

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО

на заседании цикловой комиссии
протокол № 11 от 23.06.2017
Председатель цикловой комиссии:
Sh (Котомов)

УТВЕРЖДАЮ

Начальник УМО

А.В. Калько А.В. Калько
«23» 06 2017 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий

По МДК 03.03. Сетевое взаимодействие в малых сетях

Специальность: 09.02.02 Компьютерные сети

Разработчик:
Зав.УВЦ Капоровский В.Е.

Методическое пособие по проведению лабораторных работ по МДК 03.03. «Сетевое взаимодействие в малых сетях» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» разработаны для студентов курса специальности 09.02.02 «Компьютерные сети» в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее СПО) 09.02.02 «Компьютерные сети».

Данное пособие содержит теоретические основы, описание хода работы, алгоритмы действий в процессе выполнения, решения задач, а также при необходимости контрольные вопросы и задания по проверке освоения материала.

В пособие даны руководства по следующим темам:

- Аппаратно-программное обеспечение сетевых устройств;
- Подключение к локальной сети;
- Подключение к сети Интернет;
- Сетевая адресация и сетевые службы;
- Беспроводные технологии;
- Основы безопасности локальных сетей;
- Диагностика и устранение неполадок в локальных сетях.

Практические занятия по МДК.03.03 «Сетевое взаимодействие в малых сетях» направлена на:

- приобретение студентами профессиональных навыков и первоначального опыта в профессиональной деятельности;
- формирование основных профессиональных компетенций, соответствующих виду профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры;
- воспитание сознательной трудовой и производственной дисциплины.

Результатом освоения МДК 03.03. «Сетевое взаимодействие в малых сетях» является овладение обучающимися видом профессиональной деятельности (ВПД) Эксплуатация объектов сетевой инфраструктуры, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Эксплуатация сетевых конфигураций
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Правила охраны труда при проведении лабораторных работ.

1. Общие требования охраны труда.
 - 1.1. К работе в учебном кабинете допускаются студенты, прошедшие инструктаж по охране труда, знающие правила пожарной безопасности.
 - 1.2. При работе в кабинете должны соблюдаться правила поведения, расписание учебных занятий, установленный режим труда и отдыха.
 - 1.3. При проведении занятий возможно воздействие на студентов следующих опасных факторов:
 - нарушение осанки, искривление позвоночника, развитие близорукости при неправильном подборе мебели;
 - нарушение остроты зрения при недостаточной освещенности в кабинете;
 - поражение электрическим током при неисправном оборудовании кабинета;
 - 1.4. В процессе занятий студенты должны соблюдать правила личной гигиены, содержать в чистоте рабочее место.
2. Требования безопасности перед началом занятия.
 - 2.1. Включить полностью освещение в кабинете, убедиться в правильности работы светильников. Наименьшая освещенность в кабинете должна быть не менее 300Лк ($20\text{Вт}/\text{м}^2$) при люминесцентных лампах.
 - 2.2. Убедиться в исправности электрооборудования кабинета: коммуникационные коробки выключателей и розеток не должны иметь трещин, сколов, а также оголенных контактов.
 - 2.3. Проверить санитарное состояние кабинета, убедиться в целостности стекол в окнах и провести сквозное проветривание кабинета.
3. Требование безопасности во время занятия.
 - 3.1. Используемые в кабинете демонстрационные электрические приборы должны быть исправны и иметь заземление и зануление.
4. Требования безопасности в аварийных ситуациях.
 - 4.1. При возникновении аварийных ситуаций немедленно эвакуировать студентов и сообщить администрации учреждения.
5. Требования безопасности по окончании занятия.
 - 5.1. Выключить демонстрационные электрические приборы;
 - 5.2. Закрыть окна и выключить свет

Практическое занятие № 1

Изучение аппаратно-программного обеспечения сетевых устройств.

Цель: Изучить аппаратно – программное обеспечение сетевых устройств.

Теоретические сведения.

Сетевые устройства

Устройства, подключенные к какому-либо сегменту сети, называют сетевыми устройствами. Их принято подразделять на 2 группы:

1. **Устройства пользователя.** В эту группу входят компьютеры, принтеры, сканеры и другие устройства, которые выполняют функции, необходимые непосредственно пользователю сети;
2. **Сетевые устройства.** Эти устройства позволяют осуществлять связь с другими сетевыми устройствами или устройствами конечного пользователя. В сети они выполняют специфические функции.

Ниже более подробно описаны типы устройств и их функции.

Типы сетевых устройств

Сетевые карты

Устройства, которые связывают конечного пользователя с сетью, называются также **оконечными узлами или станциями (host)**. Примером таких устройств является обычный персональный компьютер или **рабочая станция** (мощный компьютер, выполняющий определенные функции, требующие большой вычислительной мощности. Например, обработка видео, моделирование физических процессов и т.д.). Для работы в сети каждый **хост** оснащен **платой сетевого интерфейса (Network Interface Card — NIC)**, также называемой **сетевым адаптером**. Как правило, такие устройства могут функционировать и без компьютерной сети.

Сетевой адаптер представляет собой печатную плату, которая вставляется в слот на материнской плате компьютера, или внешнее устройство. Каждый адаптер NIC имеет уникальный код, называемый MAC-адресом. Этот адрес используется для организации работы этих устройств в сети. Сетевые устройства обеспечивают транспортировку данных, которые необходимо передавать между устройствами конечного пользователя. Они удлиняют и объединяют кабельные соединения, преобразуют данные из одного формата в другой и управляют передачей данных. Примерами устройств, выполняющих перечисленные функции, являются **повторители, концентраторы, мосты, коммутаторы и маршрутизаторы**.

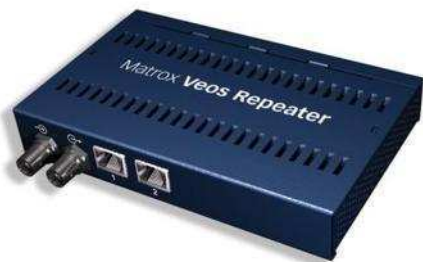


Сетевой адаптер (NIC)

Повторители

Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Для того чтобы понять работу повторителя, необходимо знать, что по мере того, как данные покидают устройство отправителя и выходят в сеть, они преобразуются в электрические или световые импульсы, которые после этого передаются по сетевой передающей среде. Такие импульсы называются **сигналами (signals)**. Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако чем больше длина кабеля, тем более слабым и менее различимым становится сигнал по мере прохождения по сетевой передающей среде. Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние. Термин повторитель (repeater) первоначально означал отдельный порт “на входе” некоторого устройства и отдельный порт на его “выходе”. В настоящее время используются также повторители с несколькими портами. В эталонной модели OSI повторители классифицируются как устройства

первого уровня, поскольку они функционируют только на битовом уровне и не просматривают другую содержащуюся в пакете информацию.



Повторитель (Repeater)

Концентраторы

Концентратор — это один из видов сетевых устройств, которые можно устанавливать на уровне доступа сети Ethernet. На концентраторах есть несколько портов для подключения узлов к сети. **Концентраторы** — это простые устройства, не оборудованные необходимыми электронными компонентами для передачи сообщений между узлами в сети. Концентратор не в состоянии определить, какому узлу предназначено конкретное сообщение. Он просто принимает электронные сигналы одного порта и воспроизводит (или ретранслирует) то же сообщение для всех остальных портов.

Для отправки и получения сообщений все порты концентратора Ethernet подключаются к одному и тому же каналу. Концентратор называется устройством с общей полосой пропускания, поскольку все узлы в нем работают на одной полосе одного канала.

Концентраторы и повторители имеют похожие характеристики, поэтому концентраторы часто называют **многопортовыми повторителями (multiport repeater)**. Разница между повторителем и концентратором состоит лишь в количестве кабелей, подсоединенных к устройству. В то время как повторитель имеет только два порта, концентратор обычно имеет от 4 до 20 и более портов.



Концентратор Cisco Fasthub 108T

Свойства концентраторов

Ниже приведены наиболее важные свойства устройств данного типа:

- концентраторы усиливают сигналы;
- концентраторы распространяют сигналы по сети;
- концентраторам не требуется фильтрация;
- концентраторам не требуется определение маршрутов и коммутации пакетов;
- концентраторы используются как точки объединения трафика в сети.

Функции концентраторов

Концентраторы считаются устройствами первого уровня, поскольку они всего лишь регенерируют сигнал и повторяют его на всех своих портах (на выходных сетевых соединениях). Сетевой адаптер узла принимает только сообщения, адресованные на правильный MAC-адрес. Узлы игнорируют сообщения, которые адресованы не им. Только узел, которому адресовано данное сообщение, обрабатывает его и отвечает отправителю.

Для отправки и получения сообщений все порты концентратора Ethernet подключаются к одному и тому же каналу. Концентратор называется устройством с общей полосой пропускания, поскольку все узлы в нем работают на одной полосе одного канала.

Через концентратор Ethernet можно одновременно отправлять только одно сообщение. Возможно, два или более узла, подключенные к одному концентратору, попытаются одновременно отправить сообщение. При этом происходит столкновение электронных сигналов, из которых состоит сообщение.

Столкнувшиеся сообщения искажаются. Узлы не смогут их прочесть. Поскольку концентратор не декодирует сообщение, он не обнаруживает, что оно искажено, и повторяет его всем портам. Область сети, в которой узел может получить искаженное при столкновении сообщение, называется доменом коллизий.

Внутри этого домена узел, получивший искаженное сообщение, обнаруживает, что произошла коллизия. Каждый отправляющий узел какое-то время ждет и затем пытается снова отправить или переправить сообщение. По мере того, как количество подключенных к концентратору узлов растет, растет и вероятность столкновения. Чем больше столкновений, тем больше будет повторов. При этом сеть перегружается, и скорость передачи сетевого трафика падает. Поэтому размер домена коллизий необходимо ограничить.

Мосты

Мост (bridge) представляет собой устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным коллизионным доменом. Иными словами, мосты предназначены для более рационального использования полосы пропускания. Целью моста является фильтрация потоков данных в LAN-сети с тем, чтобы локализовать внутрисегментную передачу данных и вместе с тем сохранить возможность связи с другими

частями (сегментами) LAN-сети для перенаправления туда потоков данных. Каждое сетевое устройство имеет связанный с NIC-картой уникальный MAC-адрес. Мост собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов. По этой причине они могут быстро пересылать данные любых протоколов сетевого уровня. На решение о пересылке не влияет тип используемого протокола сетевого уровня, вследствие этого мосты принимают решение только о том, пересылать или не пересылать фрейм, и это решение основывается лишь на MAC-адресе получателя. Ниже приведены наиболее важные свойства мостов.

Свойства мостов

- Мосты являются более «интеллектуальными» устройствами, чем концентраторы. «Более интеллектуальные» в данном случае означает, что они могут анализировать входящие фреймы и пересылать их (или отбросить) на основе адресной информации.
- Мосты собирают и передают пакеты между двумя или более сегментами LAN-сети.
- Мосты увеличивают количество доменов коллизий (и уменьшают их размер за счет сегментации локальной сети), что позволяет нескольким устройствам передавать данные одновременно, не вызывая коллизий.
- Мосты поддерживают таблицы MAC-адресов.



Сетевой мост

Функции мостов

Отличительными функциями моста являются фильтрация фреймов на втором уровне и используемый при этом способ обработки трафика. Для фильтрации или выборочной доставки данных мост создает таблицу всех MAC-адресов, расположенных в данном сетевом сегменте и в других известных ему сетях, и преобразует их в соответствующие номера портов. Этот процесс подробно описан ниже.

<p>Этап 1.</p>	<p>Если устройство пересылает фрейм данных впервые, мост ищет в нем MAC-адрес устройства отправителя и записывает его в свою таблицу адресов.</p>
<p>Этап 2.</p>	<p>Когда данные проходят по сетевой среде и поступают на порт моста, он сравнивает содержащийся в них MAC-адрес пункта назначения с MAC-адресами, находящимися в его адресных таблицах.</p>
<p>Этап 3.</p>	<p>Если мост обнаруживает, что MAC-адрес получателя принадлежит тому же сетевому сегменту, в котором находится отправитель, то он не пересылает эти данные в другие сегменты сети. Этот процесс называется <i>фильтрацией (filtering)</i>. За счет такой фильтрации мосты могут значительно уменьшить объем передаваемых между сегментами данных, поскольку при этом исключается ненужная пересылка трафика.</p>
<p>Этап 4.</p>	<p>Если мост определяет, что MAC-адрес получателя находится в сегменте, отличном от сегмента отправителя, он направляет данные только в соответствующий сегмент.</p>
<p>Этап 5.</p>	<p>Если MAC-адрес получателя мосту неизвестен, он рассылает данные во все порты, за исключением того, из которого эти данные были получены. Такой процесс называется <i>лавинной рассылкой (flooding)</i>. Лавинная рассылка фреймов также используется в коммутаторах.</p>
<p>Этап 6.</p>	<p>Мост строит свою таблицу адресов (зачастую ее называют мостовой таблицей или таблицей коммутации), изучая MAC-адреса отправителей во фреймах. Если MAC-адрес отправителя блока данных, фрейма, отсутствует в таблице моста, то он вместе с номером интерфейса заносится в адресную таблицу. В коммутаторах, если рассматривать (в самом простейшем приближении) коммутатор как многопортовый мост, когда устройство обнаруживает, что MAC-адрес отправителя, который ему известен и вместе с номером порта занесен в адресную таблицу устройства, появляется на другом порту коммутатора, то он обновляет свою таблицу коммутации. Коммутатор предполагает, что сетевое устройство было физически перемещено из одного сегмента сети в другой.</p>

Коммутаторы

Коммутаторы используют те же концепции и этапы работы, которые характерны для мостов. В самом простом случае коммутатор можно назвать многопортовым мостом, но в некоторых случаях такое упрощение неправомерно.

Коммутатор Ethernet используется на уровне доступа. Как и концентратор, коммутатор соединяет несколько узлов с сетью. В отличие от концентратора, коммутатор в состоянии передать сообщение **конкретному** узлу. Когда узел отправляет сообщение другому узлу через коммутатор, тот принимает и декодирует кадры и считывает физический (MAC) адрес сообщения.

В таблице коммутатора, которая называется таблицей MAC-адресов, находится список активных портов и MAC-адресов подключенных к ним узлов. Когда узлы обмениваются сообщениями, коммутатор проверяет, есть ли в таблице MAC-адрес. Если да, коммутатор устанавливает между портом источника и назначения временное соединение, которое называется канал. Этот новый канал представляет собой назначенный канал, по которому два узла обмениваются данными. Другие узлы, подключенные к коммутатору, работают на разных полосах пропускания канала и не принимают сообщения, адресованные не им. Для каждого нового соединения между узлами создается новый канал. Такие отдельные каналы позволяют устанавливать несколько соединений одновременно без возникновения коллизий.

Поскольку коммутация осуществляется на аппаратном уровне, это происходит значительно быстрее, чем аналогичная функция, выполняемая мостом с помощью программного обеспечения (Следует обратить внимание, что мост считается устройством с программной, коммутатор □ □ □ □ с аппаратной коммутацией.). Каждый порт коммутатора можно рассматривать как отдельный микромост. При этом каждый порт коммутатора предоставляет каждой рабочей станции всю полосу пропускания передающей среды. Такой процесс называется микросегментацией.

Микросегментация (microsegmentation) позволяет создавать частные, или выделенные сегменты, в которых имеется только одна рабочая станция. Каждая такая станция получает мгновенный доступ ко всей полосе пропускания, и ей не приходится конкурировать с другими станциями за право доступа к передающей среде. В дуплексных коммутаторах не происходит коллизий, поскольку к каждому порту коммутатора подсоединено только одно устройство.

Однако, как и мост, коммутатор пересылает ширококвещательные пакеты всем сегментам сети. Поэтому в сети, использующей коммутаторы, все сегменты должны рассматриваться как один ширококвещательный домен.

Некоторые коммутаторы, главным образом самые современные устройства и коммутаторы уровня предприятия, способны выполнять операции на нескольких уровнях. Например, устройства серий Cisco 6500 и 8500 выполняют некоторые функции третьего уровня.



Коммутаторы Cisco серии Catalyst 6500

Иногда к порту коммутатора подключают другое сетевое устройство, например, концентратор. Это увеличивает количество узлов, которые можно подключить к сети. Если к порту коммутатора подключен концентратор, MAC-адреса всех узлов, подключенных к концентратору, связываются с одним портом. Бывает, что один узел подключенного концентратора отправляет сообщения другому узлу того же устройства. В этом случае коммутатор принимает кадр и проверяет местонахождение

узла назначения по таблице. Если узлы источника и назначения подключены к одному порту, коммутатор отклоняет сообщение.

Если концентратор подключен к порту коммутатора, возможны коллизии. Концентратор передает поврежденные при столкновении сообщения всем портам. Коммутатор принимает поврежденное сообщение, но, в отличие от концентратора, не переправляет его. В итоге у каждого порта коммутатора создается отдельный домен коллизий. Это хорошо. Чем меньше узлов в домене коллизий, тем менее вероятно возникновение коллизии.

Маршрутизаторы

Маршрутизаторы (router) представляют собой устройства объединенных сетей, которые пересылают пакеты между сетями на основе адресов третьего уровня. Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных. Функционируя на третьем уровне, маршрутизатор может принимать решения на основе сетевых адресов вместо использования индивидуальных MAC-адресов второго уровня. Маршрутизаторы также способны соединять между собой сети с различными технологиями второго уровня, такими, как Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI — распределенный интерфейс передачи данных по волоконно-оптическим каналам). Обычно маршрутизаторы также соединяют между собой сети, использующие технологию асинхронной передачи данных АТМ (Asynchronous Transfer Mode — АТМ) и последовательные соединения. Вследствие своей способности пересылать пакеты на основе информации третьего уровня, маршрутизаторы стали основной магистралью глобальной сети Internet и используют протокол IP.



Маршрутизатор Cisco 1841

Функции маршрутизаторов

Задачей маршрутизатора является инспектирование входящих пакетов (а именно, данных третьего уровня), выбор для них наилучшего пути по сети и их коммутация на соответствующий выходной порт. В крупных сетях маршрутизаторы являются главными устройствами, регулирующими перемещение по сети потоков данных. В принципе маршрутизаторы позволяют обмениваться информацией любым типам компьютеров.

Как маршрутизатор определяет нужно ли пересылать данные в другую сеть? В пакете содержатся IP-адреса источника и назначения и данные пересылаемого сообщения. Маршрутизатор считывает сетевую часть IP-адреса назначения и с ее помощью определяет, по какой из подключенных сетей лучше всего переслать сообщение адресату.

Если сетевая часть IP-адресов источника и назначения не совпадает, для пересылки сообщения необходимо использовать маршрутизатор. Если узел, находящийся в сети 1.1.1.0, должен отправить сообщение узлу в сети 5.5.5.0, оно переправляется маршрутизатору. Он получает сообщение, распаковывает и считывает IP-адрес назначения. Затем он определяет, куда переправить сообщение. Затем маршрутизатор снова инкапсулирует пакет в кадр и переправляет его по назначению.

Брандмауэры

Термин **брандмауэр (firewall)** используется либо по отношению к программному обеспечению, работающему на маршрутизаторе или сервере, либо к отдельному аппаратному компоненту сети.

Брандмауэр защищает ресурсы частной сети от несанкционированного доступа пользователей из других сетей. Работая в тесной связи с программным обеспечением маршрутизатора, брандмауэр

исследует каждый сетевой пакет, чтобы определить, следует ли направлять его получателю. Использование брандмауэра можно сравнить с работой сотрудника, который отвечает за то, чтобы только разрешенные данные поступали в сеть и выходили из нее.



Аппаратный брандмауэр Cisco PIX серии 535

Голосовые устройства, DSL-устройства, кабельные модемы и оптические устройства

Возникший в последнее время спрос на интеграцию голосовых и обычных данных и быструю передачу данных от конечных пользователей в сетевую магистраль привел к появлению следующих новых сетевых устройств:

- голосовых шлюзов, используемых для обработки интегрированного голосового трафика и обычных данных;
- мультиплексоров DSLAM, используемых в главных офисах провайдеров служб для концентрации соединений DSL-модемов от сотен индивидуальных домашних пользователей;
- терминальных систем кабельных модемов (Cable Modem Termination System — CMTS), используемых на стороне оператора кабельной связи или в головном офисе для концентрации соединений от многих подписчиков кабельных служб;
- оптических платформ для передачи и получения данных по оптоволоконному кабелю, обеспечивающих высокоскоростные соединения.

Беспроводные сетевые адаптеры

Каждому пользователю беспроводной сети требуется беспроводной сетевой адаптер NIC, называемый также адаптером клиента. Эти адаптеры доступны в виде плат PCMCIA или карт стандарта шины PCI и обеспечивают беспроводные соединения как для компактных переносных компьютеров, так и для настольных рабочих станций. Переносные или компактные компьютеры PC с беспроводными адаптерами NIC могут свободно перемещаться в территориальной сети, поддерживая при этом непрерывную связь с сетью. Беспроводные адаптеры для шин PCI (Peripheral Component Interconnect — 32-разрядная системная шина для подключения периферийных устройств) и ISA (Industry-Standard Architecture — структура, соответствующая промышленному стандарту) для настольных рабочих станций позволяют добавлять к локальной сети LAN конечные станции легко, быстро и без особых материальных затрат. При этом не требуется прокладки дополнительных кабелей. Все адаптеры имеют антенну: карты PCMCIA обычно выпускаются со встроенной антенной, а PCI-карты комплектуются внешней антенной. Эти антенны обеспечивают зону приема, необходимую для передачи и приема данных.



Беспроводной сетевой адаптер

Точки беспроводного доступа

Точка доступа (Access Point — AP), называемая также базовой станцией, представляет собой беспроводной передатчик локальной сети LAN, который выполняет функции концентратора, т.е. центральной точки отдельной беспроводной сети, или функции моста — точки соединения проводной и беспроводной сетей. Использование нескольких точек AP позволяет обеспечить выполнение функций роуминга (roaming), что предоставляет пользователям беспроводного доступа свободный доступ в пределах некоторой области, поддерживая при этом непрерывную связь с сетью.



Точка беспроводного доступа Cisco AP 541N

Беспроводные мосты

Беспроводной мост обеспечивает высокоскоростные беспроводные соединения большой дальности в пределах видимости (до 25 миль) между сетями Ethernet. В беспроводных сетях Cisco любая точка доступа может быть использована в качестве повторителя (точки расширения).

Задание: Изучить следующее представленное оборудование: D-Link Des-1210-28, 3Com Switch 5500-SI, Cisco Catalyst 3550 series, Cisco 2600 series, Cisco Catalyst 1900.

Ответить на вопросы:

1. К какому типу сетевых устройств относится данное оборудование.
 2. Рассмотреть все разъемы на данных устройствах. Для чего они предназначены?
 3. Каким образом подключается данное оборудование
 4. Общая информация об устройстве
- Результаты отобразить в виде отчета.

Практическое занятие № 2

Изучение виртуальной сетевой среды для проектирования локальных сетей

Цель: Получить навыки по моделированию локальных компьютерных сетей с использованием среды CISCO Packet Tracer.

Теоретическое введение

1. Общие сведения о среде Cisco Packet Tracer

В процессе проектирования компьютерных важным этапом является исследование технических решений на предмет выполнения ими заданных функций. Такое исследование может быть проведено двумя способами: натурным экспериментом и компьютерным имитационным моделированием. В первом случае проектировщики, используя реальное оборудование, собирают требуемую компьютерную сеть и проводят необходимые эксперименты. Очевидно, что стоимость таких экспериментов достаточно высока и определяется в большей степени стоимостью используемого оборудования. С целью сокращения стоимости экспериментов используется компьютерное имитационное моделирование, в котором вместо реального оборудования используется их программные аналоги.

На рынке программного обеспечения существует множество различных сред имитационного моделирования компьютерных сетей. Наибольшую популярность получили две среды имитационного моделирования компьютерных сетей: GNS3¹ и CISCO Packet Tracer². Первая среда является свободно распространяемой и реализует имитационное моделирование путем виртуализации реального оборудования. Вторая среда распространяется свободно, но в рамках сетевых академий компании Cisco systems, Inc, и моделирует только оборудование этого производителя. В рамках лабораторных работ, в основном, будет использоваться среда CISCO Packet Tracer.

2. Графический интерфейс среды Cisco Packet Tracer

Запустив программу, пользователь видит основное окно (рисунок 1), содержащее:

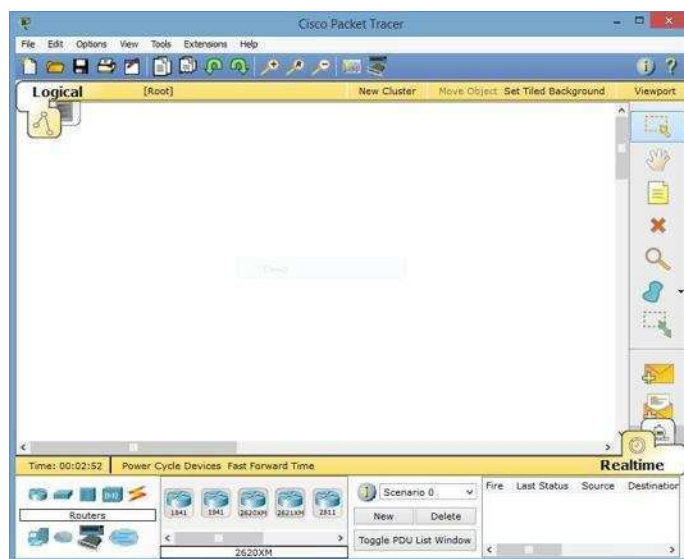


Рисунок 1 – Основное окно системы Cisco Packet Tracer

- Панели инструментов (главную, вертикальную и нижнюю);
- Переключатели режимов моделирования (реального времени и пошаговый) и видов схем (логическая и физическая).



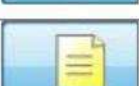





Основное меню программы содержит пункты: Файл (File), Редактирование (Edit), Настройки (Options), Вид (View), Утилиты (Tools), Дополнения (Extensions), Помощь (Help). Пункт меню «Файл» используется для выполнения операций с текущим файлом (открыть, закрыть, сохранить, распечатать и т.п.), а также позволяет завершить работу среды. В пункте «Редактирование» содержатся стандартные операции с буфером обмена (скопировать выделенный объект в буфер, вырезать, вставить), а также управления действиями в среде (отменить и повторить последнее действие). Пункт «Настройки» позволяет сконфигурировать среду моделирования и пользовательское окружение. Пункт меню «Вид» настраивает масштаб отображения объектов в рабочей области и режим отображения панелей инструментов. В пункте «Утилиты» содержатся ссылки на вывод панели графических объектов и создания собственного устройства. Управлять дополнениями возможно в меню «Дополнения». К таким дополнениям, например, относится взаимодействие между несколькими средами моделирования (об этом см. ниже).

Панели инструментов по умолчанию отображаются три: главная, вертикальная и нижняя. Доступна также панель графических примитивов.

Главная панель инструментов дублирует некоторые пункты основного меню, обеспечивая быстрый и удобный доступ к созданию нового файла, сохранения и печати текущей схемы, отображения окна дополнения «Самопроверка заданий (Activity Window)», действий с буфером обмена, изменения масштаба отображения схемы, доступа к панели графических примитивов и создания нового объекта моделирования.

Вертикальная панель инструментов содержит действия, выполняемый с объектами моделируемой схемы сети (см. Таблицу 1).

