Лекция 1. Задачи и цели сетевого администрирования, понятие о сетевых протоколах и службах

Данная лекция знакомит с базовым набором задач, которые должен выполнять сетевой администратор в своей профессиональной деятельности; здесь также описаны две общепринятые модели межсетевого взаимодействия.

1.1. Задачи и цели сетевого администрирования

Современные корпоративные информационные системы по своей природе всегда являются распределенными системами. Рабочие станции пользователей, серверы приложений, серверы баз данных и прочие сетевые узлы размещены на большой территории. В крупной компании офисы и площадки соединены различными видами коммуникаций, использующих различные технологии и сетевые устройства. Главная задача сетевого администратора — обеспечить надежную, бесперебойную, производительную и безопасную работу всей этой сложной системы.

Будем рассматривать сеть как совокупность программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Все сети можно условно разделить на 3 категории:

- локальные сети (LAN, Local Area Network);
- глобальные сети (WAN, Wide Area Network);
- городские сети (MAN, Metropolitan Area Network).

Глобальные сети позволяют организовать взаимодействие между абонентами на больших расстояниях. Эти сети работают на относительно низких скоростях и могут вносить значительные задержки в передачу информации. Протяженность глобальных сетей может составлять тысячи километров. Поэтому они так или иначе интегрированы с сетями масштаба страны.

Городские сети позволяют взаимодействовать на территориальных образованиях меньших размеров и работают на скоростях от средних до высоких. Они меньше замедляют передачу данных, чем глобальные, но не могут обеспечить высокоскоростное взаимодействие на больших расстояниях. Протяженность городских сетей находится в переделах от нескольких километров до десятков и сотен километров.

Локальные сети обеспечивают наивысшую скорость обмена информацией между компьютерами. Типичная локальная сеть занимает одно здание. Протяженность локальных сетей составляет около одного кило-

метра. Их основное назначение состоит в объединении пользователей (как правило, одной компании или организации) для совместной работы.

Механизмы передачи данных в локальных и глобальных сетях существенно отличаются. Глобальные сети ориентированы на соединение — до начала передачи данных между абонентами устанавливается соединение (сеанс). В локальных сетях используются методы, не требующие предварительной установки соединения, — пакет с данными посылается без подтверждения готовности получателя к обмену.

Кроме разницы в скорости передачи данных, между этими категориями сетей существуют и другие отличия. В локальных сетях каждый компьютер имеет сетевой адаптер, который соединяет его со средой передачи. Городские сети содержат активные коммутирующие устройства, а глобальные сети обычно состоят из групп мощных маршрутизаторов пакетов, объединенных каналами связи. Кроме того, сети могут быть частными или сетями общего пользования.

Сетевая инфраструктура строится из различных компонент, которые условно можно разнести по следующим уровням:

- кабельная система и средства коммуникаций;
- активное сетевое оборудование;
- сетевые протоколы;
- сетевые службы;
- сетевые приложения.

Каждый из этих уровней может состоять из различных подуровней и компонент. Например, кабельные системы могут быть построены на основе коаксиального кабеля («толстого» и тонкого»), витой пары (экранированной и неэкранированной), оптоволокна. Активное сетевое оборудование включает в себя такие виды устройств, как повторители (репитеры), мосты, концентраторы, коммутаторы, маршрутизаторы. В корпоративной сети может быть использован богатый набор сетевых протоколов: TCP/IP, SPX/IPX, NetBEUI, AppleTalk и др.

Основу работы сети составляют так называемые сетевые службы (или сервисы). Базовый набор сетевых служб любой корпоративной сети состоит из следующих служб:

- службы сетевой инфраструктуры DNS, DHCP, WINS;
- службы файлов и печати;
- службы каталогов (например, Novell NDS, MS Active Directory);
- службы обмена сообщениями;
- службы доступа к базам данных.

Самый верхний уровень функционирования сети — сетевые приложения.

