

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:
Или (Или)

УТВЕРЖДАЮ
Начальник УМО

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий

По УП 03.03. Сетевое взаимодействие в малых сетях

Специальность: 09.02.02 Компьютерные сети

Разработчик:
Зав.УВЦ Капоровский В.Е.

2017г

Введение

Методическое пособие по проведению практических работ по УП 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».

Настоящее методическое пособие рассчитано на самостоятельную работу обучающихся в учебном кабинете под руководством преподавателя, а также является руководством для преподавателей при подготовке к проведению учебной практики.

Для успешного прохождения учебной практики могут быть использованы теоретические знания полученные обучающимися при прохождении ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

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.

УП.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;
- усвоение студентами основ законодательства об охране труда, системы стандартов безопасности труда, требований правил гигиены труда и производственной санитарии, противопожарной защиты, охраны окружающей среды в соответствии с новыми нормативными и законодательными актами.

Программа учебной практики УП.03.03 «Сетевое взаимодействие в малых сетях» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.02 Компьютерные сети (базовой подготовки) в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и формирование следующих профессиональных компетенций (ПК):

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.

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. Закрывать 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 широкоэвещательные пакеты всем сегментам сети. Поэтому в сети, использующей коммутаторы, все сегменты должны рассматриваться как один широкоэвещательный 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:

- 1) Изучить следующее представленное оборудование: D-Link Des-1210-28, 3Com Switch 5500-SI, Cisco Catalyst 3550 series (3 шт.), Cisco 2600 series, Cisco Catalyst 1900. (группа делится на подгруппы, каждой подгруппе свой перечень оборудования)
- 2) Выполнить подключение оборудования к своему рабочему месту (ПК).
- 3) Проверить настройки оборудования.
- 4) Ответить на вопросы:
 1. К какому типу сетевых устройств относится данное оборудование.
 2. Рассмотреть все разъемы на данных устройствах. Для чего они предназначены?
 3. Сравнить предоставленное оборудование по типу, по разъемам, по настройкам. 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:

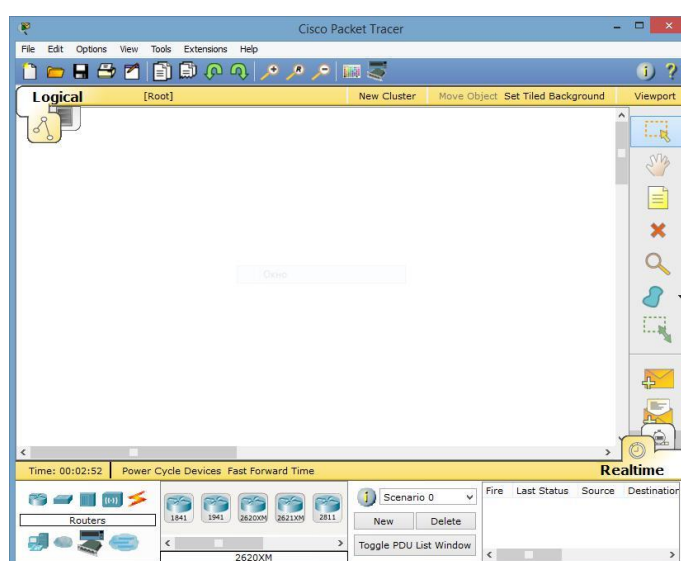


Рисунок 1 – Основное окно системы Cisco Packet Tracer

- Основное меню;
- Панели инструментов (главную, вертикальную и нижнюю);
- Переключатели режимов моделирования (реального времени и пошаговый) и видов

схем (логическая и физическая).

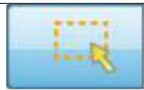

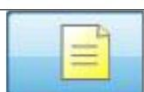





Основное меню программы содержит пункты: Файл (File), Редактирование (Edit), Настройки (Options), Вид (View), Утилиты (Tools), Дополнения (Extensions), Помощь (Help). Пункт меню «Файл» используется для выполнения операций с текущим файлом (открыть, закрыть, сохранить, распечатать и т.п.), а также позволяет 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).

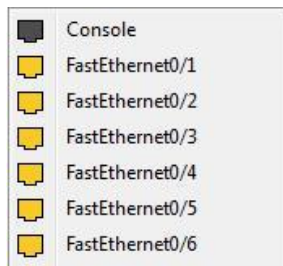
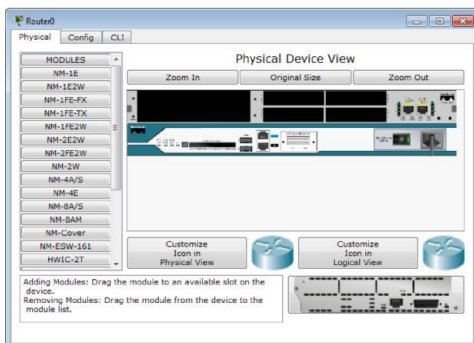


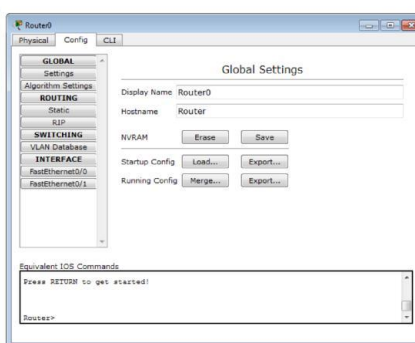
Рисунок 4 – Меню выбора сетевого интерфейса коммутатора

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).

