ISO-ITU. В свою очередь, организация ISO создала ветвь для стандартов, создаваемых национальными и международными организациями (ветвь огд). Стандарты Internet создавались под эгидой Министерства обороны США (Departament of Defence, DoD), поэтому стандарты MIB попали в поддерево dod-internet, а далее, естественно, в группу стандартов управления сетью - ветвь mgmt. Объекты любых стандартов, создаваемых под эгидой ISO, однозначно идентифицируются составными символьными именами, начинающимися от корня этого дерева. В сообщениях протоколов символьные имена не используются, а применяются однозначно соответствующие им составные числовые имена. Каждая ветвь дерева имен объектов нумеруется в дереве целыми числами слева направо, начиная с единицы, и эти числа и заменяют символьные имена. Поэтому полное символьное имя объекта MIB имеет вид: iso.org.dod.internet.mgmt.mib, а полное числовое имя: 1.3.6.1.2.1.

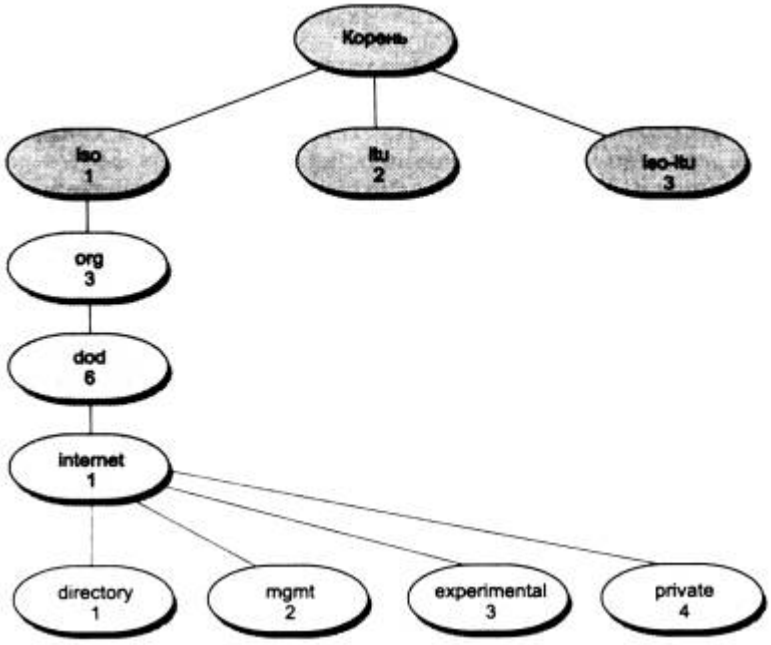

Рис. 7.7. Пространство имен объектов ISO

Группа объектов private (4) зарезервирована за стандартами, создаваемыми частными компаниями, например Cisco, Hewlett-Packard и т. п. Это же дерево регистрации используется для именования классов объектов CMIP и TMN.

Соответственно, каждая группа объектов MIB-I и MIB-II также имеет кроме кратких символьных имен, приведенных выше, полные символьные имена и соответствующие им числовые имена. Например, краткое символьное имя группы System имеет полную форму iso.org.dod.internet.mgmt.mib.system, а ее соответствующее числовое имя - 1.3.6.1.2.1. Часть дерева имен ISO, включающая группы объектов MIB, показана на рис. 7.8.

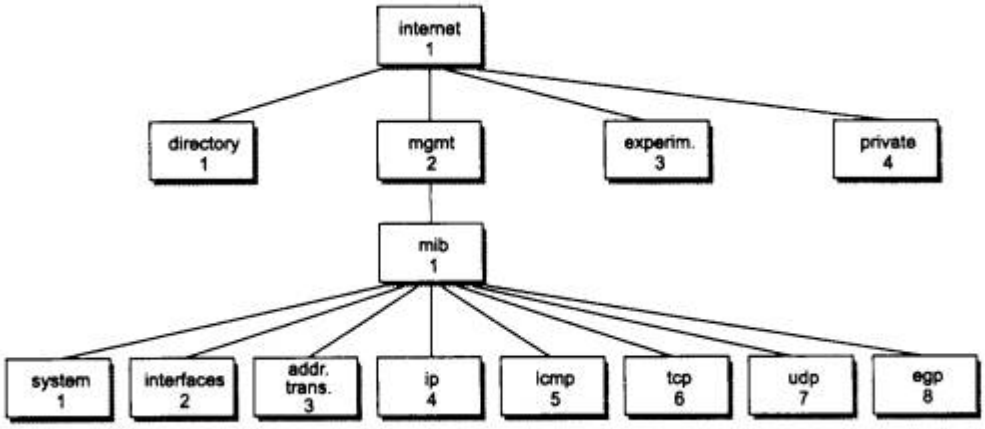

Рис. 7.8. Часть дерева имен ISO, включающая группы объектов MIB-I

Формат сообщений SNMP

Протокол SNMP обслуживает передачу данных между агентами и станцией, управляющей сетью. SNMP использует дейтаграммный транспортный протокол UDP, не обеспечивающий надежной доставки сообщений. Протокол, организующий надежную передачу дейтаграмм на основе соединений TCP, весьма загружает управляемые

устройства, которые на момент разработки протокола SNMP были не очень мощные, поэтому от услуг протокола TCP решили отказаться.

SNMP часто рассматривают только как решение для управления сетями TCP/IP. Хотя SNMP чаще всего и работает над UDP (он может также работать и над TCP), он может работать и над транспортными сетевыми протоколами стека OSI - TPO, TP4, CNLS, а также над протоколами MAC - уровня. Растет поддержка протокола SNMP и в других транспортных средах. Например, фирма Novell начала поддерживать протокол SNMP с версии NetWare 3.11, а некоторые производители оборудования (например, Bay Networks) реализуют в своих устройствах передачу сообщений SNMP с помощью как IP, так и IPX.

Сообщения SNMP, в отличие от сообщений многих других коммуникационных протоколов, не имеют заголовков с фиксированными полями. В соответствии с нотацией ASN.1 сообщение SNMP состоит из произвольного количества полей, и каждое поле предваряется описателем его типа и размера.

Любое сообщение SNMP состоит из трех основных частей: версии протокола (version), идентификатора общности (community), используемого для группирования устройств, управляемых определенным менеджером, и области данных, в которой собственно и содержатся описанные выше команды протокола, имена объектов и их значения. Область данных делится на блоки данных протокола (Protocol Data Unit, PDU).

Общий формат сообщения SNMP в нотации ASN.1 выглядит следующим образом:>

```
SNMP-Message ::=

SEQUENCE {

version INTEGER {

version-1 (0)

},

community

OCTET STRING,

SNMP-PDUs

ANY

}
```

Область данных может содержать пять различных типов PDU, соответствующих пяти командам протокола SNMP:

```
SNMP-PDUs :: =

CHOICE {
```

get-request

GetRequest-PDU,

get-next-request

GetNextRequest-PDU,

get-response

GetResponse-PDU,

set-request

SetRequest-PDU,

trap

Trap-PDU,

}

И наконец, для каждого типа PDU имеется определение его формата. Например, формат блока GetRequest-PDU описан следующим образом:

GetRequest-PDU ::=

IMPLICIT SEQUENCE {

request-id

RequestID,

error-status

ErrorStatus,

error-index

ErrorIndex,

variable-bindings

VarBindList

}

Далее стандарт SNMP определяет соответственно формат переменных блока GetRequest-PDU. Переменная Request ID - это 4-байтовое целое число (используется для установления соответствия ответов запросам), ErrorStatus и ErrorIndex - это однобайтовые целые, которые в запросе должны быть установлены в 0. VarBindList - это

список числовых имен объектов, значениями которых интересуется менеджер. В нотации ASN.1 этот список состоит из пар «имя - значение». При запросе значение переменной должно быть установлено в null.

Вот пример сообщения протокола SNMP, которое представляет собой запрос о значении объекта SysDescr (числовое имя 1.3.6.1.2.1.1.1).