Сеть позволяет легко взаимодействовать друг с другом самым различным видам компьютерных систем благодаря стандартизованным ме-

тодам передачи данных, которые позволяют скрыть от пользователя все многообразие сетей и машин.

Все устройства, работающие в одной сети, должны общаться на одном языке – передавать данные в соответствии с общеизвестным алгоритмом в формате, который будет понят другими устройствами. *Стандарты – ключевой фактор при объединении сетей*.

Для более строгого описания работы сети разработаны специальные модели. В настоящее время общепринятыми моделями являются модель OSI (Open System Interconnection) и модель TCP/IP (или модель DARPA). Обе модели будут рассмотрены в данной лекции ниже.

Прежде чем определить задачи сетевого администрирования в сложной распределенной корпоративной сети, сформулируем определение термина «корпоративная сеть» (КС). Слово «корпорация» означает объединение предприятий, работающих под централизованным управлением и решающих общие задачи. Корпорация является сложной, многопрофильной структурой и вследствие этого имеет распределенную иерархическую систему управления. Кроме того, предприятия, отделения и административные офисы, входящие в корпорацию, как правило, расположены на достаточном удалении друг от друга. Для централизованного управления таким объединением предприятий применяется корпоративная сеть.

Основная задача КС заключается в обеспечении передачи информации между различными приложениями, используемыми в организации.

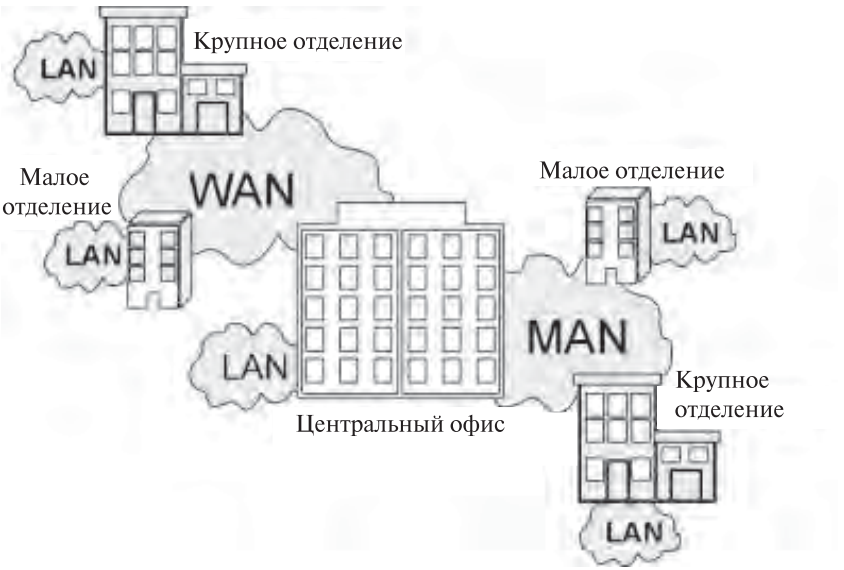

Рис. 1.1. Обобщенная схема КС

Под приложением понимается программное обеспечение, которое непосредственно нужно пользователю, например, бухгалтерская программа, программа обработки текстов, электронная почта и т. д. Корпоративная сеть позволяет взаимодействовать приложениям, зачастую расположенным в географически различных областях, и обеспечивает доступ к ним удаленных пользователей. На рис. 1.1 показана обобщенная функциональная схема корпоративной сети.

Обязательным компонентом корпоративной сети являются локальные сети, связанные между собой.

В общем случае КС состоит из различных отделений, объединенных сетями связи. Они могут быть глобальными (WAN) или городскими (MAN).

Итак, сформулируем задачи сетевого администрирования в сложной распределенной КС.

1. Планирование сети.

Несмотря на то, что планированием и монтажом больших сетей обычно занимаются специализированные компании-интеграторы, сетевому администратору часто приходится планировать определенные изменения в структуре сети — добавление новых рабочих мест, добавление или удаление сетевых протоколов, добавление или удаление сетевых служб, установка серверов, разбиение сети на сегменты и т. д. Данные работы должны быть тщательно спланированы, чтобы новые устройства, узлы или протоколы включались в сеть или исключались из нее без нарушения целостности сети, без снижения производительности, без нарушения инфраструктуры сетевых протоколов, служб и приложений.