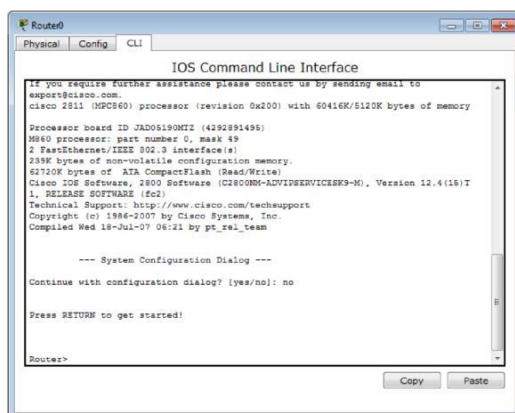
Для оконечных устройств реализованы дополнительные вкладки (см., например, рисунок 5г). На вкладке «Desktop» расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). «Software/Services» - конфигурирование программного обеспечения, которое должно быть установлено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

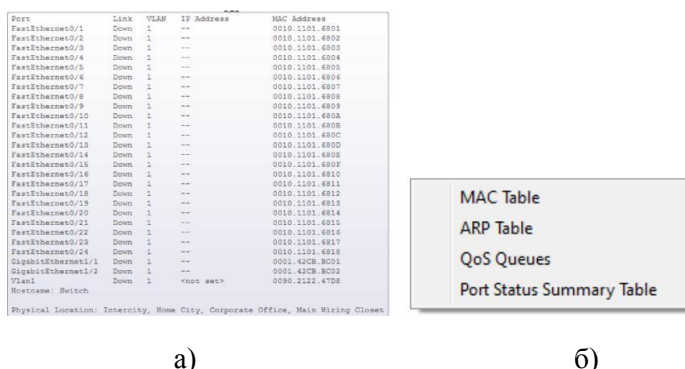


Рисунок 6 – Всплывающая подсказка (а) и меню инструмента Inspect (б)

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.

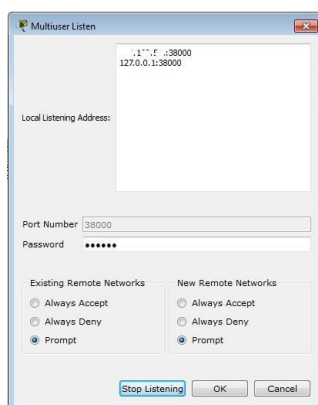


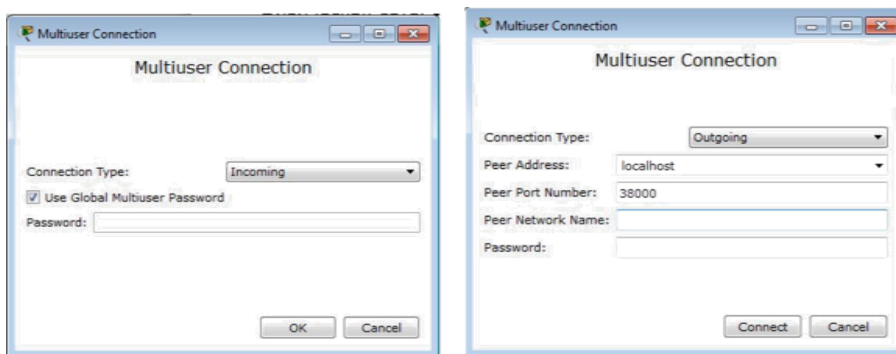
Рисунок 7 – Окно настройки удалённого взаимодействия

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 ICPM (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.

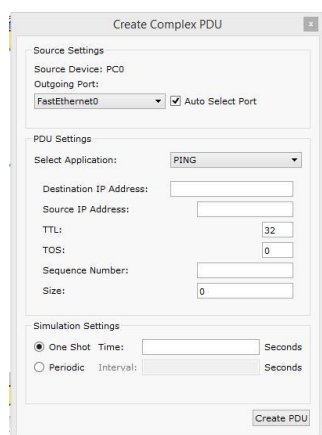


Рисунок 9 – Окно настроек параметров передачи информации по сети

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	

Рисунок 11 – Панель настроек пошагового моделирования

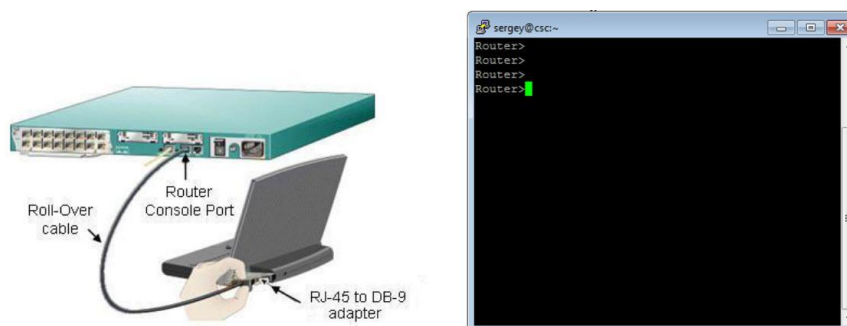
б. Командная строка управления устройствами (CLI)

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 по (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). Едиными 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 интерфейса*. Каждый сетевой интерфейс (или кратко – интерфейс) имеет свои 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). Вернутся 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

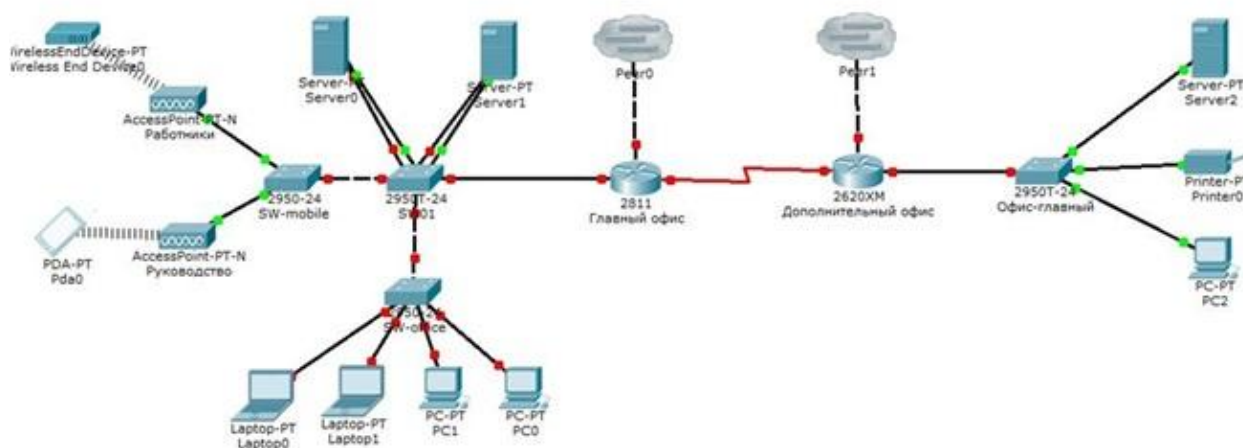
Конфигурацию оборудования можно стереть, сохранить в отдельный файл и затем восстановить её из него. Сделать это можно с помощью окна настроек оборудования (вкладка `Config`). Следует отметить, что конфигурация оборудования изменяется в режиме реального времени. Перегрузка устройства приведет к тому, 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.
2. Сконфигурируйте в среде моделирования сеть, представленную на рисунке.



