1. **Понятие, цель и задачи сетевого администрирования.**

*Сетевое администрирование* – управление ресурсами и инфраструктурой сети для обеспечения эффективного, надежного и безопасного доступа к её ресурсам.

Цель создания любой компьютерной сети – предоставление доступа к её ресурсам.

Виды ресурсов:

* + данные (файлы и папки)
  + устройства (принтеры, сканеры, модемы)
  + вычислительные возможности, обеспечиваемые процессорами

Группы задач сетевого администрирования:

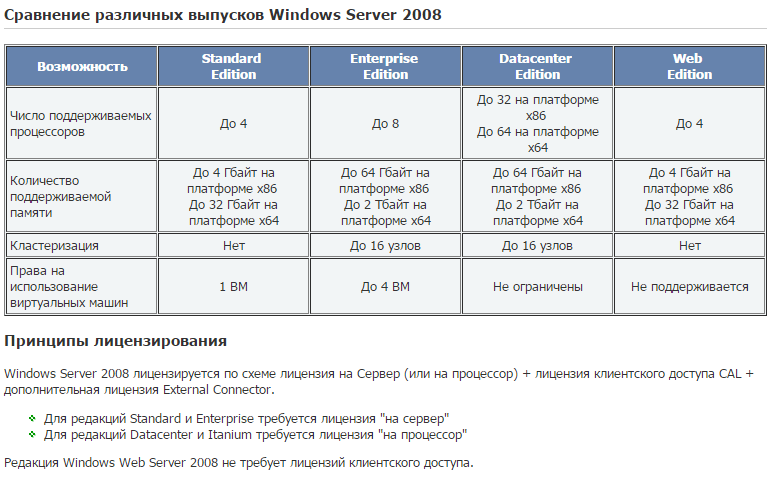
* задачи планирования (продуманная организация всех её компонентов, предусмотреть возможность расширения на 30-50%)
* задачи установки и настройки программного и аппаратного обеспечения
* задачи управления безопасностью (контроль доступа и сохранение целостности всех данных, сюда входит резервное копирование данных, разработка политики безопасности аккаунтов пользователей, использование защищенной коммуникации и др.)
* задачи управления производительностью (речь идет о предоставлении статистической информации о работе сети за указанный отрезок времени. Делается это с целью минимизации затрат ресурсов и энергии, а также с целью планирования ресурсов на будущие нужды)



1. **Семейства операционных систем Windows Server 2008.**

Версии Microsoft Windows Server 2008:

* Windows Server 2008 Standard Edition (стандартная версия)
* Windows Server 2008Enterprise Edition (корпоративная версия)
* Windows Server 2008Datacenter Edition (версия для центра обработки данных)
* Windows Server 2008 Web Edition  
  (версия для web-узлов)

 [1] Каждому пользователю или устройству, которые обращаются к серверу, требуются лицензии клиентского доступа (Client Access Licenses, CAL). См. Product Use Rights («Права на использование продукта») для получения более подробной информации.

1. **Инструменты администрирования.**

* Графические инструменты
  + *Диспетчер серверов* управление несколькими удаленными серверами с помощью единой консоли диспетчера серверов.
  + *Консоль управления Microsoft (Microsoft Management Console, MMC)* представляет собой унифицированную среду для выполнения административных задач. Администратор, имея в распоряжении такую среду, может помещать в неё одну или несколько утилит, называемых *оснастками* (snap-in), для решения текущей проблемы. Консоль управления позволяет одинаково отображать любые оснастки и использовать для управления ими похожие приемы. Смысл применения консоли управления в том, чтобы сделать среду выполнения административных утилит единообразной и удобной
  + *Административные мастера* представляют собой программы, которые проводят администратора по всем этапам решения какой-либо задачи. На каждом этапе возможен выбор одного или нескольких способов решения или параметров настройки. Часто также мастера предоставляют возможность выбора параметров по умолчанию. Использование мастеров позволяет сократить время установки и настройки компонентов операционной системы или время решения другой административной задачи. Кроме того, параметры по умолчанию чаще всего обеспечивают вполне работоспособный режим, хотя, возможно, и не самый эффективный.
* *Утилиты командной строки* являются самыми старыми инструментами администрирования, ведущими свою историю от первых операционных систем без графического интерфейса. В то время альтернативы утилитам командной строки не было. Сегодня большинство задач управления можно решить без использования утилит, однако многие администраторы считают, что утилиты командной строки удобнее графического интерфейса. Кроме того, такой вид утилит, как утилиты диагностики стека протоколов TCP/IP, не имеют стандартного графического аналога.
* *Windows PowerShell* позволяет автоматизировать массу разнообразных задач. С его помощью можно управлять файлами, службами, процессами, аккаунтами и настройками. Язык PowerShell понимает многие команды из обычной Командной строки Windows (CMD), но он имеет и свой собственный язык, состоящий из собственных команд, которые здесь называются командлетами.

Выбор инструмента обусловливается, в основном, личными предпочтениями системного администратора.

1. **Система доменных имен. Записи о ресурсах.**

Система DNS основана на иерархической древовидной структуре, называемой *пространством доменных имен*. Доменом является каждый узел и лист этой структуры. На рис. 5.1 приведен фрагмент пространства доменных имен Интернета.

Самый верхний домен называется *корневым* (root domain). Корневой домен как реальный узел не существует, он исполняет роль вершины дерева. Непосредственные его потомки (поддомены) – домены первого уровня TLD (Top-Level Domain – домены верхнего уровня). Их можно разделить на три группы:

* **.arpa** – особый домен, используемый для преобразования IP-адресов в доменные имена (обратное преобразование). Содержит единственный дочерний домен – **in-addr**;
* домены организаций – **.com** (коммерческие организации), **.org** (некоммерческие организации), **.edu** (образовательные учреждения) и т. д.;
* домены стран (географические домены) – **.ru** (Россия), **.fr** (Франция), **.de** (Германия) и т. д.

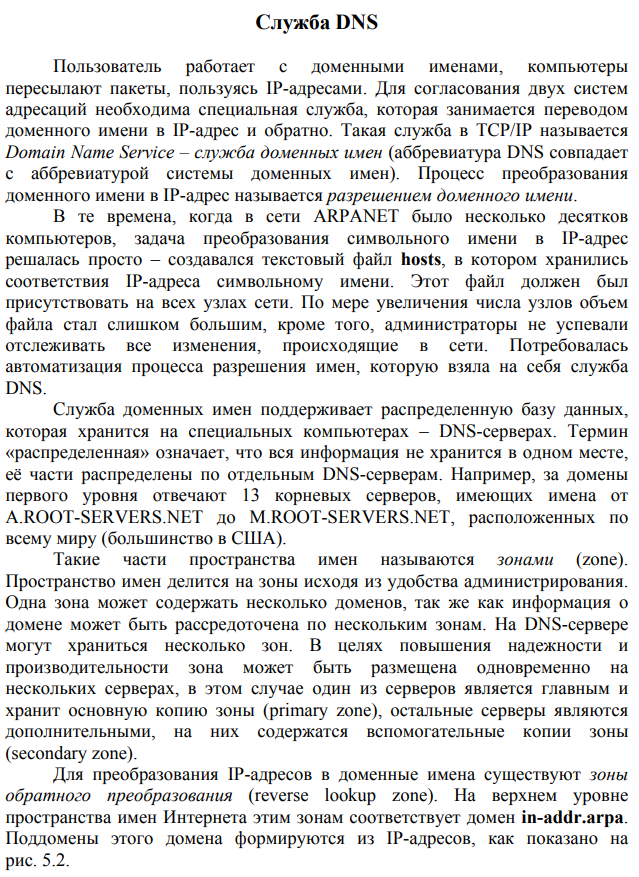


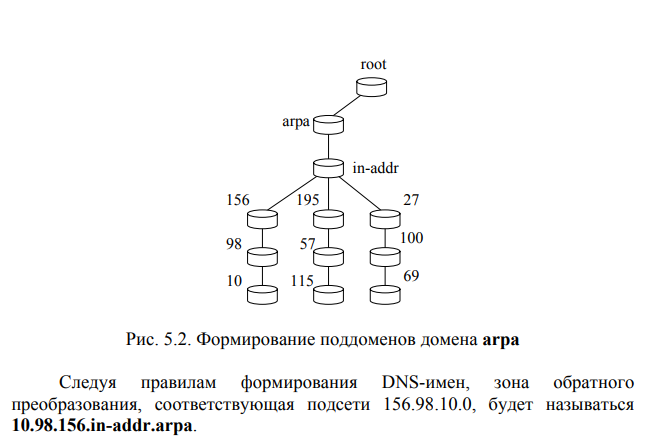
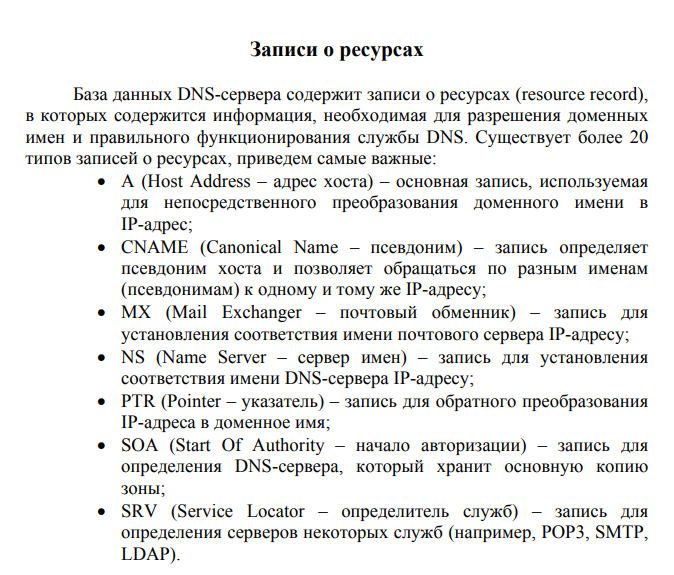
Домены первого уровня включают только домены второго уровня, записи об отдельных хостах могут содержаться в доменах, начиная со второго уровня.