30	29	02	01	00			
SEQUENCE	len = 41	INTEGER	len=1	vers = 0			
04	06	70	75	62	6C	69	63
string	len = 6	p	u	b	l	i	c
A0	1C	02	04	05	AE	66	02
getreq	len = 28	INTEGER	len = 4	--------	requested ID	--------	--------
02	01	00	02	01	00		
INTEGER	len = 1	status	INTEGER	len = 1	error	index	
30	0E	30	0C	06	08		
SEQUENCE	len = 14	SEQUENCE	len = 12	objectid	len = 8		
2B	06	01	02	01	01	01	00
1,3	6	1	2	1	1	1	0
05	00						
null	len = 0						

Как видно из описания, сообщение начинается с кода 30 (все коды шестнадцатеричные), который соответствует ключевому слову SEQUENCE (последовательность). Длина последовательности указывается в следующем байте (41 байт). Далее следует целое число длиной 1 байт - это версия протокола SNMP (в данном случае О, то есть SNMP v.l, а 1 означала бы SNMP v.2). Поле community имеет типstring (строка символов) длиной в 6 байт со значением public. Остальную часть сообщения составляет блок данных GetRequest-PDU . То, что это операция Get-request, говорит код АО (это значение определено в протоколе SNMP, а не в нотации ASN.1), а общая длина блока данных - 28 байт. В соответствии со структурой блока Getrequest-PDU, далее идет идентификатор запроса (он определен как целое 4-байтовое число). Затем в блоке следуют два однобайтовых целых числа статуса и индекса ошибки, которые в запросе установлены в 0. И наконец, завершает сообщение список объектов, состоящий из одной пары - имени 1.3.6.1.2.1.1.1.0 и значения null.

Спецификация RMON MIB

Новейшим добавлением к функциональным возможностям SNMP является спецификация RMON, которая обеспечивает удаленное взаимодействие с базой MIB. До появления RMON протокол SNMP не мог использоваться удаленным образом, он допускал только локальное управление устройствами. База RMON MIB обладает улучшенным набором свойств для удаленного управления, так как содержит агрегированную информацию об устройстве, не требующую передачи по сети больших объемов информации. Объекты RMON MIB включают дополнительные счетчики ошибок в пакетах, более гибкие средства анализа трендов и статистики, более мощные средства фильтрации для захвата и анализа отдельных пакетов, а также более сложные условия установления сигналов предупреждения. Агенты RMON MIB более интеллектуальны по сравнению с агентами

MIB-I или MIB-II и выполняют значительную часть работы по обработке информации об устройстве, которую раньше выполняли менеджеры. Эти агенты могут располагаться внутри различных коммуникационных устройств, а также быть выполнены в виде отдельных программных модулей, работающих на универсальных персональных компьютерах и ноутбуках.

Объекту RMON присвоен номер 16 в наборе объектов MIB, а сам объект RMON объединяет 10 групп следующих объектов.

- Statistics - текущие накопленные статистические данные о характеристиках пакетов, количестве коллизий и т. п.
- History - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
- Alarms - пороговые значения статистических показателей, при превышении которых агент RMON посылает сообщение менеджеру.
- Hosts - данные о хостах сети, в том числе и о их MAC - адресах.
- HostTopN - таблица наиболее загруженных хостов сети.
- Traffic Matrix - статистика об интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы.
- Filter - условия фильтрации пакетов.
- Packet Capture - условия захвата пакетов.
- Event - условия регистрации и генерации событий.

Данные группы пронумерованы в указанном порядке, поэтому, например, группа Hosts имеет числовое имя 1.3.6.1.2.1.16.4.

Десятую группу составляют специальные объекты протокола Token Ring.

Всего стандарт RMON MIB определяет около 200 объектов в 10 группах, зафиксированных в двух документах - RFC 1271 для сетей Ethernet и RFC 1513 для сетей Token Ring.

Отличительной чертой стандарта RMON MIB является его независимость от протокола сетевого уровня (в отличие от стандартов MIB-I и MIB-II, ориентированных на протоколы TCP/IP). Поэтому он удобен для гетерогенных сред, использующих различные протоколы сетевого уровня.

Рассмотрим более подробно группу Statistics, которая определяет, какую информацию о кадрах (называемых в стандарте пакетами) Ethernet может предоставить агент RMON. Группа History основана на объектах группы Statistics, так как ее объекты просто позволяют строить временные ряды для объектов группы Statistics.

В группу Statistics входят наряду с некоторыми другими следующие объекты.

- etherStatsDropEvents - общее число событий, при которых пакеты были проигнорированы агентом из-за недостатка его ресурсов. Сами пакеты при этом не обязательно были потеряны интерфейсом.
- etherStatsOrtets - общее число байт (включая ошибочные пакеты), принятых из сети (исключая преамбулу н включая байты контрольной суммы).
- etherStatsPkts - общее число полученных пакетов (включая ошибочные).

- etherStatsBroadcastPkts - общее число хороших пакетов, которые были посланы по широковещательному адресу.
- etherStatsMulticastPkts - общее число хороших пакетов, полученных по мультивещательному адресу.
- etherStatsCRCAlign Errors - общее число полученных пакетов, которые имели длину (исключая преамбулу) между 64 и 1518 байт, не содержали целое число байт (alignment error) или имели неверную контрольную сумму (FCS error).
- etherStatsUndersizePkts - общее число пакетов, которые имели длину меньше, чем 64 байт, но были правильно сформированы.
- etherStatsOversizePkts - общее число полученных пакетов, которые имели длину больше, чем 1518 байт, но были тем не менее правильно сформированы.
- etherStatsFragments - общее число полученных пакетов, которые не состояли из целого числа байт или имели неверную контрольную сумму и имели к тому же длину, меньшую 64 байт.
- etherStatsJabbers - общее число полученных пакетов, которые не состояли из целого числа байт или имели неверную контрольную сумму и имели к тому же длину, большую 1518 байт.
- etherStatsCollisions - наилучшая оценка числа коллизий на данном сегменте Ethernet.
- etherStatsPkts640ctets - общее количество полученных пакетов (включая плохие) размером 64 байт.
- etherStatsPkts65to1270ctets - общее количество полученных пакетов (включая плохие) размером от 65 до 127 байт.
- etherStatsPktsl28to2550ctets - общее количество полученных пакетов (включая плохие) размером от 128 до 255 байт.
- etherStatsPkts256to5110ctets - общее количество полученных пакетов (включая плохие) размером от 256 до 511 байт.
- etherStatsPkts512tol0230ctets - общее количество полученных пакетов (включая плохие) размером от 512 до 1023 байт.
- etherStatsPktsl024tol5180ctets - общее количество полученных пакетов (включая плохие) размером от 1024 до 1518 байт.

Как видно из описания объектов, с помощью агента RMON, встроенного в повторитель или другое коммуникационное устройство, можно провести очень детальный анализ работы сегмента Ethernet или Fast Ethernet. Сначала можно получить данные о встречающихся в сегменте типах ошибок в кадрах, а затем целесообразно собрать с помощью группыHistory зависимости интенсивности этих ошибок от времени (в том числе и привязав их ко времени). После анализа временных зависимостей часто уже можно сделать некоторые предварительные выводы об источнике ошибочных кадров и на этом основании сформулировать более тонкие условия захвата кадров со специфическими признаками (задав условия в группеFilter), соответствующими выдвинутой версии. После этого можно провести еще более детальный анализ за счет изучения захваченных кадров, извлекая их из объектов группыPacket Capture.

Позже был принят стандарт RMON 2, который распространяет идеи интеллектуальной RMON MIB на протоколы верхних уровней, выполняя часть работы анализаторов протоколов.

Недостатки протокола SNMP

Протокол SNMP служит основой многих систем управления, хотя имеет несколько принципиальных недостатков, которые перечислены ниже.