3. Используя командную строку задайте сетевым узлам:
 - 1) Уникальные сетевые имена;
 - 2) Приветственные приглашения, в которых будет указываться краткая информация о сетевом устройстве;
 - 3) Пароли для подключения к устройствам;
 - 4) Задайте описания для соответствующих сетевых интерфейсов.
4. Сохраните настройки сетевых устройств в их энергонезависимой памяти. Для маршрутизаторов, соединяющих основной и дополнительный офисы сохраните конфигурацию в отдельные файлы.
5. Проверьте работоспособности сети командой ping.
 - a. ping от компьютера PC1 в главном офисе до компьютера PC2 в дополнительном офисе;
 - b. ping от компьютера PC0 в главном офисе до сервера Server0 в главном корпусе;
 - c. ping от компьютера PC2 в главном офисе до сервера Server2 в дополнительном офисе;

Результаты отобразите в виде отчета.

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. Физическое подключение двух компьютеров для работы в одноранговой сети. Изготовить сетевой кабель для соединения “компьютер-компьютер”. Соединить два рядом стоящих компьютера.

Задание 2. 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. Настроить параметры протокола TCP/IP, для объединения двух компьютеров в сеть. (ip адрес должен быть из той же сети, что и у соседа).
3. Задать рабочую группу (название указывает преподаватель)

Примечание. Название рабочей группы должно быть одинаковым для всех компьютеров класса.

4. Включить общий доступ к файлам и принтерам.
5. Проверьте командой ping, что компьютер “соседа” доступен.

Задание 3. Предоставление папки в общий доступ

1. Войдите в систему с учетной записью, входящей в локальную группу «Администраторы»
2. На локальном диске (C:) создайте папку, введите имя папки, совпадающее с именем вашей учетной записи.
3. Откройте общий доступ к этой папке и Разрешите изменение файлов по сети.
4. Выполните двойной щелчок мышью на значке созданной папки.
5. В открывшемся окне папки создайте текстовый файл с именем, совпадающим с именем вашей учетной записи.

Задание 4. Работа с общими папками в одноранговой сети

Найдите через сеть файл, созданный вашим партнером. Откройте его и внесите свои изменения, после чего сохраните файл.

Результаты отобразите в виде отчета.

Практическое занятие № 4

Организация общего доступа к сетевым дискам.

Теоретические сведения

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

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, удалять 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. Для этой папки задать общий доступ.
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.
7. Настройте доступ для вашей папки таким образом, чтобы один файл смогли бы открыть только вы под своей учетной записью для редактирования, а другой файл мог бы открыть сосед только для чтения.

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 № 5. **Настройка сетевых устройств. NAT, DHCP.**

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.

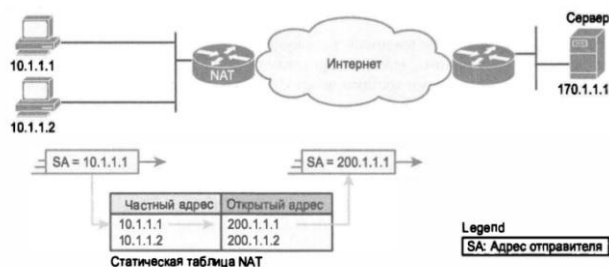
Идентификатор частной сети	Маска подсети	Диапазон IP-адресов
10.0.0.0	255.0.0.0	10.0.0.1 – 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 – 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 – 192.168.255.254

