НАСТРОЙКА ОБЩЕЙ КОНФИГУРАЦИИ СЕТИ.

Данная работа посвящена введению в IOS, изучению основных команд, необходимых для настройки сети.

Цель работы: Определить роль Межсетевой Операционной системы (IOS). Получить практические навыки по:

- настройке паролей;
- конфигурированию основных команд на маршрутизаторе и коммутаторе;
- проверке конфигурации;
- сохранению конфигурации.

Теоритические сведения

Подобный персональному компьютеру, маршрутизатор или коммутатор не могут функционировать без операционной системы. Без операционной системы у аппаратных средств нет никаких возможностей. Cisco Internetwork Operating System (IOS) является системным программным обеспечением в устройствах Cisco. Cisco IOS используется для большинства устройств Cisco независимо от размера и типа устройства. Cisco IOS предоставляет устройствам следующие сетевые службы:

- Основное направление и переключение функций
- Надежный и безопасный доступ к сетевым ресурсам
- Сетевая масштабируемость

К конфигурированию Cisco IOS получают доступ, используя интерфейс командной строки (CLI). Возможности, доступные через CLI, различаются в зависимости от версии IOS и типа устройства. Размер самого файла IOS составляет несколько мегабайтов и хранится в полупостоянной области памяти, названной флэш-памятью. Флэш-память обеспечивает энергонезависимое хранение. Это означает, что содержание памяти не потеряно, когда устройство выключено. Даже при том, что содержание не потеряно, они могут быть изменены или перезаписаны при необходимости. Использование флэш-памяти позволяет IOS быть модернизированным до более новых версий или добавлять новые функции.

Методы доступа к CLI

Есть несколько способов получить доступ к CLI. Самые обычные методы:

- Console
- Telnet или SSH
- Порт AUX

Console

К CLI можно получить доступ через console порт. Console использует низкоскоростное последовательное соединение, чтобы непосредственно соединить компьютер или терминал к порту console на маршрутизаторе или коммутаторе. Console порт обеспечивает доступ к маршрутизатору. Он доступен, даже если никакие сетевые сервисы не сконфигурированы на устройстве. Примеры использования console:

- Начальная конфигурация сетевого устройства
- Процедуры аварийного восстановления и поиск неисправностей, где удаленный доступ не возможен
- Процедуры восстановления пароля

Telnet и SSH

Метод для получения удаленного доступа к маршрутизатора CLI через telnet. В отличие от console-соединения, сессии Telnet требуют активных сетевых сервисов на устройстве. У сетевого устройства должен быть по крайней мере один активный интерфейс, сконфигурированный IP адрес. Устройства Cisco включают процесс сервера Telnet, когда устройство запущено. IOS также поддерживает клиент Telnet. Хост с клиентом Telnet может получить доступ к vty сессиям, работающим на устройстве Cisco. Из соображений безопасности IOS требует, чтобы сессия Telnet использовала пароль как минимальный опознавательный метод.

SSH протокол является более безопасным методом для отдаленного доступа устройства. Этот протокол подобен Telnet, за исключением того, что он использует более безопасные сетевые службы. SSH обеспечивает более сильное установление подлинности пароля чем Telnet и использует шифрование, транспортируя данные о сессии. Сессия SSH шифрует все связи между клиентом и устройством. *(Совет: всегда используйте SSH вместо Telnet при любой возможности.)* Большинство более новых версий IOS содержит сервер SSH. В некоторых устройствах этот сервис включен по умолчанию. Другие устройства требуют, чтобы сервер SSH был включен.

AUX

Другой способ установить сессию CLI отдаленно через телефонную связь, через модем, соединенный с портом AUX маршрутизатора. Подобный соединению console, этот метод не требует, чтобы никакие сетевые сервисы были сконфигурированы, или доступны на устройстве. Порт AUX может также использоваться как порт console, с прямой связью с компьютером, выполняющим предельную программу эмуляции. Вообще, порт AUX используется вместо порта console тогда, когда есть проблемы с console портом.