- Отсутствие средств взаимной аутентификации агентов и менеджеров. Единственным средством, которое можно было бы отнести к средствам аутентификации, является использование в сообщениях так называемой «строки сообщества» - «community string». Эта строка передается по сети в открытой форме в сообщении SNMP и служит основой для деления агентов и менеджеров на «сообщества», так что агент взаимодействует только с теми менеджерами, которые указывают в поле community string ту же символьную строку, что и строка, хранящаяся в памяти агента. Это, безусловно, не способ аутентификации, а способ структурирования агентов и менеджеров. Версия SNMP v.2 должна была ликвидировать этот недостаток, но в результате разногласий между разработчиками стандарта новые средства аутентификации хотя и появились в этой версии, но как необязательные.
- Работа через ненадежный протокол UDP (а именно так работает подавляющее большинство реализации агентов SNMP) приводит к потерям аварийных сообщений (сообщений trap) от агентов к менеджерам, что может привести к некачественному управлению. Исправление ситуации путем перехода на надежный транспортный протокол с установлением соединений чревато потерей связи с огромным количеством встроенных агентов SNMP, имеющихся в установленном в сетях оборудовании. (Протокол CMIP изначально работает поверх надежного транспорта стека OSI и этим недостатком не страдает.) Разработчики платформ управления стараются преодолеть эти недостатки. Например, в платформе HP 0V Telecom DM TMN, являющейся платформой для разработки многоуровневых систем управления в соответствии со стандартами TMN и ISO, работает новая реализация SNMP, организующая надежный обмен сообщениями между агентами и менеджерами за счет самостоятельной организации повторных передач сообщений SNMP при их потерях.

7.2.3. Стандарты управления OSI

Модель сетевого управления OSI - OSI Management Framework - определена в документе ISO/IEC 7498-4: Basic Reference Model, Part 4, Management Framework.Она является развитием общей семиуровневой модели взаимодействия открытых систем для случая, когда одна система управляет другой.

Документ ISO/IEC 7498-4 состоит из следующих основных разделов.

- Термины и общие концепции.
- Модель управления системами.
- Информационная модель.
- Функциональные области управления системами.
- Структура стандартов управления системами.

Функциональные области управления системами уже были рассмотрены в разделе 7.1, как имеющие общее значение для любых систем управления.

Стандарты ISO в области управления использует терминологию, которая частично совпадает с терминологией систем управления SNMP, а частично от нее отличается.

Как показано на рис. 7.9, обмен управляющей информацией с использованием протокола управления (Management Protocol) происходит между субъектами приложений управления системами (Systems Management Application Entities, SMAE). Субъекты SMAE расположены на прикладном уровне семиуровневой модели OSI и являются элементами службы управления. Под субъектом в модели OSI понимается активный в данный момент элемент протокола какого-либо уровня, участвующий во взаимодействии. Примерами SMAE являются агенты и менеджеры систем управления.

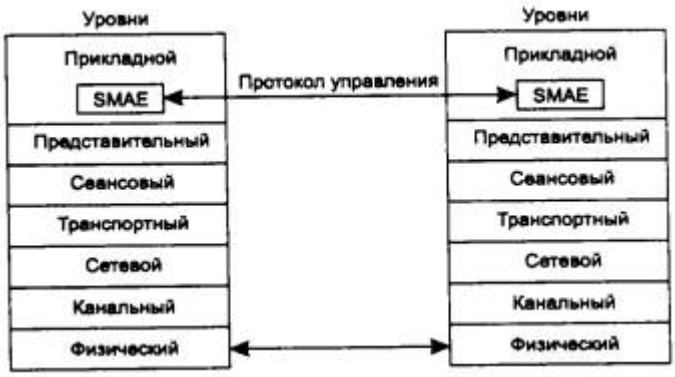

Рис. 7.9. Концепция SMAE

Агенты и менеджеры

Определения функций агентов и менеджеров в стандартах OSI достаточно хорошо согласуются с определениями систем SNMP, за некоторыми исключениями в терминологии. Сообщения, которые агент посылает менеджеру по своей инициативе, называются *уведомлениями - notifications.*

Например, если некоторый элемент сети X отказал, то менеджеру необходимо обновить свою базу данных конфигурации сети. Элемент X, который является для системы управления управляемым объектом (managed object), может послать уведомление агенту. Элемент X может находиться в той же управляемой системе, что и агент, или может находиться в другой системе. В свою очередь агент посылает уведомление менеджеру о том, что элемент X отказал. В соответствии с этим уведомлением менеджер обновляет базу данных конфигурации.

ПРИМЕЧАНИЕ В стандартах Internet под объектом понимается отдельный атрибут базы MIB, являющейся моделью управляемого ресурса, а в стандартах ISO объект обозначает всю модель управляемого ресурса.

Менеджер не только собирает и сопоставляет данные, получаемые от агентов, на основе этих данных он может также выполнять административные функции, управляя операциями удаленных агентов.

В стандартах OSI границы между менеджерами и агентами не очень четкие. Субъект SMAE, выполняющий в одном взаимодействии роль менеджера, может в другом взаимодействии выполнять роль агента, и наоборот.

Стандарты OSI не определяют способов взаимодействия агента с управляемыми объектами. Стандарты OSI также не говорят о том, как агент взаимодействует с управляемыми объектами, которые находятся за пределами управляемой системы, то есть объектами, с которыми нужно взаимодействовать через сеть. В таких случаях может потребоваться, например, чтобы один агент запросил данные о некотором объекте от другого агента. Порядок такого рода взаимодействия также не определяется стандартами OSI.

Чтобы менеджер и агент смогли взаимодействовать, каждый должен иметь определенные знания о другом. Эти знания модель OSI называет контекстом приложения (Application Context, AC). AC описывает элементы прикладного уровня стека OSI, которые используются агентами и менеджерами.

ПРИМЕЧАНИЕ Необходимо отметить, что стандарты управления OSI в значительной степени ориентированы на стек протоколов OSI (именно стек, а не модель OSI), так же как системы управления SNMP ориентированы на работу со стеком TCP/IP.

Прикладной уровень стека OSI включает несколько вспомогательных служб общего назначения, которые используются прикладными протоколами и пользовательскими приложениями (в том числе и приложениями управления) для автоматизации наиболее часто выполняемых действий. Это не законченные протоколы прикладного уровня, подобные протоколам ftp, telnet или NCP, с помощью которых пользователь сети может выполнить какое-то полезное действие, а вспомогательные системные функции, которые помогают разработчику прикладного протокола или приложения написать его программу компактно и эффективно. На прикладном уровне стека OSI существуют следующие вспомогательных службы.

- ACSE (Association Control Service Element). Отвечает за установление соединений между приложениями различных систем. Соединение (сессия, сеанс) на прикладном уровне OSI носит название ассоциации. Ассоциации бывают индивидуальными и групповыми (shared).
- RTSE (Reliable Transfer Service Element). Занимается поддержкой восстановления диалога, вызванного разрывом нижележащих коммуникационных служб, в рамках ассоциации.
- ROSE (Remote Operations Service Element). Организует выполнение программных функций на удаленных машинах (аналог службы вызова удаленных процедур RPC).

Протокол CMIP, используемый в стандартах OSI для взаимодействия между менеджерами и агентами, а также программные реализации менеджеров и агентов широко пользуются услугами данных вспомогательных служб, в особенности службы ROSE для вызова удаленных процедур.

Управление системами, управление уровнем и операции уровня

Основная модель управления OSI включает: управление системами, управление N-уровнем и операции N-уровня. Это разбиение на три области сделано для того, чтобы учесть все возможные ситуации, возникающие при управлении.

Управление системами имеет дело с управляемыми объектами на всех семи уровнях OSI, включая прикладной уровень. Оно основано на надежной передаче с установлением соединения управляющей информации между конечными системами. Необходимо подчеркнуть, что модель управления OSI не разрешает использования служб без установления соединения.

Управление N-уровнем ограничено управляемыми объектами какого-то определенного уровня семиуровневой модели. Протокол управления использует при этом коммуникационные протоколы нижележащих уровней. Управление N-уровнем полезно, когда нет возможности использовать все семь уровней OSI. В этом случае допускается пользоваться протоколом управления N-уровня, который строго предназначен для данного уровня. Примерами уровневого протокола управления являются протоколы управления для локальных сетей, разработанные институтом IEEE (SMT технологии FDDI), которые ограничены уровнями 1 и 2.

Наконец, *операции N-уровня* сводятся к мониторингу и управлению на основе управляющей информации, содержащейся в коммуникационных протоколах только данного уровня. Например, данные мониторинга сети, содержащиеся в кадрах STM-n технологии SDH, относятся к операциям N-уровня, а именно физического уровня.

Стандарты на управление N-уровнем и операции N-уровня не входят в набор стандартов управления OSI. Стандарты OSI рассматривают только управление системами с помощью полного семиуровневого стека.

