Министерство образования Республики Беларусь

Учреждение образования «Белорусский Государственный Университет Информатики и Радиоэлектроники»

Кафедра «Информатика»

Проект

«Сеть небольшого предприятия»

по курсу «Компьютерные сети»

**Выполнил:**

Волчецкий А. М., гр. 253505

**Проверил:**

Ганжа В. А.

Минск 2015

# **Постановка задачи:**

Сеть небольшого предприятия - 50 сотрудников (файловый сервер, почтовый сервер, сервер печати, поддержка пакета "Бухгалтерия", поддержка пакета "Кадры")

# **Функциональная схема локальной вычислительной сети**



# **Способ управления сетью**

Для управления сетью достаточно главного администратора для настройки сервера и 1-2 помощников для прокладки кабеля и обслуживания оборудования.

# **Архитектура сети (схема, описание)**

Применяемая архитектура сети – звезда.

При использовании топологии "звезда", каждый компьютер подключается к специальному концентратору. Преимуществом этой топологии является ее устойчивость к повреждениям кабеля - при обрыве перестает работать только один из узлов сети и поиск повреждения значительно упрощается. Недостатком является более высокая стоимость.

Сервер находится в проветриваемом охраняемом помещении.

Для выхода в глобальную сеть используется оптоволокно, идущее к серверам провайдера.

# **Описание сервера**

**Конфигурации**

• ОС: Windows Server 2012

• процессор: 64-разрядный процессор с тактовой частотой 2,2 ГГц

• ОЗУ: от 16 Гб

• свободное место на жестком диске: от 2 Тб

**Описание ОС**

*Поддержка следующих сетевых служб :*

• Dynamic Host Configuration Protocol (DHCP) Server — обеспечивает централизованную конфигурацию и управление временными IP-адресами и соответствующей информацией для клиентских компьютеров;

• Domain Name System (DNS) Server — транслирует доменные и компьютерные DNS-имена в IP-адреса. Такой сервер проще в управлении, если он установлен на том же сервере, что и доменные сервисы Active Directory Domain Services;

• Active Directory Certificate Services (AD CS) — позволяет создавать цифровые сертификаты для пользователей, компьютеров и организаций и управлять ими; представляет собой часть инфраструктуры поддержки публичных ключей (public key);

• Active Directory Domain Services (AD DS) — хранит информацию о сетевых объектах и делает ее доступной для пользователей и сетевых администраторов. Для своей работы AD DS использует контроллеры доменов для предоставления сетевым пользователям ресурсов в любой точке сети;

• Active Directory Federation Services (AD FS) — обеспечивает упрощенный, зашифрованный способ передачи идентификационной информации и поддержку единого доступа к ресурсам (Web single sign-on, SSO);

• Network Access Services — поддерживает роутинг сетевого трафика через LAN и WAN, создание и применение правил сетевого доступа (network access policies) и доступ к сетевым ресурсам через VPN-соединения и dial-up;

# **Сетевые Службы**

Основным элементом функционирования сети является службы DHCP

## **Служба DHCP**

DHCP (*Dynamic Host Configuration Protocol*) — [сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), позволяющий компьютерам автоматически получать [IP-адрес](http://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) и другие параметры, необходимые для работы в сети [TCP/IP](http://ru.wikipedia.org/wiki/TCP/IP). Данный протокол работает по модели «[клиент-сервер](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80)». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому [*серверу*](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%28%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%29) *DHCP*, и получает от него нужные параметры. [Сетевой администратор](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80) может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

Протокол DHCP предоставляет три способа распределения [IP-адресов](http://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81):

* *Ручное распределение.* При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это [MAC-адрес](http://ru.wikipedia.org/wiki/MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81)) каждого [клиентского](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82_%28%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%29) компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на [сервере](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%28%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5%29) DHCP), и потому их проще изменять при необходимости.
* *Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
* *Динамическое распределение.* Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется *арендой адреса*. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи [DNS](http://ru.wikipedia.org/wiki/DNS), соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в [RFC 2136](http://tools.ietf.org/html/rfc2136).

**Служба DNS**

DNS ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Domain Name System* — система доменных имён) — компьютерная [распределённая система](http://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B1%D0%B0%D0%B7%D1%8B_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) для получения информации о [доменах](http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F). Чаще всего используется для получения IP-адреса по имени [хоста](http://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82) (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

Основой DNS является представление об иерархической структуре [доменного имени](http://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F) и *зонах*. Каждый сервер, отвечающий за имя, может *делегировать* ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Основное назначение DNS состоит в преобразовании имени хоста в его IP-адрес. На самом деле DNS является системой, не зависимой от протокола сетевого уровня, т. е. она может быть реализована не только в среде TCP/IP.

