Владимирский государственный университет

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным занятиям

Владимир 2022

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным занятиям

Составитель
С. В. КУРОЧКИН

Электронное издание

Владимир 2022

УДК 004.7
ББК 32.97135

Рецензент
Кандидат технических наук
доцент кафедры радиотехники и радиосистем
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
Н. Н. Корнеева

Компьютерные сети [Электронный ресурс] : метод. указания к лаб. занятиям / Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых ; сост. С. В. Курочкин. – Владимир : Изд-во ВлГУ, 2022. – 35 с. – Электрон. дан. (688 Кб). – 1 электрон. опт. диск (DVD-ROM). – Систем. требования: Intel от 1,3 ГГц ; Windows XP/7/8/10 ; Adobe Reader ; дисковод DVD-ROM. – Загл. с титул. экрана.

Содержат методические указания для выполнения лабораторных занятий по дисциплинам «Компьютерные сети» и «Информационные сети».

Предназначены для студентов высших учебных заведений, обучающихся по специальностям 09.03.02 «Информационные системы и технологии», 09.03.04 «Программная инженерия», а также для студентов СПО, обучающихся по специальности 09.02.07 «Информационные системы и программирование».

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО и СПО.

Табл. 18. Библиогр.: 2 назв.

УДК 004.7
ББК 32.97135

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Материал методических указаний призван дать студентам навыки по организации и конфигурированию компьютерных сетей, их созданию и анализу, а также эффективному использованию, в том числе аппаратных и программных компонентов. Выполнение цикла лабораторных занятий позволит студентам:

- работать с протоколами разных уровней (например, стека протоколов: TCP/IP, IPX/SPX);
- устанавливать и настраивать параметры протоколов;
- обнаруживать и устранять ошибки при передаче данных.

Лабораторная работа 1
РАБОТА С ДИАГНОСТИЧЕСКИМИ УТИЛИТАМИ ПРОТОКОЛА TCP/IP

Цель работы: практически освоить работу с утилитами стека TCP/IP.

Диагностические утилиты TCP/IP

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения (табл. 1).

1. Проверка правильности конфигурации TCP/IP с помощью ipconfig

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита **ipconfig**.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all **-** выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] **-** обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] **-** освобождает выделенный DHCP IP-адрес;

adapter – имя сетевого адаптера;

displaydns **-** выводит информацию о содержимом локального кэша клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита **ipconfig** позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP-адреса:

- если конфигурация инициализирована, то появляется IP-адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;

- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0.

Таблица 1

Перечень диагностических утилит TCP/IP

Утилита	Применение
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу)
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
telnet	Осуществляет соединение с другим хостом по протоколу эмуляции терминала TELNET. Используется для проверки работоспособности сетевых служб, использующих tcp-порты (например, возможности соединения с почтовым сервером по протоколам POP3 и SMTP).

2. Тестирование связи с использованием утилиты ping

Утилита **ping** (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование **ping** лучший способ проверки того, что между локальным

компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда **ping** проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. **Ping** ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений **ping** станет ясно, сколько пакетов потеряно.

По умолчанию передается четыре эхо-пакета длиной 32 байта (возможны и другие варианты значения по умолчанию) - периодическая последовательность символов алфавита в верхнем регистре. **Ping** позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни ***(ttl)*** устанавливать, можно ли фрагментировать пакет и т. д.. При получении ответа в поле ***time*** указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение ***«Request time out»*** (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа ***–w***.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если **ping** с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Утилита **ping** используется следующими способами:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде **ping** задается адрес петли обратной связи ***(loopback address)***: ***ping 127.0.0.1***

Если тест успешно пройден, то вы получите следующий ответ:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

ping [IP-адрес_локального_хоста]

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping [IP-адрес_шлюза]

4) Для проверки возможности установления соединения через маршрутизатор в команде **ping** задается IP-адрес удаленного хоста:

Ping [IP-адрес_удаленного хоста]

Синтаксис:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] |

[-k host-list]] [-w timeout] destination-list

Параметры:

-t - выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a - позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count - посылает количество пакетов ECHO, указанное параметром count;

-l length - посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f - посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl - устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos - устанавливает тип поля «сервис» в величину tos;

-r count - записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count - позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list **-** направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list **-** направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout **-** указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

destination-list **-** указывает удаленный хост, к которому надо направить пакеты ping.

3. Изучение маршрута между сетевыми соединениями с помощью утилиты tracert.

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита **tracert** может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*****), либо сообщения типа *«Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded»*.

Утилита **tracert** работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра **-** ***w***). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP «*Time*

Exeeded» (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра ***- h***).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите **tracert**.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [имя_целевого_хоста]

Параметры:

-d **-** указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops **-** указывает максимальное число хопов для того, чтобы искать цель;

-j host-list **-** указывает нежесткую статическую маршрутизацию в соответствии с ***host-list***;

-w timeout **-** указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

4. Утилита arp.

Основная задача протокола **ARP** – трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

Синтаксис:

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]

Параметры:

-s **-** занесение в кэш статических записей;

-d **-** удаление из кэша записи для определенного IP-адреса;

-a **-** просмотр содержимого кэша для всех сетевых адаптеров локального компьютера;

inet_addr **-** IP-адрес;

eth_addr - MAC-адрес.

5. Утилита route.

Утилита **route** предназначена для работы с локальной таблицей маршрутизации. Она имеет следующий

Синтаксис:

route [-f] [-p] [команда [узел] [MASK маска] [шлюз] [METRIC метрика] [IF интерфейс]]

Параметры:

-f **-** Очистка таблицы маршрутизации;

-p **-** при указании совместно с командой ADD создает постоянную запись, которая сохраняется после перезагрузки компьютера, по умолчанию записи таблицы маршрутов не сохраняются при перезагрузке;

- ***команда*** **-** одна из четырех команд:

а) ***PRINT*** - вывод информации о маршруте;

б) ***ADD*** - добавление маршрута;

в) ***DELETE*** - удаление маршрута;

г) ***CHANGE*** - изменение маршрута.

- ***узел*** **-** адресуемый узел;

маска **-** маска подсети; по умолчанию используется маска 255.255.255.255;

шлюз **-** адрес шлюза;

метрика **-** метрика маршрута;

интерфейс **-** идентификатор интерфейса, который будет использован для пересылки пакета

Для команд ***PRINT*** и ***DELETE*** возможно использование символов подстановки при указании адресуемого узла или шлюза. Параметр шлюза для этих команд может быть опущен. При добавлении и изменении маршрутов утилита route осуществляет проверку введенной информации на соответствие условию (УЗЕЛ & МАСКА) == УЗЕЛ. Если это условие не выполняется, то утилита выдает сообщение об ошибке и не добавляет или не изменяет маршрут. Утилита осуществляет поиск имен сетей в файле *networks*. Поиск имен шлюзов осуществляется в

файле hosts. Оба файла расположены в папке *%systemroot%\system32\drivers\etc*. Наличие и заполнение этих файлов не обязательно для нормального функционирования утилиты route и работы маршрутизации. Хотя в большинстве случаев на рабочей станции это не требуется, можно вручную редактировать таблицы маршрутизации.

6. Утилита netstat.

Утилита **netstat** позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Синтаксис:

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]

Параметры:

-a **-** выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e **-** выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n **-** выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s **-** выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет просмотреть информацию постранично;

-r **-** выводит содержимое таблицы маршрутизации.

7. Утилита nslookup.

Утилита **nslookup** предназначена для диагностики службы DNS, в простейшем случае - для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса. В общем случае утилита позволяет просмотреть любые записи DNS-сервера:

- ***A*** – каноническое имя узла, устанавливает соответствие доменного имени ip-адресу.

- ***SOA*** – начало полномочий, начальная запись, единственная для зоны;

- ***MX*** – почтовые серверы (хосты, принимающие почту для заданного домена);

- ***NS*** – серверы имен (содержит авторитетные DNS-серверы для зоны);

- ***PTR*** – указатель (служит для обратного преобразования ip-адреса в символьное имя хоста)

- и т. д.