Сетевые устройства зависят от двух типов программного обеспечения для их работы: операционная система и конфигурация. Как операционная система в любом компьютере, здесь она также облегчает основную работу компонентов аппаратных средств устройства. Конфигурационные файлы содержат команды программного обеспечения Cisco IOS, используемые для настройки функциональности устройства Cisco. Администратор сети создает конфигурацию, которая определяет желаемую функциональность устройства

Cisco [2].

Типы Конфигурационных файлов

Устройство сети Cisco содержит два конфигурационных файла:

- Рабочий конфигурационный файл - используемый во время текущей работы устройства.
- Конфигурационный файл стартапа - используемый в качестве резервной конфигурации и загружен, когда устройство запущено.

Конфигурационный файл может также быть сохранен отдаленно на сервере как резервная копия. Конфигурационный файл стартапа используется во время системного стартапа, чтобы сконфигурировать устройство. Конфигурационный файл стартапа или файл конфигурации стартапа сохранены в энергонезависимой оперативной памяти (NVRAM). Так как NVRAM является энергонезависимой, когда устройство Cisco выключено, файл остается неповрежденным. Файлы конфигурации стартапа загружаются в оперативную память каждый раз, когда маршрутизатор запущен или перезагружен. Как только конфигурационный файл загружен в оперативную память, то это считается рабочей конфигурацией. Рабочая конфигурация изменяется, когда администратор сети выполняет конфигурацию устройства. Изменения рабочей конфигурации немедленно затронут работу устройства Cisco. После произведения любых изменений у администратора есть опция сохранения изменений файла конфигурации стартапа так, чтобы они использовались в следующий раз при запуске устройства.

Поскольку рабочий конфигурационный файл находится в оперативной памяти, он будет потерян, если устройство будет выключено или перезапущено. Изменения, произведенные в файле рабочей конфигурации, будут также потеряны, если они не будут сохранены в файле конфигурации стартапа прежде, чем устройство будет отключено.

Для работы в IOS существуют два основных режима работы:

- Пользовательский режим EXEC
- Привилегированный режим EXEC

В целях безопасности, программное обеспечение Cisco IOS разделяет сессии EXEC на два режима доступа. У каждого режима есть подобные команды. Однако у привилегированного режима EXEC есть более высокий уровень управления.

Пользовательский Режим EXEC

Пользовательский режим EXEC ограничен возможностям, но полезен для некоторых основных операций. Пользовательский режим EXEC позволяет работать только с ограниченным количеством основных команд. Данный режим работы не допускает выполнение команд, которые могли бы изменить конфигурацию устройства. Пользовательский режим EXEC идентифицирован подсказкой CLI, которая заканчивается символом «>»:

Router>

Привилегированный режим EXEC

Выполнение некоторых конфигураций требует, чтобы администратор сети использовал привилегированный режим EXEC. Привилегированный режим EXEC может быть идентифицирован подсказкой, заканчивающейся символом «#»:

```
Switch#
```

Глобальный режим конфигурации и другие, более определенные режимы конфигурации, могут только быть достигнуты из привилегированного режима EXEC. Команды enable и disable, используются для перехода между пользовательским режим EXEC и привилегированным режимом EXEC, соответственно. Чтобы получить доступ к привилегированному режиму EXEC, необходимо использовать команду enable. Синтаксис для ввода команды «enable»:

```
Router>enable
```

После ввода команды пользователь получает доступ к привилегированному режиму(знак «#» в конце подсказки указывает, что маршрутизатор находится теперь в привилегированном режиме EXEC):

```
Router#
```

Если было сконфигурировано установление подлинности для привилегированного режима EXEC, то для входа необходимо ввести пароль. Например:

```
Router>enable
Password:
Router#
```

Команда «disable» используется, чтобы перейти от привилегированного режима EXEC к режиму пользователя EXEC. Например:

```
Router#disable
Router>
```

Каждая команда IOS имеет определенный формат или синтаксис. Общий синтаксис для команды: команда, сопровождаемая любыми соответствующими ключевыми словами и аргументами. Некоторые команды включают подмножество ключевых слов и аргументов, которые обеспечивают дополнительную функциональность. Ключевые слова

