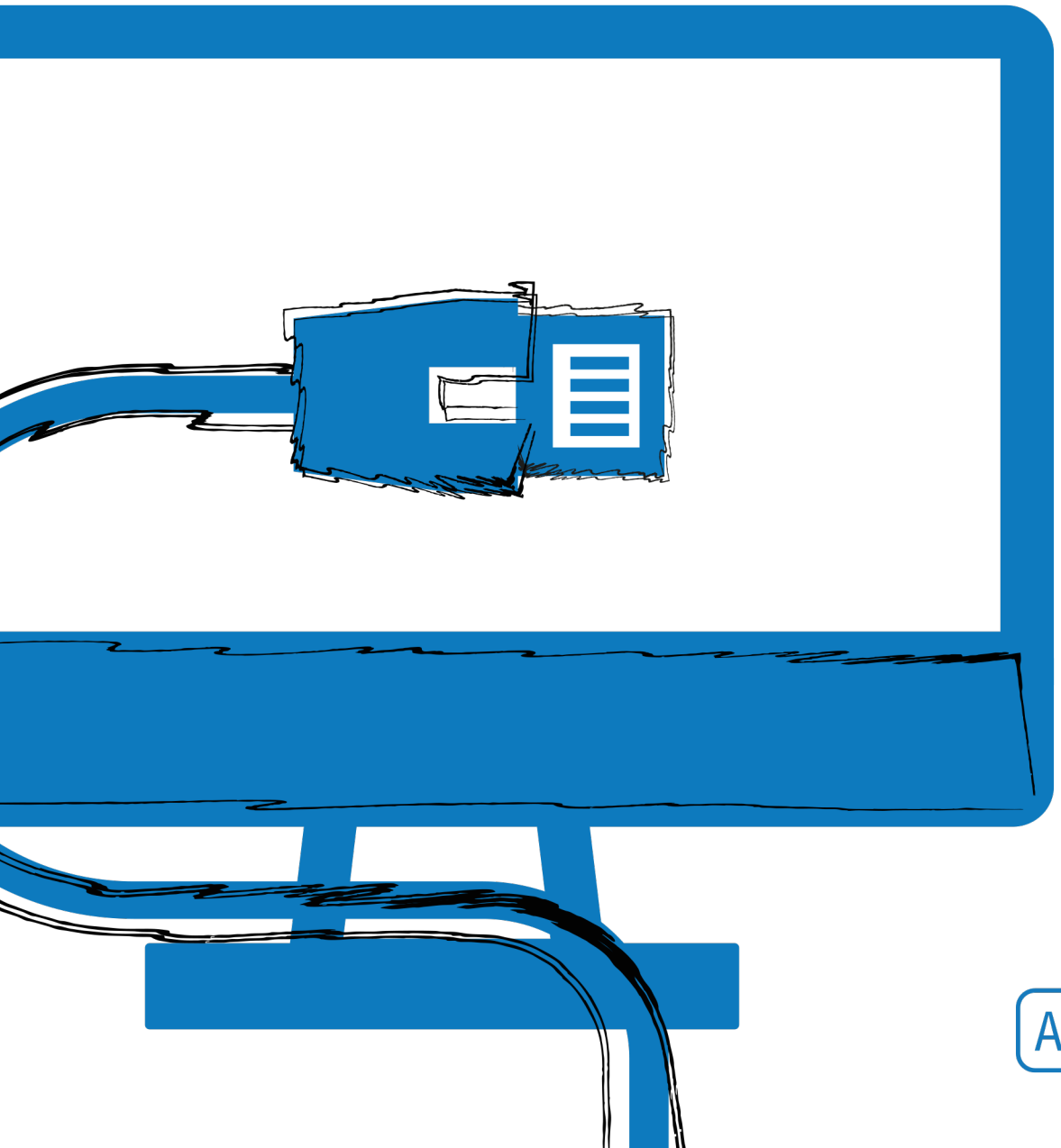
Курс AL-1704

Сборник практических заданий для курса



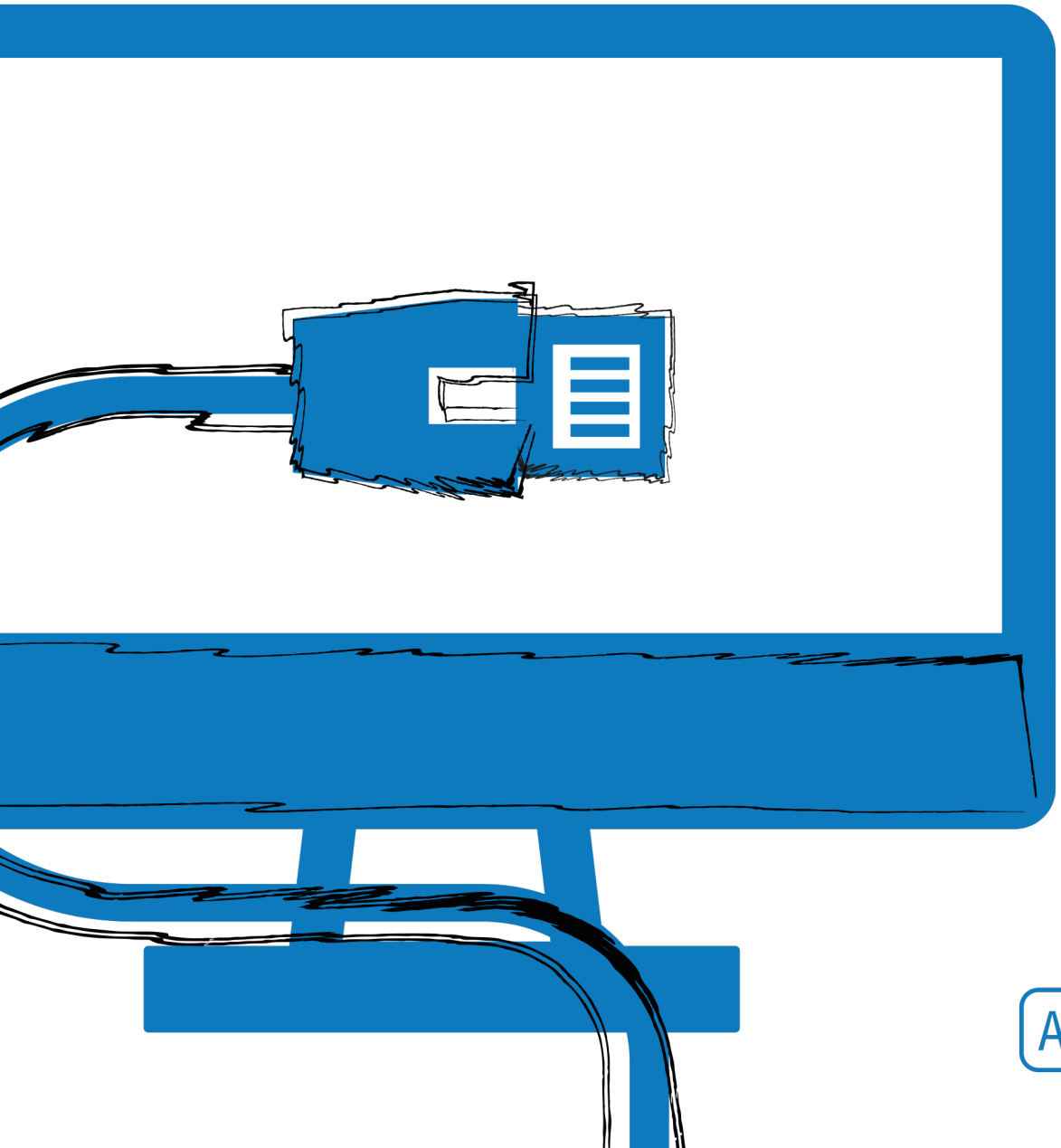
ASTRA LINUX®

Оглавление

Сборник практических заданий для курса «AL-1704. Сетевое администрирование Astra Linux 1.7»....4
Модуль 1. Основы TCP/IP сетей. Настройка и диагностика сети....5
Модуль 2. Настройка удаленного доступа....9
Модуль 3. Служба DNS....13
Модуль 4. Служба DHCP и настройка динамического DNS....18
Модуль 5. Прокси-сервер SQUID....23
Модуль 6. Синхронизация времени по сети....27
Модуль 7. Управление конфигурациями с помощью Ansible....30
Модуль 8. Служба каталогов на базе решения FreeIPA....35
Модуль 9. Веб-сервер на основе Apache....45
Модуль 10. Система электронной почты на базе Exim и Dovecot....53
Модуль 11. Защищенный комплекс программ для печати и маркировки документов....60
Модуль 12. Установка Astra Linux по сети....68
Модуль 13. Основы IPv6....73

Модуль 1

Основы TCP/IP сетей. Настройка и диагностика сети



ASTRA LINUX®

Сборник практических заданий для курса «AL-1704. Сетевое администрирование Astra Linux 1.7»

Требования:

- Компьютер со следующими характеристиками:
  - процессор архитектуры AMD64 (x86_64) не менее 8 ядер;
  - RAM не менее 32 ГБ;
  - NVME или SATA SSD диски, не менее 300ГБ свободного места.
- ОС GNU/Linux или Windows 10 (или более новые версии).
- VirtualBox 6.1

Материалы:

- Эталонная виртуальная машина template_1704_3:
  - Процессор — 1.
  - RAM — 2 ГБ.
  - Диск — 30 ГБ.
  - Сетевой адаптер — тип подключения «Сетевой мост».
  - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

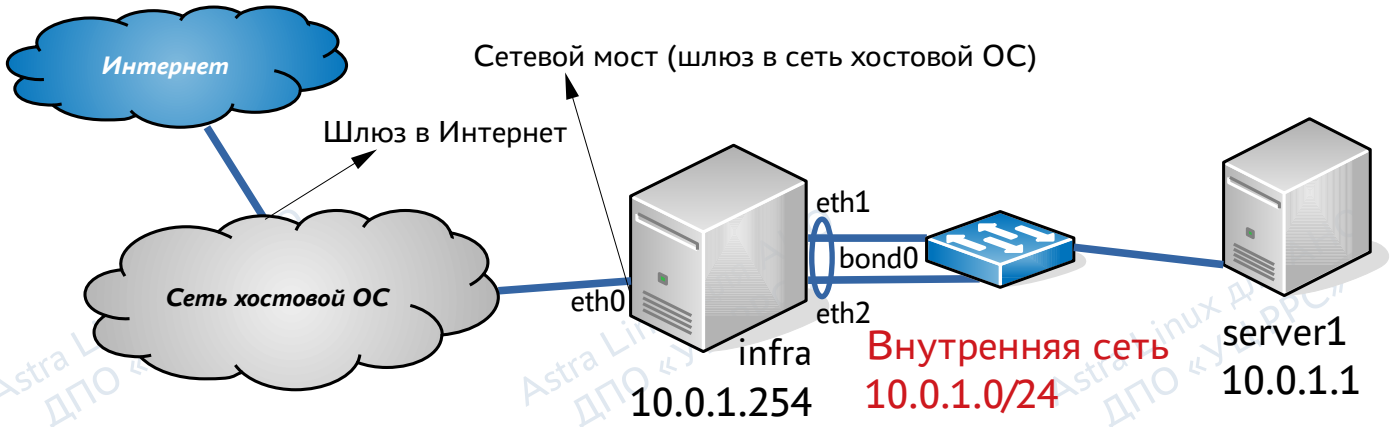
- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную ВМ должны быть внесены соответствующие изменения.

Модуль 1. Основы TCP/IP сетей. Настройка и диагностика сети

Описание практического задания

- Настройка сетевых интерфейсов в виртуальной машине (ВМ) infra с помощью Network Manager.
- Настройка сетевого интерфейса в ВМ server1 с помощью ifup/ifdown команд.
- Агрегирование (объединение) Ethernet интерфейсов на ВМ infra.

Схема сети



Настройка ВМ infra

Задание: Настроить ВМ infra, первоначально изменив имя хоста (infra), а затем настроить сетевое подключение, соответствующее интерфейсу eth0, с использованием Network Manager. Далее внести информацию об имени и адресе хоста в файл /etc/hosts и включить внутреннюю маршрутизацию.

1 Клонировать ВМ template_1704_3 и назвать новую ВМ infra.

2 Не запуская ВМ infra, добавить два сетевых интерфейса (всего три). Один (первый) интерфейс — сетевой мост, два других — внутренняя сеть.

3 Запустить ВМ infra.

4 Сменить имя хоста на infra с помощью команды hostnamectl.

5 Создать запись для infra в файле /etc/hosts.

6 Изменить имена соединений в Network Manager на net1, net2, net3 так, чтобы названия сетевых соединений для первого (eth0), второго (eth1) и третьего (eth3) интерфейсов имели вид net1, net2, net3.

7 Проверить, получил ли внешний интерфейс (сетевой мост) сетевые настройки по DHCP.

8 Настроить соединение net2: IP-адрес - 10.0.1.254/24. Проверить, что настройка сетевого соединения произведена успешно.

9 Включить внутреннюю маршрутизацию.

10 Настроить автоматическое включение маршрутизации при загрузке системы путем внесения изменений в файл /etc/sysctl.conf.

Настройка ВМ server1

Задание: Настроить ВМ server1, первоначально изменив имя хоста (server1), затем настроить сетевой интерфейс eth0 с использованием файла interfaces и внести информацию об имени и адресе хоста в файл /etc/hosts.

1 Клонировать ВМ template_1704_3 и назвать новую ВМ — server1.

2 Запустить ВМ.

3 Сменить имя хоста на server1 командой hostnamectl.

4 Добавить в файл /etc/hosts запись о server1.

5 Остановить и запретить запуск Network Manager.

6 Настроить сетевой интерфейс eth0 в файле /etc/network/interfaces:

- IP-адрес - 10.0.1.1/24;
- шлюз - 10.0.1.254

7 Перезапустить службу и проверить настройки сетевого интерфейса и доступность шлюза.

Настройка агрегации Ethernet интерфейсов

Задание: Настроить агрегацию сетевых интерфейсов eth1 и eth2 в режиме active-backup на хосте infra с использованием Netwotk Manager, затем произвести сетевые настройки агрегированного интерфейса и с помощью утилиты tcpdump проверить работоспособность агрегированного сетевого интерфейса путем отключения/включения интерфейсов.

1 Настройка производится на ВМ infra.

2 Убрать настройки и отключить сетевое соединение net2.

3 Создать (добавить) логический ведущий (master) интерфейс типа bond с именем сетевого интерфейса bond0 с помощью Network Manager.

4 Настроить Ethernet интерфейсы eth1 и eth2 как подчиненные (slave) интерфейсы.

5 Определить название сетевого соединения типа bond

6 Настроить статический адрес 10.0.1.254 на интерфейсе bond0.

7 Активировать настройки bond0.

8 Проверить, что интерфейс bond0 настроен и server1 доступен.

9 Включить на интерфейсе bond0 режим «активный-резервный».

10 Включить на интерфейсе bond0 режим переназначения MAC адреса на активный интерфейс (параметр fail_over_mac).

11 Активировать изменения на интерфейсе bond0 и проверить, что режимы агрегирования настроены верно.

12 Установить tcpdump.

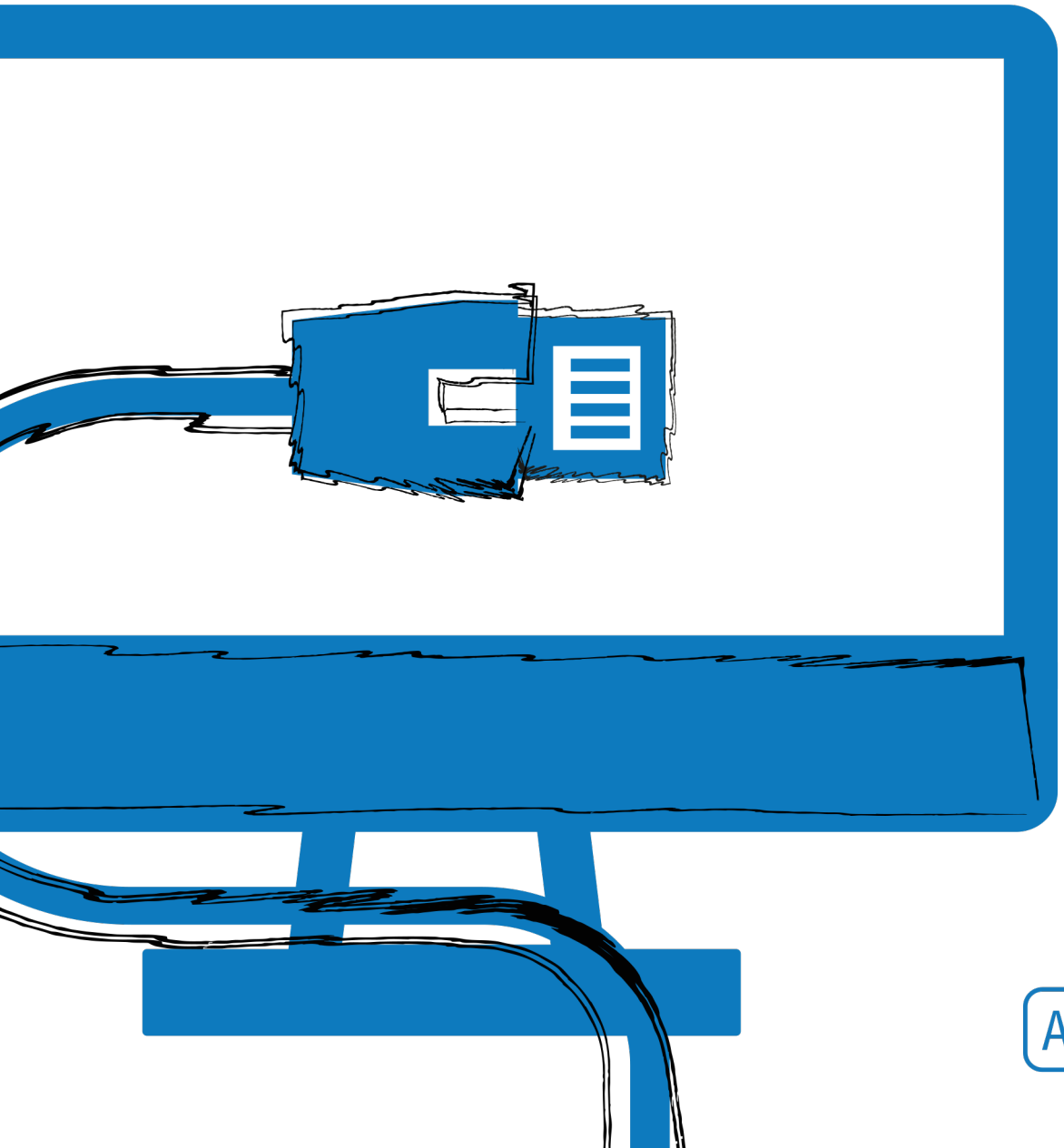
13 Запустить непрерывную проверку доступности хоста 10.0.1.1.

14 Запустить еще два терминала, в которых осуществлять перехват ICMP сообщений на интерфейсах eth1 и eth2.

15 В VirtualBox отключить сетевую карту (Устройства ➞ Сеть ➞ Подключить сетевой адаптер 2), по которой передаются данные и проверить, что передача данных производится по резервному каналу. Снова включить сетевую карту (сетевой адаптер 2).

Модуль 2

Настройка удаленного доступа



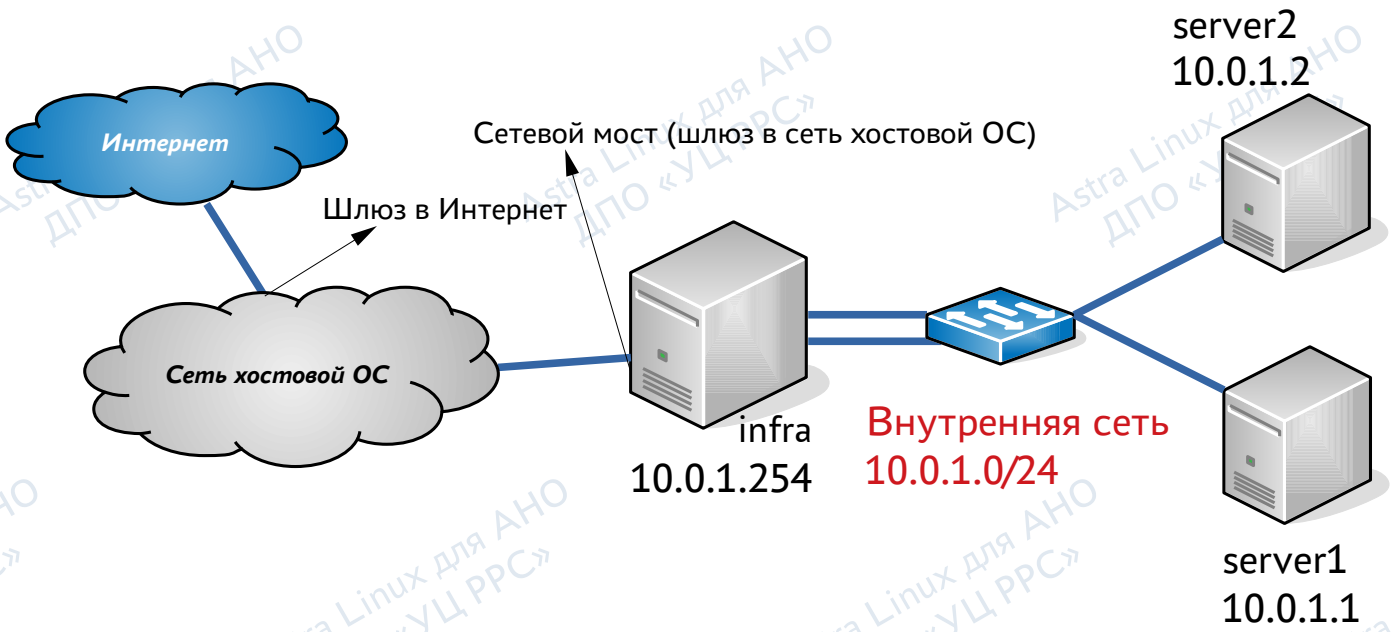
ASTRA LINUX®

Модуль 2. Настройка удаленного доступа

Описание практического задания

- Настройка аутентификации по ключам при подключении по SSH с ВМ infra к ВМ server1.
- Создание и настройка ВМ server2.
- Настройка аутентификации по ключам при подключении по SSH с ВМ infra к ВМ server2.
- Переадресация портов с помощью SSH:
  - динамическая переадресация и настройка утилиты apt;
  - переадресация локального порта для доступа к сетевым службам.

Схема сети



Настройка аутентификации по ключам

Задание: На хосте infra настроить аутентификацию по ключам при подключении к хосту server1 по SSH. Настроить ВМ server2:

- изменить имя хоста (server2),
- настроить сетевой интерфейс eth0 на server2 с использованием файла interfaces.