Основная модель управления системами подразумевает выполнение управляющих операций и передачу уведомлений между одноранговыми системами, что означает необязательность жесткого распределения ролей на управляющие и управляемые системы. Эта модель облегчает реализацию распределенных аспектов управления. С другой стороны, допускается реализация одноранговых систем как управляющих и управляемых.

Информационная модель управления

Управляемый объект - это представление OSI о ресурсе в целях управления. Ресурс может быть описан как управляемый объект. Конкретный управляемый объект - это экземпляр (instance) некоторого класса управляемых объектов. Модель управления OSI широко использует объектно-ориентированный подход. Класс управляемых объектов - это набор свойств, которые могут быть обязательными или условными. С помощью описания одного класса управляемых объектов, например коммутаторов, можно создать другой класс управляемых объектов, например коммутаторов, поддерживающих технику VLAN, унаследовав все свойства класса коммутаторов, но добавив новые атрибуты.

Для управления ресурсами менеджер и агент должны быть осведомлены о деталях этих ресурсов. Детализация представления управляемых объектов, которые требуются для выполнения функций управления, хранится в репозитории, известном как Management Information Base (MIB). Базы MIB OSI хранят не только описания классов управляемых объектов, но и характеристики сети и ее элементов. Базы MIB содержат характеристики

каждой части управляемого оборудования и ресурсов. MIB также включает описание действий, которые могут выполняться на основе собранных данных или же вызываемые внешними командами. Базы MIB позволяют внешним системам опрашивать, изменять, создавать и удалять управляемые объекты (реальные ресурсы сети при этом, естественно, продолжают работать). Протокол CMIP и локальные интерфейсы управления обеспечивают доступ к этим возможностям.

MIB - это концептуальная модель, и она не имеет никакой связи со способом физического или логического хранения данных в ресурсе. Стандарты не определяют аспекты собственно хранения данных. Протоколы OSI определяют синтаксис информации, хранящейся в MIB, и семантику обмена данными.

Управляющие знания и деревья знаний

Крупная система управления обычно состоит из большого количества агентов и менеджеров. Для организации автоматического взаимодействия между менеджерами и агентами необходимо каким-то образом задать данные, содержащие характеристики агентов и менеджеров. Менеджеру необходимо знать о том, какие агенты работают в системе управления, их имена и сетевые адреса, поддерживаемые ими классы управляемых объектов и т. п. Агенту также необходима аналогичная информация о менеджерах, так как ему нужно отправлять по своей инициативе уведомления и отвечать на запросы менеджеров.

Такие данные называются в модели OSI *разделяемыми управляющими знаниями (shared management knowledge)* между менеджером и агентом. (В системах SNMP организация этих данных не стандартизована, и в каждой конкретной системе управления эти данные хранятся в индивидуальной форме).

Разделяемые управляющие знания должны быть известны до установления ассоциации между агентом и менеджером. Обычно они хранятся в каком-либо файле или распределенной базе данных и запрашиваются каждый раз, когда устанавливается ассоциация. Во время установления ассоциации происходит обмен разделяемыми управляющими знаниями.>

В OSI стандартизуются различные аспекты организации управляющих знаний и доступа к ним. Следование объектно-ориентированному подходу обусловило использование для хранения этих знаний специальных системных объектов.

Стандарт ISO 10164-16.2 определяет модель объектов управляющих знаний и классы таких объектов. Кроме того, определены функции работы с управляющими знаниями.

Имеются три типа управляющих знаний и, соответственно, три типа объектов, которые описывают эти знания.

- *Знания репертуара (Repertoire Knowledge)* описывают возможности управляемой системы, включающие перечень поддерживаемых классов управляемых объектов, поддерживаемые функции управления и именования. Знания репертуара помогают менеджеру идентифицировать возможности управляемых систем без доступа к ним.

- *Знания определений (Definition Knowledge)* включают формальные описания классов управляемых объектов, категории тестов, классов взаимосвязей и определения управляющей информации, понимаемой управляемой системой.
- *Знания об экземплярах (Instance Knowledge)* обеспечивают информацию о конкретных экземплярах управляемых объектов, имеющихся в управляемой системе.

Использование древовидных баз данных для хранения управляющих знаний

В системе управления знания о поддерживаемых классах объектов и о порожденных экземплярах объектов должны храниться в какой-либо форме, удобной для предоставления модулям системы управления доступа к этой информации. Архитектура управления OSI предусматривает несколько схем базы данных об управляемых объектах и их классах. Эти схемы обычно называют деревьями из-за иерархической организации информации. Существуют следующие деревья.

- *Дерево наследования (Inheritance Tree)*, называемое также деревом регистрации. Описывает отношения между базовыми и производными классами. Подчиненный класс наследует все характеристики суперкласса и дополняет их специфическими расширениями (дополнительными атрибутами, поведениями и действиями). Классы объектов OSI регистрируются в том же дереве, что и объекты MIB Internet. Дерево наследования может быть глобальным, то есть начинаться с корня, представляющего весь мир, или локальным, имеющим корень, соответствующий верхнему уровню объектов данной организации или сети. Все управляемые объекты OSI должны быть зарегистрированы в глобальном дереве ISO (в котором зарегистрированы объекты MIB-I, MIB-II, RMON MIB стандарта SNMP). Объекты, представляющие международные стандарты, регистрируются в международной ветви дерева, а частные модели, разработанные производителями систем управления, регистрируются в ветвях дерева, начинающихся с ветви private.
- *Дерево включений (Containment Tree)*. Описывает отношения включения управляемых объектов реальной системы.

ПРИМЕЧАНИЕ Между деревом исследования и деревом включений нет прямой связи. Например, в дереве включений объект «корпоративный концентратор» может включать объекты «интерфейс Ethernet» и «модуль удаленного доступа», которые представляют модели реальных модулей, установленных в слоты корпоративного концентратора. В то же время в дереве наследования класс объектов «интерфейсы Ethernet» подчинен классу объектов «интерфейсы», а класс объектов «модуль удаленного доступа» подчинен классу «коммуникационное оборудование третьего уровня», на основании которого он порожден.

- *Дерево имен (naming tree)* определяет способ именования объектов в системе управления. Объекты OSI могут иметь имена нескольких типов: относительное отличительное имя (Relative Distinguished Name, RDN), отличительное имя (Distinguished Name, DN), иногда называемое полным отличительным именем (Full Distinguished Name, FDN), и локальное отличительное имя (Local Distinguished Name, LDN). Эти имена связаны с деревом включений, так как определяют имена

объектов относительно включающих их объектов. Относительное имя, RDN, соответствует короткому имени, которое однозначно определяет объект среди множества других объектов, подчиненных тому же родительскому объекту. Например, имя interface_a является RDN-именем, уникально характеризующим объект среди объектов, подчиненных объекту node_a. Полное отличительное имя FDN представляет собой последовательность RDN-имен, начинающуюся в вершине глобального дерева имен, то есть дерева, описывающего некоторую глобальную сеть. Наконец, локальное отличительное имя - это последовательность RDN-имен, но начинающаяся не в глобальном корне, а в корне дерева имен локальной системы управления, отвечающей за часть глобального дерева имен данной сети.

Дерево имен обычно совмещается с деревом включений.

Пример дерева включений показан на рис. 7.10. Экземпляр управляемого объекта класса corp-conc (корпоративный концентратор) имеет имя B1, а также атрибут max-slotes, описывающий максимальное количество слотов данного класса концентраторов, равный в данном случае 14. В этот объект включено ряд других объектов: объекты класса repeator, switch и RAS, которые в свою очередь включают объекты типа interface, описывающие порты модулей концентратора.