2. Установка и настройка сетевых узлов (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникаций).

Данные работы могут включать в себя замену сетевого адаптера в ПК с соответствующими настройками компьютера, перенос сетевого узла (ПК, сервера, активного оборудования) в другую подсеть с соответствующими изменениями сетевых параметров узла, добавление или замена сетевого принтера с соответствующей настройкой рабочих мест.

3. Установка и настройка сетевых протоколов.

Данная задача включает в себя выполнение следующих работ: планирование и настройка базовых сетевых протоколов корпоративной сети, тестирование работы сетевых протоколов, определение оптимальных конфигураций протоколов.

4. Установка и настройка сетевых служб.

Корпоративная сеть может содержать большой набор сетевых служб. Кратко перечислим основные задачи администрирования сетевых служб:

a. установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей);
b. установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;
c. администрирование служб каталогов (Novell NDS, Microsoft Active Directory), составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;
d. администрирование служб обмена сообщениями (системы электронной почты);
e. администрирование служб доступа к базам данных.

5. Поиск неисправностей.

Сетевой администратор должен уметь обнаруживать широкий спектр проблем — от неисправного сетевого адаптера на рабочей станции пользователя до сбоев отдельных портов коммутаторов и маршрутизаторов, а также неправильные настройки сетевых протоколов и служб.

6. Поиск узких мест сети и повышения эффективности работы сети.

В задачу сетевого администрирования входит анализ работы сети и определение наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест, либо изменения конфигурации отдельных сегментов сети.

7. Мониторинг сетевых узлов.

Мониторинг сетевых узлов включает в себя наблюдение за функционированием сетевых узлов и за корректностью выполнения возложенных на данные узлы функций.

8. Мониторинг сетевого трафика.

Мониторинг сетевого трафика позволяет обнаружить и ликвидировать различные виды проблем: высокую загруженность отдельных сетевых сегментов, чрезмерную загруженность отдельных сетевых устройств, сбои в работе сетевых адаптеров или портов сетевых устройств, нежелательную активность или атаки злоумышленников (распространение вирусов, атаки хакеров и др.).

9. Обеспечение защиты данных.

Защита данных включает в себя большой набор различных задач: резервное копирование и восстановление данных, разработка и осуществление политик безопасности учетных записей пользователей и сетевых служб (требования к сложности паролей, частота смены паролей), построение защищенных коммуникаций (применение протокола IPSec, построение виртуальных частных сетей, защита беспроводных сетей), планирование, внедрение и обслуживание инфраструктуры открытых ключей (PKI).

1.2. Модели межсетевого взаимодействия (модель OSI, модель TCP/IP)

Модели межсетевого взаимодействия предназначены для формального и в то же время наглядного описания взаимодействия сетевых узлов между собой. В настоящее время наибольшее распространение получили и являются стандартами для описания межсетевого взаимодействия две сетевые модели: OSI и TCP/IP. Обе модели разбивают процесс взаимодействия сетевых узлов на несколько уровней, каждый конкретный уровень одного узла обменивается информацией с соответствующим уровнем другого узла.

Каждую из этих моделей можно представлять как объединение двух моделей:

- горизонтальная модель (на базе протоколов, обеспечивающая обмен данными одного типа между программами и процессами, которые работают на одном и том же уровне на различных сетевых узлах);
- вертикальная модель (на основе услуг, предоставляемых соседними уровнями друг другу на одном сетевом узле).

В горизонтальной модели двум программам, работающим на различных сетевых узлах, требуется общий протокол для обмена данными. В вертикальной — соседние уровни обмениваются данными, выполняя необходимые преобразования с использованием соответствующих программных интерфейсов.