На хосте infra настроить аутентификацию по ключам при подключении к хосту server2 по SSH.

1 На server1 проверить работоспособность службы ssh. При необходимости запустить службу ssh и добавить ее в автозагрузку.

2 На infra настроить аутентификацию по ключам с server1 под учетными записями sa на клиенте и сервере.

3 Создать ВМ server2 путем клонирования ВМ template_1704_3.

4 В созданной ВМ server2 сменить имя хоста на server2.

5 Добавить в файл /etc/hosts запись для server2.

6 Остановить и запретить запуск Network Manager.

7 Настроить сетевой интерфейс eth0 в файле /etc/network/interfaces:

- IP адрес 10.0.1.2/24;
- шлюз 10.0.1.254

8 Перезапустить службу networking. Проверить настройки и доступность шлюза.

9 На server2 запустить проверить работоспособность службы ssh.

10 На infra настроить аутентификацию по ключам с server2 под учетными записями sa на клиенте и сервере.

Переадресация портов.

Задание: В первой части задания на хосте server1 запустить SOCKS-прокси с помощью SSH-туннеля через хост infra и настроить работу утилиты apt через SOCKS-прокси.

Во второй части задания на хосте server1 установить и запустить веб-сервер Apache. Отключить на веб-сервере режим работы AstraMode и обеспечить доступ к веб-серверу только по адресу 127.0.0.1. На хосте infra с помощью SSH настроить переадресацию локального порта для доступа к веб-серверу, работающему на хосте server1.

1 На ВМ server1 настроить динамическую переадресацию (SOCKS-прокси) на хост infra.

2 Проверить, что SOCKS-прокси запустился.

3 Настроить работу утилиты apt через SOCKS-прокси:

- создать файл /etc/apt/apt.conf.d/70proxy;
- добавить в файл настройки для прокси;
- проверить, что apt работает через прокси.

4 На ВМ server1 установить веб-сервер apache2.

5 В файл /var/www/html/index.html поместить файл test.txt.

6 Произвести следующие настройки apache2:

- в файле /etc/apache2/apache2.conf задать параметр `AstraMode off`
- в файле /etc/apache2/ports.conf задать параметр `Listen 127.0.0.1:80`

7 Перезапустить службу apache2.

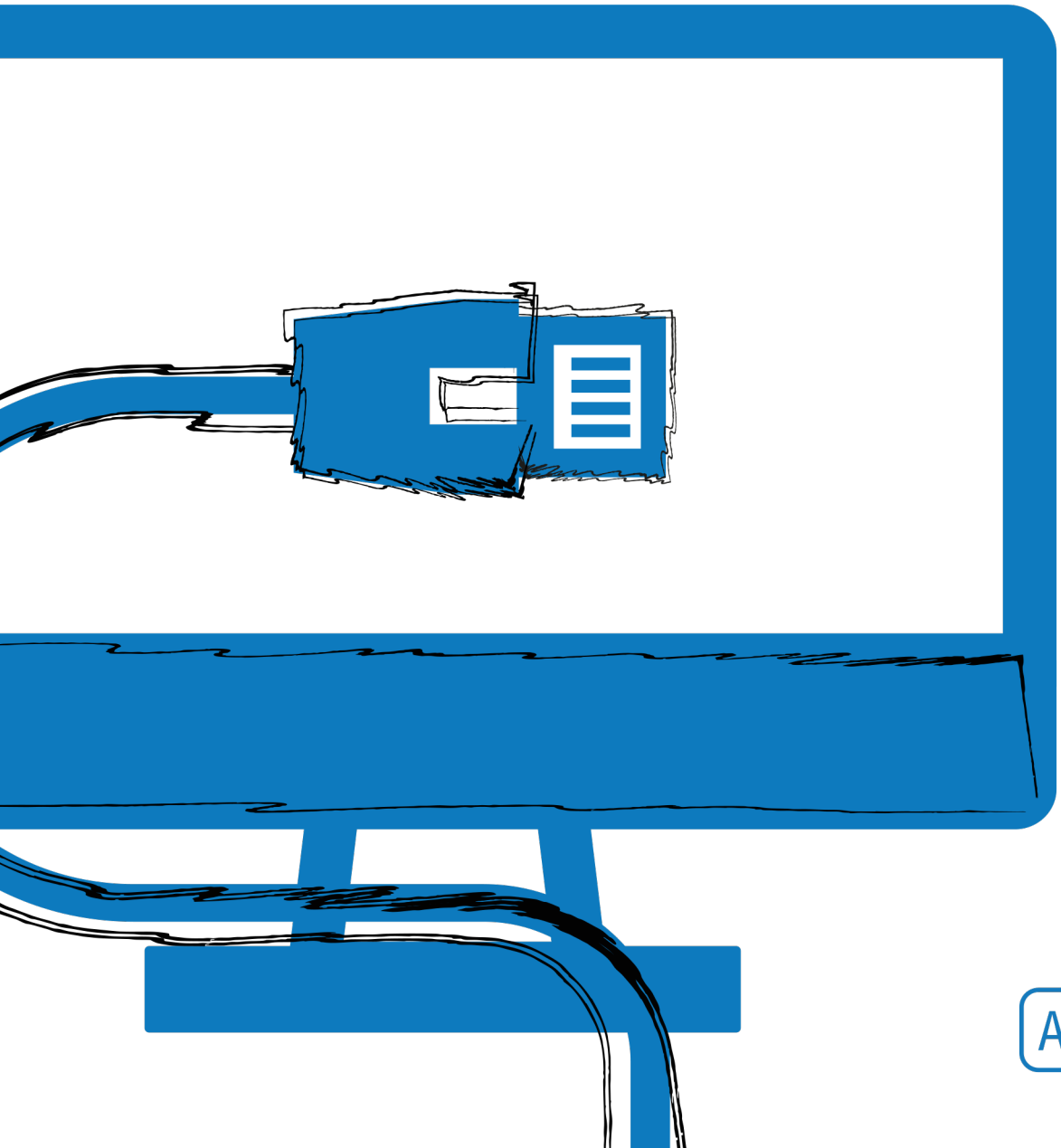
8 Проверить работоспособность apache2 сервера и что сервер доступен только локально.

9 На ВМ infra проверить доступ к веб- серверу, установленному на ВМ server1, с помощью утилиты curl.

10 Настроить локальную переадресацию порта 8080 на ВМ infra на порт 80 в ВМ server1.

11 Получить файл test.txt с FTP сервера с помощью утилиты curl.

Модуль 3
Служба DNS



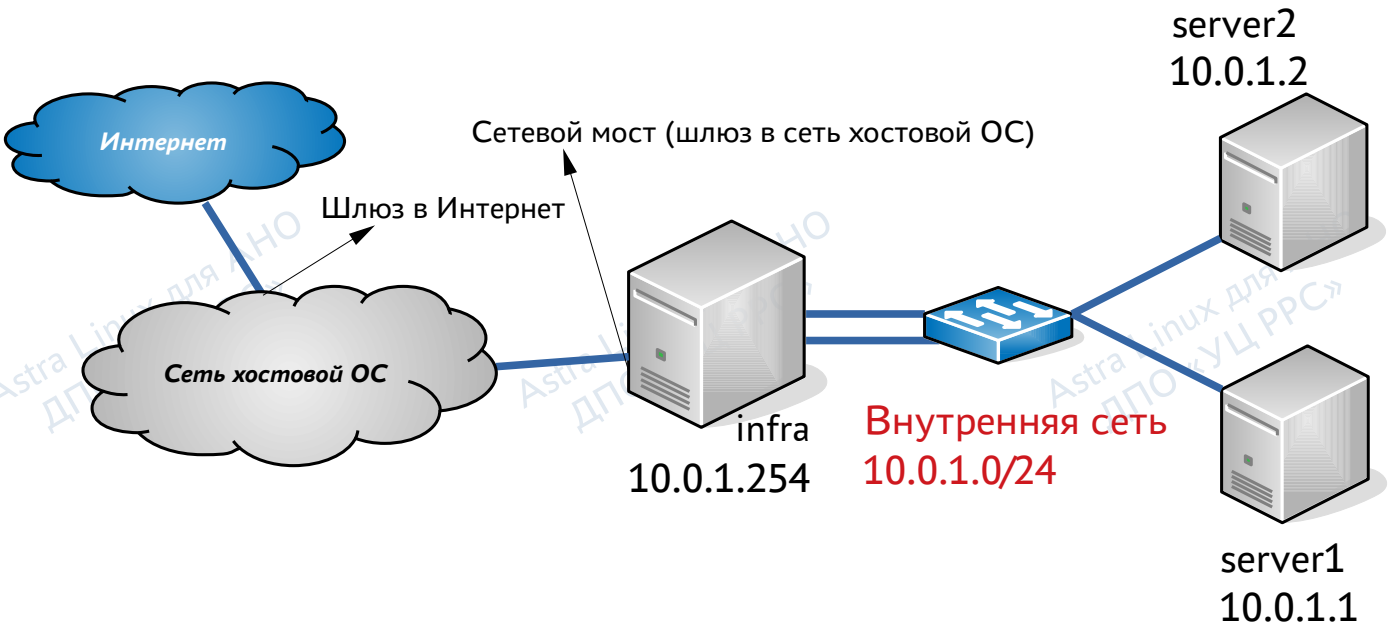
ASTRA LINUX®

Модуль 3. Служба DNS

Описание практического задания

- Настройка ведущего DNS сервера.
- Настройка подчиненного DNS сервера.
- Настройка кэширующего сервера.
- Настройка клиентской части DNS.

Схема сети



Настройка ведущего сервера DNS для зон astra.test и 1.0.10.in-addr.arpa

Задание: На хосте server1 установить DNS-сервер bind9. Настроить на хосте server1 ведущий (master) DNS-сервер для зон astra.test и 1.0.10.in-addr.arpa: в файле /etc/bind/named.conf.local создать описание для этих зон и создать файлы с зонной информацией.

Зонная информация должна включать записи типа SOA и NS (DNS-серверы: server1.astra.test и server2.astra.test), а также информацию о хостах infra, server1 и server2. Для имени server1.astra.test требуется определить псевдоним www.astra.test.

1 В ВМ server1 установить bind9.
Примечание: следует использовать SOCKS-прокси.

2 В файле /etc/bind/named.conf.local описать зону astra.test, для которой server1 является ведущим сервером DNS.

3 В файле /etc/bind/named.conf.local описать зону 1.0.10.in-addr.arpa, для которой server1 является ведущим сервером DNS.

4 Проверить правильность внесенных изменений в настройки сервера DNS.

5 Создать каталог /var/cache/bind/master. Назначить группу bind группой — владельцем созданного каталога и установить бит защиты sgid.

6 Создать файл astra.test в каталоге /var/cache/bind/master с ресурсными записями для зоны astra.test:

- SOA;
- NS (server1.astra.test и server2.astra.test);
- A – для server1.astra.test, server2.astra.test, infra.astra.test (внутренний интерфейс);
- CNAME www → server1.

7 Проверить правильность внесения зонной информации в файл astra.test.

8 Создать файл 10.0.1 в каталоге /var/cache/bind/master с ресурсными записями для зоны 1.0.10.in-addr.arpa:

- SOA;
- NS (server1.astra.test и server2.astra.test);
- PTR (для адресов 10.0.1.1, 10.0.1.2, 10.0.1.254).

9 Проверить правильность внесения зонной информации в файл 10.0.1.

10 Перезапустить сервер DNS и проверить, что служба DNS работает.

Настройка подчиненного сервера DNS для зон astra.test и 1.0.10.in-addr.arpa

Задание: На хосте server2 установить DNS-сервер bind9. Настроить на хосте server2 подчиненный (slave) DNS-сервер для зон astra.test и 1.0.10.in-addr.arpa. Для этого в файле /etc/bind/named.conf.local нужно создать описание для этих зон, указав в качестве ведущего DNS-сервера server1. Убедиться, что трансфер зонной информации прошел успешно.

1 В ВМ server2 установить bind9.
Примечание: использовать SOCKS-прокси и настроить работу apt через прокси.

2 Проверить запущена ли служба bind9. Если не служба не работает, то запустить.

3 Создать каталог /var/cache/bind/slave. Назначить группу bind группой — владельцем созданного каталога и установить на каталог бит защиты sgid.

4 Настроить server2 как подчиненный (slave) сервер для зоны astra.test. Для этого внести соответствующие изменения в файл /etc/bind/named.conf.local. Зонную информацию хранить в файле /var/cache/bind/slave/astra.test.

5 Настроить server2 как подчиненный (slave) сервер для зоны 1.0.10.in-addr.arpa. Для этого внести соответствующие изменения в файл /etc/bind/named.conf.local. Зонную информацию хранить в файле /var/cache/bind/slave/10.0.1.

6 Проверить правильность внесенных изменений в настройки сервера DNS.

7 Перезапустить сервер DNS и проверить, что служба DNS работает.

8 Настроить перенаправление DNS запросов по разрешению имен внешних (Интернет) DNS имен на кэширующий сервер (infra). Для этого внести изменения в файл /etc/bind/named.conf.options на server2.

Настройка кэширующего сервера DNS

Задание: На хосте infra настроить кэширующий DNS-сервер. На DNS-серверах server1 и server2 настроить ретрансляцию запросов на DNS-сервер infra.

1 Настройка производится на ВМ infra.

2 В ВМ infra установить bind9.

3 Проверить запущена ли служба bind9. Если не служба не работает, то запустить.

4 На DNS-серверах server1 и server2 настроить ретрансляцию DNS-запросов на кэширующий DNS-сервер infra. Для этого внести соотвествующие изменения в файлы /etc/bind/named.conf.options.

Настройка клиентской части DNS

Задание: На хостах server1 и server2 настроить DNS-клиент, внеся изменения в файл resolv.conf. Для хостов server1 и server2 в качестве DNS-сервера указать адрес локального хоста. Настроить DNS-клиент на хосте infra с помощью Network Manager. В качестве DNS-серверов указать адреса хостов server1 и server2.

1 Настроить клиентскую часть DNS, указав в качестве DNS серверов:

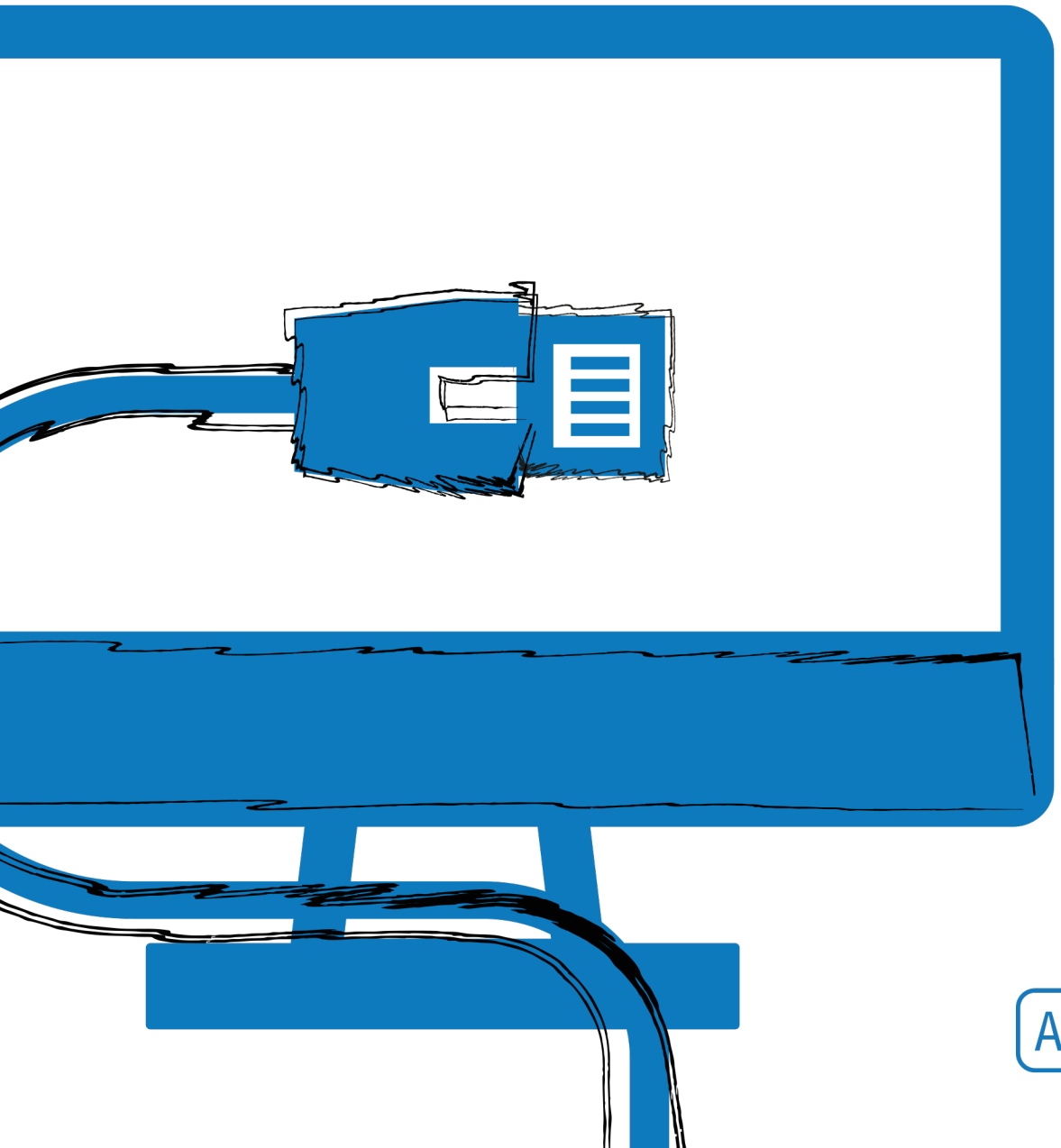
- на server1 — DNS-сервер - localhost;
  В файл /etc/resolv.conf внести запись.

- на server2 — DNS-сервер localhost;
  В файл /etc/resolv.conf внести запись.
- на infra — server1 и server2.

2 Убедиться, что разрешаются имена и адреса как во внутренней сети, так и в сети Интернет во всех трех ВМ: server1, server2, infra.

Модуль 4

Служба DHCP и настройка динамического DNS



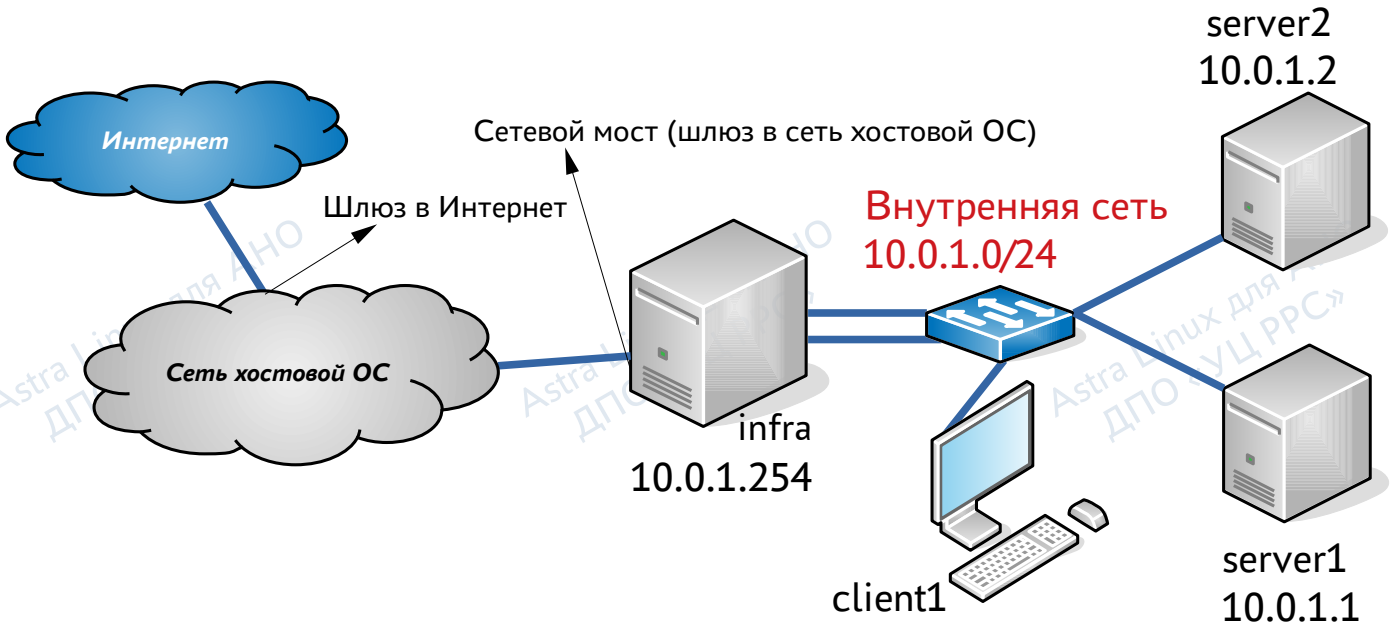
ASTRA LINUX®

Модуль 4. Служба DHCP и настройка динамического DNS

Описание практического задания

- Настройка службы DHCP для выдачи и получения динамического IP адреса.
- Настройка службы DHCP для выдачи и получения фиксированного IP адреса.
- Настройка динамического DNS.

Схема сети



Настройка выдачи и получения динамических IP адресов

Задание: На хосте server1 установить DHCP-сервер. Настроить DHCP-сервер для выдачи динамических IP-адресов из диапазона 10.0.1.101-10.0.1.199, передавая клиентам сетевые настройки (адреса DNS-серверов и шлюза). Создать и настроить ВМ client1. Убедиться, что хост client1 получил IP-адрес и сетевые настройки от DHCP-сервера. На хосте server1 получить информацию о выданных в аренду адресах.

1 На server1 установить сервер DHCP.

2 В файле /etc/default/isc-dhcp-server определить, на каком сетевом интерфейсе будет работать сервер DHCP.

3 Выделить диапазон 10.0.1.101-10.0.1.199 для выдачи динамических IP адресов. Сервер DHCP должен передавать адрес шлюза (10.0.1.254) и адреса серверов DNS (10.0.1.1, 10.0.1.2). Внести соответствующие изменения в файл /etc/dhcp/dhcpd.conf.

4 Запустить службу DHCP и проверить, что служба запущена.

5 Путем клонирования ВМ template_1704_3 создать и запустить ВМ client1.

6 Изменить имя хоста на client1.

7 В файла /etc/hosts заменить astra на client1:
```
127.0.1.1    client1
```

8 Подумать, какой dhcp клиент используется в ВМ client1 и почему?

9 Проверить, что IP адрес и другие настройки в ВМ client1 были получены от DHCP-сервера server1. Определить срок аренды.

10 На сервере DHCP (ВМ server1) с помощью команды `dhcp-lease-list` получить информацию о выданных IP-адресах.

Настройка выдачи и получения фиксированного IP адреса

Задание: На хосте server2 настроить получение IP-адреса по DHCP и узнать MAC-адрес сетевого интерфейса.