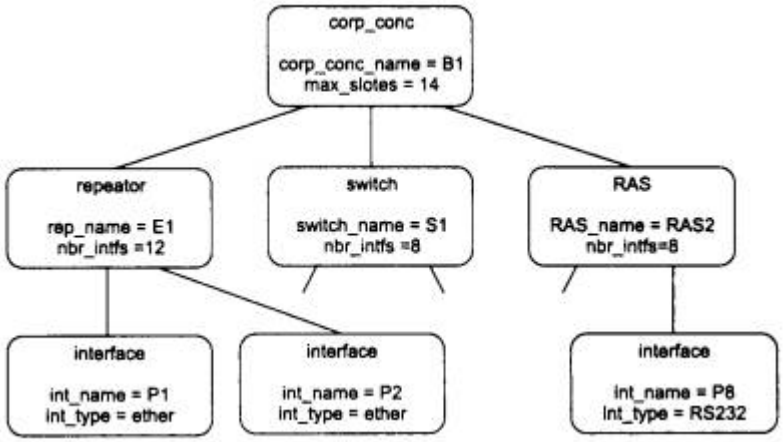

Рис. 7.10. Пример дерева включений

Имя класса объекта позволяет обратиться к описанию класса и узнать полный список атрибутов этого класса или ссылку на родительский класс, у которого наследуются все или некоторые атрибуты. Имя экземпляра объекта дает информацию о принадлежности конкретного модуля или интерфейса определенному коммуникационному устройству, например имя B1.E1.P2 определяет второй порт модуля повторителя E1, входящего в состав корпоративного концентратора B1.

Правила определения управляемых объектов

Классы управляемых объектов OSI должны определяться в соответствии со стандартом GDMO (Guidelines for the Definition of Managed Objects - Правила определения управляемых объектов), являющимся стандартом ISO 10165-4.

В GDMO определяется несколько шаблонов (templates) - пустых форм, которые заполняются для описания определенного класса управляемых объектов. В шаблоне

класса перечисляются комплекты свойств (PACKAGES), которые составляют класс. Шаблон комплекта свойств PACKAGE перечисляет Атрибуты, Группы атрибутов, Действия, Поведение и Уведомления , то есть свойства, сгруппированные для удобства описания класса объектов. Отношения наследования между классами описываются с помощью шаблона Связывание имен .

Атрибуты и Группы атрибутов определяют параметры объекта, которые можно читать и узнавать из них о состоянии объекта. СвойстваДействия описывают возможные управляющие воздействия, которые допускается применять к данному объекту - например, мультиплексировать несколько входных потоков в один выходной. Свойство Поведение описывает реакцию объекта на примененное к нему действие. Уведомления составляют набор сообщений, которые генерирует объект по своей инициативе.

Заполненные шаблоны GDMO определяют представление класса и его свойств.

Заполнение шаблонов выполняется в соответствии с нотацией ASN.1. В отличие от стандартов SNMP, использующих только подмножество типов данных ASN.1, в GDMO и CMIP применяется полная версия ASN.1.

На основании правил GDMO определено несколько международных стандартов на классы управляемых объектов. Документы Definition of Management Information (DMI, ISO/IEC 10165-2:1991) и Generic Management Information (GMI, ISO/IEC CD 10165-5:1992) являются первыми определениями M1B на основе окончательной версии GDMO. Эти MIB могут рассматриваться как ISO-эквивалент для Internet MIB II, так как они создают основу для построения более специфических MIB. Например, DMI определяет класс объектов, называемый Top, который является верхним суперклассом, - он содержит атрибуты, которые наследуются всеми другими классами управляемых объектов. Определены также классы объектов System и Network, занимающие верхние позиции в дереве наследования, так что любой агент должен понимать их атрибуты.

В 1992 году была завершена работа и над более специфическими классами объектов - объектами сетевого и транспортного уровней (ISO/IEC 10737-1 и ISO/ IEC 10733).

Сегодня многие организации работают над созданием классов объектов на основе GDMO. Это и международные организации по стандартизации - ISO, ITU-T, ANSI, ETSI, X/Open, и организации, разрабатывающие платформы и инструментальные средства для систем управления, такие как SunSoft, Hewlett-Packard, Vertel, ISR Global. Для телекоммуникационных сетей в рамках архитектуры TMN разработан стандарт M.3100, который описывает ряд специфических для телекоммуникационных сетей классов объектов.

Описания классов управляемых объектов OSI регистрируются как в частных ветвях дерева ISO - ветвях компаний Sun, Hewlett-Packard, IBM и т. п., так и в публичных ветвях, контролируемых ISO или другими международными органами стандартизации.

В отсутствие одной регистрирующей организации, такой как IETF Internet, использование классов объектов OSI представляет собой непростую задачу.

Протокол CMIP и услуги CMIS

Доступ к управляющей информации, хранящейся в управляемых объектах, обеспечивается с помощью элемента системы управления, называемого службой CMSIE (Common Management Information Service Element). Служба CMSIE построена в архитектуре распределенного приложения, где часть функций выполняет менеджер, а часть - агент. Взаимодействие между менеджером и агентом осуществляется по протоколу CMIP. Услуги, предоставляемые службой CMSIE, называются услугами CMIS (Common Management Information Services).

Протокол CMIP и услуги CMIS определены в стандартах X.710 и X.711 ITU-T.

Услуги CMIS разделяются на две группы - услуги, инициируемые менеджером (запросы), и услуги, инициируемые агентом (уведомления).

Услуги, инициируемые менеджером, включают следующие операции:

- M-CREATE инструктирует агента о необходимости создать новый экземпляр объекта определенного класса или новый атрибут внутри экземпляра объекта;
- M-DELETE инструктирует агента о необходимости удаления некоторого экземпляра объекта определенного класса или атрибута внутри экземпляра объекта;
- M-GET инструктирует агента о возвращении значения некоторого атрибута определенного экземпляра объекта;
- M-SET инструктирует агента об изменении значения некоторого атрибута определенного экземпляра объекта;
- M-ACTION инструктирует агента о необходимости выполнения определенного действия над одним или несколькими экземплярами объектов.

Агент инициирует только одну операцию:

M-EVENT_REPORT - отправка уведомления менеджеру.

Для реализации своих услуг служба CMISE должна использовать службы прикладного уровня стека OSI - ACSE, ROSE.

Отличие услуг CMIS от аналогичных услуг SNMP состоит в большей гибкости. Если запросы GET и SET протокола SNMP применимы только к одному атрибуту одного объекта, то запросы M-GET, M-SET, M-ACTION и M-DELETE могут применяться к более чем одному объекту. Для этого стандарты CMIP/CMIS вводят такие понятия, как *обзор (scoping), фильтрация (filtering)* и *синхронизация (synchronization).*

Обзор

Запрос CMISE может использовать обзор, чтобы опросить одновременно несколько объектов. Вводятся четыре уровня обзора:

- базовый объект, определенный своим отличительным именем FDN;
- объекты, расположенные на n-м уровне подчинения относительно базового (сам базовый объект находится на уровне 0) в дереве включения;
- базовый объект и все объекты, расположенные на подчиненных ему уровнях до n-го (включительно) в дереве включения;
- поддерево - базовый объект и все ему подчиненные в дереве включения.

Фильтрация

Фильтрация заключается в применении булевого выражения к запросу менеджера. Запрос применяется только к тем объектам и их атрибутам, для которых данное булево выражение верно. Булевы выражения могут включать операторы отношения =>, <=,<,> или определенные атрибуты. Возможно построение сложных фильтров на основе объединения нескольких фильтров в один составной.

Синхронизация

При выполнении запросов к нескольким объектам используется одна из двух схем синхронизации: атомарная или «по возможности». При атомарной схеме запрос выполняется только в том случае, когда все объекты, попадающие в область действия обзора или фильтра, могут успешно выполнить данный запрос. Синхронизация «по возможности» подразумевает передачу запроса всем объектам, к которым запрос относится. Операция завершается при выполнении запроса любым количеством объектов.

Протокол CMIP представляет собой набор операций, прямо соответствующих услугам CMIS. Таким образом, в протоколе CMIP определены операции M-GET, M-SET, M-CREATE и т. д. Для каждой операции определен формат блока данных, переносимых по сети от менеджера агенту, и наоборот.

Формат протокольных блоков данных CMIP описывается нотацией ASN.1 и имеет гораздо более сложную структуру, чем блоки SNMP. Например, блок данных операции M-GET имеет поля для задания имен атрибутов, значения которых запрашивает менеджер, а также поля задания параметров обзора и фильтрации, определяющих множество экземпляров объектов, на которые будет воздействовать данный запрос. Имеются также поля для задания параметров прав доступа к объекту.