Таблица 1 – Кнопки вертикальной панели инструментов

	Инструмент Select (быстрый доступ – Esc). Позволяет выделить один или несколько объектов моделируемой компьютерной сети (логической или физической топологии)
	Инструмент Move Layout (быстрый доступ - M). Используется для прокрутки схемы модулируемой сети в основном окне рабочего пространства. Для выполнения этого действия могут также использоваться полосы прокрутки.
	Инструмент Place Note (быстрый доступ - N). Позволяет добавить в текущую моделируемую схему текстовую надпись.
	Инструмент Delete (быстрый доступ – Del). Переключает в режим удаления выделяемых объектов схемы компьютерной сети.
	Инструмент Inspect (быстрый доступ – I). Позволяет просматривать таблицы состояния (таблица маршрутизации и т.п.) объектов моделируемой компьютерной сети.
	Инструмент Resize Shape (быстрой доступ – Alt+R). Используется для изменения размеров графических объектов, размещаемых на схеме с использованием панели «Графические объекты».
	Инструмент Add Simple PDU (быстрый доступ – P). Позволяет создать эмуляцию простой передачи пакета данных (ICMP, ping) от одного устройства сети к другому.
	Инструмент Add Complex PDU (быстрый доступ – P). Создает эмуляцию передачи пакета данных от одного устройства к другому. Позволяет задать параметры пакета (тип протокола, исходящий порт и т.п.).

Нижняя панель инструментов позволяет создавать объекты исследуемой схемы компьютерной сети а также задавать задачи по эмуляции передачи данных в ней

В области задач по моделированию передачи данных по сети располагается перечень действий, созданных кнопками Add Simple PDU и Add Complex PDU. Таких перечней (сценариев) пользователь может создать несколько. Подробнее об использовании сетевых объектов и сценариев будет сказано ниже.

Между верхней панелью инструментов и рабочим пространством находится строка *переключения режима отображения моделируемой сети*: логическая или физическая топология (см. рисунок 3). В режиме «логическая сеть» располагаются сетевые объекты и указываются связи между ними. В режиме «физическая сеть» указывается расположение сетевых объектов и каналов связей в помещениях (как они расположены, в каких стойках и т.п.). В этой же строке располагаются кнопки управления отображением: «<Root>» - уровень детализации, «New Cluster» - создать объединенное устройство, «Set Tiled Background» - установить фон рабочей области, «NAVIGATION» - навигация между уровнями отображения физической сети (Район, Город, этаж

После рабочего пространства располагается строка *переключения режимов моделирования*: реального времени или пошаговое моделирование (см. рисунок 3). В режиме пошагового моделирования пользователю предоставляется возможность посмотреть, как передается информация между сетевыми устройствами в заданных им ситуациях (подробнее см. ниже). В реальном масштабе времени указывается лишь состояние сетевых устройств, результаты передачи отображаются «по факту».

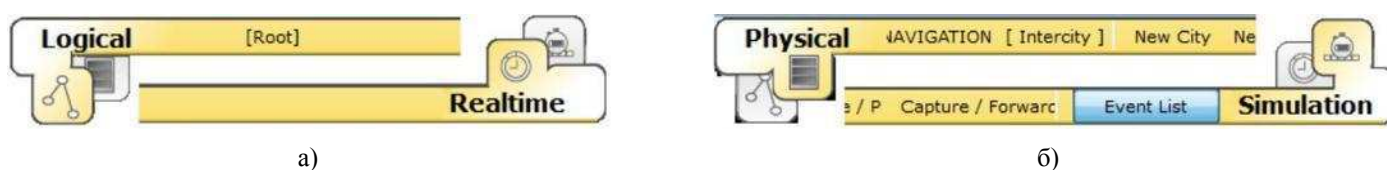


Рисунок 3 – Переключатели режимов рабочей области и модельного времени (а – логическая сеть и режим реального времени,
б – физическая сеть и режим пошагового выполнения)

3. Работа с объектами компьютерной сети

Для размещения сетевого объекта на схеме необходимо выбрать в нижней панели инструментов его класс (маршрутизаторы (routers), коммутаторы (switches), концентраторы (hubs), беспроводные устройства (wireless devices), соединительные кабели (connections), терминальные устройства (End devices), «интернет» (WAN emulation), пользовательские объекты и «многопользовательское соединение»), а затем модель (например, маршрутизатор 1841 или Laptop-PT). Выбрав необходимое оборудование его можно «перетащить» в рабочую область или щелчком мышки указать место в рабочей области, куда следует его поместить³.

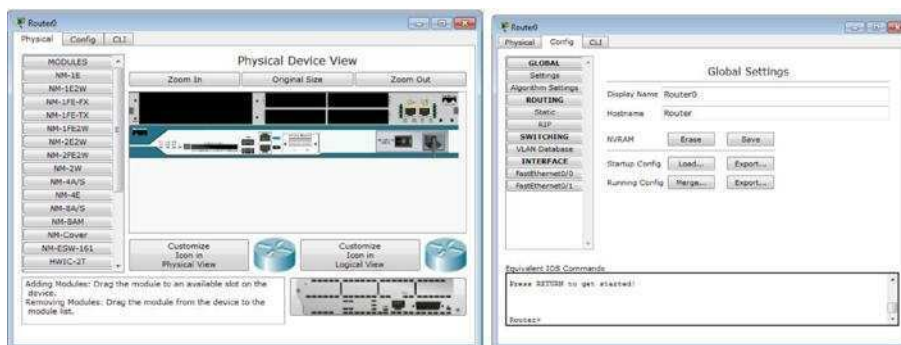
Для соединения сетевых устройств необходимо выбрать класс «Соединительные кабели», далее выбрать необходимый тип кабеля (или выбрать «автоматическое определение»), указать начальное устройство, выбрать один из его сетевых портов (см. рисунок 4), затем указать окончное устройство и один из его портов. В случае применения объекта «Автоматическое определение типа сетевого кабеля», порт и тип кабеля будут выбираться автоматически (номер порта будет выбираться в порядке возрастания).



Рисунок 4 – Меню выбора сетевого интерфейса коммутатора

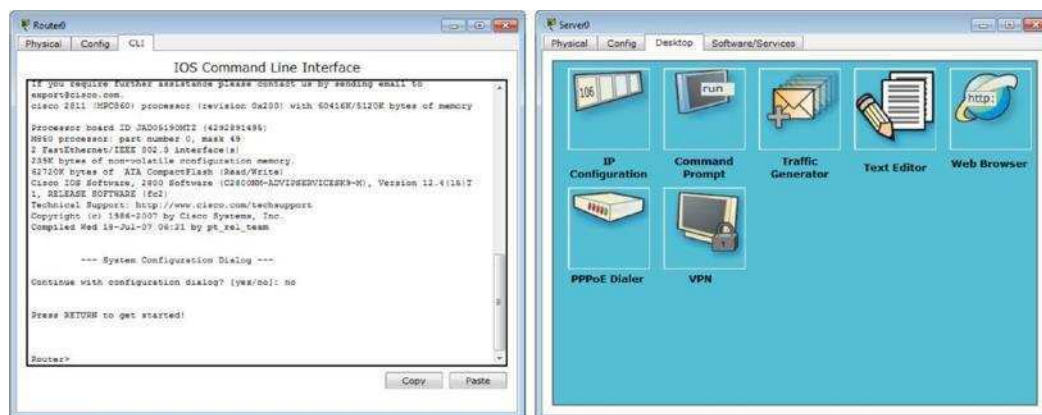
Конфигурирование сетевого устройства производится по двойному щелчку на нем (см. рисунок 5а-в). В открывшемся окне пользователь может включить/выключить устройство (соответствующим тумблером на его изображении в области «Physical Device View»), изменить аппаратную конфигурацию добавив или удалив модули⁵, используя область MODULES, изменить картинку для отображения этого устройства в режиме логической сети и в режиме физической сети. Выбрав вкладку «Config» пользователь может задать некоторые конфигурационные параметры (например, настроить сетевой интерфейс, определить имя устройства и т.п.). На вкладке «CLI» предоставляется доступ к командному интерфейсу устройства (если он предусмотрен).

Для оконечных устройств реализованы дополнительные вкладки (см., например, рисунок 5г). На вкладке «Desktop» расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). «Software/Services» - конфигурирование программного обеспечения, которое должно быть установлено на реально действующем оконечном устройстве.



а)

б)



в)

г)

Рисунок 5 – Окно конфигурирования сетевого устройства

Наведя курсор мышки на объект и подождав несколько секунд пользователь получит краткую информацию о состоянии объекта. Более подробную информацию пользователь может получить воспользовавшись инструментом «Inspect». Следует отметить, что всплывающая подсказка при наведении мыши соответствует пункту меню «Port Status Summary Table» инструмента «Inspect».

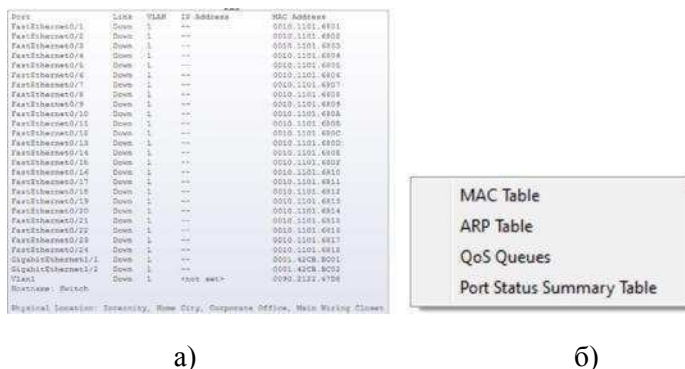


Рисунок 6 – Всплывающая подсказка (а) и меню инструмента Inspect (б)

4. Многопользовательская работа

Среда CISCO Packet Tracer позволяет организовать обмен информацией между несколькими моделируемыми сетями. При этом сети могут моделироваться как на одном, так и на разных компьютерах. В последнем случае для взаимодействия моделируемых сетей используется физическая сеть, соединяющая компьютеры.

Настройка среды удалённого взаимодействия (многопользовательского режима) производится в меню «Extensions»->«Multiuser». Настроить необходимо сетевой порт, который будет использоваться на компьютере для взаимодействия с другими средами имитационного моделирования, а также поведение системы моделирования при создании новых исходящих и входящих соединений⁶.



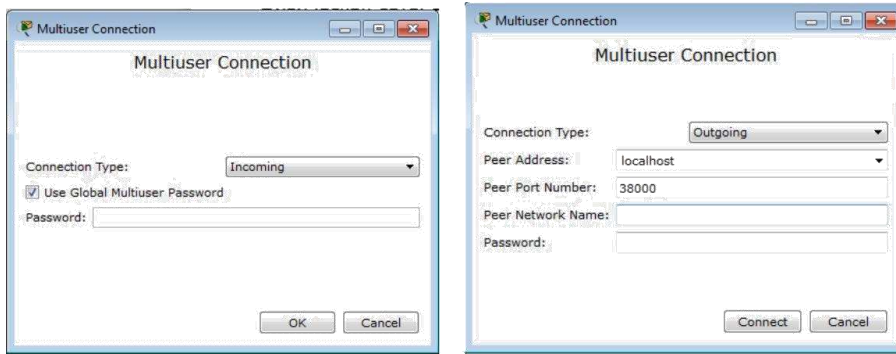
Рисунок 7 – Окно настройки удалённого взаимодействия

Для обозначения взаимодействия с другими средами моделирования используется объект «Remote network» из класса «Multiuser Connections». В свойствах этого объекта указывается тип создаваемого подключения (входящий или исходящий, в зависимости от того, какая система имитационного моделирования инициирует подключение), а также параметры второй среды имитационного моделирования.

Взаимодействие двух систем моделирования всегда начинается с установления связи между ними. И лишь после успешного установления связи, начинается процесс имитационного моделирования, в котором данные передаются от одной части сети к другой.

Пример настройки мультипользовательской среды находится в файле multiuser-config.swf

Пример создания двух сегментов сети, взаимодействующих между собой через удалённое соединение, показан в файле multiuser-modeling.swf



а) б) Рисунок 8 – Окна конфигурирования удалённого подключения

5. Пошаговая отладка передачи информации в исследуемой сети

Отладка исследуемой сети может производиться двумя способами: имитируя деятельность администратора с реальным оборудованием и с применением средств моделирования. В первом случае пользователь среды может выполнять необходимые действия над сетевыми объектами и принимать решения о функциональности собранной им сети. Во втором случае используются встроенные средства среды имитационного моделирования, которые позволяют пошагово наглядно продемонстрировать этапы передачи информации по сети.

Анализируемые задания по передаче данных по сети объединяются в сценарий. В среде допускается создавать несколько сценариев и переключаться между ними для анализа работы сети.

Для создания задания по передаче данных по протоколу ICMP (ping) используется кнопка «Add Simple PDU». Пользователь задает начальный сетевой узел (который будет генерировать данные) и конечный сетевой узел. В результате автоматически создается одно задание в текущем сценарии.

Для формирования передач данных по сети с указанием параметров передаваемой информации (протокол, порт и т.п.) используется кнопка «Add Complex PDU». Нажав на соответствующую кнопку в вертикальной панели пользователь должен указать протокол передачи, источник передаваемой информации и задать параметры: сетевой порт через который данные будут передаваться, адрес источника и получателя, порт получателя и отправителя, время жизни и обслуживания, номер пакета в последовательности, размер пакета, а также определить будет ли эта передача носить разовый характер или повторяться в течение некоторого периода времени.



Рисунок 9 – Окно настроек параметров передачи информации по сети

Результаты выполнения заданий по передаче данных отображаются в области сценариев. В режиме реального времени результаты выполнения заданий выводятся сразу же по окончании имитации.

В случае, если пользователь попытается при создании простого задания указать устройство (источник или приемник), не имеющего настроенного сетевого интерфейса, то сразу будет выдано сообщение об ошибке.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num
	Failed	PC0	10.10.10.2	TCP		10.000	N	0
	Successful	PC0	PC1	ICMP		0.000	N	1

Рисунок 10 – Пример результатов выполнения сценария передачи данных (в реальном времени)

Переключившись в режим пошагового выполнения пользователь получает возможность наглядно посмотреть каким образом передаются данные по сети (согласно созданным заданиям). Переход к следующему шагу производится нажатием на кнопку «Capture / Forward». Перейти к предыдущему шагу можно нажав на клавишу «Back». Нажав на кнопку «Auto Capture / Play» запускается автоматический переход к следующему шагу (время перехода указывается в области настроек пошагового выполнения, см. рисунок 10). Кнопка «Power Cycle Device» - сбрасывает исследуемую сеть в исходное состояние.

В панели настроек можно указать дополнительные фильтры на вывод информации о передаче данных по сети (указать интересные протоколы).

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.000	--	PC0	ARP	
	0.001	PC0	Switch0	ARP	
	0.003	Switch0	PC1	ARP	
	0.005	PC1	Switch0	ARP	
	0.007	Switch0	PC0	ARP	
	0.007	--	PC0	ICMP	
	0.009	PC0	Switch0	ICMP	
	0.011	Switch0	PC1	ICMP	

Reset Simulation Constant Delay Captured to: 0.011 s

Play Controls: Back, Auto Capture / Play, Capture / Forward

Event List Filters - Visible Events:
 ACL Filter, ARP, BGP, CDP, DHCP, DNS, DTP, EIGRP, FTP, H.323, HSRP, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, LACP, NTP, OSPF, PAgP, POP3, RADIUS, RIP, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP

Edit Filters Show All

Рисунок 11 – Панель настроек пошагового моделирования

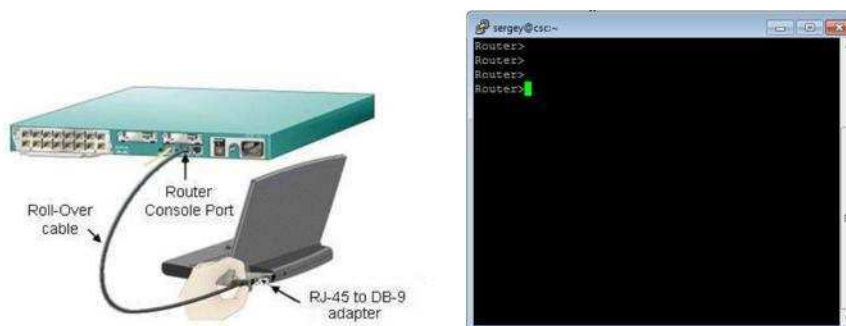
6. Командная строка управления устройствами (CLI)

Большинство сетевых устройств компании CISCO допускают конфигурирование. Для этого администратор сети должен подключиться к устройству используя: прямое кабельное (консольное) подключение, удалённое терминальное подключение или Web-интерфейс. Задавая параметры устройства, администратор сети определяет его поведение и настраивает порядок его работы.

Подключившись к устройству напрямую (см. рисунок 12а) или через удалённый терминал (см. рисунок 12б) пользователю предлагается командная строка (Command Line Interface – CLI), в которой он может задавать необходимые действия и, тем самым, определять параметры конфигурации оборудования.

В среде моделирования интерфейс командной строки для устройств доступен в окне настроек параметров сетевого устройства на вкладке «CLI». Это окно имитирует прямое кабельное

(консольное) подключение к сетевому устройству. Создав новое устройство в этом окне можно наблюдать процесс его загрузки (сервисные сообщения).



а) б) Рисунок 12 – Пример подключения к сетевому устройству⁸.

Для управления сетевыми устройствами чаще всего используется интерфейс командной строки. Поэтому в рамках изучения дисциплины «Сети ЭВМ и телекоммуникации» в лабораторном практикуме внимание будет уделяться только этому способу управления. Принципы настройки оборудования с использованием Web-интерфейса аналогичны и отличаются лишь внешним видом.

Следует отметить, что при подключении к устройству напрямую для начала сессии администратору

необходимо нажать хотя бы один раз клавишу <ENTER>. При других способах подключения сессия начинается автоматически.

6.1 Общие сведения о командной строке

Командная строка представляет собой место, куда пользователь вводит символы, формирующие управляющее воздействие. Это место обозначается: приглашением и следующим за ним курсором (который может мигать). Приглашение командной строки обычно содержит имя сетевого узла и один (или несколько) специальных символов, отвечающих за подсказку администратору, в каком режиме сейчас находится командная строка или в какой части конфигурационных параметров сейчас будут производиться действия. Ввод команд завершается нажатием клавиши <ENTER>.

Команда начинает интерпретироваться (исполняться) после нажатия клавиши <ENTER>. Если команда написана правильно, то будет выполнено соответствующее действие. Иначе появится сообщение об ошибке, указывающее на некорректное место в командной строке.

Пользователь может набрать несколько букв в командной строке и нажать клавишу <TAB>. В этом случае команда или её параметр будет продолжен (если набранная последовательность однозначно определяет их) или не произойдет никаких действий. Проверить почему команда или параметр не были продолжены можно с помощью контекстной помощи. Набрав ?, администратору будут показаны возможные альтернативы (см. ниже).

Для отмены действия, выполненного какой-либо командой, необходимо выполнить её ещё раз указав перед ней команду no (см. ниже, рисунок 14).

В случае, если в результате выполнения команды выводится информация, не помещающаяся в одном окне, то в нижней строке выводится фраза More-. Построчная прокрутка текста осуществляется клавишей <Enter>. Постраничная прокрутка – клавише <Пробел>.

6.2 Режимы работы с устройством при использовании CLI

Работа с командной строкой осуществляется в нескольких режимах (см. таблицу 1). Единными для всех устройств режимами являются: пользовательский, привилегированный и глобальной конфигурации. Остальные режимы зависят от типа устройства и его внутренней организации.

Таблица 1 – Режимы командного интерфейса

Режим	Переход в режим	Вид командной строки	Выход из режима
Пользовательский (User EXEC)	Подключение	Router>	logout
Привилегированный (Privileged EXEC)	enable.	Router#	disable
Глобальная конфигурация	configure terminal	Router(config)#	exit, end или Ctrl-Z
Настройка интерфейсов	Interface	Router(config-if)	exit
ROM monitor	В привилегированном режиме необходимо выполнить команду reload, а затем при перезагрузке устройства нажать клавишу Break.		continue

Подключившись к устройству, администратор получает командную строку, находящуюся в пользовательском режиме. В этом режиме доступны команды, позволяющие посмотреть некоторую (открытую) часть текущей конфигурации сетевого устройства, запустить процесс проверки работоспособности сети (команды ping и traceroute), открыть терминальную сессию для подключения к другому сетевому устройству и т.п.

В привилегированном режиме администратору доступно больше информации о всех конфигурации сетевого устройства, а также предоставляется доступ к команде перехода в режим конфигурирования (изменения конфигурационной информации).

6.3 Встроенная в CLI контекстная система документации

Внутри командной строки имеется встроенная контекстная документация (подсказка или помощь), выводимая командой help или ? (см., например, рисунок 13). Если знает начальные символы команды, но не помнит её продолжение, или не уверен какие параметры следует указать команде, то он указывает в нужном месте командной строки знак ? и ему выводится информация о соответствующих командах или параметрах.

Router>? <Enter>

Exec commands:

<1-99> Session number to resume
connect Open a terminal connection

disable Turn off privileged commands

6.4 Настройка имени сетевого узла и приветственного сообщения

В качестве примеров настройки устройства приведем команды изменения имени устройства и определения сообщения, выдаваемого администратору при подключении (вход в пользовательский режим).

Для этого необходимо подключиться к устройству, перейти в привилегированный режим, затем в режим глобальной конфигурации. Команда для изменения имени – *hostname*¹⁰, для определения приветственного сообщения – *banner* (см. рисунок 14).

¹⁰ Пример изменения имени сетевого устройства с помощью команды *hostname* приведен в файле *change-hostname.swf*.

Все сетевые устройства имеют одно или несколько подключений к телекоммуникационной сети – *сетевых интерфейсов*. Каждый сетевой интерфейс (или кратко – интерфейс) имеет свой тип, определяющий способ подключения к нему (например, Ethernet, FastEthernet, Serial и т.п.) и уникальный номер. Номер интерфейса, обычно, имеет вид: номер контроллера/номер интерфейса внутри контроллера. Например, запись Ethernet 0/1 означает интерфейс с типом подключения Ethernet, расположенные на контроллере с номером 0 и имеющий на нем порядковый номер 1.

```
Router>enable
Router#configure
terminal
Router(config)#hostname
MainRouter
MainRouter(config)#banner motd
/
Enter TEXT message.        End with the character '/'.
#####
# Hello world! #
#####
/
MainRouter(config)#no
hostname Router (config)#
```

Для конфигурирования сетевого интерфейса необходимо в режиме глобальной конфигурации ввести команду *interface* с указанием его типа и номера (см. рисунок 15). Вернуться в режим глобальной конфигурации можно командой *exit*.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#description Connect to main office
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
```

Каждый интерфейс в зависимости от своего типа имеет ряд настроек. Для всех интерфейсов присутствует две настройки: описание и состояние (включен или нет). Первая настройка задается командой *description*, вторая – *shutdown*. На рисунке 15 приведен пример задания описания и включения интерфейса *fastEthernet 0/1*.

Если администратору необходимо произвести одинаковую настройку для нескольких однотипных интерфейсов, то он может сделать это «в один прием», указав в команде *interface* диапазон конфигурируемых интерфейсов (параметр *range*). Диапазон задается следующим образом. Указывается тип интерфейсов, а в номере указывается

диапазон. Например, запись `range fastEthernet 0/1-4` означает, что будут задаваться параметры для интерфейсов 0/1, 0/2, 0/3 и 0/4 с типом `fastEthernet` (см. Рисунок 16).

```
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#description Connect to main office
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
```

Посмотреть текущие настройки сетевого интерфейса можно в привилегированном режиме с помощью команды `show interface` (см. рисунок 17). Чтобы посмотреть настройки сразу всех интерфейсов используется команда `show interfaces`.

6.6 Настройка режимов подключения к устройству для его администрирования

Подключившись к устройству администратор по умолчанию получает полный доступ не вводя никаких авторотационных данных. Очевидно, что такой режим в действующих сетях не всегда приемлем. Задать параметры авторизации можно в режиме глобальной конфигурации с помощью команды `line`. В качестве параметров команды указывается способ подключения (консоль или удалённый терминал) и номер линии для подключения. Пример настройки пароля для доступа к устройству приведен на рисунке 17.

```
Switch(config)#line console 0
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 3
Switch(config-line)#password qwerty
Switch(config-line)#login
Switch(config-line)#transport input telnet
Switch(config-line)#exit
Switch(config)#
```

6.7 Сохранение и восстановление конфигурации оборудования

Конфигурацию оборудования можно стереть, сохранить в отдельный файл и затем восстановить её из него. Сделать это можно с помощью окна настроек оборудования (вкладка `Config`). Следует отметить, что конфигурация оборудования изменяется в режиме реального времени. Перезагрузка устройства приведет к тому, что изменения не будут сохранены. Чтобы изменения сохранились и остались неизменными при перезагрузке устройства, то их надо сохранить в энергонезависимой памяти. Для этого в привилегированном режиме следует выполнить команду `copy running-config startup-config` или выбрать соответствующие кнопки в окне свойств сетевого объекта.

Посмотреть содержимое текущей конфигурации или конфигурации, сохранённой на диске, можно в привилегированном режиме с помощью команды `show` (см. рисунок 18).

