

В конце 80-х, в 90-е годы XX века глобальная сеть Интернет еще не получила столь массового распространения, как в наши дни. В качестве сетевой операционной системы в то время чаще всего использовалось программное обеспечение от компании Novell – **Novell NetWare** и основными протоколами локальных сетей были протоколы **IPX/SPX** (**I**nternet **P**acket **eX**change/**S**equenced **P**acket **eX**change). Сейчас любая локальная сеть, как правило, имеет подключение к глобальной сети Интернет. В Интернет передача данных осуществляется с помощью протоколов **TCP/IP** (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) и в локальной сети эти протоколы оказываются также необходимы. Но использование протоколов стека **TCP/IP** позволяет решать и задачи обмена информацией между локальными компьютерами. Выпуск в 1999г. компанией Microsoft операционной системы Windows 2000, имеющей хорошую поддержку сетевых функций и достаточно качественных сетевых версий этой операционной системы, привел к массовому распространению локальных сетей, построенных на продуктах Microsoft. В таких локальных сетях нет необходимости в использовании протоколов IPX/SPX. Использование Novell NetWare в локальной сети усложняет работу администратора, поэтому администраторы локальных сетей все реже используют эту операционную систему. Применение в локальных сетях протоколов TCP/IP сближает их с глобальными компьютерными сетями в смысле использования подобных способов адресации и методов администрирования.

IP-адресация

Передача сообщений в Интернет основана на том, что каждый компьютер сети имеет индивидуальный адрес – IP-адрес. Этот адрес выражается одним 32-разрядным числом, имеющим две смысловые части. Одна часть IP-адреса определяет номер сети, вторая – номер узла(компьютера) в сети. Так как оперировать длинными двоичными числами достаточно сложно, число, определяющее IP-ад-

рес, разбивают на 4 октета – восьмиразрядных двоичных числа, а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса,
10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

В сети Интернет различные глобальные сети, в зависимости от размера, делятся по классам:

Сети класса А: большие сети общего пользования, первый октет определяет номер сети, три последующие октета – номер узла;

Сети класса В: сети среднего размера. Два первых октета определяют номер сети, два оставшихся – номер узла;

Сети класса С: сети малого размера. В этих сетях три первых октета определяют номер сети и последний октет – номер узла.

В таблице 1 представлена общая характеристика схемы Интернет-адресации.

Таблица 1

Класс	Диапазон значений первого октета	Общее количество сетей	Максимальное количество узлов в каждой сети
A	1 – 126	126	16 777 214
B	128 – 191	16 382	65 534
C	192 – 223	2 097 150	254

Некоторые IP-адреса имеют специальное назначение, например, адрес:

- 0.0.0.0 представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети;

рес, разбивают на 4 октета – восьмиразрядных двоичных числа, а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса,
10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

В сети Интернет различные глобальные сети, в зависимости от размера, делятся по классам:

Сети класса А: большие сети общего пользования, первый октет определяет номер сети, три последующие октета – номер узла;

Сети класса В: сети среднего размера. Два первых октета определяют номер сети, два оставшихся – номер узла;

Сети класса С: сети малого размера. В этих сетях три первых октета определяют номер сети и последний октет – номер узла.

В таблице 1 представлена общая характеристика схемы Интернет-адресации.

Таблица 1

Класс	Диапазон значений первого октета	Общее количество сетей	Максимальное количество узлов в каждой сети
A	1 – 126	126	16 777 214
B	128 – 191	16 382	65 534
C	192 – 223	2 097 150	254

Некоторые IP-адреса имеют специальное назначение, например, адрес:

- 0.0.0.0 представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети;

- 127.любое число (часто 127.0.0.1) – адрес «петли». Данные, переданные по этому адресу, поступают на вход компьютера, как полученные по сети. Такой адрес необходим при отладке сетевых программ;
- 255.255.255.255 – широковещательный адрес. Сообщения, переданные по этому адресу, получают все узлы локальной сети, содержащей компьютер-источник сообщения (в другие локальные сети оно не передается);
- Номер сети . все нули – адрес сети;
- Все нули . номер узла – узел в данной сети. Может использоваться для передачи сообщений конкретному узлу внутри локальной сети;
- Номер сети . все единицы (двоичные) – все узлы указанной сети.