описывают определенные параметры переводчику команды. Например, команда **«show»** используется для вывода информации на экран об устройстве. У этой команды есть различные ключевые слова, которые могут использоваться, чтобы определить, что именно должно быть выведено на экран. Например:

```
Switch#show running-config
```

Команда **«show»** сопровождается ключевым словом **«running-config».** Ключевое слово обозначает, что рабочая конфигурация должна быть выведена на экран. Команда могла бы потребовать одного или более аргументов. В отличие от ключевого слова, аргумент - вообще не предопределенное слово. Аргумент - значение или переменная, определенная пользователем. Как пример, применяя описание к интерфейсу командой **«description»** вводят:

```
Switch(config-if)#description Fa1/0 – to R1 Switch
```

В данном случае команда – **description**, аргумент – **Fa1/0 – to R1 Switch.** Пользователь определяет аргумент. Для этой команды аргумент может быть любой текстовой строкой до 80 символов. После ввода каждой полной команды, включая любые ключевые слова и аргументы, нажимают клавишу **<ENTER>,** чтобы представить команду интерпретатору команд.

Глобальный конфигурационный режим

Основной конфигурационный режим называется global configuration или global config. Глобальный режим конфигурации используется для доступа к определенным режимам конфигурации. Команда **«configure terminal»** используется для перехода от привилегированного режима EXEC к глобальному режиму конфигурации:

```
Router#configure terminal
```

Как только команда выполнена, то маршрутизатор находится в глобальном режиме конфигурации:

```
Router(config)#
```

Помимо глобального режима конфигурации есть много различных режимов конфигурации. Каждый из этих режимов позволяет конфигурировать какую-то часть устройства:

- Interface mode – для конфигурации одного из сетевых интерфейсов (Fa0/0, S0/0/0..)
- Line mode – для конфигурации одной из сессий (физической или виртуальной) (console, AUX, VTY..)

- Router mode – для конфигурации одного из протоколов маршрутизации.

Так как изменения конфигурации произведены в пределах интерфейса или процесса, то изменения только затрагивают тот интерфейс или процесс. Чтобы выйти из определенного режима конфигурации и возвратиться к глобальному режиму конфигурации, необходимо ввести **«exit»**. Чтобы возвратиться к привилегированному режиму EXEC, необходимо ввести **«end»** или сочетание клавиш Ctrl-Z. После проведения некоторых изменений желательно сохранить их в конфигурационном файле стартапа, сохраненном в NVRAM. Это препятствует тому, чтобы изменения были потеряны из-за перебоя в питании или преднамеренного перезапуска. Команда для сохранения рабочей конфигурации:

```
Router#copy running-config startup-config
```

Назначение имени устройству

Если имя узла явно не сконфигурировано, маршрутизатор использует имя узла по умолчанию "Router". У коммутатора имя по умолчанию "Switch". Получая доступ к удаленному устройству, используя Telnet или SSH, важно иметь подтверждение, что подключение было сделано к нужному устройству. Если бы все устройства оставили с их именами по умолчанию, то мы не могли бы идентифицировать, к какому устройству подсоединились. Поэтому уникальное имя узла должно быть сконфигурировано для каждого устройства.

Возьмем в качестве примера три маршрутизатора (Рисунок 1), соединенных в сети, охватывающей три различных города (Минск, Москва, Прага). В этом примере каждый маршрутизатор как офис компании для определенного города. Именами маршрутизаторов могут быть названия городов Минск, Москва, Прага.

