Методические рекомендации
для проведения практического этапа
Конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» по направлению Технологии связи

Назначение конкурсных материалов

Материалы практического этапа Конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» по направлению программирование предназначены для оценки уровня практической подготовки участников конкурса.

Содержание и структура практического этапа Конкурса

Индивидуальный вариант участника Конкурса включает 1 задание. Задание заключается в сборке схемы и программировании активного сетевого оборудования

Система оценивания задания

Задание считается полностью выполненным, если соблюдены критерии оценивания, приведенные в задании. Соблюдение каждого критерия оценивается в 10 баллов. Максимальный балл за выполнение задания 60 баллов. Для получения максимального балла на практическом этапе необходимо соблюдение всех 6 критериев.

1. Учащийся должен знать:
   - Принципы работы сетевых устройств;
   - Правила ip адресации;
   - Правила разбиения сетей на подсети.
   - Порты популярных сетевых сервисов
2. Учащийся должен уметь:
   - Осуществлять базовую конфигурацию сетевых устройств;
   - Конфигурацию сетевых параметров оконечных устройств;
   - Настраивать статическую маршрутизацию;
   - Настраивать различные реализации технологии NAT;
   - Настраивать удаленное подключение по протоколам ssh и telnet;
   - Настраивать работу DHCP сервера на сетевом оборудовании;
   - Реализовывать ip адресацию в сети согласно плану.

Демонстрационный вариант
конкурсных заданий практического этапа
Конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» по направлению Технологии связи

Задание:

Собрать макет локальной вычислительной сети, настроить сетевые устройства, в том числе для возможности удаленного управления ими с персонального компьютера PC, получить доступ к сети Интернет на персональном компьютере PC.

Элементы для сборки схемы:

- Персональный компьютер (PC);
- Коммутатор Cisco 2960 или аналог;
- Маршрутизатор Cisco 2811 или аналог;
- Оборудование провайдера услуг Интернет (настраивается преподавателем, используется только для физического подключения);

  Для организации подключения к сети Интернет необходимо использовать подсеть 193.41.143.4 /30, шлюз по умолчанию 193.41.143.6. Адресация сегмента ЛВС может быть произвольной из пространства приватных IP адресов

Критерии оценивания:

№ п/п	Критерий	Максимальный балл
1	Использование всех перечисленных в задании элементов (0 – если использованы не все устройства, 10 – использованы все устройства)	10
2	Правильность сборки схемы и адресации устройств, приведение краткого описания макета (0 – если собранная схема не работоспособна, 5 – если схема работоспособна, но есть ошибки в адресации, 10 – схема работоспособна, ошибок нет)	10
3	Конфигурирование доступа для удаленного управления по протоколам telnet или SSH на маршрутизаторе (0 – не сконфигурировано или сконфигурировано но не работоспособно, 5 – сконфигурирован только протокол telnet с авторизацией по паролю, 10 – сконфигурированы оба протокола, авторизация по имени пользователя и паролю)	10
4	Конфигурирование NAT/PAT на маршрутизаторе (доступ в Интернет) (0 – не сконфигурировано или неработоспособно, 5 –	10

	сконфигурирован NAT без PAT, 10 – полная корректная конфигурация)	
5	Конфигурирование DHCP сервера на маршрутизаторе (0 - не сконфигурировано или неработоспособно, 5- работоспособно, но с ошибками, 10 –работоспособно, без ошибок)	10
6	Конфигурирование доступа для удаленного управления по протоколам telnet или SSH на коммутаторе(0 – не сконфигурировано или сконфигурировано но не работоспособно, 5 – сконфигурирован только протокол telnet с авторизацией по паролю, 10 – сконфигурированы оба протокола, авторизация по имени пользователя и паролю)	10
Итого:		60

Ответ на билет:

Схема макета ЛВС:

На рисунке 1 приведена схема соединений сетевых устройств.