В локальных сетях используются специальные, так называемые «серые» IP-адреса. Они определены документом RFC 1918 (RFC – Requests For Comments, предлагаемый проект стандарта, большинство документов, регламентирующих Интернет, описано в RFC) и приведены в табл. 2:

Таблица 2

Диапазоны IP-адресов, используемых в локальных сетях
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

В небольших по размеру локальных сетях обычно применяется последний диапазон адресов. Сетевые маршрутизаторы не передают информацию для узлов с этими адресами, поэтому она оказывается «запертой» внутри локальной сети. Такая схема позволяет в разных локальных сетях использовать одни и те же IP-адреса и не приводит к конфликтам.

Для повышения гибкости использования IP-адресов деление адреса на части с использованием классов дополняется технологией CIDR (Classless Inter-Domain Routing) – бесклассовой междоменной маршрутизации. В этом случае адрес сети формируется с помощью двух чисел: адреса и **маски**. Маска это тоже

32-разрядное двоичное число, с помощью которого из IP-адреса выделяется адрес сети. Схема формирования адреса сети с использованием маски проста, ее можно пояснить на примере, допустим, адрес представлен двоичным числом 110101, маска числом 111100. Маска накладывается на адрес, как трафарет, в котором единицы соответствуют прорезам, в которых мы «увидим» адрес сети, в нашем примере адрес сети соответствует числу 110100. Маска всегда содержит такое двоичное число, старшие разряды которого подряд единицы, а младшие – нули, единицы представляют «прозрачную» часть трафарета, а нули – «непрозрачную». Маска так же, как и адрес, записывается в виде четырех десятичных чисел, разделенных точками и представляющих двоичные октеты. Для компактной записи пары чисел: IP-адрес-маска, используется также другая форма, например: 10.0.0.8/30. Число до слеша представляет собой IP-адрес, а число после слеша – количество разрядов в IP-адресе, отводимых для адресации сети. Число 30 после слеша соответствует маске 255.255.255.252. После определения адреса сети, оставшаяся часть IP-адреса используется для адресации узлов в сети.

Символьное представление имени компьютера в сети

Каждый компьютер в сети имеет уникальный адрес. При использовании IP-адресации это IP-адрес. Однако человеку достаточно трудно оперировать длинными наборами цифр, не несущих смысловой нагрузки, поэтому всегда применяются системы преобразования имен, ставящие в соответствие цифровому адресу компьютера его символьное имя. В глобальных сетях и сети Интернет это служба DNS (Domain Name System) – распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Определенные части базы данных доменных имен хранятся на специальных серверах – DNS-серверах, обрабатывающих запросы любого компьютера и определяющие имя, соответствующее IP-адресу или наоборот. В каждой локаль-

ной сети, подключенной к Интернет, работает по крайней мере один DNS-сервер. База данных DNS имеет структуру дерева, называемого доменным пространством имен, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, а точки в имени отделяют части, соответствующие узлам домена, например, www.tusur.ru.

Для именования компьютеров в локальных сетях используются плоские (не имеющие иерархии) символьные имена, так называемые NetBIOS-имена. Протокол NetBIOS (Network Basic Input/Output System), как расширение стандартных функций базовой системы ввода-вывода, был разработан в 1984г. компанией IBM и широко применяется в ее продуктах, а также продуктах компании Microsoft. В протоколе NetBIOS реализован механизм широковещательного разрешения имен, когда все компьютеры в локальной сети получают запрос на разрешение имени, соответствующего некоторому IP-адресу. Кроме того, компания Microsoft для своей сетевой операционной системы Windows NT разработала централизованную службу разрешения имен WINS(Windows Internet Name Service). WINS-сервер, работающий в локальной сети, централизованно обрабатывает все запросы, касающиеся разрешения имен в сетях Windows. При большом числе компьютеров в локальной сети WINS-сервер необходим. Однако в малых сетях, содержащих менее 10 компьютеров, часто используется широковещательный механизм разрешения имен протокола NetBIOS, упрощающий административное обслуживание таких сетей.

Автоматизация процесса назначения IP-адресов узлам сети

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора достаточно сложную и длительную процедуру, если количество компьютеров в локальной сети достаточно велико. Если происходят изменения в сети, например, появляются новые компьютеры, процедуру необходимо выполнить и для них, а в некоторых случаях и выполнить коррек-

цию предыдущих настроек на уже работающих компьютерах. Протокол DHCP (Dynamic Host Configuration Protocol) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. В локальной сети, содержащей DHCP-сервер, каждый компьютер при включении посылает запрос этому серверу на получение IP-адреса. Способы выдачи адресов могут быть различными.