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

```

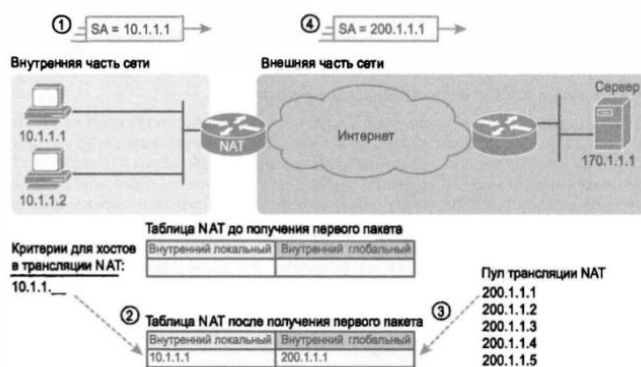
Статические соответствия создаются с помощью команды *ip nat inside source static*. Ключевое слово *inside* означает, что NAT транслирует адреса для хостов, находящихся во внутренней части сети. Ключевое слово *source* означает, что NAT транслирует IP-адреса в пакетах, поступающих на ее внутренние интерфейсы. 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) Запустите среду моделирования Cisco packet tracer.
- 2) Придумайте сеть которая будет состоять из роутера, коммутатора, и двух ПК.
- 3) Настроить статическую трансляцию NAT для роутера. Данные для интерфейсов взять у преподавателя
- 4) Настроить динамическую трансляцию NAT для роутера. Данные для интерфейсов взять у преподавателя
- 5) Настроить роутер, который будет выдавать по DHCP сеть X начиная с ip адреса Y. Значения X и Y взять у преподавателя.

Практическое занятие № 6

Изучение протокола FTP

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.

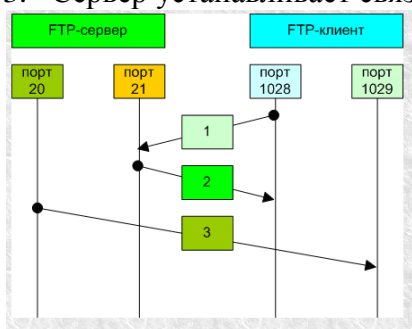
Протокол FTP предусматривает два возможных режима установления связи для обмена файлами:

- **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.

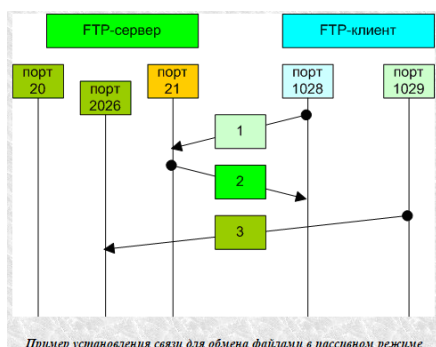


Активный режим выгоден для FTP-сервера, но вреден для клиента. Так как FTP сервер пытается соединиться со случайным высоким (по номеру) портом на клиенте, то такое соединение может быть заблокировано брандмауэром на стороне клиента.

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

Ход работы:

1. Войдите в систему с учетной записью, входящей в локальную группу «Администраторы»
2. Установите FTP-сервер.
Примечание: FTP-сервер входит в состав служб IIS. Включаем следующие компоненты: Службу FTP и Консоль управления IIS.
3. Настройте FTP-сервер.
Примечание: Открываем Диспетчер служб IIS. Добавить FTP-сайт.
4. В мастере создания ftp-сайта указать его название и расположение (по умолчанию c:\inetpub\ftproot).
5. Далее указать параметры привязки и SSL. Раздел привязка оставить без изменений. Опцию «Запускать ftp-сайт автоматически» отключить. В разделе SSL выставить опцию «Без SSL».
6. Настройте дополнительные параметры.
Ограничьте максимальное количество одновременных подключений. И еще какой-нибудь параметр по вашему усмотрению.
7. Настройте брандмауэр Windows для FTP.

- 1) Задайте «Правила для входящих подключений».
- 2) Задайте «Правила для исходящих подключения»