Однако функции DNS этим не ограничиваются. DNS позволяет получить следующую информацию:

* IP-адрес хоста;  
  доменное имя хоста по его IP-адресу;
* псевдонимы хоста, тип центрального процессора и операционной системы хоста;
* сетевые протоколы, поддерживаемые хостом;
* почтовый шлюз;
* почтовый ящик:
* почтовую группу;
* IP-адрес и доменное имя сервера имен доменов.

# **8. Защита информации в сети**

**Протокол HTTPS**

HTTPS - HyperText Transfer Protocol Secure — расширение [протокола](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) [HTTP](http://ru.wikipedia.org/wiki/HTTP), поддерживающее [шифрование](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол [SSL](http://ru.wikipedia.org/wiki/SSL) или [TLS](http://ru.wikipedia.org/wiki/TLS). В отличие от HTTP, для HTTPS по умолчанию используется [TCP](http://ru.wikipedia.org/wiki/TCP)-[порт](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D1%82_%28TCP/IP%29) 443.

Протокол был разработан компанией [Netscape Communications](http://ru.wikipedia.org/wiki/Netscape_Communications) для браузера [Netscape Navigator](http://ru.wikipedia.org/wiki/Netscape_Navigator) в 1994 году. HTTPS широко используется в мире [веб](http://ru.wikipedia.org/wiki/%D0%92%D1%81%D0%B5%D0%BC%D0%B8%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B0%D1%83%D1%82%D0%B8%D0%BD%D0%B0) и поддерживается всеми популярными [браузерами](http://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80).

HTTPS не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы [SSL](http://ru.wikipedia.org/wiki/SSL) и [TLS](http://ru.wikipedia.org/wiki/TLS). Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от [снифферских](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0) атак и атак типа [man-in-the-middle](http://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA_%D0%BF%D0%BE%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5) при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют.

В HTTPS для шифрования используются ключи длиной 40, 56, 128 или 256 бит. Лишь старые версии браузеров используют 40-битные ключи ([IE](http://ru.wikipedia.org/wiki/Internet_Explorer) версий до 4.0), что связано с экспортными ограничениями в США. Длина ключа 40 бит не является сколько-нибудь надёжной. Многие современные сайты требуют использования новых версий браузеров, поддерживающих шифрование с длиной ключа 128 бит, с целью обеспечить достаточный уровень безопасности. Такое шифрование значительно затрудняет злоумышленнику поиск паролей и другой личной информации.

**Протокол SSL и SSL-сертификаты**

SSL ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Secure Sockets Layer — уровень защищённых сокетов) — [криптографический протокол](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), который обеспечивает безопасность связи. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко используется для обмена мгновенными сообщениями и передачи голоса через [IP](http://ru.wikipedia.org/wiki/IP) ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Voice over IP — [VoIP](http://ru.wikipedia.org/wiki/VoIP)), в таких приложениях, как [электронная почта](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0), Интернет-факс и др.

SSL поддерживает 3 типа аутентификации:

* аутентификация обеих сторон (клиент — сервер),
* аутентификация сервера с неаутентифицированным клиентом,
* полная анонимность.

Если сервер аутентифицирован, то его сообщение о сертификации должно обеспечить верную сертификационную цепочку, ведущую к приемлемому центру сертификации. Проще говоря, аутентифицированный клиент должен предоставить допустимый сертификат серверу. Каждая сторона отвечает за проверку того, что сертификат другой стороны ещё не истек и не был отменен. Всякий раз, когда сервер аутентифицируется, канал устойчив (безопасен) к попытке перехвата данных между веб-сервером и браузером, но полностью анонимная сессия по своей сути уязвима к такой атаке. Анонимный сервер не может аутентифицировать клиента. Главная цель процесса обмена ключами — это создание секрета клиента (pre\_master\_secret), известного только клиенту и серверу. Секрет (pre\_master\_secret) используется для создания общего секрета (master\_secret). Общий секрет необходим для того чтобы создать сообщение для проверки сертификата, ключей шифрования, секрета [MAC](http://ru.wikipedia.org/wiki/Message_authentication_code) (message authentication code) и сообщения «finished». Отсылая сообщение «finished», стороны указывают, что они знают верный секрет (pre\_master\_secret).