При автоматическом статическом способе выделения адреса DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IP-адресов. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом в этом случае, как и при ручном назначении, существует постоянное соответствие.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время (время подключения к сети), что дает возможность впоследствии повторно использовать этот же IP-адрес другими компьютерами (пользователями).

Адресация компьютеров на канальном уровне

Каждый компьютер, подключенный к сети, имеет сетевой адаптер (сетевую карту) с присвоенным ему адресом. Этот адрес носит название MAC-адреса, он задается при изготовлении сетевого адаптера и впоследствии не изменяется. Длина и другие особенности MAC-адреса зависят от используемой в локальной сети технологии. В сетях Ethernet MAC-адрес имеет длину 6 байт, записанных в шестнадцатеричном формате и разделенных дефисами (например 00-AA-00-4F-2A-9C). Для определения локального адреса по IP-адресу используется протокол разрешения адреса ARP (Address Resolution Protocol). Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется RARP – реверсивный ARP, и использу-

ется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения. Работа протокола ARP начинается с просмотра так называемой ARP-таблицы (рис.). Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Поле «Тип записи» может содержать одно из двух значений – «динамический» или «статический». Статические записи создаются вручную с помощью утилиты **arp** и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор не будут выключены. Динамические же записи создаются модулем протокола ARP, использующим широковещательные возможности локальных сетевых технологий. Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш. После того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес, а затем отправляет его уже по адресу

компьютера, сформировавшего запрос, так как в адрес отправителя указан в самом запросе.

Сетевые утилиты

В операционной системе Windows существует большое число утилит (специальных программ), предназначенных для управления и анализа сетевых соединений, рассмотрим три из них: IPCONFIG, ARP, NETSTAT.

Утилита IPCONFIG

Позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений, с ее помощью можно определить IP-адрес данного компьютера. Запущенная без параметров, команда `ipconfig` выдает в качестве результата текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений (рис. 1).

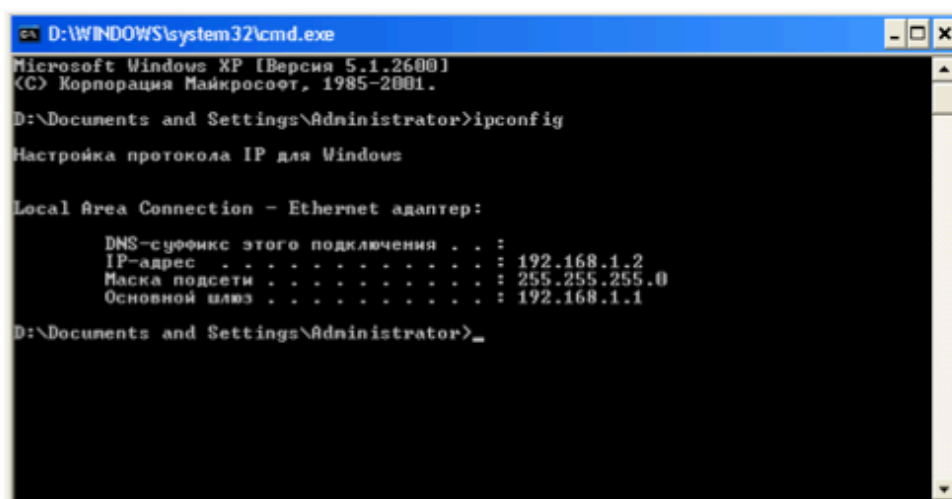
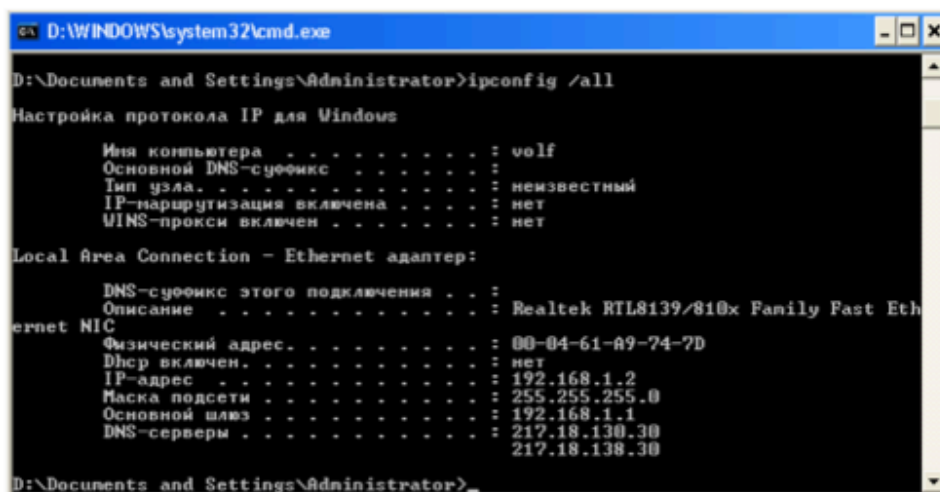