Настроить DHCP сервер на хосте server1 для выдачи адреса 10.0.1.2 хосту server2 и передачи сетевых настроек (адрес DNS-сервера - 127.0.0.1 и адрес шлюза).

1 В ВМ server2 настроить получение адреса по DHCP. Внести соответствующие изменения в файл /etc/network/interfaces.

2 Деактивировать сетевой интерфейс.

3 Перезапустить службу networking и проверить, что IP адрес получен с сервера DHCP.

4 В ВМ server1 настроить службу DHCP для выдачи фиксированного IP адреса (10.0.1.2/24) хосту server2. Внести соответствующие изменения в файл /etc/dhcp/dhcpd.conf, указав в параметрах шлюз по умолчанию, а в качестве сервера DNS — localhost.
Примечание: узнать MAC адрес сетевого интерфейса хоста server2 можно, например, командой dhcp-lease-list.

5 Перезапустить службу DHCP:

6 На хосте server2 деактивировать сетевой интерфейс, перезапустить службу networking и проверить получение IP адреса, маршрут по умолчанию и разрешение имен DNS.

Настройка динамического обновления зонной информации на DNS сервере

Задание: На хосте server1 создать ключ (алгоритм MD5, длина ключа 128 бит) и добавить описание ключа в настройки ведущего DNS-сервера (файл /etc/bind/named.conf.local). В настройках ведущего DNS-сервера разрешить обновление зонной информации с использованием созданного ключа.

Далее в настройках DHCP-сервера включить возможность передачи данных о хостах, которым выданы динамические IP-адреса, DNS-серверу. Определить параметр, задающий имя домена, добавить информацию о ключе и зонах, в которых должна обновляться информация, указав адрес ведущего DNS-сервера. В заключении убедиться, что информация об имени и IP-адресе хоста client1 добавилась в зоны astra.test и 1.0.10.in-addr.arpa.

1 Настроить службу DNS (server1):

- Убедиться, что пользователь bind имеет право создавать файлы в каталоге, в котором хранятся файлы с зонной информацией.
- С помощью утилиты dnssec-keygen создать ключ с именем dhcp-dns, используя алгоритм хеширования MD5 для формирования кода аутентификации сообщений (HMAC-MD5). Длина ключа — 128 бит.
- Значение ключа сохраняется в файл в текущем каталоге с суффиксом .private.
- В файл /etc/bind/named.conf.local добавить секцию типа key, в которой описываются параметры созданного ключа.
- В секции типа zone добавить разрешение обновлять зонную информацию с помощью созданного ключа.
- Перезапустить службу DNS и проверить ее статус.

2 Настроить службу DHCP (server1):

- В файл /etc/dhcp/dhcpd.conf внести следующие изменения:

– Определить параметр domain-name.

– Определить параметры ddns-update-style и ddns-updates.

– Добавить секцию типа key с описанием параметров созданного ранее ключа (такую же, как в настройках службы DNS).

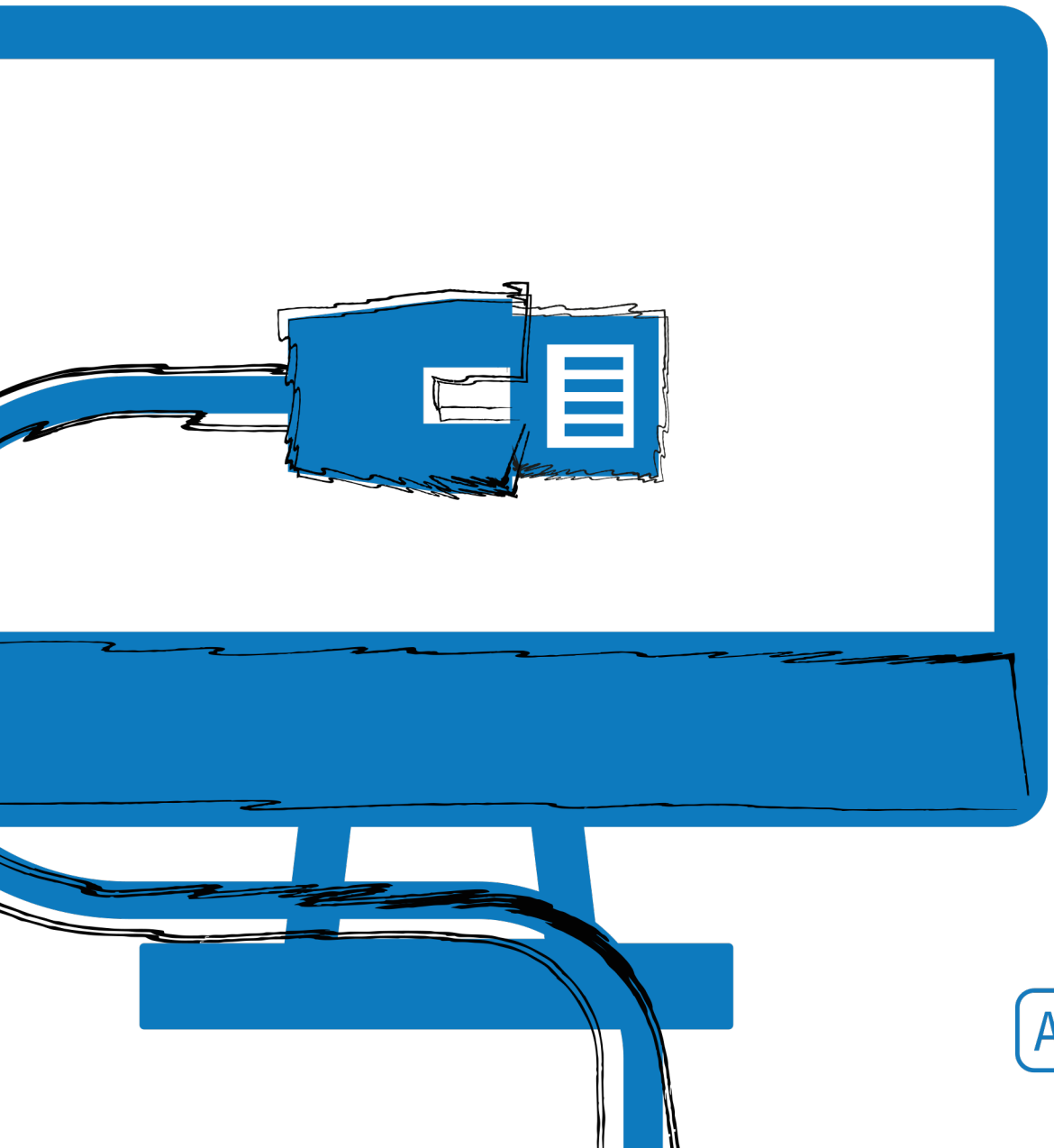
– Создать секции типа zone для зон astra.test и 1.0.10.in-addr.arpa, в которых определяются ведущий сервер DNS и используемый для обновления ключ.

- Перезапустить службу DHCP и проверить статус службы:

3 В ВМ client1 активировать сетевое соединение командой nmcli.

4 Проверить, что зонная информация обновилась на обоих серверах DNS (server1 и server2) и включает ресурсные записи для хоста client1 в зонах astra.test и 1.0.10.in-addr.arpa.

Модуль 5
Прокси-сервер SQUID



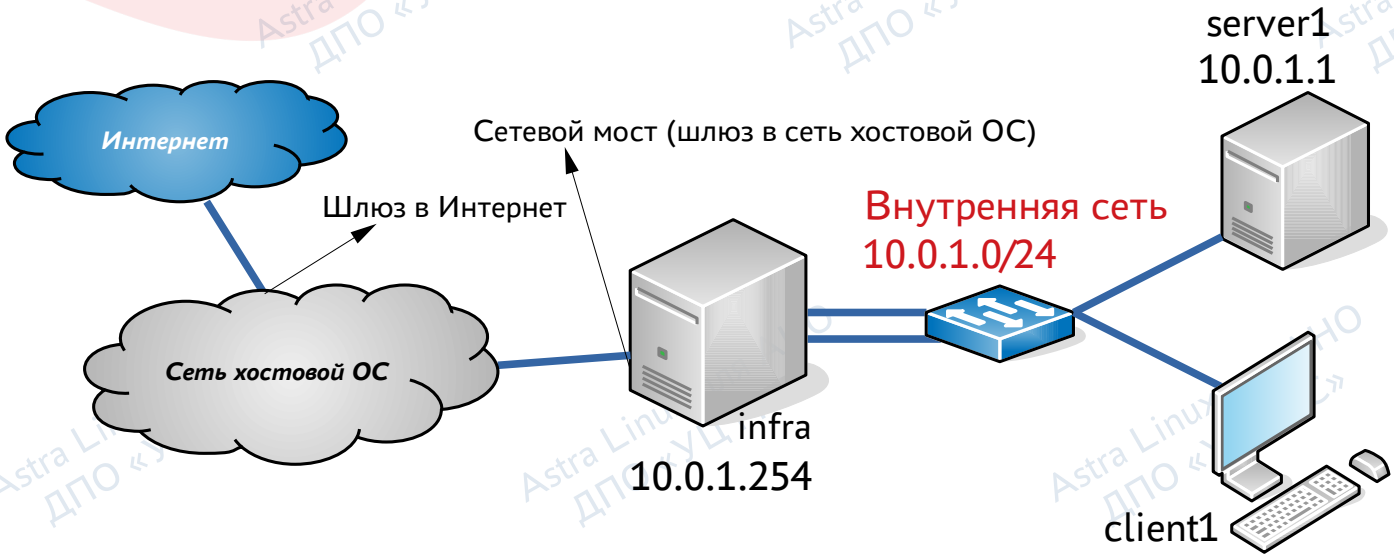
ASTRA LINUX®

Модуль 5. Прокси-сервер SQUID

Описание практического задания

- Установка и первоначальная настройка SQUID.
- Настройка базовой аутентификации в SQUID.
- Настройка ограничения доступа пользователей к web-ресурсам по времени.

Схема сети



Установка и первоначальная настройка SQUID

Задание: На хосте infra установить прокси-сервер SQUID и разрешить доступ к прокси-серверу для хостов из сети 10.0.1.0/24.

1 Установить SQUID на ВМ infra.

2 Сохранить исходный вариант конфигурационного файла SQUID.

3 На основе исходного конфигурационного файла SQUID создать новый конфигурационный файл, исключив комментарии и пустые строки, содержащиеся в исходном файле.

4 Создать в конфигурационном файле /etc/squid/squid.conf список управления доступом типа src с именем localnet, добавив в этот список управления доступом все хосты из сети 10.0.1.0/24.

5 Включить в /etc/squid/squid.conf правило разрешающее хостам, определенным в списке управление доступом localnet, обращаться к прокси-серверу.
Примечание: правило должно быть размещено до запрещающего правила http_access deny all.

6 Выполнить команду, которая позволяет перечитать измененный конфигурационный файл.

7 Проверить доступность сервера SQUID и возможность доступа к Интернет ресурсам на ВМ client1 (используйте браузер Firefox).

Настройка базовой аутентификацию NCSA

Задание: На хосте infra установить программный пакет apache2-util. С помощью команды htpasswd создать учетную запись пользователя iuser, при этом пароли пользователей хранить в файле /etc/squid/passwd. Настроить на прокси-сервере SQUID NCSA аутентификацию пользователей. Убедиться, что аутентификация пользователей на прокси-сервере работает правильно.

1 Установить программный пакет apache2-utils на infra.

2 Командой htpasswd создать пользователя iuser на infra.
Примечание: используйте параметр `-c имя_файла_с_паролями`, когда первый раз выполняете команду `htpasswd`.

3 Установить владельцев proxy:proxy и права 640 на файл с паролями.

4 Внести изменения в конфигурационный файл SQUID:

- Настроить схему аутентификации NCSA с помощью директивы auth_param.
- Определить список управления доступом типа proxy_auth с именем authusers, который содержит всех валидных пользователей.
- Добавить правило, запрещающее доступ пользователям, не указанным в списке управления доступом authusers, и правило, разрешающее доступ валидным пользователям.
  Примечание: правила должны быть размещены до последнего правила, запрещающего доступ всем, и до правила localnet.

5 Выполнить перечитывание конфигурационного файла сервером SQUID.

6 Проверить, работает ли аутентификация для SQUID с ВМ client1.

Настройка запрета доступа к веб-ресурсам в указанный временной диапазон (запретить доступ к youtube в рабочее время)

Задание: Добавить в настройки прокси-сервера два списка управления доступом: один соответствует домену назначения youtube.com, другой – диапазону рабочего времени (с 9 до 18 часов). Создать на прокси-сервере правило, запрещающее доступ к ресурсам из домена youtube.com в рабочее время. Убедиться, что правило работает.

1 На хосте client1 проверить доступность youtube.com.

2 Создать список управления доступом типа dstdomain, который включает домен youtube.com.

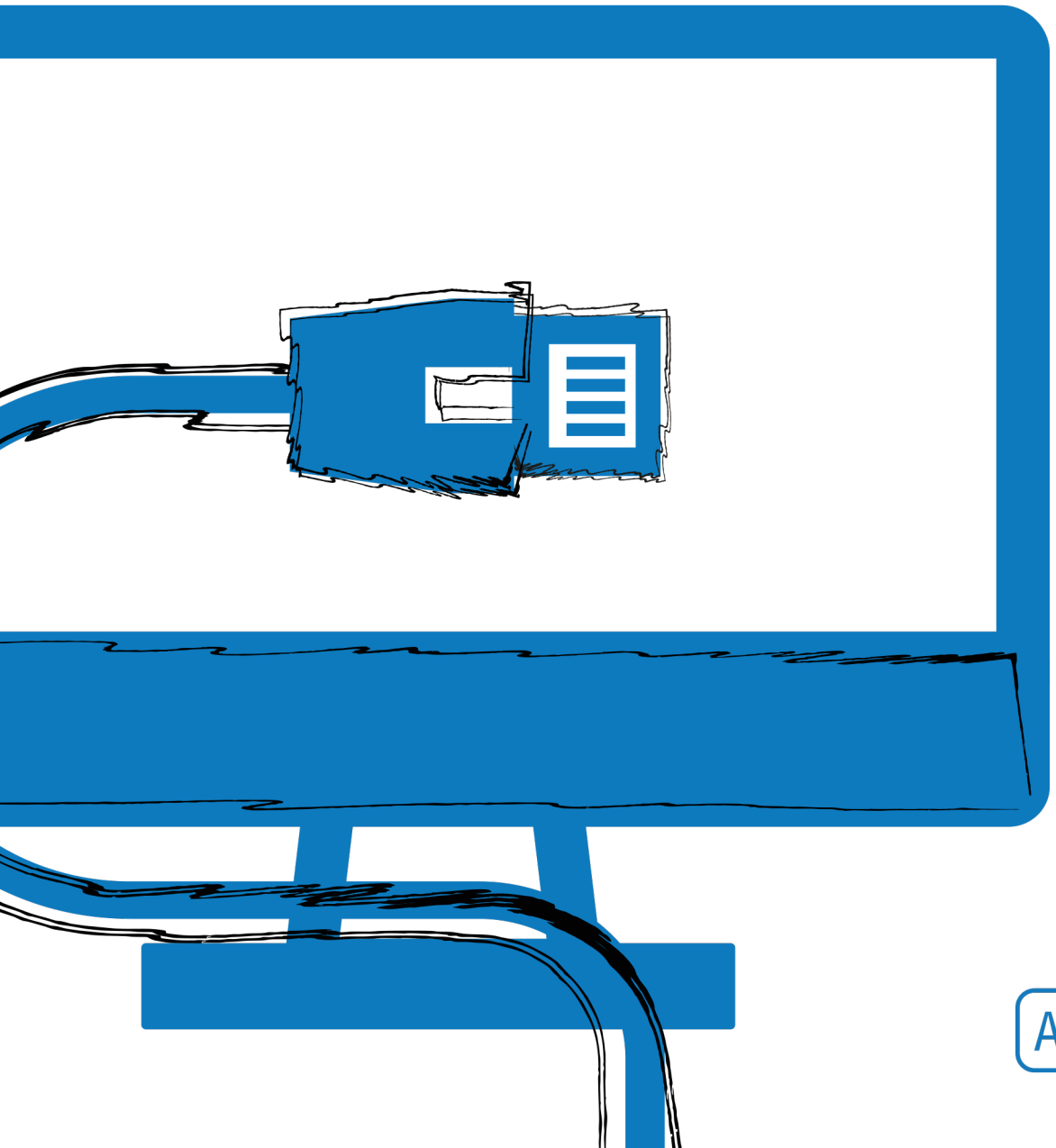
3 Создать список управления доступом типа time, который определяет рабочее время.

4 Добавить правило, которое запрещает доступ к сайтам в домене youtube.com в рабочее время, указав одновременно оба списка управления доступом.
Примечание: поместите правило в нужно место в файле /etc/squid/squid.conf, чтобы оно сработало.

5 На хосте client1 проверить доступность youtube.com.

Модуль 6

Синхронизация времени по сети



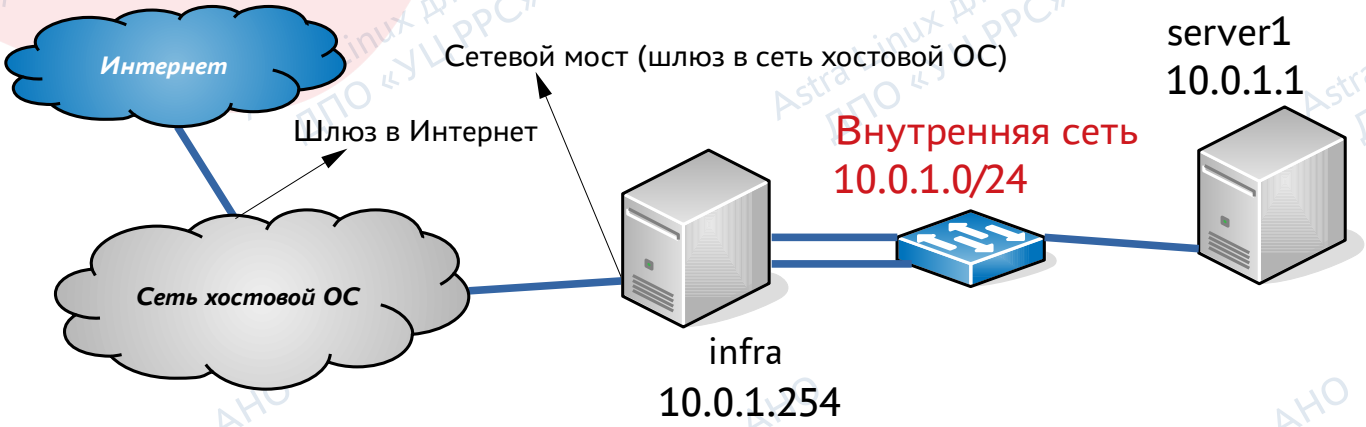
ASTRA LINUX®

Модуль 6. Синхронизация времени по сети

Описание практического задания

- Настройка службы chrony.
- Настройка встроенной в systemd службы синхронизации времени.

Схема сети



Настройка синхронизации времени с помощью службы chrony

Задание: На хосте infra настроить службу chrony, указав в качестве источников времени публичные NTP-серверы. Разрешить только хостам из сети 10.0.1.0/24 использовать сервер infra в качестве источника времени. Убедиться, что синхронизация времени на хосте infra происходит успешно.

1 Настроить службу chrony на ВМ infra:
   - В качестве источников времени выбрать сервер ntp1.vniiftri.ru и пул ru.pool.ntp.org. Убрать все лишние источники времени.
   - Разрешить доступ к серверу infra только хостам из сети 10.0.1.0/24.
   - Для параметра maxupdateskew установить значение, характерное для надежного быстрого сетевого соединения.

2 С помощью утилиты chronyc проверить, что синхронизация времени производится.

Настройка синхронизации времени с помощью systemd

Задание: На хосте server1 настроить синхронизацию, используя службу systemd-timesyncd. В качестве источника времени использовать сервер infra.

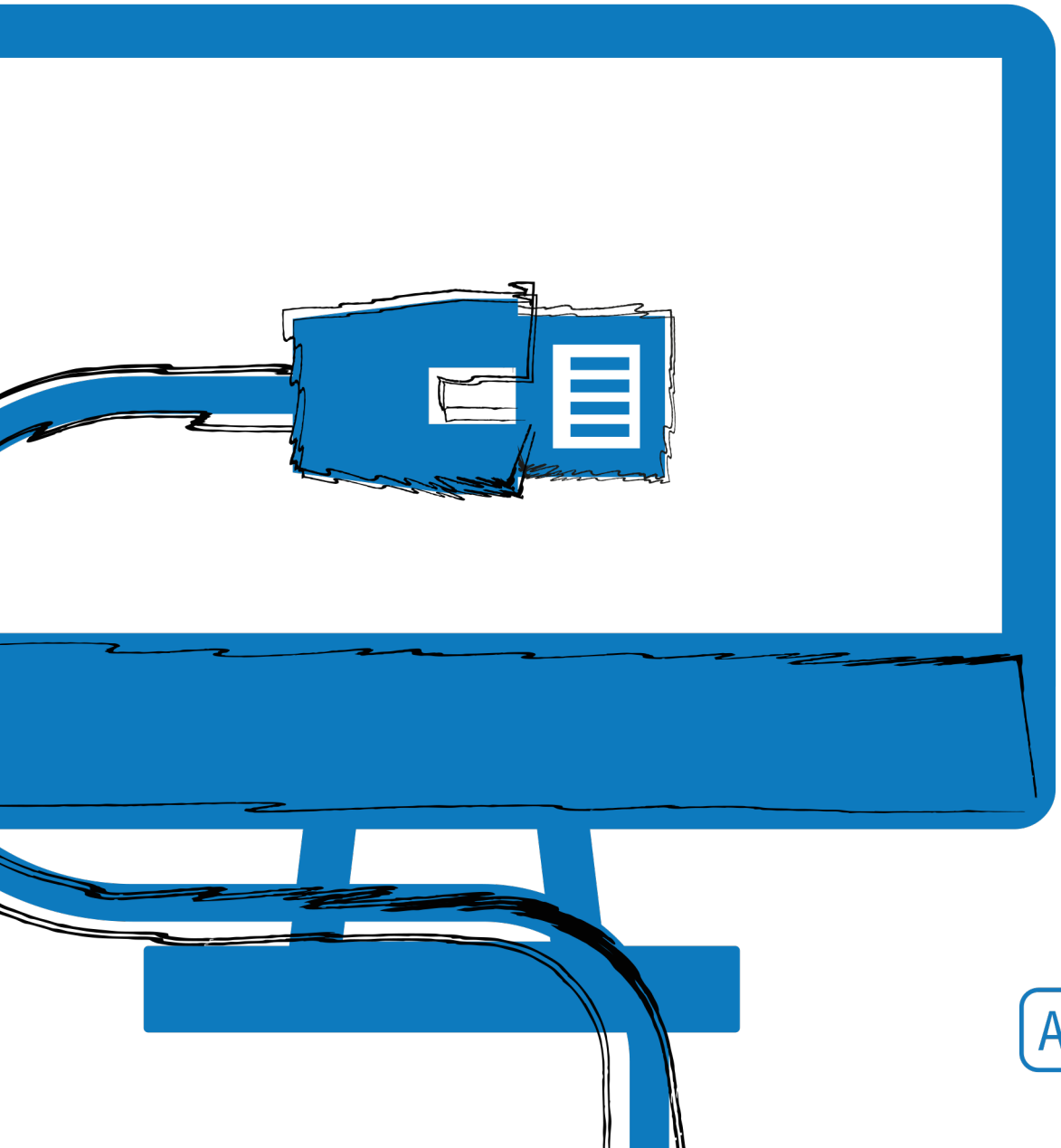
1 Удалить службу ntpd.

2 Настроить синхронизацию времени для ВМ server1, используя встроенную в systemd NTP службу. Источник времени — infra.
Примечание: для выполнения данного задания требуется снять запрет на запуск службы systemd-timesyncd путем комментирования в файле /lib/systemd/system/systemd-timesyncd.service.d/disable-with-time-daemon.conf строки
ConditionFileIsExecutable=!/usr/sbin/VboxService

3 Убедиться, что синхронизация времени проходит успешно.

Модуль 7

Управление конфигурациями с помощью Ansible



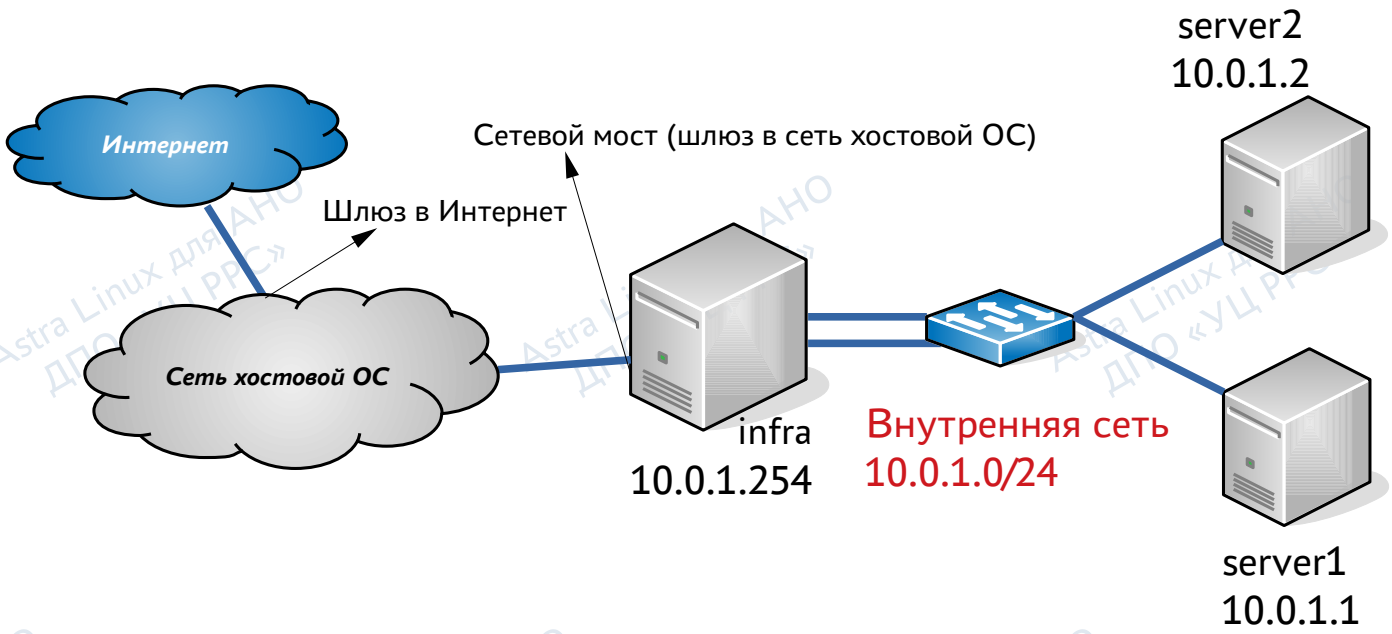
ASTRA LINUX®

Модуль 7. Управление конфигурациями с помощью Ansible

Описание практического задания

- Установка Ansible.
- Создание инвентаризационного файла.
- Использование ansible в командной строке.
- Автоматизация установки и настройки веб-сервера Apache.

Схема сети



Установка ansible, использование ansible в командной строке и создание файла инвентаризации

Задание: На хосте infra. Создать каталог ansible, в котором будут размещаться все файлы проекта. В этом каталоге создать файл инвентаризации hosts, в котором описать хосты server1, server2, infra и группу хостов servers, состоящую их server1 и server2.

Создать конфигурационный файл ansible.cfg, в котором произвести настройки, позволяющие использовать файл инвентаризации по умолчанию. С помощью команды ansible получить текущие даты и время всех хостов. В качестве дополнительного задания, используя команду ansible и модуль replace, привести строку в файле /etc/hosts, содержащую адрес и имя хоста к виду:
IP_адрес имя_хоста.astra.test имя_хоста.

1 Установить ansible на ВМ infra.

2 Настроить на ВМ infra SSH-аутентификацию по ключам с хостами server1 и server2.
Примечание: это должно было сделано ранее в Модуле 2 «Настройка удаленного доступа».

3 Дальнейшие действия осуществлять под учетной записью администратора системы (sa).

4 Создать в домашнем каталоге подкаталог ansible и перейти в него. Дальнейшие действия осуществлять в созданном каталоге.

5 Создать файл hosts, в который добавить:

- записи для хостов server1, server2 и infra;
- группу servers для хостов server1 и server2;
- переменные ansible_host для каждого хоста.

6 Настроить так, чтобы созданный файл инвентаризации использовался в командах Ansible по умолчанию. Для этого создать файл ~/ansible/ansible.cfg и внести в него соответствующие настройки.
Примечание: можно посмотреть содержимое файла /etc/ansible/ansible.cfg и сделать по аналогии.

7 С помощью команды ansible получить значения текущих дат и времени на server1 и server2.

8 (Дополнительное задание) Изменить информацию в файлах /etc/hosts, используя команду ansible:

- Просмотреть содержимое файлов /etc/hosts.
- Заменить строки вида:
  IP_адрес имя_хоста
  на
  IP_адрес имя_хоста.astra.test имя_хоста.
  Использовать модуль replace.
- Проверить новое содержимое файлов /etc/hosts.

Работа с переменными, создание плейбука (playbook)

Задание: С помощью сбора фактов получить информацию об использовании оперативной памяти на хосте server1. Создать плейбук, который на группы хостов servers:

- устанавливает веб-сервер Apcahe;

- отключает режим AstraMode;
- копирует разные файлы index.html на рабочий веб-сервер (server1) и тестовый веб-сервер (server2);
- перезапускает веб-серверы;
- получает содержимое веб-страниц index.html и выводит их на экран.

1 Получить информацию («факты») о хосте server1 с помощью команды ansible и узнать информацию об объеме и использовании оперативной памяти.
Примечание: используйте параметр filter модуля сбора фактов.

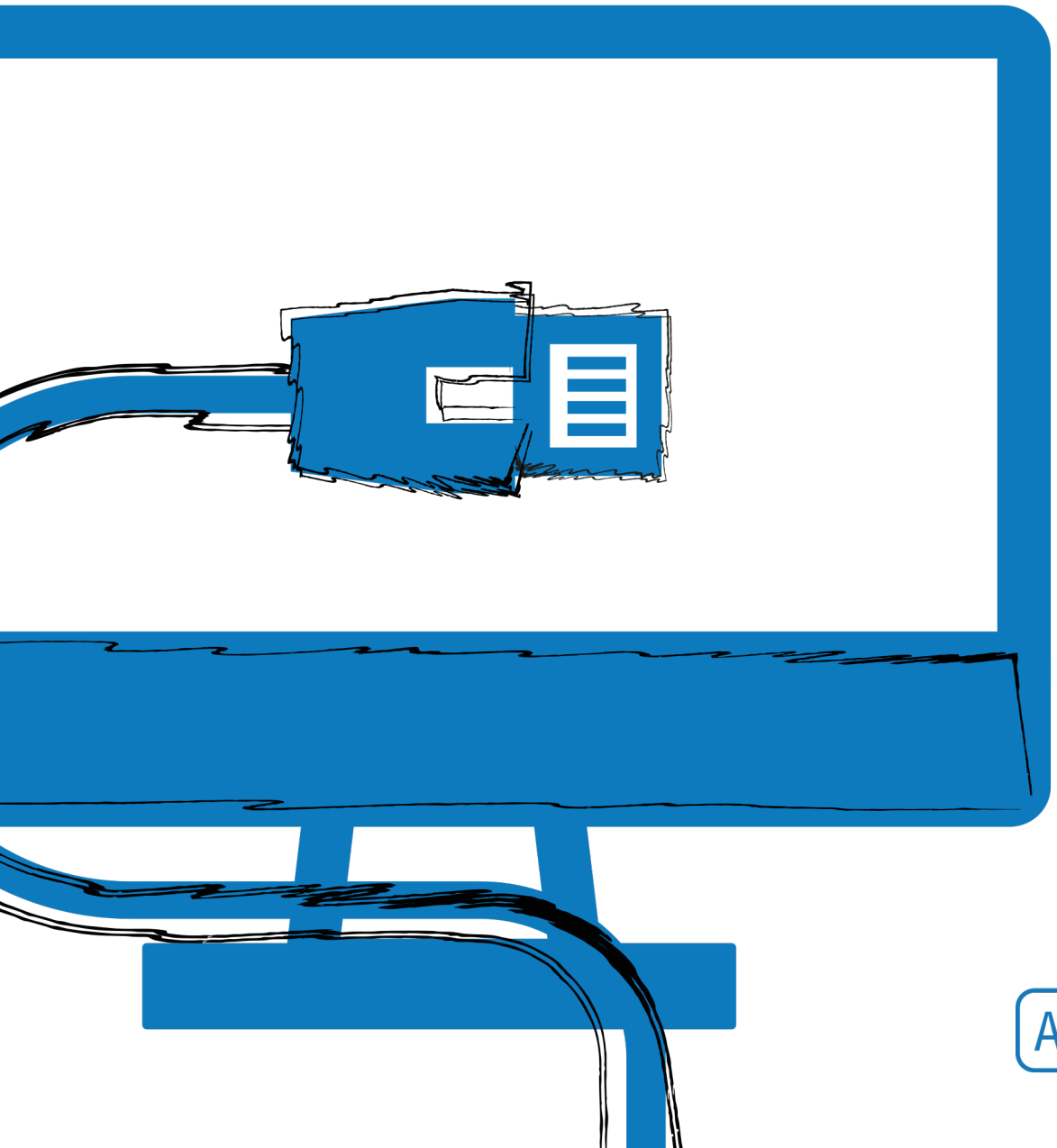
2 Создать плейбук apache.yml, в который включить следующие задания (tasks):

- Установить последнею версии Apache. Обновить кэш репозитория, если кэш не обновлялся больше часа (модуль apt).
- Копировать файлы index.html на продуктивный веб-сервер server1 и на тестовый веб-сервер server2:
    - создать два index-prod.html и index-test.html для продуктивного веб сервера server1 и тестового веб сервера server2, соответственно, следующего содержания (точки заменить на текст, в котором упоминается информация о типе веб-сервера):
    ```
    <body>
     <h1> .....</h1>
    </body>
    ```
    - Файлы разместить в подкаталоге files, предварительно создав этот каталог.
    - С помощью модуля copy настроить копирование этих файлов в каталог /var/www/html на оба сервера под именами index.html.
    Примечание: использовать переменную для хостов, задать этой переменной разные значения для разных серверов (prod для server1 и test для server2) и сформировать имена файлов-источников с использованием значений этой переменной.
- Отключить параметр AstraMode в Apache (файл /etc/apache2/apache2.conf). Вставить строку
AstraMode off
после
AstraMode on
- Перезапустить службу apache2 на обоих серверах. Сделать так, чтобы служба Apache2 автоматически запускался при загрузке обоих серверов.

- Проверить содержимое стартовых страниц веб-серверов (index.html). Для этого использовать модуль uri с параметром return_content=yes, с помощью register поместить веб-страницу в переменную и вывести ее на экран с помощью модуля debug.

Модуль 8

Служба каталогов на базе решения FreeIPA



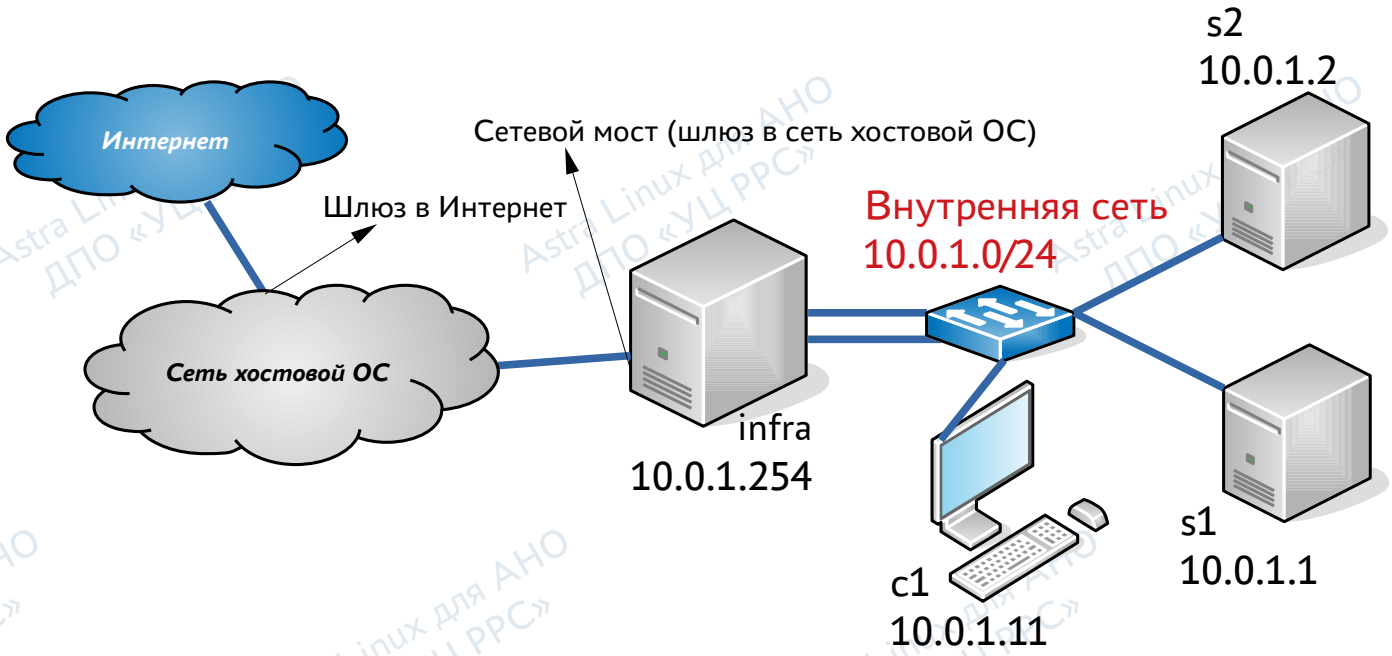
ASTRA LINUX®

Модуль 8. Служба каталогов на базе решения FreeIPA

Описание практического задания

- Установка и запуск сервера FreeIPA.
- Установка клиента FreeIPA и ввод клиента в домен.
- Управление доменными учетными записями.
- Управление доступом на базе узла.
- Регистрация сетевых служб в домене FreeIPA на примере прокси-сервера SQUID.
- Установка и запуск реплики FreeIPA.

Схема сети



Действия, которые следует выполнить перед началом выполнения заданий

1 Остановить ВМ server1, server2, client1. В дальнейших заданиях эти ВМ не используются.

2 В ВМ infra :

- отключить базовую аутентификацию в SQUID-прокси, настроенную ранее.

- сетевой интерфейс net1 настроить на автоматическое получение по DHCP адресов DNS-серверов.
  nmcli con mod net1 ipv4.ignore-auto-dns no ipv4.dns ""
  nmcli con up net1
- выключить режим проверки DNSSEC и перезапустить DNS-сервер.
  файл /etc/bind/named.conf.options
  dnssec-validation no;
  sudo systemctl restart bind9

Развертывание первого сервера FreeIPA

Задание: Создать ВМ s1 и увеличить RAM до 3Гб, а количество ядер до 3х. Настроить имя хоста (s1.astra.test) и сетевые параметры интерфейса (10.0.1.1/24, шлюз и DNS-сервер 10.0.1.254). Внести информацию об имени адресе хоста s1.astra.test в файл /etc/hosts.

Настроить доступ к репозиториям ПО с помощью прокси-сервера infra. Установить серверное ПО FreeIPA. Изменить DNS-сервер на локальный хост. Развернуть первый сервер FreeIPA. Настроить ретрансляцию DNS-запросов на DNS-сервер infra.

1 Создать ВМ s1 путем клонирования ВМ template_1704_3. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта одна, подключена к внутренней сети. Запустить ВМ.

2 Изменить имя хоста на s1.astra.test.

3 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.1/24; DNS сервер — 10.0.1.254, шлюз — 10.0.1.254).

4 Добавить в /etc/hosts запись о s1.astra.test:

```
127.0.0.1 localhost localhost.localdomain
10.0.1.1 s1.astra.test s1
```

5 Проверить доступность ВМ infra.

6 Настроить доступ к репозиториям Astra Linux, используя прокси SQUID, развернутый на хосте infra.

7 Обновить кэш с метаданными репозиториев.

8 Установить серверное программное обеспечение FreeIPA.

9 Установить клиентское программное обеспечение FreeIPA.

10 Изменить DNS сервер на 127.0.0.1

11 Развернуть сервер FreeIPA (все по умолчанию и задать пароль для доменной учетной записи admin).

12 Проверить статус служб FreeIPA командой ipactl.

13 Проверить доступность административной веб-консоли FreeIPA через браузер Firefox (пользователь: admin, пароль был введен во время запуска сервера FreeIPA)
https://s1.astra.test

14 Настроить ретрансляцию DNS запросов с сервера FreeIPA s1.astra.test на кэширующий DNS сервер infra:

- Перейти в веб-консоль https://s1.astra.test.
- Выбрать Сетевые службы → DNS → Глобальная конфигурация DNS → Глобальные перенаправители → Ввести 10.0.1.254 → Сохранить.

Установка клиента и ввод клиента в домен

Задание: Создать ВМ c1. Настроить имя хоста (c1.astra.test) и сетевые параметры интерфейса (10.0.1.11/24, шлюз 10.0.1.254 и DNS-сервер 10.0.1.1). Внести информацию об имени адресе хоста c1.astra.test в файл /etc/hosts. Настроить доступ к репозиториям ПО с помощью прокси-сервера infra. Установить клиентское ПО FreeIPA. Ввести хост c1.astra.test в домен.

1 Создать ВМ c1 путем клонирования template_1704_3 и запустить ее.

2 Задать имя хоста c1.astra.test.

3 Настроить сетевой интерфейс (IP адрес 10.0.1.11/24; dns сервер — s1.astra.test, шлюз — 10.0.1.254).

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Настроить доступ к репозиториям Astra Linux, используя прокси SQUID, развернутый на хосте infra.

6 Обновить кэш с метаданными репозиториев.

7 Установить пакет dnsutils.

8 Проверить разрешение имени сервера в DNS.

9 Внести изменения в файл /etc/hosts:

```
127.0.0.1       localhost
10.0.1.11       c1.astra.test c1
```

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить хост c1.astra.test.

13 На сервере FreeIPA s1.astra.test проверить, что хост c1.astra.test добавлен в домен.

Управление учетными записями

Задание: Создать учетную запись ipauser1 (минимальный уровень конфиденциальности – 0, максимальный – 1) из веб-консоли и ipauser2 (минимальный уровень конфиденциальности – 0, максимальный – 2) с помощью консольных утилит.

1 Создать учетную запись доменного пользователя ipauser1 из веб-консоли https://s1.astra.test (мин. уровень конфиденциальности — 0, макс. — 1):
   - Идентификация ➞ Пользователи ➞ Добавить (заполнить обязательный поля и задать пароль).
   - Щелкнуть по имени добавленной учетной записи.
   - В Параметрах идентификации задать минимальный (0) и максимальные уровни конфиденциальности (1).

2 Создать учетную запись пользователя ipauser2 и задать пароль из командной строки с помощью утилиты ipa (мин. уровень конфиденциальности — 0, макс. — 2).

3 На клиенте c1.astra.test зайдите под учетными записями ipauser1 и ipauser2 с разными уровнями конфиденциальности.

Управление доступом на основе узла

Задание: Создать правило, которое разрешает доступ пользователю admin ко всем службам на всех хостах. Создать правило, которое разрешает пользователю ipauser2 осуществлять графический вход вход в систему на хосте c1.astra.test. Отключить правило, разрешающее доступ любым пользователям к любым службам на любых хостах. Задание можно выполнять как с помощью консольных утилит, так и через веб-консоль.

1 Создать правило admin_rule, разрешающее пользователю admin доступ ко всем службам на всех хостах.

2 Просмотреть информацию о всех настроенных службах из командной строки и проверить, есть ли в списке служба fly-dm.

3 Создать правило, которое разрешает доменному пользователю ipauser2 графический вход в систему на хосте c1.astra.test:
   - На сервере FreeIPA добавить службу fly-dm.
   - Создать «пустое» правило ipauser2_flydm с именем ipuser2_flydm.
   - Добавить в правило flydm учетную запись пользователя ipauser2.
   - Добавить в правило flydm хост c1.astra.test.
   - Добавить в правило flydm службу fly-dm.

4 Просмотреть правило flydm.

5 Отключить правило allow_all.

6 Зайти под учетными записями ipauser1 и ipauser2 на хостах s1.astra.test и c1.astra.test через графический вход.

7 Сделать попытку зайти пользователем ipauser2 в c1.astra.test через виртуальный терминал.

Настройка правил SUDO

Задание: Создать SUDO-правила, которое разрешает пользователю ipauser2 просматривать журнальный файл /var/log/auth.log с помощью команды cat на хосте c1.astra.test. Задание можно выполнить как из веб-консоли, так и с помощью консольных уттилит.

1 Проверить, что пользователь ipauser2 не может просмотреть файл /var/log/auth.log на хосте c1.astra.test.

2 Добавить команду для просмотра файла /var/log/auth.log в список SUDO-команд.

3 Создать «пустое» правило ipauser2_sudo

4 Добавить в SUDO-правило пользователя ipauser2.

5 Добавить в SUDO-правило хост c1.astra.test

ipa sudorule-add-host ipauser2_sudo --hosts=c1.astra.test

6 Добавить в SUDO-правило команду

7 Добавить в SUDO-правило имя учетной записи пользователя (root), от имени которого будет выполняться команда.

8 Добавить в SUDO-правило параметр, который позволяет выполнять команду без ввода пароля.

9 Проверить, что созданное правило позволяет пользователю ipauser2 на хосте c1.astra.test просматривать файл /var/log/auth.log

Регистрация сетевых служб во FreeIPA (SQUID) (опциональное)

Задание: Ввести хост infra в домен astra.test. Настроить Kerberos-аутентификацию на прокси-сервере infra.astra.test, которая позволяет получать доступ к прокси-серверу только доменным пользователям.

1 На ВМ infra выполнить следующее:

- Изменить имя хоста.

- Внести изменения в /etc/hosts:

```
127.0.0.1    localhost
10.0.1.254   infra.astra.test infra
```

- На сетевом интерфейсе net1 запретить автоматическое получение адреса DNS-сервера по DHCP и добавить DNS-сервер 10.0.1.1 (s1.astra.test).
- На кэширующем DNS сервере (ВМ infra) настроить ретрансляцию запросов на внешний DNS 8.8.8.8. Внести соответствующие изменения в файле /etc/bind/named.conf.options:
- Убедиться, что разрешаются как внешние DNS имена, так и имена в домене astra.test.
- Установить клиент FreeIPA.
- Запустить клиент FreeIPA (ввести хост infra в домен astra.test).

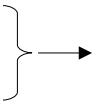
2 Проверить, что хост infra введен в домен astra.test.

3 Зарегистрировать службу squid в домене.

4 На прокси-сервере infra.astra.test выполнить следующие действия:

- Создать файл /etc/squid/squid.keytab с ключом для службы squid.
- Назначить на файл /etc/squid/krb5.keytab владельца proxy и группу-владельца proxy, задать права доступа 640.
- В файле /etc/squid/squid.conf настроить аутентификацию SQUID через Kerberos:
    - Закомментировать строку, содержащую разрешающее правило для localnet.
    - Закомментировать или удалить строки с настройками других видов аутентификации (например, аутентификации NCSA, которая настраивалась в предыдущей практической работе Модуль 5 «Прокси-сервер SQUID»).
    - Перед последним правилом http_access deny all добавить строки, которые разрешают использовать SQUID доменным пользователям (настроить аутентификацию SQUID через Kerberos).

```
auth_param negotiate program
/usr/lib/squid/negotiate_kerberos_auth -s
HTTP/infra.astra.test -k
/etc/squid/squid.keytab
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl kerb_users proxy_auth REQUIRED
http_access allow kerb_users
```



- Перезапустить systemd и службу squid (может занять продолжительное время) и убедиться, что служба squid была запущена успешно.

5 На хосте c1.astra.test выполнить следующие действия:

- Зайти под локальной учетной записью администратора (sa).
- Проверить, что внешние DNS имена и имена из домена astra.test разрешаются.
- В браузере Firefox настроить прокси для доступа в Интернет (ручная настройка прокси): infra.astra.test, порт 3128, установить параметр «Также использовать этот прокси для HTTPS», в поле «Не использовать прокси для» указать 10.0.1.0/24.
- В адресной строке браузер Firefox ввести www.astralinux.ru и сделать попытку зайти на сайт.
- Зайти под доменной учетной записью ipauser2 с нулевым уровнем конфиденциальности.
- Настроить в браузере Firefox прокси таким же образом, как и для локального пользователя sa, и зайти на сайт www.astralinux.ru.

6 После выполнения задания отключить на прокси-сервере Kerberos-аутентификацию и разрешить всем хостам их сети 10.0.1.0/24 получать доступ к прокси-серверу.

Установка реплики FreeIPA

Задание: Создать ВМ s2 и увеличить RAM до 3Гб, а количество ядер до 3х. Настроить имя хоста (s2.astra.test) и сетевые параметры интерфейса (10.0.1.2/24, шлюз 10.0.1.254 и DNS-сервер 10.0.1.1). Внести информацию об имени адресе хоста s2.astra.test в файл /etc/hosts. Настроить доступ к репозиториям ПО с помощью прокси-сервера infra. Установить серверное ПО FreeIPA. Изменить DNS-сервер на локальный хост. Развернуть реплику FreeIPA.

1 Создать новую ВМ s2 с помощью клонирования template_1704_3. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта - одна, подключена к внутренней сети. Запустить ВМ.

2 Изменить имя хоста на s2.astra.test.

3 Настроить сетевой интерфейс через Network Manager (IP - 10.0.1.2/24; DNS сервер - 10.0.1.1 (s1.astra.test), шлюз - 10.0.1.254).

4 Добавить в /etc/hosts запись о s2.astra.test.

5 Проверить доступность ВМ s1.astra.test.

6 Настроить доступ к репозиториям Astra Linux, используя прокси-сервер, развернутый на хосте infra.

7 Обновить кэш с метаданными репозиториев.

8 Установить пакет dnsutils.

9 Проверить разрешение имени сервера s1.astra.test в DNS.

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить хост s2.astra.test.

13 На сервере FreeIPA s1.astra.test проверить, что хост s2.astra.test добавлен в домен.

14 На сервере FreeIPA s1.astra.test с помощью утилиты astra-freeipa-server-crt создать сертификат для s2.astra.test и передать его на s2.astra.test.

15 На сервере FreeIPA s1.astra.test создать PTR запись для s2.astra.test, или из веб-консоли, или с помощью команды ipa dnsrecord-add.

16 На хосте s2.astra.test установить серверное программное обеспечение FreeIPA.

17 На хосте s2.astra.test запустить реплику FreeIPA, указав имя файла с сертификатом.

18 На s2.astra.test изменить DNS сервер на 127.0.0.1:

19 На s2.astra.test проверить, что реплика работает путем выполнения команды ipactl status
и входа в администраторскую веб-консоль hhtps://s2.astra.test
(IPA-сервер→Топология→IPA-сервер,
IPA-сервер→Топология→Topology Graph).

Настройка синхронизации времени в домене (опционально).

Задание: Используя BM infra как управляющий хост, написать и выполнить playbook, который передает на все хосты домена конфигурационный файл для службы chrony. В качестве источника времени использовать хост infra.astra.test.

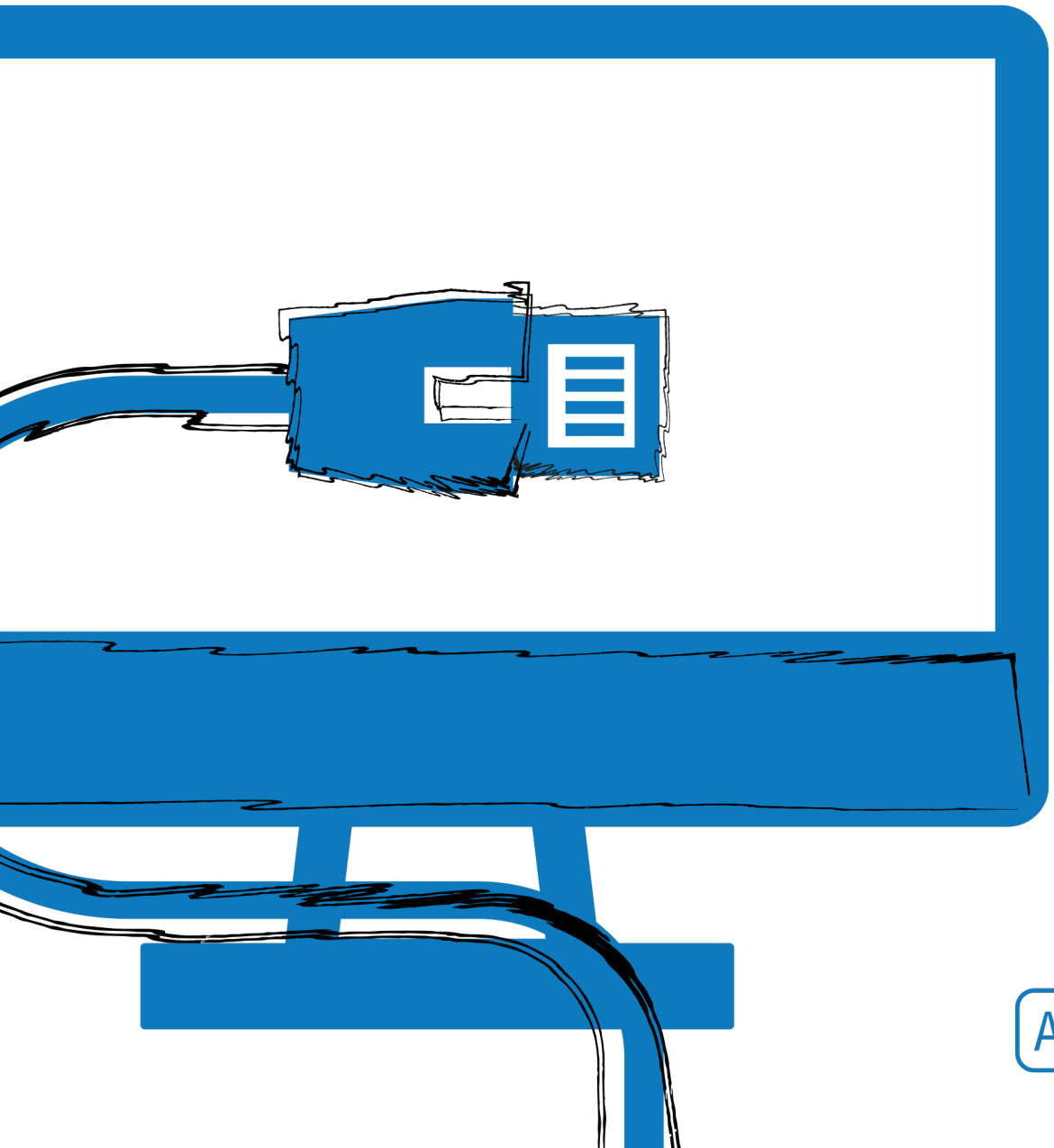
1 На BM infra зайти под учетной записью локального или доменного администратора.

2 Настроить аутентификацию по ключам для SSH-серверов s1.astra.test, s2.astra.test, c1.astra.test.

3 Создать конфигурационный файл для службы chrony, в котором в качестве источника времени указать сервер infra.astra.test (10.0.1.254).

4 Создать и выполнить плейбук, который скопирует созданный конфигурационный файл на хосты s1, s2, c1 и перезапустит на них службу chrony.

Модуль 9
Веб-сервер на основе Apache



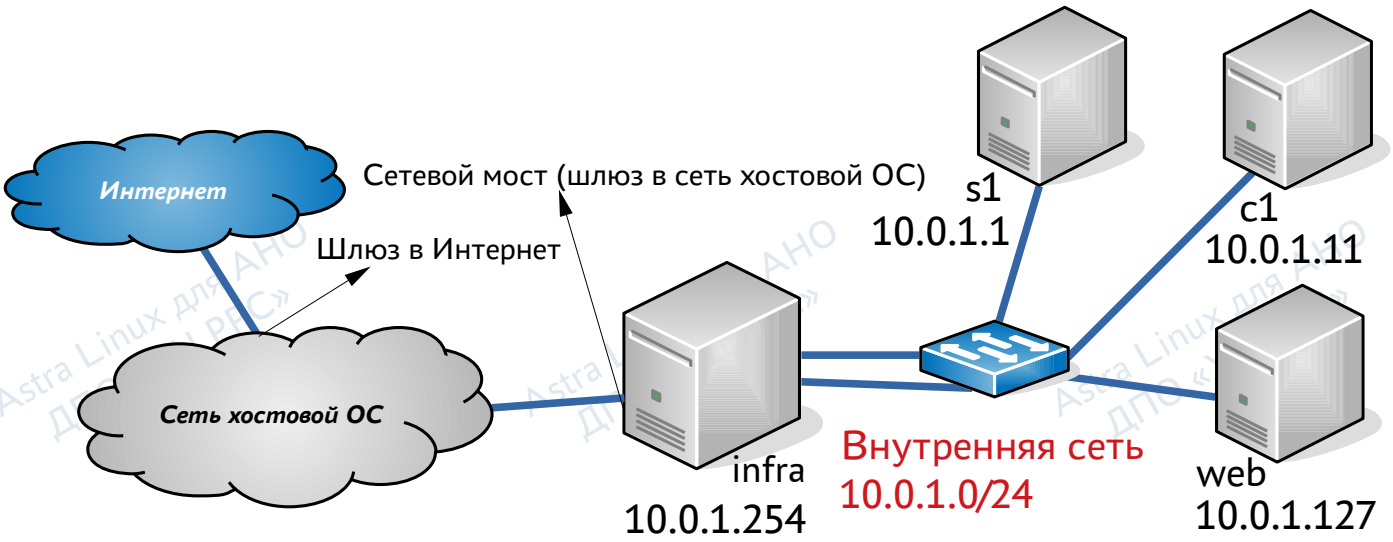
ASTRA LINUX®

Модуль 9. Веб-сервер на основе Apache

Описание практического задания

- Установка веб-сервера «доступного из Интернет» на виртуальной машине (ВМ) infra.
- Установка веб-сервера для локального доступа на ВМ server1.
- Настройка авторизации с применением FreeIPA.
- Работа со страницами с мандатными метками.

Схема сети



Действия, которые следует выполнить перед началом выполнения заданий

Если в практической работе по модулю 8 не было выполнено опциональное задание, в котором хост infra вводился как клиент в домен, то следует на хосте infra:

1 Указать в сетевом соединении net1 в качестве DNS-servera s1.astra.test (10.0.1.1) и сделать A-запись для infra.astra.test.

2 На кэширующем DNS сервере (ВМ infra) настроить ретрансляцию запросов на внешний DNS 8.8.8.8. Внести соответствующие изменения в файле /etc/bind/named.conf.options.

Настройка Apache2 на ВМ infra

Задание: Установить Apache2. Создать и активировать конфигурационный файл для отключения режима AstraMode. Настроить виртуальный веб-сервер infra.astra.test. Файлы виртуального веб-сервера infra,astra.test разместить в каталоге /var/www/infra. Отключить виртуальный веб-сервер, активированнный по умолчанию во время установки Apache2. Установить модуль Apache для поддержки PHP.

1 Установить apache2 на ВМ infra.

2 Создать конфигурационный файл astramode_off.conf в каталоге /etc/apache2/conf-available, в котором настроить отключение режима AstraMode.

3 Отключить режим AstraMode, активировав настройку из файла astramode_off.conf.

4 В конфигурационный файл виртуального веб-сервера по умолчанию /etc/apache2/sites-available/000-default.conf добавить параметр:
```
ServerName 10.0.1.254
```

5 Создать конфигурационный файл виртуального веб-сервера infra.astra.test в /etc/apache2/sites-available путем копирования файла 000-default.conf в файл infra.conf.

6 Отредактировать конфигурационный файл и виртуального веб-сервера infra.astra.test, указав доменное имя сервера infra.astra.test в параметре ServerName и путь к каталогу с веб-страницами /var/www/infra.

7 Создать каталог для размещения веб-страниц сайта infra.astra.test.

8 Разместить в созданном каталоге веб-страницу index.html со следующим содержимым:
```
<html>
  <head>
    <title>Welcome to infra</title>
  </head>
  <body>
    <h1>Welcome to infra</h1>
    <p>Hello!</p>
  </body>
</html>
```

9 Активировать сайт, описанный в конфигурации виртуального хоста infra.astra.test.

10 В браузере получить доступ к настроенным сайтам, набрав в адресной строке браузера http://infra.astra.test и http://10.0.1.254 .

11 Деактивировать виртуальный веб-сервер по умолчанию и снова в адресной строке браузера набрать http://infra.astra.test и http://10.0.1.254

12 Установить php и модуль php для Apache2.

13 Проверить версию php:

```
php -v
```

14 Создать в каталоге виртуального хоста infra.astra.test файл info.php с содержимым:

```
<?php
phpinfo();
?>
```

15 Проверить в браузере отображение страницы, сгенерированной info.php.

Настройка самоподписанных сертификатов (опциональное задание)

Задание: Создать самподписанный сертификат для веб-сайта infra.astra.test. Настроить веб-сайт infra.astra.test для работы с использованием протокола TLS (SSL).

1 Создать удостоверяющий центр – CA (Certification Authority):

```
sudo -i
cd /etc/apache2/
mkdir ssl
chmod 700 ssl
cd ssl
openssl genrsa -des3 -out my-ca.key
```

2 Создать сертификат для удостоверяющего центра:

```
openssl req -new -x509 -days 3650 -sha256 \
 -key my-ca.key -out my-ca.crt
```

3 В конфигурационном файле /etc/ssl/openssl.cnf найти и раскомментировать строку:

```
req_extensions = v3_req
```

4 В секции [v3_req] после строк:

```
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
```

следует добавить строку:

```
subjectAltName = @alt_names
```

после которой создать новую секцию [alt_names].

5 В новую секцию `[ alt_names ]` добавить строки вида `DNS.X = домен`, указав домены, для которых выпускается сертификат, где X=1,2,3 и т. д. Можно указать несколько доменов/поддоменов.

6 Создать файл ключа для веб-сервера (размер ключа - 2048 бита):

```
openssl genrsa -des3 -out my-apache.key 2048
```

7 Удалить пароль из файла ключа веб-сервера:

```
openssl rsa -in my-apache.key -out new.my-apache.key
mv new.my-apache.key my-apache.key
```

8 Создать запрос на подпись сертификата Certificate Signature Request (csr) в удостоверяющем центре:

```
openssl req -new -key my-apache.key -out my-apache.csr
```

9 Подписать сертификат Apache в удостоверяющем центре:

```
openssl x509 -req -in my-apache.csr \
-out my-apache.crt -sha256 -CA my-ca.crt \
-CAkey my-ca.key -CAcreateserial -days 366
```

10 Назначить права только на чтение только для владельца на файлы ключей.

11 Назначить каталогу /etc/apache2/ssl и файла внутри этого каталога владельца www-data и группу-владельца www-data.

12 Отредактировать файл /etc/apache2/sites-available/default-ssl.conf:

```
SSLCertificateFile /etc/apache2/ssl/my-apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/my-apache.key
SSLCACertificateFile /etc/apache2/ssl/my-ca.crt
```

13 Активировать модуль mod_ssl.

14 Активировать сайт, настройки которого хранятся в конфигурационном файле default-ssl.conf.

15 Перезапустить службу apache2.

16 Проверить работоспособность сайта – ввести в адресную строку браузера https://infra.astra.test.

Настройка BM web

Задание: Создать ВМ web. Настроить ВМ web: имя хоста – web.astra.test, IP адрес – 10.0.1.127/24, шлюз – 10.0.1.254, DNS-сервер – 10.0.1.1. Внести информацию об имени и адресе хоста в /etc/hosts. Ввести хост web.astra.test в домен.

1 Клонировать ВМ template_1704_3 и назвать новую виртуалку web.

2 Запустить виртуалку.

3 Сменить имя хоста на web.

4 Поправить /etc/hosts, добавив соответствие доменного имени машины и ее IP-адреса.

5 Остановить и запретить запуск Network Manager.

6 Настроить сетевой интерфейс eth0 с IP-адресом 10.0.1.127 в файле /etc/network/interfaces.

7 Указать IP-адрес DNS-сервера 10.0.1.1 в файле /etc/resolv.conf.

8 Перезапустить службу и проверить настройки и доступность шлюза.

9 Настроить работу apt через прокси-сервер infra.astra.test.

10 Обновить локальный кэш с метаданными репозиториев.

11 Установить клиент FreeIPA.

12 Ввести ВМ web в домен.

13 Перезагрузить ВМ web.

14 Проверить, что хост web.astra.test введен в домен.

Настройка Kerberos авторизации веб-сервера Apache в домене FreeIPA

Задание: Установить Apache и модуль Kerberos-аутентификации для Apache на хосте web.astra.test. Зарегистрировать веб-службу, работающую на хосте web.astra.test, в домене. Разместить файл с ключом для веб-службы на хосте web.astra.test. Настроить Kerberos-аутентификацию для сайта по умолчанию ().

1 Зайти на ВМ web под учетной записью доменного администратора.

2 На ВМ web установить apache2 и модуль аутентификации через Kerberos.

3 Зарегистрировать веб-службу web.

4 В ВМ web записать ключи для web-службы в файл /etc/apache2/keytab.

5 Установить права и владельца на файл keytab.

6 Настроить Kerberos-аутентификацию на веб-сервере, включив секцию <Directory> в конфигурационный файл виртуального веб-сервера /etc/apache2/sites-enabled/000-default.conf.

7 Перезапустить веб-сервер.

Создание веб-страниц с разными уровнями конфиденциальности в BM web

Задание: На хосте web.astra.test назначить метку безопасности на каталоги /var/www и /var/www/html: уровень конфиденциальности – 2, все категории, уровень мандатной целостности – 63, дополнительный атрибут – 63. В каталоге /var/www/html создать две веб-страницы с разными уровнями конфиденциальности level1.html – уровень конфиденциальности 1 и level2.html - уровень конфиденциальности – 2.

1 В BM web установить уровень конфиденциальности 2 и атрибут ccnr на каталоги /var/www, /var/www/html

2 Перейти в каталог /var/www/html.

3 Создать файлы для проверки доступа на уровнях конфиденциальности 1 и 2 с названиями level1.html и level2.html с содержимым, явно указывающим на уровень конфиденциальности файла (например, выводящих текст Level1 и Level2).

4 Назначить созданным файлам соответствующие уровни конфиденциальности.

5 Изменить владельца и группу-владельца файлов .html на www-data.

Настройка клиента для работы с локальным веб-сервером Apache2

Задание: Зайти под учетными записями ipauser1 и ipauser2 с разными уровнями конфиденциальности, настроить браузер Firefox для поддержки Kerberos-аутентификации и вывести содержимое страниц level1.html и level2.html.

1 Зайти на c1 по очереди: локальным пользователем sa, доменными пользователями ipaser1, ipauser2 (с уровнями конфиденциальности 0,1,2).

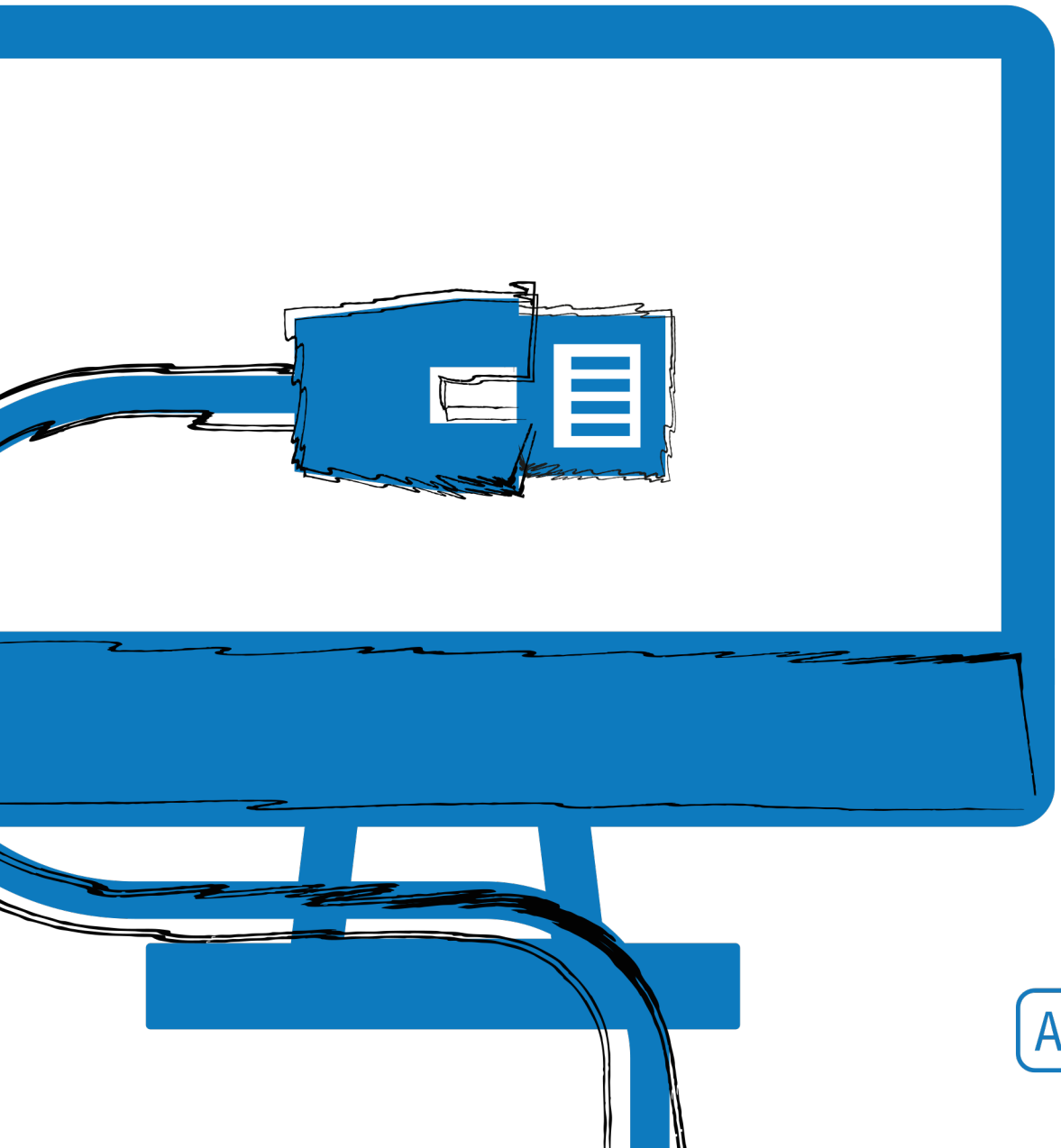
2 Настроить поддержку Kerberos-аутентификацию в Firefox:

- в адресной строке набрать about:config;
- найти параметры, содержащие negotiate;
- параметрам network.negotiate-auth.delegation-uris и network.negotiate-auth.trusted-uris задать значение http://, https://

3 Зайти в браузере на страницы http://web.astra.test, http://web.edu.test/level1.html, http://web.astra.test/level2.html. Сравнить результаты при входе разными пользователями с разными уровнями конфиденциальности.

Модуль 10

Система электронной почты на базе Exim и Dovecot



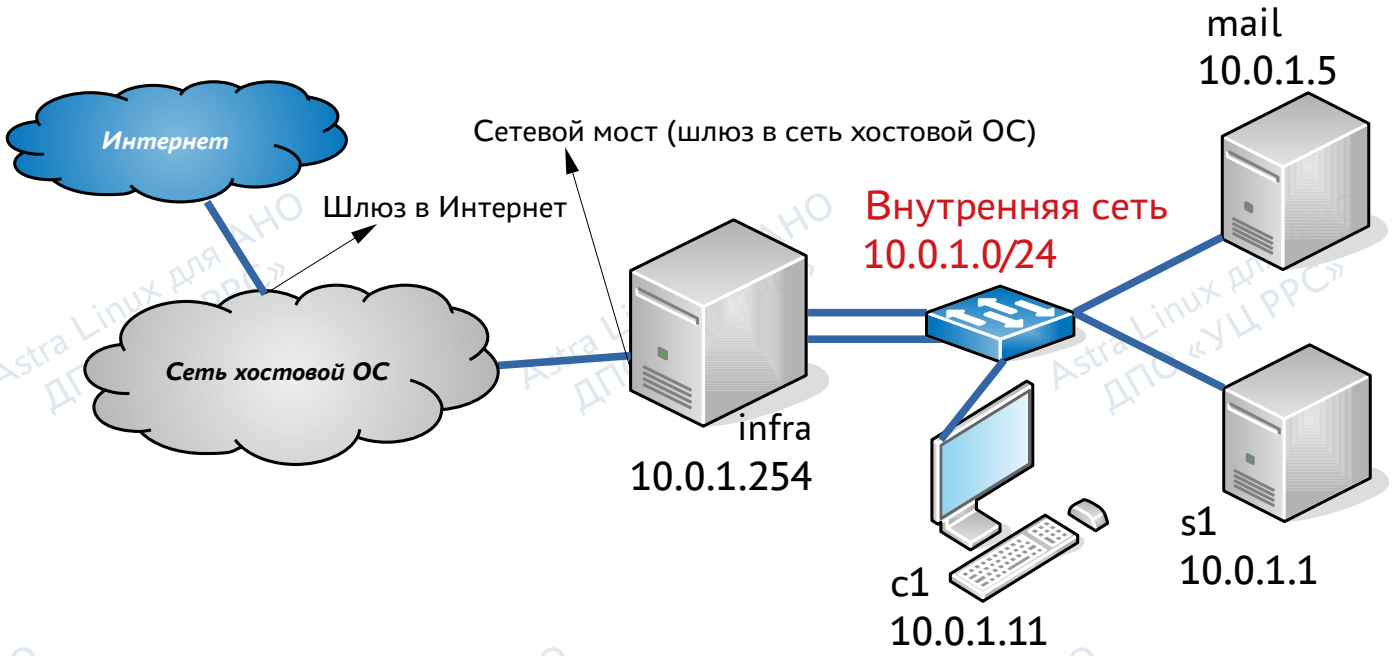
ASTRA LINUX®

Модуль 10. Система электронной почты на базе Exim и Dovecot

Описание практического задания

- Установка и первоначальная настройка защищенного программного почтового комплекса.
- Настройка аутентификации почтовых служб через Kerberos.
- Настройка почтового клиента Thunderbird.

Схема сети



Создание и настройка ВМ для почтового сервера

Задание: Создать ВМ mail. Настроить ВМ mail: имя хоста - mail.astra.test, IP адрес- 10.0.1.5/24, шлюз - 10.0.1.254, DNS-сервер - 10.0.1.1. Внести информацию об имени и адресе хоста в /etc/hosts. Ввести хост mail.astra.test в домен.

1 Создать ВМ mail путем клонирования ВМ template_1704_3. Запустить ВМ и зайти под учетной записью локального администратора (sa).

2 Изменить имя хоста на mail.astra.test.

3 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.5/24; DNS сервер — s1.astra.test (10.0.1.1), шлюз — 10.0.1.254).

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Настроить доступ к репозиториям через прокси-сервер infra.astra.test.

6 Обновить кэш с метаданными репозиториев.

7 Установить пакет dnsutils.

8 Проверить разрешение имени сервера в DNS.

9 Внести изменения в файл /etc/hosts:

```
127.0.0.1       localhost
10.0.1.5        mail.astra.test mail
```

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить mail.astra.test.

13 Проверить, что хост mail.astra.test введен в домен.

Установка программного обеспечения и первоначальная настройка

Задание: Установить exim4 и dovecot. Произвести первоначальную настройку exim4 (метод доставки локальной почты - maildir).

1 На хосте mail.astra.test установить защищенный комплекс программ электронной почты.

2 Произвести первоначальную настройку exim4.

3 Ввести следующие ответы на вопросы во время первоначальной настройки (результаты запомнятся в файле /etc/exim4/update-exim4.conf.conf):

- Тип почтовой конфигурации: Интернет сайт; ...
- Почтовое имя системы: astra.test
- IP адреса, с которых ожидаются входящие SMTP соединения: 10.0.1.5
- Места назначения, для которых должна приниматься почта: astra.test
- Домены для релейной передачи почты: пусто
- Хосты для релейной передачи почты: пусто
- Сокращать количество DNS-запросов: нет
- Метод доставки локальной почты: Maildir формат в /var/mail
- Разделить конфигурацию на маленькие файлы: Да

Настройка аутентификации СЭП через Kerberos

Задание: зарегистрировать в домене службы exim4 (smtp) и dovecot (imap). На почтовом сервере mail.astra.test создать keytab-файл с ключами для smtp и imap служб. Добавить MX-запись в зону DNS astra.test. Настроить Kerberos-аутентификацию для служб smtp и imap.

1 Зарегистрировать почтовые службы smtp (exim4) и imap (dovecot), которые будут работать на хосте mail.astra.test.

2 Используя веб-консоль freeIPA, добавить ресурсные записи DNS:

- MX запись для зоны astra.test, почтовый сервер mail.astra.test.
- PTR запись для хоста mail.astra.test.

3 На сервере mail.astra.test создать файл с ключами для почтовых служб ./var/lib/dovecot/dovecot.keytab.

4 Дать пользователю dovecot право на чтение для keytab-файла.

5 На почтовом сервере mail.astra.test настроить dovecot для обеспечения аутентификации через Kerberos:

- В файле /etc/dovecot/conf.d/10-auth.conf:
  - Раскомментировать строку:
    ```
    disable_plaintext_auth = yes
    ```
  - Раскомментировать строку и задать значение – имя почтового сервера:
    ```
    auth_gssapi_hostname = mail.astra.test
    ```
  - Раскомментировать строку и задать значение – абсолютное имя keytab-файла:
    ```
    auth_krb5_keytab = /var/lib/dovecot/dovecot.keytab
    ```
  - Изменить значение параметра на gssapi
    ```
    auth_mechanisms = gssapi
    ```
- В файле /etc/dovecot/conf.d/10-master.conf внутри секции service auth { ... } внести следующую подсекцию (exim будет использовать сокет службы dovecot для аутентификации через Kerberos – даем соответствующие права доступа):
  ```
  unix_listener auth-client {
      mode = 0600
      user = Debian-exim
  }
  ```

6 Перезапустить службу dovecot и проверить статус службы.

7 Настроить exim4 для аутентификации через Kerberos. На почтовом сервере mail.astra.test создать файл /etc/exim4/conf.d/auth/22_exim4-dovecot-kerberos-ipa со следующим содержимым:

```
dovecot_gssapi:
driver = dovecot
public_name = GSSAPI
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

8 Перезапустить службу exim4 и проверить статус.

Настройка почтового клиента «Почта Thunderbird»

Задание: зайти под учетными записями пользователей ipauser1 и ipauser2 с разными уровнями конфиденциальности, настроить Thunderbird и отправить друг другу почтовые сообщения.

1 Зайти на хосте c1.astra.test под доменной учетной записью ipauser2 с разными уровнями конфиденциальности: 0, 1 и 2.

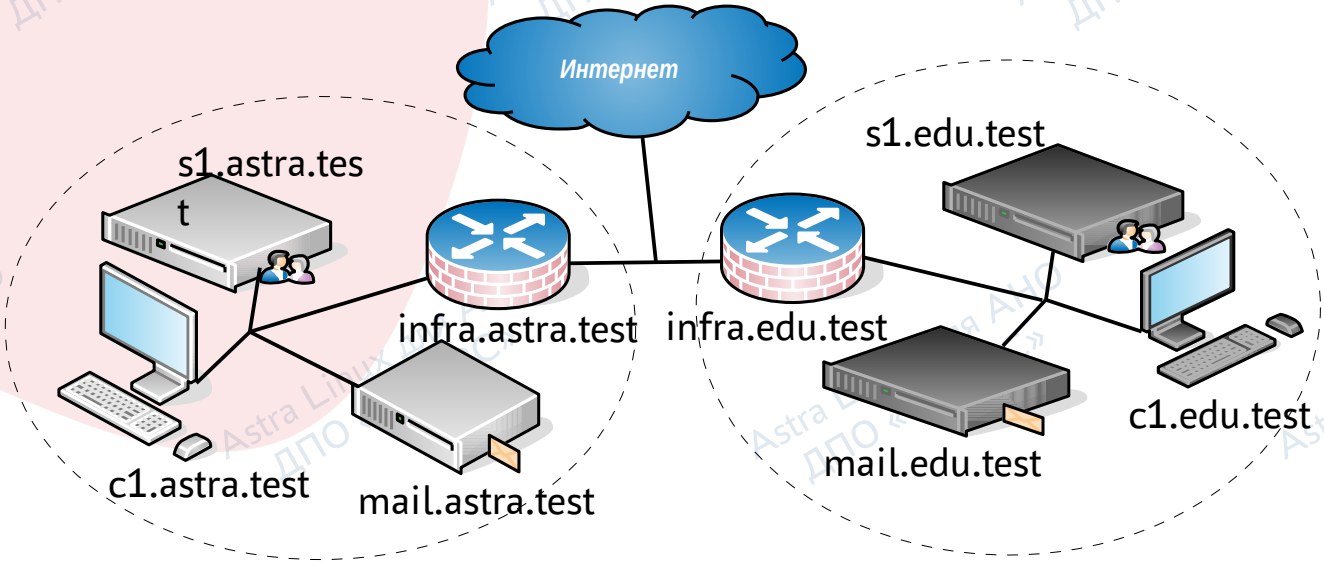
2 Настроить почтовый клиент «Почта Thunderbird» для учетной записи ipauser2 на каждом уровне конфиденциальности и отправить письма пользователю ipauser1.

3 Зайти на хосте c1.astra.test под доменной учетной записью ipauser1 с разными уровнями конфиденциальности: 0 и 1.

4 Настроить почтовый клиент «Почта Thunderbird» для учетной записи ipauser1 на каждом уровне конфиденциальности и прочитать полученные письма.

Настройка взаимодействия двух СЭП (опциональное задание)

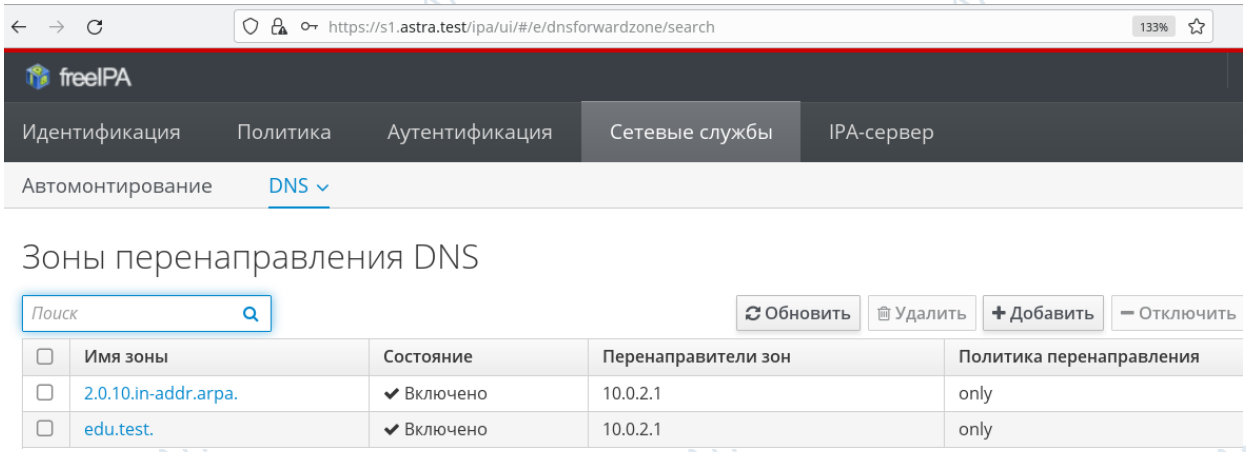
Схема стенда



1 Данное задание предполагает, что:

- Имеется два набора по 4 виртуальных машины в каждой.
- В домене edu.test ВМ настроены аналогично, как и в astra.test.
- Между сетями 10.0.1.0/24 и 10.0.2.0/24 настроена маршрутизация. Статические маршруты определены на infra.astra.test и infra.edu.test.

2 На DNS сервере s1. astra.test (10.0.1.1) настроить перенаправление (forwarding) зон edu.test. и 2.0.10.in-addr.arpa. на DNS сервер s1.edu.test (10.0.2.1). Аналогичные действия сделать на DNS сервере s1.edu.test (10.0.2.1) для зон astra.test. и 1.0.10.in-addr.arpa. (воспользуйтесь веб-консолью freeIPA).



3 Проверить на mail.astra.test и mail.edu.test разрешаются ли ресурсные записи DNS типа MX для доменов astra.test и edu.test. Используйте команду `nslookup` или `dig`.

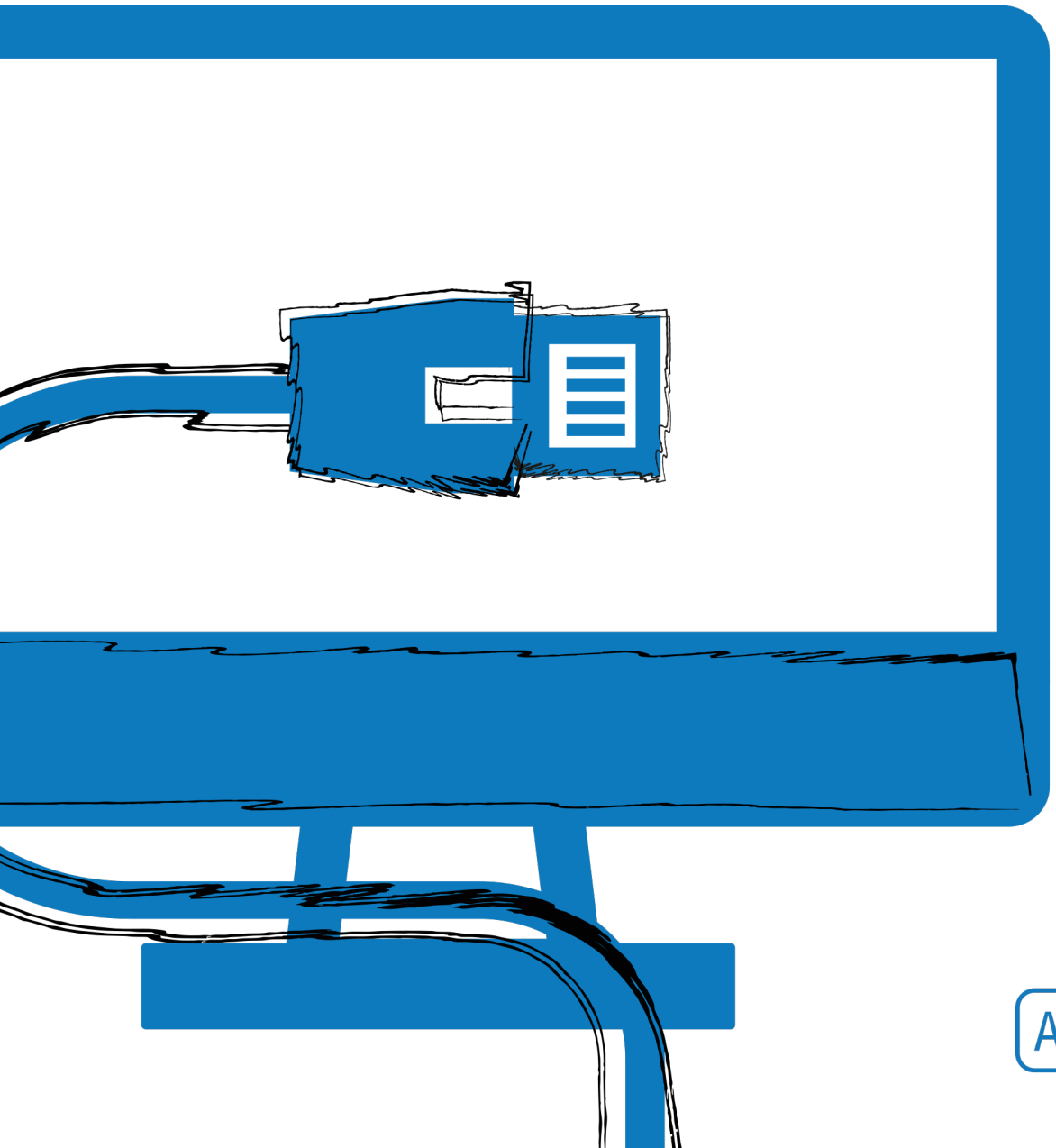
4 На mail.astra.test разрешить отправку почты (relay) в домен edu.test. Это можно сделать, установив параметр dc_relay_domains='edu.test' в файле /etc/exim4/update-exim4.conf.conf или с помощью dpkg-reconfigure exim4-config

5 Аналогичные действия произведите на mail.edu.test.

6 На c1.astra.test и c1.edu.test проверьте, что можно отправлять почтовые сообщения пользователям доменов astra.test и edu.test с различными уровнями конфиденциальности.

Модуль 11

Защищенный комплекс программ для печати и маркировки документов



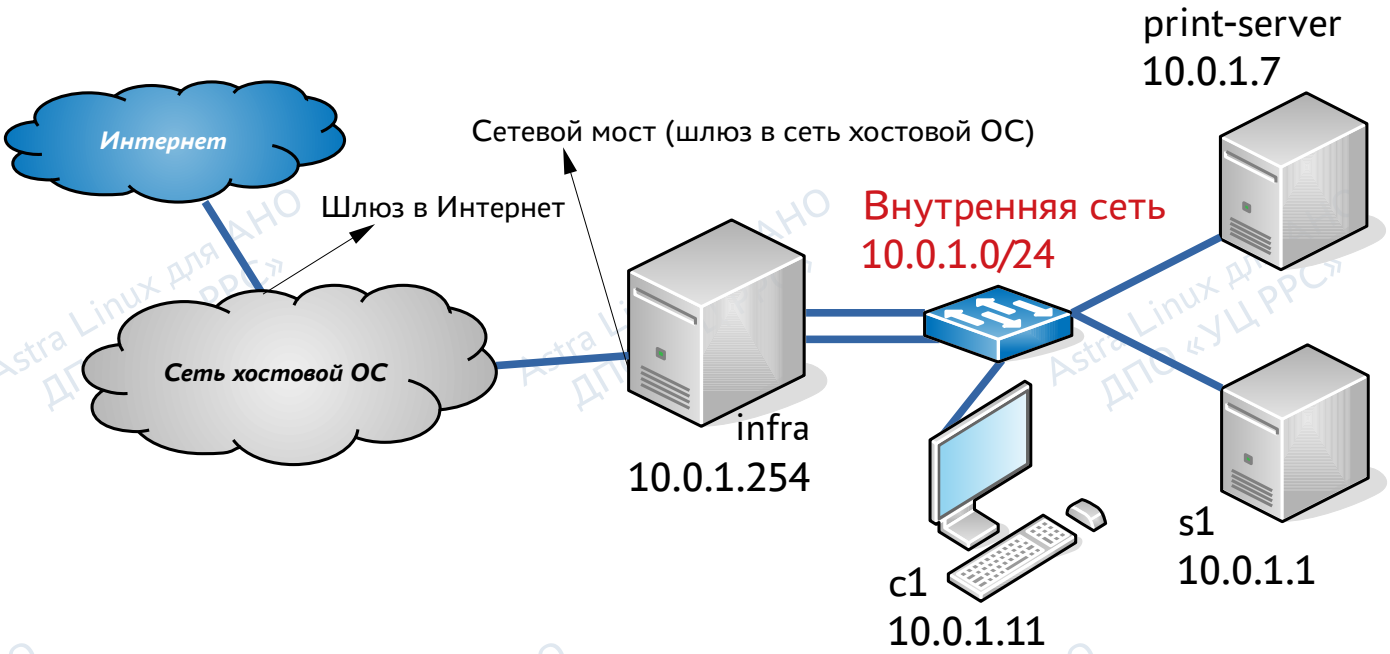
ASTRA LINUX®

Модуль 11. Защищенный комплекс программ для печати и маркировки документов

Описание практического задания

- Настройка сервера печати.
- Настройка клиента печати.
- Интеграция службы печати и FreeIPA.
- Маркировка документов.

Схема сети



Создание и настройка ВМ print-server

Задание: Создать ВМ print-server. Настроить ВМ print-server: имя хоста – print-server.astra.test, IP адрес – 10.0.1.7/24, шлюз - 10.0.1.254, DNS-сервер – 10.0.1.1. Внести информацию об имени и адресе хоста в /etc/hosts. Настроить доступ к репозиториям через прокси infra.astra.test. Установить драйвер принтера, выводящего документы в pdf-файл.

1 Создать ВМ print-server путем клонирования ВМ template_1704_3. Запустить ВМ и зайти под учетной записью локального администратора (sa).

2 Изменить имя хоста на print-server.astra.test:

3 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.7/24; DNS сервер — s1.astra.test (10.0.1.1), шлюз — 10.0.1.254):

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Внести изменения в файл /etc/hosts:

```
127.0.0.1       localhost
10.0.1.7        print-server.astra.test print-server
```

6 Настроить доступ к репозиториям через прокси-сервер infra.astra.test.

7 Обновить кэш с метаданными репозиториев.

8 Установить пакет dnsutils.

9 Проверить разрешение имени сервера FreeIPA в DNS.

10 Установить драйвер принтера для печати в PDF-файл.

Настройка сервера печати и аутентификации службы печати

Задание: Ввести хост printer-server в домен astra.test. Создать учетную записью администратора службы печати cups_admin и включить ее в локальные группы lpadmin и lpmac. Зарегистрировать службу печати в домене. На сервере печати добавить ключи для службы cups (протокол IPP) в keytab-файл /etc/krb5.keytab. Разрешить службе cups принимать задания от удаленных хостов. Настроить Kerberos-аутентификацию для службы печати и включить поддержку мандатного управления доступом. Настроить принтер так, чтобы pdf-файлы создавались в каталоге /opt/cups-pdf. Разрешить общий доступ к принтеру. Установить принтер для печати в pdf-файл по умолчанию для всех, настроить минимальные и максимальные классификационные метки.

1 Установить на ВМ print-server клиента FreeIPA и ввести данных хост в домен FreeIPA.

2 Перезагрузить ВМ print-server.

3 На сервере FreeIPA (s1.astra.test) создать доменную учетную запись cups_admin (с помощью утилиты ipa или веб-консоли).

4 На сервере FreeIPA зарегистрировать службу печати cups, которая использует протокол IPP.

5 Зайти в ВМ print-server под учетной записью локального администратора (sa) добавить ключ для службы CUPS в keytab-файл /etc/krb5.keytab.

6 Включить доменного пользователя cups_admin в локальные группы lpadmin и lpmac и проверить успешность выполнения этих действий.

7 Разрешить службе CUPS принимать задания и команды с удаленных хостов, а также установить значение * для параметра ServerAlias и задать имя сервера печати в параметре ServerName.

8 Настроить аутентификацию службы CUPS через Kerberos и включить поддержку мандатного управления доступом. Внесите следующие изменения в настройки CUPS:

```
sudo cupsctl DefaultPolicy=parsec
sudo cupsctl MacEnable=On
sudo cupsctl DefaultAuthtype=Negotiate
```

9 В файле /etc/cups/cupsd.conf заменить строку