```
Switch#show running-conf
Building configuration...
Current configuration : 1235 bytes
!
```

```
version 12.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
...
Switch#copy running-config startup-config
Switch#
```

Задание

1. Запустите среду моделирования Cisco packet tracer. Ознакомьтесь с её интерфейсом.
2. Придумайте сеть, которая будет состоять из коммутатора и двух ПК.
3. Сконфигурируйте в среде моделирования вашу сеть.
4. Используя командную строку задайте сетевым узлам:
 - a. Уникальные сетевые имена;
 - b. Приветственные приглашения, в которых будет указываться краткая информация о сетевом устройстве;
 - c. Пароли для прямого подключения к устройствам и режим их проверки;
 - d. Задайте описания для соответствующих сетевых интерфейсов.
5. Сохраните настройки сетевых устройств в их энергонезависимой памяти.
6. Проверьте работоспособности сети командой ping.

Практическое занятие № 3

Построение одноранговой сети

Цели:

1. с помощью Мастера настройки сети научиться конфигурировать свой компьютер с ОС Windows для работы в одноранговой сети;
2. выборочно предоставлять папки на своем компьютере в совместный доступ;
3. подключаться к общей папке, настроенной на другом компьютере, и работать с находящимися там файлами.

Задание 1.

Настройка компьютера с ОС Windows для работы в одноранговой сети.

1. Войдите в систему как локальный пользователь, с учетной записью, указанной преподавателем.

Примечание. Этот пользователь входит в локальную группу «Администраторы» вашего компьютера, поэтому при выполнении этого и последующих заданий вы сможете менять настройки своего компьютера.

2. В меню **Пуск** выберите пункт **Панель управления**.
3. В открывшемся окне **Панель управления** щелкните мышью на ссылке **Центр управления сетями и общим доступом**.
4. Далее выбираем “**Изменение параметров адаптера**”, “**Подключение по локальной сети**”, “**Свойства**”.
5. Настраиваем **параметры протокола TCP/IP**. (ip адрес из той же сети что и у соседа).
6. Открываем окно “**Свойства системы**”. Задаем рабочую группу (название указывает преподаватель)

Примечание. Название рабочей группы должно быть одинаковым для всех компьютеров класса, иначе могут возникнуть проблемы с отображением значков компьютеров в сети.

7. На странице **Центр управления сетями и общим доступом** выбираем “**Изменить дополнительные параметры общего доступа**”

8. Выберите радиокнопку **Включить общий доступ к файлам и принтерам**.

Задание 2. Предоставление папки в общий доступ

1. Войдите в систему с учетной записью, входящей в локальную группу «Администраторы»
2. В меню **Пуск** выберите пункт **Мой компьютер**.
3. В открывшемся окне **Мой компьютер** выполните двойной щелчок мышью на значке одного из жестких дисков (например, Локальный диск (C:)).
4. В окне **Локальный диск (C:)** щелкните правой кнопкой мыши на любом свободном участке окна, выберите в контекстном меню пункт **Создать, Папку**, введите имя папки, совпадающее с именем вашей учетной записи (например, User1) и нажмите клавишу Enter.
5. Щелкните правой кнопкой мыши на значке только что созданной папки и выберите в контекстном меню пункт **Общий доступ и безопасность**.
6. В открывшемся окне свойств папки убедитесь, что вы находитесь на вкладке **Доступ**. В разделе **Общий доступ и безопасность** пометьте флажки **Открыть общий доступ к этой папке** и **Разрешить изменение файлов по сети**, после чего щелкните мышью на кнопке **ОК**.
Изменился ли значок выбранной папки после ее предоставления в общий доступ?
7. Выполните двойной щелчок мышью на значке созданной папки.
8. В открывшемся окне папки создайте текстовый файл с именем, совпадающим с именем вашей учетной записи (например, User1).

9. Отредактируйте созданный файл, поместив туда несколько строк текста, и сохраните изменения.

10. Закройте все окна.

Задание 3. Работа с общими папками в одноранговой сети

1. Найдите через сеть файл, созданный вашим партнером (например, файл User2.txt). Откройте его и внесите свои изменения, после чего сохраните файл

Практическое занятие №4

Сетевая адресация (канальный, сетевой, транспортный уровни)

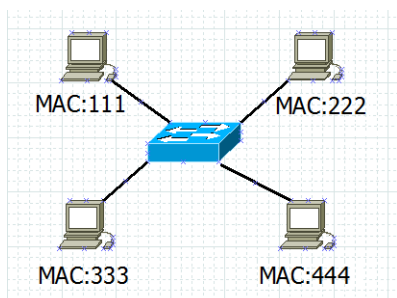
Теоретические сведения

У вас есть оконечное сетевое устройство. Не важно компьютер, ноутбук, планшет смартфон или еще что. Каждое из этих устройств работает по стеку TCP/IP. А значит, оно соблюдает его правила.

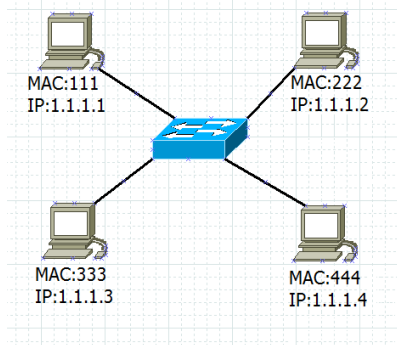
- 1) Прикладной уровень. Тут работает само сетевое приложение.
- 2) Транспортный уровень. У приложения или службы должен быть порт, который он слушает и по которому с ним можно связаться.
- 3) Сетевой уровень. Здесь присутствует IP-адрес. Его еще называют логическим адресом устройства в сети. При помощи него можно связаться с компьютером.
- 4) Канальный уровень. Это сама сетевая карточка. У неё есть физический адрес для идентификации. Это среда, которая свяжет компьютер с другими участниками.

На этом уровне работают MAC-адреса, которые еще называют физическими адресами.

Термин «физические адреса» ввели не просто так. Каждая сетевая карта или антенна имеет вшитый адрес, который ей присваивает производитель. На канальном уровне работают свои протоколы и количество их не маленькое. Самые популярные — это Ethernet (используется в локальных сетях), PPP и HDLC (они используются в глобальных сетях). Это конечно далеко не все, но Cisco в своей сертификации CCNA рассматривает только их. Объясним на картинке.



У каждого компьютера есть свой MAC-адрес, который идентифицирует его в сети. Он должен быть обязательно уникальным. Хотя здесь он отмечен 3-х значными цифрами, это далеко не так. Эти 4 компьютера образуют простенькую локальную сеть и одну канальную среду. Отсюда и название уровня. Но для корректной работы узлов в сетях TCP/IP, недостаточно адресации на канальном уровне. Важна еще адресация на сетевом уровне, которая всем известна, как IP-адресация. Теперь вспоминаем про IP-адреса. И присвоим их нашим компьютерам.



Адреса присвоили символически, чтобы на базовом уровне понять, как они работают. Вот эти две адресации (канальная и сетевая) работают в тесной связке между собой и по отдельности работать не смогут. Мы в повседневной жизни работаем только с IP-адресами или именами. С MAC-адресами мы фактически не работаем. С ними работают сами компьютеры.

Рассмотрим ситуацию. Сидим за верхним левым компьютером с IP: 1.1.1.1 и MAC: 111. Свяжемся с ПК, который имеет MAC:444. Мы сможем связаться с ним, если будем знать его IP-адрес. MAC-адрес его не интересен. Мы знаем, что IP-адрес у него 1.1.1.4. И решаем воспользоваться утилитой ping (утилита проверки доступности узла).

Для того, чтобы узнать MAC-адрес по IP-адресу, придумали протокол ARP. (ответ будет «1.1.1.4 — это я. Мой MAC — 444».)

Дальше нужно научиться отличать одну подсеть от другой. И как компьютер понимает, в одной подсети находится он с другим узлом или в разных. Для этого на помощь приходит маска подсети.

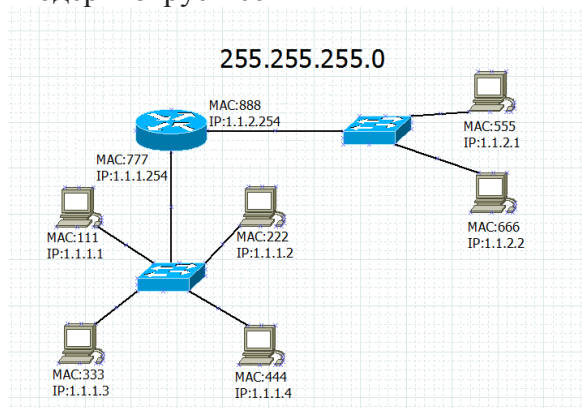
Надо понять, в одной канальной среде мы или нет. Его адрес 1.1.1.4 и маска 255.255.255.0. Маска говорит, что 3 октета фиксированы и не должны меняться, а четвертый может быть любым в пределах от 1 до 254. Я накладываю маску на его адрес и на свой адрес и смотрю совпадения и различия.

1.1.1.1

1.1.1.4

Как видим, у 2-х хостов она одинакова. Значит, они находятся в одной подсети.

Модернизируем сеть



Добавился маршрутизатор. Основная его роль — это соединение сетей и выбор лучшего маршрута, о чем будет в дальнейшем рассказано более подробно. И добавился, справа, один коммутатор, с которым соединены 2 компьютера. Маска для всех устройств не изменилась (255.255.255.0).

Посмотрите внимательно на адреса всех устройств. Можно заметить, что у новых узлов и старых отличается 3-ий октет. Давайте разберемся с этим. Например находимся за ПК с MAC:111 и IP:1.1.1.1. Хотим отправить информацию одному из новых узлов. Давайте пусть это будет верхний правый компьютер с MAC:555 и IP:1.1.2.1. Накладываем маску и смотрим.

1.1.1.1

1.1.2.1

И тут уже другая картина. 3-ие октеты различаются, а значит, узлы находятся в разных сетях (правильнее подсетях). Для разрешения таких ситуации, в настройках каждой операционной системы есть основной шлюз. Используется он, как раз, в том случае, когда нужно отправить информацию узлу, находящемуся в другой канальной среде. Для нашего ПК адрес шлюза — 1.1.1.254. А для компьютера, которому мы отправляю данные 1.1.2.254. Логика работы здесь простая. Если узлу, который находился в одной канальной среде, информация доходила напрямую, то для узла находящегося в другой канальной среде, путь будет через маршрутизатор.

На канальном уровне данные будут отправлены на MAC:777, а на сетевом, на IP:1.1.2.1. Это значит, что MAC-адрес передается только в своей канальной среде, а сетевой адрес не меняется на всем своем пути. Маршрутизатор поймет, что на канальном уровне данные предназначались ему, но когда увидит IP-адрес, то поймет, что он промежуточное звено и передать надо в другую канальную среду. Его второй порт смотрит в нужную подсеть.

Значит, ему все пришло верно. Но он не знает MAC-адрес адресата. Он начинает так же кричать на всю сеть: «Кто такой 1.1.2.1?». И ПК с MAC-адресом 555 отвечает ему.

Много раз упоминался термин «**MAC-адрес**». Давайте разберем, что это такое.

Это уникальный идентификатор сетевого устройства. Он уникален и не должен нигде повторяться. Состоит он из 48 бит, из которых первые 24 бита — это уникальный идентификатор организации, который присваивается комитетом IEEE (Институт инженеров электротехники и электроники). А вторые 24 бита назначаются производителем оборудования. Посмотреть его можно разными способами. Например, в ОС Windows, открыв командную строку, ввести `ipconfig /all`.

Раз мы разобрали адрес на канальном уровне, пришло время разобрать протокол, работающий на данном уровне. Самый популярный на сегодняшний момент протокол, используемый в локальных сетях — это **Ethernet**. IEEE описала его стандартом 802.3. Так что, все версии, которые начинаются с 802.3, относятся именно к нему. Например, 802.3z — это GigabitEthernet через волоконно-оптический кабель; 1 Гбит/с, а 802.3af — это электропитание через Ethernet (PoE — Power over Ethernet).

Так как сам протокол **Ethernet** (придуман в 1973 году), то он много раз модернизировался и менял свой формат.

Ethernet-кадр					
8 байт	6 байт	6 байт	2 байта	46-1500 байт	4 байта
Преамбула	MAC-адрес получателя	MAC-адрес источника	Тип (длина)	SNAP/LLC и данные	FCS (Frame Check Sequence)-контроль суммы

1) **Преамбула**. Поле, используемое для указания начала кадра. То есть, чтобы приемник смог понять, где начало нового кадра. Раньше, когда использовалась топология с общей шиной и были коллизии, преамбула помогала предотвращать коллизии.

2) **MAC-адрес получателя**. Поле, куда записывается адрес получателя.

3) **MAC-адрес отправителя**. Соответственно сюда записывается адрес отправителя.

4) **Тип (длина)**. Раньше в этом поле указывалось, какому вышестоящему протоколу передается данный кадр, но в дальнейшем от этого отказались и ввели поле «Длина». Оно указывает длину поля данных, которое варьируется от 46-1500 байт.

5) **Поле SNAP/LLC + данные**. Как раз SNAP/LLC указывает какому вышестоящему протоколу передать кадр. Это может быть IP, IPX и другие протоколы сетевого уровня. Также в этом поле содержатся данные, полученные с высших уровней.

6) **FCS (от англ. Frame Check Sequence — контрольная сумма кадра)**. Поле в котором подсчитана чек-сумма. По ней получатель понимает, побился кадр или нет.

Переходим к сетевому уровню. Раз мы говорим о сетевом уровне, то значит протокол, работающий на этом уровне, должен каким-то образом уметь передавать данные из одной канальной среды в другую. Но для начала посмотрим, что это за протокол и из чего он состоит.

IP (от англ. Internet Protocol). Протокол семейства TCP/IP, который был разработан в 80-х годах. Используется для объединения отдельных компьютерных сетей между собой. Также важной его особенностью является адресация, которую называют **IP-адресацией**. На текущий момент существуют 2 версии протокола: IPv4 и IPv6. Пару слов о них:

1) **IPv4**. Использует 32-битные адреса, которые записываются в формате четырёх десятичных чисел (от 0 до 255), разделённых точками. Например, адрес 192.168.0.4. Каждое число разделённое точками называют октетом. Это самая популярная версия на сегодняшний день.

2) **IPv6**. Использует 128-битные адреса, которые записываются в формате восьми четырехзначных шестнадцатеричных чисел (от 0 до F). Например, адрес 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d. Каждое число разделённое точками называют хекстетом. На заре всеобщей компьютеризации появилась проблема. Стали заканчиваться IP-адреса и нужен был новый протокол, который смог бы обеспечить больше адресов. Так и появился в 1996 году протокол IPv6. Но благодаря технологии

NAT, которая будет рассмотрена позже, была частично решена проблема нехватки адресов, и, в связи с этим, внедрение IPv6 затянулось по сегодняшний день. Думаю понятно, что обе версии предназначены для одних и тех же целей. Итак, протокол IP работает с блоком информации, который принято называть IP-пакет.

Остался последний уровень из стека TCP/IP. Это **транспортный уровень**. Пару слов о нем. Он предназначен для доставки данных определенному приложению, которое он определяет по номеру порта. В зависимости от протокола, он выполняет разные задачи. 2 самых известных протокола транспортного уровня — это UDP и TCP. Поговорим о каждом из них подробнее, и начну с UDP, в силу его простоты. Ну и по традиции показываю, из чего он состоит.

Порт источника (16 бит)	Порт назначения (16 бит)
Длина UDP (16 бит)	Контрольная сумма UDP
Данные	

Как видите, у него не так много полей. Его задачи — это нумерация портов и проверять побился кадр или нет. Протокол простой и не требовательный к ресурсам. Однако он не может обеспечивать контроль доставки и повторно запрашивать побитые куски информации. Из известных сервисов, которые работают с этим протоколом — это DHCP, TFTP.

Переходим к более сложному протоколу. Встречаем протокол TCP.

Порт источника		Порт назначения	
Порядковый номер (Sequence Number)			
Номер подтверждения (Acknowledgment Number)			
Длина заголовка	Зарезервирован	Флаги	Размер окна
Контрольная сумма TCP		Указатель важности	
Опции			
Данные			

- 1) **Порт источника и порт назначения.** Выполняют те же роли, что и в UDP, а именно нумерация портов.
- 2) **Порядковый номер.** Номер, который используется для того, чтобы на другой стороне было понятно какой этот сегмент по счету.
- 3) **Номер подтверждения.** Это поле используется, когда ожидается доставка или подтверждается доставка. Для этого используется параметр ACK.
- 4) **Длина заголовка.** Используется для того, чтобы понять какой размер у TCP-заголовка (это все поля представленные на картинке выше, кроме поля данных), а какой у данных.
- 5) **Зарезервированный флаг.** Значение этого поля должно устанавливаться в ноль. Оно зарезервировано под специальные нужды. Например, чтобы сообщить о перегрузках в сети.
- 6) **Флаги.** В это поле устанавливаются специальные биты для установления или разрыва сессии.
- 7) **Размер окна.** Поле, указывающее, на сколько сегментов требовать подтверждения. Наверное, каждый из вас наблюдал такую картину. Вы скачиваете какой-то файл и видите скорость и время скачивания. И тут сначала он показывает, что осталось 30 минут, а через 2-3 секунды уже 20 минут. Еще спустя секунд 5, показывает 10 минут и так далее. Это и есть размер окна. Сначала размер окна устанавливается таким образом, чтобы получать больше подтверждений о каждом отправленном сегменте. Далее все идет хорошо и сеть не сбоят. Размер окна меняется и передается больше сегментов и, соответственно, требуя меньше отчетов о доставке. Таким образом, скачивание выполняется быстрее. Как только

сеть даст краткий сбой, и какой то сегмент придет побитым, то размер опять изменится и потребуется больше отчетов о доставке. В этом суть данного поля.

8) Контрольная сумма TCP. Проверка целостности TCP-сегмента.

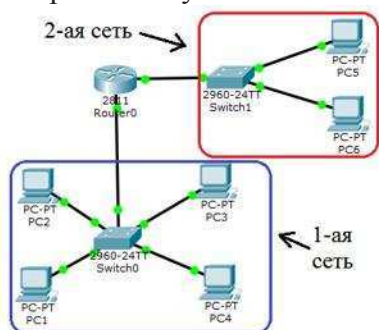
9) Указатель важности. Это смещение последнего октета важных данных относительно SEQ для пакетов с установленным флагом URG. В жизни применяется, когда необходимо осуществить контроль потока или состояния протокола верхнего уровня со стороны передающего агента (например, если принимающий агент может косвенно сигнализировать передающему, что не справляется с потоком данных).

10) Опции. Используется для каких нибудь расширенных или дополнительных параметров.

11) Данные. Практически тоже самое, что и в протоколе UDP. Здесь инкапсулированы данные с вышестоящего уровня.

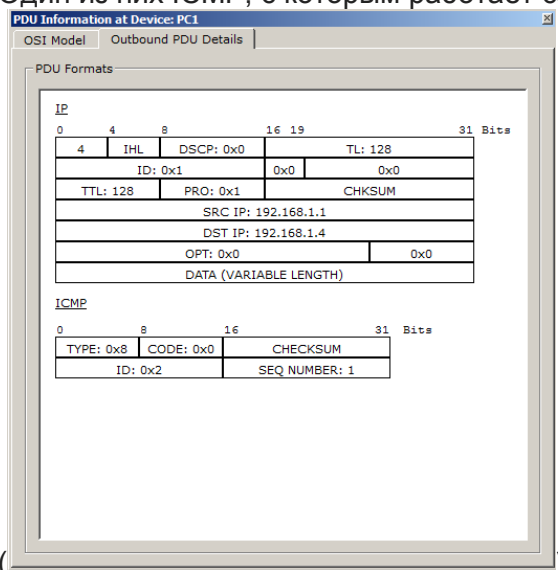
Задание:

- 1) Открыть Cisco Packet Tracer.
- 2) Собрать схему:



Смоделируйте такую ситуацию: Первую сеть, состоящую из 4-х компьютеров и коммутатора, который объединяет эти компьютеры. И 2-ую сеть, состоящую из двух компьютеров и коммутатора. Объединяет эти 2 сети маршрутизатор. Задайте свою Ip –адресацию для этих сетей.

- 3) Проверьте доступность узлов командой ping, которые лежат в 1-ой сети. Как только нажмете ENTER, на схеме появляются конверты. Один из них ICMP, с которым работает сама команда ping. Откройте его.



Что тут можно увидеть? (цифра 4 в верхнем левом углу данных IP, которая говорит о том, что используется протокол IPv4. И 2 поля с IP-адресом источника и назначения (SRC:192.168.1.1 и DST:192.168.1.4))

Тут ping сталкивается с проблемой. Он не знает MAC-адрес получателя. То есть, адрес канального уровня. Для этого он использует протокол ARP, который сможет опросить участников сети и узнать MAC-адрес.

- 4) Посмотрите второй пакет. Что тут можно увидеть?
- 5) Протокол ARP опрашивает все хосты в локальной сети. Какие ответят на него? (1)
<https://habrahabr.ru/post/308636/>

Практическое занятие № 5

Технологии информационного обмена. Общий доступ. Сетевые диски.

Теоретические сведения

Общие папки (shared folders) обеспечивают доступ полномочных пользователей сети к файловым ресурсам.

<http://pandia.ru/text/78/408/18807.php>

Разрешения доступа к общей папке

Общая папка может содержать приложения, данные пользователя. Каждый тип данных требует различных разрешений доступа.

Поскольку разрешения доступа применяются ко всей общей папке, а не к отдельным файлам, они предоставляют менее избирательную защиту, чем разрешения NTFS.

Разрешения доступа к общей папке не ограничивают доступ пользователей, работающих на компьютере, где расположена эта папка. Они применяются только к тем, кто обращается к папке по сети.

Разрешения доступа к общей папке — единственный способ обеспечить безопасность сетевых ресурсов на томе FAT. Разрешения NTFS на томах FAT недоступны.

По умолчанию группа Everyone (Все) получает разрешение Full Control (Полный доступ) для всех новых общих папок.

В Windows Explorer (Проводник) общую папку легко узнать по значку

Разрешения доступа к общим папкам

Разрешение	Позволяет
Изменение	Создавать папки, добавлять к ним файлы, изменять и добавлять данные в файлах, изменять атрибуты файла, удалить папки (файлы) и выполнять действия, допускаемые разрешением Read.
(Чтение)	Просматривать список папок и файлов, содержание файлов и их атрибуты; запускать программы и изменять папки, вложенные в общую папку.
(Полный доступ)	Изменять разрешения для файлов, вступать во владение (Полный доступ) файлами и выполнять все действия, допускаемые разрешением Change.

Можно предоставлять (отменять) разрешения доступа к общей папке. Обычно удобнее назначать разрешения группе, чем отдельным пользователям. Отменять же разрешения следует, только чтобы предотвратить применение нежелательных разрешений. Обычно это происходит, когда в полномочную группу включен пользователь, для которого надо ограничить доступ. Чтобы запретить *все* виды доступа к общей папке, отмените разрешение Full Control.

Применение разрешений доступа к общей папке

Вид доступа к общей папке зависит от разрешений, назначенных учетным записям пользователей и групп. Далее рассматриваются последствия применения разных разрешений.

- **Несколько разрешений совмещаются.** Пользователь может участвовать в нескольких группах, каждая из которых имеет разные разрешения с разными уровнями доступа к общей папке. Действующие разрешения пользователя являются комбинацией разрешений его собственных группы, членом которой он является. Например, имея разрешение Read

(Чтение) и, будучи членом группы, с разрешением Change (Изменить), пользователь будет обладать разрешением Change, включающим в себя Read.

- **Запрет приоритетнее разрешения.** Если пользователю запрещен доступ к общей папке, он не будет иметь его, даже если это разрешено группе, к которой он принадлежит.
- **Для доступа к ресурсам на томах NTFS требуются разрешения NTFS.** Разрешений общей папки достаточно, чтобы получить доступ к ресурсам на томе FAT, но не на томе NTFS. Для доступа к общей папке на диске NTFS помимо разрешения доступа к общей папке требуются и соответствующие разрешения NTFS для каждого общего файла и папки.
- **Общий доступ к скопированным или перемещенным папками прекращается.** При копировании общей папки, общим останется оригинал, но не копия. Перемещенная папка перестает быть общей.

Основные правила назначения разрешений на доступ к общей папке

Основные правила назначения разрешений на доступ к общей папке можно сформулировать следующим образом.

- Определите группы, которым необходим доступ к данному ресурсу и требуемый уровень доступа.
- Назначайте разрешения группам, а не отдельным учетным записям пользователей.
- Назначайте для ресурса максимально строгие разрешения, позволяющие пользователям выполнять только необходимые задачи. Например, если пользователям нужно только читать информацию в папке, а не удалять или создавать в ней файлы, назначьте разрешение Read.
- Папки с одинаковыми требованиями безопасности должны принадлежать одной папке. Скажем, если пользователям требуется разрешение Read для нескольких папок приложения, поместите их в одну и предоставьте к ней совместный доступ (вместо предоставления доступа для каждой папки в отдельности).

Планирование общих папок

Продуманная структура общих папок позволяет централизовать администрирование и упростить доступ к данным. Общие папки могут содержать программы и данные и позволяют создать места для централизованного хранения пользователями своих данных. Общие папки программ применяют для серверных приложений, к которым может обращаться компьютер клиента. Главный плюс общих приложений в том, что вам не нужно устанавливать и поддерживать их компоненты на каждом компьютере. В то время как файлы программ для приложений могут храниться на сервере, данные о конфигурации большинства сетевых программ, как правило, хранятся на компьютерах клиентов. Способ открытия доступа к папкам программ во многом зависит от конкретного приложения, параметров сети и организации работы на предприятии.

- Создав одну папку и разместив в ней все ваши программы, вы устанавливаете единое место для размещения и модернизации ПО.
- Назначьте группе Administrators (Администраторы) разрешение Full Control (Полный доступ) для папки программ, чтобы группа могла управлять прикладным ПО и контролировать разрешения пользователей.
- Отмените разрешение Full Control для группы Everyone (Все) и назначьте разрешение Read (Чтение) для группы Users (Пользователи). Это повысит безопасность, так как группа Users включает только созданные вами учетные записи, а группа Everyone — любого, кто получил доступ к сетевым ресурсам, в том числе учетную запись Guest(Гость).

Для обмена по сети рабочими и общими данными служат папки данных. Папки данных лучше хранить на отдельном томе, где не установлена ОС или приложения. Файлы данных рекомендуется регулярно архивировать, и если они будут храниться на отдельном томе, этот процесс упростится. Кроме того, том с папками данных не будет затронут, если потребуется переустановить ОС.

Предоставляя доступ к папкам общих данных: используйте централизованные папки данных, чтобы было легче их архивировать; назначьте группе Users разрешение Change (изменение)— это обеспечит пользователям единое общедоступное место для хранения данных, которыми они хотят обмениваться; пользователи также смогут получать доступ к папкам, читать, создавать или изменять в них файлы. Открывая доступ к папке рабочих файлов, необходимо: назначить группе (Администраторы) разрешение (Полный доступ) для главной папки данных, чтобы администраторы могли централизованно выполнять ее обслуживание; предоставить доступ к вложенным папкам данных, задав разрешение (Изменение) соответствующим группам.

Открытие доступа к папкам

Открыть доступ к ресурсам можно, сделав общими содержащие их папки. Для этого вы должны быть членом одной или нескольких групп, в зависимости от роли компьютера, на котором находятся общие папки. Доступом к папке и ее содержимому можно управлять, ограничивая количество пользователей, которые могут одновременно к ней обращаться, и назначая разрешения отдельным пользователям и группам. Вы можете изменить параметры общей папки: закрыть к ней доступ, изменить ее сетевое имя, а также разрешения пользователей и групп.

Открыть доступ к папкам вправе только члены встроенных групп Administrators (Администраторы) и Power Users (Опытные пользователи). Какие другие группы могут это делать, и на каких машинах, зависит от того, входят они в рабочую группу или домен, а также от типа компьютера, хранящего общие папки.

- В домене участникам групп Administrators и Server Operators (Операторы сервера) разрешено открывать доступ к папкам на любой машине домена. Power Users могут открыть доступ к папкам только на изолированном сервере или компьютере Windows 2000 Professional, где зарегистрирована эта группа.
- В рабочей группе участникам групп Administrators и Power Users разрешено открывать доступ к папкам на изолированном сервере, где зарегистрирована эта группа.

Для доступа к папке на томе NTFS требуется минимум разрешение Read (Чтение).

Windows автоматически открывает доступ к административным папкам. Эти папки обозначаются знаком доллара (\$), который скрывает общие папки от пользователей, просматривающих содержание компьютера. Корневая папка каждого тома, системная папка и местоположение драйверов принтеров — все это скрытые общие папки, к которым можно получить доступ по сети

Перечень скрытых общих папок не ограничивается теми, которые система создает автоматически. Можно открыть доступ к другим папкам, а если добавить (\$) в конце их сетевого имени, к ней смогут обратиться только пользователи, знающие имя папки и имеющие разрешение на доступ к ней.

Задание:

1. На диске C: создать папку с вашей фамилией и поместить в неё 2 любых файла.
2. На диске C: задать общий доступ для вашей папки.
3. Настроить доступ Чтение и запись для вашей папки
4. Создать сетевой диск из папки Преподаватель, расположенной на ПК Virtual. Сетевой диск должен отображаться в папке Мой компьютер.
5. Отключите сетевой диск Преподаватель.
6. Подключить скрытый диск C, который находится на соседнем компьютере с помощью команды net use.

Сделайте отчет по работе, включив туда скриншоты выполнения работы

Контрольные вопросы

1. Как назначить папке общий доступ? Как отключить общий доступ?
2. Что такое сетевой диск и как его подключить.
3. В чём отличие сетевого диска от папки с общим доступом?

Практическое занятие № 6

Сетевые утилиты, отслеживающие прохождение сетевого трафика.

Теоретические сведения.

Команда PING Команда PING является едва ли не самой используемой в локальных сетях командой. Она позволяет тестировать сетевое соединение, получая информацию о различных его аспектах. Неудачная попытка соединения с каким либо компьютером, или ошибка получения доступа к общим файлам и папкам, находящимся на других компьютерах локальной сети, может быть вызвана тем, что другие компьютеры просто не получают отправленных им по сети запросов.

После введения в командной строке имени команды, в качестве параметра для нее, указывается адрес по которому будут направляться специальные эхо-пакеты, это может быть IP-адрес (рис. 1), или символьное имя компьютера. Получив эхо-запрос, удаленный компьютер сразу же отправляет его обратно по тому адресу, откуда он пришел, команда ping позволяет узнать, пришли ли обратно посланные запросы, проверяя таким образом не только целостность физической среды передачи данных, но и корректную обработку информации на всех остальных семи уровнях модели OSI. При успешном возвращении запросов можно быть уверенным в том, что среда передачи данных, программное обеспечение TCP/IP, а также все устройства (маршрутизаторы, повторители и др.), встретившиеся на пути между двумя компьютерами, работают нормально. Необходимо отметить, что даже при отсутствии каких-либо неисправностей на пути между двумя компьютерами, один или сразу несколько пакетов могут быть утеряны, как правило, это бывает в случае перегруженности сети, а также с тем, что диагностирующие пакеты имеют очень низкий приоритет и могут быть отброшены в процессе передачи. Если хотя бы один из посланных пакетов вернется, это уже будет означать исправность работы сети. По-умолчанию размер эхо-пакета составляет 32 байта, по указанному адресу направляются эхо-пакеты и после выполнения команды выводится статистика прохождения эхо-пакетов по сети.

Команда TRACERT Эта команда подобна команде PING, обе посылают в точку назначения эхо-пакеты и затем ожидают их возвращения. Отличие пакетов команды TRACERT от пакетов PING заключается в том, что они имеют различный срок жизни (Time to Live, TTL). Каждый маршрутизатор при прохождении через него пакета уменьшает значение поля TTL в нем на единицу. Первые пакеты, отправляемые командой TRACERT имеют TTL=1, поэтому первый маршрутизатор, получив такой пакет и уменьшив на единицу поле TTL, обнаруживает, что пакет не может быть доставлен по адресу (пакет с TTL=0 не передается маршрутизатором) и возвращает сообщение об ошибке, содержащее IP-адрес маршрутизатора. Получив это сообщение, команда выводит на экран информацию об IP-адресе маршрутизатора и отправляет по прежнему адресу эхо-пакет с TTL=2. Количество маршрутизаторов, через которые может пройти пакет, будет каждый раз увеличиваться на единицу до тех пор, пока пакет не достигнет точки назначения. Таким образом, с помощью команды tracert можно получить подробный маршрут прохождения пакетов данных между компьютером, на котором была запущена tracert, и любым удаленным компьютером сети. Это делает tracert весьма ценным средством обнаружения неисправностей в сетевом соединении: в случае возникновения проблемы с подключением к Web-узлу или к какой-нибудь другой службе Internet можно определить участок, на котором она возникла.

Утилита NSLOOKUP Утилита nslookup (англ. name server lookup поиск на сервере имён) — утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS (проще говоря, DNS-клиент). Позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера.

Задание

Используя сетевые утилиты PING, TRACEROUTE и NSLOOKUP исследовать свойства сетевых соединений компьютера.

Порядок выполнения задания. С помощью утилиты PING протестировать соединения с серверами находящимися на разном "расстоянии" от нас: в российском сегменте Интернет, в "мировом" интернете. С помощью утилиты TRACERT протестировать соединения с серверами находящимися на разном "расстоянии" от нас: в российском сегменте Интернет, в "мировом" интернете. С помощью утилиты NSLOOKUP определить IP-адреса нескольких интернет ресурсов.

По итогам выполнения работы подготовить отчет.

Практическое занятие № 7

Элементы структурированных кабельных сетей

Теоретические сведения

ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ РАБОЧЕГО МЕСТА.

Основные задачи проектирования В процессе проектирования подсистемы рабочего места решаются следующие основные задачи:

- выбирается конфигурация информационной розетки типичного пользовательского рабочего места и ее конструктивное исполнение;
- рассчитывается количество рабочих мест;
- определяется категория розеточных модулей и абонентских шнуров;
- рассчитывается общее количество абонентских шнуров и их распределение по длинам.

Информационные розетки

Информационные розетки, являющиеся составной частью стационарной линии горизонтальной подсистемы, служат для подключения активного терминального оборудования рабочих мест к СКС абонентскими шнурами.

Согласно стандарту ISO/IEC 11801 одна информационная розетка содержит минимум два модуля Категории 5e/6/7, один из которых может быть заменен на оптический разъём. Такая ИР должна обслуживать примерно 10 м² рабочей площади.

Корпуса информационных розеток делятся на: внешние и внутренние.

Внешний корпус закрывает розеточный модуль со всех сторон, а внутренний выполнен в виде декоративной лицевой панели или иного монтажного основания и оставляет открытой заднюю (кабельную) часть розеточного модуля.

Корпуса внутренней розетки устанавливаются на штатное посадочное место с помощью защёлок.

Посадочные размеры розеток типа Mosaic 45 соответствуют системе Mosaic 45 компании Legrand (22,5x45 мм).

Настенные розетки монтируются непосредственно на поверхность.

Определение количества модулей информационных розеток

Количество модулей информационных розеток зависит от схемы построения горизонтальной подсистемы СКС, в т.ч.

- от наличия решения класса "волокно до рабочего места";
- категории применяемой элементной базы;
- требований ТЗ по конфигурации подсистемы рабочего места СКС.

В соответствии с нормами СанПиН, одно рабочее место занимает:

- 4 кв. м площади для размещения пользователей в офисных зданиях;
- 6 кв. м площади в КБ и иных аналогичных помещениях;
- в случае открытых офисов ожидаемая плотность рабочих мест увеличивается на 10 %.

Площадь для размещения пользователей связана с рабочим коэффициентом 0,66 (0,8 при оценке сверху).

При расчете числа рабочих мест результат всегда округляется до ближайшего целого сверху. Дополнительные розетки обеспечивают эксплуатационную гибкость и используются для подключения групповых устройств типа принтеров, сканеров и т.д. Данный расчет выполняется для каждого пользовательского помещения.

В типовой конфигурации кабельной системы количество розеточных модулей в два раза превышает количество пользовательских информационных розеток. Категория розеточных модулей определяется категорией горизонтальной подсистемы.

Конструктивное исполнение пользовательской информационной розетки зависит от способа ее монтажа на рабочем месте (в короб, на короб, рядом с коробом, в стену и т.д.).

Расчет абонентских шнуров

Общее количество абонентских шнуров рассчитывается в соответствии с одним из четырех принципов:

- по числу рабочих мест;
по требованиям ТЗ;
- по первоначальному количеству пользователей;
- по числу портов коммутаторов уровня рабочей группы.

Размер, на который увеличивается объем поставки, обычно составляет 10 % от общего количества шнуров. Учитываются только шнуры для подключения рабочих станций. Если не указано иное, то шнур для подключения обычного аналогового или цифрового телефонного аппарата считается входящим в комплект его поставки.

Наиболее распространены абонентские шнуры длиной 3 м. Категория и вид исполнения абонентского шнура по экранирующим покрытиям совпадает с аналогичными параметрами самой горизонтальной подсистемы.

ЭЛЕМЕНТЫ ФОРМИРОВАНИЯ КАБЕЛЬНЫХ ТРАСС

Каналы для прокладки кабелей СКС - общие требования. При реализации горизонтальной подсистемы СКС используются каналы следующих разновидностей:

- Короба;
- Лотки;
- Закладные трубы.

При реализации подсистемы внутренних магистралей СКС на переходах через перекрытия и стены используются каналы следующих разновидностей:

- Слот;
- Рукав;
- Закладная труба.

Каналы любого типа должны обеспечивать соблюдение допустимого радиуса изгиба прокладываемых по ним кабелей и не должны иметь острых кромок.

Кабельные лотки не должны повреждать оболочку прокладываемых кабелей. Выпускаются следующие разновидности металлических лотков (в зависимости от назначения:



Проще всего в монтаже — проволочные лотки. Они не требуют специальных аксессуаров — только два-три крепёжных элемента; все соединения, повороты и ответвления выгибаются в процессе монтажа. В этом случае нет необходимости подсчитывать число поворотов, ответвлений и так далее. Однако такие лотки довольно дороги по причине трудоёмкости их производства, поэтому и стоимость монтажа самая высокая (при соответствующем качестве). Обеспечивают прямую видимость кабелей в трассе. Нельзя размещать соединители непосредственно над опорами и по лоткам запрещается ходить.

Наиболее экономичные — штампованные перфорированные или сплошные лотки. Они удобны в реализации при условии наличия аксессуаров: поворотов, ответвлений, вводов и т.д. Возможен вариант, когда все эти элементы выполняются «на месте» болгаркой, при этом могут оставаться острые кромки, а выдержать минимальный радиус изгиба кабелей очень непросто. Штампованные лотки — достаточно гибкое решение: с помощью той же болгарки опытные монтажники «обойдут» лотком любое препятствие на пути кабельной трассы.

Закладные трубы

Широко применяются в нашей стране. Тянущее усилие, прикладываемое к кабелю во время его протяжки, является размеров и конфигурации кабельного канала. На

величину усилия тяжения существенное влияние оказывает радиус изгиба и их количество, а также диаметр и количество прокладываемых кабелей с определённой площадью поперечного сечения.



Сеть закладных металлических или пластиковых труб различного диаметра аналогично подпольным каналам с прямоугольным поперечным сечением устанавливается в структуре междуэтажного перекрытия перед «чистой заливкой» пола.

Такая сеть может делиться на две подсистемы: магистральную и распределительную. Сеть закладных труб согласно стандарту TIA/EIA-569 проектируется таким образом, чтобы в общем случае в ней отсутствовали секции, имеющие более двух изгибов под прямым углом между точками вытяжки кабелей или промежуточными вытяжными коробками, а также с длиной более 30 м. Отечественный ОСТН-600-93 в пункте 2.72 - ограничивает эту длину до 15 м. Укладка труб согласно нормам ОСТН-600-93 осуществляется с уклоном в сторону одной из протяжных коробок. Разность уровней концов труб должна быть не менее 10 мм. Толщина чистого пола над верхней в пакете трубой по СНиП 3.05.06-85, пункт 3.48 должна составлять не менее 20 мм.

Величина радиуса изгиба круглого кабельного канала подбирается с учётом диаметра трубы и типа прокладываемых в них кабелей. Значение радиуса изгиба 400 мм предпочтительно для организации вертикальных выводов. Ни одна из закладных труб не должна иметь более двух изгибов при угле поворота не более 90 градусов.

Ёмкость трубчатых кабельных каналов - это количество кабелей, которые могут в ней размещаться, а следовательно зависит от размеров этих кабелей и самой трубы. Не рекомендуется прокладывать кабели с низким и высоким уровнями сигналов в одной трубе. Таблица на следующем слайде взята из ANSI/EIA/TIA-569-A, одобрена National Electrical Code (NEC, USA), а диаметры подсчитаны для 40% заполнения трубы кабелями.

Данная таблица содержит сведения о ёмкости горизонтальных труб, имеющих не больше двух прямых углов и не длиннее 30 метров. Каждый поворот трубы под прямым углом увеличивает силу трения на величину, равную возникающей на 10 метровом прямом участке трубы.

Таблица ёмкости трубчатых кабельных каналов

Внутренний диаметр трубы, мм	Количество кабеля определенного внешнего диаметра					
	4.6 мм	5.6 мм	6.1 мм	7.4 мм	7.9 мм	9.4 мм
19 (0,75")	5	4	3	2	2	1
25 (1")	8	7	6	3	3	2
32 (1,25")	14	12	10	6	4	3
38 (1,5")	18	16	15	7	6	4
50 (2")	26	22	20	14	12	7
63 (2,5")	40	36	30	17	14	12
76 (3")	60	50	40	20	20	17
102 (4")						30

Расчет количества кабеля горизонтальной подсистемы

В процессе проектирования линейной части горизонтальной подсистемы СКС решается ряд задач:

- определяется конструктивное исполнение и категория линейного кабеля;
- определяется исполнение горизонтального кабеля в отношении его противопожарных параметров;

-определяется ожидаемая величина расхода горизонтального кабеля.

Горизонтальный кабель получил свое название из-за способа укладки на трассе. Предназначен для использования преимущественно в горизонтальной подсистеме, на участке от коммутационного оборудования в техническом помещении этажа (ПУЭ) до информационных розеток (ИР) рабочих мест.

Действующие редакции стандартов допускают применение кабелей с волновым сопротивлением только 100 Ом. Горизонтальный кабель всегда содержит 4 пары. Внешние оболочки обычно изготавливают из поливинилхлорида (PVC). Переход на оболочку из негорючих материалов (LSZH, LSHF, LS0H, LSNH) увеличивает цену кабеля на 20 - 30%, а компаунды, не содержащие галогенов, обладают низкой огнестойкостью. Добавление в исходное сырьё мела обеспечивает необходимую в процессе разделки кабелей хрупкость внешней оболочки (обеспечивает точный и надёжный надрез в выбранном месте).

Стандарт ISO/IEC в Приложении E (информационное) вводит формат построения идентификатора конструкций симметричного кабеля. Идентификатор позволяет в явном виде указать наличие или отсутствие дополнительных экранирующих покрытий отдельных витых пар и/или сердечника в целом.

Идентификатор имеет вид - XX/YYZ, где:



Основной разновидностью горизонтального кабеля является неэкранированный 4-парный кабель с конструкцией U/UTP.

Экранированные конструкции применяются в случаях:

- выдвигаются особые требования по обеспечению конфиденциальности передаваемой информации;

- при работе в сложной помеховой обстановке хотя бы на части кабельной трассы. Используются преимущественно кабели категории 5е, обеспечивающие скорость до 1 Гбит/с, категория 6 применяется при особых требованиях к качеству функционирования канала. В зависимости от конструкции линейной части кабельной трассы используют кабели:

- с оболочкой из негорючего малодымного компаунда LSZH - при прокладке в пленум-полостях;

- более бюджетный кабель с ПВХ-оболочкой - при прокладке в закрытых каналах из негорючего материала.

Алгоритм расчета расхода горизонтального кабеля

При расчете ожидаемого расхода горизонтального кабеля применяется следующая 5-шаговая процедура.

1. Определяем среднюю длину проброса по формуле: $L_{avg} = \frac{L_{max} + L_{min}}{2}$, где L_{max} и L_{min} длина наиболее длинной и наиболее короткой кабельных линий. b - запасы на разделку кабеля (обычно 0,6 - 0,8 м).

2. Делением длины упаковки горизонтального кабеля на среднюю длину проброса с округлением до ближайшего целого снизу находим количество пробросов с одной упаковки.

3. Умножением количества рабочих мест на 2 находим общее количество пробросов.

4. Деля число пробросов на число из шага 2 с округлением до ближайшего целого, сверху находим количество упаковок.

5. Умножением числа упаковок на ее длину находим расход кабеля.

Особенности реализации и ограничения алгоритма

При задании величин L_{max} и L_{min} на шаге 1 учитываем все подъемы, спуски и повороты. Кроме того, наибольшая и наименьшая по длине кабельные трассы должны обязательно иметь одинаковую структуру. Необходимо контролировать выполнение «Правила 12/70»:

-Все кабельные трассы, имеющие длину менее 12 м, не учитываются в общем количестве кабельных трасс.

-Расход кабеля для реализации всех кабельных трасс с длиной свыше 70 м (в правильно спроектированной СКС их не должно быть свыше 5 %) определяется отдельно по тому же алгоритму. Эти трассы также не учитываются в общем количестве кабельных трасс.

Некоторые приемы по ускорению расчетов

При выполнении расчетов горизонтального кабеля могут быть задействованы некоторые приемы, позволяющие несколько сократить время на реализацию алгоритма за счет потери точности.

- В качестве оценки L_{min} можно использовать величину 12 м.

- В качестве оценки L_{max} можно использовать значение полупериметра области установки горизонтальной подсистемы.

- Среднее значение длины стационарной линии по полной совокупности проектов (с учетом отходов) составляет примерно 45 м.

- Последнее при наиболее популярных на практике 305-метровых } упаковках позволяет применить оценку вида «7 портов - коробка».

Задание:

1. Спроектировать подсистемы рабочих мест для предложенной СКС
2. Выполнить расчет горизонтальной подсистемы предложенной СКС

Практическое занятие №8

Расчет адресных пространств локальных сетей.

Задача

1. Приведите примеры адресов конечных узлов классов А, В, С. Используя стандартные маски, рассчитайте адреса соответствующих сетей.
2. Переведите адреса 10.169.77.19, 172.18.190.59 и 192.168.55.112 в двоичную систему.
3. Рассчитайте максимальное количество хостов в подсетях 10.169.77.16/28, 172.18.190.16/27 и 192.168.55.112/29.
4. Для выделенного диапазона адресов 172.16.10.0/24 сформируйте 10 подсетей по 8-14 компьютеров в каждой. Какова будет сетевая маска?
5. Для выделенного адреса 10.1.5.0/24 сформируйте 2 подсети по 50-60 компьютеров, 2 подсети по 25-30 компьютеров, 2 подсети по 10-12 компьютеров, 2 подсети по 5 – 6 компьютеров
6. Каким агрегированным адресом может быть представлена группа из четырех подсетей: 172.16.16.0/24, 172.16.17.0/24, 172.16.18.0/24, 172.16.19.0/24?
7. Оформить отчет.

Контрольные вопросы:

1. Какие размеры имеют стандартные маски адресов классов А, В, С?
2. Какое максимальное число узлов могут задавать адреса класса С?
3. Для чего нужны сетевые маски?
4. Для чего используются частные адреса в локальных сетях?
5. Каковы диапазоны частных адресов?
6. Можно ли использовать частные адреса в сети Интернет?
7. Что переводит частные адреса в общественные?

Практическое занятие № 9. **Настройка сетевых устройств. DHCP, NAT.**

Теоретические сведения

1) Протокол **DHCP** – позволяет производить автоматическую настройку сети на компьютерах и других устройствах. DHCP может быть настроен на маршрутизаторах Cisco или на базе любого сервера. Мы рассмотрим настройку DHCP сервера на маршрутизаторе Cisco. Однако, маршрутизатор может работать и как DHCP клиент – получая адрес на один из своих интерфейсов. Настройка DHCP сервера на маршрутизаторе это удобно в том плане, что если уже есть работающий маршрутизатор, то проще повесить на него максимальное количество функционала (интернет, NAT, DHCP и т.п.) чтобы каждое устройство занималось своим делом. DHCP позволяет автоматически настраивать на клиенте следующие основные параметры:

1. IP адрес
2. Основной шлюз
3. Маска подсети
4. DNS сервера
5. Имя домена

Это наиболее частое использование DHCP, но можно передавать и огромное количество других параметров. Например, можно передавать дополнительные маршруты, чтобы в разные сети компьютер ходил через разные шлюзы. Или, с помощью DHCP можно организовывать загрузку устройств по сети. В этом случае клиент получает помимо основных параметров, адрес TFTP сервера и имя файла на нём (я имею в виду имя файла – загрузчика ОС, которую необходимо загрузить по сети).

Когда клиент, например, обычный компьютер, запускается, ОС видит, что для некоей сетевой карты стоит «Получить параметры по DHCP». Такой компьютер не имеет пока IP адреса и происходит следующая процедура получения:

1. Компьютер отправляет широковещательный запрос. При этом на втором уровне в фрейме стоит мак адрес отправителя – адрес компьютера, мак адрес получателя – ffff.ffff.ffff, а на третьем уровне – в пакете адрес отправителя отсутствует, адрес получателя стоит 255.255.255.255. Такое DHCP сообщение называется «DHCP discover».
2. Далее все устройства в сети получают это широковещательное сообщение. DHCP сервера (а их теоретически может быть несколько) отвечают клиенту. Сервер резервирует в своём пуле адресов какой-то адрес (если не было резервации до этого для данного мас-адреса клиента) и выделяет этот ip клиенту на какое-то время (lease time). Берутся другие настройки и всё вместе высылается. При этом в качестве адресов получателя используется уже новый выделенный клиентский ip и клиентский мас. Это называется «DHCP offer».
3. Клиент выбирает понравившийся ему сервер (обычно он всего один) либо выбирается тот кто ответил первым. И отправляет со своего мас и нового ip на мас и ip уже конкретного сервера «DHCP request» – согласие с полученными параметрами.
4. Сервер резервирует за клиентом выделенный адрес на какое-то время (lease time). До этого момента адрес был выделен, но не зарезервирован. Теперь же он окончательно закреплён за клиентом. Сервер вносит так же строчку в свою ARP таблицу и высылает клиенту, сообщение, что он успешно зарегистрирован – «DHCP Acknowledge».

5. Клиент начинает работать.

Есть одна странная, на первый взгляд вещь, на цисках DHCP как бы не привязан к конкретному интерфейсу, то есть просто создаётся пул и маршрутизатор раздаёт адреса где хочет. На самом деле, адреса раздаются не всем, а только на том интерфейсе, на котором IP адрес из той же сети, что упоминается в пуле: действительно, какой смысл выдавать компьютеру адрес шлюза, который находится не в его сети.

Настроим маршрутизатор, который будет выдавать по DHCP сеть 192.168.1.0/24 начиная с 192.168.1.11.

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Мы просим маршрутизатор не выдавать адреса с 192.168.1.1 по 192.168.1.10. Так как первый адрес будет использоваться самим маршрутизатором (шлюз), а остальные девять имеет смысл зарезервировать под различные сервера в этой сети. Серверам не стоит выдавать адреса по DHCP – к ним часто обращаются, поэтому адрес должен быть вбит статически и никогда не меняться. В нашем примере, например, присутствует DNS сервер с адресом 192.168.1.5, который вбит статикой. Теперь создаём пул:

```
R1(config)#ip dhcp pool MY-POOL
```

```
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
```

```
R1(dhcp-config)#default-router 192.168.1.1
```

```
R1(dhcp-config)#domain-name my-domain.com
```

```
R1(dhcp-config)#dns-server 192.168.1.5
```

```
R1(dhcp-config)#exit
```

Выдаваться адреса будут из сети 192.168.1.0/24 (кроме тех что мы исключили ранее), в качестве шлюза будем выдавать 192.168.1.1 – наш маршрутизатор. Сам этот адрес надо ещё настроить:

```
R1(config)#interface fa0/0
```

```
R1(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
R1(config-if)#exit
```

```
R1(config)#exit
```

```
R1#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

После того, как компьютер получил адрес, можно проверить список выданных адресов:

```
R1#show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.11	000A.F337.2447	--	Automatic

2) Настройка NAT

NAT (Network address translation) — технология трансляции сетевых адресов. Технология NAT позволила решить наибольшую проблему протокола IPv4: к середине 1990-х годов пространство IPv4-адресов могло быть полностью исчерпано. Если бы технологию NAT не изобрели то, рост Интернета значительно замедлился бы. Конечно, на сегодня создана новая версия протокола IP — IPv6. Данная версия поддерживает огромное количество IP-адресов, что существование NAT — бессмысленно. Однако, до сих пор довольно много организаций используют в своей работе протокол IPv4 и полный переход на IPv6 состоится не скоро. Поэтому есть смысл изучить технологию NAT.

Трансляция сетевых адресов NAT позволяет хосту, не имеющего «белого IP», осуществлять связь с другими хостами через Интернет. Белый IP-адрес представляет из себя зарегистрированный, уникальный, глобальный IP-адрес в сети Интернет. Есть также «серые IP-адреса», которые используются в частной сети и не маршрутизируются в сети Интернет. Поэтому необходима технология NAT, которая будет подменять серый IP-адрес на белый. Диапазон «серых IP-адресов» представлен в таблице.

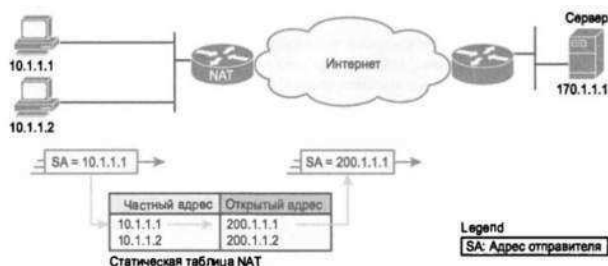
Идентификатор частной сети	Маска подсети	Диапазон IP-адресов
10.0.0.0	255.0.0.0	10.0.0.1 – 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 – 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 – 192.168.255.254

Осуществляя трансляцию NAT, маршрутизатор изменяет IP-адрес отправителя в тот момент, когда пакет покидает частную сеть. Маршрутизатор также изменяет адрес получателя каждого пакета, который возвращается в частную сеть. Программное обеспечение Cisco IOS поддерживает несколько разновидностей трансляции NAT:

1. Статическая трансляция NAT — каждому частному IP-адресу соответствует один публичный IP. При использовании статической трансляции маршрутизатор NAT просто устанавливает взаимно однозначное соответствие между частным и зарегистрированным IP-адресом, от имени которого он выступает.
2. Динамическая трансляция NAT — преобразование внутренних IP-адресов во внешние происходит динамически. Создается пул возможных публичных IP-адресов и из этого пула динамически выбираются IP-адреса для преобразования.
3. Трансляция адресов портов PAT — позволяет выполнить масштабирование для поддержки многих клиентов с использованием всего лишь нескольких открытых IP-адресов. PAT транслирует сетевой адрес в зависимости от TCP/UDP-порта получателя.

Рассмотрим более подробно каждый из видов трансляции.

Статическая трансляция NAT делает точное соответствие между частным и публичным IP-адресом. Рассмотрим на примере.



Провайдер ISP компании назначает ей зарегистрированный номер сети 200.1.1.0. Соответственно маршрутизатор NAT должен сделать так, чтобы этот частный адрес выглядел таким образом, как если бы находился в сети 200.1.1.0. Для этого маршрутизатор изменяет IP-адрес отправителя в пакетах, которые как на рисунке пересылаются слева направо. В данном примере маршрутизатор изменяет частный IP-адрес 10.1.1.1 на открытый 200.1.1.1. Другому частному адресу 10.1.1.2 соответствует публичный 200.1.1.2. Далее рассмотрим настройку статического NAT в Cisco.

Настройка статической трансляции NAT на оборудовании Cisco по сравнению с другими ее вариантами требует наименьших действий. При этом нужно установить соответствие между локальными (частными) и глобальными (открытыми) IP-адресами. Кроме того, необходимо указать маршрутизатору, на каких интерфейсах следует использовать трансляцию NAT, поскольку она может быть включена не на всех интерфейсах. В частности, маршрутизатору нужно указать каждый интерфейс и является ли он внутренним или внешним.

Пример конфигурации для роутера:

```
NAT_GW>enable - переходим в расширенный режим
NAT_GW#configure terminal - переходим в режим конфигурации
NAT_GW(config)#interface fa0/0 - настройка интерфейса в сторону частной сети
NAT_GW(config-if)#description LAN - описание интерфейса
NAT_GW(config-if)#ip address 192.168.1.1 255.255.255.0 - задаем шлюз по-умолчанию
NAT_GW(config-if)#no shutdown - включаем интерфейс физически
NAT_GW(config-if)#ip nat inside - настраиваем интерфейс как внутренний
NAT_GW(config-if)#exit
NAT_GW(config)#interface fa0/1 - настройки интерфейса в сторону провайдера
NAT_GW(config-if)#description ISP - описание интерфейса
NAT_GW(config-if)#ip address 100.0.0.253 255.255.255.0 - задаем Ip и маску
NAT_GW(config-if)#no shutdown - включаем интерфейс физически
NAT_GW(config-if)#ip nat outside - настраиваем интерфейс как внешний
NAT_GW(config-if)#exit
NAT_GW(config)#ip nat inside source static 192.168.1.2 100.0.0.1 - статическое сопоставление
адресов
NAT_GW(config)#ip nat inside source static 192.168.1.3 100.0.0.2 - статическое сопоставление
адресов
NAT_GW(config)#ip nat inside source static 192.168.1.4 100.0.0.3 - статическое сопоставление
адресов
NAT_GW(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.254 - статический маршрут в сторону провайдера
```

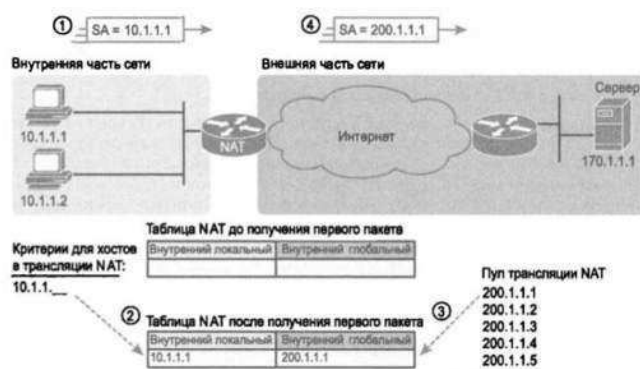
Статические соответствия создаются с помощью команды *ip nat inside source static*. Ключевое слово *inside* означает, что NAT транслирует адреса для хостов, находящихся во внутренней части сети. Ключевое слово *source* означает, что NAT транслирует IP-адреса в пакетах, поступающих на ее внутренние интерфейсы. Ключевое слово *static* означает, что эти параметры определяют статическую запись, которая никогда не удалится из таблицы NAT в связи с истечением периода времени. При создании записей статической трансляции NAT маршрутизатору необходимо знать, какие интерфейсы являются внутренними (*inside*), а какие внешними (*outside*). Подкоманды интерфейса *ip nat inside* и *ip nat outside* соответствующим образом идентифицируют каждый интерфейс.

Для просмотра важной информации о NAT существует две команды *show ip nat translations*, *show ip nat statistics*.

Первая команда выводит три записи статической трансляции NAT, созданной в конфигурации. Вторая команда выводит статистическую информацию, такую, как количество активных в данный момент записей в таблице трансляции. Эта статистика

также включает в себя количество повторных попаданий (hit), которое увеличивается на единицу с каждым пакетом, для которого NAT должна транслировать адреса.

Перейдем далее к **динамической трансляции сетевых адресов NAT**. Динамическая трансляция создает пул возможных глобальных внутренних адресов и определяет критерий соответствия для определения того, какие внутренние глобальные IP-адреса должны транслироваться с помощью NAT. Например, в схеме ниже был установлен пул из пяти глобальных IP-адресов в диапазоне 200.1.1.1 — 200.1.1.5. Трансляция NAT также настроена для преобразования всех внутренних локальных адресов, которые начинаются с октетов 10.1.1



При настройке динамической трансляции NAT на оборудовании Cisco по-прежнему требуется идентификация каждого интерфейса как внутреннего, так и внешнего, но уже не нужно задавать статическое соответствие. Для указания частных IP-адресов, подлежащих трансляции, динамическая трансляция NAT использует списки управления доступом ACL а также определяет пул зарегистрированных открытых IP-адресов, которые будут выделяться из этого. Итак, алгоритм настройки динамической трансляции:

1. Настроить интерфейсы, которые будут находится во внутренней подсети, с помощью команды *ip nat inside*.
2. Настроить интерфейсы, которые будут находится во внешней подсети, с помощью команды *ip nat outside*.
3. Настроить список ACL, соответствующий пакетам, поступающим на внутренние интерфейсы, для которых должна быть применена трансляция NAT
4. Настроить пул открытых зарегистрированных IP-адресов с помощью команды режима глобального конфигурирования *ip nat pool имя первый-адрес последний-адрес netmask маска-подсети*.
5. Включить динамическую трансляцию NAT, указав в команде глобального конфигурирования *ip nat inside source list номер-acl pool имя-пула*

Пример конфигурации для роутера:

```
NAT_GW>enable - переходим в расширенный режим
NAT_GW#configure terminal - переходим в режим конфигурации
NAT_GW(config)#interface fa0/0 - настройка интерфейса в сторону частной сети
NAT_GW(config-if)#description LAN - описание интерфейса
NAT_GW(config-if)#ip address 192.168.1.1 255.255.255.0 - задаем шлюз по-умолчанию
NAT_GW(config-if)#no shutdown - включаем интерфейс физически
NAT_GW(config-if)#ip nat inside - настраиваем интерфейс как внутренний
NAT_GW(config-if)#exit
NAT_GW(config)#interface fa0/1 - настройки интерфейса в сторону провайдера
NAT_GW(config-if)#description ISP - описание интерфейса
NAT_GW(config-if)#ip address 100.0.0.253 255.255.255.0 - задаем Ip и маску
```



```
NAT_GW(config-if)#no shutdown - включаем интерфейс физически
NAT_GW(config-if)#ip nat outside - настраиваем интерфейс как внешний
NAT_GW(config-if)#exit
NAT_GW(config)#ip nat pool testPool 100.0.0.1 100.0.0.252 netmask 255.255.255.0- создаем динамический пул
NAT_GW(config)#access-list 1 permit 192.168.1.1 0.0.0.255 - создаем список доступа 1, в котором разрешаем транслировать Ip-адреса из подсети 192.168.1.1/24
NAT_GW(config)#ip nat inside source list 1 pool testPool - включаем динамическую трансляцию
NAT_GW(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.254 - статический маршрут в сторону провайдера
```

Задание:

- 1) Настроить статическую трансляцию NAT для роутера. Данные для интерфейсов взять у преподавателя
- 2) Настроить динамическую трансляцию NAT для роутера. Данные для интерфейсов взять у преподавателя
- 3) Настроить маршрутизатор, который будет выдавать по DHCP сеть X начиная с ip адреса Y. Значения X и Y взять у преподавателя.

Практическое занятие № 10.

Отслеживание разрешения DNS-имени. Изучение веб-запросов.

Теоретические сведения

Ежедневно для получения доступа к услугам, доступным по сети Интернет, мы обращаемся к тысячам серверов, расположенных в различных географических точках. Каждому из этих серверов присваивается уникальный **IP-адрес**, по которому он идентифицируется в подключенной локальной сети. Было бы невозможно запомнить все IP-адреса всех серверов, предоставляющих различные услуги по сети Интернет. Вместо этого предлагается более простой способ поиска серверов – сопоставить имя с некоторым IP-адресом. Служба доменных имен (**DNS**) позволяет использовать имя узла для запроса IP-адреса отдельного сервера. Регистрация и организация имен в этой системе выполняется по специальным высокоуровневым группам, именуемым доменами. В DNS-сервере записана специальная таблица, ассоциирующая имена узлов в домене с соответствующим IP-адресом. Если клиент знает имя сервера, например, веб-сервера, но требуется найти IP-адрес, он направляет запрос на этот DNS-сервер через порт 53. Клиент использует этот IP-адрес DNS-сервера, прописанного в настройках DNS раздела конфигурации IP этого узла. При получении запроса DNS-сервер выясняет по своей таблице, имеется ли соответствие между запрашиваемым IP-адресом и веб-сервером. Если на DNS-сервере отсутствует запись о запрашиваемом имени, он опрашивает другой DNS-сервер в пределах своего домена. После распознавания IP-адреса DNS-сервер отправляет результат обратно к клиенту. Если DNS-серверу не удалось определить IP-адрес, клиент не сможет установить связь с этим веб-сервером и получит сообщение об истечении времени ожидания. Команда `nslookup` – команда операционных систем UNIX и Windows для запроса информации с серверов доменных имен в Интернете. Требуются следующие ресурсы:

- компьютер под управлением Windows с подключением к Интернету;
- доступ к команде Run.

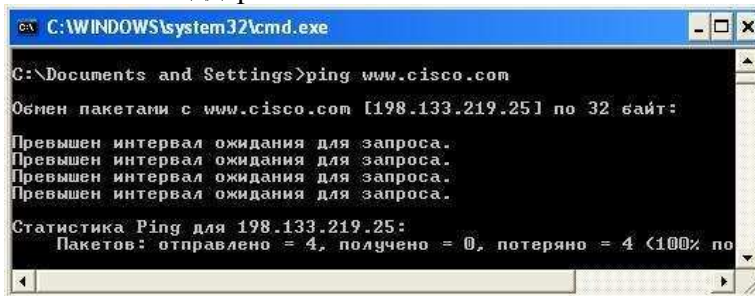
Ход работы:

1. Отслеживание преобразований DNS.

а. Нажмите кнопку «Пуск», выберите команду «Выполнить», введите команду `cmd`, а затем нажмите кнопку «ОК». Откроется окно командной строки.

б. В командной строке введите `ping www.cisco.com`. Компьютеру необходимо преобразовать `www.cisco.com` в IP-адрес, чтобы знать, куда отправлять ICMP-пакеты. Команда `ping` отправляет пакеты этого типа.

в. В первой строке выходных данных показано имя `www.cisco.com`, преобразованное в IP-адрес системой DNS. Результаты работы системы DNS должны быть видны, даже если в учебном учреждении есть межсетевой экран, блокирующий обмен пакетами, или если компания Cisco не поддерживает обмен пакетами со своими веб-серверами.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>ping www.cisco.com
Обмен пакетами с www.cisco.com [198.133.219.25] по 32 байт:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Статистика Ping для 198.133.219.25:
Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% по
```

г. Какой IP-адрес показан на экране?

д. Совпадает ли он с адресом, показанным на представленном выше рисунке?

2. Проверка работы системы DNS с помощью команды `nslookup`.

а. В командной строке введите команду `nslookup`.

б. Какой DNS-сервер используется по умолчанию?

в. Обратите внимание на изменение командной строки. Это командная строка **NSLOOKUP**. В данной командной строке можно вводить команды, относящиеся к системе DNS.

г. В командной строке введите **?**, чтобы просмотреть список всех команд, доступных в режиме **NSLOOKUP**.

д. Запишите три команды, которые можно использовать в режиме **NSLOOKUP**.

е. В командной строке **NSLOOKUP** введите **www.cisco.com**.

ж. Каков преобразованный IP-адрес?

з. Совпадает ли он с адресом из выходных данных команды **ping**?

и. В командной строке введите IP-адрес только что обнаруженного веб-сервера Cisco. С помощью команды **NSLOOKUP** можно узнать доменное имя IP-адреса, если URL-адрес не известен. Используя описанные выше процедуры, найдите IP-адрес, соответствующий имени www.google.com.

3. Определение почтовых серверов с помощью команды nslookup.

а. В командной строке введите **set type=mx**, чтобы с помощью команды **NSLOOKUP** определить почтовые серверы.

б. В командной строке введите **www.cisco.com**.

в. Какие у данного сервера: основное имя, ответственный почтовый адрес и время жизни (TTL) по умолчанию?

г. В командной строке введите команду **exit**, чтобы вернуться к обычной командной строке.

д. В этой командной строке введите **ipconfig /all**.

е. Запишите IP-адреса всех используемых в локальной сети DNS-серверов.

ж. Введите команду **exit**, чтобы закрыть окно командной строки.

Контрольные вопросы:

1. Какие требуются ресурсы для отслеживания разрешения DNS-имен?
2. Что происходит, если на DNS-сервере отсутствует запись о запрашиваемом имени?
3. Для чего нужна команда nslookup?

Практическое занятие № 11

Изучение протокола FTP. Настройка клиента электронной почты.

Теоретические сведения

Протокол FTP позволяет переместить файл с удаленного компьютера на локальный. FTP также поддерживает несколько команд просмотра удаленного каталога и перемещения по каталогам удаленной файловой системы. Поэтому FTP используется для доступа к тем файлам, данные которых нет смысла просматривать удаленно, а гораздо эффективней переместить на клиентский компьютер. В протокол FTP встроены примитивные средства авторизации удаленных пользователей на основе передачи по сети пароля в открытом виде. Кроме того, поддерживается анонимный доступ, не требующий указания имени пользователя и пароля; такой способ доступа часто рассматривается как более безопасный, так как он не подвергает пароли пользователей угрозе перехвата.

Клиент посылает запросы серверу, принимает и передает файлы.

Сервер обрабатывает запросы клиента, передает и принимает файлы

FTP-серверы, как правило, доступны только для зарегистрированных пользователей и требуют при подключении: ввода идентификатора (login – входное имя) и пароля (password).

Большинство Web-браузеров обеспечивают доступ к FTP-серверам без использования специальных FTP-клиентов. Например, URL-адрес: ftp://ftp.ware.ru/pub/win/internet/ftp/dl.zip означает “связаться с FTP-сервером с правами для анонимных пользователей

Сеанс работы с FTP-сервером можно провести в режиме командной строки. Для этого необходимо ввести команду ftp и после пробела ввести IP-адрес или DNS-адрес FTP-сервера. Если регистрация прошла успешно и связь установлена, то с помощью команд FTP можно выполнить все действия по работе с файлами.

Основные модули службы FTP

FTP-клиент состоит из трех основных функциональных модулей.

- **User Interface** (аналог агента пользователя) — пользовательский интерфейс, принимающий от пользователя команды и отображающий состояние FTP-сеанса на экране.

User-PI — интерпретатор команд пользователя. Этот модуль взаимодействует с модулем Server-PI FTP-сервера.

User-DTP — модуль, осуществляющий передачу данных файла по командам, получаемым от модуля User-PI по протоколу клиент-сервер. Этот модуль взаимодействует с локальной файловой системой клиента.

FTP-сервер включает два модуля.

- **Server-PI** — модуль, который принимает и интерпретирует команды, передаваемые по сети модулем User-PI.

- **Server-DTP** — модуль, управляющий передачей данных файла по командам от модуля Server-PI. Взаимодействует с локальной файловой системой сервера.

Управляющий сеанс и сеанс передачи данных

FTP-клиент и FTP-сервер поддерживают параллельно два сеанса — управляющий сеанс и сеанс передачи данных. *Управляющий сеанс* открывается при установлении первоначального FTP-соединения клиента с сервером, причем в течение одного управляющего сеанса может последовательно выполняться несколько *сеансов передачи данных*, в рамках которых передаются или принимаются несколько файлов.

Общая схема взаимодействия клиента и сервера выглядит следующим образом.

1. FTP-сервер всегда открывает управляющий TCP-порт 21 для прослушивания, ожидая прихода запроса на установление управляющего FTP-соединения от удаленного клиента.
2. После установления управляющего соединения FTP-клиент отправляет на сервер команды, которые уточняют параметры соединения: имя и пароль клиента, роль участников соединения (активная или пассивная), порт передачи данных, тип передачи,

тип передаваемых данных (двоичные данные или код ASCII), директивы на выполнение действий (читать файл, писать файл, удалить файл и т. п.).

3. После согласования параметров пассивный участник соединения переходит в режим ожидания открытия соединения на порт передачи данных. Активный участник инициирует это соединение и начинает передачу данных.

4. После окончания передачи данных соединение по портам данных закрывается, а управляющее соединение остается открытым. Пользователь может по управляющему соединению активизировать новый сеанс передачи данных.

Порты передачи данных выбирает FTP-клиент (по умолчанию клиент может использовать для передачи данных порт управляющего сеанса), а сервер должен задействовать порт, номер которого на единицу меньше номера порта клиента.

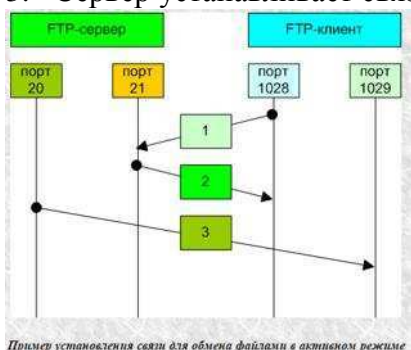
Протокол FTP предусматривает два возможных режима установления связи для обмена файлами:

- **активный режим;**
- **пассивный режим.**

Активный режим

Действия клиента и сервера:

1. Клиент устанавливает связь и посылает с нестандартного порта N ($N > 1024$) запрос на 21 порт сервера;
2. Сервер посылает ответ на порт N клиента;
3. Сервер устанавливает связь для передачи данных по порту 20 на порт клиента N+1.

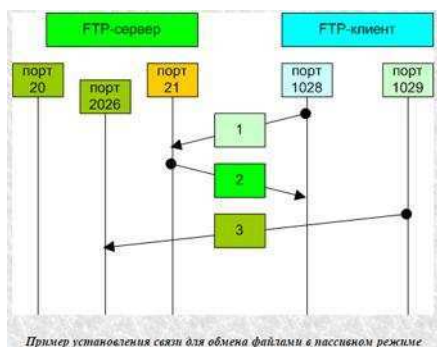


Активный режим выгоден для FTP-сервера, но вреден для клиента. Так как FTP сервер пытается соединиться со случайным высоким (по номеру) портом на клиенте, то такое соединение может быть заблокировано брандмауэром на стороне клиента.

Пассивный режим

Действия клиента и сервера

1. Клиент устанавливает связь и посылает запрос (сообщает, что надо работать в пассивном режиме) на 21 порт сервера с нестандартного порта N ($N > 1024$);
2. Сервер назначает нестандартный порт P для канала данных ($P > 1024$) и посылает на порт N клиента ответ, в котором сообщает номер порта P;
3. Клиент устанавливает связь для передачи данных по порту N+1 на порт сервера P.



Пассивный режим выгоден для клиента, но вреден для FTP-сервера. Клиент будет делать два соединения к серверу, при этом второе будет к случайному высокому порту. Такое соединение может быть заблокировано брандмауэром на стороне сервера.

Команды взаимодействия FTP-клиента с FTP-сервером

В протоколе FTP предусмотрены специальные команды для взаимодействия FTP-клиента с FTP-сервером (не следует их путать с командами пользовательского интерфейса клиента, ориентированные на применение человеком). Эти команды делятся на три группы.

- **Команды управления доступом к системе** доставляют серверу имя и пароль клиента, изменяют текущий каталог на сервере, повторно инициализируют, а также завершают управляющий сеанс.

Команды управления потоком данных устанавливают параметры передачи данных.

Служба FTP может применяться для передачи разных типов данных (код ASCII или двоичные данные), работать как со структурированными данными (файл, запись, страница), так и с неструктурированными.

- **Команды службы FTP** управляют передачей файлов, операциями над удаленными файлами и каталогами. Например, команды RETR и STOR запрашивают передачу файла соответственно от сервера на клиентский хост, и наоборот. Параметрами каждой из этих команд является имя файла. Может быть задано также смещение от начала файла — это позволяет начать передачу файла с определенного места при непредвиденном разрыве соединения. Команды DELE, MKD, RMD, LIST соответственно удаляют файл, создают каталог, удаляют каталог и передают список файлов текущего каталога. Каждая команда протокола FTP передается в виде одной строки кода ASCII.

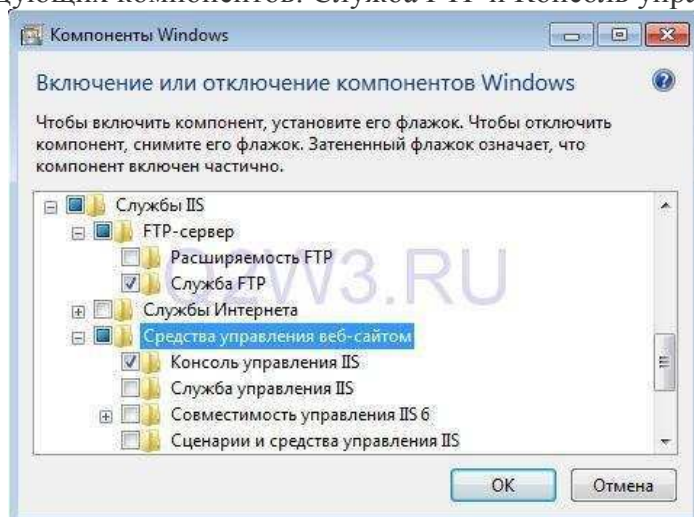
Работа FTP на пользовательском уровне при передаче файлов **содержит несколько этапов:**

1. Идентификация (ввод имени-идентификатора и пароля);
2. Выбор каталога;
3. Определение режима обмена:
 - передача файлов в текстовом виде;
 - передача файлов в бинарном виде;
4. Выполнение команд обмена;
5. Завершение работы
- 6.

Ход работы:

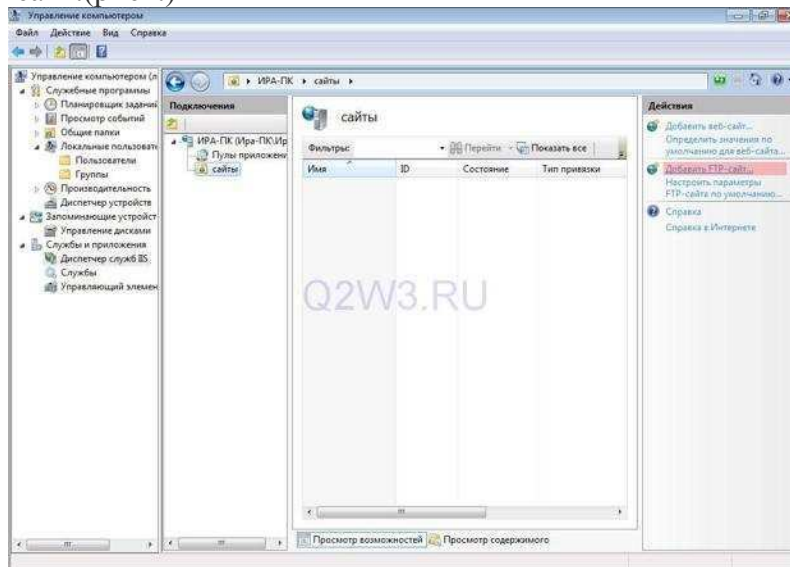
1. Установка FTP-сервера.

FTP-сервер входит в состав служб IIS. Для его установки открываем Панель управления -> Программы -> Включение или отключение компонентов Windows. Раскрываем раздел Службы IIS и ставим галочки напротив следующих компонентов: Служба FTP и Консоль управления IIS.(рис1.)

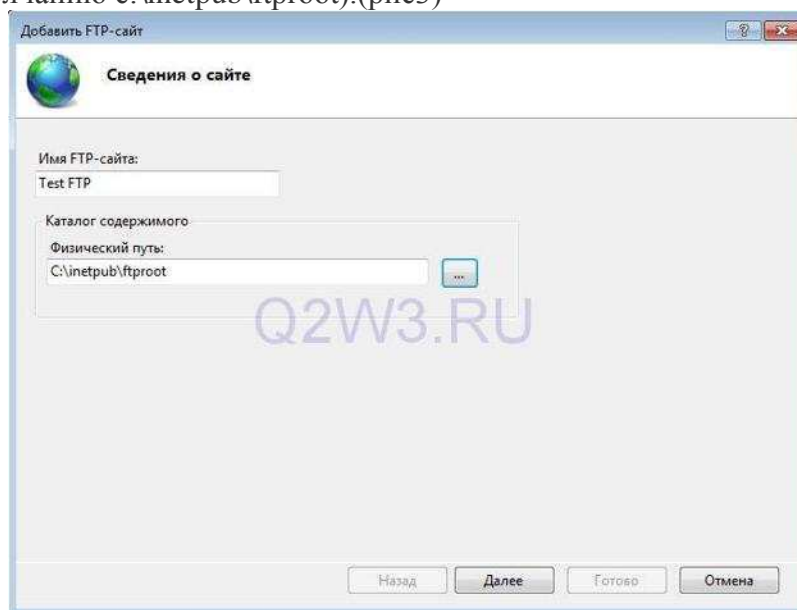


2. Настройка FTP-сервера.

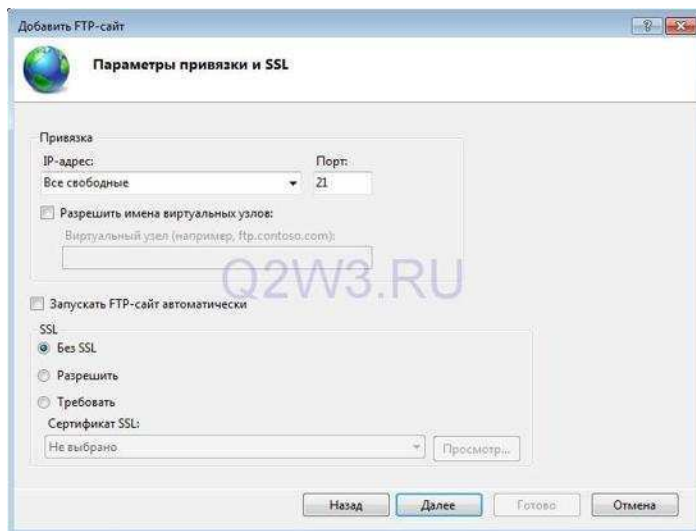
Открываем Панель управления -> Система и безопасность -> Администрирование -> Управление компьютером (можно быстрее: меню Пуск -> правый клик на Компьютер -> в меню выбрать пункт Управление). В открывшемся окне раскрываем группу Службы и приложения и открываем Диспетчер служб IIS. В окне Подключения выбираем папку Сайты, затем в правом окне Действия нажимаем на ссылку Добавить FTP-сайт.(рис2.)