Сравнение протоколов SNMP и CMIP

- Применение протокола SNMP позволяет строить как простые, так и сложные системы управления, а применение протокола CMIP определяет некоторый, достаточно высокий начальный уровень сложности системы управления, так как для его работы необходимо реализовать ряд вспомогательных служб, объектов и баз данных объектов.
- Агенты CMIP 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 CMIP всегда передаются с помощью надежного транспортного протокола и в случае потери будут переданы повторно.
- Решение части проблем SNMP может быть достигнуто за счет применения более интеллектуальных MIB (к которым относится RMON MIB), но для многих устройств и ситуаций таких MIB нет (или нет стандарта, или нет соответствующей MIB в управляемом оборудовании).

- Протокол CMIP рассчитан на интеллектуальных агентов, которые могут по одной простой команде от менеджера выполнить сложную последовательность действий.
- Протокол CMIP 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.

Выводы

- Существуют два популярных семейства стандартов систем управления: стандарты Internet, описывающие системы управления на основе протокола SNMP, и международные стандарты управления открытых систем (OSI), разработанные ISO и ITU-T, опирающиеся на протокол управления CMIP. Семейство стандартов Internet специфицирует минимум аспектов и элементов системы управления, а семейство стандартов ISO/ITU-T - максимум.
- Системы управления SNMP основаны на следующих концепциях, ориентированных на минимальную загрузку управляемых устройств:
  - агент выполняет самые простые функции и работает в основном по инициативе менеджера;
  - система управления состоит из одного менеджера, который периодически опрашивает всех агентов;
  - протокол взаимодействия между агентом и менеджером SNMP опирается на простой ненадежный транспортный протокол UDP (для разгрузки управляемого устройства) и использует два основных типа команд - get для получения данных от агента и set для передачи управляющих воздействий агенту;
  - агент может послать данные менеджеру по своей инициативе с помощью команды trap, но число ситуаций, в которых он применяет эту команду, очень невелико
- Базы управляющей информации MIB в стандартах Internet состоят из дерева атрибутов, называемых объектами и группами объектов.
- Первые MIB Internet были ориентированы на управление маршрутизаторами: MIB-I - только контроль, MIB-II - контроль и управление. Более поздняя разработка RMON MIB была направлена на создание интеллектуальных агентов, контролирующих нижний уровень, - интерфейсы Ethernet и Token Ring. Имена объектов стандартных MIB Internet зарегистрированы в дереве регистрации имен стандартов ISO.
- Стандарты ISO/ITU-T для представления управляемых устройств используют объектно-ориентированный подход. Определено несколько суперклассов обобщенных управляемых объектов, на основании которых путем наследования свойств должны создаваться более специфические классы объектов.
- Для описания управляемых объектов OSI разработаны правила GDMO, основанные на формах определенной структуры, заполняемых с помощью языка ASN.1.
- Для представления знаний об управляемых объектах, агентах и менеджерах системы управления OSI используется три древовидные базы данных: дерево наследования, которое описывает отношения наследования между классами объектов, дерево включения, которое описывает отношения соподчинения между конкретными элементами системы управления, и дерево имен, которое определяет иерархические имена объектов в системе.
- Протокол CMIP, 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.

7.3. Мониторинг и анализ локальных сетей

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. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

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.

7.3.1. Классификация средств мониторинга и анализа

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

- Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.
- Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей,

приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

- Анализаторы протоколов (Protocol analyzers). Представляют собой програмные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, - обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.
- Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.
- Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.
- Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирование кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика - средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.
- Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.
- Кабельные сканеры используются для диагностики медных кабельных систем.
- Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.
- Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

7.3.2. Анализаторы протоколов

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный

специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим *«беспорядочного» захвата - promiscuous mode.*

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т. п. В состав некоторых анализаторов может входить также экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Анализаторы протоколов имеют некоторые общие свойства.

- Возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент.
- Возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP.
- Наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации.
- Фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, так как исключает захват или просмотр ненужных в данный момент пакетов.
- Использование триггеров. Триггеры - это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата.
- Многоканальность. Некоторые анализаторы протоколов позволяют проводить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети. Возможности анализа проблем сети на физическом уровне у анализаторов протоколов минимальные, поскольку всю информацию они получают от стандартных сетевых адаптеров. Поэтому они передают и обобщают информацию физического уровня, которую сообщает им сетевой адаптер, а она во многом зависит от типа сетевого адаптера. Некоторые сетевые адаптеры сообщают более детальные данные об

ошибках кадров и интенсивности коллизий в сегменте, а некоторые вообще не передают такую информацию верхним уровням протоколов, на которых работает анализатор протоколов.

С распространением серверов Windows NT все более популярным становится анализатор Network Monitor фирмы Microsoft. Он является частью сервера управления системой SMS, а также входит в стандартную поставку Windows NT Server, начиная с версии 4.0 (версия с усеченными функциями). Network Monitor в версии SMS является многоканальным анализатором протоколов, поскольку может получать данные от нескольких агентов Network Monitor Agent, работающих в среде Windows NT Server, однако в каждый момент времени анализатор может работать только с одним агентом, так что сопоставить данные разных каналов с его помощью не удастся. Network Monitor поддерживает фильтры захвата (достаточно простые) и дисплейные фильтры, отображающие нужные кадры после захвата (более сложные). Экспертной системой Network Monitor не располагает.

7.3.3. Сетевые анализаторы

Сетевые анализаторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов. Сетевые анализаторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

Многие производители дополняют сетевые анализаторы функциями статистического анализа трафика - коэффициента использования сегмента, уровня широковещательного трафика, процента ошибочных кадров, а также функциями анализатора протоколов, которые обеспечивают захват пакетов разных протоколов в соответствии с условиями фильтров и декодирование пакетов.

7.3.4. Кабельные сканеры и тестеры

Основное назначение кабельных сканеров - измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т. д.) используется метод «отраженного импульса» (Time Domain Reflectometry, TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле. В различных кабелях она будет разной. Скорость распространения электромагнитных волн в кабеле (Nominal Velocity of

Propagation, NVP) обычно задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных о NVP для всех основных типов кабелей, что дает возможность пользователю устанавливать эти параметры самостоятельно после предварительной калибровки.

Кабельные сканеры - это портативные приборы, которые обслуживающий персонал может постоянно носить с собой.

Кабельные тестеры - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

7.3.5. Многофункциональные портативные приборы мониторинга

В последнее время начали выпускаться многофункциональные портативные приборы, которые объединяют в себе возможности кабельных сканеров, анализаторов протоколов и даже некоторые функции систем управления, сохраняя в то же время такое важное свойство, как портативность. Многофункциональные приборы мониторинга имеют специализированный физический интерфейс, позволяющий выявлять проблемы и тестировать кабели на физическом уровне, который дополняется микропроцессором с программным обеспечением для выполнения высокоуровневых функций.

Рассмотрим типичный набор функций и свойств такого прибора, который оказывается очень полезным для диагностики причин разнообразных неполадок в сети, происходящих на всех уровнях стека протоколов, от физического до прикладного.

Интерфейс пользователя

Прибор обычно предоставляет пользователю удобный и интуитивно понятный интерфейс, основанный на системе меню. Графический интерфейс пользователя реализован на многострочном жидкокристаллическом дисплее и индикаторах состояния на светодиодах, извещающих пользователя о наиболее общих проблемах наблюдаемых сетей. Имеется обширный файл подсказок оператору с уровневым доступом в соответствии с контекстом. Информация о состоянии сети представляется таким образом, что пользователи любой квалификации могут ее быстро понять.

Функции проверки аппаратуры и кабелей

Многофункциональные приборы сочетают наиболее часто используемые на практике функции кабельных сканеров с рядом новых возможностей тестирования.

Сканирование кабеля

Функция позволяет измерять длину кабеля, расстояние до самого серьезного дефекта и распределение импеданса по длине кабеля. При проверке неэкранированной витой пары могут быть выявлены следующие ошибки: расщепленная пара, обрывы, короткое замыкание и другие виды нарушения соединения.

Для сетей Ethernet на коаксиальном кабеле эти проверки могут быть осуществлены на работающей сети.

Функция определения распределения кабельных жил.

Осуществляет проверку правильности подсоединения жил, наличие промежуточных разрывов и перемычек на витых парах. На дисплей выводится перечень связанных между собой контактных групп.

Функция определения карты кабелей

Используется для составления карты основных кабелей и кабелей, ответвляющихся от центрального помещения.