Рис. 1.

Команду `ipconfig` следует первой использовать для диагностирования возможных проблем с соединением TCP/IP. С ее помощью можно определить, был ли вообще назначен IP-адрес сетевому адаптеру, а также узнать адрес шлюза.

Запустив команду `ipconfig` с параметром `/all`, получаем большую часть информации, о параметрах настройки сетевого соединения и сетевом окружении (рис. 2).



```
D:\WINDOWS\system32\cmd.exe
D:\Documents and Settings\Administrator>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : volf
Основной DNS-суффикс . . . . . :
Тип узла . . . . . : неизвестный
IP-настройка включена . . . . . : нет
WINS-прокси включен . . . . . : нет

Local Area Connection - Ethernet адаптер:

DNS-суффикс этого подключения . . :
Описание . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
Физический адрес . . . . . : 00-04-61-A9-74-7D
DHCP включен . . . . . : нет
IP-адрес . . . . . : 192.168.1.2
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 192.168.1.1
DNS-серверы . . . . . : 217.18.130.30
                        217.18.138.30

D:\Documents and Settings\Administrator>
```

Рис. 2

Утилита NETSTAT

Команда позволяет получить подробную информацию о соединениях, активных в настоящее время. Дополнительные ключи позволяют также получить информацию о сетевых портах, об IP-адресах компьютеров, участвующих в подключении, а также о других сетевых параметрах.

Параметры:

- а Вывод всех активных подключений TCP и прослушиваемых компьютером портов TCP и UDP (рис.).
- е Вывод статистики Ethernet, например количества отправленных и принятых байтов и пакетов. Этот параметр может комбинироваться с ключом `-s`.
- n Вывод активных подключений TCP с отображением адресов и номеров портов в числовом формате без попыток определения имен.

```

D:\WINDOWS\system32\cmd.exe
Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние      PID
D:\Documents and Settings\Administrator>netstat -a
Активные подключения
Имя      Локальный адрес      Внешний адрес      Состояние
TCP      volf:epmap           volf:0             LISTENING
TCP      volf:microsoft-ds    volf:0             LISTENING
TCP      volf:1025            volf:0             LISTENING
TCP      volf:nethios-ssn     volf:0             LISTENING
UDP      volf:microsoft-ds    *:*
UDP      volf:isakmp          *:*
UDP      volf:1030            *:*
UDP      volf:4500            *:*
UDP      volf:ntp             *:*
UDP      volf:1900            *:*
UDP      volf:ntp             *:*
UDP      volf:nethios-ns      *:*
UDP      volf:nethios-dgm     *:*
UDP      volf:1900            *:*
D:\Documents and Settings\Administrator>

```

Рис. 3. Вывод активных подключений с помощью команды netstat.

-o вывод активных подключений TCP и включение кода процесса (PID) для каждого подключения. Код процесса позволяет найти приложение на вкладке **Процессы** диспетчера задач Windows. Этот параметр может комбинироваться с ключами **-a**, **-n** и **-p**.

-p *протокол* Вывод подключений для протокола, указанного параметром *протокол*. В этом случае параметр *протокол* может принимать значения **tcp**, **udp**, **tcpv6** или **udpv6**. Если данный параметр используется с ключом **-s** для вывода статистики по протоколу, параметр *протокол* может иметь значение **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6** или **ipv6**.

-s Вывод статистики по протоколу. По умолчанию выводится статистика для протоколов TCP, UDP, ICMP и IP. Если установлен протокол IPv6 для Windows XP, отображается статистика для протоколов TCP через IPv6, UDP через IPv6, ICMPv6 и IPv6. Параметр **-p** может использоваться для указания набора протоколов.