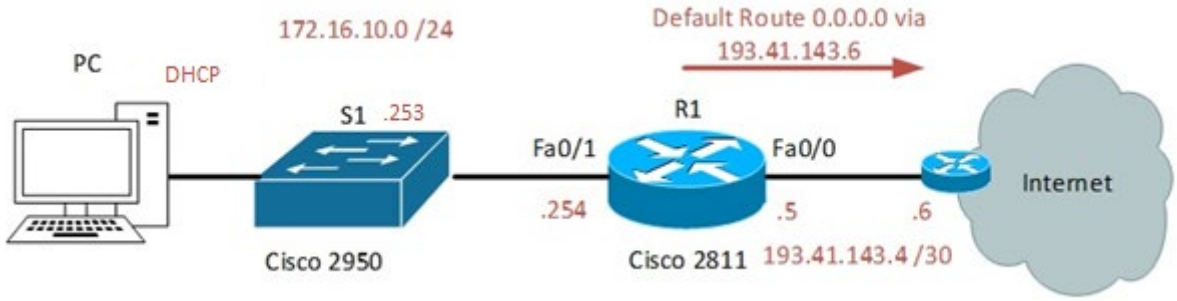

Рис. 1. Схема соединений устройств.

Краткое описание макета:

Рабочая станция пользователя PC подключается сетевым интерфейсом к коммутатору Cisco 2960 при помощи коммутационного шнура RJ45 – RJ45 категории 5e (используется произвольный порт). В свою очередь коммутатор Cisco 2960 подключен при помощи коммутационного шнура RJ45 – RJ45 категории 5e к маршрутизатору Cisco 2811 в порт FastEthernet 0/1. С провайдерским оборудованием маршрутизатор коммутируется при помощи порта FastEthernet 0/0.

Так как для выхода в сеть Интернет была выделена подсеть 193.41.143.4 /30 со шлюзом по умолчанию 193.41.143.6, на интерфейсный порт Fa 0/0 маршрутизатора 2811 назначается адрес 193.41.143.5 /30.

В сегменте локальной вычислительной сети, который находится за интерфейсным портом маршрутизатора Cisco 2811 использована адресация 172.16.10.0/24 в качестве адреса подсети. На интерфейс FastEthernet 0/1 маршрутизатора Cisco 2811 назначен адрес 172.16.10.254. Данный интерфейс является шлюзом по умолчанию для устройств в данной подсети (172.16.10.0/24).

Для доступа в сеть Интернет из сегмента локальной вычислительной сети на маршрутизаторе конфигурируется NAT трансляция адресов приватного пространства 172.16.10.0 /24 в один публичный IP адрес 193.41.143.5 с использованием PAT.

Для динамической раздачи IP адресов в подсети 172.16.10.0 /24 на маршрутизаторе Cisco 2811 конфигурируется DHCP сервер с диапазоном выдачи адресов 172.16.10.11 – 250. На компьютере PC в настройках адаптера выбирается автоматическое получение IPv4-адреса.

В качестве имени домена используется имя altair.edu. В качестве сервера имен используется публичный DNS сервер Yandex 77.88.8.1

Для возможности удаленного управления коммутатором и маршрутизатором на обеих устройствах конфигурируется удаленный доступ по протоколу telnet. При этом на коммутатор Cisco 2960 на интерфейс SVI Vlan 1 присваивается адрес 172.16.10.253. На устройствах также возможно сконфигурировать доступ по протоколу SSH.

После подключения устройств согласно предложенной топологии, их инициализации и перезагрузки, приступим к их настройке.

Шаг 1: Базовая настройка коммутатора Cisco 2811, конфигурация протокола telnet

a. Подключимся к маршрутизатору и войдем в режим глобальной конфигурации с помощью команд

```
enable
configure terminal
```

b. Настроим имя маршрутизатора и настроим IP-адресы на портах в соответствии с топологией; зададим имя домена и пароль для привилегированного режима

```
hostname R1
ip domain-name altair.edu
interface FastEthernet0/1
ip address 172.16.10.254 255.255.255.0
no shutdown
interface FastEthernet0/0
ip address 193.41.143.5 255.255.255.252
no shutdown
exit
enable password cisco
```

c. Для конфигурации доступа по telnet создадим пользователя с паролем, зададим способ подключения через линии vty и включим доступ для локальных пользователей

```
username cisco password cisco
line vty 0 4
login local
transport input telnet
exit
```

Шаг 2: Настройка доступа к R1 по протоколу SSH

a. Сгенерируем ключи шифрования для протокола SSH

```
crypto key generate rsa general-keys modulus 1024
```

b. Разрешим локальную аутентификацию не терминальных линиях. По усмотрению можно оставить возможность подключения и по telnet, и по ssh или один из этих вариантов

```
transport input all
```

Аутентификация будет производиться для пользователя, созданного в шаге 1.