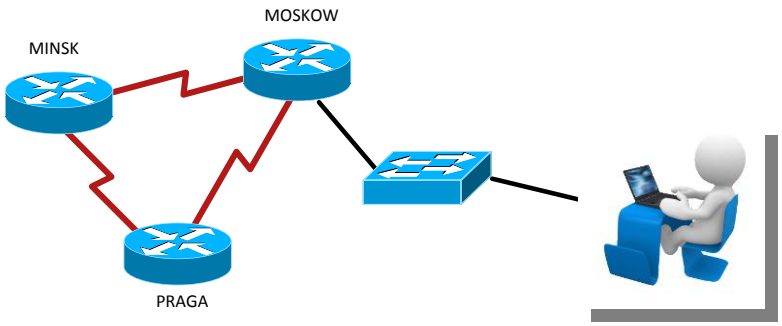

Рисунок 1

Для конфигурация имени узла необходимо перейти в глобальный режим конфигурации:

```
Router#configure terminal
```

В глобальном режиме необходимо ввести имя узла:

```
Router(config)#hostname MOSKOW
```

После того, как команда выполнена, имя маршрутизатора изменится

на:

```
MOSKOW(config)#
```

Чтобы удалить название устройства необходимо ввести:

```
MOSKOW(config)# no hostname
Router(config)#
```

Настройка паролей

Физически ограничивающий доступ к сетевым устройствам с заблокированными стойками - хорошая практика; однако, пароли - основная защита против несанкционированного доступа к сетевым устройствам. На каждом устройстве должны быть сконфигурированы пароли для ограничения доступа. IOS использует иерархические режимы для обеспечения безопасности. Таким образом, несколько паролей позволяют различные привилегии доступа устройству. Некоторые виды паролей:

- Console password – ограничивает доступ к устройству, используя консольное соединение.
- Enable password – ограничивает доступ к привилегированному режиму EXEC.
- Enable secret password – зашифрованный пароль, ограничивает доступ к привилегированному режиму EXEC.
- VTY password – ограничивает доступ к устройству, используя Telnet соединение.

Для надежной работы лучше всего использовать различные пароли для каждого из этих уровней доступа. Хотя вхождение в систему с многократными и различными паролями неудобно, это - необходимая предосторожность, чтобы должным образом защитить сетевую инфраструктуру от несанкционированного доступа.

Console password.

Следующие команды используются в глобальном режиме конфигурации:

```
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#login
```

В команде **line console 0** ноль используется, для предоставления первого (и в большинстве случаев последнего) интерфейса консоли для маршрутизатора. Вторая команда, **password *cisco*** определяет пароль для доступа через консоль. Как только эти три команды выполнены, необходимо будет вводить пароль каждый раз, когда пользователь пытается получить доступ к консольному порту.

Enable password и Enable secret password

Для обеспечения дополнительной безопасности, используйте команды **Enable *password*** или **Enable secret *password***. Любая из этих команд может использоваться для получения доступа к привилегированному

режиму EXEC. Следующие команды используются для установки пароля:

```
Router(config)#enable password password
Router(config)#enable secret password
```

VTY Пароль

Vty сессии предоставляют доступ к маршрутизатору через Telnet. По умолчанию большинство устройств Cisco поддерживают пять сессий VTY, которые пронумерованы от 0 до 4. Пароль должен быть установлен для всех доступных vty сессий. Тот же самый пароль может быть установлен для всех соединений. Следующие команды используются для установки пароля на vty сессиях:

```
Router(config)#line vty 0 4
Router(config-line)#password password
Router(config-line)#login
```

Отображение пароля в зашифрованном виде

Другая полезная команда препятствует тому, чтобы пароли воспринимались как простой текст, просматривая конфигурационные файлы. Это - команда **service password-encryption**. Эта команда шифрует пароли после того, как они сконфигурированы. Команда шифрования пароля сервиса применяет слабое шифрование ко всем незашифрованным паролям. Цель этой команды состоит в том, чтобы препятствовать посторонним людям просматривать пароли в конфигурационном файле.

Сообщения баннера

Хотя требование паролей является одним способом ограничить доступ к оборудованию, но также очень важно предупредить неуполномоченных людей об ответственности при входе на устройство. Здесь лучше всего использовать баннеры. Они могут быть важной частью судебного процесса, когда кто-то преследуется по суду за то, что он получил несанкционированный доступ к устройству. Точная формулировка баннера зависят от местных законов и корпоративной политики. Вот некоторые примеры информации в баннерах:

- "Использование устройства определенно для уполномоченного персонала."
- "Деятельность может быть проверена."
- "Судебный иск будет преследоваться для любого несанкционированного использования."

