Лабораторная работа №2
«Основы сетевого администрирования»

Цель работы:

Продолжительность работы: 4 часа

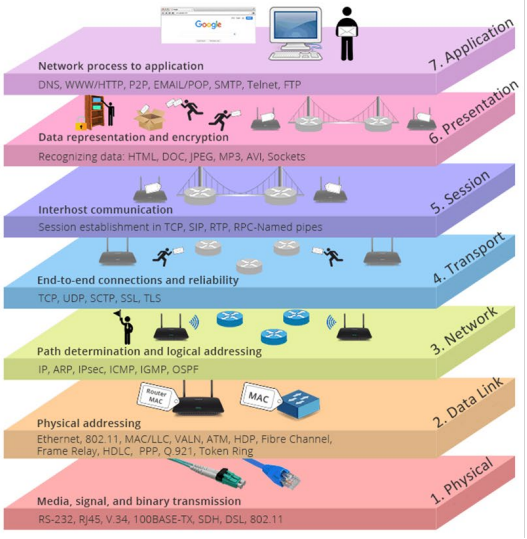
1. Теоретическая часть

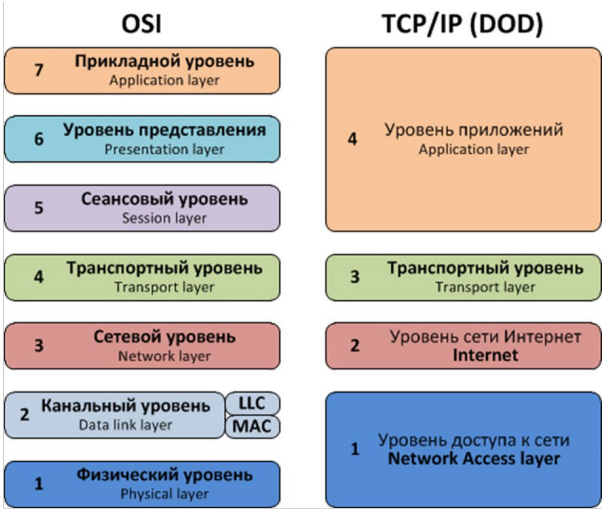
1.1. Введение в сетевое администрирование

Локальная вычислительная сеть (ЛВС, локальная сеть; англ. Local Area Network, LAN) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

В сети должен происходить обмен данными между вычислительными устройствами — компьютерами, серверами, маршрутизаторами, принтерами и другим оборудованием. Для передачи информации могут быть использованы различные среды передачи данных (витая пара, оптоволокно, радиоволны).

Всю работу сети можно проанализировать как по модели OSI (англ. The **O**pen **S**ystems **I**nterconnection model) , так и по модели TCP/IP.





В обязанности сетевого администратора входит построение ЛВС, её настройка, поддержка и улучшение. И это лишь малая часть, чем может заниматься специалист в данной области. Обязанности могут различаться в зависимости от масштабов сетей, специфики работы какой-либо компании и т.д.

1.2. Роль Linux в управлении ЛВС

Несмотря на то, что в локальную сеть могут входить пользовательские компьютеры, где чаще всего используется операционная система Windows для выполнения повседневных задач, администрирование сети происходит с помощью устройств (серверов) под управлением операционной системы на базе ядра Linux.

Используются как широко распространённые дистрибутивы GNU/Linux с графическим интерфейсом, так и дистрибутивы, предоставляющие для управления только командную строку. Это связано с тем, что использовать GNU/Linux на серверах выгодно, потому что эта операционная система бесплатна и можно сразу же развернуть нужный образ GNU/Linux на сервере. Это обеспечивает надёжность, гибкость и масштабируемость.

1.3. Базовые утилиты для работы с сетью

Для работы с сетевыми соединениями необходимо владеть несколькими базовыми инструментами, которые помогут при настройке и анализе сети.

Приведем их в виде таблицы. В столбце «Пример работы» указаны наиболее часто используемые параметры. Более подробно вы можете изучить в документации на каждую из утилит.

