**РАБОТА 1.**
**КОМАНДЫ ДИАГНОСТИКИ СЕТИ**
Команды тестирования сети входят в состав сетевых операционных
систем и позволяют просмотреть параметры отдельных узлов сети, про
верить их работоспособность и в случае обнаружения проблемы – опре
делить проблемный участок.
**Используемые утилиты**
**Программа ipconfig**
Консольная утилита ipconfig предназначена для отображения
всех текущих значений конфигурации сети TCP/IP, а также обновления
параметров DHCP и DNS. Полезнее всего данная утилита в тех ситуаци
ях, когда конфигурация сети устанавливается автоматически и требует
ся определить присланные DHCP-сервером параметры.
При использовании без параметров, утилита ipconfig отобража
ет IP-адрес, маску сети, шлюз по умолчанию и другую информацию для
каждого из адаптеров. Кроме того, могут использоваться следующие
ключи:
/all Отобразить полную конфигурацию TCP/IP для всех адапте
ров. Без этого параметра ipconfig отображает только основные данные.
Адаптеры представляют как физические интерфейсы, например, сете
вые карты, так и логические интерфейсы, такие как установленные со
единения или виртуальные адаптеры.
/renew Обновить конфигурацию DHCP для всех (или указанного)
адаптера. Действует только на компьютерах с автоматической конфигу
рацией DHCP.
/release Отправить сообщение DHCPRELEASE серверу DHCP,
чтобы освободить IP-адрес и удалить конфигурацию на всех (или ука
занном) адаптере.
/flushdns Очистить содержимое кэша DNS-клиента.
/displaydns Отобразить содержимое DNS-клиента, включая за
писи, находящиеся в файле hosts.
/registerdns Ручная регистрация DNS-имени и IP-адреса. Мо

**Программа ping**
Консольная утилита ping проверяет IP-соединение с другим ком
пьютером TCP/IP посылая ему эхо-запрос (Echo Request) по протоколу
ICMP. Полученные эхо-ответы отображаются вместе с длительностью
запроса. Ping это основная команда для диагностики соединения, дос
тупности и разрешения имен.
При запуске без параметров утилита отображает справку. При за
дании имени хоста или IP-адреса утилита проверяет доступность хоста.
Также могут использоваться следующие параметры:
-t Бесконечный цикл отправки эхо-запросов. Прерывание осуще
ствляется клавишами <Ctrl>+<C>.
-n Указывает количество эхо-запросов, по умолчанию 4.
-l Указывает длину поля данных эхо-запроса. Значение по умол
чанию 32, максимальное значение 65527.
-i Указывает значение поля TTL в заголовке IP для эхо-запроса.
Для Windows XP это значение обычно равно 128, максимальное значе
ние 255.
-w Указывает время ожидания эхо-ответа (в миллисекундах). Если
время ожидания будет превышено, утилита отобразит сообщение «Пре
вышен интервал ожидания для запроса». Значение по умолчанию – 4000
(4 секунды).
**Программа tracert**
Консольная утилита tracert определяет путь до точки назначе
ния, отправляя ICMP эхо-запросы с увеличивающимся значением поля
Time to Live (TTL). Путь отображается в виде списка маршрутизаторов
между исходным и конечным хостами.
Каждый маршрутизатор по пути следования пакета уменьшает по
ле TTL на единицу. Таким образом, поле TTL означает максимальное
количество маршрутизаторов, по которым пройдёт IP-пакет. Когда поле
TTL становится равным нулю, маршрутизатор должен удалить пакет и
вернуть ICMP-сообщение исходному компьютеру. Утилита Tracert
определяет путь путём отправки первого эхо-пакета со значением TTL
равным 1 и увеличивает его на единицу для каждого последующего па
кета до максимального количества прыжков. Путь определяется по со