Модель OSI

В 1983 году с целью упорядочения описания принципов взаимодействия устройств в сетях Международная организация по стандартизации (International Organization of Standardization, ISO) предложила семиуровневую эталонную коммуникационную модель «Взаимодействие Открытых Систем», модель OSI (Open System Interconnection).

Эталонная модель OSI сводит передачу информации в сети к семи относительно простым подзадачам.

Модель OSI стала основой для разработки стандартов на взаимодействие систем. Она определяет только схему выполнения необходимых задач, но не дает конкретного описания их выполнения. Это описывается конкретными протоколами или правилами, разработанными для определенной технологии с учетом модели OSI. Уровни OSI могут реализовываться как аппаратно, так и программно.

Основная идея модели OSI заключается в том, что одни и те же уровни на разных системах, не имея возможности связываться непосредствен-

но, должны работать абсолютно одинаково. Одинаковым должен быть и сервис между соответствующими уровнями различных систем. Нарушение этого принципа может привести к тому, что информация, посланная от одной системы к другой, после всех преобразований не будет идентична исходной.

Существует семь основных уровней модели OSI (таблица 1.1). Они начинаются с физического уровня и заканчиваются прикладным. Каждый уровень предоставляет услуги для более высокого уровня. Седьмой уровень обслуживает непосредственно пользователей.

Таблица 1.1

7. Прикладной (Application)
6. Представления (Presentation)
5. Сеансовый (Session)
4. Транспортный (Transport)
3. Сетевой (Network)
2. Канальный (Data Link)
1. Физический (Physical)

Модель OSI описывает путь информации через сетевую среду от одной прикладной программы на одном компьютере до другой программы на другом компьютере. При этом пересылаемая информация проходит вниз через все уровни системы.

Уровни на разных системах не могут общаться между собой напрямую. Это умеет только физический уровень.

По мере прохождения информации вниз внутри системы она преобразуется в вид, удобный для передачи по физическим каналам связи.

Для указания адресата к этой преобразованной информации добавляется заголовок с адресом. После получения адресатом эта информация проходит через все уровни наверх. По мере прохождения она преобразуется в первоначальный вид.

Каждый уровень системы должен полагаться на услуги, предоставляемые ему смежными уровнями.

1. Физический уровень. На данном уровне выполняется передача битов по физическим каналам (коаксиальный кабель, витая пара, оптоволокно).
2. Канальный уровень. Данный уровень определяет методы доступа к среде передачи данных и обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией по физическому адресу сетевого устройства. Адреса, используемые на канальном уровне в локальных сетях, часто называют MAC-адреса-

ми (MAC — Media Access Control, управление доступом к среде передачи данных).

3. Сетевой уровень. Обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом не гарантируется надежная доставка данных от узла-отправителя к узлу-получателю. На этом уровне выполняются такие функции, как маршрутизация логических адресов сетевых узлов, создание и ведение таблиц маршрутизации, фрагментация и сборка данных.
4. Транспортный уровень. Обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для выполнения этой задачи на транспортном уровне имеются механизмы установления соединения между сетевыми узлами, нумерации, буферизации и упорядочивания пакетов, передаваемых между узлами сети.
5. Сеансовый уровень. Реализует средства управления сессией, диалогом, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями, контроля над ошибками, обработки транзакций, поддержки вызова удаленных процедур RPC.
6. Уровень представления. На этом уровне могут выполняться различные виды преобразования данных, такие как компрессия и декомпрессия, шифровка и дешифровка данных.
7. Прикладной уровень. Набор сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примеры таких сервисов — обмен сообщениями электронной почты, передача файлов между узлами сети, приложения управления сетевыми узлами.

Функционирование первых трех уровней — физического, канального и сетевого — обеспечивается в основном активным сетевым оборудованием и, как правило, реализуется следующими компонентами: сетевыми адаптерами, репитерами, мостами, концентраторами, коммутаторами, маршрутизаторами.