Название утилиты	Описание работы	Пример работы	Комментарий
ifconfig	Настройка сетевых интерфейсов	*ifconfig eth0*	Просмотр текущих сетевых соединений Не всегда установлена. В AL выполняется только с правами администратора.

ip	Замена для ifconfig, более мощная утилита для работы с сетевыми интерфейсами.	`ip a` `ip route`	Просмотр текущих сетевых соединений. Просмотр таблицы маршрутизации
ping	Проверка доступности удалённого хоста	`ping google.com` `ping 192.168.122.1`	Возможно указывать IP адрес или доменное имя
netstat/ss	Показ активных соединений и портов	`netstat -tulpn` `ss -tulpn`	Удобно проверять, какие порты заняты какими приложениями. Для указания имен приложений требуются права администратора
traceroute	Показ маршрута до удалённого хоста	`traceroute google.com`	Отслеживает путь, по которому пакеты данных проходят от компьютера до целевого хоста. Помогает выявить, где могут возникать задержки или разрывы связи
nslookup / dig	Проверка DNS-запросов	`nslookup google.com` `dig google.com`	По умолчанию не установлены. Расположены в пакете *dnsutils*.
curl / wget	Получение данных с веб-серверов	`wget http://example.com/file.zip` `curl -I http://example.com`	wget по умолчанию сохраняет загруженные файлы на диск, может рекурсивно загружать сайты
nmap	Сканирование сети и открытых портов	`nmap 192.168.1.1`	По умолчанию не установлен. Расположен в пакете *nmap*.

1.4. Базовые настройки системы GNU/Linux

После установки какого-либо дистрибутива GNU/Linux для подключения к локальной или глобальной сети необходимо произвести базовые настройки. Это возможно сделать несколькими способами – вручную, настраивая конфигурационные файлы или используя сторонние утилиты.

Рассмотрим первый способ настройки. Основные параметры компьютера устанавливаются в следующих конфигурационных файлах:

Путь к файлу	Назначение
/etc/hostname	Настройка имени компьютера
/etc/hosts	Настройка разрешения доменных имен
/etc/resolv.conf	Настройка адресов серверов имен, к которым имеет доступ данная система
/etc/network/interfaces	Настройка сетевых интерфейсов
/etc/apt/sources.list	Настройка списка репозиториев

Рассмотрим эти файлы подробнее:

1. Файл **/etc/hostname** предназначен для настройки имени компьютера. Текущее имя компьютера можно узнать командой **hostname** или по переменной

окружения **HOSTNAME**. После редактирования файла необходимо выполнить перезагрузку системы.

2. Файл **/etc/hosts** представляет собой список доменных имён. В качестве аналогии можно привести телефонный справочник, только вместо номера телефона указывается IP-адрес, а вместо имени человека – доменное имя. При использовании команды **ping** указывается либо IP-адрес устройства, либо его доменное имя. При указании имени система обращается к файлу **/etc/hosts**, определяет по имени соответствующий IP-адрес, затем происходит обращение к целевому устройству по протоколу ICMP.

3. Файл **/etc/resolv.conf** хранит доменное имя и IP-адрес DNS-сервера. В случае, если при указании имени система не находит соответствующий IP-адрес в локальном файле **/etc/hosts**, она делает запрос в DNS-сервер. Если и там нет информации об указанном доменном имени, то выдаётся ошибка разрешения имён.

4. В файле **/etc/network/interfaces** хранятся параметры сетевых интерфейсов (например, Ethernet или WiFi). По умолчанию содержит следующие строки:

1) **source /etc/network/interfaces.d/***. Команда **source** вставляет в текущий файл **interfaces** содержимое папки **interfaces.d** (обычно изначально пустого). Удобен для соблюдения принципа модульности.

2) **auto lo**. Директива **auto** означает, что интерфейс, указанный справа, должен быть автоматически запущен во время загрузки системы.

lo (loopback, обратная петля) - виртуальный сетевой интерфейс, не связанный с каким-либо оборудованием, но при этом полностью интегрированный во внутреннюю сетевую инфраструктуру системы. Любой трафик, который посылается программой на интерфейс loopback, тут же получается тем же интерфейсом.

Он может быть использован сетевым клиентским программным обеспечением, чтобы общаться с серверным приложением, расположенным на том же компьютере. То есть если на компьютере, на котором запущен веб-сервер, указать в веб-браузере URL http://127.0.0.1/ или http://localhost/, то он попадает на веб-сайт этого компьютера.

Этот механизм работает без какого-либо активного подключения, поэтому он полезен для тестирования служб, не подвергая их безопасность риску, как при удаленном сетевом доступе. Подобным образом, пингование адреса loopback — это основной тест функционирования IP стека в операционной системе.