Автоматическая проверка кабеля

В зависимости от конфигурации возможно определить длину, импеданс, схему подключения жил, затухание и параметр NEXT на частоте до 100 МГц. Автоматическая проверка выполняется для:

- коаксиальных кабелей;
- экранированной витой пары с импедансом 150 Ом;
- неэкранированной витой пары с сопротивлением 100 Ом.

Целостность цепи при проверке постоянным током

Эта функция используется при проверке коаксиальных кабелей для верификации правильности используемых терминаторов и их установки.

Определение номинальной скорости распространения

Функция вычисляет номинальную скорость распространения (Nominal Velocity of Propagation, NVP) по кабелю известной длины и дополнительно сохраняет полученные результаты в файле для определяемого пользователем типа кабеля (User Defined cable type) или стандартного кабеля.

Комплексная автоматическая проверка пары «сетевой адаптер-концентратор»

Этот комплексный тест позволяет последовательно подключить прибор между конечным узлом сети и концентратором. Тест дает возможность автоматически определить местонахождение источника неисправности - кабель, концентратор, сетевой адаптер или программное обеспечение станции.

Автоматическая проверка сетевых адаптеров

Проверяет правильность функционирования вновь установленных или «подозрительных» сетевых адаптеров. Для сетей Ethernet по итогам проверки сообщаются: MAC - адрес, уровень напряжения сигналов (а также присутствие и полярность импульсов Link Test для 10BASE-T). Если сигнал не обнаружен на сетевом адаптере, то тест автоматически сканирует соединительный разъем и кабель для их диагностики.

Функции сбора статистики

Эти функции позволяют в реальном масштабе времени проследить за изменением наиболее важных параметров, характеризующих «здоровье» сегментов сети. Статистика обычно собирается с разной степенью детализации по разным группам.

Сетевая статистика

В этой группе собраны наиболее важные статистические показатели - коэффициент использования сегмента (utilization), уровень коллизий, уровень ошибок и уровень широковещательного трафика. Превышение этими показателями определенных порогов в первую очередь говорят о проблемах в том сегменте сети, к которому подключен многофункциональный прибор.

Статистика ошибочных кадров

Эта функция позволяет отслеживать все типы ошибочных кадров для определенной технологии. Например, для технологии Ethernet характерны следующие типы ошибочных кадров.

- Укороченные кадры (Short frames). Это кадры, имеющие длину, меньше допустимой, то есть меньше 64 байт. Иногда этот тип кадров дифференцируют на два класса - просто короткие кадры (short), у которых имеется корректная контрольная сумма, и «коротышки» (runts), не имеющие корректной контрольной суммы. Наиболее вероятными причинами появления укороченных кадров являются неисправные сетевые адаптеры и их драйверы.
- Удлиненные кадры (Jabbers). Это кадры, имеющие длину, превышающую допустимое значение в 1518 байт с хорошей или плохой контрольной суммой. Удлиненные кадры являются следствием затянувшейся передачи, которая появляется из-за неисправностей сетевых адаптеров.
- Кадры нормальных размеров, но с плохой контрольной суммой (Bad FCS) и кадры с ошибками выравнивания по границе байта. Кадры с неверной контрольной суммой являются следствием множества причин - плохих адаптеров, помех на кабелях, плохих контактов, некорректно работающих портов повторителей, мостов, коммутаторов и маршрутизаторов. Ошибка выравнивания всегда сопровождается ошибкой по контрольной сумме, поэтому некоторые средства анализа трафика не делают между ними различий. Ошибка выравнивания может быть следствием прекращения передачи кадра при распознавании коллизии передающим адаптером.
- Кадры-призраки (ghosts) являются результатом электромагнитных наводок на кабеле. Они воспринимаются сетевыми адаптерами как кадры, не имеющие нормального признака начала кадра - 10101011. Кадры-призраки имеют длину более 72 байт, в противном случае они классифицируются как удаленные коллизии. Количество обнаруженных кадров-призраков в большой степени зависит от точки подключения сетевого анализатора. Причинами их возникновения являются петли заземления и другие проблемы с кабельной системой. Знание процентного распределения общего количества ошибочных кадров по их типам может многое подсказать администратору о возможных причинах неполадок в сети. Даже небольшой процент ошибочных кадров может привести к значительному снижению полезной пропускной способности сети, если протоколы, восстанавливающие искаженные кадры, работают с большими тайм-аутами ожидания квитанций. Считается, что в нормально работающей сети процент

ошибочных кадров не должен превышать 0,01 %, то есть не более 1 ошибочного кадра из 10 000.

Статистика по коллизиям

Эта группа характеристик дает информацию о количестве и видах коллизий, отмеченных на сегменте сети, позволяет определить наличие и местонахождение проблемы. Анализаторы протоколов обычно не могут дать дифференцированной картины распределения общего числа коллизий по их отдельным типам, в то же время знание преобладающего типа коллизий может помочь понять причину плохой работы сети.

Ниже приведены основные типы коллизий сети Ethernet.

- Локальная коллизия (Local Collision). Является результатом одновременной передачи двух или более узлов, принадлежащих к тому сегменту, в котором производятся измерения. Если многофункциональный прибор не генерирует кадры, то в сети на витой паре или волоконно-оптическом кабеле локальные коллизии не фиксируются. Слишком высокий уровень локальных коллизий является следствием проблем с кабельной системой.
- Удаленная коллизия (Remote Collision). Эти коллизии происходят на другой стороне повторителя (по отношению к тому сегменту, в котором установлен измерительный прибор). В сетях, построенных на многопортовых повторителях (10Base-T, 10Base-FL/FB, 100Base-TX/FX/T4, Gigabit Ethernet), все измеряемые коллизии являются удаленными (кроме тех случаев, когда анализатор сам генерирует кадры и может быть виновником коллизии). Не все анализаторы протоколов и средства мониторинга одинаковым образом фиксируют удаленные коллизии. Это происходит из-за того, что некоторые измерительные средства и системы не фиксируют коллизии, происходящие при передаче преамбулы.
- Поздняя коллизия (Late Collision). Это коллизия, которая происходит после передачи первых 64 байт кадра (по протоколу Ethernet коллизия должна обнаруживаться при передаче первых 64 байт кадра). Результатом поздней коллизии будет кадр, который имеет длину более 64 байт и содержит неверное значение контрольной суммы. Чаще всего это указывает на то, что сетевой адаптер, являющийся источником конфликта, оказывается не в состоянии правильно прослушивать линию и поэтому не может вовремя остановить передачу. Другой причиной поздней коллизии является слишком большая длина кабельной системы или слишком большое количество промежуточных повторителей, приводящее к превышению максимального значения времени двойного оборота сигнала. Средняя интенсивность коллизий в нормально работающей сети должна быть меньше 5 %. Большие всплески (более 20 %) могут быть индикатором кабельных проблем.

Распределение используемых сетевых протоколов

Эта статистическая группа относится к протоколам сетевого уровня. На дисплее отображается список основных протоколов в убывающем порядке относительно процентного соотношения кадров, содержащих пакеты данного протокола к общему числу кадров в сети.

Основные отправители (Top Sendes)

Функция позволяет отслеживать наиболее активные передающие узлы локальной сети. Прибор можно настроить на фильтрацию по единственному адресу и выявить список основных отправителей кадров для данной станции. Данные отражаются на дисплее в виде диаграммы вместе с перечнем основных отправителей кадров.

Основные получатели (Top Receivers)

Функция позволяет следить за наиболее активными узлами-получателями сети. Информация отображается в виде, аналогичном приведенному выше.

Основные генераторы широковещательного трафика (Top Broadcasters)

Функция выявляет станции сети, которые больше остальных генерируют кадры с широковещательными и групповыми адресами.

Генерирование трафика (Traffic Generation)

Прибор может генерировать трафик для проверки работы сети при повышенной нагрузке. Трафик может генерироваться параллельно с активизированными функциями *Сетевая статистика*, *Статистика ошибочных кадров* и *Статистика по коллизиям*.

Пользователь может задать параметры генерируемого трафика, такие как интенсивность и размер кадров. Для тестирования мостов и маршрутизаторов прибор может автоматически создавать заголовки IP- и IPX-пакетов, и все что требуется от оператора - это внести адреса источника и назначения.

В ходе испытаний пользователь может увеличить на ходу размер и частоту следования кадров с помощью клавиш управления курсором. Это особенно ценно при поиске источника проблем производительности сети и условий возникновения отказов.