```
Port 631
```

на

```
Listen 0.0.0.0:631
```

10 Командой cupsctl параметр MarkerUser установить в значение ipp.

11 Создайте каталог /opt/cups-pdf.

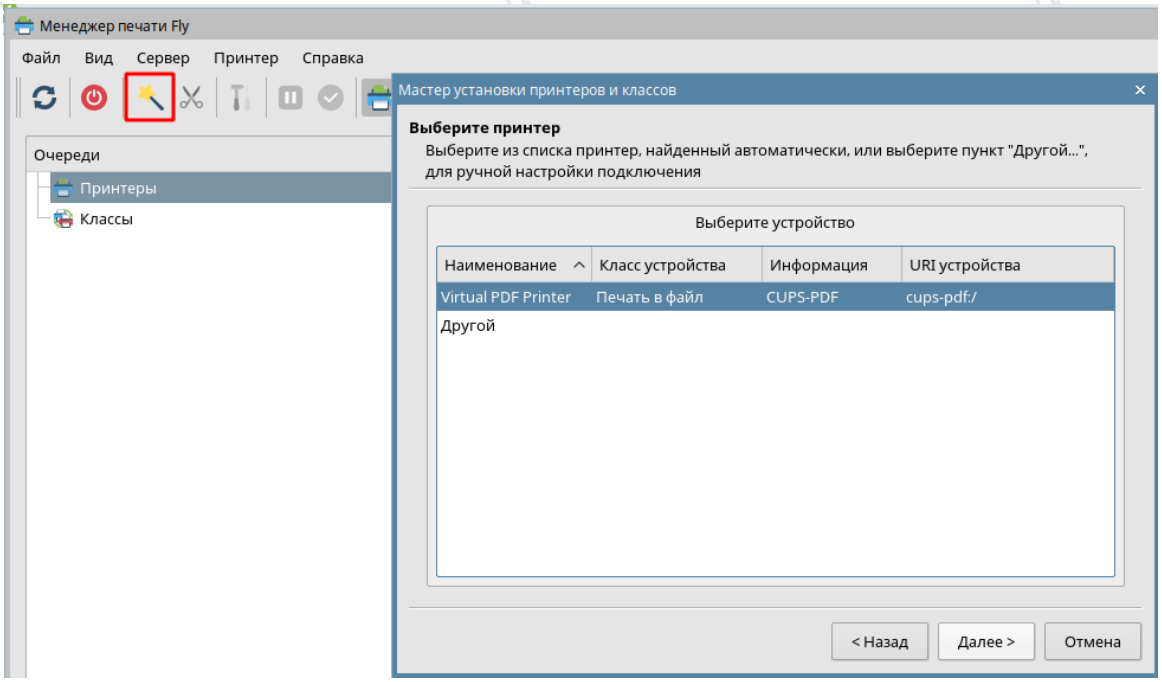
12 В файле /etc/cups/cups-pdf.conf изменить значения параметра Out (каталог, куда будут помещаться pdf файлы) на /opt/cups-pdf/${USER}.

13 Перезапустить службу CUPS.

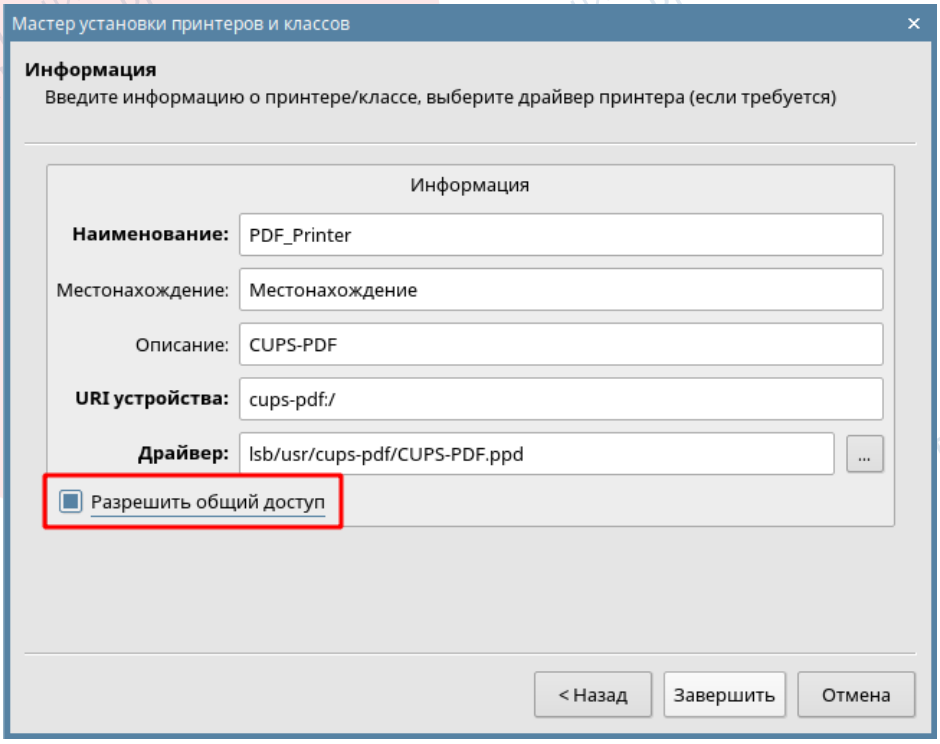
14 Зайти в ВМ print-server под доменной учетной записью cups_admin.

15 Вызвать «Менеджер печати Fly» командой fly-admin-printer.

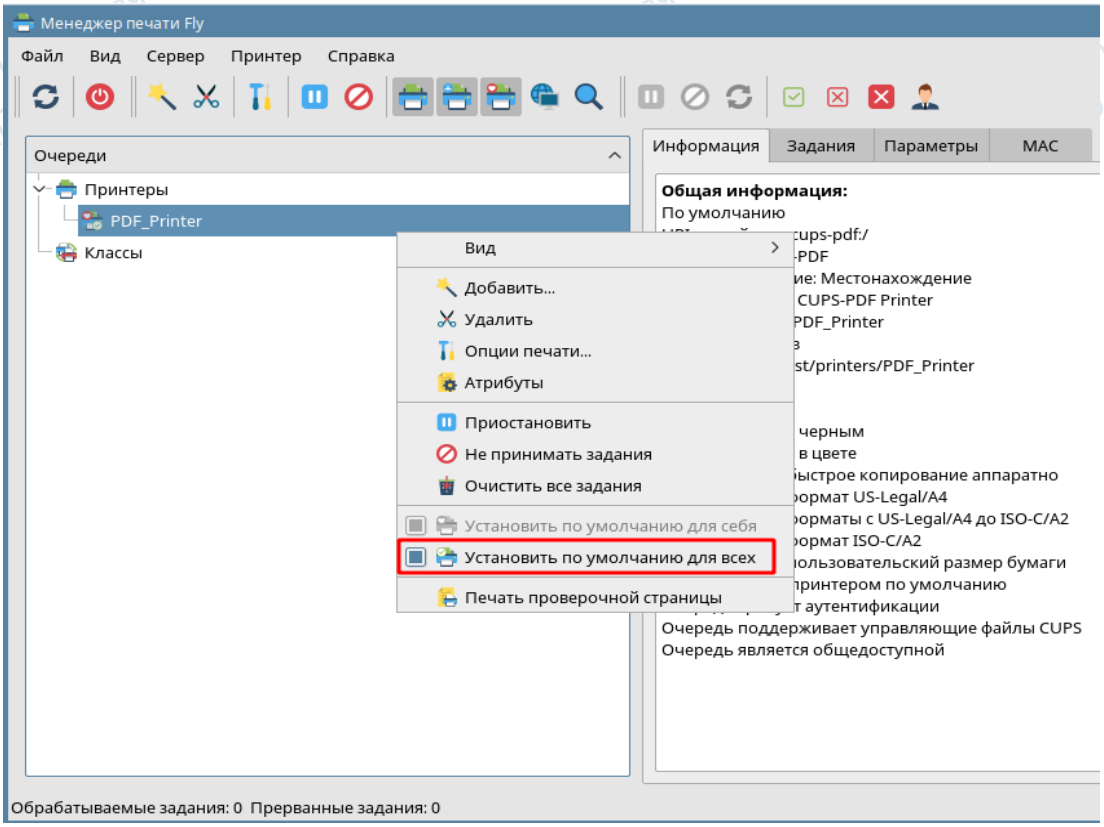
16 Нажать кнопку «Добавить ...» на панели инструментов. В появившемся окне «Мастера установки принтеров и классов» выбрать обнаруженный принтер и нажать кнопку «Далее».



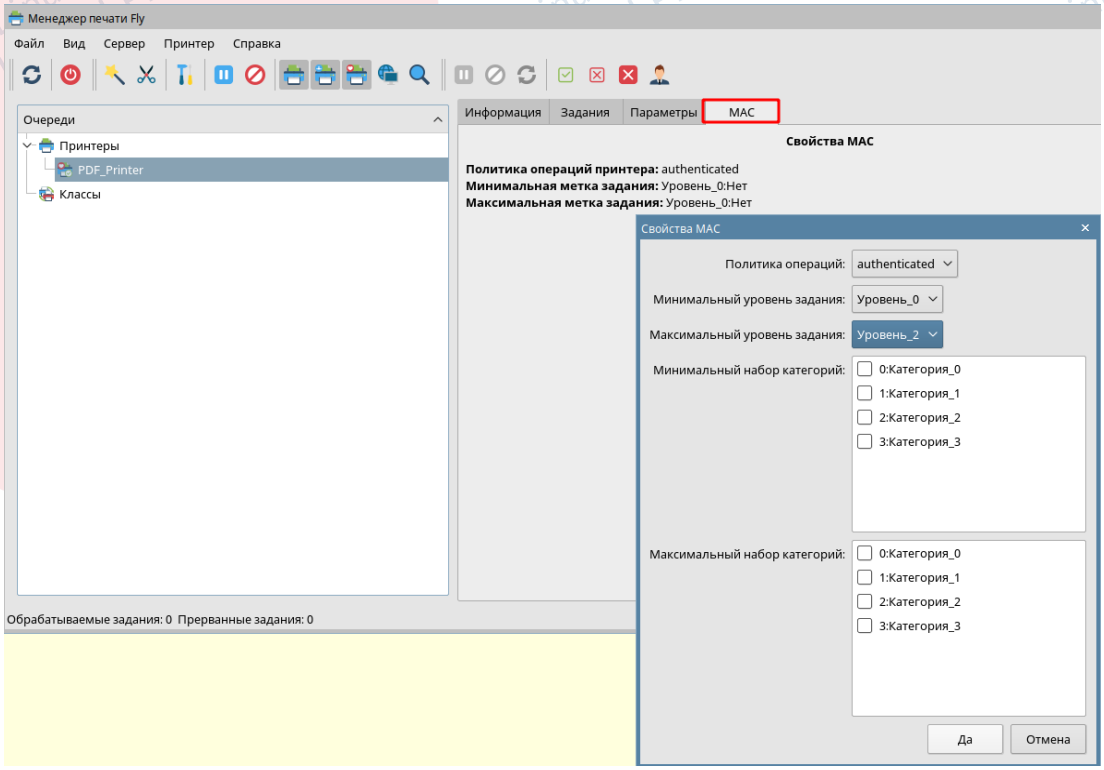
17 В следующем окне «Мастера установки принтеров и классов» установить параметр «Разрешить общий доступ». Также можно изменить название принтера (поле «Наименование»). Нажать кнопку «Завершить».



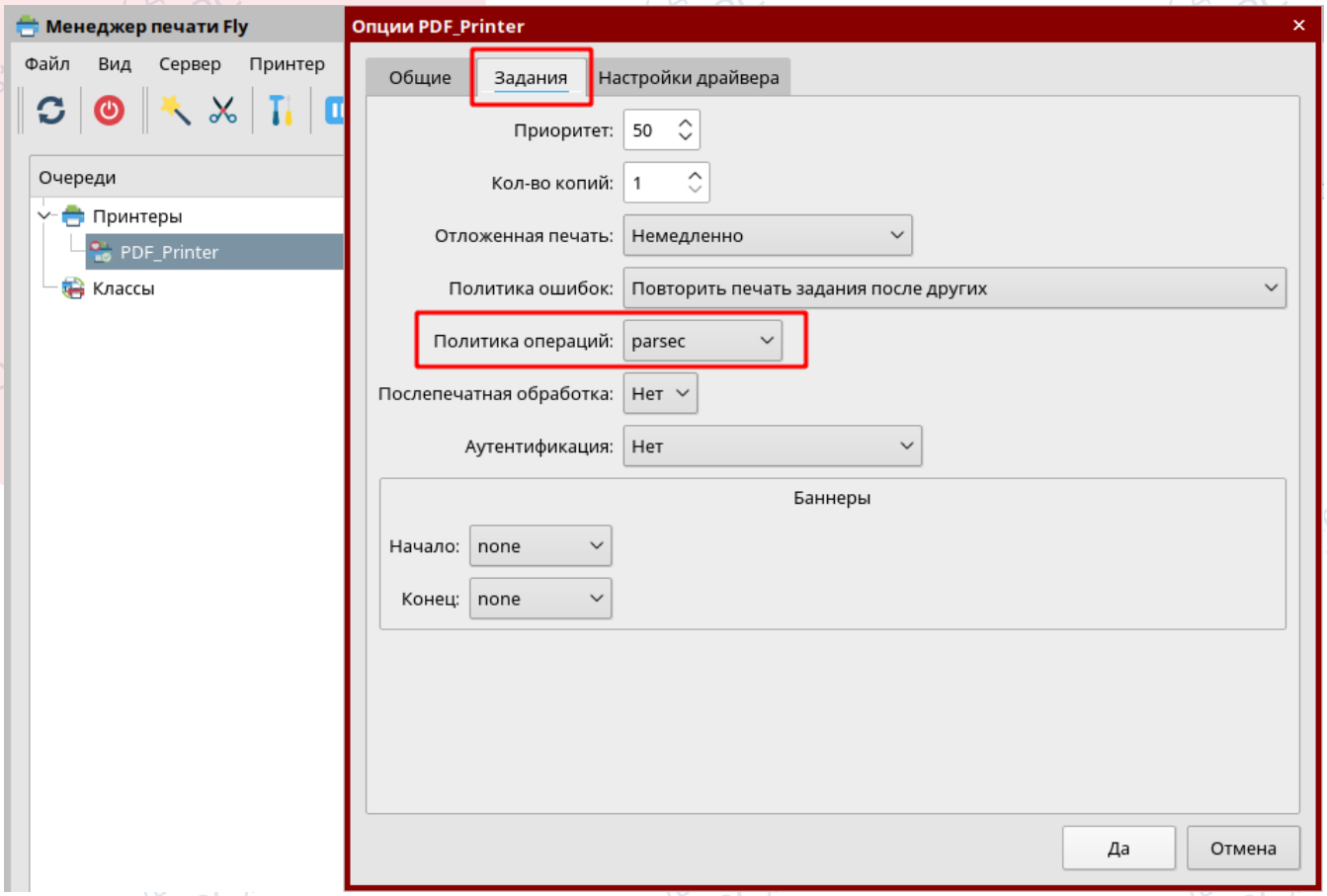
18 Назначить установленный принтер как принтер по умолчанию для всех.



19 На вкладке «MAC» ввести минимальную и максимальную метки для заданий. Установить минимальный уровень — 0, максимальный — 2.



20 В главном меню выбрать пункт «Принтер», в выпадающем меню выбрать пункт «Опции печати ...». В появившемся окне перейти на вкладку «Задания» и установить значение параметра «Политика операция» равным «parsec».



Настройка клиента службы печати, печать файлов

Задание: Настроить на хосте c1.astra.test клиентскую часть службу печати. Отправить несколько заданий, входя в сеанс под учетной записью доменного пользователя ipauser2 с нулевой и ненулевыми метками безопасности. Зайти на сервер печати под учетной записью cups-admin и произвести маркировку заданий на печать с помощью программы fly-print-station.

1 Зайти под учетной записью локального администратора (sa) на ВМ c1.astra.test.

2 В файле /etc/cups/client.conf определить параметр ServerName, присвоив значение равное DNS имени сервера печати.

3 В командной строке проверить доступность сетевого принтера.

4 С помощью утилиты командной строки отправить на печать файл /etc/cups/client.conf.

5 Зайти на ВМ c1.astra.test под доменной учетной записью пользователя ipauser2 с уровнем конфиденциальности 0.

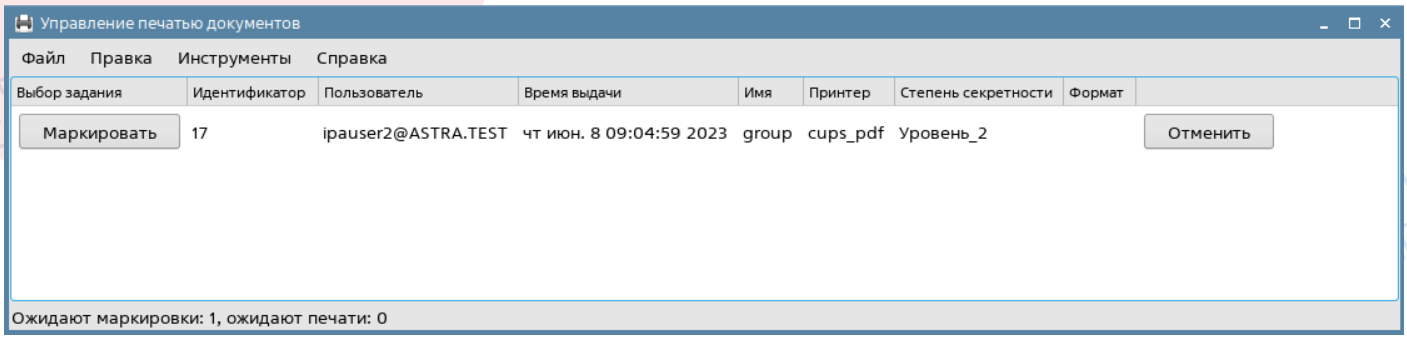
6 В редакторе kate открыть файл /etc/hosts и отправить его на печать.

7 Зайти на ВМ c1.astra.test под доменной учетной записью пользователя ipauser2 с уровнем конфиденциальности 1.

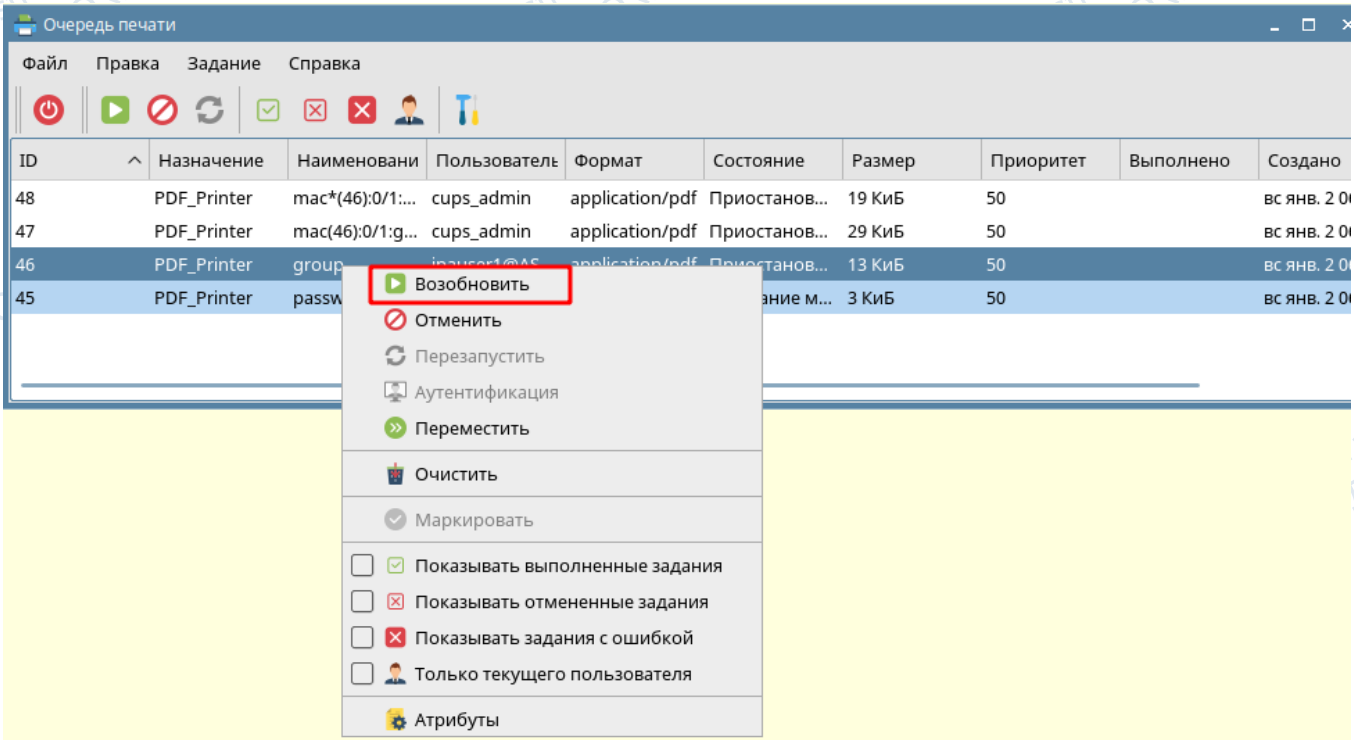
8 Напечатать с помощью утилиты командной строки файл /etc/passwd.

9 Открыть в редакторе kate файл /etc/group и отправить его на печать.

10 На ВМ print-server.astra.test под учетной записью cups_admin произвести маркировку с помощью утилиты fly-print_station.

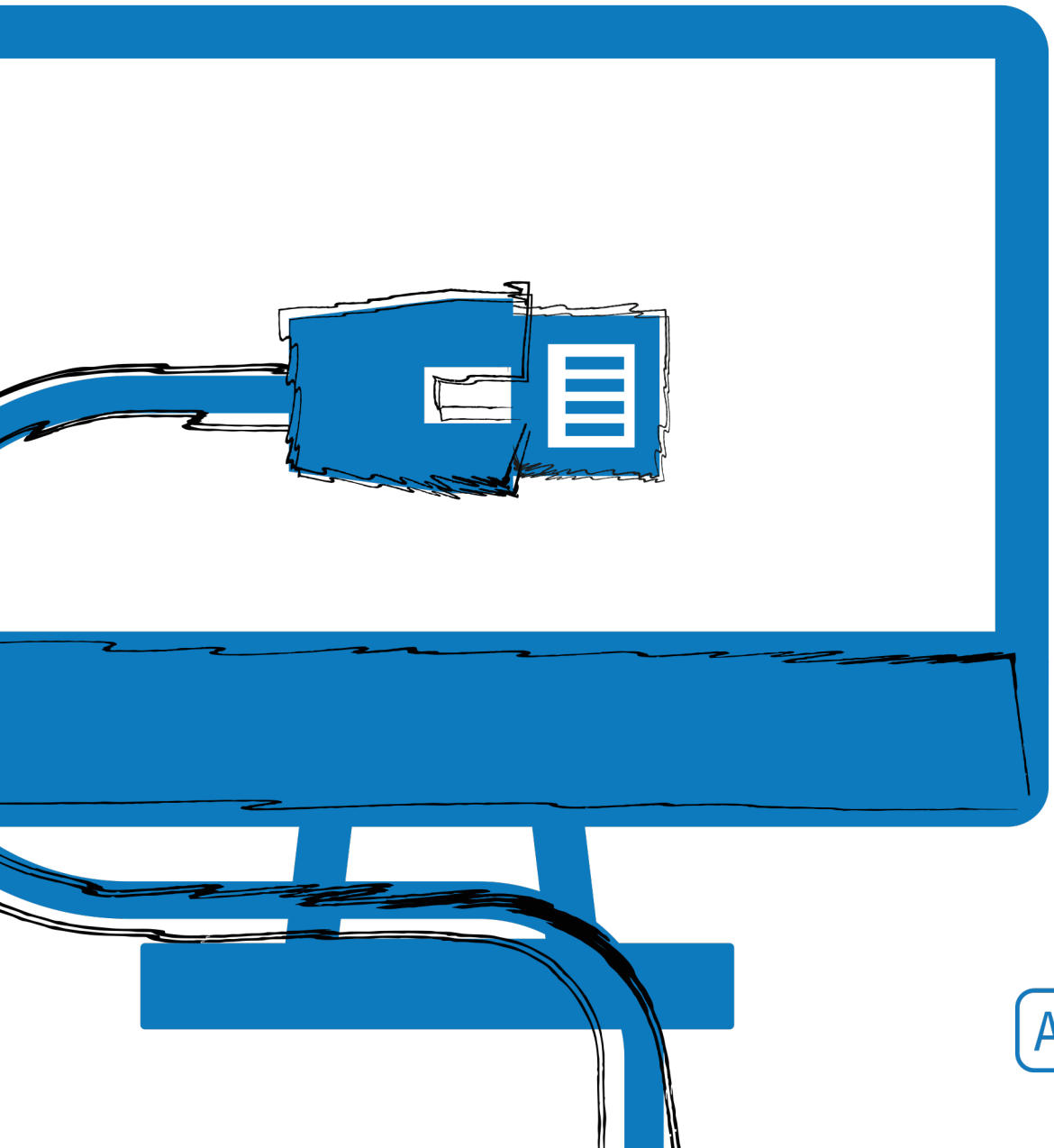


11 После выполнения маркировки задания в контекстном меню задания выбрать пункт «Возобновить», чтобы распечатать документ.
Примечание: кроме основного задания, маркировка создаст еще два дополнительных задания. Для возобновления печати следует выбрать основное задание.



Модуль 12

Установка Astra Linux по сети



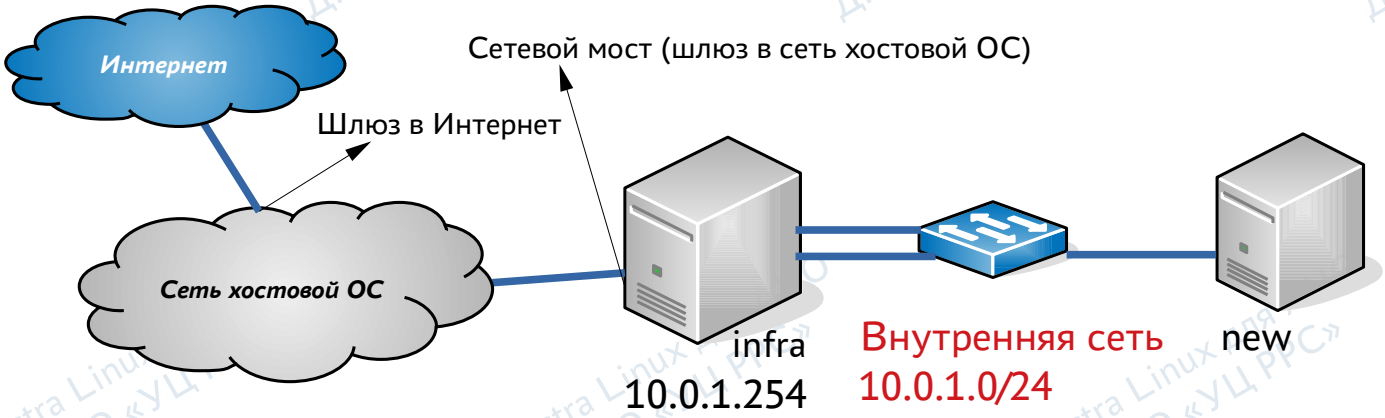
ASTRA LINUX®

Модуль 12. Установка Astra Linux по сети

Описание практического задания

- Создание сетевого репозитория.
- Установка TFTP-сервера.
- Настройка DHCP-сервера.
- Выполнение автоматической удаленной установки.

Схема сети



Создание репозитория Astra Linux

Задание: На ВМ infra создать образ загрузочного компакт-диска с ОС Astra Linux. Настроить автоматическое монтирование образа загрузочного диска в каталог /var/www/infra/astra.

1 Предполагается, что веб-сервер Apache2 уже установлен. Режим AstraMode выключен.

2 Создать образ загрузочного компакт-диска с именем /iso/1.7.3.iso.

3 Добавить строку в файл /etc/fstab для постоянного монтирования образа дистрибутива в /var/www/infra/astra.

4 Выполнить монтирование до перезагрузки.

Установка и настройка TFTP-сервера

Задание: Установить TFTP-сервер. Настроить параметры для запуска TFTP-сервера в конфигурационном файле /etc/default/tftpd-hpa. Скопировать в каталог /srv/tftp файлы с установочного диска, необходимые для сетевой установки ОС. Создать конфигурационный файл для PXE-загрузчика /srv/tftp/pxelinux.cfg/default, взяв за основу пример файла с wiki.astralinix.ru

1 Установить TFTP-сервер.

2 Изменить параметр TFTP_OPTIONS в файле /etc/default/tftpd-hpa, добавив необходимые параметры.

3 Скопировать файлы, необходимые для сетевой установки, в каталог /srv/tftp.

4 Создать каталог `/srv/tftp/pxelinux.cfg`.

5 В этом каталоге создать конфигурационный файл PXE-загрузчика с именем default . Файл /srv/tftp/pxelinux.cfg/default можно взять из статьи wiki.astralinux.ru «Установка ОС Astra Linux по сети» по адресу: https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277939.

6 Указать в файле /srv/tftp/pxelinux.cfg/default используемые протокол и адрес сервера, на котором будет размещен файл с ответами на вопросы установщика ОС. В данной практической работе файл будет находиться на веб-сервере, запущенном в ВМ infra – http://10.0.1.254.

Установка и настройка DHCP-сервера

Задание: На ВМ infra установить DHCP-сервер. Указать имя сетевого интерфейса (bond0) в конфигурационном файле /etc/default/isc-dhcp-server. Настроить пул динамических адресов 10.0.1.100-10.0.1.120, указав адреса шлюза и DNS-севера и имя файла с PXE-загрузчиком.

1 Установить DHCP-сервер.

2 В файле /etc/default/isc-dhcp-server указать имя интерфейса bond0.

3 В файле /etc/dhcp/dhcpd.conf добавить описание топологии сети 10.0.1.0/24:

- диапазон адресов 10.0.1.100-10.0.1.120;
- адрес DNS серверов- 10.0.1.254;
- адрес шлюза - 10.0.1.254;
- указать имя файла с PXE-загрузчиком.

4 Перезапустить DHCP-сервер.

Создание файла с ответами и установка ОС по сети

Задание: Создать файл с ответами /var/www/infra/preseed.cfg, используя пример из wiki.astralinux.ru. Изменить в файле строки, относящиеся к описанию репозитория Astra Linux. Изменить имя учетной записи, создаваемой в процессе установки. Указать метод автоматической разметки диска, который помещает все файлы в один раздел и создает область подкачки. Выполнить установку ОС по сети.

1 В каталоге /var/www/infra создать файл с ответами для автоматической установки preseed.cfg .
Пример файла можно скачать по адресу:
https://wiki.astralinux.ru/pages/viewpage.action?pageId=263031386

2 В файле preseed.cfg нужно указать:

- имя протокола, адрес сервера и каталог, в котором находится дистрибутив.
- Указать учетную запись пользователя sa и задать для него пароль (12345678).
- схему разметки диска с одним разделом под все файлы.
- (опционально) убрать или закомментировать все лишние строки. С помощью команды
  sudo debconf-set-selections -c preseed.cfg
  проверить корректность формата файла.

3 Создать новую виртуальную машину new:

- процессор — 1;
- RAM — 2 ГБ;
- диск — 30 ГБ;
- сетевой адаптер — внутренняя сеть;
- операционную систему вручную не устанавливать, виртуальный компакт-диск в виртуальный привод не вставлять.

4 При запуске машины new следует выбрать установку по сети.
Примечание: для VirtualBox следует нажать F12 и появится меню. В меню выбирать загрузку по сети путем нажатия на клавишу l — LAN.

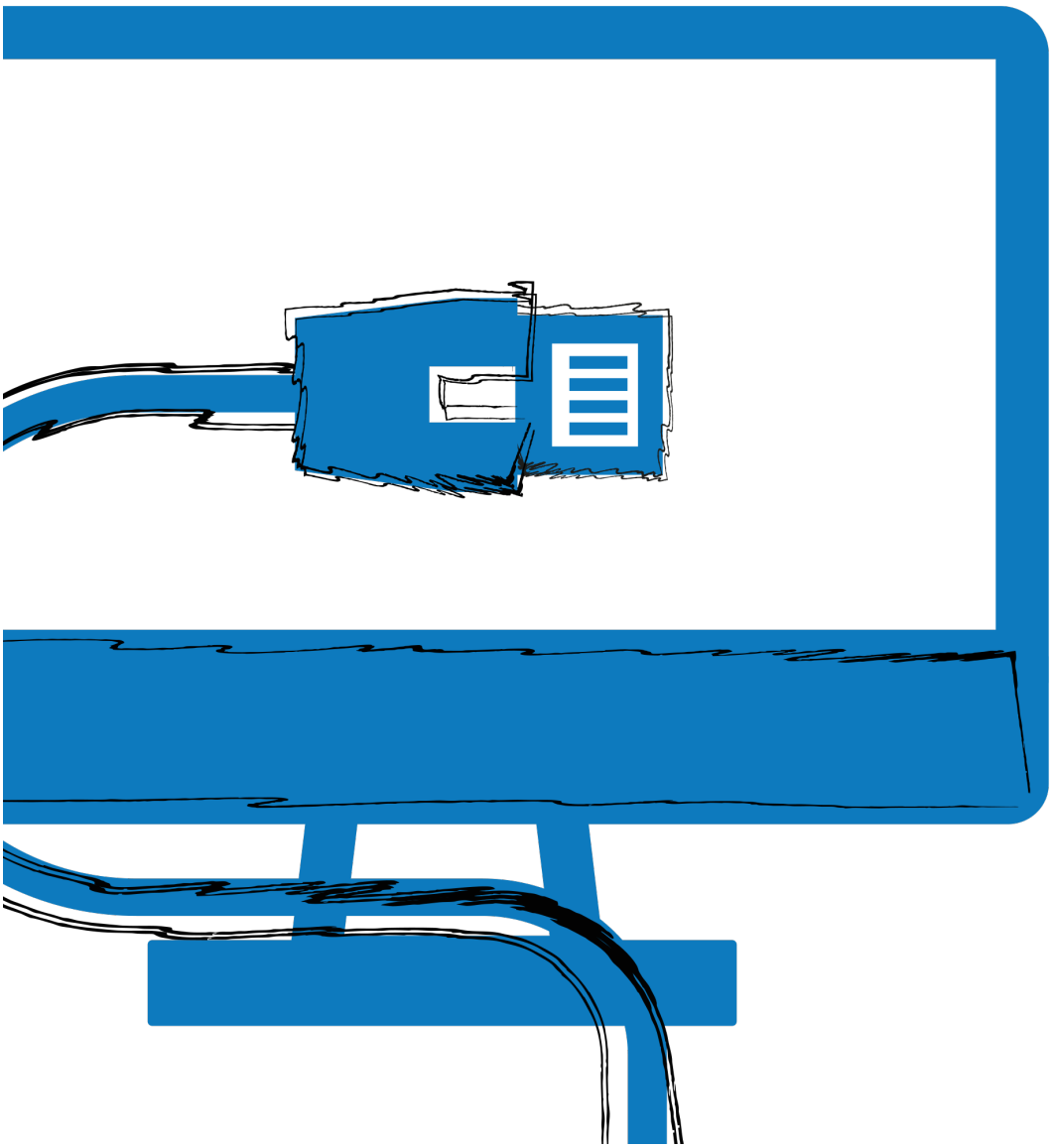
5 Установка будет выполнена автоматически:

- Если возникнет ошибка или появится сообщение, требующее ответа, то это означает, что один из разобранных выше шагов был выполнен некорректно. Тогда следует вернуться, обнаружить и исправить ошибки.

В случае, если все было настроено верно, то установка будет произведена без участия человека, ВМ будет перезагружена, и будет доступно окно входа в систему.

Модуль 13 (опциональный)

Основы IPv6



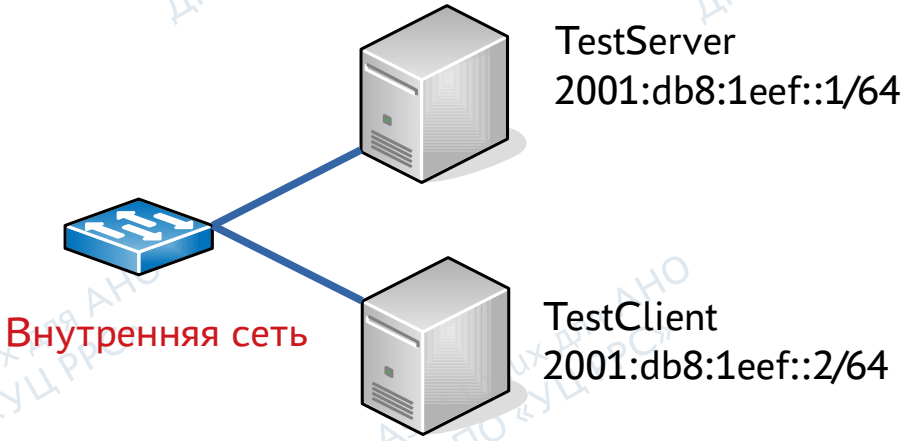
ASTRA LINUX®

Модуль 13. Основы IPv6

Описание практического задания

- Проверка связи по IPv6 с использованием Link-Local адресов.
- Проверка связи по IPv6 с использованием статически назначенных адресов.
- Настройка клиента для получения адреса с помощью RA.
- Настройка клиента для получения адреса с помощью DHCPv6.

Схема сети



Проверка связи с использованием Link Local адресов

1 Создать ВМ TestServer и TestClient путем клонирования ВМ template_1704_3.

2 На TestServer посмотреть IPv6 адрес.

3 На TestClient выполнить ping хоста TestServer, используя IPv6 адрес TestServer.

Назначение статических IPv6 адресов

1 На обеих ВМ отключить и замаскировать NetworkManager.

2 На TestServer настроить статический IPv6 адрес 2001:db8:1eef::1 путем внесения изменений в файл /etc/network/interfaces.

3 Активировать сетевой интерфейс eth0 на TestServer и проверить, что требуемый IPv6 адрес назначен.

4 На TestClient настроить статический IPv6 адрес 2001:db8:1eef::2 путем внесения изменений в файл /etc/network/interfaces.

5 Активировать сетевой интерфейс eth0 на TestClient и проверить, что требуемый IPv6 адрес назначен.

6 На TestClient проверить доступность TestServer командой ping, используя назначенный статический адрес.

7 Назначить на TestClient произвольный статический IPv6-адрес в той же сети.

8 Обновить сетевой интерфейс eth0, убедиться, что адрес назначен.

9 На TestServer с помощью команды ping проверить доступность TestClient по новому адресу.

Настройка radvd для имитации маршрутизатора на сервере TestServer

1 На TestServer установить radvd.
Примечание: следует вставить образ установочного компакт-диска с Astra Linux 1.7.3 в привод ВМ и настроить компакт-диск в качестве репозитория ПО.

2 На TestServer сконфигурировать radvd для объявления префикса 2001:db8:1eef::/64.

3 Запустить службу radvd.

Настройка получения IPv6 адресов на TestClient с применением RA

1 Настроить на TestClient в /etc/network/interfaces получение IPv6 по RA. Статические настройки удалить.

2 На TestClient применить настройки IPv6, проверить получение IPv6. адреса.
Примечание: если назначение адресов не произошло, перезагрузите ВМ TestClient.

3 На TestServer проверить пинг полученного из EUI-64 Global Unicast-адреса, и пинг до временного адреса.

4 Посмотреть таблицу маршрутизации.

Настройка на TestServer isc-dhcp-server для выдачи IPv6-адресов по dhcpv6

1 Установить isc-dhcp-server.

2 Включить в файле /etc/default/isc-dhcp-server.

3 Добавить настройку префикса сети для выдачи по DHCPv6 в файле /etc/dchp/dhcpd6.conf.

```
sudo vi /etc/dchp/dhcpd6.conf
subnet6 2001:db8:1eef::/64 {
       range6 2001:db8:1eef::dfc5:d0
2001:db8:1eef::dfc5:ff;
}
```

4 Запустить isc-dhcp-server, при необходимости установить автоматический запуск службы.

Настройка получения IPv6 адресов на TestClient с применением по DHCPv6

1 Настроить на TestClient в /etc/network/interfaces получение IPv6 по DHCPv6.

2 На TestClient применить настройки IPv6, проверить получение IPv6 адреса.

3 На TestServer проверить пинг полученного из EUI-64 Global Unicast-адреса, и пинг до временного адреса.

4 Посмотреть таблицу маршрутизации.

5 Если нет пинга или default-маршрута то необходимо проверить состояние radvd (так как default gateway получается с помощью RA, а не DHCPv6), при необходимости включить и добавить в автозапуск.