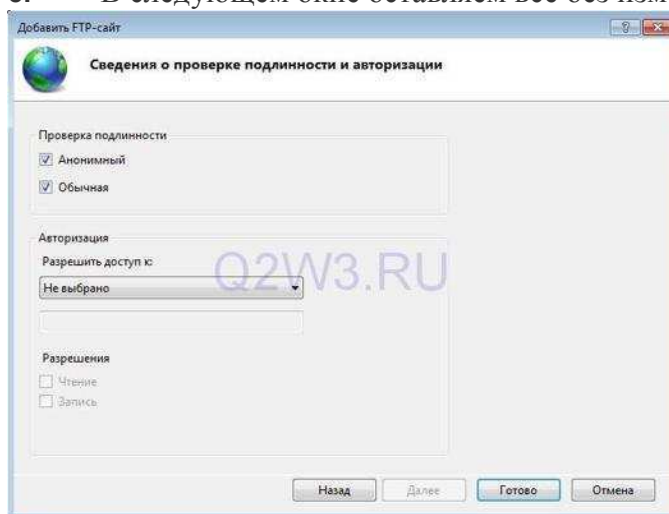
3. В мастере создания ftp-сайта указываем его название и расположение (по умолчанию c:\inetpub\ftproot).(рис3)



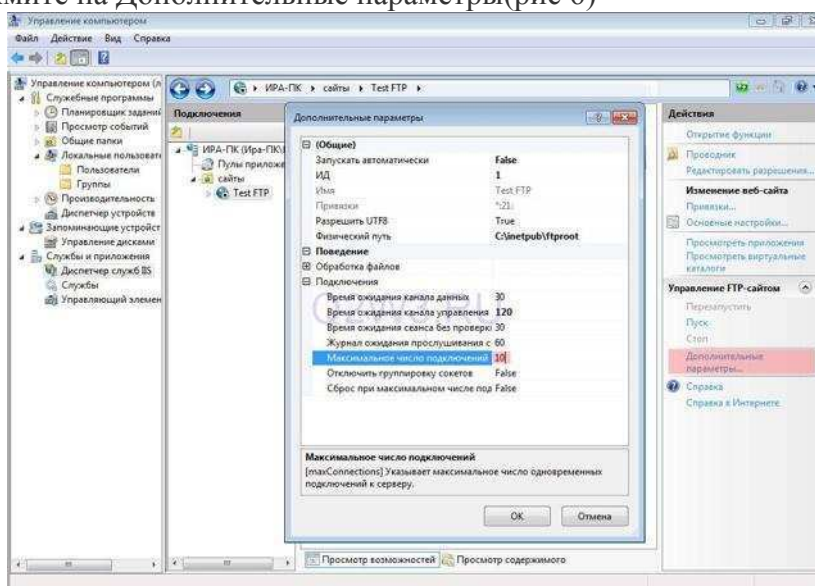
4. Далее указываем параметры привязки и SSL. Раздел привязка оставляю без изменений. Опцию «Запускать ftp-сайт автоматически» отключаю (ftp мне нужен только время от времени). В разделе SSL выставляю опцию «Без SSL».(рис4)



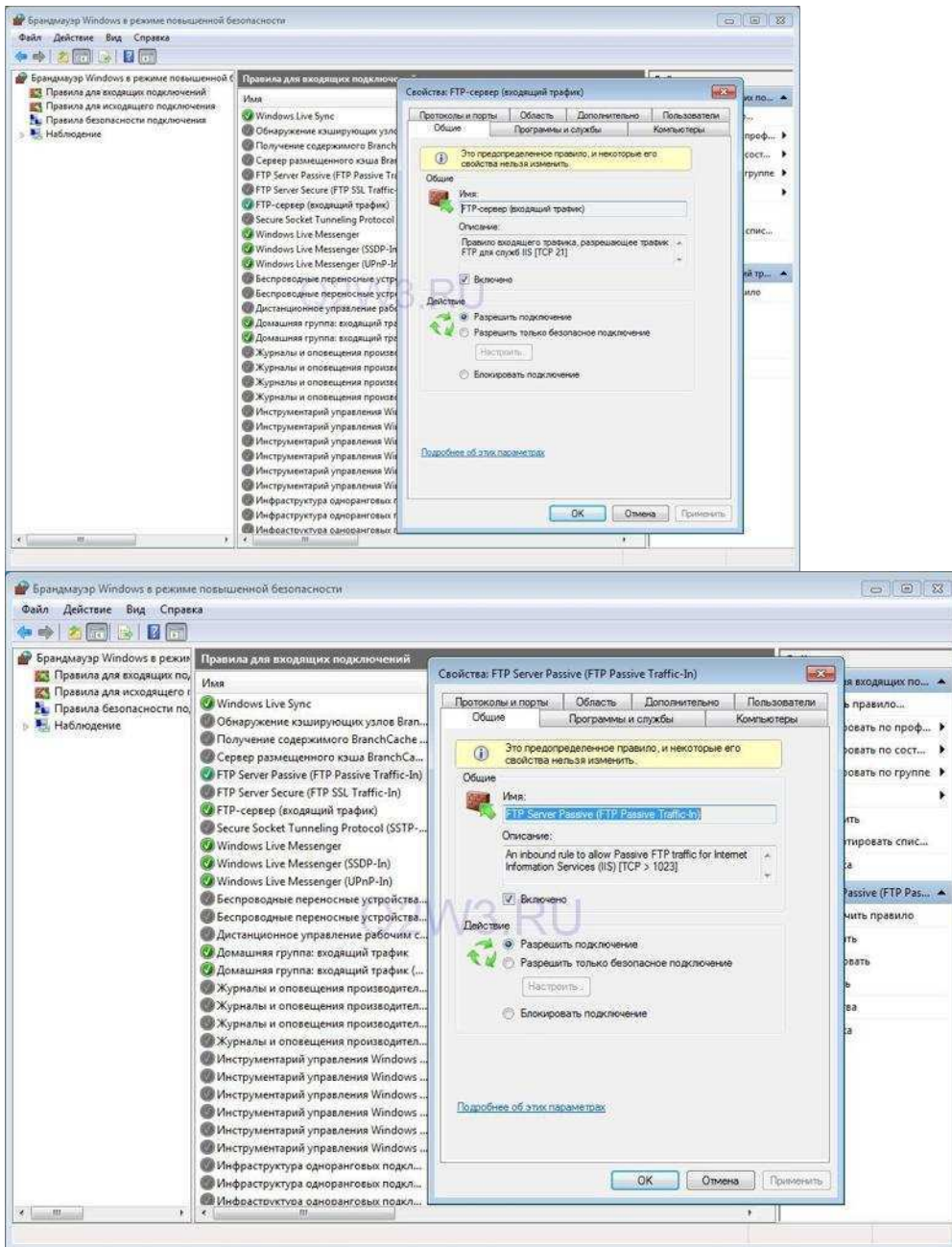
5. В следующем окне оставляем все без изменений и нажимаем Готово.(рис5)



6. Сайт создан. Теперь можно перейти к дополнительным параметрам для тонкой настройки (например ограничить максимальное количество одновременных подключений). Выделите только что созданный сайт, справа в панели Действия нажмите на Дополнительные параметры(рис 6)

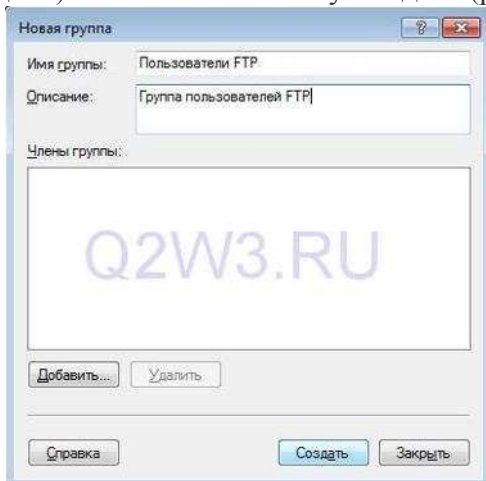


7. Следующий этап — настройка брандмауэра Windows. Откройте Панель управления -> Система и безопасность -> Брандмауэр Windows -> Дополнительные параметры. В разделе «Правила для входящих подключений» находим и активируем «FTP-сервер (входящий трафик)» и «FTP Server Passive (FTP Passive Traffic-In)». Последнее правило позволяет подключаться ftp-клиенту в пассивном режиме.(рис7,8)

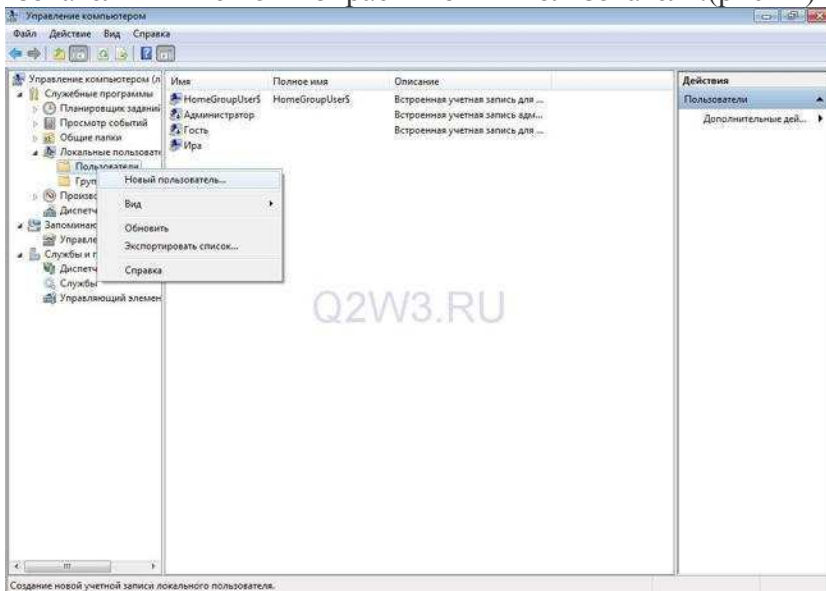


8. В разделе «Правила для исходящего подключения» находим и активируем «FTP Server (FTP Traffic-Out)».(рис9)

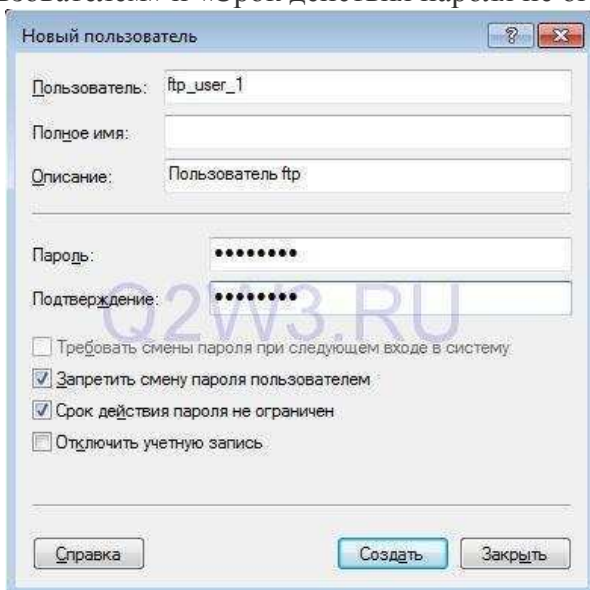
11. Вводим название группы — Пользователи FTP, описание (можно не вводить) и нажимаем кнопку Создать.(рис11)



12. Теперь необходимо создать пользователя. Делаем правый клик на папке Пользователи и в меню выбираем Новый пользователь.(рис 12)

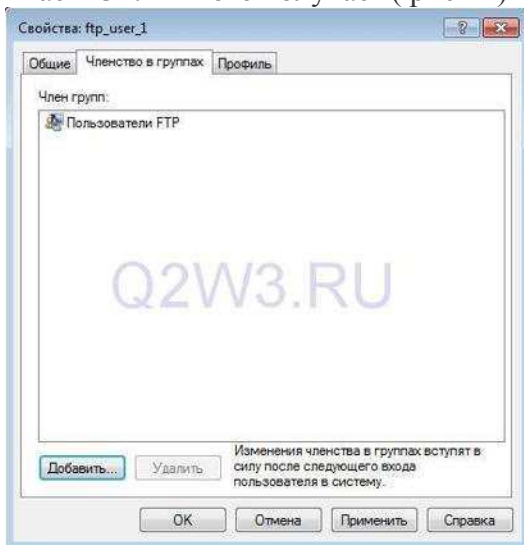


13. Вводим имя пользователя (например ftp_user_1), пароль (не менее 6 символов), выставляем галочки напротив опций «Запретить смену пароля пользователем» и «Срок действия пароля не ограничен».(рис 13)



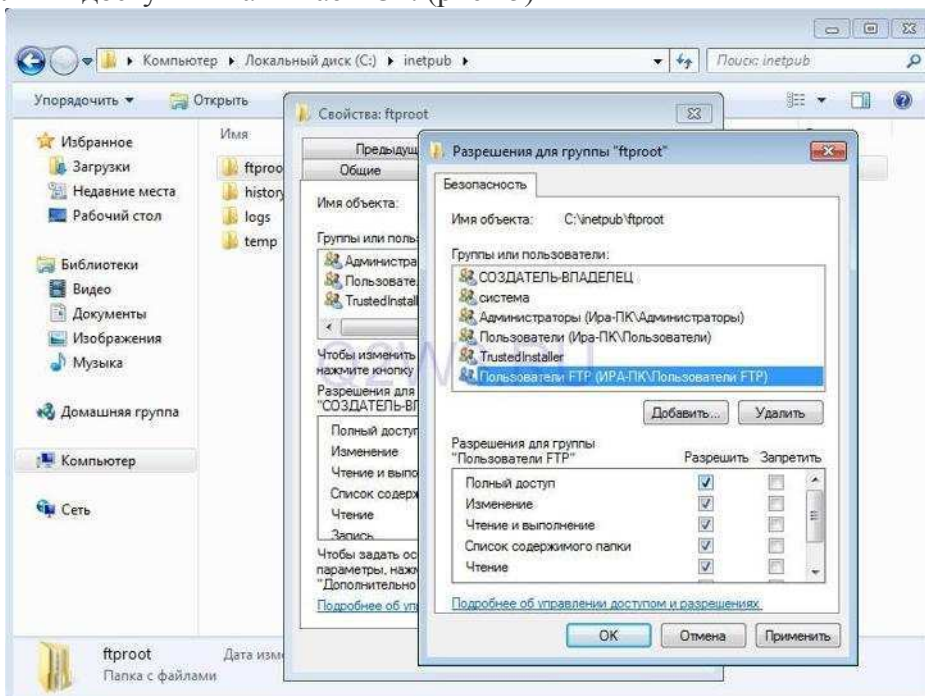
14. Пользователь создан. Теперь необходимо присвоить ему ранее созданную группу Пользователи ftp. Для этого открываем свойства пользователя и переходим на

закладку «Членство в группах». По умолчанию новому пользователю присваивается группа Пользователи, удаляем ее. Нажимаем кнопку Добавить -> Дополнительно -> Поиск. Откроется список групп пользователей. Выбираем группу Пользователи FTP и нажимаем Ок. В итоге получаем(рис 14)

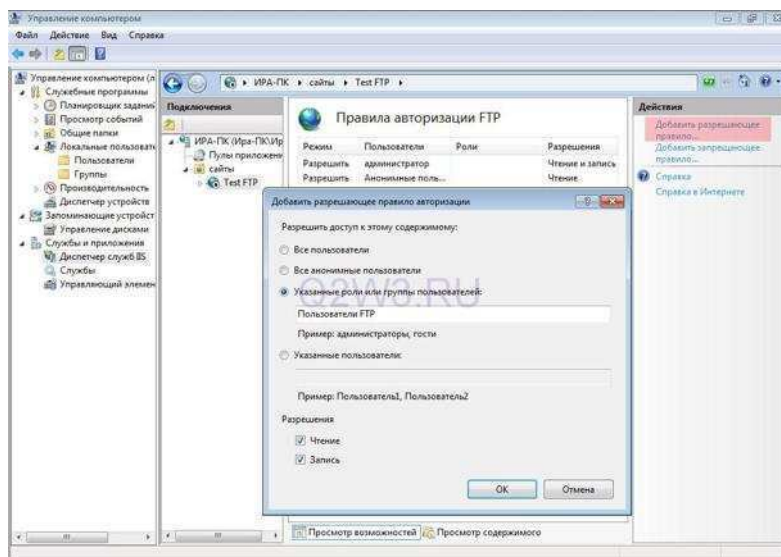


15. Нажимаем Ок и переходим к следующему этапу.

На этапе создания ftp-сайта нам было необходимо выбрать рабочий каталог (с:\inetpub\ftproot). Теперь для группы «Пользователи FTP» необходимо настроить права доступа к этому каталогу. Открываем с:\inetpub в проводнике, открываем свойства папки ftproot, переходим на закладку Безопасность и нажимаем кнопку Изменить. В открывшемся окне нажимаем кнопку Добавить и выбираем группу «Пользователи FTP» (как при создании пользователя). Устанавливаем уровень прав — «Полный доступ» и нажимаем Ок. (рис 15)



16. Последний этап. Вновь открываем Диспетчер служб IIS и выделяем наш ftp-сервер (Test FTP). В панели управления ftp-сайтом выбираем «Правила авторизации FTP». Добавляем разрешающее правило. В открывшемся окне выбираем опцию «Указанные роли или группы пользователей». Внизу в текстовом поле руками прописываем название нашей группы (Пользователи FTP), далее ставим галочки в разделе Разрешения напротив Чтение и Запись и нажимаем Ок. (рис 16)



17. На этом настройка завершена.

В начале мы не выбрали опцию автоматического запуска сервера, поэтому не забываем запустить его вручную (правый клик на названии сайта -> Управление FTP-сайтом -> Пуск).

Как подключиться?

Вариант с использованием проводника Windows. Открываем Компьютер Для анонимного доступа просто вводим в адресную строку адрес сервера (ftp://192.168.10.4). Чтобы войти с именем пользователя и паролем вводим адрес вида: ftp://[имя пользователя]:[пароль]@[адрес ftp-сервера]. Например ftp://ftp_user_1:qwerty@192.168.10.4 — для подключения из локальной сети. Для подключения из Интернет локальный адрес заменяем на внешний или на доменное имя.

Настройка клиента электронной почты

Теоретические сведения

Электронная почта основана на взаимодействии двух программ. Одна из них **сервер**, другая – **клиент**. Они взаимодействуют по определенным правилам, заданным в **протоколах**.

Почтовые серверы получают сообщения от клиентов и пересылают их по цепочке к почтовым серверам адресатов, где эти сообщения накапливаются. При установлении соединения между адресатом и его почтовым сервером происходит автоматическая передача поступивших сообщений на компьютер адресата.

Для работы электронной почты применяются два основных протокола.

1. **POP3** (Post Office Protocol) - протокол приема почтовых сообщений (протокол почтовой службы);
2. **SMTP** (Simple Mail Transfer Protocol) - простой протокол передачи почты.

Иногда для приема почты используется более современный протокол – **IMAP** (Internet Message Access Protocol), который позволяет, в частности, выборочно копировать пришедшие для вас письма с почтового сервера на ваш компьютер. Чтобы использовать этот протокол, необходимо, чтобы он поддерживался как вашим провайдером, так и вашей почтовой программой.

Адрес электронной почты – запись, однозначно определяющая путь доступа к электронному «почтовому ящику» адресата.

Адрес электронной почты выглядит примерно следующим образом:

Имя пользователя@доменное имя

Первая часть адреса включает в себя имя пользователя. Это имя или псевдоним, которые Вы выбираете сами, или которые назначает вам поставщик услуг. Символ @ используется для отделения пользовательского имени от доменного. Доменное имя указывает на имя компьютера вашего поставщика услуг Интернета. Таким образом, понятно, что сочетание вашего пользовательского имени и имени почтового сервера вашего поставщика услуг обеспечивает точное указание того, куда должна быть отправлена почта. Большие и маленькие буквы в почтовом адресе не различаются.

Для работы с электронной почтой используются различные почтовые клиенты, отличающиеся функциями, интерфейсом и т.д. Одной из распространенных программ работы с электронными сообщениями является Outlook Express.

Дополнительные функции клиентов электронной почты предназначены для автоматизации основных операций или для повышения удобства работы со службой. Перечислим самые распространенные из них.

1. *Поддержка множественных идентификационных записей.* Идентификационной записью называется совокупность настроек программы на конкретного пользователя.
2. *Поддержка Адресной книги.* **Адресная книга** – это удобное средство для работы с адресами электронной почты. Это средство управления базой данных, обычно встроенное в почтовую программу, которое позволяет вести учет контактов. **Контактами** называются записи адресной книги, соответствующие регулярным корреспондентам и содержащие данные о людях и их адресах электронной почты.
3. *Функции оповещения.* В качестве сигнала оповещения поступления новой почты может использоваться звуковой или визуальный сигнал (диалоговое окно). Большинство средств оповещения могут сигнализировать о поступлении новой почты запуском заданной программы.
4. *Фильтрация сообщений.* Фильтрацию используют для борьбы со спамом.
5. *Поддержка «черного» и «белого» списков.* Средства фильтрации могут работать с заранее заготовленными списками почтовых адресов. «Черным» называется список адресов электронной почты, сообщения от которых автоматически блокируются и уничтожаются непосредственно на сервере без загрузки на локальный компьютер. «Белый список» используют, чтобы пропускать избранные сообщения в тех случаях, когда почтовый клиент настроен на блокирование всех поступающих сообщений.
6. *Функции автоматической генерации ответа и переадресации.* Автоматическая генерация ответа на поступившее почтовое сообщение позволяет соблюсти этикет электронной почты и оперативно ответить на поступившее сообщение, когда нет возможности ответить обычным способом.

Безопасность электронной почты. Методы борьбы со спамом

С точки зрения безопасности, при работе с электронной почтой выделяют следующие угрозы и уязвимости: утечка конфиденциальной информации; отказ в обслуживании; заражение компьютерным вирусом.

Во избежание утечки конфиденциальной информации необходимо шифровать электронные сообщения. Большинство современных почтовых клиентов делают эти операции автоматически, «прозрачно» (то есть незаметно) как для отправителя, так и для адресата.

Угроза, называемая «отказом в обслуживании», связана с целенаправленным выведением из строя почтового сервера адресата, например в результате переполнения,

поступающими сообщениями. В качестве меры противодействия, во-первых, используют почтовые клиенты, способные анализировать поступающие сообщения на сервере, без загрузки их на компьютер пользователя. Во-вторых, во избежание переполнения «почтового ящика» не следует широко публиковать свой адрес электронной почты. По электронной почте можно получить как «классические» компьютерные вирусы, так и особые «почтовые» вирусы. Классические вирусы распространяются в виде исполнимых файлов, вложенных в сообщения электронной почты. Таким методом могут поражаться любые компьютерные системы, независимо от используемого почтового клиента.

Для срабатывания «почтового вируса» даже не требуется запускать на исполнение файл, полученный в качестве почтового вложения, – достаточно просто его открыть.

спам – это рассылка незатребованной корреспонденции. Спам (наряду с компьютерными вирусами) еще одна неприятная сторона работы с электронной почтой. Самый эффективный путь борьбы со спамом – изменение время от времени адреса своей электронной почты.

Задание.

1. Создать почтовый ящик.
2. Настроить почтовый клиент Outlook Express, который будет работать с вашим почтовым ящиком.
3. Какие преимущества при работе с Outlook Express

Практическое занятие № 12

Настройка точки беспроводного доступа.

Цель работы: Создание простейшей сети Wi-Fi.

Задачи:

Изучить оборудование беспроводных сетей;

Ознакомиться с настройками беспроводной сети;

Отработать практические навыки создания и настройки беспроводной сети.

Оборудование: Ноутбук, точка доступа WiFi.

Теоретические сведения.

В современном мире все большее применение находят беспроводные сети Wi-Fi, позволяющие давать клиентам доступ к ресурсам сетей, например к **Internet**, с ноутбука или персонального компьютера, используя в качестве среды передачи данных радиоканал, что не требует наличия специальных проводных соединений клиентов с сетью, обеспечивая, таким образом, их мобильность.

Преимущества Wi-Fi

- **Отсутствие проводов.** Передача данных в сети осуществляется по радиоканалу. Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например на выставках, залах для совещаний.

- **Мобильность, как рабочих мест, так и самого офиса.**

Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется/демонтируется, при переезде в другое помещение Вы можете даже забрать свою сеть с собой.

Недостатки Wi-Fi

- Относительно высокая стоимость оборудования

- Небольшая дальность действия – 50-100 метров

- Велика опасность несанкционированного подключения к сети сторонних пользователей

В предлагаемой работе *мы освоим* создание простейшей сети Wi-Fi на примере подключения ноутбуков к точке доступа Wi-Fi с использованием статической и динамической IP-адресации.

Задание 1. Настройка сети со статическим адресом компьютера клиента.

Настройка сети заключается в установке **протоколов ноутбука клиента**, которые необходимы для его работы, а так же включение и настройка **ДНСП-сервера**, который находится в точке.

Запомните. **Протокол** – это специальная программа, посредством которой компьютеры сети обмениваются между собой данными по специальным правилам.

В нашей сети рабочим протоколом будет протокол **ТСР/IP**. Чтобы компьютеры могли обмениваться между собой данными этот протокол должен быть установлен на всех компьютерах, которые находятся в сети.

На **ноутбуке сервере** протокол ТСР/IP уже установлен, нам осталось установить и настроить этот протокол на **ноутбуке клиенте**. *Помните*, что все пункты настройки должны выполняться в той последовательности, в которой они указаны. Не нарушайте последовательность настройки.

На ноутбуке выполните следующие действия:

1. Щелкните правой клавишей мыши на значке «**Мое сетевое окружение**», выберите в меню «**Свойства**». Откроется список сетевых подключений (рис.1.).

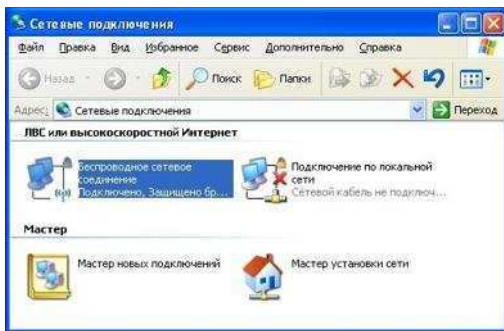


Рис.1.

2. Выберите в списке «Беспроводное сетевое соединение», щелкните по нему правой клавишей мыши и выберите пункт «Свойства». Откроется окно свойств соединения (рис.2.).

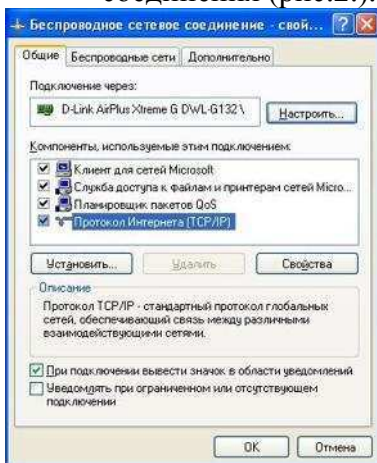


Рис.2.

3. В появившемся окне выберите «Протокол Интернета (TCP/IP)», нажмите «Свойства». Откроется окно настроек протокола (рис.3.). Активируйте флажок «Использовать следующий IP-адрес». Введите в поля IP-адрес и Маска подсети адреса установок, которые изображены на рис.3.

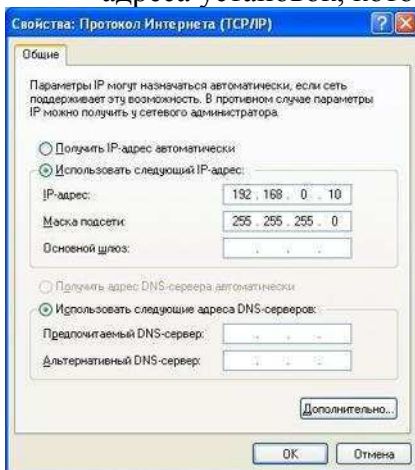


Рис.3.

Здесь

192.168.0.10 – это IP-адрес компьютера в сети.

255.255.255.0 – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

4. После ввода настроек, нажмите «ОК», окно «Свойства: Протокол Интернета (TCP/IP)» закроется. В окне «Беспроводное сетевое соединение» (рис.2.) нажмите «ОК».

Мы настроили ноутбук клиент для работы с беспроводной сетью. Для ноутбука прописан статический IP-адрес, это означает, что мы присвоили ноутбуку выделенный,

постоянный IP-адрес и прочие настройки, которые можно менять и назначать только вручную. Статический IP-адрес нам необходим для того, чтобы подключиться к точке доступа Wi-Fi и чтобы другие компьютеры в сети могли с ним связываться.

Для того чтобы начала функционировать сеть **Wi-Fi** необходимо настроить точку доступа.

Задание 2 Настройка точки доступа Wi-Fi и DHCP-сервера.

1. Загрузите обозреватель **Internet Explorer**. Введите в его адресной строке адрес: <http://192.168.0.50/> .Это IP-адрес **точки доступа Wi-Fi**. По этому адресу расположена система ее конфигурации. Вход в систему конфигурации защищен логином и паролем и на экране появится окно для ввода этих данных. Введите **Пользователь – admin, Пароль – 12345678** и нажмите кнопку «ОК».

Откроется главная страница систему конфигурации точки доступа Wi-Fi.

2. Щелкните по **Advanced**. Откроется страница расширенных настроек точки доступа.
3. Щелкните по **DHCP Server**. Откроется страница для изменения настроек **DHCP-сервера**.

Сохраните сделанные настройки. Точка доступа **Wi-Fi** уйдет на перезагрузку, которая занимает примерно полминуты.

Задание 3 Проверка работы беспроводной сети.

Запомните. Статическая IP-адресация имеет следующие недостатки:

1. Для того, чтобы узнать все настройки сети, необходимо обратиться к администратору сети, который должен индивидуально выделить для каждого клиента свой уникальный IP-адрес. Это неудобно как для клиента, так и для администратора.
2. При подключении к какой-либо другой беспроводной сети, настройки компьютера клиента приходится снова изменять под новую сеть, узнавая их у администратора.
3. Если случайно ваши настройки совпадут с настройками другого клиента, вы не сможете подключиться к сети.

Всех указанных недостатков лишена **динамическая IP-адресация**.

Задание 4 Настройка сети с динамическим адресом компьютера клиента.

Динамическая IP-адресация осуществляется с помощью **DHCP-сервера**, который находится в точке доступа. Разберемся что это такое.