8. Настроить права пользователей. Сделать доступ для доверенных пользователей, которые имели бы права записи и изменения файлов.
Примечания Если оставить все как есть, то подключиться к ftp-серверу сможет любой пользователь (включен анонимный доступ) с правами только на чтение (можно скачивать, но записывать и изменять файлы нельзя).
В группе Локальные пользователи и группы создайте Группу «Пользователи FTP». В этой группе поместите своего пользователя.
9. Для группы «Пользователи FTP» необходимо настроить права доступа к вашему рабочему каталогу. Устанавливаем уровень прав — «Полный доступ».
10. В панели управления ftp-сайтом выбирать «Правила авторизации FTP». Добавить разрешающее правило. В разделе Разрешения - Чтение и Запись.
11. Запускаем FTP сервер вручную.
12. Подключитесь к ftp серверу через проводник Windows.

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 Thunderbird, который будет работать с вашим почтовым ящиком.
3. Какие преимущества при работе с Thunderbird.

Практическое занятие № 7

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.

- 1) Войдите в систему как локальный пользователь, с учетной записью, указанной преподавателем.
- 2) Настройте сеть на рабочем месте, для подключения Беспроводного маршрутизатора TP-Link.

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

- 1) Загрузите обозреватель Internet Explorer.
- 2) Через браузер зайдите на настройки Беспроводного маршрутизатора TP-Link.
- 3) Настройте DHCP Server.

Задание 3

1) Настройте ПК на динамическую IP-адресацию. Ваш ПК должен получить ip адрес от DHCP сервера Беспроводного маршрутизатора TP-Link.

2) Проверьте командой ipconfig, что ваш Ip адрес находится в нужном диапазоне.

Задание 4.

Изучите дополнительные настройки, которые можно задать для Беспроводного маршрутизатора TP-Link.

Практическое занятие № 8

Настройка политик доступа.

Теоретические сведения

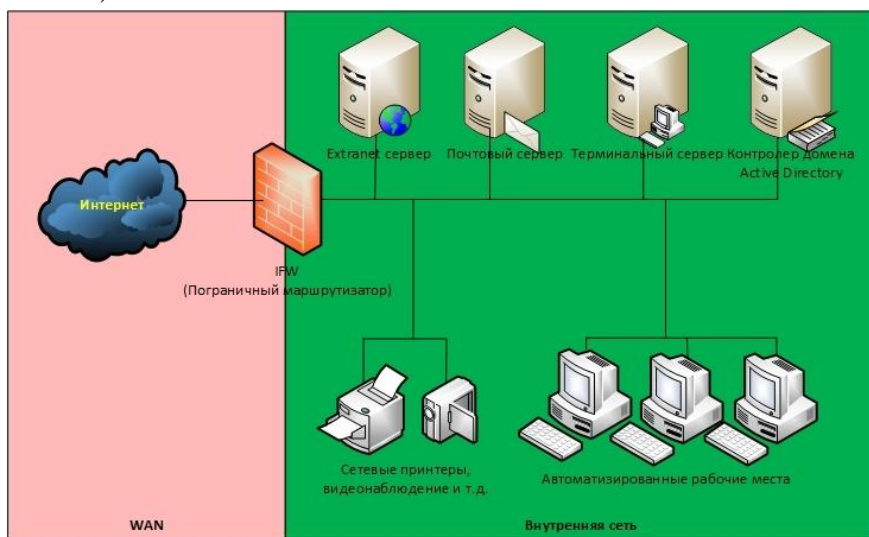
Данная статья содержит обзор *пяти* вариантов решения задачи организации доступа к сервисам корпоративной сети из Интернет. В рамках обзора приводится анализ вариантов на предмет безопасности и реализуемости, что поможет разобраться в сути вопроса, освежить и систематизировать свои знания как начинающим 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:

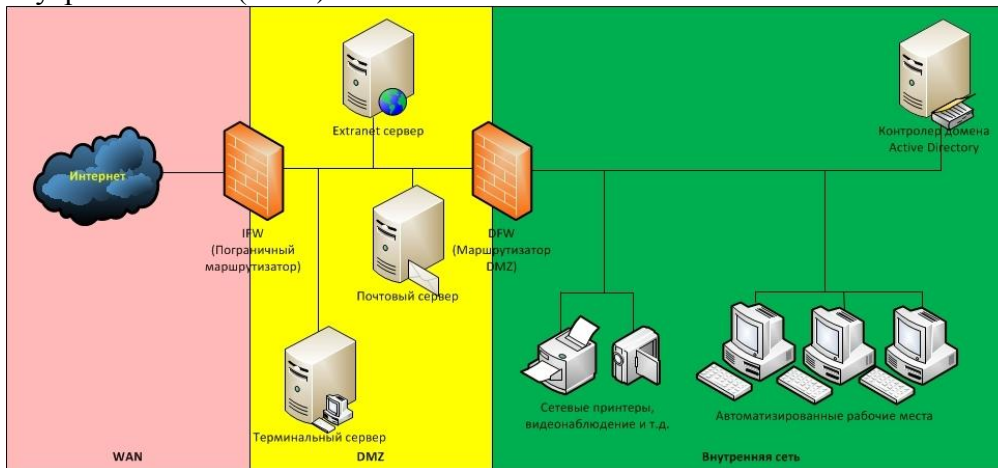
1. Минимальный уровень безопасности. В случае взлома, при котором Нарушитель получит контроль над одним из опубликованных в Интернете серверов, ему для дальнейшей атаки становятся доступны все остальные узлы и каналы связи корпоративной сети.