При использовании без параметров утилита отображает справку.
При задании имени хоста или IP-адреса утилита отображает пусть к
хосту. Также могут использоваться следующие параметры:
-d Отключить разрешение IP-адресов в имена для маршрутизато
ров. Используется для ускорения работы утилиты за счёт меньшей
наглядности.
-h Задаёт максимальное количество прыжков в пути поиска хоста
назначения. Значение по умолчанию – 30.
-w Задаёт значение времени ожидания (в миллисекундах). Если от
вет не был получен в течение указанного времени, отображается звез
дочка (\*). Значение по умолчанию – 4000 (4 секунды).
**Программа nslookup**
Консольная утилита nslookup служит для диагностики инфра
структуры системы доменных имен (DNS).
При запуске без параметров утилита входит в интерактивный ре
жим и ожидает ввода команд, поэтому проще запускать утилиту с ука
занием требуемого имени хоста или IP-адреса.
В интерактивном режиме программа позволяет узнать больше па
раметров об интересующем домене. Например, команда
set type=ANY
даст DNS-серверу указание выводить все поля для указанного до
мена, после чего можно набрать имя домена
tpu.ru
и программа покажет все доступные для данного домена DNS
записи. Более подробную информацию о командах интерактивного ре
жима можно получить, набрав в интерактивном режиме команду help.
**Программа netstat**
Консольная утилита netstat отображает активные
TCP-соединения, порты, которые прослушиваются на компьютере, ста
тистику Ethernet, таблицу маршрутизации, статистику IPv4 (для прото
колов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP
через IPv6 и UDP через IPv6).

-e Отобразить статистику Ethernet, например, количество пере
еденных и полученных байт и пакетов. Данный ключ может быть ском
бинирован с ключом -s.
-n Отобразить активные TCP-соединения, но адреса и порты ото
бразить числами, не именами.
-o Отобразить активные TCP-соединения и включить идентифика
торы процессов для каждого соединения. Идентификаторы процессов
могут быть сопоставлены с процессами в Диспетчере задач.
-p Отобразить соединения по указанному протоколу (tcp, udp,
tcpv6 или udpv6). Можно скомбинировать данный ключ с ключом -s для
отображения статистики – в этом случае протоколы могут быть tcp, udp,
icmp, ip, tcpv6, udpv6, icmpv6 или ipv6.
-s Отобразить статистику по протоколам.
-r Отобразить содержимое таблицы маршрутизации.
**Задание**
Использовать команды сетевой диагностики nslookup, ping,
tracert для получения информации о двух доменах, проверки их рабо
тоспособности, отслеживания пути. Домены можно выбрать произволь
ные, но не рекомендуется использовать домены томской сети, а также
широко известные домены (такие, как google.com или yandex.ru).
Использовать команду ipconfig для выяснения IP-адреса компь
ютера, маски сети и шлюза по умолчанию, а также дополнительных па
раметров. Отобразить кэш DNS.
Использовать команду netstat для отображения статистики про
токолов и открытых соединений/портов. Привести список процессов,
прослушивающих порты.
Для каждой из команд следует постараться максимально использо
вать доступные опции.

**РАБОТА 2.**
**АНАЛИЗ ПАКЕТОВ ЛОКАЛЬНОЙ СЕТИ**
В обычном режиме работы сетевая карта узла обрабатывает только
те пакеты, которые адресованы данному узлу, или же всем узлам сети,
если пакет широковещательный. Однако существует и другой режим
работы сетевой карты – так называемый *неразборчивый режим* (Promis
cuous mode), в котором сетевая карта получает все проходящие по сети
пакеты.
Поскольку данный режим позволяет при определенных условиях
перехватывать и анализировать трафик, предназначенный для чужих
узлов, использование данного режима является незаконным в ряде
стран, но даже если закон не запрещает его использование явно, пере
хват чужих данных может привести к возникновению административ
ной или уголовной ответственности. Тем не менее, данный режим поле
зен в ряде случаев администраторам сети, поскольку позволяет отсле
дить проблемный трафик (например, широковещательный шторм) и вы
яснить его причину.
Анализатор трафика (sniffer, сниффер) – это программа, предназна
ченная для перехвата и анализа сетевого трафика.
Чтобы перевести сетевую карту в неразборчивый режим, требуют
ся привилегии администратора локальной машины, поэтому данная ла
бораторная работа в учебной аудитории выполняется на виртуальной
машине.
**Задание**
Выполнить захват трафика, произвести его анализ. Уметь объяс
нять все параметры пакетов, выводимые сниффером.
Запустите программу Wireshark с административными привиле
гиями.
1) В секции *Capture* в окне программы Wireshark выберите сете
вую карту, подключенную к интернету.
2) Откройте какой-либо сайт в браузере.
3) С помощью фильтра на панели инструментов отфильтруйте за
4) Скопируйте в отчёт строки анализатора трафика, относящиеся к
следующим событиям (если за время захвата трафика было установлено
несколько TCP-соединений, удалите из отчёта лишние строки):
a) установка TCP-соединения;

b) передача данных;
c) завершение TCP-соединения.
5) Закройте Wireshark (на вопрос программы о сохранении ре
зультатов ответьте отрицательно).

**РАБОТА 3.**
**РАЗБИЕНИЕ НА ПОДСЕТИ**
*Префикс сети* показывает количество бит, отводимых под номер
сети. Оставшиеся биты отведены под номер хоста. Например, префикс
/24 говорит о том, что старшие 24 бита адреса отводятся под номер сети,
а оставшиеся (32–24)=8 бит – под номер хоста.
Исходя из количества бит, отводимых под номер хоста, можно оп
ределить максимальное количество компьютеров в подсети. Так, с по
мощью восьми бит можно закодировать 256 различных чисел, однако
первое и последнее число не могут использоваться в качестве номеров
хостов, поскольку им назначена особая роль. Если в номере хоста все
биты равны нулю, то такой адрес называется *номером сети*. Если же в
номере хоста все биты равны единице, то такой адрес является *широко*
*вещательным адресом* для данной сети.
**Пример:**
IP-адрес: 192.168.1.18 /24
В двоичном виде: 11000000 10101000 00000001 00010010
Маска: 11111111 11111111 11111111 00000000
Номер сети: 11000000 10101000 00000001 **00000000**
Широковещат. адрес: 11000000 10101000 00000001 **11111111**
Кроме номера сети и широковещательного адреса подсеть обычно
содержит шлюз, роль которого, как правило, выполняет один из интер
фейсов маршрутизатора. Часто шлюз получает первый либо последний
адрес, который можно назначить хосту.
Подсеть разбивается на более мелкие подсети увеличением пре
фикса подсети. Поскольку префикс задаёт количество бит в номере се
ти, такая операция всегда делит общее количество адресов подсети, на
число, кратное степени двойки.
**Пример:**
Исходная подсеть: 192.168.1.0 /24
В двоичном виде: **11000000 10101000 00000001** 00000000
Новые подсети: 192.168.1.0 /25
192.168.1.128 /25
Маска: 11111111 11111111 11111111 10000000
Таким образом, процесс разбиения исходной сети на нужное коли
чество подсетей сводится к дихотомическому делению исходной подсе
ти до тех пор, пока для каждого набора компьютеров не будет найдена
сеть минимально необходимого размера.
Каждая пара маршрутизаторов также соединяется между собой от
дельной подсетью. Поскольку такая подсеть содержит только два хоста,
для неё достаточно использовать префикс подсети /30.
**Методика выполнения**
Исходную сеть и её подсети можно представить в виде графа, вер
шиной которого будет исходная сеть, а каждый дочерний узел получа
ется в результате разбиения сети на две подсети:


Рис. 1. Граф подсетей
Деление продолжается до тех пор, пока для каждой физической
подсети не будет найдена подходящая по размерам подсеть.
Другой наглядный метод разбиения на подсети заключается в ис
пользовании программ для работы с электронными таблицами, напри
мер, Microsoft Excel. Каждая ячейка представляет некоторый диапазон
адресов, например, подсеть с префиксом /30. Объединенные ячейки
представляют собой более крупные сети, которые затем можно делить


Разумеется, оба эти способа позволяют узнать лишь начальный ад
рес подсети, остальные данные необходимо рассчитать на основе этих
данных.
**Задание**
Используя схему сети, приведенную на рис. 3, а также информацию
о количестве компьютеров в отделах предприятия (табл. 3), разбей
те сеть на соответствующее количество подсетей.

Разбиение должно быть оптимальным, то есть не следует использо
вать для отдела подсеть, если достаточно будет половины подсети. Что
бы увеличить эффективность распределения адресов, лучше всего вы
делять подсети для отделов, начиная с самого большого и далее по
уменьшению.
В отчете приведите:
1) схему сети с подписанными подсетями;
2) параметры каждой подсети:
a) адрес сети (в двоичном и десятичном виде);
b) префикс;
c) маска (в двоичном и десятичном виде);
d) широковещательный адрес
e) адрес шлюза;
f) максимальное количество хостов;