# **Программное обеспечение**

Все компьютеры под управлением ОС Windows 8.1

Так же для обеспечения безопасности на каждом компьютере установлен антивирус Avast

# **Оборудование**

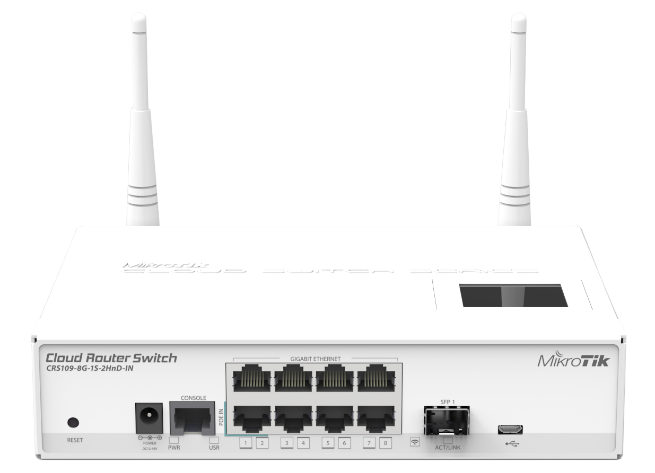
* **CRS125-24G-1S-2HnD-IN**

CRS125-24G-1S-2HnD-IN - это L3-коммутатор, функционирующий под управлением стандартной RouterOS v6 L5. Также может работать как беспроводная 2.4GHz 802.11n MIMO 2x2 1000mW точка доступа с антеннами 4dbi. Оснащен сенсорным экраном LCD, возможно подключение USB 3G/4G модема



* **CRS109-8G-1S-2HnD-IN**

CRS109-8G-1S-2HnD-IN - это L3-коммутатор, функционирующий под управлением стандартной RouterOS v6 L5. Также может работать как беспроводная 2.4 ГГц 802.11n MIMO 2x2 1000mW точка доступа с антеннами 2.5 dbi. Оснащен сенсорным экраном LCD, возможно подключение USB 3G/4G модема.



* **D-Link DGS-1510-20/A1A**

Стекируемый гигабитный коммутатор SmartPro с 16 портами 10/100/1000Base-T + 2 портами Gigabit SFP и 2 портами 10G SFP+.

DGS-1510-20/A1A

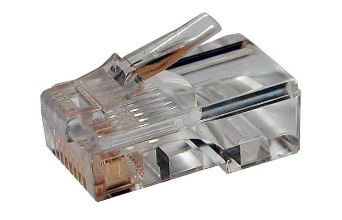
* **TP-Link PrintServer TL-PS310U**

Принт-сервер для МФУ с функцией хранения данных TL-PS310U идеален для организации совместного доступа к USB-устройствам домашней или рабочей сети. Устройство совместимо с большинством принтеров и многофункциональных принтеров, представленных на рынке, и позволяет совместно использовать и управлять этими устройствами с подключенных к сети компьютеров. К устройству также можно подключать и работать с 4 устройствами на базе USB, такими как сканеры, карты флэш-памяти, колонки или веб-камеры с помощью USB дока, подключенного к серверу. Эти устройства будут доступны из любой точки сети и даже по беспроводному соединению, если принт-сервер подключить к беспроводному маршрутизатору.



* **Витая пара CAT6 RJ45**Применяется в сетях [Fast Ethernet](https://ru.wikipedia.org/wiki/Fast_Ethernet" \o "Fast Ethernet) и [Gigabit Ethernet](https://ru.wikipedia.org/wiki/Gigabit_Ethernet" \o "Gigabit Ethernet), состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с на расстояние до 55 м. Большинство компьютеров и ноутбуков имеют разъем для коннектора RJ45, через который подключается кабель.



* **Коннектор RJ45**для подключения кабелей витой пары.  
  ****
* **Инструмент T-210/НТ-210С/HT-210N для обжима коннекторов RJ-45  
  **

# **Приблизительные затраты на создание сети**

|  |  |  |
| --- | --- | --- |
| **Наименование** | **Количество** | **стоимость** |
| инструмент для обжима | 1 шт. | 20$ |
| Сетевой кабель витая пара CAT6 RJ 45 40м. | 1 шт. | 20$ |
| коннекторов RJ45 | 110 шт. | 5$ |
| DGS-1510-20/A1A | 2 шт. | 250$ |
| CRS125-24G-1S-2HnD-IN | 1 шт. | *305$* |
| CRS109-8G-1S-2HnD-IN | 1 шт. | *230* |
| TP-Link PrintServer TL-PS310U | 1 шт. | *50$* |
| *Итого:* |  | *1675$* |