КУРСОВОЙ ПРОЕКТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| д-р техн. наук, профессор |  |  |  | А. в. Гордеев |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОМУ ПРОЕКТУ |
| РАЗРАБОТКА ДОМЕННОЙ СЕТИ СО СЛУЖБОЙ КАТАЛОГА ALD |
| по дисциплине: АДМИНИСТРИРОВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ |
|  |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 4134к |  |  |  | Д. В. Самарин |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Оглавление

[Топология сети 3](#_Toc194440697)

[Настройки DHCP 3](#_Toc194440698)

[Настройки DNS 5](#_Toc194440699)

[IP адреса устройств в сети 7](#_Toc194440700)

[Соответствие доменных имен и IP 7](#_Toc194440701)

[Настройки FTP 8](#_Toc194440702)

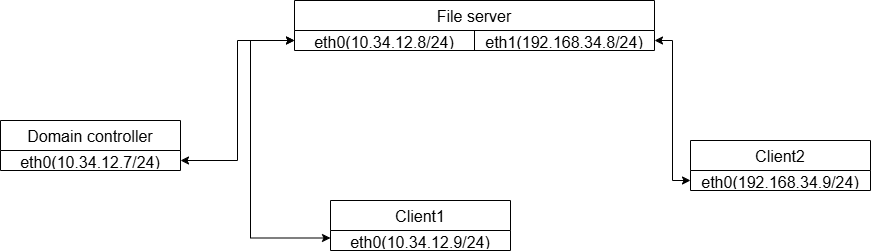
[Настройки SAMBA 9](#_Toc194440703)

[Таблицы маршрутизации 10](#_Toc194440704)

[Заключение 12](#_Toc194440705)

# Топология сети

Этот раздел описывает **структуру и логику подключения устройств**: кто с кем соединён, какие подсети используются.



В представленной сети контроллер домена, первый клиент и первый сетевой интерфейс файлового сервера (eth0) находятся в одной подсети, а второй клиент и второй сетевой интерфейс файлового сервера (eth1) в другой.

# Настройки DHCP

Данный блок отвечает за автоматизированное управление сетевыми настройками клиентов в локальной сети.

|  |
| --- |
| option domain-name "samarin.g4134.guap.local";  default-lease-time 86400;  max-lease-time 86400;  include "/etc/bind/rndc.key";  ddns-updates on;  ddns-update-style interim;  ignore client-updates;  update-static-leases on;  zone samarin.g4134.guap.local. {  primary 10.34.12.7;  key rndc-key;  }  zone 12.34.10.in-addr.arpa. {  primary 10.34.12.7;  key rndc-key;  }  subnet 10.34.12.0 netmask 255.255.255.0 {  option broadcast-address 10.34.12.255;  option routers 10.34.12.8;  option domain-name "samarin.g4134.guap.local";  option domain-search "samarin.g4134.guap.local";  option domain-name-servers 10.34.12.7;  range 10.34.12.9 10.34.12.254;  }  subnet 192.168.34.0 netmask 255.255.255.0 {  option broadcast-address 192.168.34.255;  option routers 192.168.34.8;  option domain-name "samarin.g4134.guap.local";  option domain-search "samarin.g4134.guap.local";  option domain-name-servers 10.34.12.7;  range 192.168.34.9 192.168.34.254;  }  host dmitriy {  hardware ethernet 08:00:27:11:ec:9e;  fixed-address 10.34.12.7;  } |

Автоматическая выдача IP-адресов (DHCP):

* Назначает клиентам IP-адреса из указанных диапазонов (range) в подсетях 10.34.12.0/24 и 192.168.34.0/24.
* Устанавливает время аренды IP-адресов (default-lease-time и max-lease-time) — 24 часа (86400 секунд).
* Назначает статический IP-адрес хосту dmitriy по его MAC-адресу (fixed-address 10.34.12.7).

Настройка сетевых параметров:

* Определяет шлюзы (routers), DNS-серверы (domain-name-servers), доменное имя (domain-name) и поисковые домены (domain-search) для клиентов.
* Указывает широковещательные адреса (broadcast-address) для подсетей.

Интеграция с DNS (DDNS):

Включает динамическое обновление DNS-записей (ddns-updates on) при выдаче или изменении IP-адресов.

Настроена обратная связь с DNS-сервером BIND через ключ rndc-key для зон:

* Прямая зона: samarin.g4134.guap.local (основной DNS-сервер — 10.34.12.7).
* Обратная зона: 12.34.10.in-addr.arpa (для PTR-записей).

Игнорирует попытки клиентов самостоятельно обновлять DNS (ignore client-updates), но разрешает обновление статических аренд (update-static-leases on).

# Настройки DNS

Данный блок отвечает за разрешение доменных имен в IP-адреса и обратно, а также управление зонами DNS-сервера.

|  |
| --- |
| zone "samarin.g4134.guap.local" {  type master;  file "/etc/bind/zones/db.samarin.g4134.guap.local";  allow-update { key "rndc-key"; };  };  zone "12.34.10.in-addr.arpa" {  type master;  file "/etc/bind/zones/db.12.34.10";  allow-update { key "rndc-key"; };  };  $TTL 604800  @ IN SOA dmitriy.samarin.g4134.guap.local. root.samarin.g4134.guap.local. (  2 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800) ; Negative Cache TTL  ;  @ IN NS dmitriy.samarin.g4134.guap.local.  dmitriy IN A 10.34.12.7  vasiliy IN A 10.34.12.8  www IN CNAME vasiliy  $TTL 604800  @ IN SOA dmitriy.samarin.g4134.guap.local. root.samarin.g4134.guap.local. (  2 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800) ; Negative Cache TTL  ;  @ IN NS dmitriy.samarin.g4134.guap.local.  7 IN PTR dmitriy.samarin.g4134.guap.local.  8 IN PTR vasiliy.samarin.g4134.guap.local. |

1. Управление зонами

Прямая зона (samarin.g4134.guap.local):

Определяет доменное пространство имен для локальной сети.

Содержит записи типа:

* A (IPv4-адреса хостов: dmitriy → 10.34.12.7, vasiliy → 10.34.12.8).
* CNAME (алиасы: www → vasiliy).
* NS (сервер имен: dmitriy.samarin.g4134.guap.local).
* SOA (административная информация: серийный номер, временные параметры).

Обратная зона (12.34.10.in-addr.arpa):

Обеспечивает обратное разрешение IP-адресов в доменные имена (PTR-записи):

* 10.34.12.7 → dmitriy.samarin.g4134.guap.local,
* 10.34.12.8 → vasiliy.samarin.g4134.guap.local.

2. Настройки безопасности и обновлений

Динамические обновления:

* Разрешены только аутентифицированные изменения через ключ rndc-key (аналогично DHCP-серверу).
* Гарантирует, что только доверенные сервисы (например, DHCP) могут обновлять DNS-записи.

3. Параметры зон

TTL (Time to Live):

Устанавливает срок жизни записей (604800 секунд = 7 дней) для кэширования на клиентских устройствах.

SOA-запись:

Управляет синхронизацией зоны:

* Serial (версия конфигурации, увеличивается при изменениях).
* Refresh , Retry , Expire — временные интервалы для проверки актуальности зоны вторичными DNS-серверами.

Ключевые компоненты

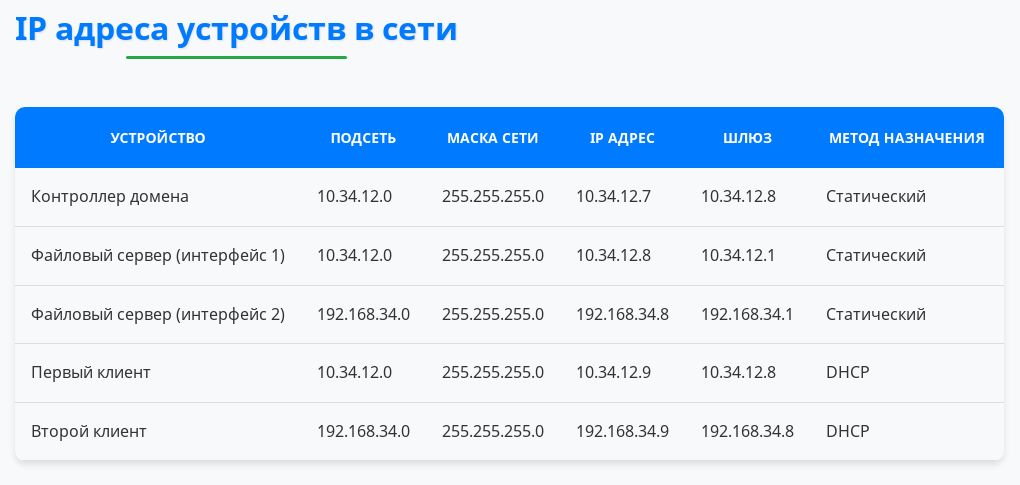
BIND — сервер, управляющий DNS-зонами.