Функции анализа протоколов

Обычно портативные многофункциональные приборы поддерживают декодирование и анализ только основных протоколов локальных сетей, таких как протоколы стеков TCP/IP, Novell NetWare, NetBIOS и Banyan VINES.

В некоторых многофункциональных приборах отсутствует возможность декодирования захваченных пакетов, как в анализаторах протоколов, а вместо этого собирается статистика о наиболее важных пакетах, свидетельствующих о наличии проблем в сетях. Например, при анализе протоколов стека TCP/IP собирается статистика по пакетам протокола ICMP, с помощью которого маршрутизаторы сообщают конечным узлам о возникновении разного рода ошибок. Для ручной проверки достижимости узлов сети в приборы включается поддержка утилиты IP Ping, а также аналогичных по назначению утилит NetWare Ping и NetBIOS Ping.

7.3.6. Мониторинг локальных сетей на основе коммутаторов

Наблюдение за трафиком

Так как перегрузки процессоров портов и других обрабатывающих элементов коммутатора могут приводить к потерям кадров, то функция наблюдения за распределением трафика в сети, построенной на основе коммутаторов, очень важна.

Однако если сам коммутатор не снабжен встроенным агентом SNMP для каждого своего порта, то задача слежения за трафиком, традиционно решаемая в сетях с разделяемыми средами с помощью установки в сеть внешнего анализатора протоколов, очень усложняется.

Обычно в традиционных сетях анализатор протоколов или многофункциональный прибор подключался к свободному порту концентратора, что позволяло ему наблюдать за всем трафиком, передаваемым между любыми узлами сети.

Если же анализатор протокола подключить к свободному порту коммутатора, то он не зафиксирует почти ничего, так как кадры ему передавать никто не будет, а чужие кадры в его порт также направляться не будут. Единственный вид трафика, который будет фиксировать анализатор, - это трафик широковещательных пакетов, которые будут передаваться всем узлам сети, а также трафик кадров с неизвестными коммутатору адресами назначения. В случае когда сеть разделена на виртуальные сети, анализатор протоколов будет фиксировать только широковещательный трафик своей виртуальной сети.

Чтобы анализаторами протоколов можно было по-прежнему пользоваться и в коммутируемых сетях, производители коммутаторов снабжают свои устройства функцией зеркального отображения трафика любого порта на специальный порт. К специальному порту подключается анализатор протоколов, а затем на коммутатор подается команда через его модуль SNMP-управления для отображения трафика какого-либо порта на специальный порт.

Наличие функции зеркализации портов частично снимает проблему, но оставляет некоторые вопросы. Например, как просматривать одновременно трафик двух портов или трафик порта, работающего в полнодуплексном режиме.

Более надежным способом слежения за трафиком, проходящим через порты коммутатора, является замена анализатора протокола на агенты RMON MIB для каждого порта коммутатора.

Агент RMON выполняет все функции хорошего анализатора протокола для протоколов Ethernet и Token Ring, собирая детальную информацию об интенсивности трафика, различных типах плохих кадров, о потерянных кадрах, причем самостоятельно строя временные ряды для каждого фиксируемого параметра. Кроме того, агент RMON может самостоятельно строить матрицы перекрестного трафика между узлами сети, которые очень нужны для анализа эффективности применения коммутатора.

Так как агент RMON, реализующий все 9 групп объектов Ethernet, стоит весьма дорого, то производители для снижения стоимости коммутатора часто реализуют только первые несколько групп объектов RMON MIB. Другим приемом снижения стоимости коммутатора является использование одного агента RMON для нескольких портов. Такой агент по очереди подключается к нужному порту, позволяя снять с него требуемые статистические данные.

Управление виртуальными сетями

Виртуальные локальные сети VLAN порождают проблемы для традиционных систем управления на платформе SNMP как при их создании, так и при наблюдении за их работой.

Как правило, для создания виртуальных сетей требуется специальное программное обеспечение компании-производителя, которое работает на платформе системы управления, например HP Open View. Сами платформы систем управления этот процесс поддержать не могут в основном из-за долгого отсутствия стандарта на виртуальные сети. Можно надеяться, что появление стандарта 802.1Q изменит ситуацию в этой области.

Наблюдение за работой виртуальных сетей также создает проблемы для традиционных систем управления. При создании карты сети, включающей виртуальные сети, необходимо отображать как физическую структуру сети, так и ее логическую структуру, соответствующую связям отдельных узлов виртуальной сети. При этом по желанию администратора система управления должна уметь отображать соответствие логических и физических связей в сети, то есть на одном физическом канале должны отображаться все или отдельные пути виртуальных сетей.

К сожалению, многие системы управления либо вообще не отображают виртуальные сети, либо делают это очень неудобным для пользователя способом, что вынуждает обращаться к менеджерам компаний-производителей для решения этой задачи.

Выводы

- Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для выполнения этих этапов разработан ряд средств, применяемых автономно в тех случаях, когда применение интегрированной системы управления экономически неоправданно.
- В состав автономных средств мониторинга и анализа сети входят встроенные средства диагностики, анализаторы протоколов, экспертные системы, сетевые анализаторы, кабельные сканеры и тестеры, многофункциональные приборы.
- Анализаторы протоколов чаще всего представляют собой специальное программное обеспечение для персональных компьютеров и ноутбуков, которое переводит сетевой адаптер компьютера в режим «беспорядочного» захвата всех кадров. Анализатор протоколов выполняет декодирование захваченных кадров для вложенных пакетов протоколов всех уровней, включая прикладной.
- Сетевые анализаторы представляют собой прецизионные приборы для сертификации кабельных систем по международным стандартам. Кроме того, эти устройства могут выполнять некоторые функции анализаторов протоколов.
- Кабельные сканеры являются портативными приборами, которые могут измерить электрические параметры кабелей, а также обнаружить место повреждения кабеля. Кабельные тестеры представляют собой наиболее простые портативные приборы, способные обнаружить неисправность кабеля.
- Многофункциональные портативные приборы сочетают в себе функции кабельных сканеров и анализаторов протоколов. Они снабжены многострочными дисплеями, контекстно-чувствительной системой помощи, встроенным микропроцессором с программным обеспечением и позволяют выполнять комплексную проверку сегментов сети на всех уровнях, от физического (что не умеют делать анализаторы

протоколов), до прикладного. Отличаются от анализаторов протоколов поддержкой только базового набора протоколов локальных сетей.

Вопросы и упражнения

1. К какой из пяти стандартных функциональных групп системы управления относится функция концентратора Ethernet по обнулению поля данных в кадрах, поступающих на порты, к которым не подключен узел назначения?
2. К какому уровню модели TMN относится большинство выпускаемых сегодня систем управления?
3. Как объяснить, что наличие в одном сегменте сети NetWare сравнительно небольшого числа (3 %) ошибочных кадров Ethernet резко снижает пропускную способность сети. Рассчитайте коэффициент снижения полезной пропускной способности сети, если при передаче файлов используется метод квитирования с простоями, причем тайм-аут ожидания квитанции составляет 0,5 с, сервер тратит на подготовку очередного кадра данных 20 мкс после получения квитанции от клиентской станции, а клиентская станция отсылает квитанции через 30 мкс после получения очередного кадра данных от сервера. Служебная информация протоколов верхних уровней занимает в кадре Ethernet 58 байт, причем данные передаются в кадрах Ethernet с полем данных максимального размера в 1500 байт, а квитанции помещаются в заголовке протокола прикладного уровня.
4. Какая функция в системах управления системами соответствует функции построения карты сети в системах управления сетями?
5. Какое свойство агента, поддерживающего RMON MIB, послужило поводом назвать данную MIB базой управляющих данных для *удаленного* мониторинга?
6. Какие действия предпринимает агент SNMP, если его сообщение о сбое управляемого устройства, посланное с помощью команды trap, потеряется?
7. Можно ли построить систему управления, работающую без платформы управления?
8. Относится ли средство, называемое community string, к средствам аутентификации?
9. Какую базу данных использует протокол CMIP для воздействия сразу на группу агентов?
10. У вас есть подозрение, что часть коллизий в вашей сети вызвана электромагнитными наводками. Сможет ли анализатор протоколов прояснить ситуацию?