Запомните. **DHCP-сервер** использует **DHCP** протокол (**англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла**) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети **TCP/IP**. Для этого компьютер, подключаемый к сети, обращается к серверу, **DHCP**, который на время проведения сеанса работы с сетью ему выдает **динамический IP-адрес**. Это позволяет избежать ручной настройки компьютеров сети, уменьшает количество ошибок и позволяет клиентам быстро подключаться к сети не тратя время на настройку протоколов связи вручную.

Задание 5 Настройка ноутбука на динамическую IP-адресацию.

1. Вернитесь к началу лабораторной работы, где вы осуществляли настройку сети ноутбука. (Раздел «**Настройка сети**»).
2. Повторите шаги 1-3, только на 3-м шаге, где вы вводили статический IP-адрес активируйте флажок «**Получить IP-адрес автоматически**». Это опция и включает динамическую IP-адресацию.
3. Нажмите «**ОК**», окно «**Свойства: Протокол Интернета (TCP/IP)**» закроется. В окне «**Беспроводное сетевое соединение**» нажмите «**ОК**».

Динамическая IP-адресация на ноутбуке настроена!

Задание 6 Проверка динамической IP-адресации.

Для того, чтобы убедиться в том, что сетевые настройки были динамически присвоены, сделайте следующее:

1. Откройте «Пуск / Стандартные / Командная строка». Появится строка для ввода команд операционной системы.
2. Введите в строке команду:
`ipconfig`

Если указанный командой IP-адрес компьютера находится в диапазоне 192.168.0.51 – 192.168.0.200, значит динамическая IP-адресация работает нормально.

Практическое занятие № 13

Настройка политик доступа и настройка DMZ.

Теоретические сведения

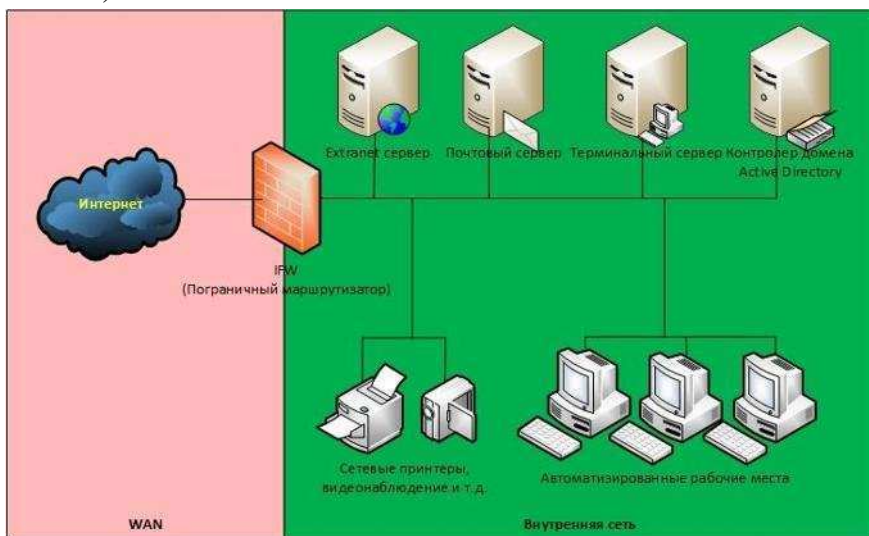
Данная статья содержит обзор *пяти* вариантов решения задачи организации доступа к сервисам корпоративной сети из Интернет. В рамках обзора приводится анализ вариантов на предмет безопасности и реализуемости, что поможет разобраться в сути вопроса, освежить и систематизировать свои знания как начинающим специалистам, так и более опытным. Материалы статьи можно использовать для обоснования Ваших проектных решений.

При рассмотрении вариантов в качестве примера возьмем сеть, в которой требуется опубликовать:

1. Корпоративный почтовый сервер (Web-mail).
2. Корпоративный терминальный сервер (RDP).
3. Extranet сервис для контрагентов (Web-API).

Вариант 1. Плоская сеть

В данном варианте все узлы корпоративной сети содержатся в одной, общей для всех сети («Внутренняя сеть»), в рамках которой коммуникации между ними не ограничиваются. Сеть подключена к Интернет через пограничный маршрутизатор/межсетевой экран (далее — *IFW*).



Вариант 1. Плоская сеть

В данном варианте все узлы корпоративной сети содержатся в одной, общей для всех сети («Внутренняя сеть»), в рамках которой коммуникации между ними не ограничиваются. Сеть подключена к Интернет через пограничный маршрутизатор/межсетевой экран (далее — *IFW*).

Доступ узлов в Интернет осуществляется через NAT, а доступ к сервисам из Интернет через [Port forwarding](#).

Плюсы варианта:

1. Минимальные требования к функционалу *IFW* (можно сделать практически на любом, даже домашнем роутере).

2. Минимальные требования к знаниям специалиста, осуществляющего реализацию варианта.

Минусы варианта:

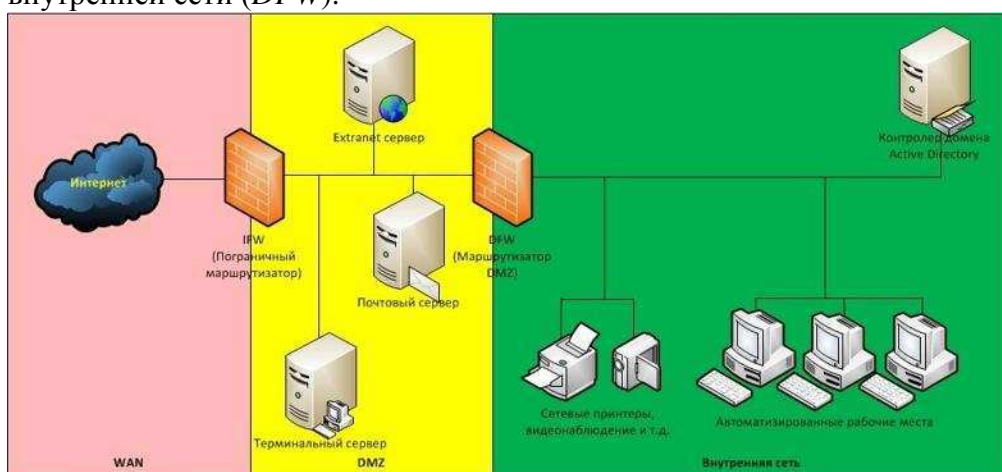
1. Минимальный уровень безопасности. В случае взлома, при котором Нарушитель получит контроль над одним из опубликованных в Интернете серверов, ему для дальнейшей атаки становятся доступны все остальные узлы и каналы связи корпоративной сети.

Аналогия с реальной жизнью

Подобную сеть можно сравнить с компанией, где персонал и клиенты находятся в одной общей комнате (open space)

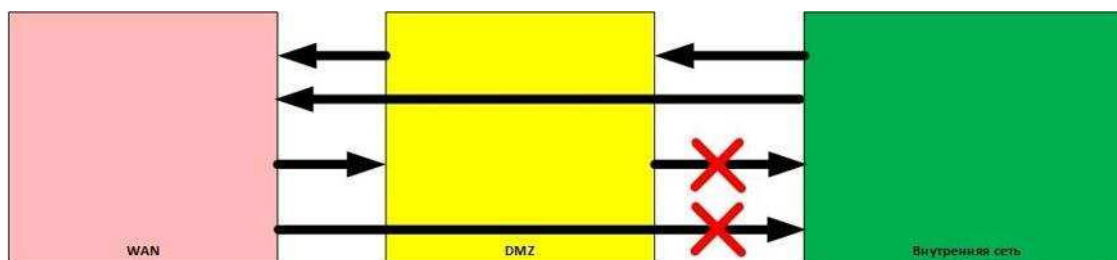
Вариант 2. DMZ

Для устранения указанного ранее недостатка узлы сети, доступные из Интернет, помещают в специально выделенный сегмент – демилитаризованную зону (DMZ). DMZ организуется с помощью межсетевых экранов, отделяющих ее от Интернет (IFW) и от внутренней сети (DFW).



При этом правила фильтрации межсетевых экранов выглядят следующим образом:

1. Из внутренней сети можно инициировать соединения в DMZ и в WAN (Wide Area Network).
2. Из DMZ можно инициировать соединения в WAN.
3. Из WAN можно инициировать соединения в DMZ.
4. Инициация соединений из WAN и DMZ ко внутренней сети запрещена.



Плюсы варианта:

1. Повышенная защищённость сети от взломов отдельных сервисов. Даже если один из серверов будет взломан, Нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т.д.).

Минусы варианта:

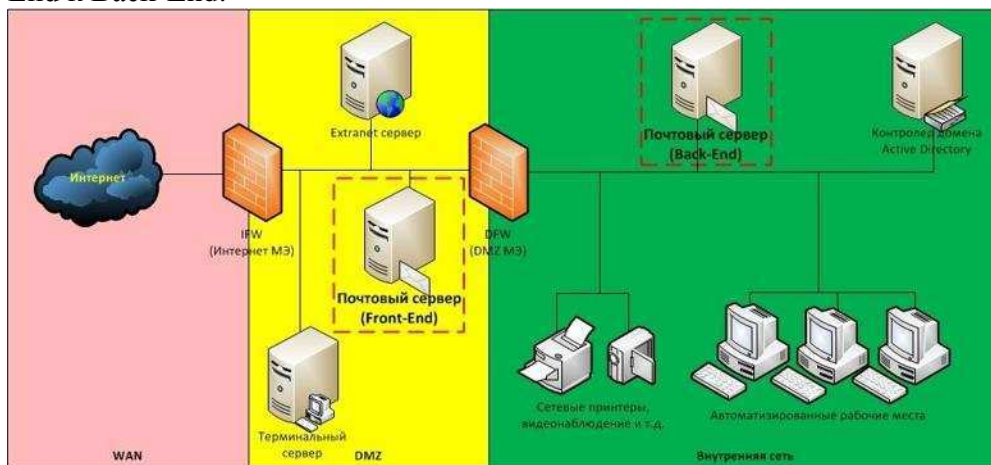
1. Сам по себе вынос серверов в DMZ не повышает их защищённость.
2. Необходим дополнительный МЭ для отделения DMZ от внутренней сети.

Аналогия с реальной жизнью

Данный вариант архитектуры сети похож на организацию рабочей и клиентской зон в компании, где клиенты могут находиться только в клиентской зоне, а персонал может быть как в клиентской, так и в рабочих зонах. DMZ сегмент — это как раз и есть аналог клиентской зоны.

Вариант 3. Разделение сервисов на Front-End и Back-End

Как уже отмечалось ранее, размещение сервера в DMZ никоим образом не улучшает безопасность самого сервиса. Одним из вариантов исправления ситуации является разделение функционала сервиса на две части: [Front-End и Back-End](#). При этом каждая часть располагается на отдельном сервере, между которыми организуется сетевое взаимодействие. Сервера Front-End, реализующие функционал взаимодействия с клиентами, находящимися в Интернет, размещают в DMZ, а сервера Back-End, реализующие остальной функционал, оставляют во внутренней сети. Для взаимодействия между ними на DFW создают правила, разрешающие инициацию подключений от Front-End к Back-End.



В качестве примера рассмотрим корпоративный почтовый сервис, обслуживающий клиентов как изнутри сети, так и из Интернет. Клиенты изнутри используют POP3/SMTP, а клиенты из Интернет работают через Web-интерфейс. Обычно на этапе внедрения компании выбирают наиболее простой способ развертывания сервиса и ставят все его компоненты на один сервер. Затем, по мере осознания необходимости обеспечения информационной безопасности, функционал сервиса разделяют на части, и та часть, что отвечает за обслуживание клиентов из Интернет (Front-End), выносится на отдельный сервер, который по сети взаимодействует с сервером, реализующим оставшийся функционал (Back-End). При этом Front-End размещают в DMZ, а Back-End остается во внутреннем сегменте. Для связи между Front-End и Back-End на DFW создают правило, разрешающее инициацию соединений от Front-End к Back-End.

Плюсы варианта:

1. В общем случае атаки, направленные против защищаемого сервиса, могут «споткнуться» об Front-End, что позволит нейтрализовать или существенно снизить возможный ущерб. Например, атаки типа [TCP SYN Flood](#) или [slow http read](#), направленные на сервис, приведут к тому, что Front-End сервер может оказаться недоступен, в то время как Back-End будет продолжать нормально функционировать и обслуживать пользователей.
2. В общем случае на Back-End сервере может не быть доступа в Интернет, что в случае его взлома (например, локально запущенным вредоносным кодом) затруднит удаленное управление им из Интернет.
3. Front-End хорошо подходит для размещения на нем межсетевого экрана уровня приложений (например, Web application firewall) или системы предотвращения вторжений (IPS, например snort).

Минусы варианта:

1. Для связи между Front-End и Back-End на *DFW* создается правило, разрешающее инициацию соединения из DMZ во внутреннюю сеть, что порождает угрозы, связанные с использованием данного правила со стороны других узлов в DMZ (например, за счет реализации атак IP spoofing, ARP poisoning и т. д.)
2. Не все сервисы могут быть разделены на Front-End и Back-End.
3. В компании должны быть реализованы бизнес-процессы актуализации правил межсетевого экранирования.
4. В компании должны быть реализованы механизмы защиты от атак со стороны Нарушителей, получивших доступ к серверу в DMZ.

Примечания

1. В реальной жизни даже без разделения серверов на Front-End и Back-End серверам из DMZ очень часто необходимо обращаться к серверам, находящимся во внутренней сети, поэтому указанные минусы данного варианта будут также справедливы и для предыдущего рассмотренного варианта.
2. Если рассматривать защиту приложений, работающих через Web-интерфейс, то даже если сервер не поддерживает разнесение функций на Front-End и Back-End, применение http reverse проху сервера (например, nginx) в качестве Front-End позволит минимизировать риски, связанные с атаками на отказ в обслуживании. Например, атаки типа SYN flood могут сделать http reverse проху недоступным, в то время как Back-End будет продолжать работать.

Аналогия с реальной жизнью Данный вариант по сути похож на организацию труда, при которой для высоко загруженных работников используют помощников — секретарей. Тогда Back-End будет аналогом загруженного работника, а Front-End аналогом секретаря.

Вариант 4. Защищенный DMZ

DMZ это часть сети, доступная из Internet, и, как следствие, подверженная максимальному риску компрометации узлов. Дизайн DMZ и применяемые в ней подходы должны обеспечивать максимальную живучесть в условиях, когда Нарушитель получил контроль над одним из узлов в DMZ. В качестве возможных атак рассмотрим атаки, которым подвержены практически все информационные системы, работающие с настройками по умолчанию:

1. CAM-table overflow
2. ARP poisoning
3. Rogue DHCP Server
4. DHCP starvation
5. VLAN hopping
6. MAC flood
7. UDP flood
8. TCP SYN flood
9. TCP session hijacking
10. TCP reset
11. Атаки на Web-приложения
12. Атаки на обход средств аутентификации и авторизацию от имени легитимного пользователя (например, подбор паролей, PSK и т.д.)
13. Атаки на уязвимости в сетевых службах, например:
 - Атака на Web-сервер — slow reading
 - DNS cache poisoning

Большая часть указанных атак (по крайней мере с 1 по 10) базируется на уязвимостях архитектуры современных Ethernet/IP сетей, заключающихся в возможности Нарушителя подделывать в сетевых пакетах MAC и IP адреса. Эксплуатацию данных уязвимостей иногда выделяют в отдельные виды атак:

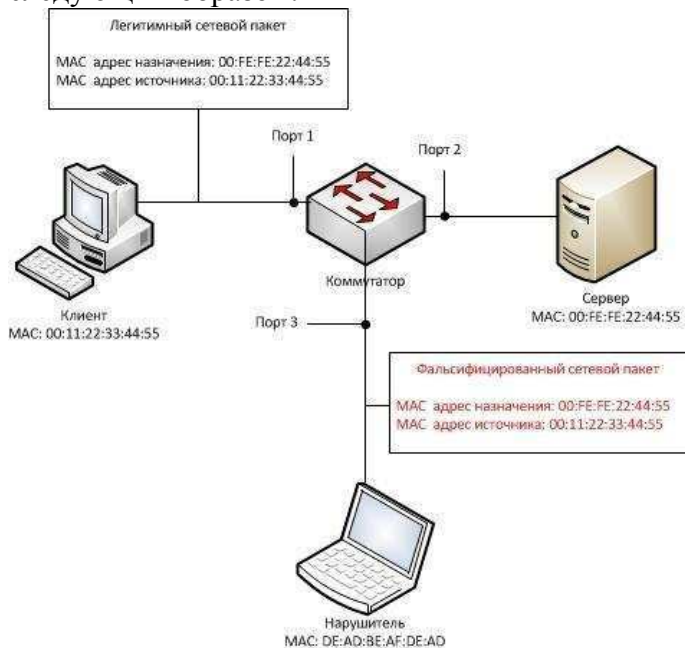
1. MAC spoofing;
2. IP spoofing.

Поэтому построение системы защиты DMZ начнем с рассмотрения способов защиты от IP spoofing и MAC spoofing.

Примечание Приведенные ниже способы защиты от данных атак не являются единственно возможными. Существуют и другие способы.

Защита от MAC spoofing

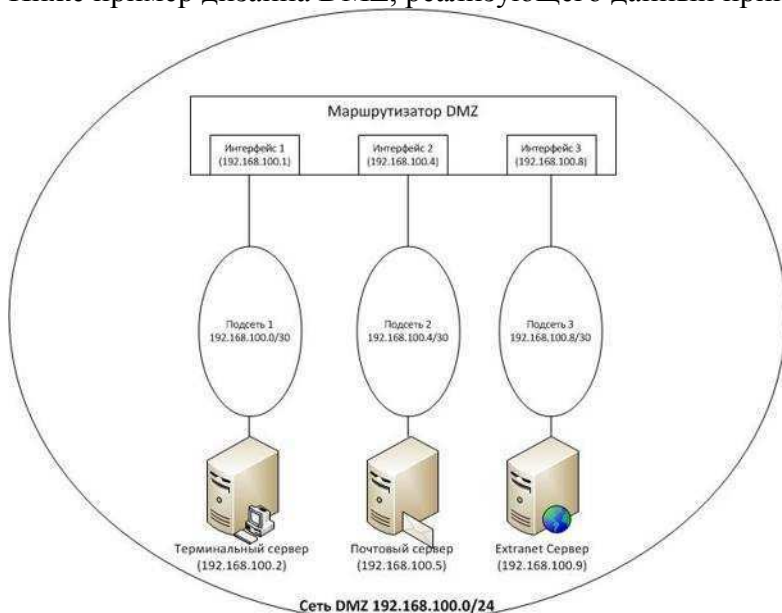
Схематически атаки, связанные с подменой MAC адреса, можно проиллюстрировать следующим образом:



Нейтрализацией данной атаки может являться фильтрация MAC-адресов на портах коммутатора. Например, трафик по порту 3 должен проходить только в случае, если в адресе источника или в адресе назначения указан MAC-адрес DE:AD:BE:AF:DE:AD или широковещательный адрес (в некоторых случаях).

Защита от IP spoofing

Схема атаки IP spoofing похожа на предыдущую, за исключением того, что Нарушитель подделывает не MAC, а IP-адрес. Защита от IP spoofing может быть реализована путем разделения IP-сети DMZ на более мелкие IP-подсети и дальнейшей фильтрацией трафика на интерфейсах маршрутизатора по аналогии с рассмотренной ранее MAC-фильтрацией. Ниже пример дизайна DMZ, реализующего данный принцип:



В DMZ располагается 3 узла:

- Терминальный сервер (192.168.100.2)

- Почтовый сервер (192.168.100.5)
- Extranet сервер (192.168.100.9)

Для DMZ выделена IP-сеть 192.168.100.0/24, в данной сети выделяются 3 IP-подсети (по числу серверов):

Подсеть 1 — 192.168.100.0/30 для терминального сервера (192.168.100.2)

Подсеть 2 — 192.168.100.4/30 для почтового сервера (192.168.100.5)

Подсеть 3 — 192.168.100.8/30 для почтового сервера (192.168.100.9)

На практике разделение сети на подобные подсети реализуют с помощью технологии VLAN. Однако, ее применение порождает риски, защиту от которых мы сейчас рассмотрим.

Защита от VLAN hopping

Для защиты от [этой атаки](#) на коммутаторе отключают возможность автоматического согласования типов ([trunk / access](#)) портов, а сами типы администратор назначает вручную. Кроме того, организационными мерами запрещается использование так называемого [native VLAN](#).

Защита от атак, связанных с DHCP

Не смотря на то, что DHCP предназначен для автоматизации конфигурирования IP-адресов рабочих станций, в некоторых компаниях встречаются случаи, когда через DHCP выдаются IP-адреса для серверов, но это довольно плохая практика. Поэтому для защиты от [Rogue DHCP Server](#), [DHCP starvation](#) рекомендуется полный отказ от DHCP в DMZ.

Защита от атак MAC flood

Для защиты от MAC flood проводят настройку на портах коммутатора на предмет ограничения предельной интенсивности широковещательного трафика (поскольку обычно при данных атаках генерируется широковещательный трафик (broadcast)). Атаки, связанные с использованием конкретных (unicast) сетевых адресов, будут заблокированы MAC фильтрацией, которую мы рассмотрели ранее.

Защита от атак UDP flood

Защита от данного типа атак производится аналогично защите от MAC flood, за исключением того, что фильтрация осуществляется на уровне IP (L3).

Защита от атак TCP SYN flood

Для защиты от данной атаки возможны варианты:

1. Защита на узле сети с помощью технологии [TCP SYN Cookie](#).
2. Защита на уровне межсетевого экрана (при условии разделения DMZ на подсети) путем ограничения интенсивности трафика, содержащего запросы TCP SYN.

Защита от атак на сетевые службы и Web-приложения

Универсального решения данной проблемы нет, но устоявшейся практикой является внедрение процессов управления уязвимостями ПО (выявление, установка патчей и т.д., например, [так](#)), а также использование систем обнаружения и предотвращения вторжений (IDS/IPS).

Защита от атак на обход средств аутентификации

Как и для предыдущего случая универсального решения данной проблемы нет.

Обычно в случае большого числа неудачных попыток авторизации учетные записи, для избежания подборов аутентификационных данных (например, пароля) блокируют. Но подобный подход довольно спорный, и вот почему.

Во-первых, Нарушитель может проводить подбор аутентификационной информации с интенсивностью, не приводящей к блокировке учетных записей (встречаются случаи, когда пароль подбирался в течении нескольких месяцев с интервалом между попытками в несколько десятков минут).

Во-вторых, данную особенность можно использовать для атак типа отказ в обслуживании, при которых Нарушитель будет умышленно проводить большое количество попыток авторизации для того, чтобы заблокировать учетные записи.

Наиболее эффективным вариантом от атак данного класса будет использование систем

IDS/IPS, которые при обнаружении попыток подбора паролей будут блокировать не учетную запись, а источник, откуда данный подбор происходит (например, блокировать IP-адрес Нарушителя).

Итоговый перечень защитных мер по данному варианту:

1. DMZ разделяется на IP-подсети из расчета отдельная подсеть для каждого узла.
2. IP адреса назначаются вручную администраторами. DHCP не используется.
3. На сетевых интерфейсах, к которым подключены узлы DMZ, активируется MAC и IP фильтрация, ограничения по интенсивности широковещательного трафика и трафика, содержащего TCP SYN запросы.
4. На коммутаторах отключается автоматическое согласование типов портов, запрещается использование native VLAN.
5. На узлах DMZ и серверах внутренней сети, к которым данные узлы подключаются, настраивается TCP SYN Cookie.
6. В отношении узлов DMZ (и желательно остальной сети) внедряется управление уязвимостями ПО.
7. В DMZ-сегменте внедряются системы обнаружения и предотвращения вторжений IDS/IPS.

Плюсы варианта:

1. Высокая степень безопасности.

Минусы варианта:

1. Повышенные требования к функциональным возможностям оборудования.
2. Трудозатраты во внедрении и поддержке.

Аналогия с реальной жизнью

Если ранее DMZ мы сравнили с клиентской зоной, оснащенной диванчиками и пуфиками, то защищенный DMZ будет больше похож на бронированную кассу.

Вариант 5. Back connect

Рассмотренные в предыдущем варианте меры защиты были основаны на том, что в сети присутствовало устройство (коммутатор / маршрутизатор / межсетевой экран), способное их реализовывать. Но на практике, например, при использовании виртуальной инфраструктуры (виртуальные коммутаторы зачастую имеют очень ограниченные возможности), подобного устройства может и не быть.

В этих условиях Нарушителю становятся доступны многие из рассмотренных ранее атак, наиболее опасными из которых будут:

- атаки, позволяющие перехватывать и модифицировать трафик (ARP Poisoning, CAM table overflow + TCP session hijacking и др.);
- атаки, связанные с эксплуатацией уязвимостей серверов внутренней сети, к которым можно инициировать подключения из DMZ (что возможно путем обхода правил фильтрации *DFW* за счет IP и MAC spoofing).

Следующей немаловажной особенностью, которую мы ранее не рассматривали, но которая не перестает быть от этого менее важной, это то, что автоматизированные рабочие места (АРМ) пользователей тоже могут быть источником (например, при заражении вирусами или троянами) вредоносного воздействия на сервера.

Таким образом, перед нами встает задача защитить сервера внутренней сети от атак Нарушителя как из DMZ, так и из внутренней сети (заражение АРМа трояном можно интерпретировать как действия Нарушителя из внутренней сети).

Предлагаемый далее подход направлен на уменьшение числа каналов, через которые Нарушитель может атаковать сервера, а таких канала как минимум два. Первый это правило на *DFW*, разрешающее доступ к серверу внутренней сети из DMZ (пусть даже и с

ограничением по IP-адресам), а второй — это открытый на сервере сетевой порт, по которому ожидаются запросы на подключение.

Закрывать указанные каналы можно, если сервер внутренней сети будет сам строить соединения до сервера в DMZ и будет делать это с помощью криптографически защищенных сетевых протоколов. Тогда не будет ни открытого порта, ни правила на *DFW*.

Но проблема в том, что обычные серверные службы не умеют работать подобным образом, и для реализации указанного подхода необходимо применять сетевое туннелирование, реализованное, например, с помощью SSH или VPN, а уже в рамках туннелей разрешать подключения от сервера в DMZ к серверу внутренней сети.

Общая схема работы данного варианта выглядит следующим образом:

1. На сервер в DMZ устанавливается SSH/VPN сервер, а на сервер во внутренней сети устанавливается SSH/VPN клиент.
2. Сервер внутренней сети инициирует построение сетевого туннеля до сервера в DMZ. Туннель строится с взаимной аутентификацией клиента и сервера.
3. Сервер из DMZ в рамках построенного туннеля инициирует соединение до сервера во внутренней сети, по которому передаются защищаемые данные.
4. На сервере внутренней сети настраивается локальный межсетевой экран, фильтрующий трафик, проходящий по туннелю.



Использование данного варианта на практике показало, что сетевые туннели удобно строить с помощью [OpenVPN](#), поскольку он обладает следующими важными свойствами:

- Кроссплатформенность. Можно организовывать связь на серверах с разными операционными системами.
- Возможность построения туннелей с взаимной аутентификацией клиента и сервера.
- Возможность использования [сертифицированной криптографии](#).

На первый взгляд может показаться, что данная схема излишне усложнена и что, раз на сервере внутренней сети все равно нужно устанавливать локальный межсетевой экран, то проще сделать, чтобы сервер из DMZ, как обычно, сам подключался к серверу внутренней сети, но делал это по зашифрованному соединению. Действительно, данный вариант закрывает много проблем, но он не сможет обеспечить главного — защиту от атак на уязвимости сервера внутренней сети, совершаемых за счет обхода межсетевого экрана с помощью IP и MAC spoofing.

Плюсы варианта:

1. Архитектурное уменьшение количества векторов атак на защищаемый сервер внутренней сети.
2. Обеспечение безопасности в условиях отсутствия фильтрации сетевого трафика.
3. Защита данных, передаваемых по сети, от несанкционированного просмотра и изменения.
4. Возможность избирательного повышения уровня безопасности сервисов.
5. Возможность реализации двухконтурной системы защиты, где первый контур обеспечивается с помощью межсетевого экранирования, а второй организуется на базе данного варианта.

Минусы варианта:

1. Внедрение и сопровождение данного варианта защиты требует дополнительных трудовых затрат.
2. Несовместимость с сетевыми системами обнаружения и предотвращения вторжений (IDS/IPS).
3. Дополнительная вычислительная нагрузка на сервера.

Аналогия с реальной жизнью

Основной смысл данного варианта в том, что доверенное лицо устанавливает связь с не доверенным, что похоже на ситуацию, когда при выдаче кредитов Банки сами перезванивают потенциальному заемщику с целью проверки данных.

Задание.

- 1) Ознакомиться с данным материалом.
- 2) Какой лучше, или хуже из 5 вариантов организации доступа к сервисам корпоративной сети из Интернет.? Попробуйте обосновать. В каком случае удобно использовать тот или иной вариант.

Практическое занятие № 14

Анализ уязвимостей сетевых систем.

Одними из главных элементов информационной безопасности сетевой инфраструктуры являются операционные системы компьютеров, так как в них аккумулируется подавляющая часть используемых механизмов защиты: средства разграничения доступа к ресурсам, аутентификация пользователей, аудит событий и др. От эффективности защиты операционных систем напрямую зависит уровень безопасности сетевой инфраструктуры организации в целом.

Принципы работы систем анализа защищенности

Для понимания принципов работы систем анализа защищенности необходимо обозначить некоторые термины и определения. Ключевое понятие данного занятия – это "уязвимость". Под уязвимостью защиты ОС понимается такое ее свойство (недостаток), которое может быть использовано злоумышленником для осуществления несанкционированного доступа (НСД) к информации. Системы анализа защищенности способны обнаруживать уязвимости в сетевой инфраструктуре, анализировать и выдавать рекомендации по их устранению, а также создавать различного рода отчеты. К типичным уязвимостям можно отнести:

- отсутствие обновлений системы безопасности ОС;
- неправильные настройки систем безопасности ОС;
- несоответствующие пароли;
- восприимчивость к проникновению из внешних систем;
- программные закладки;
- неправильные настройки системного и прикладного ПО, установленного на ОС.

Большинство систем анализа защищенности (XSpider, Internet Scanner, LanGuard, Nessus) обнаруживают уязвимости не только в операционных системах, но и в наиболее распространенном прикладном ПО. Существуют два основных подхода, при помощи которых системы анализа защищенности обнаруживают уязвимости: сканирование и зондирование. Из-за первого подхода системы анализа защищенности еще называют "сканерами безопасности" или просто "сканерами".

При сканировании система анализа защищенности пытается определить наличие уязвимости по косвенным признакам, т.е. без фактического подтверждения ее наличия – это пассивный анализ. Данный подход является наиболее быстрым и простым в реализации. При зондировании система анализа защищенности имитирует ту атаку, которая использует проверяемую уязвимость, т.е. происходит активный анализ. Данный подход медленнее сканирования, но позволяет убедиться, присутствует или нет на анализируемом компьютере уязвимость.

На практике эти два подхода реализуются в сканерах безопасности через следующие методы проверки:

- Проверка заголовков (Banner check);
- Активные зондирующие проверки (Active probing check);
- Имитация атак (Exploit check).

Первый метод основан на подходе "сканирование" и позволяет делать вывод об уязвимостях, опираясь на информацию в заголовке ответа на запрос сканера безопасности. Примером такой проверки может быть анализ заголовков почтовой программы Sendmail, в результате которого можно узнать ее версию и сделать вывод о наличии в ней уязвимости. Активные зондирующие проверки также основаны на подходе "сканирование". Данный метод сравнивает фрагменты сканируемого программного обеспечения с сигнатурой известной уязвимости, хранящейся в базе данных системы анализа защищенности. Разновидностями этого метода являются, например, проверки контрольных сумм или даты сканируемого программного обеспечения.

Метод имитации атак основан на использовании различных дефектов в программном обеспечении и реализует подход зондирования. Существуют уязвимости, которые не

могут быть обнаружены без блокирования или нарушения функционирования сервисов операционной системы в процессе сканирования. При сканировании критичных серверов корпоративной сети нежелательно применение данного метода, т. к. он может вывести их из строя – и в таком случае сканер безопасности успешно реализует атаку "Denial of service" (отказ в обслуживании). Поэтому в большинстве систем анализа защищенности по умолчанию такие проверки, основанные на имитации атак, выключены

Microsoft Baseline Security Analyzer (MBSA) – свободно распространяемое средство анализа защищенности операционных систем Windows и ряда программных продуктов компании Microsoft (Internet Information Services, SQL Server, Internet Explorer и др.). Термин "Baseline" в названии MBSA следует понимать как некоторый эталонный уровень, при котором безопасность ОС можно считать удовлетворительной. MBSA позволяет сканировать компьютеры под управлением операционных систем Windows на предмет обнаружения основных уязвимостей и наличия рекомендованных к установке обновлений системы безопасности. Критически важно знать, какие обновления установлены, а какие еще следует установить на вашей ОС. MBSA обеспечивает подобную проверку, обращаясь к постоянно пополняемой Microsoft базе данных в формате XML, которая содержит информацию об обновлениях, выпущенных для каждого из программных продуктов Microsoft]. Работать с программой MBSA можно через графический интерфейс и командную строку. На данном занятии будет рассмотрен только первый вариант работы.

Интерфейс MBSA выполнен на основе браузера Internet Explorer. Главное окно программы разбито на две области. Так как сеанс работы с MBSA настраивается с помощью мастера, то в левой области представлены шаги мастера, а в правой – основное окно с описанием действий каждого шага



На первом шаге "Welcome" необходимо выбрать одно из действий:

- Сканировать данный компьютер (Scan a computer);
- Сканировать несколько компьютеров (Scan more than one computer);
- Просмотреть существующие отчеты, сделанные MBSA ранее (View existing security reports).

При первом запуске MBSA необходимо выбрать первый или второй вариант. На следующем шаге мастера в основном окне нужно задать параметры сканирования компьютера(ов) под управлением ОС Windows. Можно ввести имя или IP-адрес сканируемого компьютера (по умолчанию выбирается компьютер, на котором был запущен MBSA).

Пользователь, запустивший MBSA, должен обладать правами администратора данного компьютера или входить в группу администраторов системы. В случае сканирования нескольких компьютеров пользователь должен обладать правами администратора на каждом из компьютеров, а лучше – правами администратора домена.

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name: WORKGROUP\CLIENT01

IP address: [] [] [] []

Security report name: %D%-%C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- Check for Windows administrative vulnerabilities
- Check for weak passwords
- Check for IIS administrative vulnerabilities
- Check for SQL administrative vulnerabilities
- Check for security updates
- Configure computers for Microsoft Update and scanning prerequisites
- Advanced Update Services options:
 - Scan using assigned Update Services servers only
 - Scan using Microsoft Update only

[Learn more about Scanning Options](#)

 Start scan

Выбрав компьютер(ы) для сканирования, необходимо задать опции сканирования:

- проверка ОС Windows;
- проверка паролей;
- проверка служб IIS;
- проверка сервера SQL;
- проверка установленных обновлений безопасности.

Более подробную информацию о проверках MBSA можно получить на официальном сайте Microsoft. Например, когда задана опция "проверка паролей", MBSA проверяет на компьютере учетные записи локальных пользователей, которые используют пустые или простые пароли (эта проверка не выполняется на серверах, выступающих в роли контроллеров домена) из следующих комбинаций:

- пароль пустой;
- пароль совпадает с именем учетной записи пользователя;
- пароль совпадает с именем компьютера;
- паролем служит слово "password";
- паролем служат слова "admin" или "administrator".

Данная проверка также выводит сообщения о заблокированных учетных записях.

После того как все опции будут заданы, необходимо нажать на ссылку внизу "Start scan" (см. рис. 3). При первом сканировании MBSA необходимо подключение к Интернету, чтобы скачать с сайта Microsoft Download Center (<http://www.microsoft.com/downloads>) XML-файл, содержащий текущую справочную базу уязвимостей. MBSA сначала скачивает этот файл в архивированном cab-файле, затем, проверив его подпись, разархивирует его на компьютер, с которого будет запускаться.

Возможна также работа MBSA без подключения к Интернету в автономном режиме. Для этого нужно скачать выше описанный файл и разместить в соответствующем каталоге.

После того как cab-файл будет разархивирован, MBSA начнет сканировать заданный компьютер(ы) на предмет определения операционной системы, наборов обновлений и используемых программ. Затем MBSA анализирует XML-файл и определяет обновления системы безопасности, которые доступны для установленного ПО. Для того чтобы MBSA определил, какое обновление установлено на сканируемом компьютере, ему необходимо знать три пункта: ключ реестра, версию файла и контрольную сумму для каждого файла, установленного с обновлением.

В случае если какие-либо данные на сканируемом компьютере не совпадут с соответствующими пунктами в XML-файле, MBSA определит соответствующее обновление как отсутствующее, что будет отражено в итоговом отчете.

После сканирования единственного компьютера MBSA автоматически запустит окно "View security report" и отобразит результаты сканирования. Если было выполнено сканирование нескольких компьютеров, то следует выбрать режим "Pick a security report to

view", чтобы увидеть результаты сканирования. Создаваемый MBSA отчет разбивается на пять секций:

- Security Update Scan Results,
- Windows Scan Results,
- Internet Information Services (IIS) Scan Results,
- SQL Server Scan Results,
- Desktop Application Scan Results.

Некоторые секции разбиваются еще на разделы, посвященные определенным проблемам безопасности компьютера, и предоставляют системную информацию по каждой из проверок. Описание каждой проверки операционной системы отражается в отчете вместе с инструкцией по устранению обнаруженных уязвимостей.

Задание. Работа с Microsoft Baseline Security Analyzer

.Сначала вы выполните настройки на компьютере позволяющие работать MBSA без подключения к Интернету, а затем выполните сканирование и сгенерируете отчет о проделанной работе.

Упражнение 1. Подготовка компьютера для работы MBSA в автономном режиме

Проверьте, есть ли на вашем рабочем столе ярлычок MBSA. Если ярлык найден то выполняйте упражнение 2.

Если ярлык не найден:

- Установите средство MBSA. Текущие версии MBSA содержатся на странице: <http://www.microsoft.com/>

Упражнение 2. Проверка локального компьютера с помощью MBSA.

1. На рабочем столе щелкните дважды на ярлык программы MBSA.
2. MBSA запустится в графическом режиме в режиме мастера, и появится первое окно "Welcome to the Microsoft Baseline Security Analyzer". Нажмите на ссылку "Scan a computer".
3. Загрузится следующее окно мастера MBSA, где необходимо задать опции сканирования. По умолчанию в поле "Computer name" отобразится имя текущего компьютера, на котором вы запустили MBSA. В опциях сканирования снимите флажок "Check for IIS administrative vulnerabilities" (проверка служб IIS).
4. Нажмите ссылку внизу "Start scan".
5. Так как соединение с Интернетом отсутствует, то под индикатором процесса выполнения сканирования сначала появится надпись "Filed to download security update database". Через несколько секунд MBSA начнет процесс сканирования в автономном режиме, при этом изменится надпись "Curently scanning <Имя компьютера>".
6. После окончания сканирования загрузится отчет с результатами.
7. Внимательно изучите отчет. Переведите его и покажите преподавателю.

Практическое занятие № 15

Использование сетевых утилит для обнаружения неисправностей в локальных сетях.

Теоретические сведения

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

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 таблиц 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.

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 .

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 отправки 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 (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) отправленный 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 выполнялась 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 ЕСНО, 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 Exceeded».

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 Exceeded» (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 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:

- PRINT - вывод информации о маршруте;
- ADD - добавление маршрута;
- DELETE - удаление маршрута;
- 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.

Пример использования утилиты route:

Добавление статического маршрута:
route add 172.16.6.0 MASK 255.255.255.0 172.16.11.1 METRIC 1 IF 0x1000003

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 прослушиваемых 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

Синтаксис:

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.

Задание

1). Выведите на экран справочную информацию по всем рассмотренным утилитам

2) Изучите ключи, используемые при запуске утилит.

2) Получение имени хоста.

Выведите на экран имя локального хоста с помощью команды hostname.

3) Изучение утилиты ipconfig.

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу:

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	

4) Тестирование связи с помощью утилиты ping.

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

5) Определение пути IP-пакета.

С помощью команды traceroute проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

- a)
- b)
- c)

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.

- 1) Узнайте ip-адреса узлов, список которых предоставит преподаватель.
- 2) Узнайте авторитетные (компетентные) сервера для этих узлов.
- 3) Получите запись SOA с одного из этих серверов для домена .

Контрольные вопросы

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 команда ping проверяет соединение с удаленным хостом?
4. Каково назначение протокола ARP?
5. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?

6. Какие могут быть причины неудачного завершения ping и tracer? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).
7. Всегда ли можно узнать символическое имя узла по его ip-адресу?
8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Практическое занятие № 16

Поиск и устранение неполадок физического подключения.

Цель: научиться определять повреждения в кабеле, находить и диагностировать неисправности.

Нарушения нормального функционирования кабельных систем на базе витой пары могут быть вызваны грубыми ошибками при монтаже, скрытыми дефектами конструкции кабеля и повреждением во время его прокладки, процессами старения самих витых пар и арматуры кабельных линий связи, а также другими причинами.

К явным недостаткам монтажа относятся ошибки соединения жил витых пар в кроссах АТС, на стыках строительных длин, в распределительных шкафах и коробках, удаленных терминалах и т. д.

В соответствии с принятой терминологией, две пары, в которых нарушен правильный порядок подключения жил, называются расщепленными (split). Признаками расщепленных пар могут быть увеличенный резистивный и емкостной дисбаланс.

Неправильно смонтированная витая пара, где прямой и обратный провода переставлены местами, называется перевернутой, или скрещенной (reversal). В кабельных линиях СКС порядок подключения жил витой пары крайне важен.

Две витые пары с ошибочным подключением к зажимам терминала называются транспонированными парами (transposition). На телефонной сети такой дефект монтажа приведет к подключению неверного номера. В случае же СКС подключенное к линии оборудование может оказаться неработоспособным.

К основным скрытым дефектам кабельных линий связи относится некачественный монтаж муфт и сростков жил на стыках строительных длин. В первом случае нарушается герметичность оболочки кабеля и возникает опасность его намокания, а для второго характерно появление плохих контактов (partial open) и даже обрыв жил витой пары (open). К таким же результатам приводит коррозия контактов кроссовых устройств и некачественная кроссировка. Дефекты и пробой изоляции жил, влага в кабеле и загрязнение терминалов нередко ведут к замыканию жил пары между собой.

Замыкание может быть низкоомным (short) или высокоомным (partial short). Еще один аналогичный вид дефектов витой пары — замыкание на землю одной или нескольких ее жил (ground). Причем контакт жилы с землей совсем не обязательно будет находиться недалеко от места повреждения изоляции жилы — электрический путь от проводника жилы к земле пройдет через экран кабеля, металлические элементы конструкции терминалов и несущие элементы кабеля.



Замыкание случается и между жилами двух различных пар, причем замкнуты могут быть как одноименные, так и разноименные жилы (cross и battery cross, соответственно). Такой вид дефектов приводит к наличию постороннего напряжения на линии, переходным явлениям, ослаблению сигнала.

Естественный процесс старения витой пары проявляется в виде увеличения вносимого ею затухания вследствие ухудшения диэлектрических свойств изоляции витой пары.

При идентификации неисправностей пары всегда нужно иметь в виду, что ее дефекты могут быть множественными (несколько однотипных дефектов) или комбинированными (несколько разнотипных дефектов), а показания приборов при измерениях с различных сторон могут существенно отличаться.

Источниками помех витой пары служат внутренние и внешние помехи



кабеля.

К основным источникам внутренних помех относят соседние витые пары того же кабеля, а к основным источникам внешних помех — помехи от сети

переменного тока и атмосферные явления, включая разряды молнии и радиопомехи.

Нарушение нормальной работы любого из них может стать причиной повышенных шумов витой пары.

Задание: обследовать образцы витой пары и указать причину неисправностей. Оформить результаты в виде таблицы.

Поиск и устранение неполадок беспроводного соединения

Задачи

Часть 1. Определение сетевых адаптеров ПК и работа с ними

Часть 2. Определение сетевых значков области уведомлений и их использование

Исходные данные/сценарий

В данной лабораторной работе вы должны определить доступность и состояние сетевых адаптеров на используемом ПК. ОС Windows предлагает множество способов просмотра и применения сетевых адаптеров.

Также в этой работе вам нужно получить доступ к данным о сетевом адаптере вашего ПК и изменить его состояние.

Необходимые ресурсы

Один ПК (ОС Windows 7 с двумя сетевыми адаптерами, проводным и беспроводным, а также с беспроводным подключением).

Примечание. В начале этой лабораторной работы проводной сетевой адаптер компьютера подключили к одному из встроенных портов коммутатора на беспроводном маршрутизаторе и активировали проводное подключение по локальной сети. Изначально беспроводной сетевой адаптер был отключён. Если проводной и беспроводной сетевые адаптеры включены, компьютеру будут присвоены два разных IP-адреса, причём беспроводной сетевой адаптер получит приоритет.

Часть 1: Определение сетевых адаптеров ПК и работа с ними

В части 1 вы определите различные типы сетевых адаптеров в используемом ПК и изучите разные способы получения данных о сетевых адаптерах, их включения и отключения.

Шаг 1: Используйте «Центр управления сетями и общим доступом».

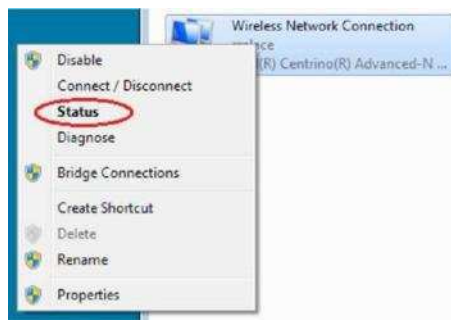
- a. Откройте **Центр управления сетями и общим доступом**, нажав кнопку **Пуск > Панель управления > Просмотр состояния сети и задач** под заголовком «Сеть и Интернет» в представлении по категориям.
- b. В левой части экрана нажмите на ссылке **Изменение параметров адаптера**.
- c. Откроется окно «Сетевые подключения» со списком доступных сетевых адаптеров. В данном окне найдите адаптеры локальной и беспроводной сети.

Шаг 2: Поработайте с беспроводным сетевым адаптером.

- a. Выберите вариант **Подключение по беспроводной сети** и нажмите на неё правой кнопкой мыши, чтобы открыть раскрывающееся меню. Если беспроводной сетевой адаптер отключён, выберите вариант **Включить**. Если сетевой адаптер уже включён, в верхней строке раскрывающегося меню будет указан вариант **Отключить**. Если **Подключение по беспроводной сети** на данный момент отключено, выберите вариант **Включить**.



- b. Нажмите правой кнопкой мыши на **Подключение по беспроводной сети** и выберите вариант **Состояние**.



- c. Откроется окно «Состояние подключения по беспроводной сети» с информацией о беспроводном соединении.



Какой идентификатор SSID соответствует беспроводному маршрутизатору вашего подключения?

Какова скорость вашего беспроводного подключения?

- d. Нажмите кнопку **Подробнее**, чтобы открыть сведения о сетевом подключении.



Откроется информация о типе мер безопасности, действующих на подключённом беспроводном маршрутизаторе. Установите флажок напротив варианта **Показать символы**, чтобы вместо скрытых символов увидеть действующий ключ безопасности сети. После этого нажмите кнопку **ОК**.



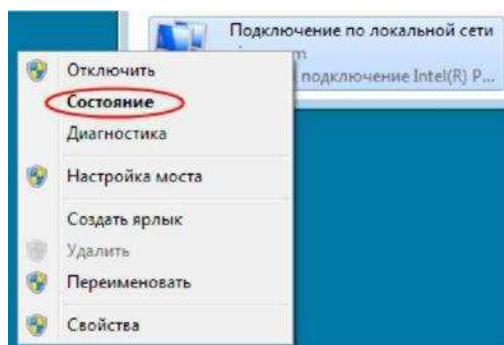
Закройте окна свойств беспроводной сети и состояния сетевого подключения. Нажмите правой кнопкой мыши на вариант **Подключение по беспроводной сети > Подключить/Отключить**.

После этого в правом нижнем углу экрана появится всплывающее окно со списком текущих подключений, а также список идентификаторов SSID, которые находятся в диапазоне беспроводного сетевого адаптера вашего ПК. Если в правой части этого окна есть полоса прокрутки, её можно использовать для просмотра дополнительных идентификаторов SSID.

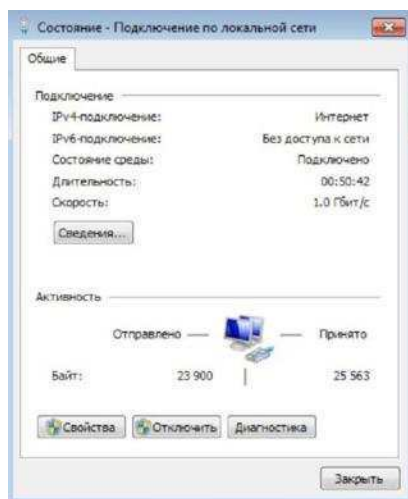


Для подключения к одному из других указанных идентификаторов SSID беспроводной сети выберите интересующий вас идентификатор и нажмите кнопку **Подключить**.

Примечание. Для просмотра состояния сетевого адаптера ПК должен быть подключён к коммутатору или аналогичному устройству с помощью кабеля Ethernet. У многих беспроводных маршрутизаторов есть небольшой встроенный коммутатор с четырьмя Ethernet-портами. Вы можете подключиться к одному из этих портов с помощью прямого кабеля Ethernet.



Откроется окно «Состояние подключения по локальной сети». В нём отображается информация о проводном подключении к локальной сети.



Чтобы увидеть данные адреса локального подключения, нажмите кнопку **Подробнее**.

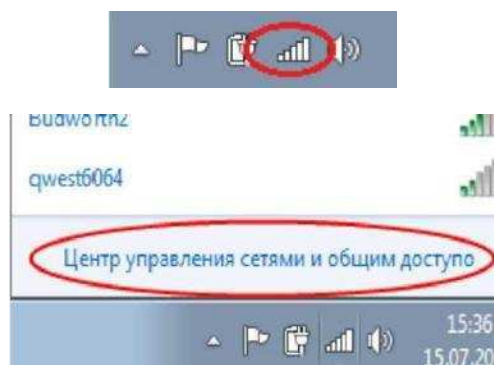
Часть 2: Определение сетевых значков области уведомлений и их использование

В части 2 вы будете использовать сетевые значки в области уведомлений для определения и контроля сетевого адаптера на вашем ПК.

Шаг 1: Используйте значок беспроводной сети.

а. Чтобы открыть всплывающее окно со списком идентификаторов SSID в диапазоне сетевого адаптера, нажмите на значок **Беспроводная сеть** в области уведомлений. Если в области уведомлений отображается значок беспроводной сети, это означает, что беспроводной сетевой адаптер работает.

б. Нажмите пункт **Открыть центр управления сетями и общим доступом**. **Примечание.** Это быстрый способ открыть это окно.



- с. В левой части экрана нажмите на ссылку **Изменение параметров адаптера**, чтобы открыть окно «Сетевые подключения».
- д. Нажмите правой кнопкой мыши на **Подключение по беспроводной сети** и выберите вариант **Отключить**, чтобы отключить беспроводной сетевой адаптер.



- е. Посмотрите на область уведомлений. Значок **Подключение по беспроводной сети** должен смениться на значок **Проводная сеть**, который показывает, что для сетевого соединения используется проводной сетевой адаптер.



Примечание. Если работают оба сетевых адаптера, то в области уведомлений отображается значок **Беспроводная сеть**.

Шаг 2: Воспользуйтесь значком проводной сети.

- а. Нажмите на значок **Проводная сеть**.

Откройте окно ввода команды и введите **ipconfig /all**. Найдите информацию о подключении по локальной сети и сравните её с информацией, указанной в окне «Сведения о сетевом подключении».

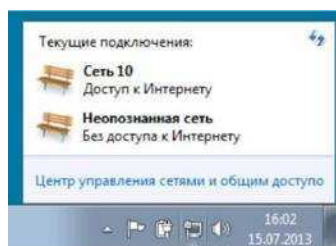


Если вы выбрали безопасный идентификатор SSID, нужно будет ввести **Ключ безопасности** для SSID. Введите ключ безопасности для этого идентификатора SSID и нажмите кнопку **ОК**. Чтобы никто не смог прочитать вводимые символы в поле **Ключ безопасности**, установите флажок напротив варианта **Скрыть символы**.



Шаг 3: Поработайте с проводным сетевым адаптером.

- а. В окне «Сетевые подключения» нажмите правой кнопкой мыши на **Подключение по локальной сети**, чтобы открыть раскрывающийся список. Если сетевой адаптер отключён, включите его и выберите вариант **Состояние**. Идентификаторы SSID больше не отображаются в этом всплывающем окне, но возможность открыть окно «Центр управления сетями и общим доступом» сохранилась.

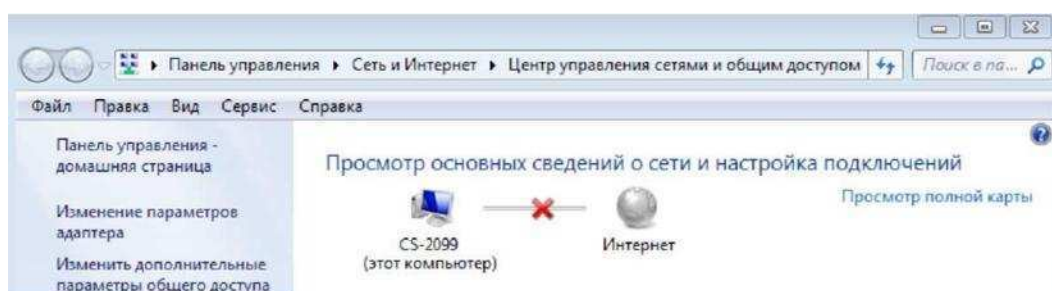


- b. Нажмите **Открыть центр управления сетями и общим доступом** > **Изменить параметры адаптера** и выберите вариант **Включить** для параметра **Подключение к беспроводной сети**. Значок **Беспроводная сеть** должен заменить значок **Проводная сеть** в области уведомлений.



Шаг 3: Определите значок «Ошибка сети»

- a. В окне «Сетевые подключения» отключите варианты **Подключение по беспроводной сети** и **Подключение по локальной сети**.
- b. Теперь в области уведомлений отображается значок **Сеть отключена**, что указывает на отсутствие сетевого подключения.
- c. Нажмите на этот значок, чтобы вернуться в раздел «Центр управления сетями и общим доступом» (изучите схему сети сверху).



Нажмите на красный **X**, чтобы ПК нашёл и устранил проблему с сетевым подключением. Средство диагностики попытается устранить неполадки с сетью.

- d. Если это не помогло и сетевой адаптер не работает, рекомендуется найти и устранить неполадки подключения вручную.

Примечание. Если сетевой адаптер включён, но не может установить сетевое подключение, то в области уведомлений появляется значок **Ошибка сети**.



Если появился такой значок, можно попытаться решить эту проблему точно так же, как указано в шаге 3с.