Создание баннеров – простой процесс; однако, баннеры должны использоваться соответственно. Когда баннер используется, он никогда не должен приветствовать кого-то в маршрутизаторе. Это должно выявлять круг людей, которым разрешено получить доступ к устройству. Далее, баннер может включать намеченные системные закрытия и другую информацию, которая затрагивает всех сетевых пользователей.

IOS обеспечивает многократные типы баннеров. Один общий баннер - сообщение MOTD. Это часто используется для юридического уведомления,

потому что это выведено на экран ко всем соединенным терминалам. Чтобы сконфигурировать MOTD в глобальном режиме конфигурации вводят команду:

Switch(config)#banner motd # WARNING!!! Computer network. Lab1 #

Как только команда выполнена, баннер будет выводиться на экран при всех последующих попытках получить доступ к устройству (пока баннер не будет удален).

Сохранение конфигурации на TFTP-server

Конфигурационные файлы должны быть сохранены как резервные файлы в случае возникновения проблем. Конфигурационные файлы могут быть сохранены на TFTP сервер, компакт-диск, карту памяти USB, или дискету. Конфигурационный файл должен также быть включен в сетевую документацию. Для сохранения конфигурации на сервере TFTP используют **команды copy running-config tftp** или **copy startup-config tftp**. Пример сохранения конфигурации на TFTP сервере:

1. Введите команду **copy running-config tftp**
2. Введите IP-адрес хоста, где будет сохранен конфигурационный файл.
3. Введите имя конфигурационного файла.
4. Введите **Yes**, чтобы подтвердить выбор.

Конфигурирование интерфейсов маршрутизатора.

У каждого интерфейса Ethernet должны быть IP-адрес и маска подсети, чтобы направлять IP пакеты. Чтобы сконфигурировать интерфейс Ethernet необходимо сделать следующие шаги:

1. Войти в глобальный режим конфигурации.
2. Войти в режим конфигурации интерфейса.
3. Назначить адрес интерфейса и маску подсети.
4. Включить интерфейс.

Для конфигурации интерфейса используются следующие команды:

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address ip_address netmask
Router(config-if)#no shutdown
```

Конфигурирование Serial интерфейса

Serial интерфейсы используются, чтобы соединить WANs с маршрутизаторами на удаленном сайте или интернет-провайдере. Чтобы сконфигурировать интерфейс Serial необходимо сделать следующие шаги:

1. Войти в глобальный режим конфигурации.
2. Войти в режим конфигурации интерфейса.

3. Назначить адрес интерфейса и маску подсети.
4. Установить тактовую частоту, если соединен кабель DCE. *(Пропустить этот шаг, если соединен кабель DTE)*.
5. Включить интерфейс.

У каждого Serial интерфейса должны быть IP-адрес и маска подсети, чтобы передавать IP пакеты. Конфигурация IP-адреса использует следующие команды:

```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address ip_address netmask
```

На serial линиях, которые непосредственно соединениы, одна сторона должна действовать в качестве DCE, чтобы обеспечивать сигнал синхронизации. Команды, используемые для установления тактовой частоты на интерфейсе Serial:

```
Router(config)#interface Serial 0/0/0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

Поскольку имя узла помогает идентифицировать устройство в сети, описание интерфейса может быть полезным для поиска неисправностей. Описание интерфейса появится в вводе следующих команд: show startup-config, show running-config, и show interfaces. Описание может помочь в определении устройств или местоположений, соединенных с интерфейсом. Для создания описания, необходимо использовать команды:

```
switch1#configure terminal
switch1(config)#interface fa0/0
switch1(config-if)#description Connects to main switch
in Building A
```

