Московский государственный технический университет им. Н.Э. Баумана

Домашнее задание по дисциплине

**«Операционные системы»**

**Вариант № 18**

**Доступ к сетевым ресурсам в ОС Linux**

**Выполнил**

**студент группы ИУ5-51Б \_\_\_\_\_\_\_\_\_\_/Цыпышев Т.А./**

**Москва 2024 г.**

**Оглавление**

[Сетевые файловые системы и протоколы 3](#_m8nuucb4jbnj)

[Управление правами доступа и сетевыми интерфейсами 4](#_8enknpe0alhl)

[Утилиты для работы с сетью и фильтрация трафика 6](#_r5nljmg3e0ck)

[Управление сетевой безопасностью 7](#_u1cysznpcctq)

[Источники 8](#_ueuznnzf3ojz)

# 

# Сетевые файловые системы и протоколы

В Linux для обеспечения доступа к удалённым файлам и каталогам через сеть используются различные сетевые файловые системы и протоколы, включая ***NFS*** *(Network File System)* и ***SMB*** *(Server Message Block)*. Эти технологии позволяют пользователям эффективно взаимодействовать с данными на удаленных серверах.

**NFS** — это распределённая файловая система для Unix-подобных ОС, обеспечивающая монтирование удаленных файловых систем так, будто они локальные. Работает по модели клиент-сервер, где клиент запрашивает доступ, а сервер предоставляет ресурсы.

Основные характеристики NFS:

* *Версии протокола:* NFS поддерживает несколько версий (NFSv2-NFSv4), каждая из которых улучшает безопасность и функциональность. NFSv4 внедряет межсетевое взаимодействие и интеграцию с Kerberos.
* *Производительность:* Оптимизирован для низкой задержки и может обслуживать множество клиентов одновременно.
* Безопасность: Реализованы механизмы безопасности, такие как Kerberos для аутентификации.

**SMB**, также известный как *Samba*, обеспечивает совместимость между Unix/Linux и Windows, позволяя обмениваться файлами и ресурсами между разными платформами.

Ключевые особенности SMB:

* *Кросс-платформенность:* Обеспечивает взаимодействие между Windows и Unix/Linux.
* *Настройка:* Для доступа требуется редактирование конфигурационного файла smb.conf, где определяются параметры доступа, права и аутентификация.
* *Поддержка протоколов:* SMB совместим с различными версиями Windows и современными стандартами безопасности.

# Управление правами доступа и сетевыми интерфейсами

В операционных системах на базе Linux управление доступом к сетевым ресурсам осуществляется через систему прав доступа на уровне файловой системы. Это позволяет администратору гибко управлять тем, какие пользователи и группы имеют доступ к определённым ресурсам, включая сетевые. Права доступа к файлам и директориям задаются с использованием утилит, таких как ***chmod***, ***chown***, и ***chgrp***. Команда ***chmod*** позволяет устанавливать права доступа к файлам (чтение, запись и выполнение) для владельца, группы и остальных пользователей, что создает многоуровневую систему безопасности.

Например, для настройки прав доступа к общему ресурсу Samba используется конфигурационный файл ***smb.conf***, где администратор может детализировать, какие пользователи имеют право на доступ к определенным каталогам, а также устанавливать маски прав на создание и редактирование файлов. Это позволяет минимизировать риски несанкционированного доступа и повысить безопасность данных.

Одним из первых шагов при организации сетевого доступа является идентификация и настройка сетевых интерфейсов. В Linux существует несколько утилит для управления сетевыми интерфейсами, наиболее распространенными из которых являются ***ip*** и ***ifconfig***. Команда ***ip***, входящая в пакет ***iproute2***, предоставляет более современные и функциональные инструменты для управления сетевыми интерфейсами, маршрутизацией и правилами брандмауэра.

С помощью команды ***ip addr*** можно просмотреть текущие IP-адреса, назначенные сетевым интерфейсам, а команда ***ip route*** позволяет настраивать маршрутизацию сетевого трафика. Например, можно добавлять и удалять маршруты, что критично для управления сетевыми соединениями и обеспечения их надежности. Кроме того, команда ***ip link*** предоставляет информацию о состоянии интерфейсов, включая их активность и параметры.

Управление доступом к сетевым ресурсам также включает в себя настройку статических и динамических IP-адресов. Динамическая конфигурация IP-адресов, как правило, осуществляется через DHCP (протокол динамической конфигурации хоста), который автоматически назначает IP-адреса устройствам в сети. Это упрощает управление адресным пространством и снижает вероятность конфликтов IP-адресов.

Для статической настройки IP-адреса в Linux, например, через файл конфигурации ***netplan*** в Ubuntu, администратору необходимо вручную указать следующие параметры:

* *IP-адрес:* уникальный адрес, назначаемый устройству.
* Маска подсети: определяет, какая часть IP-адреса относится к сети, а какая — к узлу.
* *Шлюз по умолчанию:* адрес маршрутизатора, через который проходят все пакеты, не предназначенные для локальной сети.
* *DNS-серверы:* адреса серверов, используемых для разрешения доменных имен.

Эти настройки обеспечивают более точный контроль над сетевыми подключениями и позволяют администраторам гарантировать стабильность и безопасность сетевой инфраструктуры.

# Утилиты для работы с сетью и фильтрация трафика

Linux предоставляет множество утилит для мониторинга и управления сетевыми соединениями. Некоторые из наиболее полезных утилит включают:

1. Утилита ***ping*** осуществляет диагностику доступности узлов, отправляя ICMP Echo Request пакеты и измеряя время отклика. Используется для оценки задержки и потерь пакетов, что помогает выявлять проблемы с сетевым соединением.

2. ***netstat*** предоставляет информацию о текущих сетевых соединениях, таблицах маршрутизации и статистике интерфейсов. С помощью команд *netstat -tuln* и *netstat -an* администраторы могут анализировать активные TCP/UDP соединения, их статусы и загруженность сети, что критично для обнаружения угроз.

3. ***tcpdump*** — утилита для захвата и анализа сетевого трафика на уровне пакетов. Она позволяет фильтровать трафик по IP-адресам, портам и протоколам, что полезно для выявления узких мест и диагностики соединений. Пример использования: команда *tcpdump -i eth0 port 80* отслеживает HTTP-трафик на интерфейсе *eth0*.

4. ***mtr*** (My Traceroute) сочетает функции *traceroute* и *ping*, обеспечивая информацию о маршруте и задержках пакетов. Визуализируя состояние сети в реальном времени, он помогает быстро диагностировать сетевые проблемы. Команда *mtr -r* генерирует отчет в удобном формате для анализа.

Важной частью управления доступом к сетевым ресурсам является организация фильтрации сетевого трафика. Для этого в Linux традиционно используется утилита ***iptables***. С его помощью можно задавать правила для фильтрации входящего и исходящего трафика, а также управлять доступом на основе различных критериев, таких как IP-адреса, порты и протоколы.

# Управление сетевой безопасностью

Управление сетевой безопасностью в Linux является критически важной задачей администрирования. Это включает в себя использование мощных инструментов и протоколов для защиты данных, передаваемых по сети.

Основным инструментом для управления сетевой безопасностью в Linux является iptables. Этот компонент позволяет настраивать правила фильтрации трафика на основе IP-адресов, портов и протоколов.

* ***Структура iptables:*** Система разделена на таблицы (*filter*, *nat*, *mangle*), каждая из которых имеет свои функции. Например, *filter* используется для контроля входящего и исходящего трафика, а *nat* для преобразования адресов.
* ***Состояние соединения:*** Поддержка stateful filtering позволяет создавать динамические правила, адаптирующиеся к состоянию соединения, что защищает от различных типов атак.
* ***nftables***: Современная замена iptables с более гибкой архитектурой и поддержкой сложных фильтров и многопоточной обработки.

Шифрование сетевого трафика критично для защиты данных. Это может быть реализовано с помощью:

* ***SSL/TLS:*** Обеспечивают шифрование и аутентификацию для защиты данных в транзите, предотвращая атаки типа «человек посередине».
* ***VPN (OpenVPN, IPsec, WireGuard):*** Создают защищенные каналы для передачи данных через ненадежные сети. Эти технологии используют различные методы шифрования и аутентификации, что особенно важно для удалённого доступа.

Для мониторинга и анализа сетевого трафика в Linux применяются инструменты:

* ***tcpdump:*** Позволяет захватывать и анализировать пакеты на уровне транспортного протокола с возможностью применения сложных фильтров.
* ***Wireshark:*** Графический инструмент для детального анализа сетевого трафика, включая визуализацию протоколов и выявление аномалий.
* ***IDS (Snort, Suricata):*** Системы обнаружения вторжений, которые анализируют сетевой трафик в реальном времени, выявляя потенциальные угрозы на основе предопределенных правил.

# Источники

1. Habr. [7 сетевых Linux-команд, о которых стоит знать системным администраторам](https://habr.com/ru/articles/513544/)

2. Habr. [Большое руководство по сетям и шифрованию трафика в Linux](https://habr.com/ru/articles/561195/)

3. Linux-console.net. [Используйте Samba в Linux для общего доступа к файлам в домашней сети](https://ru.linux-console.net/)

4. Arch linux. [Network configuration] (https://wiki.archlinux.org/title/Network\_configuration)

5. FB. [Настройка сети Linux: полное руководство](https://fb.ru/article/534887/2023-nastroyka-seti-linux-polnoe-rukovodstvo)

6. Network admin. [Справочник по сетевым командам в операционной системе Linux](https://networkadmin.ru/reference-network-commands-in-linux/)

7. OLP. [Настройка сети в Linux: полное руководство для популярных дистрибутивов](https://www.olp.kz/articles/55-nastroika-seti-v-linux-polnoe-rukovodstvo-dlia-populiarnyx-distributivov)