Созданием и управлением доменами первого уровня с 1998 года занимается международная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers – Корпорация Интернет по присвоению имен и адресов, www.icann.org). Домены второго уровня, находящиеся в географических доменах, распределяются специальными национальными организациями, которым ICANN передало полномочия в этом вопросе. Управлением доменами третьего и следующего уровней занимаются владельцы соответствующих доменов второго уровня.

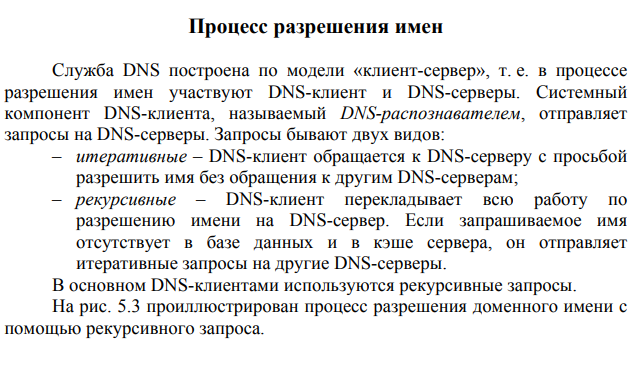
Полностью определенное доменное имя FQDN записывается следующим образом. Сначала идет имя хоста (лист в дереве пространства имен), затем через точку следует DNS-суффикс – последовательность доменных имен всех уровней до первого включительно. Запись оканчивается точкой, после которой подразумевается корневой домен. Пример FQDN для хоста www домена vshu: [www.vshu.kirov.ru](http://www.vshu.kirov.ru).

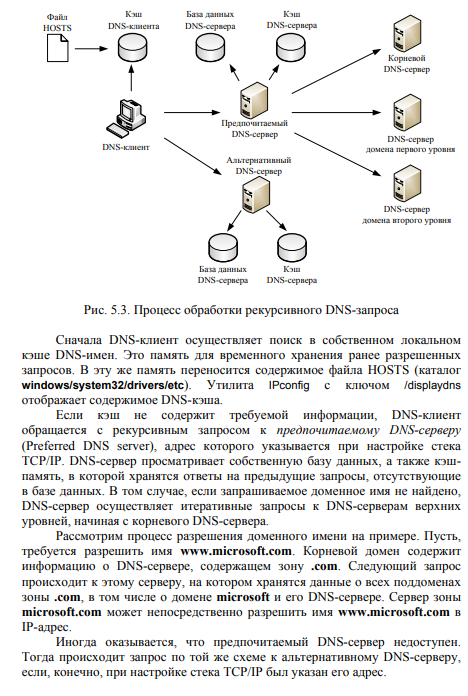
В этой записи www – имя хоста, vshu.kirov.ru. – DNS-суффикс. Точку в конце FQDN обычно можно опускать.

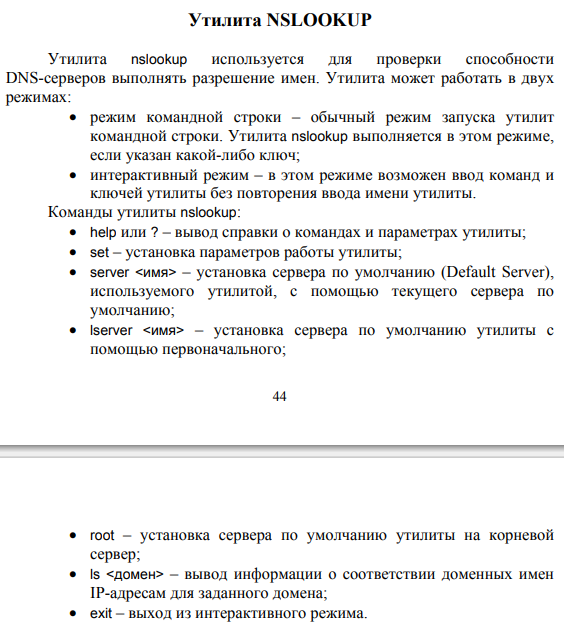


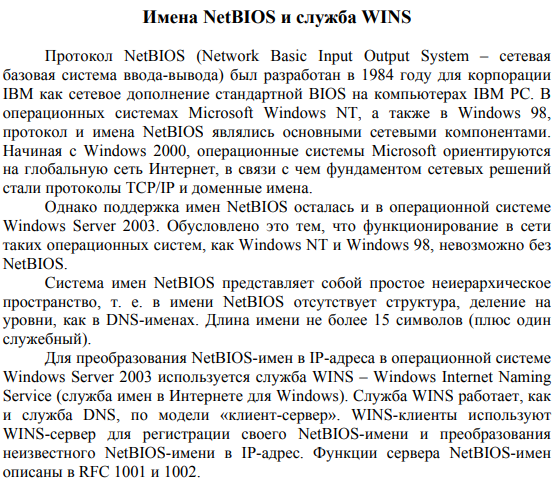
1. **Процесс разрешения имен. Утилита NSLOOKUP.**



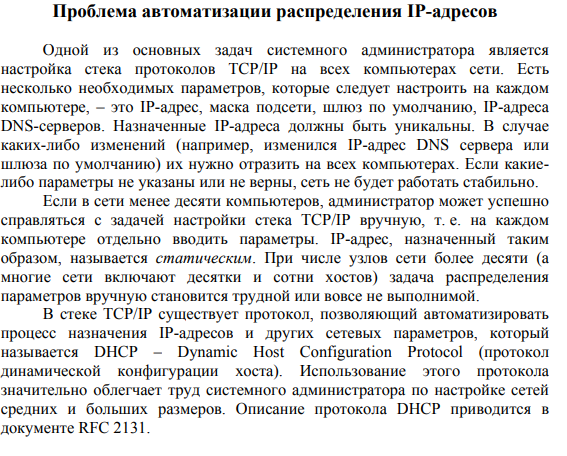


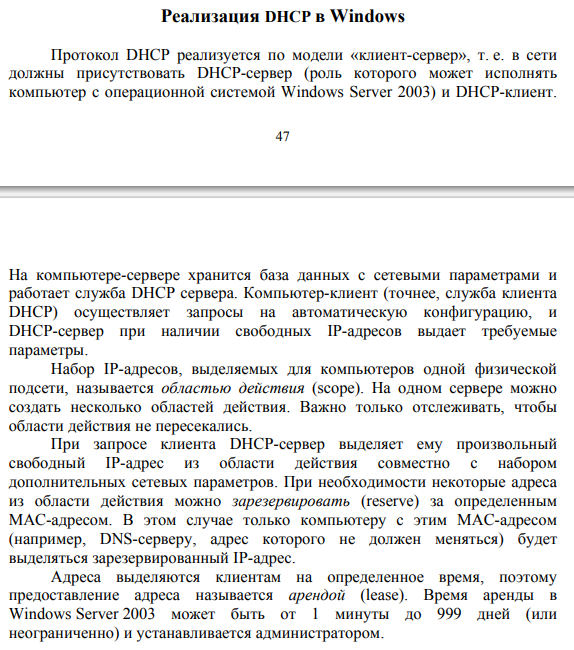


1. **Имена NetBIOS и служба WINS.**

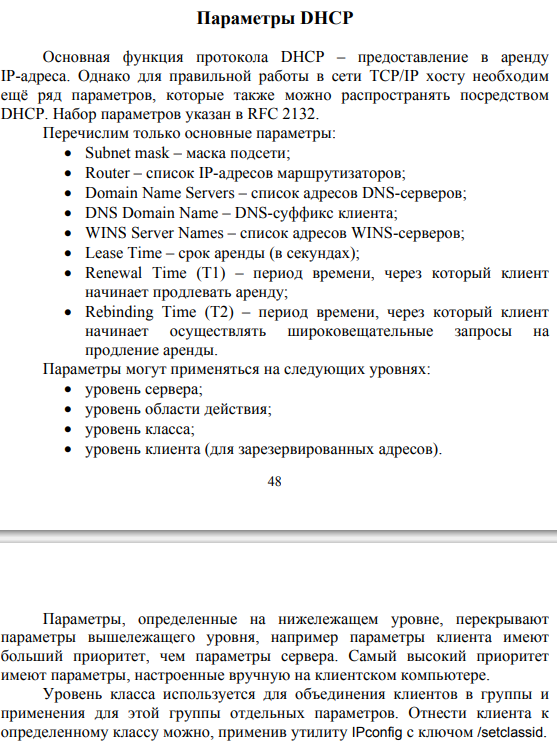


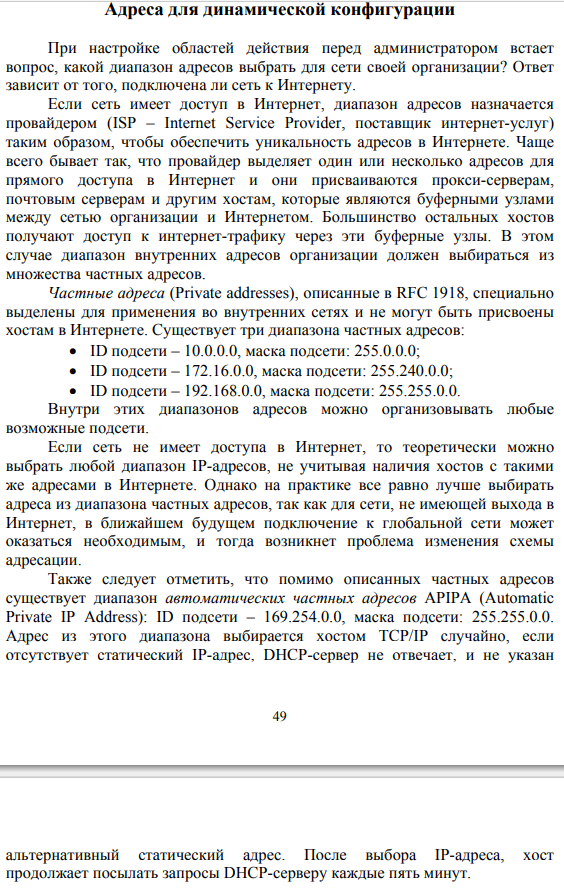
1. **Реализация DHCP в Windows. Параметры DHCP. Адреса для динамической конфигурации.**





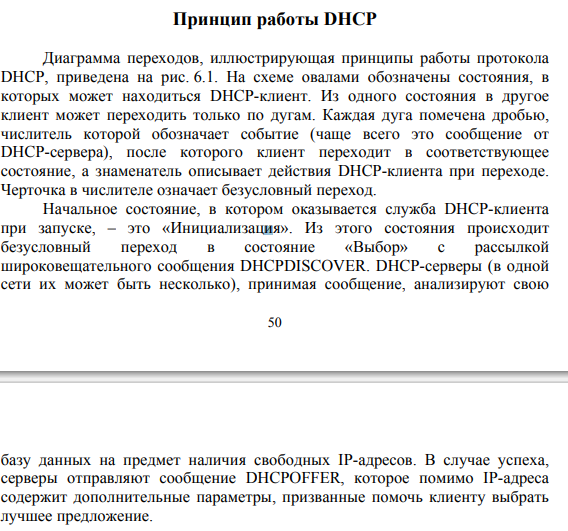
\*Администратор должен следить за отсутствием пересечений (сама служба не следит).



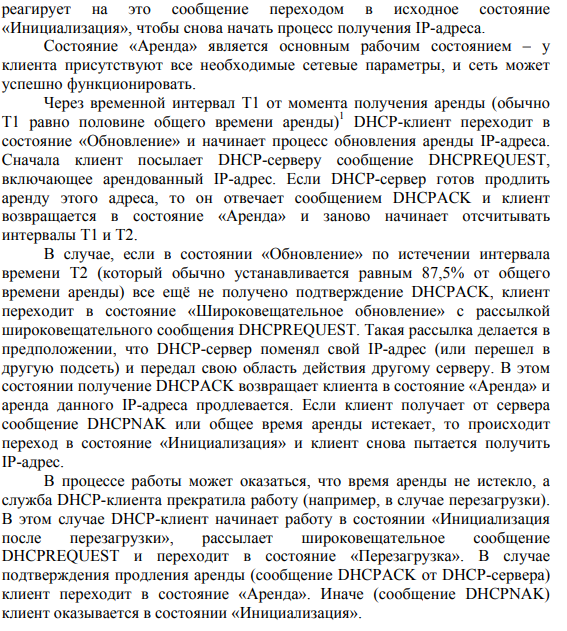


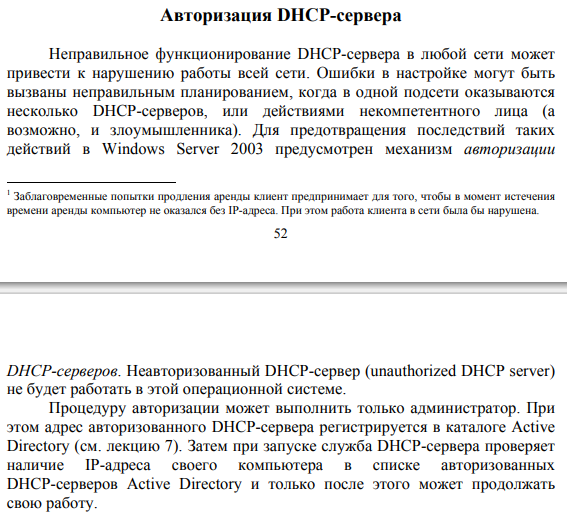
1. **DHCP-сообщения. Принцип работы DHCP. Авторизация DHCP-сервера.**





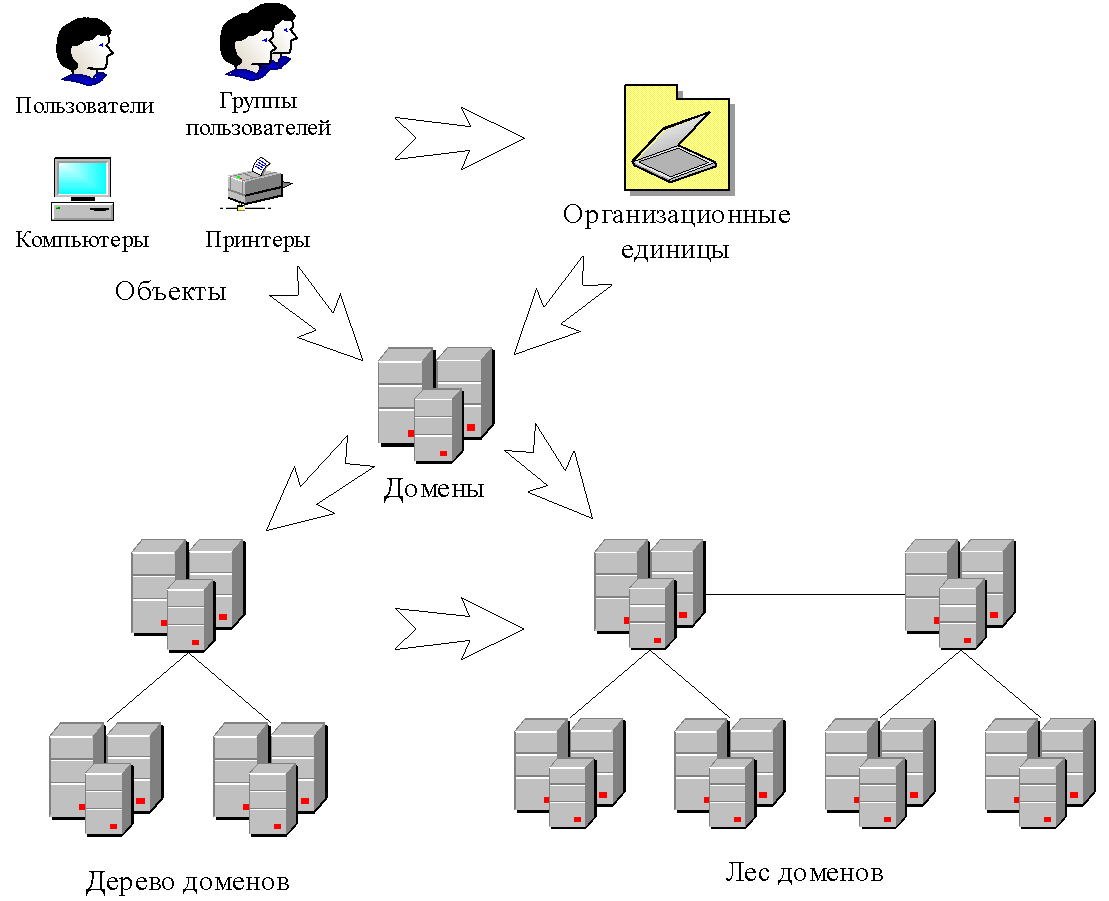






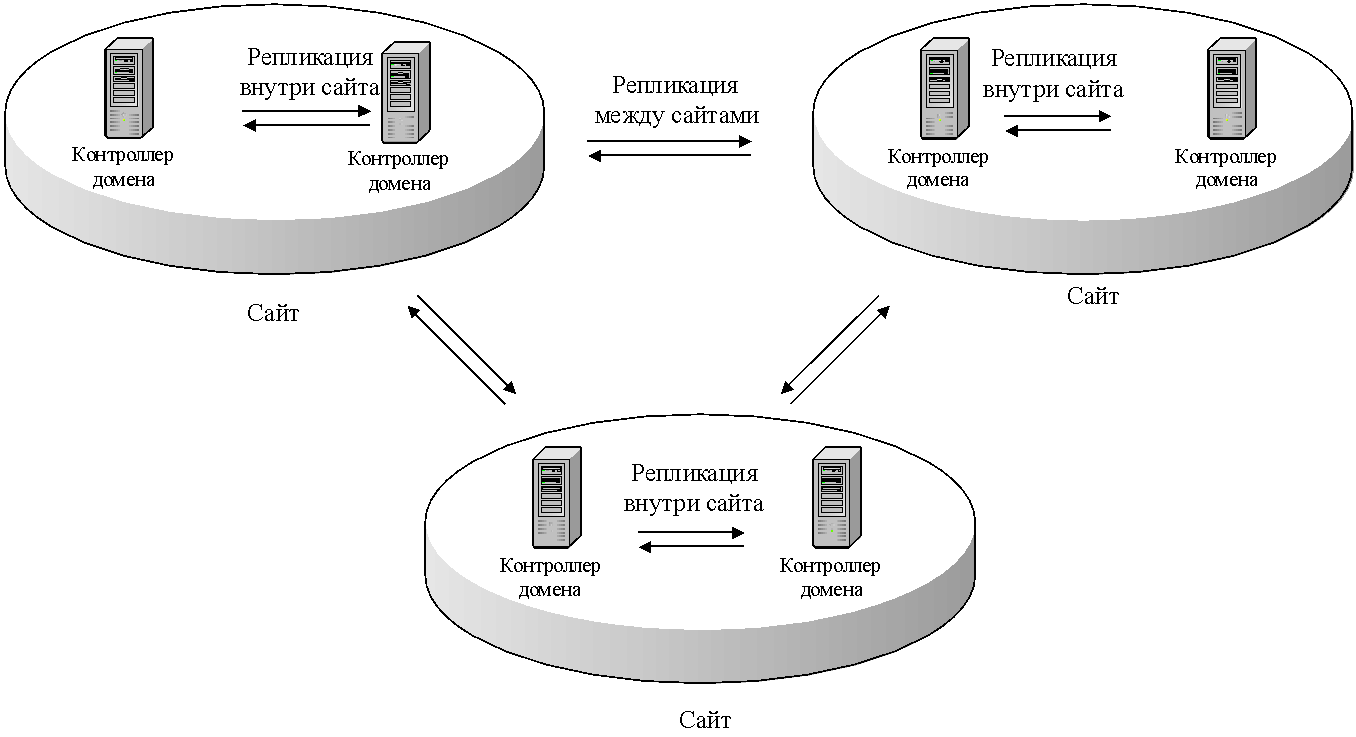
1. **Понятие Active Directory. Структура каталога Active Directory. Объекты каталога и их именование.**

**Active** **Directory** — это иерархически организованное хранилище данных об **объектах** сети, обеспечивающее удобные средства для поиска и использования этих данных.



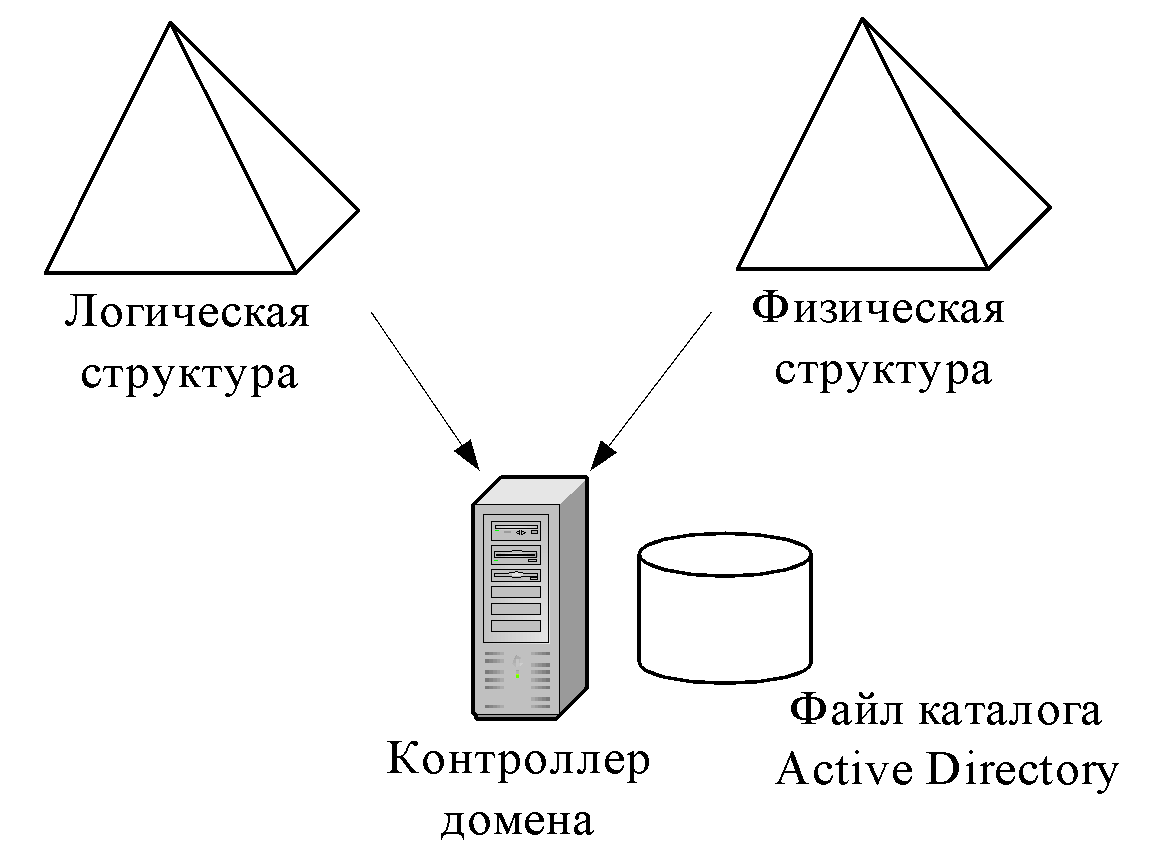
*Логическая*

*структура*



*Физическая*

*структура*



**Ntds.dit** состоит из нескольких разделов:

* *раздел домена* (domain partition)
* *раздел схемы* (schema partition)
* *раздел конфигурации* (configuration partition)
* *раздел приложений* (application partition)
* *раздел глобального каталога*(global catalog partition)

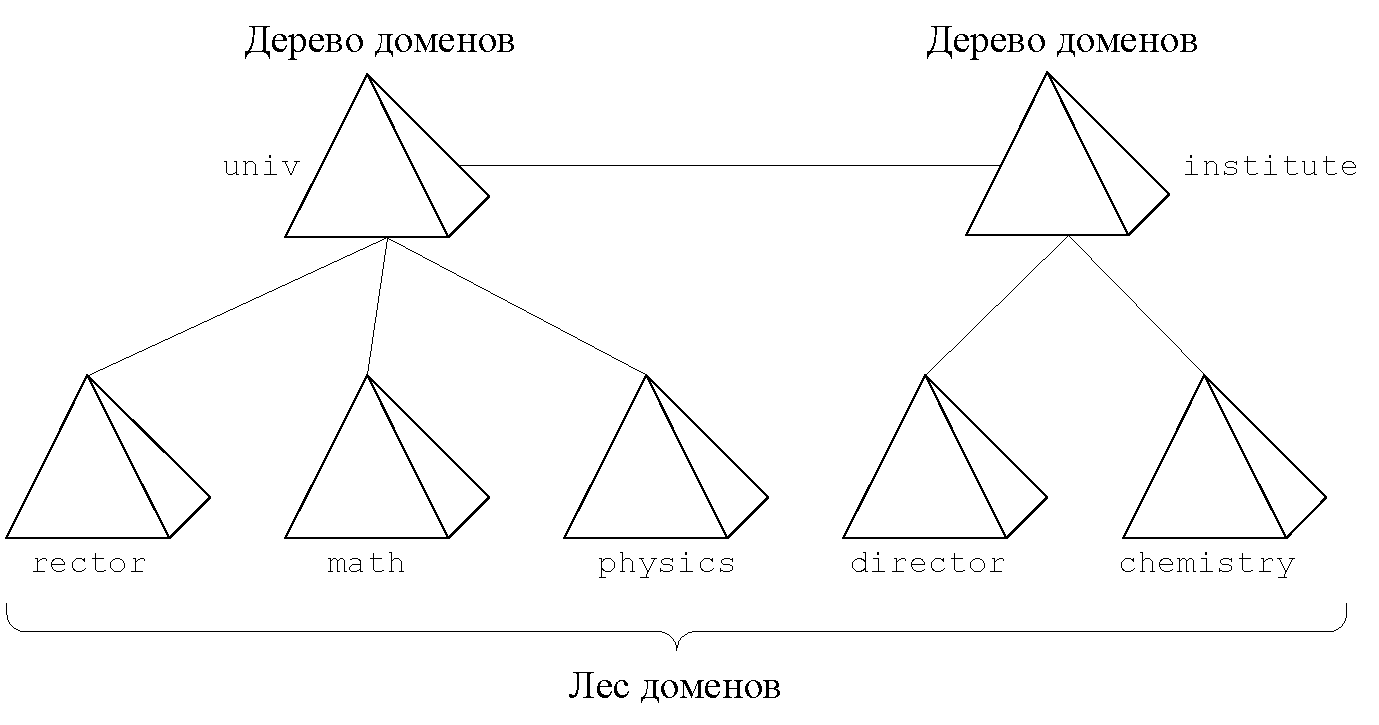
Основные типы объектов каталога Active Directory, не являющихся контейнерами:

* пользователь (user)
* группы пользователей (group)
* контакты (contact)
* компьютеры (computer)
* принтеры (printer)
* общедоступные папки (shared folder)

Способы именования объектов в Active Directory:

* *Различающееся имя* (Distinguished Name, DN)
  + DC (Domain Component) – домен
  + OU (Organizational Unit) – организационное подразделение
  + CN (Common Name) – общее имя
  + Пример:  
    **DC = ru, DC = faculty, OU = teachers, CN = users, CN = petrov**
* *Относительное различающееся имя   
  (Relative Distinguished Name, RDN)*
  + Пример: **CN = petrov**
* *Основное имя пользователя* (User Principal Name, UPN)
  + Пример: **petrov@faculty.ru**
* *Глобальный уникальный идентификатор*(Global Unique Identifier, GUID)

1. Иерархия доменов. Доверительные отношения. Организационные подразделения.



* *Аутентификация* (authentication)
* *Авторизация* (authorization)

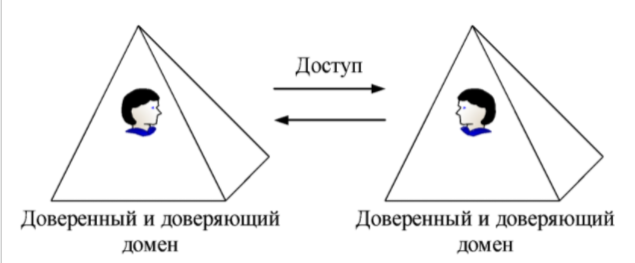
Для доступа к ресурсам другого домена между доменами должны быть установлены *доверительные отношения* (trust relationship).

Виды доверительных отношений:

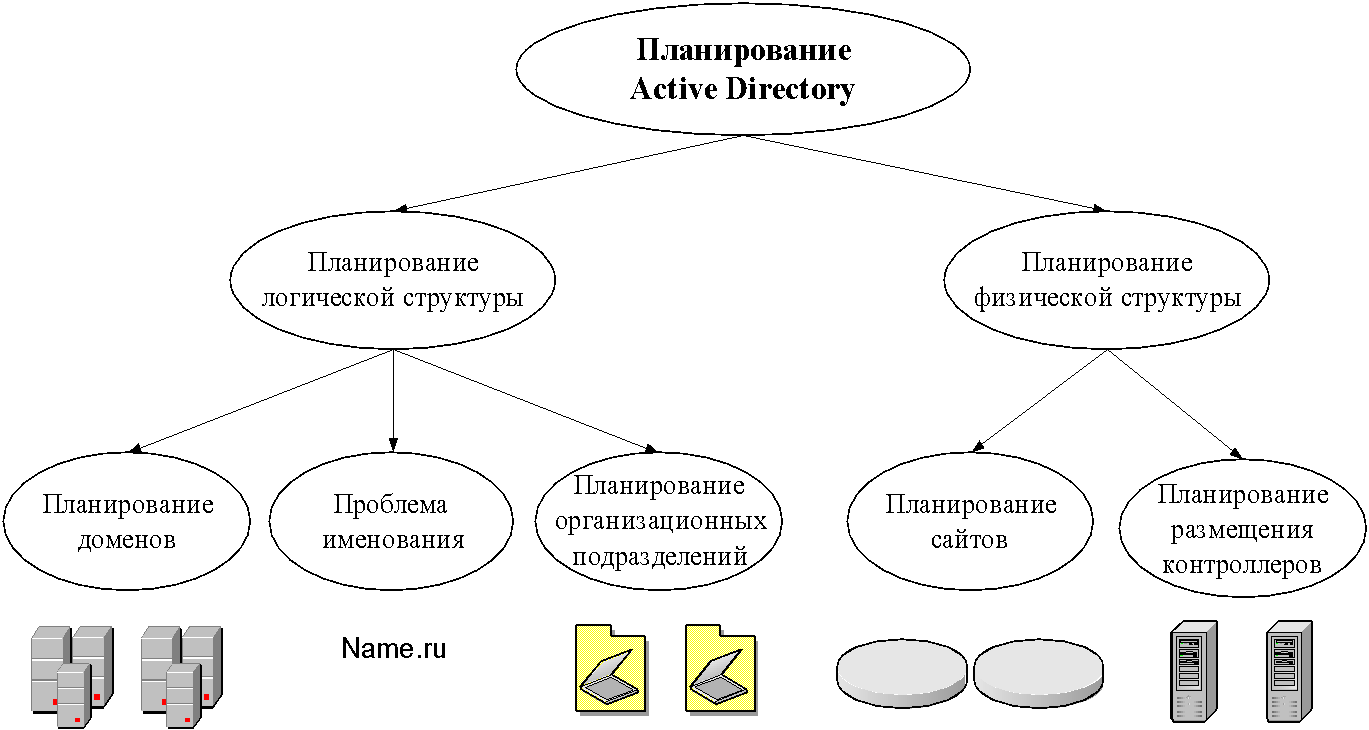
* *односторонние* (one-way trust relationship)
* *двусторонние* (two-way trust relationship) –

Изображение выглядит как легкий, темный

Автоматически созданное описание

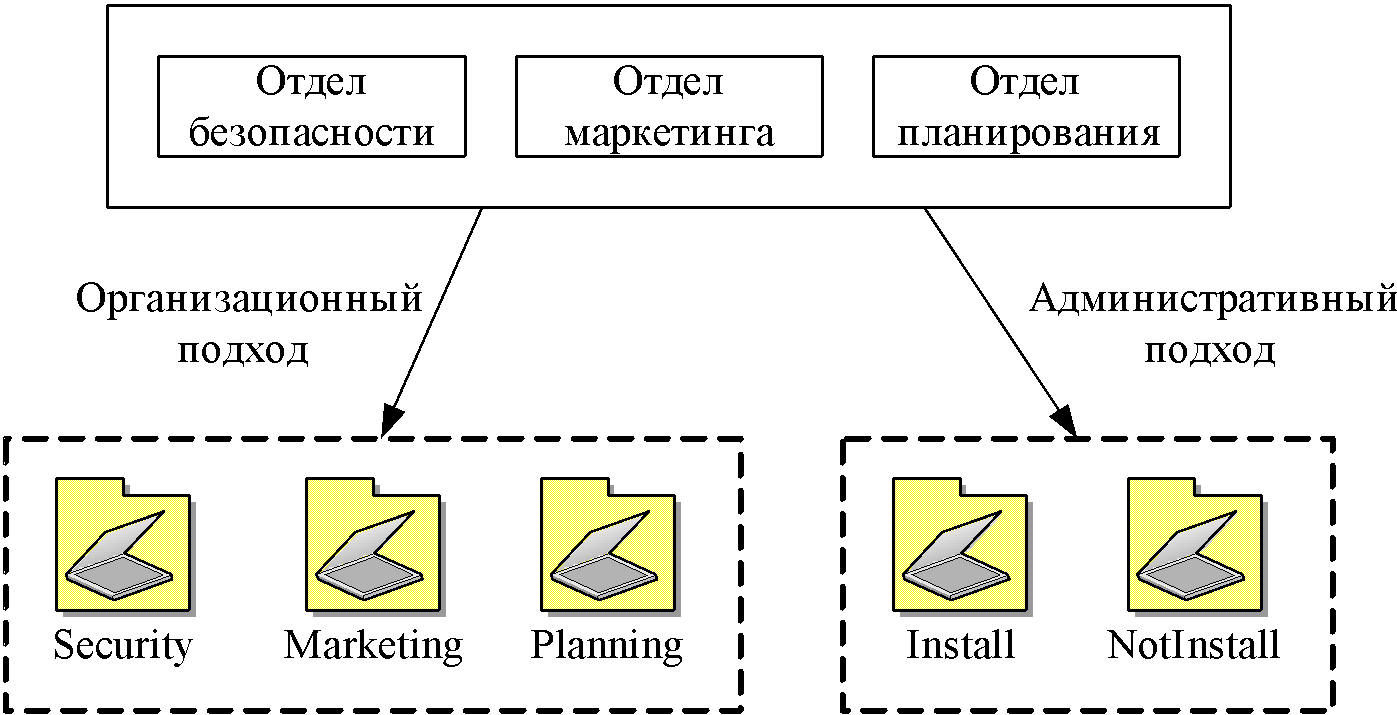


1. **Планирование логической и физической структуры каталога Active Directory.**



Признаки, по которым выбирается вариант  
*с одним доменом*:

* в организации менее миллиона пользователей
* отсутствие удаленных филиалов
* относительная стабильность структуры организации
* отсутствие потребности в разных доменных именах
* централизованный способ администрирования
* единая политика безопасности



1. Учетные записи. Группы пользователей. Групповые политики.

*Права пользователя* – это список действий, которые может выполнять пользователь.

Виды прав:

* привилегия (privilege)
* право на вход в систему (logon right)
* разрешение доступа (access permission)

Изображение выглядит как текст, телевидение, экран, темный

Автоматически созданное описание

Области действия групп пользователей:

* доменная локальная   
  (domain local scope)
* глобальная (global scope)
* универсальная (universal scope)
* *Групповые политики* (group policy) – способ автоматизации работы по настройке рабочих столов пользователей и параметров компьютеров.
* Групповые политики представляют собой наборы правил конфигурирования, применяемых к компьютеру или пользователю. Каждый такой набор правил называется *объектом групповой политики* (Group Policy Object, GPO).

Один или несколько объектов групповой политики могут применяться к трем видам объединений:

* сайтам
* доменам
* организационным подразделениям

Для каждого компьютера может быть определен *объект локальной групповой политики*(Local Group Policy Object, LGPO).

Основные части объекта групповой политики:

* **Конфигурация компьютера**(Computer Configuration)
* **Конфигурация пользователя**(User Configuration)

**Каждая из этих частей содержит разделы:**

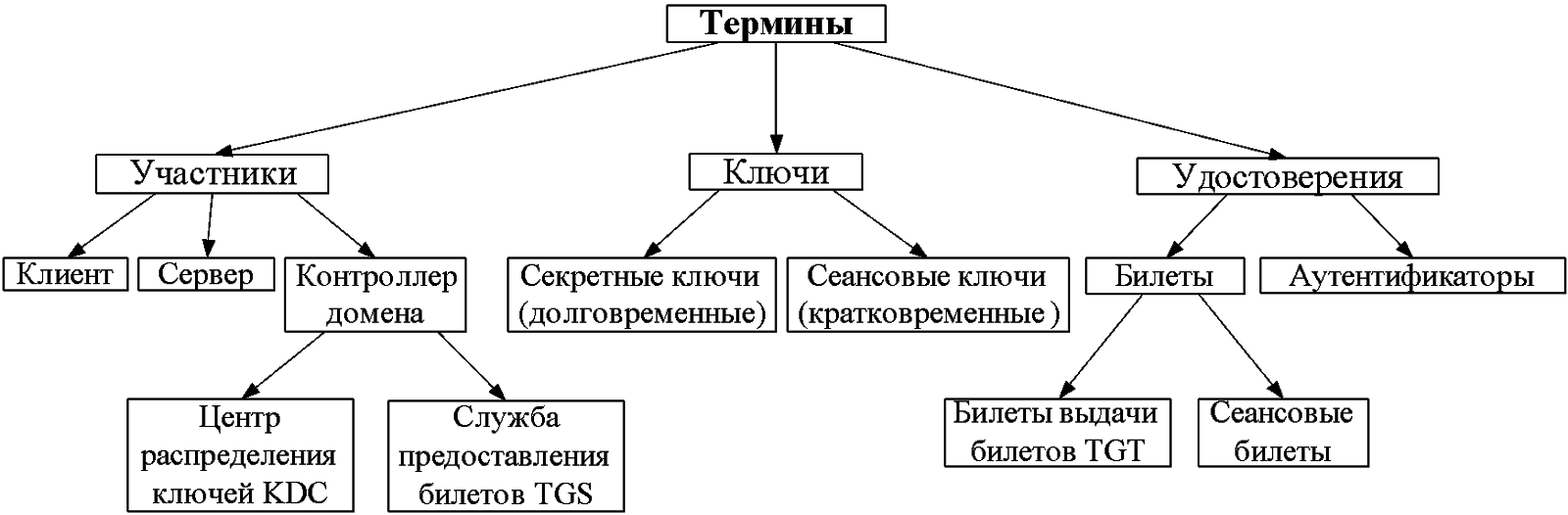
* **Настройки приложений** (Software Settings)
* **Настройки Windows** (Windows Settings)

**Административные** **шаблоны**(Administrative Templates)

1. **Средства сетевой безопасности Windows Server. Протокол аутентификации Kerberos. Термины, используемые в протоколе Kerberos. Основные этапы аутентификации в протоколе Kerberos.**

* Основной метод аутентификации в Windows Server –  протокол Kerberos v5.
* Также поддерживается протокол NTLM (NT LAN Manager).
* Для защищенной передачи сообщений наиболее надежным и перспективным считается протокол IPsec.
* Начало 80-х гг., Массачусетский технологический институт (Massachusetts Institute of Technology, MIT)
* RFC 1510

Для шифрования применяется алгоритм DES   
(Data Encryption Standard – стандарт шифрования данных)



Термины, используемые   
в протоколе Kerberos

Изображение выглядит как стол

Автоматически созданное описание

Изображение выглядит как стол

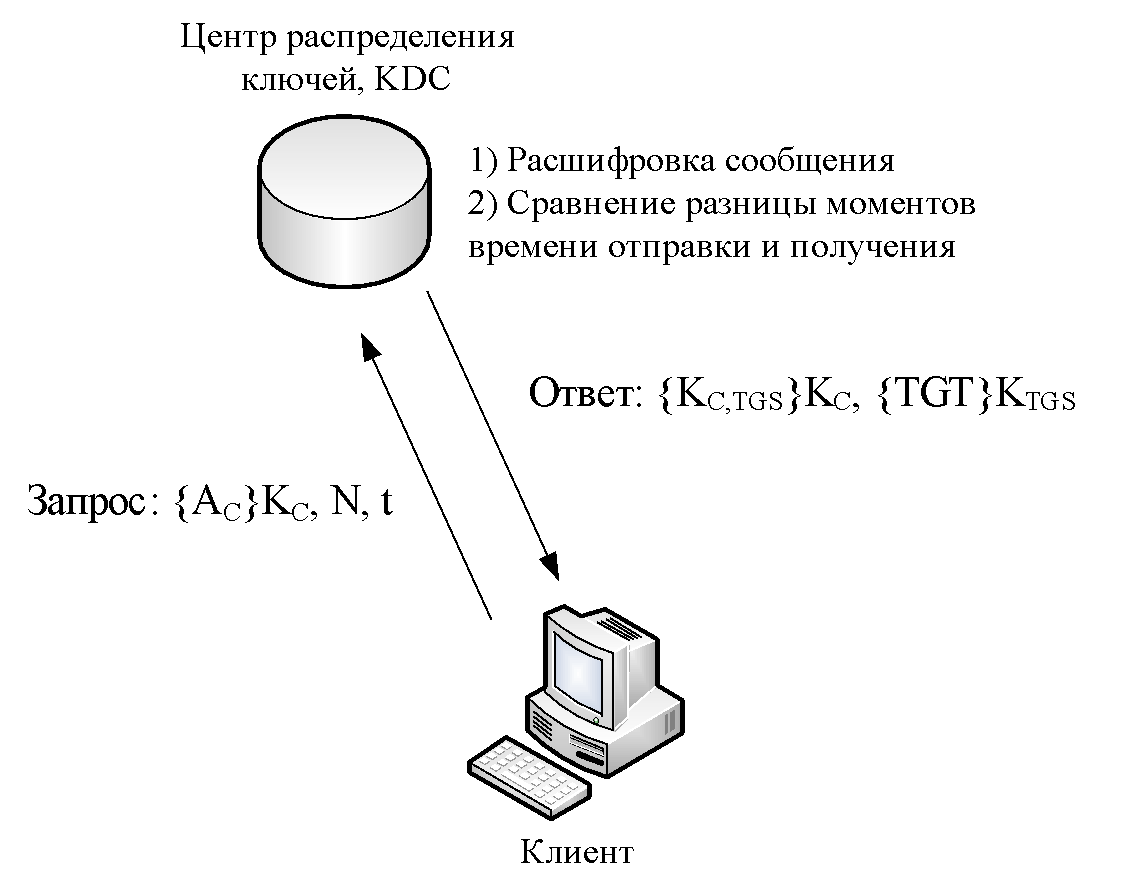
Автоматически созданное описание

Основные этапы аутентификации

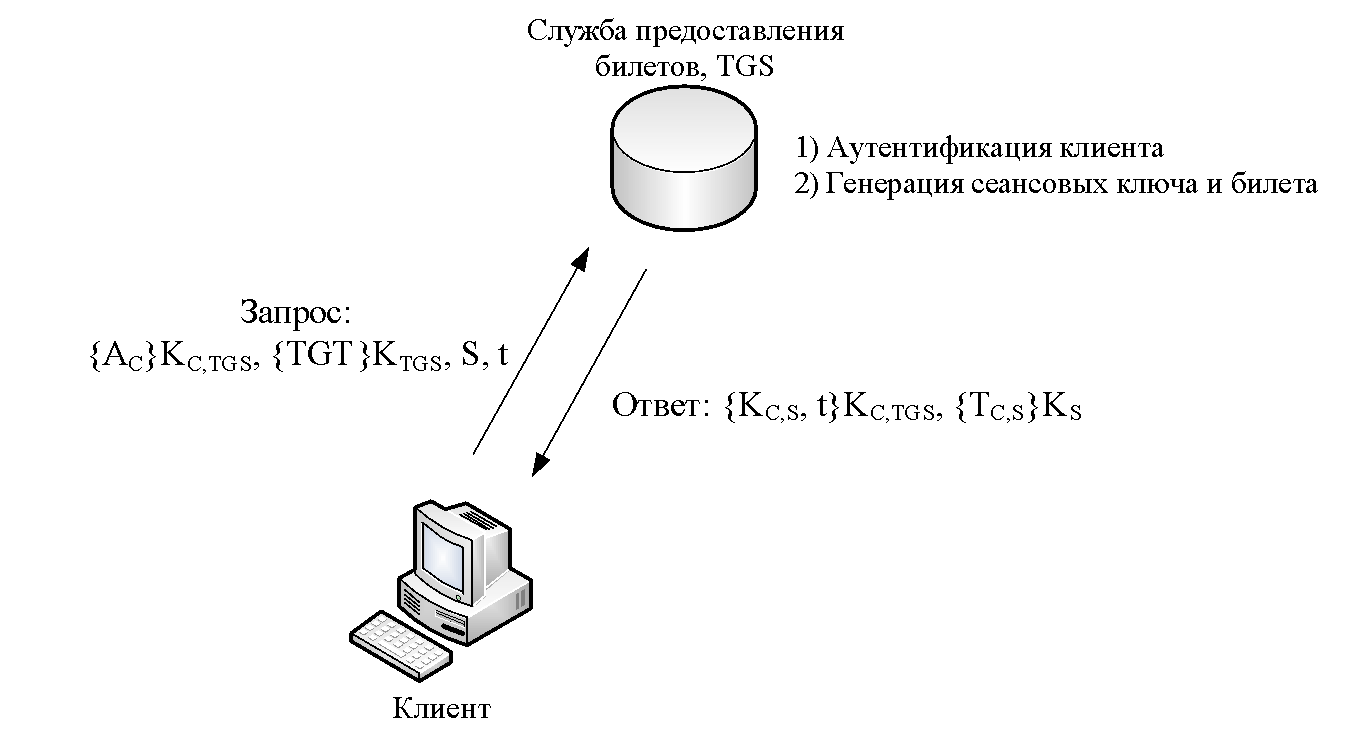
Изображение выглядит как текст

Автоматически созданное описание

Этап регистрации клиента



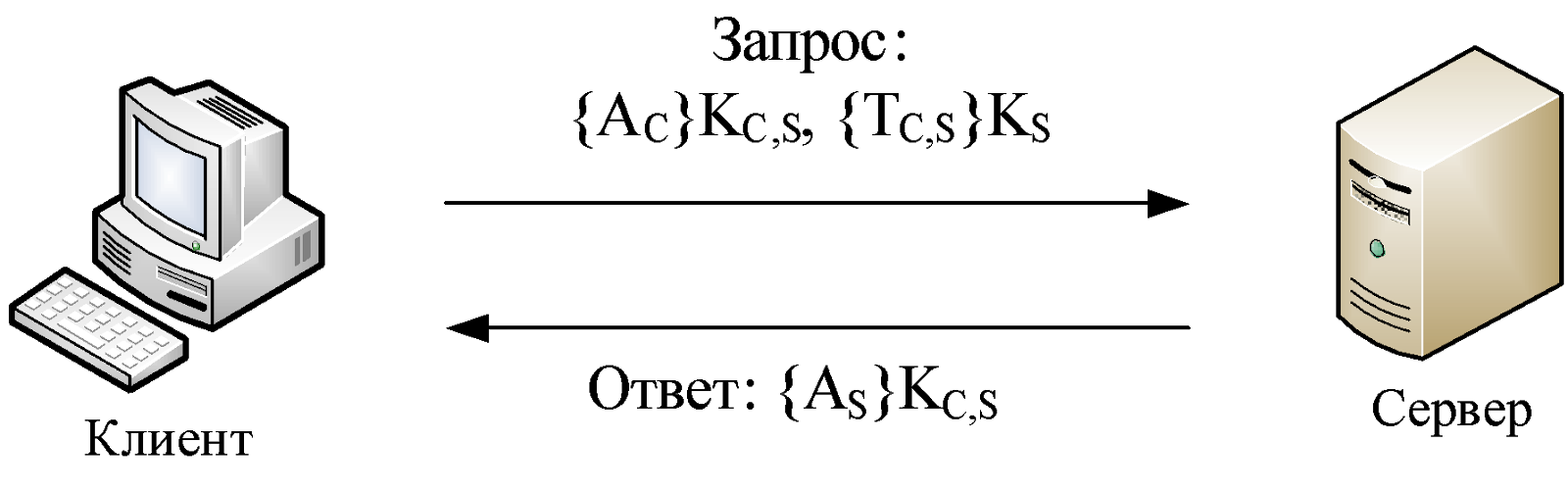
Этап получения   
сеансового билета



Этап получения   
сеансового билета

Сеансовый билет TC,S содержит следующие данные:

* имя сервера
* имя клиента
* сеансовый ключ
* время начала действия билета
* время окончания действия билета
* список возможных сетевых адресов клиента
* Этап доступа к серверу



**Средства шифрования Kerberos**

* Алгоритм шифрования DES
* Используются
  + AES256-CTS-HMAC-SHA1-96
  + AES128-CTS-HMAC-SHA1-96
  + RC4-HMAC

PKINIT

В июне 2006 года был представлен [RFC 4556](https://tools.ietf.org/html/rfc4556) описывающий расширение для 5-й версии под названием PKINIT

* Пользователь идентифицируется в системе и предъявляет свой закрытый ключ.
* Клиентская машина формирует запрос на СА (AS\_REQ), указывает, что будет использоваться асимметричное шифрование. Запрос подписывается и, кроме стандартной информации, содержит сертификат открытого ключа пользователя.
* KDC проверяет достоверность сертификата пользователя, а затем электронную подпись. После этого KDC проверяет локальное время, присланное в запросе.
* KDC формирует ответ (AS\_REP), в котором сеансовый ключ зашифровывается открытым ключом пользователя. Кроме того, ответ содержит сертификат KDC и подписывается его закрытым ключом.
* Получив ответ, пользователь проверяет подпись KDC и расшифровывает свой сеансовый ключ.

1. Протокол IPsec. Функции протокола IPsec. Протоколы AH, ESP и IKE.

* 1994 г., Совет по архитектуре Интернета (Internet Architecture Board, IAB), RFC 1636 «*Report of IAB Workshop on Security in the Internet Architecture* » – «Отчет семинара IAB по безопасности в архитектуре Интернета»

*IPsec* (IP Security – безопасность IP),   
RFC 2401-2412

Функции протокола IPsec

* аутентификация
* целостность
* конфиденциальность
* распределение секретных ключей

Основные протоколы:

* AH (Authentication Header   
  – заголовок аутентификации)
* ESP (Encapsulating Security Payload   
  – инкапсуляция зашифрованных данных)
* IKE (Internet Key Exchange   
  – обмен ключами Интернета)

Изображение выглядит как текст

Автоматически созданное описание

Протоколы AH и ESP

Протокол AH (RFC 2402) снабжает пакет IPsec своим незашифрованным заголовком, который обеспечивает:

* аутентификацию исходных данных
* целостность данных
* защиту от дублирования уже полученных данных

Задачи протокола ESP (RFC 2406):

* обеспечение аутентификации и целостности исходных данных
* защита от дублирования пакетов
* предоставление средств обеспечения конфиденциальности данных при помощи алгоритмов шифрования (DES и 3DES)

Протокол IKE  
Протокол IKE (RFC 2409) основан на двух протоколах:

* ISAKMP (Internet Security Association and Key Management Protocol – протокол межсетевой ассоциации защиты и управления ключами)
* протокол определения ключей Оакли   
  (Oakley Key Determination Protocol),   
  RFC 2412, метод обмена ключами Диффи-Хэллмена (Diffie-Hellman)

1. **Удаленный доступ. Виды коммутируемых линий. Протоколы удаленного доступа. Протоколы аутентификации.**

Виды удаленного доступа:

* соединение по коммутируемой линии (dial-up connection)
* соединение с использованием виртуальных частных сетей   
  (Virtual Private Networks, VPN)
* *Клиент удаленного доступа*
* *Сервер удаленного доступа*(Remote Access Server, RAS)
* *Служба маршрутизации и удаленного доступа* (Routing and Remote Access Service, RRAS)

Виды коммутируемых линий

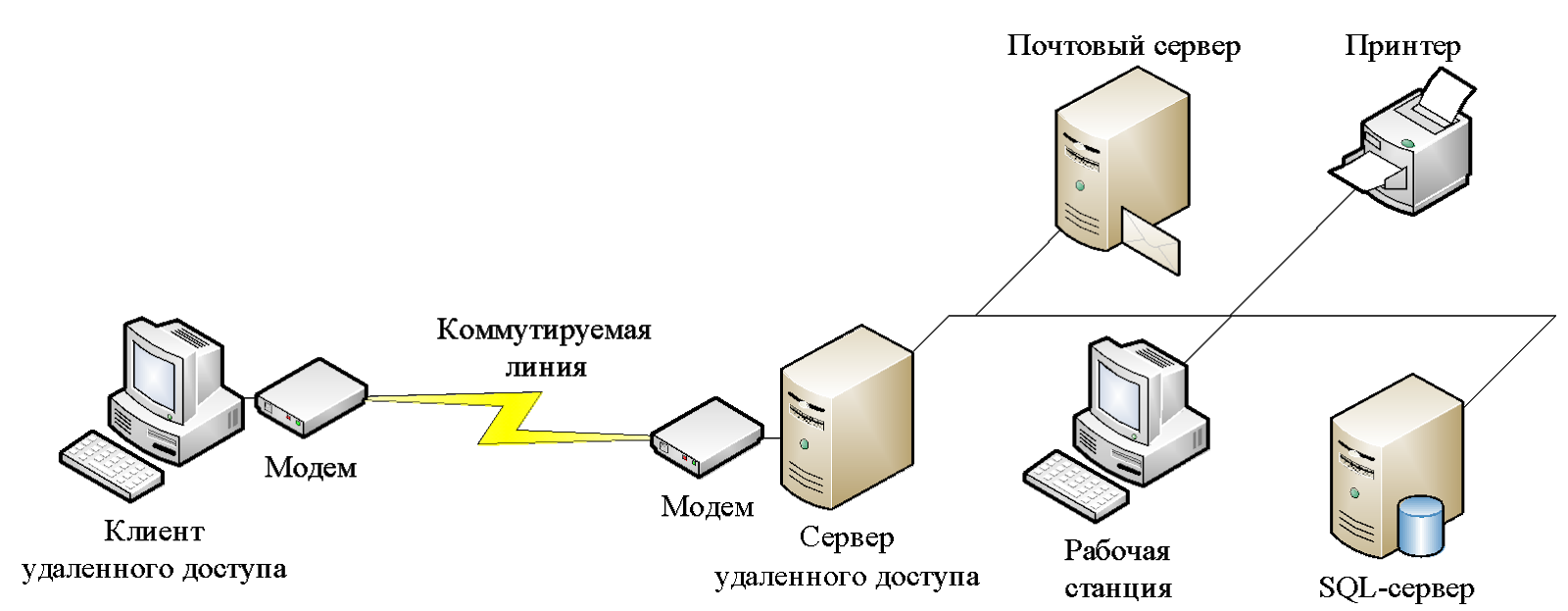
Коммутируемые линии:

* телефонные сети: 56,6 кбит/с
* сети ISDN (Integrated Services Digital Network – цифровая сеть с комплексными услугами): 128 кбит/с
* ATM поверх ADSL – передача трафика АТМ (Asynchronous Transfer Mode – асинхронный режим передачи) посредством линий ADSL   
  (Asymmetric Digital Subscriber Line –   
  асимметричная цифровая абонентская линия):  
  20 Мбит/с для входящего трафика  
  1 Мбит/с для исходящего трафика

Протоколы удаленного доступа

Основные этапы подключения клиента удаленного доступа:

* установка соединения
* аутентификация и авторизация клиента удаленного доступа
* сервер удаленного доступа выступает в роли маршрутизатора, предоставляя доступ клиенту к ресурсам локальной сети



* протокол SLIP (Serial Line Internet Protocol – межсетевой протокол для последовательного канала), RFC 1055
* протокол РРР (Point-to-Point Protocol – протокол соединения «точка-точка»),   
  RFC 1332, 1661 и 1662

Этапы установки соединения «точка-точка»:

1. Настройка параметров канального уровня.
2. Аутентификация клиента.
3. Обратный вызов (callback).
4. Настройка протоколов верхних уровней.
5. Протоколы аутентификации
6. PAP (Password Authentication Protocol) –   
   протокол аутентификации по паролю, RFC 1334
7. CHAP (Challenge Handshake Authentication Protocol) –   
   протокол аутентификации   
   с предварительным согласованием вызова,   
   MD-5, RFC 1994
8. MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) – реализация протокола CHAP, разработанная Microsoft,   
   MD-4, RFC 2433
9. MS-CHAP v2 – вторая версия протокола MS-CHAP,  
   MD-4, RFC 2759
10. EAP (Extensible Authentication Protocol) –   
    расширяемый протокол аутентификации, RFC 2284

**Основные понятия и виды виртуальных частных сетей. Протоколы виртуальных частных сетей.**

*Виртуальные частные сети* (Virtual Private Network, VPN) –защищенное соединение двух узлов через открытые сети.

*VPN-клиент* – компьютер, инициирующий VPN-соединение.

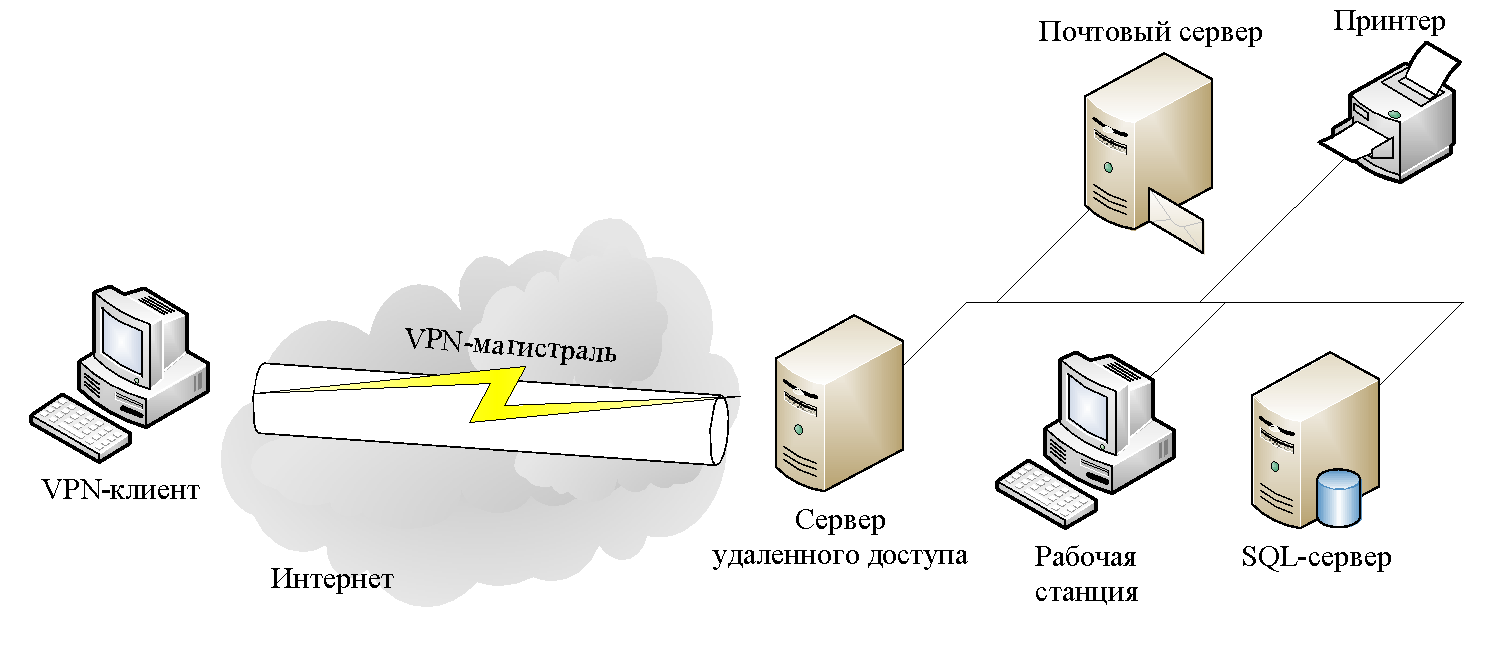
*VPN-сервер* – компьютер, с которым устанавливается соединение.

*VPN-магистраль* – последовательность каналов связи открытой сети, через которые проходят пакеты виртуальной частной сети.

Типы VPN-соединений:

* соединение с удаленными пользователями   
  (Remote Access VPN Connection)

соединение маршрутизаторов   
(Router-to-Router VPN Connection)



Изображение выглядит как текст, внутренний

Автоматически созданное описание

VPN формируется на основе трех технологий, которые образуют защищенное соединение:

* Аутентификация
* Туннелирование
* Шифрование
* *Туннелирование* (tunneling) – процесс включения IP-пакетов в пакеты другого формата, позволяющий передавать зашифрованные данные через открытые сети.
* Шифрование

Windows Server 2008 поддерживает две технологии шифрования:

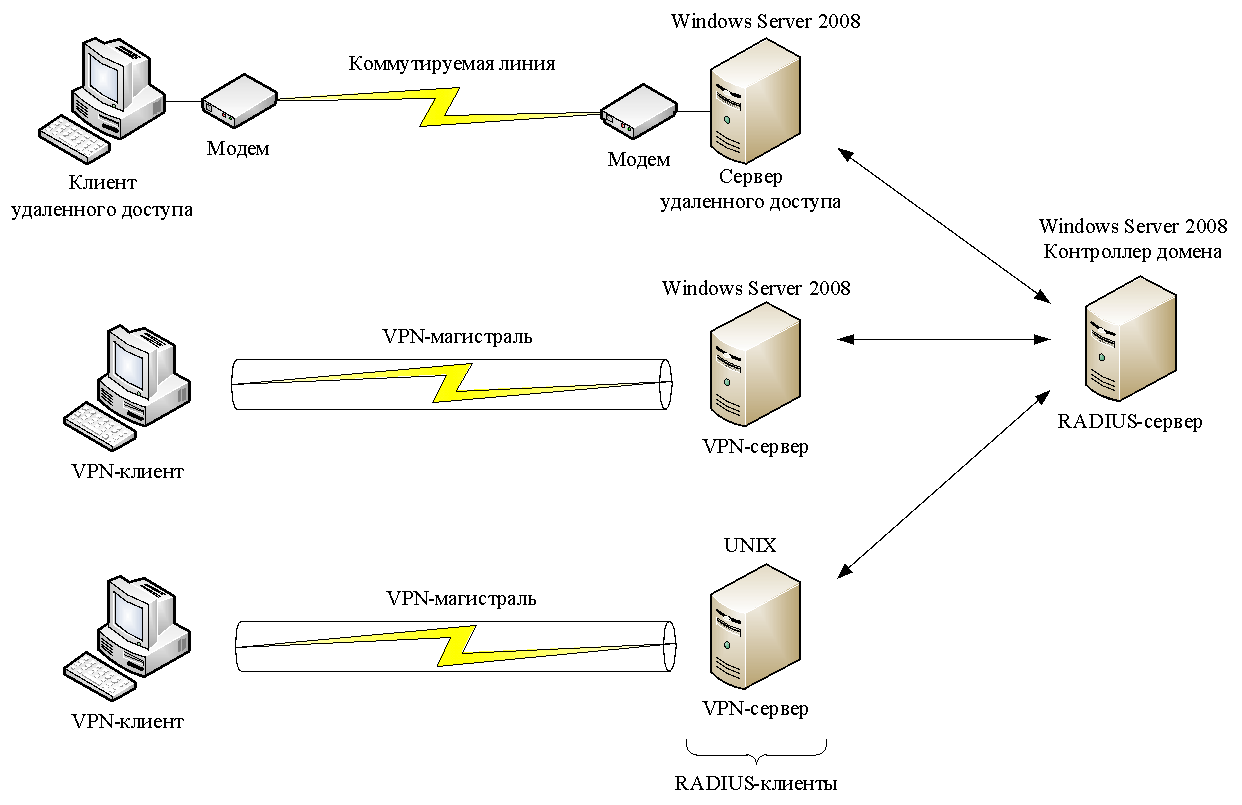
* Microsoft Point-to-Point Encryption (MPPE)
  + алгоритм шифрования RSA/RC4
  + не сжимает данных
  + используется совместно с Microsoft Point-to-Point Compression, предназначенным для этих целей
  + MPPE поддерживается далеко не всеми маршрутизаторами и является частым источником несовместимости оборудования
* IPSec
  + метод шифрования DES (Data Encryption Standard) или 3DES (Triple DES)
  + Поддерживает сжатие данных
* Протоколы виртуальных частных сетей
* PPTP (Point-to-Point Tunneling Protocol) – протокол туннелирования соединений «точка-точка», основан на протоколе РРР, RFC 2637.
  + Поддерживает все возможности РРР, в частности аутентификацию по протоколам PAP, CHAP,   
    MS-CHAP, MS-CHAP v2, EAP
  + Шифрование данных методом MPPE   
    (Microsoft Point-to-Point Encryption), алгоритм RSA/RC4
  + Сжатие данных по протоколу MPPC   
    (Microsoft Point-to-Point Compression), RFC 2118
  + Работает только поверх TCP/IP
  + Недостаток – относительно низкая скорость передачи данных
* IPsec может работать в транспортном и туннельном режимах.
  + Транспортный режим используется в связке с другими реализациями
  + туннельный сам по себе может являться методом создания VPN-туннеля.
* IPsec не создает в системе дополнительный виртуальный сетевой адаптер, а использует стандартный внешний интерфейс.
* IPsec является даже не реализацией VPN, а инструментом защиты от подмены передаваемых IP-пакетов.
* L2TP (Layer 2 Tunneling Protocol – туннельный протокол канального уровня) – протокол туннелирования, основанный на протоколе   
  L2F (Layer 2 Forwarding) и протоколе PPTP.  
  Описан в RFC 2661.
  + Поддерживает те же протоколы аутентификации,   
    что и PPP
  + Шифрование данных по протоколу IPsec
  + Поддерживает сжатие данных
  + может работать поверх протоколов X.25, Frame Relay, ATM, но в системе Windows работает только поверх TCP/IP
* SSTP (Secure Socket Tunneling Protocol)
* Для защиты трафика VPN применяет протокол защищенных сокетов (SSL- Secure Socket Layer) на порте 443
* Для шифрования используется стойкий AES (до 256 бит шифрование с сертификатами до 2048-бит)
* [**OpenVPN**](https://ru.wikipedia.org/wiki/OpenVPN) – open-source реализация VPN, распространяемая под лицензией GNU GPL.
* Безопасность разворачиваемых туннелей здесь обеспечивается библиотекой [OpenSSL](https://www.openssl.org/) , которая предлагает большой ассортимент открытых инструментов шифрования (Blowfish, AES, Camelia, 3DES, CAST и т.д.).
* От выбранного алгоритма зависит и скорость работы OpenVPN.
* В OpenVPN также используется инструмент LZO для сжатия данных.
* Вопросы реализации VPN

Перед реализацией VPN нужно учесть следующие факторы:

* Безопасность
* Финансовые вопросы
* Пропускная способность

1. **Протокол RADIUS.**

* Протокол RADIUS (Remote Authentication Dial-In User Service – служба аутентификации пользователей удаленного доступа) предназначен для аутентификации, авторизации и учета удаленных пользователей и обеспечивает единый интерфейс для систем на разных платформах (Windows, UNIX)
* RFC 2865 и 2866
* В Windows Server 2008 протокол RADIUS входит в состав двух служб:
  + RADIUS-сервер реализуется службой Интернет-аутентификации IAS (Internet Authentication Service)
  + RADIUS-клиент можно настроить при помощи службы маршрутизации и удаленного доступа RRAS

 Типы сообщений RADIUS

Cообщения RADIUS передаются в форме пакетов UDP.

В поле данных пакета UDP всегда помещается только одно сообщение RADIUS.

**Типы сообщений RADIUS:**

* Access-Request – запрос доступа
* Access-Accept – доступ разрешен
* Access-Reject – доступ не разрешен
* Access-Challenge – вызов запроса
* Accounting-Request – запрос учета

1. Настройка сети в Linux.
2. Настройка протокола DHCP в Linux.
3. Настройка службы DNS в Linux.