Модель TCP/IP

Модель TCP/IP называют также моделью DARPA (сокращение от Defense Advanced Research Projects Agency, организация, в которой в свое время разрабатывались сетевые проекты, в том числе протокол TCP/IP, и которая стояла у истоков сети Интернет) или моделью министерства обороны США (модель DoD, Department of Defense; проект DARPA работал по заказу этого ведомства).

Модель TCP/IP создавалась для описания стека протоколов TCP/IP (Transmission Control Protocol/Internet Protocol). Она появилась значительно раньше, чем модель OSI.

Формальные правила, определяющие последовательность и формат сообщений на одном уровне, называются протоколами. Иерархически организованная совокупность протоколов называется стеком коммуникационных протоколов.

Модель состоит из четырех уровней, представленных в таблице 1.2.

Таблица 1.2

1. Прикладной уровень (Application)	WWW, FTP, TFTP, SNMP, Telnet, SMTP DNS, DHCP, WINS
2. Транспортный уровень (Transport)	TCP, UDP
3. Уровень межсетевого взаимодействия (Internet)	ARP, IP, ICMP, RIP, OSPF
4. Уровень сетевого интерфейса (Network Interface)	Не регламентируется спецификациями стека TCP/IP (Ethernet, Token Ring, FDDI, ATM, X.25, Frame Relay, SLIP, PPP)

Приближенное соответствие между моделями OSI и TCP/IP представлено в таблице 1.3.

Таблица 1.3

7. Прикладной (Application)	1. Прикладной уровень (Application)
6. Представления (Presentation)	
5. Сеансовый (Session)	
4. Транспортный (Transport)	2. Транспортный уровень (Transport)
3. Сетевой (Network)	3. Уровень межсетевого взаимодействия (Internet)
2. Канальный (Data Link)	4. Уровень сетевого интерфейса (Network Interface)
1. Физический (Physical)	

Преимущества стека протоколов TCP/IP

- Основное достоинство стека протоколов TCP/IP заключается в том, что он обеспечивает надежную связь между сетевым оборудованием от различных производителей.
- Независимость от сетевой технологии: стек только определяет элемент передачи, дейтаграмму, и описывает способ ее движения по сети.
- Всеобщая связанность: стек позволяет любой паре компьютеров, которые его поддерживают, взаимодействовать друг с другом.

Каждому компьютеру назначается логический адрес, а каждая передаваемая дейтаграмма содержит логические адреса отправителя и получателя. Промежуточные маршрутизаторы используют адрес получателя для принятия решения о маршрутизации.

- Подтверждения. Протоколы стека обеспечивают подтверждения правильности прохождения информации при обмене между отправителем и получателем.
- Стандартные прикладные протоколы. Протокола стека TCP/IP включают в свой состав средства поддержки основных приложений, таких как электронная почта, передача файлов, удаленный доступ и т. д.

Кратко опишем уровни модели TCP/IP.

1. Уровень сетевого интерфейса не регламентирован спецификациями стека TCP/IP, и фактически к стеку TCP/IP относят уровни с 1 по 3 модели TCP/IP. Данный уровень соответствует физическому и канальному уровням модели OSI.

2. Уровень межсетевого взаимодействия. На данном уровне функционирует целое семейство протоколов. Основная задача данного уровня — доставка пакетов от узла-отправителя к узлу-получателю.

a. Эту задачу выполняет протокол IP (Internet Protocol, протокол межсетевого взаимодействия). Протокол IP — базовый протокол стека TCP/IP и основной протокол сетевого уровня. Отвечает за передачу информации по сети. В его основу заложен дейтаграммный метод, который не гарантирует доставку пакета.

b. Протокол ARP (Address Resolution Protocol, протокол разрешения физических адресов) служит связующим звеном между уровнем межсетевого взаимодействия и уровнем сетевого интерфейса. Он преобразует IP-адреса сетевых узлов в физические MAC-адреса соответствующих сетевых адаптеров. Протокол ARP предполагает, что каждое устройство знает как свой IP-адрес, так и свой физический адрес. ARP динамически связывает их и заносит в специальную таблицу, где хранятся пары «IP-адрес – физический адрес» (обычно каждая запись в ARP-таблице имеет время жизни 10 мин.).