Практическая часть

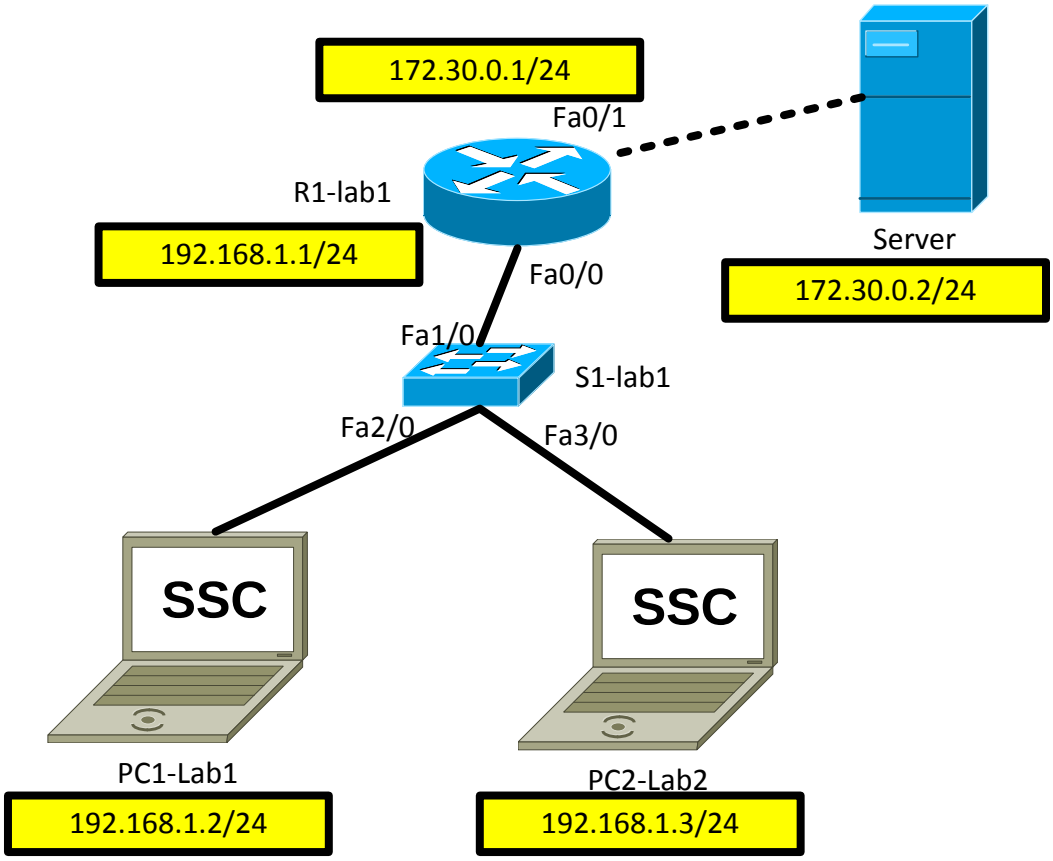

Рисунок 2 – Топология сети

Задание для выполнения лабораторной работы:

1. Войдите в привилегированный режим на маршрутизаторе.
2. Задайте имена маршрутизатору и коммутатору в соответствии с рисунком 2.
3. Настройте пароли для:

- Telnet pass “CISCO”;
- EXEC режима pass “LAB1”;
- Console “CLASS”.

4. Задайте Banner-сообщение: “Computer network. Lab1”
5. Задайте Ip-адреса на маршрутизаторах в соответствии с рисунком 2.
6. Задайте описание на портах коммутатора:

Fa1/0 – to R1;
Fa2/0 – to PC1;
Fa3/0 – to PC 2.

7. Настройте на компьютерах и сервере IP-адреса, маски подсети и шлюзы по умолчанию.
8. Просмотрите настроенную конфигурацию с помощью команды **show running-config**
9. Проверьте работоспособность сети с помощью команды ping

10. Сохраните конфигурацию на TFTP-server (название конфигурационного файла lab1)

Контрольные вопросы:

1) Какая последовательность команд задает доступ к пяти виртуальным линиям (TELNET) с паролем cisco?
2) Какая команда включает интерфейс на маршрутизаторе?
3) Для чего нужна команда **enable secret?**
4) Какая служебная утилита предназначена для определения маршрутов следования данных в сетях TCP/IP?
5) Дайте определение IOS?
6) Какие типы памяти Вы знаете?