Аналогия с реальной жизнью

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

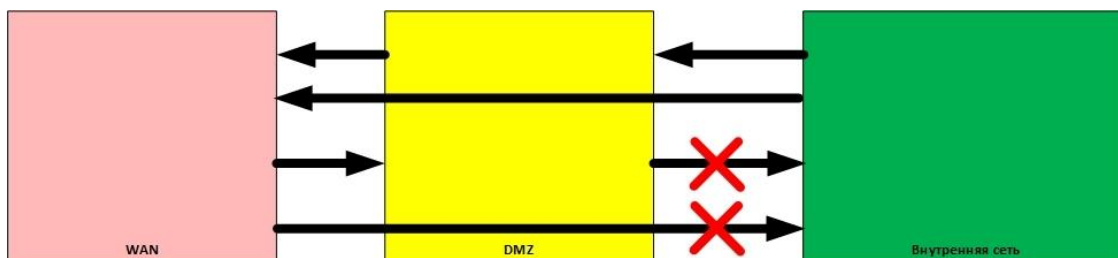
Вариант 2. DMZ

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:

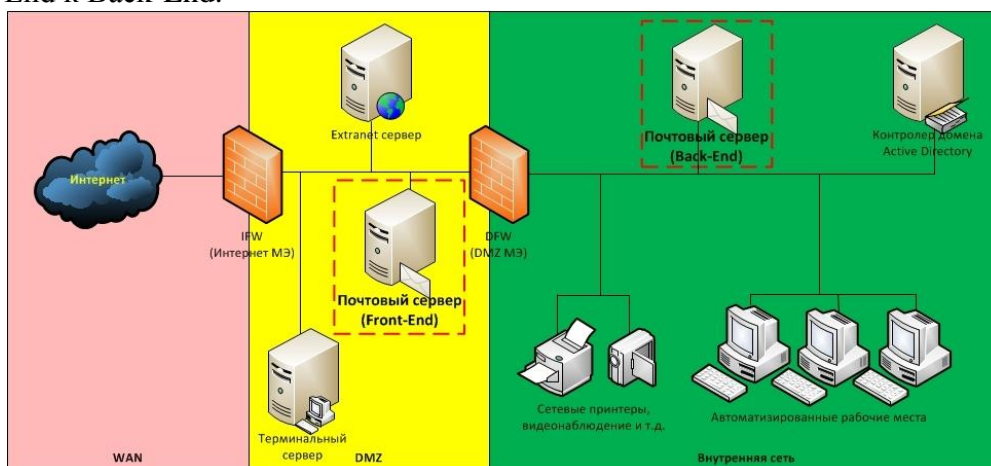
1. Сам по себе вынос серверов в DMZ не повышает их защищенность.
2. Необходим дополнительный МЭ для отделения DMZ от внутренней сети.

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 proxy 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 proxy 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:

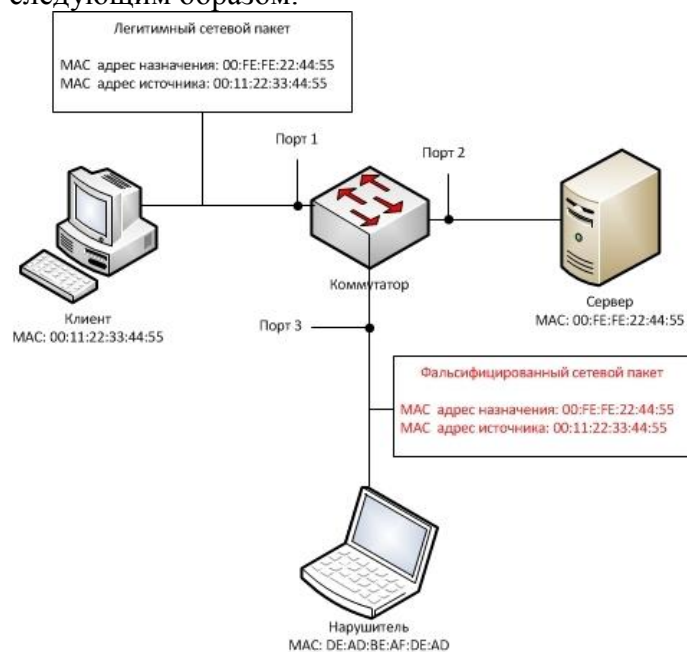
1. MAC spoofing;
2. IP spoofing.

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

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

Защита от MAC spoofing

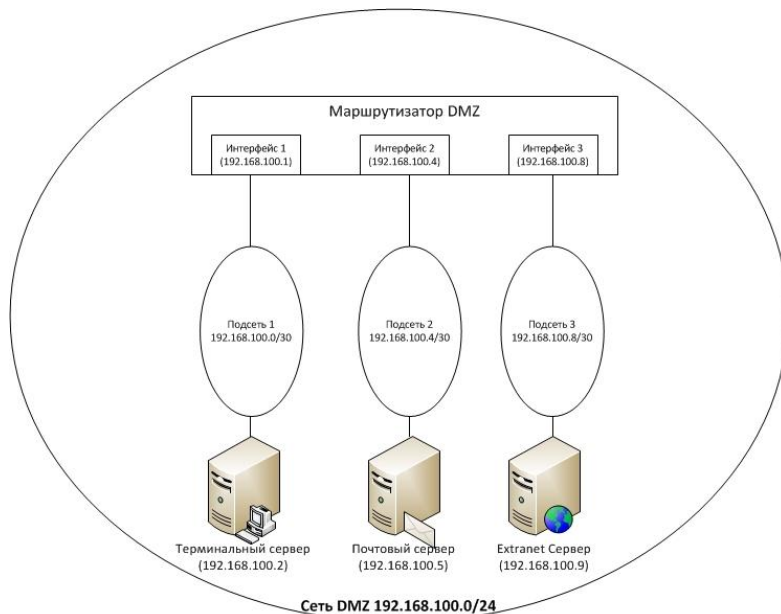
Схематически атаки, связанные с подменой MAC адреса, можно проиллюстрировать следующим образом:



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 деление 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, SAM 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).

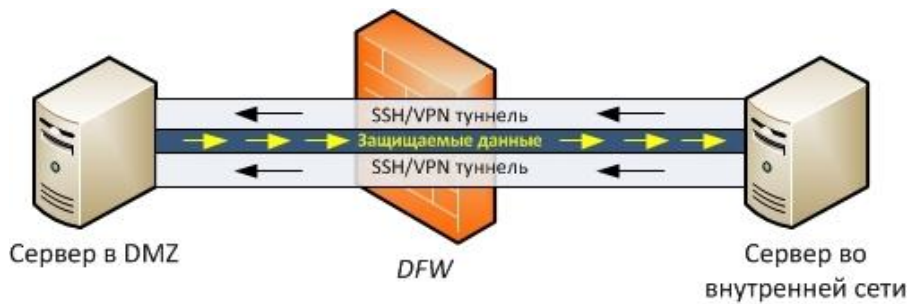
Предлагаемый далее подход направлен на уменьшение числа каналов, через которые Нарушитель может атаковать сервера, а таких канала как минимум два. Первый это правило на *DFW*, разрешающее доступ к серверу внутренней сети из DMZ (пусть даже и с ограничением по IP-адресам), а второй — это открытый на сервере сетевой порт, по которому ожидаются запросы на подключение.

Закрыть 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 меж сетевого 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) Придумать свою организацию, где требуется использовать различные виды DMZ.
- 3) Составить схему размещения DMZ.
- 4) Обоснуйте необходимость установки DMZ.
- 5) Результаты отобразить в виде отчета.

Практическое занятие № 10

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.

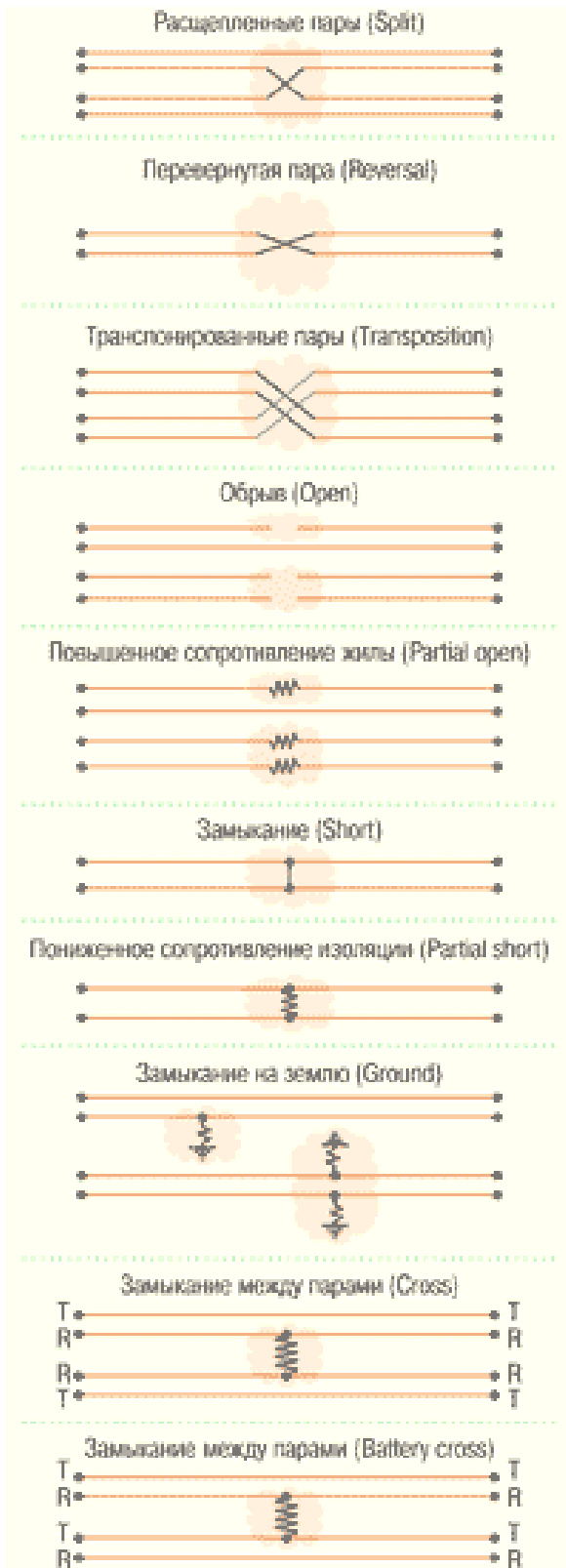
В соответствии с принятой терминологией, две пары, в которых нарушен правильный порядок подключения жил, называются расщепленными (split). Признаками расщепленных пар могут быть увеличенный резистивный и емкостной дисбаланс.

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.

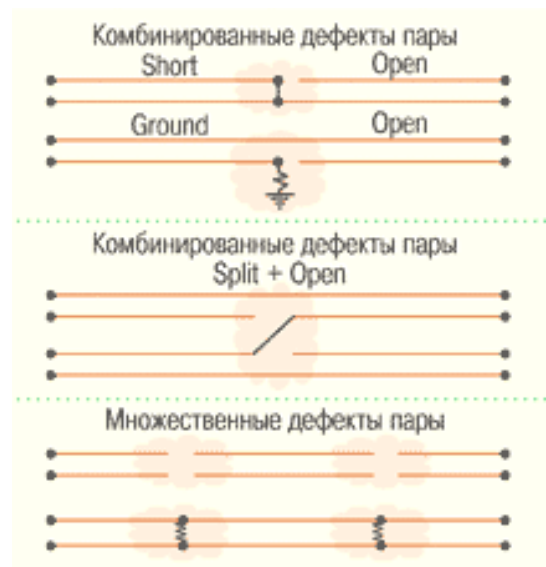