Шаг 3: Конфигурация DHCP сервера

a. Исключим адреса, настраиваемые вручную, из списка DHCP

```
ip dhcp excluded-address 172.16.10.1 172.16.10.10
ip dhcp excluded-address 172.16.10.251 172.16.10.254
```

b. Настроим пул раздаваемых адресов: зададим имя, список доступных для выделения адресов, адрес шлюза по умолчанию и dns сервер

```
ip dhcp pool Altair
network 172.16.10.0 255.255.255.0
default-router 172.16.10.254
dns-server 77.88.8.1
exit
```

Шаг 4: Конфигурация доступа в Интернет с помощью NAT с PAT

a. Включим маршрутизацию и настроим статический маршрут по умолчанию для пересылки пакетов, направленных во внешнюю сеть, в интернет, через IP-адрес интерфейса роутера, выделенного провайдером

```
ip routing
ip route 0.0.0.0 0.0.0.0 193.41.143.6
```

b. Создадим лист доступа (ACL) для указания трафика, который мы будем транслировать во внешний адрес. В нашем случае это весь трафик из сети 172.16.10.0/24, при этом не забываем, что вместо обычной маски здесь используется инвертированная маска wildcard

```
ip access-list standard For_NAT
permit 172.16.10.0 0.0.0.255
exit
```

c. Настроим PAT, использовав вместо пула адресов для трансляции единственный адрес внешнего интерфейса Fa0/0. После этого включим NAT на внешнем и внутреннем портах маршрутизатора, и сохраним конфигурацию

```
ip nat inside source list For_NAT interface FastEthernet0/0 overload

interface FastEthernet0/0

ip nat outside

interface FastEthernet0/1

ip nat inside

end

copy running-config startup-config
```

Шаг 5: Базовая настройка коммутатора Cisco 2960, конфигурация протоколов telnet и SSH

a. Аналогично шагу 1 задаем базовые параметры коммутатора

```
enable

configure terminal

hostname S1

ip domain-name altair.edu

enable password cisco
```

b. Зададим адрес шлюза по умолчанию – адрес внутреннего порта коммутатора R1

```
ip default-gateway 172.16.10.254
```

c. Для обеспечения доступа по telnet, SSH зададим IP-адрес коммутатора на виртуальном интерфейсе VLAN 1, создадим локального пользователя, сгенерируем ключи SSH и включим сам доступ к коммутатору и сохраняем конфигурацию

```
interface Vlan1
ip address 172.16.10.253 255.255.255.0
no shutdown
username cisco password cisco
crypto key generate rsa general-keys modulus 1024
line vty 0 15
login local
transport input all
end
copy running-config startup-config
```

Шаг 6: Проверка адресов и подключения

a. На компьютере PC с помощью командной строки и команды *ipconfig* проверяем, получил ли компьютер адрес от DHCP сервера R1.
b. Также на компьютере с помощью команды *ping* поочередно проверяем подключение к коммутатору, интерфейсам маршрутизатора R1 и к интернету (или адресу провайдера).

Замечания, типичные ошибки

- Учащиеся должны иметь опыт работы с сетевыми устройствами, с работой в консоли, её структурой. Не обязательно наизусть помнить все команды, необходимые для выполнения заданий. Стоит обратить внимание учащихся на возможности консоли: автозаполение команд на «Tab», использование «?» для просмотра возможных аргументов команд. Таким образом, если учащийся уже был знаком с процессом конфигурации сетевых устройств по консоли и имел возможность самому настроить устройство, то он будет способен выполнить процесс конфигурации, не помня необходимых команд полностью.
- Часто встречающейся ошибкой является неактивное состояние портов. Многие учащиеся, настроив оборудование, забывают включить интерфейс командой *no shutdown*, из-за чего схема не предоставляет подключения. Наиболее удобной командой для диагностики этой проблемы является *show ip interface brief*, которая выводит адреса и состояния всех интерфейсов.
- Также значительную часть ошибок представляют собой ошибки некорректной адресации (использование неправильных IP-адресов и масок подсетей, использование обычных масок вместо wildcard масок и проч.). Поэтому стоит обратить внимание учащихся на дополнительную сверку со схемой адресации. Ошибки в использовании неверной маски (обычная-wildcard) можно также избежать, используя «?»; некоторые устройства автоматически могут транслировать обычную маску в wildcard, но далеко не все.