c. Протокол ICMP (Internet Control Message Protocol, протокол межсетевых управляющих сообщений) служит для обмена информацией об ошибках. С помощью специальных пакетов ICMP сообщает сетевым узлам информацию о невозможности доставки пакета, о превышении времени жизни пакета и др.

d. Протоколы RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First) служат для построения таблиц маршрутиза-

ции и вычисления маршрутов при отправке пакетов между различными IP-сетями.

3. Транспортный уровень.
   a. Протокол TCP (Transmission Control Protocol, протокол управления передачей) обеспечивает, базируясь на услугах протокола IP, надежную передачу сообщений между сетевыми узлами с помощью образования соединений (сеансов) между данными узлами. Такие протоколы прикладного уровня, как HTTP и FTP, передают протоколу TCP свои данные для транспортировки. Поэтому скоростные характеристики TCP оказывают непосредственное влияние на производительность приложений. Кроме того, протокол TCP используется для обработки запросов на вход в сеть, разделения ресурсов и т. д. На протокол TCP, в частности, возложена задача управления потоками и перегрузками. Он отвечает за согласование скорости передачи данных с техническими возможностями рабочей станции-получателя и промежуточных устройств в сети.
   b. Протокол UDP (User Datagram Protocol, протокол дейтаграмм пользователя) обеспечивает передачу прикладных пакетов дейтаграммным способом (т. е. не гарантирующим доставку пакетов). Работа этого протокола аналогична IP, но основной его задачей является связь сетевого протокола и различных приложений.

4. Прикладной уровень. Приложения, перечисленные в таблице 1.2, специально разрабатывались для функционирования в сетях TCP/IP.
   a. Протоколы для формирования сетевой инфраструктуры (DNS, DHCP, WINS) будут рассмотрены в следующих лекциях данного курса.
   b. Приложения WWW (World Wide Web, Всемирная паутина) — основа для работы сегодняшней сети Интернет. Протокол FTP (File Transfer Protocol, протокол передачи файлов) реализует удаленную передачу файлов между узлами сети.
   c. Протокол TFTP (Trivial File Transfer Protocol, простейший протокол пересылки файлов) — более простой способ передачи файлов, в отличие от FTP не требующий аутентификации пользователя на удаленном узле и использующий протокол UDP для передачи информации.
   d. Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) применяется для организации управления сетевыми узлами.

Более подробную и глубокую информацию по моделям межсетевого взаимодействия можно прочитать в книгах [1, 2].

Резюме

Корпоративная сеть — сложная система, которая состоит из программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Основу работы сети составляют сетевые службы (или сервисы).

Базовый набор сетевых служб корпоративной сети:
- службы сетевой инфраструктуры DNS, DHCP, WINS;
- службы файлов и печати;
- службы каталогов;
- службы обмена сообщениями;
- службы доступа к базам данных.

Администрирование сетей на платформе MS Windows Server — это планирование, установка, настройка, обслуживание корпоративной сети с использованием серверов Windows, обеспечение ее надежной, бесперебойной, высокопроизводительной и безопасной работы.

Задачи сетевого администрирования:
1. Планирование сети.
2. Установка и настройка сетевых узлов.
3. Установка и настройка сетевых протоколов.
4. Установка и настройка сетевых служб.
5. Поиск неисправностей.
6. Поиск узких мест сети и повышение эффективности работы сети.
7. Мониторинг сетевых узлов.
8. Мониторинг сетевого трафика.
9. Защита информации в сети.

Для формального описания взаимодействия сетевых узлов используются модели межсетевого взаимодействия. В настоящее время стандартными моделями являются две сетевые модели: семиуровневая модель OSI, разработанная организацией ISO (Международная Организация по Стандартам), и четырехуровневая модель TCP/IP, созданная в рамках проекта DARPA.