Замыкание случается и между жилами двух различных пар, причем замкнуты могут быть как одноименные, так и разноименные жилы (cross и battery cross, соответственно). Такой вид дефектов приводит к наличию постороннего напряжения на линии, переходным явлениям, ослаблению сигнала.

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: 1. обследовать образцы витой пары и указать причину неисправностей.

2. Исследовать сеть (подробности запросить у преподавателя). Найти неисправность.

Практическое занятие № 11

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 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

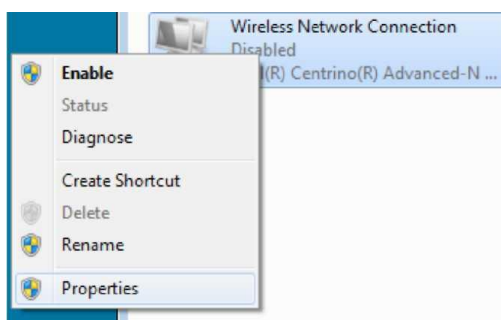
В части 1 вы определите различные типы сетевых адаптеров в используемом ПК и изучите разные способы получения данных о сетевых адаптерах, их включения и отключения.

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

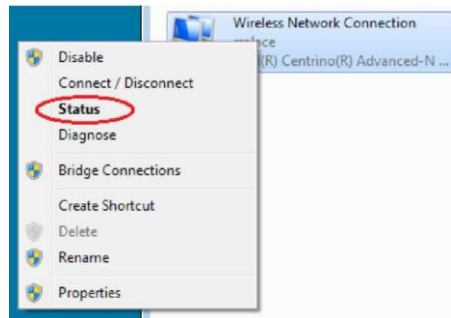
- Откройте **Центр управления сетями и общим доступом**, нажав кнопку **Пуск > Панель управления > Просмотр состояния сети и задач** под заголовком «Сеть и Интернет» в представлении по категориям.
- В левой части экрана нажмите на ссылку **Изменение параметров адаптера**.
- Откроется окно «Сетевые подключения»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

Шаг 2: Поработайте с беспроводным сетевым адаптером.

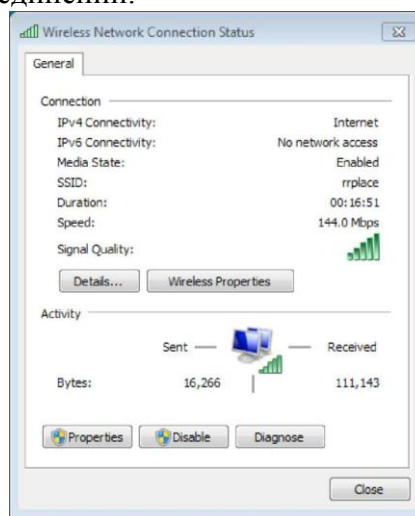
- Выберите вариант **Подключение по беспроводной сети** и нажмите на неё правой кнопкой мыши, чтобы открыть раскрывающееся меню. Если беспроводной сетевой адаптер отключён, выберите вариант **Включить**. Если сетевой адаптер уже включён, в верхней строке раскрывающегося меню будет указан вариант **Отключить**.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



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



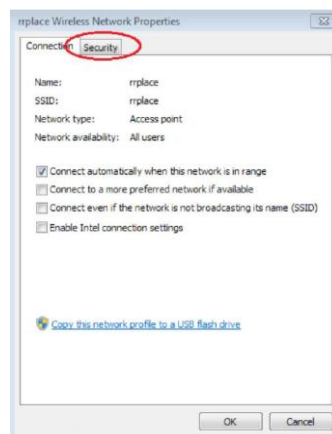
с. Откроется окно «Состояние подключения по беспроводной сети» с информацией о беспроводном соединении.



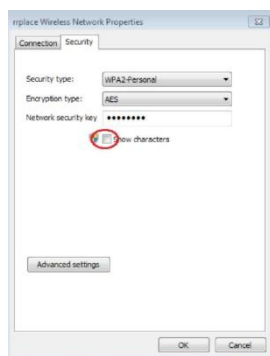
Какой идентификатор SSID соответствует беспроводному маршрутизатору вашего подключения?

Какова скорость вашего беспроводного подключения?

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

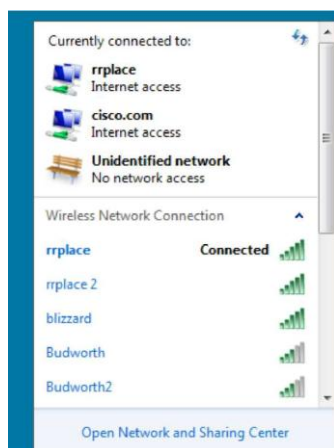


Откроется информация о типе мер безопасности, действующих на подключённом беспроводном маршрутизаторе. Установите флажок напротив варианта **Показать символы**, чтобы вместо скрытых символов увидеть действующий ключ безопасности сети. После этого нажмите кнопку **ОК**.



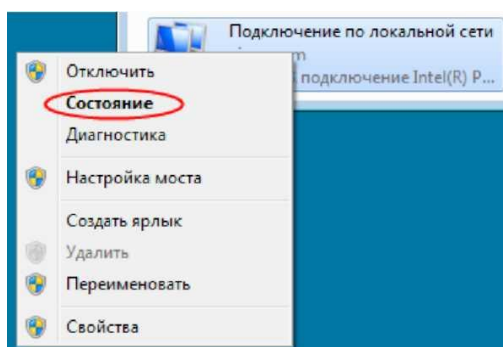
Закройте окна свойств беспроводной сети и состояния сетевого подключения. Нажмите правой кнопкой мыши на вариант **Подключение по беспроводной сети > Подключить/Отключить**.

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.

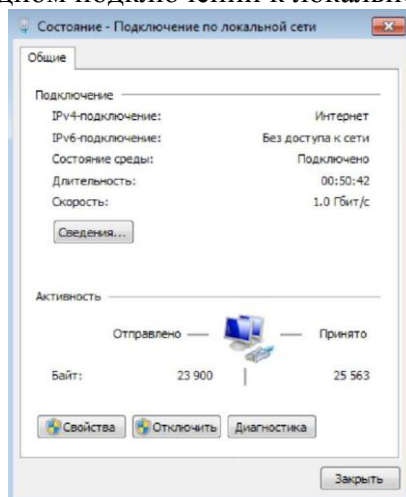


Для подключения к одному из других указанных идентификаторов SSID беспроводной сети выберите интересующий вас идентификатор и нажмите кнопку **Подключить**.

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**.

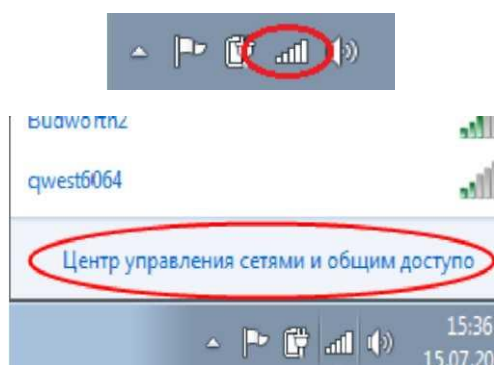
Часть 2: Определение сетевых значков области уведомлений и их использование

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

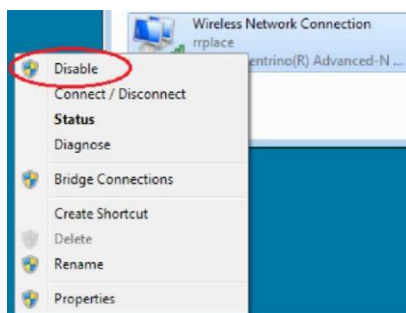
Шаг 1: Используйте значок беспроводной сети.

i. 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.

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



- c. В левой части экрана нажмите на ссылку **Изменение параметров адаптера**, чтобы открыть окно «Сетевые подключения».
- d. 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.

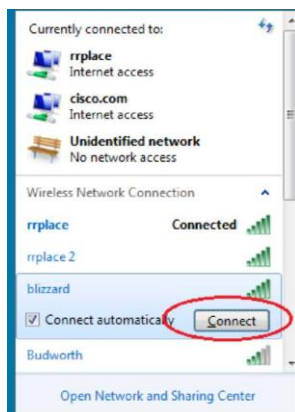


Примечание. Если работают оба сетевых адаптера, то в области уведомлений отображается значок **Беспроводная сеть**.

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».

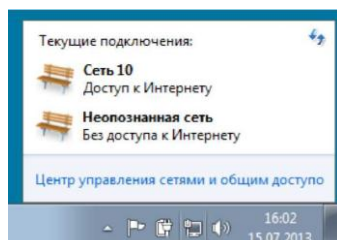


Если вы выбрали безопасный идентификатор SSID, нужно будет ввести **Ключ безопасности** для SSID. Введите ключ безопасности для этого идентификатора SSID и нажмите кнопку **ОК**. Чтобы никто не смог прочитать вводимые символы в поле **Ключ безопасности**, установите флажок напротив варианта **Скрыть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



Шаг 3: Поработайте с проводным сетевым адаптером.

- a. 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.

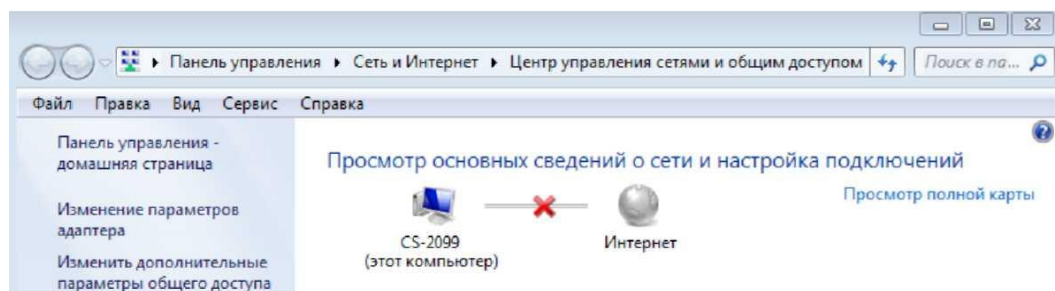


- b. Нажмите **Открыть центр управления сетями и общим доступом > Изменить параметры адаптера** и выберите вариант **Включить** для параметра **Подключение к беспроводной сети**. Значок **Беспроводная сеть** должен заменить значок **Проводная сеть** в области уведомлений.



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.

Задача

Выявление и устранение неправильной настройки беспроводного устройства.

Исходные данные

Владелец небольшой компании узнал, что беспроводной пользователь не может подключиться к сети. На всех ПК настроена статическая IP-адресация. Выявите причину проблемы и устраните ее.

Шаг 1. Проверка подключения