3) **iface lo inet loopback**. Директива **iface** описывает сетевой интерфейс **lo**, **inet** означает семейство интернет-протоколов (IPv4).

4) **auto eth0**. Директива **auto** предписывает автоматически включить сетевой интерфейс eth0 во время загрузки. В Astra Linux используется по умолчанию традиционная схема именования сетевых Ethernet интерфейсов: eth0, eth1 и т.д.

5) **iface eth0 inet dhcp**. Описание интерфейса **eth0** с присвоением IP-адреса по протоколу DHCP, то есть автоматически при обращении к DHCP-серверу.

Пользователь может самостоятельно назначать интерфейсу статический IP-адрес. Для этого в конфигурационном файле **/etc/network/interfaces** необходимый интерфейс описывается в следующем формате:

```
auto IFACE_NAME
iface IFACE_NAME inet static
address A.B.C.D
netmask A.B.C.D
gateway A.B.C.D
```

При этом **static** означает, что интерфейсу присваивается адрес статически, **address A.B.C.D** – это назначаемый IP-адрес интерфейса, **netmask A.B.C.D** – маска подсети, **gateway A.B.C.D** – шлюз по умолчанию.

После сохранения изменений необходимо перезагрузить интерфейс для установления введённых параметров. Для этого используются команды **ifdown IFACE_NAME** и **ifup IFACE_NAME**.

Установившиеся настройки можно посмотреть с помощью команды **ifconfig** (с применением **sudo**) или с помощью стандартной команды **ip a**.

Ниже приведен пример настройки сетевого интерфейса:

```
auto eth0
iface eth0 inet static
address 192.168.1.2
netmask 255.255.255.0
gateway 192.168.1.1
```

С помощью указанной конфигурации настраивается статический IP адрес со значением 192.168.1.2. Маска подсети – 255.255.255.0, адрес шлюза – 192.168.1.1.

Обратите внимание! Для работы с конфигурационным файлом /etc/network/interfaces используется служба networking.service. При запущенной утилите NetworkManager конфигурационный файл interfaces не перечитывается. Для корректной работы убедитесь, что служба NetworkManager остановлена и удалена из автозагрузки, а служба networking – запущена.

1.8. Настройка сети с использованием утилиты Network Manager.

Конфигурационные файлы, отвечающие за настройку сетевого оборудования, могут отличаться в разных дистрибутивах Linux. Утилита Network Manager представляет собой универсальный способ настройки сети. Основной командой для управления является nmcli. Она позволяет создавать, изменять, удалять, активировать и деактивировать сетевые подключения.

Синтаксис команды:

```
nmcli опции объект команда
```

Где:

- опции — дополнительные параметры для команды, такие как -t для вывода без форматирования или -p для вывода с использованием форматирования.
- объект — сущность, с которой вы хотите взаимодействовать

Чаще всего в nmcli используются следующие объекты:

- **device** - управление сетевыми интерфейсами (lo, enp1s0 и др.);
- **connection** - управление соединениями;
- **networking** - управление сетью в целом;
- **general** - показывает состояние всех сетевых протоколов и NetworkManager в целом;
- **radio** - управление сетевыми протоколами, wifi, ethernent и т д.

- команда — действие, которое вы хотите выполнить над объектом (например, show, up, down, add, edit, delete).

Перед началом работы с Network Manager убедитесь, что служба NetworkManager.service запущена, а служба networking.service – отключена.

За настройку службы отвечает конфигурационный файл /etc/NetworkManager/NetworkManager.conf. Проверьте, что параметр managed в разделе [ifupdown] равен true. Если нет, то исправьте это.

Примеры работы:

Проверка статуса работы службы

```
nmcli networking
```

Определение сетевых интерфейсов

```
nmcli device
```

Определение сетевых подключений

```
nmcli connection show
```

Добавить сетевое подключение my-eth через интерфейс enp1s0

```
nmcli connection add type ethernet con-name my-eth ifname enp1s0
```

Удалить сетевое подключение

```
nmcli connection delete my-eth
```

Назначить соединению статический метод конфигурации IP

```
nmcli connection mod my-eth ipv4.method manual
```

Назначить соединению динамический метод конфигурации IP

```
nmcli connection mod my-eth ipv4.method auto
```