-r Вывод содержимого таблицы маршрутизации IP (рис.). Эта команда эквивалентна команде **route print**.

```

D:\WINDOWS\system32\cmd.exe
D:\Documents and Settings\Administrator>netstat -r

Таблица маршрутов
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 04 61 a9 74 7d ..... Realtek RTL8139 Family PCI Fast Ethernet NIC - P
acket Scheduler Miniport
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
-----
0.0.0.0            0.0.0.0         192.168.1.1      192.168.1.2    20
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
192.168.1.0        255.255.255.0   192.168.1.2      192.168.1.2    20
192.168.1.2        255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.1.255      255.255.255.255 192.168.1.2      192.168.1.2    20
224.0.0.0          240.0.0.0       192.168.1.2      192.168.1.2    20
255.255.255.255    255.255.255.255 192.168.1.2      192.168.1.2    1
Основной шлюз:
192.168.1.1
=====
Постоянные маршруты:
Отсутствует
D:\Documents and Settings\Administrator>

```

Рис. 4. Вывод таблицы маршрутизации с помощью команды netstat.

интервал

Обновление выбранных данных с интервалом, определенным параметром *интервал* (в секундах). Нажатие клавиш CTRL+C останавливает обновление. Если этот параметр пропущен, **netstat** выводит выбранные данные только один раз.

/? Отображение справки в командной строке.

Утилита ARP

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица. Запущенная без параметров, команда **arp** выводит справку.

Параметры

-а Вывод таблиц текущего протокола ARP для всех интерфейсов (рис. 5).


```
D:\Documents and Settings\Administrator>arp -a
Interface: 192.168.1.2 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           00-0f-a3-92-34-52     dynamic
D:\Documents and Settings\Administrator>
```

Рис. 5. Результат выполнения команды `arp -a`.

Чтобы вывести записи ARP для определенного IP-адреса, следует указать его после ключа через пробел:

Arp -a *IP-адрес*

Чтобы вывести таблицы кэша ARP для определенного интерфейса, следует указать параметр **-N**

Arp -a -N *иф_адрес*

иф_адрес, где *иф_адрес* – это IP-адрес, назначенный интерфейсу. Параметр **-N** вводится с учетом регистра.

-g Выполняет те же функции, что и **-a**.

-d *IP-адрес* [*иф_адрес*]

Выполняет удаление записи с определенным IP-адресом. Чтобы удалить запись таблицы для определенного интерфейса, следует указать этот интерфейс после IP-адреса. Чтобы удалить все записи, нужно ввести звездочку (*) вместо параметра *IP-адрес*.

-s *IP-адрес Ethernet_адрес* [*иф_адрес*]

Добавление статической записи, которая сопоставляет IP-адрес с физическим адресом в кэш ARP. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, следует указать параметр *иф_адрес*, где *иф_адрес* – это IP-адрес, назначенный интерфейсу.

/? Отображение справки в командной строке.

Выполнение лабораторной работы

Работа выполняется индивидуально. С помощью утилит IPCONFIG, ARP, NETSTAT необходимо получить информацию для заполнения таблиц 3-5.

Табл. 3

Символьное имя компьютера	Адрес локальной сети	IP-адрес компьютера	MAC-адрес компьютера	Используемая в локальной сети технология

Табл. 4

Таблица маршрутизации. Активные маршруты:				
Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика

Табл. 5

Таблица ARP-кэша:		
IP-адрес	MAC-адрес	Тип

Кроме этого, необходимо определить используются ли в локальной сети серверы DNS, WINS, DHCP и если используются, указать их IP-адреса.

Контрольные вопросы

1. Почему IP-адресация используется не только в глобальных, но и в локальных компьютерных сетях.
2. Назовите диапазоны IP-адресов, специально предназначенные для использования в локальных сетях.
3. Каково назначение сервера WINS, что произойдет, если такой сервер отсутствует в локальной сети.

4. Какие операции можно выполнить с использованием команды NETSTAT.
5. Можно ли с помощью команды IPCONFIG назначить IP-адрес компьютеру.
6. Почему для одного и того же компьютера используется несколько различных типов адресов.
7. Как определить MAC-адрес сетевого адаптера, установленного в компьютере.
8. Какие функции выполняет сервер DHCP в локальной сети.
9. Символьные имена какого типа используются в локальных компьютерных сетях.
10. Как определить адрес, принадлежащий всей локальной сети, по IP-адресу одной из рабочих станций.