* Мастер-зоны (type master) — зоны, которые обслуживаются локально (не реплицируются с других серверов).
* Файлы зон (/etc/bind/zones/db.\*) — хранят записи ресурсов (A, PTR, CNAME и др.).
* Динамические обновления — интеграция с DHCP для автоматического обновления записей при изменении IP-адресов.
* Аутентификация — использование ключа rndc-key для защиты от несанкционированных изменений.

Таким образом, этот блок обеспечивает:

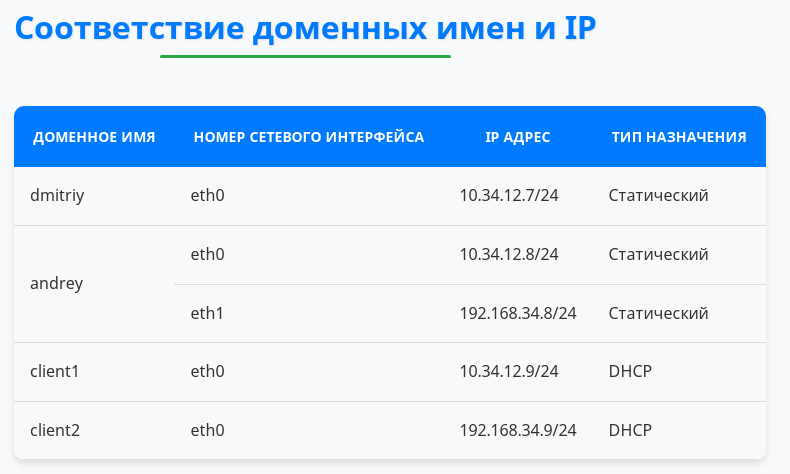
* Работу DNS-сервера для преобразования доменных имен в IP и обратно.
* Синхронизацию с DHCP через динамические обновления (DDNS).
* Безопасность за счет ограничения прав на изменение зон.
* Управление кэшированием и репликацией зон через SOA-параметры.

# IP адреса устройств в сети



# Соответствие доменных имен и IP

Таблица, где описана, связь между доменными именами, сетевыми интерфейсами и IP-адресами устройств в локальной сети.



# Настройки FTP

Данный блок настраивает работу FTP-сервера для загрузки и скачивания файлов.

|  |
| --- |
| listen\_ipv6=NO  anonymous\_enable=YES  local\_enable=YES  dirmessage\_enable=YES  use\_localtime=YES  xferlog\_enable=YES  connect\_from\_port\_20=YES  secure\_chroot\_dir=/var/run/vsftpd/empty  pam\_service\_name=vsftpd  rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem  rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key  ssl\_enable=NO |

1. Основные настройки

Режим работы:

* listen\_ipv6=NO — сервер принимает соединения только через IPv4.
* connect\_from\_port\_20=YES — активный режим FTP (порт 20 используется для передачи данных).

Доступ:

* anonymous\_enable=YES — разрешен анонимный доступ (без аутентификации).
* local\_enable=YES — локальные пользователи системы могут подключаться к серверу.

2. Безопасность и изоляция

Chroot-окружение:

secure\_chroot\_dir=/var/run/vsftpd/empty — изолирует пользователей в их домашних каталогах, предотвращая доступ к остальной файловой системе.

Отключено шифрование:

ssl\_enable=NO — соединения не используют SSL/TLS, что делает передачу данных незащищенной (логины, пароли и файлы передаются в открытом виде).

3. Логирование и удобство

Лог-файлы:

* xferlog\_enable=YES — включено логирование всех операций (загрузки/скачивания).
* use\_localtime=YES — время в логах отображается в локальном часовом поясе.

Сообщения:

* dirmessage\_enable=YES — при входе в каталог пользователю показывается файл .message (если он существует).

4. Аутентификация

PAM-модуль:

pam\_service\_name=vsftpd — использует стандартный PAM-профиль для проверки учетных данных пользователей.

Ключевые компоненты

Сертификаты (неактивные):

* rsa\_cert\_file и rsa\_private\_key\_file указывают на сертификаты, но из-за ssl\_enable=NO они не используются.

Анонимный доступ:

* Пользователь anonymous может подключаться без пароля, но его права ограничены настройками сервера.

# Настройки SAMBA

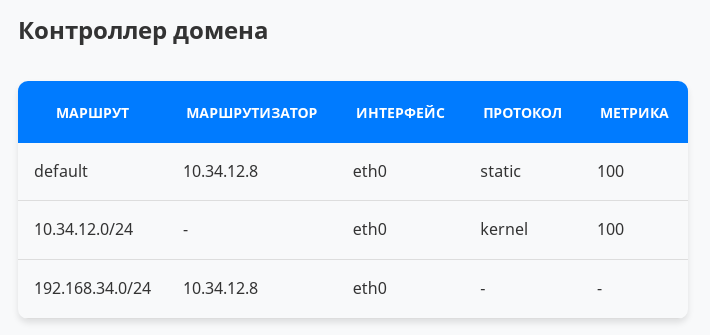
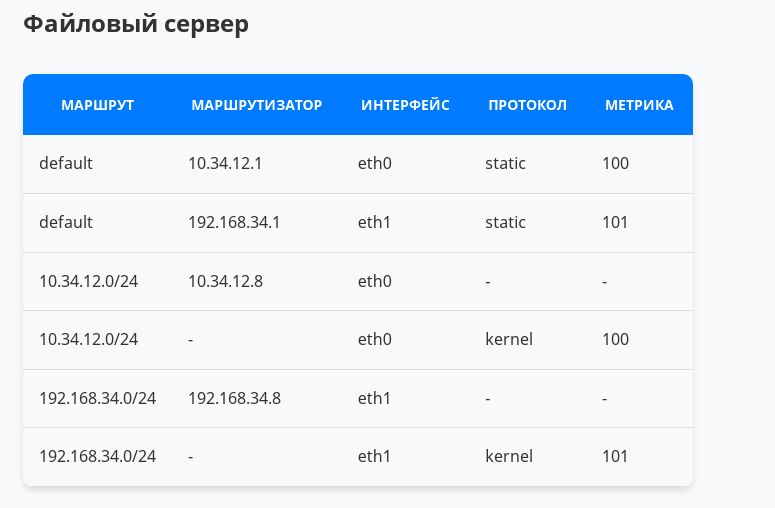
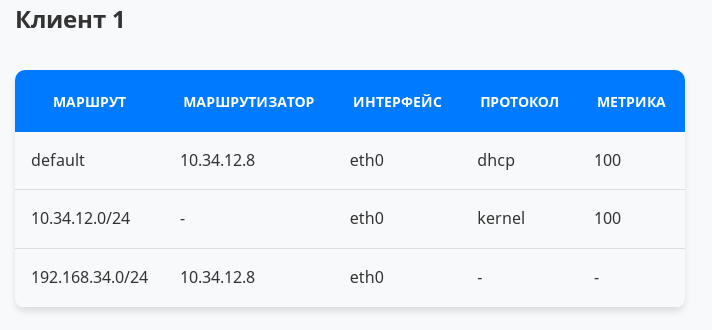
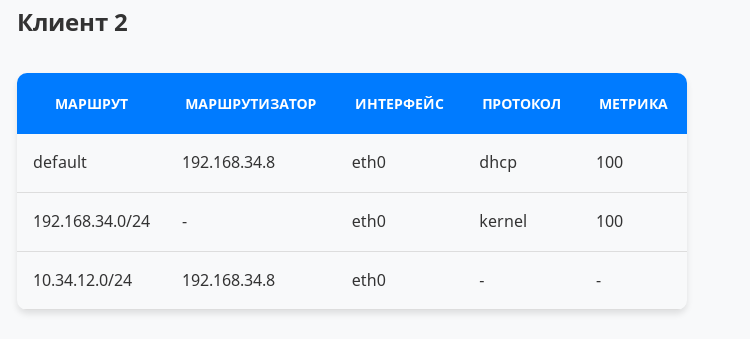
Samba предоставляет доступ к файлам по протоколу SMB (Windows-сети).

|  |
| --- |
| [global]  workgroup = WORKGROUP  log file = /var/log/samba/log.%m  max log size = 1000  logging = file  panic action = /usr/share/samba/panic-action %d  server role = standalone server  obey pam restrictions = yes  unix password sync = yes  passwd program = /usr/bin/passwd %u  passwd chat = \*Enter\snew\s\*\spassword:\* %n\n \*Retype\snew\s\*\spassword:\* %n\n \*password\supdated\ssuccessfully\* .  pam password change = yes  map to guest = bad user  usershare allow guests = no  [homes]  comment = Home Directories  browseable = no  read only = yes  create mask = 0700  directory mask = 0700  valid users = %S  [dir1]  path = /srv/dir1  writable = yes  browseable = yes  valid users = @editors, @watchers  create mask = 0775  directory mask = 0775  [dir3]  path = /srv/dir3  writable = yes  browseable = yes  valid users = @editors, @watchers  create mask = 0775  directory mask = 0775  hosts deny = 192.168.34.0/24 |

1. В разделе [global] — основные параметры, включая логирование, синхронизацию паролей, поведение при ошибках.
2. [homes] — автоматическая домашняя папка для каждого пользователя.
3. [dir1] и [dir3] — это общие каталоги, с разными правами доступа.
4. hosts deny — запрет доступа к dir3 из подсети 192.168.16.0/24 (например, для изоляции пользователей).

# Таблицы маршрутизации

Таблицы маршрутизации описывают правила передачи данных между устройствами в сети. Контроллер домена использует шлюз 10.34.12.8 для связи с подсетью 10.34.12.0/24 и доступа к 192.168.34.0/24. Файловый сервер с двумя интерфейсами (eth0 и eth1) связывает подсети напрямую, маршрутизируя трафик через шлюзы 10.34.12.1 и 192.168.34.1. Клиенты автоматически получают шлюзы через DHCP: клиенты из 10.34.12.0/24 используют 10.34.12.8, а из 192.168.34.0/24 — 192.168.34.8, что обеспечивает связь между сегментами сети через указанные шлюзы.

# Заключение

В рамках курсового проекта реализована локальная вычислительная сеть архитектуры «клиент-сервер» на платформе Astra Linux Special Edition с применением виртуализации. Инфраструктура включает два серверных узла и две клиентские станции, распределённые по двум подсетям. Сервер на базе имени студента функционирует как контроллер домена с интеграцией DNS и DHCP, обеспечивая централизованное управление ресурсами. Второй сервер, названный в честь отца, объединяет роли файлового хранилища, веб- и FTP-сервера, а также маршрутизатора между сегментами сети.

Ключевыми этапами стали: развёртывание службы каталога Astra Linux Directory для авторизации пользователей, настройка групповых политик с выделением домашних каталогов на сервере, организация разграничения прав доступа к трём файловым ресурсам через протоколы CIFS и NFS. Установлены и настроены DNS, DHCP, FTP и HTTP-серверы, реализована маршрутизация между подсетями. Техническая документация по проекту, включая копию отчёта, размещена на веб- и FTP-серверах.

Проверка показала корректную работу всех компонентов: клиенты успешно проходят аутентификацию в домене, получают IP-адреса, разрешают DNS-имена и взаимодействуют с файловыми ресурсами в соответствии с заданными правилами. Результат подтверждает освоение методов администрирования защищённых ОС и построения сетевых решений на основе свободного программного обеспечения.