Назначить соединению статический ip адрес

```
nmcli connection mod my-eth ipv4.addresses 192.168.122.3/24
```

Назначить соединению шлюз по-умолчанию

```
nmcli connection mod my-eth ipv4.gateway 192.168.122.1
```

Назначить соединению IP-адреса DNS-сервера

```
nmcli connection mod my-eth ipv4.dns '8.8.8.8'
```

Включить сетевой интерфейс

```
nmcli connection up my-eth
```

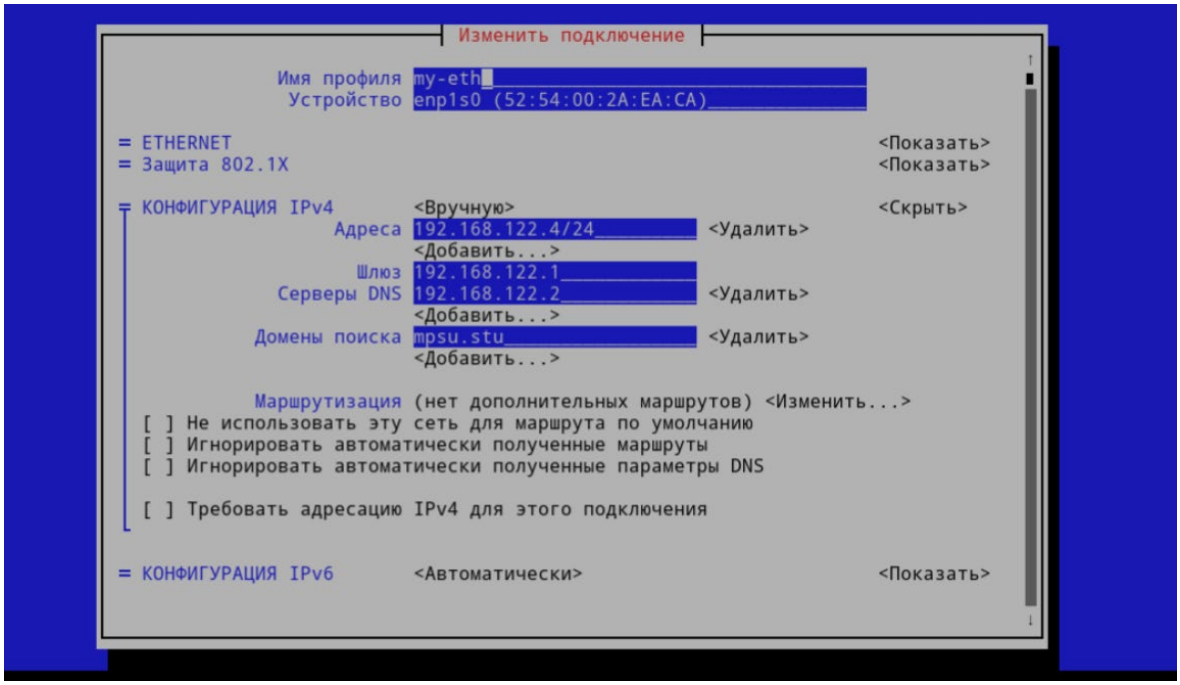
Отключить сетевой интерфейс

```
nmcli connection down my-eth
```

Созданные настройки сохраняются в виде конфигурационного файла в директории /etc/NetworkManager/system-connections/. При необходимости возможно отредактировать его вручную. После редактирования необходимо перегрузить службу NetworkManager.

Для большего удобства настройки существует утилита nmtui с псевдографическим интерфейсом. С его помощью возможно настраивать основные параметры сети не прибегая к командам.

```
nmtui
```



1.9. Подключение к системе по SSH

SSH (англ. Secure Shell — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой

SSH работает в режиме точка-многоточка. В этом режиме есть некоторый узел, к которому могут подключаться другие узлы — сервер. Все клиенты подключаются к этому серверу.

В Linux системах обычно используется OpenSSH, где сервер обозначается sshd, что означает SSH демон (Daemon), а клиент SSH — ssh.