Утилита **nslookup** достаточно сложна и содержит свой собственный командный интерпретатор. В простейшем случае (без входа в командный режим) утилита ***nslookup*** имеет следующий с**интаксис:**

nslookup хост [сервер]

Параметры:

хост - DNS-имя хоста, которое должно быть преобразовано в IP-адрес.

сервер - Адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут последовательно использованы адреса DNS-серверов из параметров настройки протокола TCP/IP.

Задания для выполнения работы

1. Получение справочной информации по командам.

Выведите на экран справочную информацию по всем рассмотренным утилитам (см. таблицу п.1). Для этого в командной строке введите имя утилиты без параметров. Для получения справочной информации по ***nslookup*** необходимо войти в командный режим, набрав ***nslookup*** без параметров, и ввести команду ***help***.

Изучите ключи, используемые при запуске утилит.

2. Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды ***hostnam***е.

3. Изучение утилиты ***ipconfig***.

Проверьте конфигурацию TCP/IP с помощью утилиты ***ipconfig***. Заполните в отчете таблицу с данными.

4. Тестирование связи с помощью утилиты ***ping***.

Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере. Проверьте, правильно ли добавлен в сеть

локальный компьютер и не дублируется ли IP-адрес. Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта. Проверьте возможность установления соединения с удаленным хостом. С помощью команды ***ping*** проверьте перечисленные ниже адреса и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ***ping*** таким образом, чтобы увеличилось время отклика. Определите IP-адрес любого узла из локальной сети

Данные сети

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

5. Определение пути IP-пакета.

С помощью команды ***tracert*** проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Время жизни установить равным 10. Отметьте их для адресов 195.82.146.114, 213.247.189.211.

6. Просмотр ARP-кэша

С помощью утилиты ***arp*** просмотрите ARP-таблицу локального компьютера.

Внести в кэш локального компьютера любую статическую запись.

7: Просмотр локальной таблицы маршрутизации.

С помощью утилиты ***route*** просмотреть локальную таблицу маршрутизации.

8. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты ***netstat*** выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

9. Получение DNS-информации с помощью ***nslookup***.

Узнайте ip-адреса узлов по индивидуальному заданию

Узнайте авторитетные (компетентные) сервера для этих узлов.

Получите запись SOA с одного из этих серверов для домена по индивидуальному заданию.

Вопросы для самоконтроля

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.
2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
3. Каким образом каманда ping проверяет соединение с удаленным хостом?
4. Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
5. Как работает утилита tracert?
6. Каково назначение протокола ARP?
7. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?
8. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
9. Объяснить, каким образом при неудачной проверке маршрута до хоста 213.247.189.211, к нему возможно подключиться через telnet.
10. Всегда ли можно узнать символьное имя узла по его ip-адресу?
11. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Лабораторная работа 2
РЕШЕНИЕ ПРОБЛЕМ С TCP/IP

Цель работы: обобщение и систематизация знаний по теме «Организация межсетевого взаимодействия»

Применение диагностических сетевых утилит

1. Проверка правильности конфигурации TCP/IP. При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig. Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

2. Тестирование связи с использованием утилиты ping. Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP. Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно. По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1

секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение ``Request time out'' (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа -w. Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем - неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

3. Изучение маршрута между сетевыми соединениями с помощью утилиты tracert. Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого. Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа ``Destination net unreachable'', ``Destination host unreachable'', ``Request time out'', ``Time Exeeded''. Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP ``Time Exeeded'' (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h). Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

4. Утилита ARP. Основная задача протокола ARP - трансляция IP-адресов в соответствующие локальные адреса. Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.

5. Утилита netstat. Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.

Задания для выполнения

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 доступа.

2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола. Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).

3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:

Использует ли машина статичную или динамичную конфигурацию?

Если используется статичная конфигурация, запишите значение IP адреса, маски 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.

5. Проверьте тип адаптера.

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

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

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

- *PING*
- *LOCALHOST*

9. Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP-адрес.

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

Вопросы для самоконтроля

1. Поясните, что может означать, если время TTL закончилось до получения ответа.

2. Как подтвердить наличие сетевого соединения?

3. Что показывает команда IPCONFIG /ALL?

4. Что означает наличие IP адрес со значением 0.0.0.0.?

5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает корректно, и что отсутствуют проблемы с стеком локального протокола TCP/IP?

6. Как производится опрос основного шлюза?

7. Как производится опрос DNS сервера?

Лабораторная работа 3
ПРЕОБРАЗОВАНИЕ ФОРМАТОВ IP-АДРЕСОВ. РАСЧЕТ IP-АДРЕСА И МАСКИ ПОДСЕТИ

Цель работы: приобретение навыков классификации и анализа IP-адресов.

IP-адреса. Введение

В IP-сетях все сетевые устройства (хосты, серверы, шлюзы, маршрутизаторы и т.д.) получают уникальные IP-адреса.

IP-адрес состоит из четырех байтов (32 битов). Этот адрес используется на сетевом уровне эталонной модели OSI. Он делится на две части. Первая часть IP-адреса задает сеть, в которой располагается сетевое устройство. Вторая часть IP-адреса однозначно задает само сетевое устройство. Для обозначения сетевых устройств используют различные термины:

- хост;
- сетевой интерфейс.
-

Таблица 2

Конструкция IP-адреса

0 1 2 …			… 29 30 31
Ключ	Номер сети		Номер устройства в сети

Адресное пространство IP-протокола делится на три класса -**A**, **B**, **C**.

Таблица 3

Адрес класса «А»

0	1 2 3 … 7	8 … … 29 30 31
0		
Номер сети		Номер устройства

Таблица 4

Адрес класса «В»

0 1	2 3 4 … …15	16… … 29 30 31
1 0		
Номер сети		Номер устройства

Таблица 5

Адрес класса «С»

0 1 2	3 4 5 … …23	24… … 29 30 31
11 0		
Номер сети		Номер устройства

IP-адреса класса «А»

Сети класса **А** имеют 8-битный сетевой префикс «/8».

Таблица 6

Структура адреса класса «А»

0	1 2 3 … 7	8 … … 29 30 31
0		
Номер сети		Номер устройства

Максимальное число сетей класса «**А**» составляет 2^7 - 2 = 126. Каждая сеть класса «**А**» поддерживает до 2^{24} - 2 = 16 777 214сетевых устройств. Адресное пространство, выделенное классу «**А**»**,** занимает 50% общего адресного пространства сети Интернет.

Таблица 7

Диапазон сетевых адресов сетей класса «А»

Класс адреса	Диапазон значений
А	**1.0.0.0—126.255.255.255**

Примеры адресов сетей класса «**А**»:
1.100.120.148
98.180.220.250
121.196.244.198

IP-адреса класса «В»

Сети класса **В** имеют 16-битный сетевой префикс «/16».

Таблица 8

Структура адреса класса «B»

0 1	2 3 4 … …15	16… … 29 30 31
1 0		
Номер сети		Номер устройства

Максимальное число сетей класса «**B**» составляет 2^{14} = 16384. Каждая сеть класса «**B**» поддерживает до 2^{16} - 2 = 65 534 сетевых устройств. Адресное пространство, выделенное классу «**B**»**,** занимает 25%общего адресного пространства сети Интернет.

Таблица 9

Диапазон сетевых адресов сетей класса «B»

Класс адреса	Диапазон значений
B	**128.0.0.0—191.255.255.255**

Примеры адресов сетей класса «**B**»:
128.100.120.148
164.180.220.250
190.196.244.198

IP-адреса класса «C»

Сети класса «**C**» имеют 24-битный сетевой префикс «/24».

Таблица 10

Структура адреса класса «C»

0 1 2	3 4 5 … …23	24… … 29 30 31
11 0		
Номер сети		Номер устройства

Максимальное число сетей класса **C** составляет 2^{21} = 2 097 152. Каждая сеть класса C поддерживает до 2^{8} - 2 = 254 сетевых устройств. Адресное пространство, выделенное классу **C,** занимает 12.5%общего адресного пространства сети Интернет.

Таблица 11

Диапазон сетевых адресов сетей класса «C»

Класс адреса	Диапазон значений
C	**192.0.0.0—223.255.255.255**

Примеры адресов сетей класса «**C**»:
192.100.120.148
212.180.220.250
223.196.244.198

Остальные IP-адреса

Оставшийся резерв IP-адресов отводится классам сетей, указанным в табл. 12.

Таблица 12

Прочие классы IP-адресов

Класс адреса	Диапазон значений
D	**224.0.0.0—239.255.255.255**
E	**240.0.0.0—247.255.255.255**
Резерв	**248.0.0.0—254.255.255.255**

В сетях класса «**D**» первые (0..3) биты адреса имеют значение **1110**. Адреса этого класса используются для поддержки групповой передачи данных. В сетях класса «**E**» первые (0..4) биты адреса имеют значение **11110**. Адреса этого класса зарезервированы для экспериментального использования.

Запись IP-адреса в различных нотациях

В табл. 13 представлена запись IP-адресов в 2-ой, 16-ой, точечно-десятичной нотациях.

Таблица 13

Примеры записи IP-адресов

0111 1001	1100 0100	1111 0100	1100 0110
79	C4	F4	C6
121.196.244.198			
1001 1001	1110 0110	1101 1010	1011 0111
99	E6	DA	B7
153.230.218.183			
1101 1110	0110 0101	0111 0101	1100 0110
DE	65	75	78
222.101.117.120			

Маска сети

Маска сети представляет собою 32-разрядный адрес, 8, 16, 24старших разрядов которого заполнены «1»**.** Маски сетей классов «**A**», «**B**», «**C**» представлены в табл. 14-17.

Таблица 14

Маска IP-адресов класса «A»

0 1 2 3 … 7	8… … 29 30 31
11111111	**00000000 00000000 00000000**
FF	**00 00 00**
255.0.0.0	
Маска сети	Номер устройства

Таблица 15

Маска IP-адресов класса «B»

0 1 2 3 4… …15	16… … 29 30 31
11111111 11111111	**00000000 00000000**
FF FF	**00 00**
255.255.0 . 0	
Маска сети	Номер устройства

Таблица 16

Маска IP-адресов класса «С»

0 1 2 3 4 5… …23	24… … 29 30 31
11111111 11111111 11111111	**00000000**
FF FF FF	**00**
255.255.255. 0	
Маска сети	Номер устройства

Таблица 17

Примеры масок сетей

IP-адрес	**Маска**
192.100.120.148	255.255.255.0
10.190.178.177	255.0.0.0
144.100.137.125	255.255.0.0
123.119.137.223	255.0.0.0
222.110.170.190	255.255.255.0

Специальные IP-адреса

Некоторые IP-адреса используются для специальных целей.

Таблица 18

Специальные IP-адреса

IP-адрес	**Пояснение**
0.0.0.0	Данный хост (любой сети)
0.200.150.100	Хост данной сети (класс А)
0.0.150.100	Хост данной сети (класс В)
0.0.0.100	Хост данной сети (класс С)
100.0.0.0	IP-адрес сети (класс А)
150.200.0.0	IP-адрес сети (класс В)
200.220.240.0	IP-адрес сети (класс С)
255.255.255.255	Широковещание в данной сети (любого класса)
100.255.255.255	Широковещание в удаленной сети класса А
150.200.255.255	Широковещание в удаленной сети класса В
200.220.240.255	Широковещание в удаленной сети класса С
127.X.X.X	Тестирование сетевого программного обеспечения

IP-адресация в подсетях

По мере роста сети Интернет все острее стала ощущаться нехватка сетевых адресов. В 1985 году данная проблема была разрешена посредством введения подсетей. Подсети формировались посредством деления IP-адреса на части, именно: номер сетевого устройства сети делится на 2 части:

• номер подсети;

• номер сетевого интерфейса в этой подсети.

Двухуровневая сетевая иерархия (без подсетей): номер сети и номер хоста в сети. Трехуровневая сетевая иерархия (с подсетями): номер сети, номер подсети и номер хоста в подсети.

Внешние маршрутизаторы (внешние по отношению к сети с заданным №) используют деление IP-адреса на 2 части: № сети и № хоста в сети (как будто никаких подсетей нет). Внутренние маршрутизаторы (функционирующие внутри сети с заданным №) используют деление IP-адреса на 3 части: № сети, № конкретной подсети и № конкретного хоста в конкретной подсети. Внешние маршрутизаторы используют в качестве сетевого префикса только адрес сети.

Внутренние маршрутизаторы используют так называемый расширенный сетевой префикс, включающий как адрес сети, так и подсети.

Пример 1.

Предположим, в сети класса «**B**», сетевой префикс которой имеет значение **150.160.0.0**, сетевой администратор 3-ий байтсетевого адреса отвел под адреса подсетей:

1-ый и 2-ой байты	3-ий байт	4-ый байт0
№ сети	№ подсети	№ хоста

В этом случае мы получаем следующие параметры сетевой архитектуры:
класс сети «**B**»:

• размер сетевого префикса: 16 разрядов;

• маска сети: **255.255.0.0**;

• адрес сети: **150.160.0.0/16**;

• размер расширенного сетевого префикса: 24 разряда;

• маска подсетей: **255.255.255.0**;

• адреса подсетей:

• **150.160.0.0/24**;

• **150.160.1.0/24**;

• **150.160.2.0/24**;
• **...** ;
• **150.160.254.0/24**;
• **150.160.255.0/24**.

Пример 2.

По заданному IP-адресу **120.140.160.170/14** определить следующие параметры сетевой архитектуры:

1. Класс сети.
2. Маску сети.
3. Адрес сети.
4. Размер расширенного сетевого префикса.
5. Маску подсети.
6. Адрес подсети.
7. Адрес хоста.

Решение:

1. Класс «**A**» (так как **0 < 120 < 127**).
2. Маска сети: **255.0.0.0**.
3. Адрес сети: **120.0.0.0**.
4. Размер расширенного сетевого префикса: **14** разрядов.
5. Так как размер расширенного сетевого префикса составляет **14** разрядов, маска подсети, представленная в 2-ой системе счисления, состоит из **14** "**1**" и (32 - 14 = 18) **18** "**0**":

14 разрядов маски подсети		**18** разрядов сетевого адреса хоста	
1111 1111	**1111 1100**	**0000 0000**	**0000 0000**
F F	**F C**	**0 0**	**0 0**
255.	**252.**	**0.**	**0**

6. Адрес подсети определяется первыми **14** разрядами заданного IP-адреса. Остальные **18** разрядов заполняются "**0**":

14 сетевых разрядов		**18** разрядов хоста	
0111 1000	**1000 1100**	**0000 0000**	**0000 0000**
7 8	**8 C**	**0 0**	**0 0**
120.	**140.**	**0.**	**0**

7. Адрес хоста определяется первыми **14** "**0**" и **18** остальными разрядами заданного IP-адреса:

14 сетевых разрядов		**18** разрядов хоста	
0000 0000	**0000 0000**	**1010 0000**	**0000 0000**
0 0	**0 0**	**A 0**	**A A**
0.	**0.**	**160.**	**170**

Задания для выполнения

По заданию преподавателя определить параметры сетевой архитектуры:

1. Класс сети.
2. Маску сети.
3. Адрес сети.
4. Размер расширенного сетевого префикса.
5. Маску подсети.
6. Адрес подсети.
7. Адрес хоста.

Вопросы для самоконтроля

1. Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте.

– 192.168.255.0
– 167.234.56.13
– 224.0.5.3
– 172.34.267.34
– 230.0.0.7
– 160.54.255.255

2. Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте.

– 255.254.128.0
– 255.255.252.0
– 240.0.0.0
– 255.255.194.0
– 255.255.128.0
– 255.255.255.244
– 255.255.255.255

3. Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.

– 165.45.67.0, маска 255.255.255.224, N=3
– 235.162.56.0, маска 255.255.255.224, N=6
– 234.49.32.0, маска 255.255.255.192, N=3

Лабораторная работа 4
НАСТРОЙКА УДАЛЕННОГО ДОСТУПА К КОМПЬЮТЕРУ

Цель работы: научиться настраивать и устанавливать параметры удаленного доступа к сети.

Удаленный доступ к компьютеру

Термин «удаленный доступ к ПК» подразумевает удаленное подключение к компьютеру с целью управления или просмотра рабочего стола, а так же выполнения сопутствующих операций, например, обмен файлами, голосовыми и видео сообщениями и прочее.

Программы удаленного доступа к компьютеру «снимают» и преобразовывают изображение на удаленной машине и отправляют его на локальный компьютер. Нажатия клавиш на клавиатуре и движения мыши передаются на удаленную машину, которая в свою очередь интерпретирует их как сигналы, введенные непосредственно от человека, сидящего за этим компьютером.

Вся информация, подлежащая передаче в ходе сеанса подключения к удаленному компьютеру, подвергается компрессии для достижения оптимальной скорости передачи изображения как для высокоскоростных, так и для низкоскоростных соединений.

Дистанционное управление компьютером позволяет получить полный контроль над удаленной машиной, а также приложениями и файлами. Наиболее общие для многих программ удаленного управления ПК функции – файловый менеджер, голосовой или текстовый чат и, непосредственно, удаленное управление компьютером.

Технология удаленного подключения к ПК открывает широкий круг возможностей как для корпоративных, так и для частных пользователей, которым необходимо иметь оперативный доступ к рабочим и домашним компьютерам из любой точки мира. Удаленная техподдержка, системное администрирование, бизнес-конференции онлайн, дистанционное обучение – наиболее широкие сферы применения данной технологии.

Последовательность настройки удаленного доступа через модем в операционной системе «Windows»

1. Установка контроллера удаленного доступа

а) Нажмите кнопку **Пуск** на панели задач. Выберете пункт ***Настройка -> Панель Управления***.

б) Откройте объект ***Установка и удаление программ***. В появившемся окне: на вкладке ***Установка Windows*** в окне ***Компоненты*** выберите пункт ***Связь*** и нажмите кнопку ***Состав*.**

в) В появившемся окне выберите пункт (установите флажок) ***Удаленный доступ к сети*** и нажмите кнопку ***ОК*.**

г) Подождите, пока система устанавливает программное обеспечение. По завершении перезагрузите компьютер.

2. Установка модема

а) Нажмите кнопку ***Пуск*** на панели задач. Выберете пункт ***Настройка -> Панель Управления***.

б) Откройте объект ***Модемы*** (появится диалоговое окно ***Установка нового модема***).

в) Установите флажок ***Не определять тип модема (выбор из списка)***. Нажмите кнопку ***Далее*.**

г) Прочитайте и законспектируйте сообщение. Выберите соответствующие пункты в рубриках ***Изготовители:*** *(Standard Modem Types)* и ***Модели***: *Standard 28800 bps Modem*. Нажмите кнопку ***Далее*.**

д) В окне ***Укажите порт, к которому он присоединен***: укажите Последовательный порт (*COM2*). Нажмите кнопку ***Далее***.

е) Подождите, пока идет установка модема. По завершении нажмите кнопку ***Готово***.

3. Создание удаленного соединения

а) Откройте объект ***Мой компьютер***.

б) Откройте объект ***Удаленный доступ к сети***.

в) Откройте объект ***Новое соединение***. В появившемся окне: введите название соединения; выберите в выпадающем списке установленный модем. Нажмите кнопку ***Далее***.

г) Введите **Код города:** 095; **Телефон:** XXXXXXX, **Код страны:** Россия (7). Нажмите кнопку **Далее**.

д) Нажмите кнопку **Готово.**

3. Настройка удаленного соединения

а) В окне ***Удаленный доступ к сети*** выберите ***Объект доступа***. Выберите в меню ***Файл*** пункт ***Свойства***. В открывшемся окне:

– на вкладке ***Общие*** проверьте код города, код страны, телефон;

– на вкладке ***Тип сервера*** отметьте тип удаленного сервера; установите ***Допустимые сетевые протоколы: TCP/IP***.

– нажмите кнопку ***OK***.

4. Установка удаленного соединения

В окне ***Удаленный доступ к сети*** откройте объект ***доступа***. В открывшемся окне:

– введите ***Имя пользователя***: XXXXX;

– введите ***Пароль***: XXXXXX;

– нажмите кнопку ***Установить связь***;

5. Фазы установления соединения:

- набор номера;
- подключение к серверу;
- согласование параметров связи;
- проверка имени пользователя и пароля;
- вход в сеть;
- установка соединения;

6. Завершение работы

а) Нажмите кнопку ***Пуск*** на панели задач. Выберете пункт ***Настройка -> Панель Управления***.

б) В окне ***Удаленный доступ к сети*** выберите название сетевого соединения. Выберите в меню ***Файл*** пункт ***Удалить.***

в) Откройте объект ***Модемы***. Выберите *Standard 28800 bps Modem*. Нажмите кнопку ***Удалить.*** Нажмите кнопку ***Закрыть***.

г) Откройте объект ***Сеть***. Выберите Контроллер удаленного доступа. Нажмите кнопку ***Удалить*** Нажмите кнопку ***OK***.

Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

1. Настройте аутентификацию устройств

При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.:

– Задайте имя устройства.

– Задайте домен для устройства.

2. Создайте ключ шифрования с указанием его длины.

Установите ключ шифрования с длиной 1024 бит.

3. Создание имени пользователя в локальной базе учетных записей

Создайте имя пользователя и пароль для него с максимальными привилегиями. Уровень привилегий 15 дает пользователю права администратора.

4. Активация протокола SSH на линиях VTY.

а) Активируйте протокол SSH на входящих линиях VTY.

б) Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей, данная команда начинается со слова ***login***.

5. Установка соединения с маршрутизатором по протоколу SSH

а) Запустите Tera Term с PC-A.

б) Установите SSH-подключение к компьютеру.

Задания для выполнения

1) Создайте ***Новое соединение с названием «Лаб4»***

2) Произведите настройку модема

3) Проведите настройку и установку удаленного соединения

4) Приведите компьютер в исходное состояние.

5) Произведите настройку маршрутизатора для доступа по протоколу SSH. Используйте имя пользователя ***SSHadmin*** и пароль ***Admin1p@55***.

6) Сохраните текущую конфигурацию в файл загрузочной конфигурации.

7) Установите SSH-подключение к компьютеру «R1_ФАМИЛИЯ» используя имя пользователя **admin** и пароль **adminpass**.

8) Приведите настройки в исходное состояние

Вопросы для самоконтроля

1. Порядок настройки удаленного доступа в сеть.
2. Что такое: ISP, DCE, DTE, канал передачи данных, модем.
3. Модемы: назначение, типы, выполняемые функции, протоколы.
4. Протоколы канального уровня: UUCP, SLIP, PPP.
5. Настройка доступа по протоколу SSH

ЗАКЛЮЧЕНИЕ

В методических указаниях рассмотрены методики работы с диагностическими утилитами протокола TCP/IP, решения проблем со стеком TCP/IP, принципы преобразования форматов IP-адресов и расчета IP-адреса и маски подсети, а также настройки удаленного доступа к компьютеру.

На лабораторных занятиях обучающийся формирует навыки:

- организации и конфигурирования компьютерных сетей;
- создания и анализа модели компьютерных сетей;
- эффективного использования аппаратных и программных компонентов компьютерных сетей при решении различных задач;
- выполнения схем и чертежей по специальности с использованием прикладных программных средств;
- работы с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX);
- установки и настройки параметров протоколов;
- обнаружения и устранения ошибок при передаче данных.

РЕКОМЕНДАТЕЛЬНЫЙ БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузин, А. В. Компьютерные сети : учеб. пособие / А. В. Кузин, Д. А. Кузин. – 4-е изд., перераб. и доп. – М. : ФОРУМ : ИНФРА-М, 2020. – 190 с.

2. Фомин, Д.В. Компьютерные сети : учеб.-метод. пособие / Д. В. Фомин. – Благовещенск : Изд-во АмГУ, 2015. – 46 с.

Электронное издание

КОМПЬЮТЕРНЫЕ СЕТИ

Методические указания к лабораторным занятиям

Составитель
КУРОЧКИН Сергей Васильевич

Издаются в авторской редакции

Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Reader; дисковод DVD-ROM.

Тираж 25 экз.

Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых
Изд-во ВлГУ
rio.vlgu@yandex.ru

Кафедра информационных систем и программной инженерии
s-2000-k@yandex.ru