**Практическая работа №4 Решение проблем с TCP/IP Цель работы:** изучение способов решения проблем с TCP/IP

# ТЕОЕРЕТИЧЕСКАЯ ЧАСТЬ

TCP/IP - это аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet). В терминологии вычислительных сетей протокол - это заранее согласованный стандарт, который позволяет двум компьюте- рам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому вы часто слышите, как его называют набором, или комплектом протоколов, среди которых TCP и IP - два основных.

Программное обеспечение для TCP/IP, на вашем компьютере, представляет собой специфичную для данной платформы реализацию TCP, IP и других членов семейства TCP/IP. Обычно в нем также имеются такие высокоуровневые прикладные программы, как FTP (File Transfer Protocol, Протокол передачи файлов), которые дают возможность через командную строку управлять обменом файлами по Сети.

TCP/IP - зародился в результате исследований, профинансированных Управлением перспективных научно-исследовательских разработок (Advanced Research Project Agency, ARPA) правительства США в 1970-х годах. Этот протокол был разработан с тем, чтобы вычислительные сети исследовательских центров во всем мире могли быть объединены в форме виртуальной "сети сетей" (internetwork). Первоначальная Internet была создана в результате преобразования существующего конгломерата вычислительных сетей, носив- ших название ARPAnet, с помощью TCP/IP.

Причина, по которой TCP/IP столь важен сегодня, заключается в том, что он позво- ляет самостоятельным сетям подключаться к Internet или объединяться для создания част- ных интрасетей. Вычислительные сети, составляющие интрасеть, физически подключают- ся через устройства, называемые маршрутизаторами или IP-маршрутизаторами. Маршру- тизатор - это компьютер, который передает пакеты данных из одной сети в другую. В ин- трасети, работающей на основе TCP/IP, информация передается в виде дискретных бло- ков, называемых IP-пакетами (IP packets) или IP-дейтаграммами (IP datagrams). Благодаря программному обеспечению TCP/IP все компьютеры, подключенные к вычислительной сети, становятся "близкими родственниками". По существу оно скрывает маршрутизаторы

и базовую архитектуру сетей и делает так, что все это выглядит как одна большая сеть. Точно так же, как подключения к сети Ethernet распознаются по 48-разрядным идентифи- каторам Ethernet, подключения к интрасети идентифицируются 32-разрядными IP- адресами, которые мы выражаем в форме десятичных чисел, разделенных точками (например, 128.10.2.3). Взяв IP-адрес удаленного компьютера, компьютер в интрасети или в Internet может отправить данные на него, как будто они составляют часть одной и той же физической сети.

TCP/IP дает решение проблемы данными между двумя компьютерами, подключен- ными к одной и той же интрасети, но принадлежащими различным физическим сетям. Решение состоит из нескольких частей, причем каждый член семейства протоколов TCP/IP вносит свою лепту в общее дело. IP - самый фундаментальный протокол из ком- плекта TCP/IP - передает IP-дейтаграммы по интрасети и выполняет важную функцию, называемую маршрутизацией, по сути дела это выбор маршрута, по которому дейтаграм- ма будет следовать из пункта А в пункт B, и использование маршрутизаторов для "прыж- ков" между сетями.

TCP - это протокол более высокого уровня, который позволяет прикладным про- граммам, запущенным на различных главных компьютерах сети, обмениваться потоками данных. TCP делит потоки данных на цепочки, которые называются TCP-сегментами, и передает их с помощью IP. В большинстве случаев каждый TCP-сегмент пересылается в одной IP-дейтаграмме. Однако при необходимости TCP будет расщеплять сегменты на несколько IP-дейтаграмм, вмещающихся в физические кадры данных, которые использу- ют для передачи информации между компьютерами в сети. Поскольку IP не гарантирует, что дейтаграммы будут получены в той же самой последовательности, в которой они бы- ли посланы, TCP осуществляет повторную "сборку" TCP-сегментов на другом конце маршрута, чтобы образовать непрерывный поток данных. FTP и telnet - это два примера популярных прикладных программ TCP/IP, которые опираются на использование TCP.

Другой важный член комплекта TCP/IP - User Datagram Protocol (UDP, протокол пользовательских дейтаграмм), который похож на TCP, но более примитивен. TCP - "надежный" протокол, потому что он обеспечивает проверку на наличие ошибок и обмен подтверждающими сообщениями чтобы данные достигали своего места назначения заве- домо без искажений. UDP - "ненадежный" протокол, ибо не гарантирует, что дейтаграммы будут приходить в том порядке, в котором были посланы, и даже того, что они придут во- обще. Если надежность - желательное условие, для его реализации потребуется про- граммное обеспечение. Но UDP по-прежнему занимает свое место в мире TCP/IP, и ис- пльзуется во многих программах. Прикладная программа SNMP (Simple Network Management Protocol, простой протокол управления сетями), реализуемый во многих во- площениях TCP/IP, - это один из примеров программ UDP.

Другие TCP/IP протоколы играют менее заметные, но в равной степени важные ро- ли в работе сетей TCP/IP. Например, протокол определения адресов (Address Resolution Protocol, ARP) ппреобразует IP-адреса в физические сетевые адреса, такие, как идентифи- каторы Ethernet. Родственный протокол - протокол обратного преобразования адресов (Reverse Address Resolution Protocol, RARP) - выполняет обеспечивает обратное действие, преобразуя физические сетевые адреса в IP-адреса. Протокол управления сообщениями Internet (Internet Control Message Protocol, ICMP) представляет собой протокол сопровож- дения, который использует IP для обмена управляющей информацией и контроля над ошибками, относящимися к передаче пакетов IP. Например, если маршрутизатор не может передать IP-дейтаграмму, он использует ICMP, с тем чтобы информировать отправителя, что возникла проблема. Краткое описание некоторых других протоколов, которые "пря- чутся под зонтиком" TCP/IP, приведено во врезке.

# ПРАКТИЧЕСКАЯ ЧАСТЬ

#### Задание 1.

− Открыть окно командной строки, ввести команду ping с IP адресом машины, при взаимодействии с которой возникают проблемы.

− Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого досту- па.

− Перейдите по спискам элементов, используемых подключением, пока не дой- дете до TCP/IP протокола (выбран на рисунке 3). Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).

− Запишите IP конфигурацию машины. Особенно важно сделать заметки следу- ющих элементов:

− Использует ли машина статичную или динамичную конфигурацию?

− Если используется статичная конфигурация, запишите значение IP адреса, мас- ки подсети и основного шлюза?

− Получает ли машина адрес DNS сервера автоматически?

− Если адрес DNS сервера вводится вручную, то какой адрес используется?

− Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.

− Проверьте тип адаптера.

− Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: IPCONFIG /ALL.

− Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.

− Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: PING LOCALHOST.

− Введите команду Nslookup, за которой должно идти полное доменное имя уда- ленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP ад- рес.

− Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: IPCONFIG /FLUSHDNS.