Запуск / статус / остановка / перезапустить / перечитать конфигурацию / включить / исключить автозагрузку:

systemctl start/status/stop/restart/reload/enable/disable sshd.service

Для аутентификации по ключам спользуется алгоритм асимметричного шифрования RSA. Пара ключей представлена публичным и приватным ключами. Ключи на клиенте хранятся в каталоге ~/.ssh в файлах :

◦ id_rsa – приватный ключ пользователя

◦ id_rsa.pub – публичный ключ пользователя

◦ known_hosts – публичные ключи ssh-серверов

На сервере командой **ssh-keygen** производится генерация ключей.

Командой **ssh-copy-id adminstd@A.B.C.D** передаётся публичный ключ на клиент по его IP-адресу A.B.C.D.

После этого клиент командой **ssh adminstd@A.B.C.D** может удалённо подключиться по протоколу SSH к серверу с IP-адресом A.B.C.D.

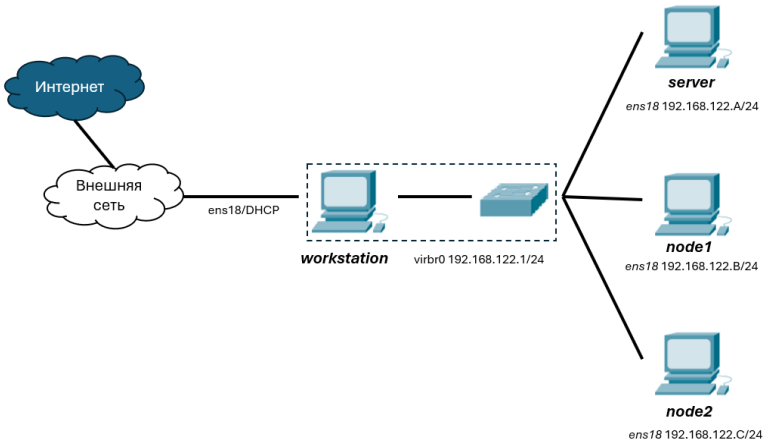
Команда scp (*Secure CoPy*) - это утилита, которая работает по протоколу SSH.

Она позволяет копировать файлы с клиента на сервер напрямую без использования протоколов FTP или SMB. Имеет следующий синтаксис:

```
$ scp опции пользователь1@хост1:файл пользователь2@хост2:файл
```

2. Практическая часть

Приведем еще раз рисунок виртуальных машин, объединенных в локальную сеть.



На машине workstation настроены два сетевых интерфейса – ens18 для выхода в интернет, адрес которого выдается динамически и интерфейс virbr0,

исполняющий роль сетевого моста между подсетью, выводящей в интернет и трех внутренних виртуальных машин. Адрес сетевого моста – 192.168.122.1/24, адреса виртуальных машин должны быть выбраны из той же подсети в соответствии с вашим вариантом (см. далее).

Задание 1

1. Используя параметры, приведённые в таблице ниже, настройте сеть, дополнив необходимые конфигурационные файлы. Server и Node1 настройте, используя конфигурационные файлы, Node2 – используя Network Manager.

Machine name	Server	Node1	Node2
Host name	server	node1	node2
IP address	192.168.122.(№ в группе + 1)	192.168.122.(№ в группе + 2)	192.168.122.(№ в группе + 3)
Mask	255.255.255.0		
Default gateway	192.168.122.1		

2. Проверьте соединение между workstation и каждой из машин используя утилиту ping. Проверьте соединение между машинами.
3. Попробуйте отправить **ping** между машинами используя доменное имя. Получилось ли это сделать? Если нет, то исправьте это.

Задание 2.

1. На машине workstation запустите службу ssh и добавьте её в автозагрузку (подробнее см. ЛР1).
2. Настройте аутентификацию по ключам с сервером и каждой из node.
3. Подключитесь из разных вкладок workstation к каждой из машин, используя созданного пользователя и доменное имя машины.

Задание 3.

1. Создайте на машине workstation файл, содержащее сообщение «Привет, сервер!» и передайте его на server используя утилиту scp.
2. Создайте на сервере в директории tmp файл и выгрузите его на машину workstation. Команду выполнить с workstation.
3. Находясь на машине workstation скопируйте файл с сообщением с сервера на любую из машин клиента.

Контрольные вопросы

1. Что такое ЛВС? Из каких устройств может состоять?
2. Из каких уровней состоит модель OSI? Для чего её создали?
3. Какие операционные системы могут использоваться на серверах?
4. Что такое виртуальная машина? Зачем она нужна?
5. Какие существуют способы передачи файлов по сети?

Список рекомендуемой литературы: