Данная работа посвящена разработке и настройке сети передачи данных на основе заданных исходных параметров. В рамках задания требуется спроектировать и настроить корпоративную IP-сеть с использованием стека протоколов TCP/IP.

Сеть должна включать 12 подсетей, что обеспечит локализацию трафика и контроль доступа пользователей к сетевым ресурсам. Кроме того, необходимо предоставить пользователям доступ к внутренним серверам компании и внешним сетям (Интернет).

Исходные данные для выполнения работы указаны в таблице 1. Они основаны на варианте задания, определяемом последней цифрой студенческого билета (вариант 48) и годом обучения (2024).

Таблица 1 – Исходные данные

Внешний IP-адрес	Кол-во VLAN	Адрес сети	VLAN (маршрутизация)
85.76.0.0	12	Ex	5,10 и 2,8

1 Построение схемы проектируемой сети

Построение схемы сети будем осуществлять в соответствии с исходными данными указанными в методических указаниях. Для построения схемы проектируемой сети будем использовать программное обеспечение Cisco Packet Tracer.

Для того, чтобы обеспечить возможность разделения разрабатываемой сети на подсети в качестве центрального сетевого устройства корпоративной сети будем использовать коммутатор уровня L3 Cisco 3560, имеющий 24 внутренних LAN-портов Fast Ethernet и 2 внешних WAN-порта Gigabit Ethernet.

Так как в соответствии с исходными данными необходимо организовать 4 Vlan, то необходимо будет организовать аналогичное количество подсетей, в каждой из которых необходимо обеспечить услугами передачи данных необходимое число пользователей. Оборудование каждого Vlan будет подключен к каждому из 4 LAN-портов Cisco 3560. Ещё два порта будут необходимы для подключения файловых серверов компании. Один порт потребуется для подключения к внешней сети.

Для объединения пользователей каждой подсети будем использовать коммутатор уровня L2. В качестве такого коммутатора будем использовать Cisco 2960-24, оснащенный 24-ю портами Fast Ethernet.

К портам коммутатора подключается оконечное оборудование пользователей.

В нашем случае таким оборудованием будут компьютеры.

Сформированная сеть компании будет подключена через ряд маршрутизаторов к удалённому офису компании. Он организован на Cisco 2960-24. К нему будут подключены сервер и компьютер.

Исходя из рассмотренных рассуждений схема сети принимает вид, показанный на рисунке 1.3. Для упрощения на рисунке в каждой подсети показано только по два компьютера. расположенные на рабочих местах сотрудников компании.

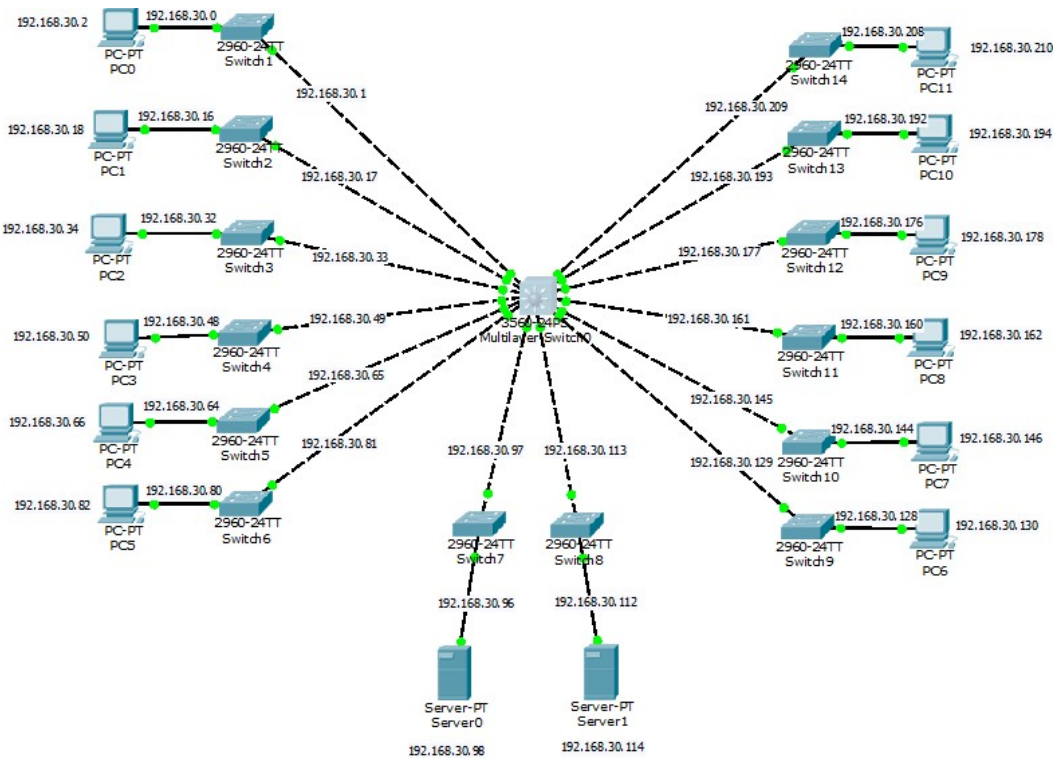

Рисунок 1.3 – Схема сети

2 Разделение сети на подсети, разделение адресного пространства

Для разделения сети на подсети будет использоваться коммутатор уровня L3 Cisco 3560, каждый из задействованных портов которого должен входить в различные подсети. Для этого каждому из портов должен быть присвоен IP-адрес, принадлежащий соответствующей подсети. Таким образом, необходимо разделить внутреннее адресное пространство между подсетями.

Для разделения адресного пространства будем использовать технологию маски переменной длины (VLSM – Variable-Length Subnet Mask). Маской называется число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность. Соответственно, с помощью маски в адресе можно выделить произвольное количество разрядов для номера сети, что частично устраняет перечисленные выше недостатки.

С учетом исходных данных на курсовую работу сеть имеет адрес класса C 192.168.30.0, соответственно, маска имеет значение 255.255.255.0. Это означает, что первые 3 байта адреса (192.168.30) относятся к адресу сети, а последний байт (0) – к адресу конечного узла в пределах этой сети. Для разделения на подсети из последнего байта необходимо «занять» дополнительные разряды, которые будут относиться к адресу подсети. В нашем случае количество подсетей составляет 14, следовательно, для подсетей необходимо «занять» 4 разряда, что даст возможность организации $2^4 = 16$ подсетей. Тогда значение маски должно быть увеличено на 4 единицы, и маска в двоичной форме примет вид:

11111111.11111111.11111111.11110000

или в десятичной форме

255.255.255.240.

С учетом этого адреса подсетей будут иметь следующий вид:

Подсеть 1:

11000000.10101000.00011110.00000000– двоичная форма;

192.168.30.0 – двоично-десятичная форма.

Подсеть 2:

11000000.10101000.00011110.00010000– двоичная форма;

192.168.30.16 – двоично-десятичная форма.

Подсеть 3:

11000000.10101000.00011110.00100000 – двоичная форма;

192.168.30.32 – двоично-десятичная форма.

Подсеть 4:

11000000.10101000.00011110.00110000 – двоичная форма;

192.168.30.48 – двоично-десятичная форма.

Подсеть 5:

11000000.10101000.00011110.01000000 – двоичная форма;

192.168.30.64 – двоично-десятичная форма.

Подсеть 6:

11000000.10101000.00011110.01010000 – двоичная форма;

192.168.30.80 – двоично-десятичная форма.

Подсеть 7:

11000000.10101000.00011110.01100000 – двоичная форма;

192.168.30.96 – двоично-десятичная форма.

Подсеть 8:

11000000.10101000.00011110.01110000 – двоичная форма;

192.168.30.112 – двоично-десятичная форма.

Подсеть 9:

11000000.10101000.00011110.10000000 – двоичная форма;

192.168.30.128 – двоично-десятичная форма.

Подсеть 10:

11000000.10101000.00011110.10010000 – двоичная форма;

192.168.30.144 – двоично-десятичная форма.

Подсеть 11:

11000000.10101000.00011110.10100000 – двоичная форма;

192.168.30.160 – двоично-десятичная форма.

Подсеть 12:

11000000.10101000.00011110.10110000 – двоичная форма;

192.168.30.176 – двоично-десятичная форма.

Подсеть 13:

11000000.10101000.00011110.11000000 – двоичная форма;

192.168.30.192 – двоично-десятичная форма.

Подсеть 14:

11000000.10101000.00011110.11010000 – двоичная форма;

192.168.30.208 – двоично-десятичная форма.

Оставшиеся диапазоны адресного пространства будут запасом на развитие сети. Таким образом, произведено разделение адресного пространства между подсетями. При дальнейшем конфигурировании сетевых устройств интерфейсам необходимо присваивать IP-адреса в соответствии с произведенным разделением.

3 Конфигурирование коммутаторов имаршрутизаторов проектируемой сети

Конфигурирование сети начнём с сети компании. Так как в качестве маршрутизатора было принято использовать коммутатор уровня L3 Cisco 3560, произведем сначала его конфигурирование.

Так как в проектируемой сети используется только статическая маршрутизация, и все подсети соединены непосредственно с интерфейсами Cisco 3560, конфигурирование заключается только в назначении интерфейсам IP-адресов.

При настройке оборудования Cisco, необходимо знать, что существует 3 типа доступа к устройству.

Первый режим – непривилегированный (EXEC). В данном режиме нельзя изменять конфигурацию устройства, но можно просмотреть некоторые его характеристики. Присутствие в данном режиме в консоли обозначается значком «>».

Второй режим – привилегированный режим (privilage EXEC). В данном режиме пользователь может просматривать информацию об устройстве, его конфигурацию, сохранять текущую конфигурацию, но не может ее изменять. В данный режим можно перейти из непривилегированного режима путем выполнения команды enable.Присутствие в данном режиме в консоли обозначается значком «#». Например, в данном режиме можно выполнить команду showrunning-config, выводящую текущую рабочую конфигурацию устройства.

Третий режим – режим глобального конфигурирования. В данном режиме нельзя просмотреть информацию об устройстве и его конфигурации, но зато можно ее изменять. Для перехода в режим конфигурации необходимо в привилегированном режиме выполнить команду configterminal.Присутствие в

данном режиме в консоли обозначается значком «(config)#».

Для назначения IP-адреса определенному интерфейсу необходимо из режима глобального конфигурирования перейти в режим конфигурирования конкретного интерфейса. Данный переход осуществляется командой interface

<протокол> <номер интерфейса>.

Назначение IP-адреса производится командой ip address <адрес> <маска>.

Кроме того, при использовании коммутаторов уровня 3 IP-адреса могут быть присвоены не интерфейсам, а виртуальным частным сетям (VLAN). Поэтому в нашем случае на Cisco 3560 необходимо настроить 4 VLAN, привязать к каждой из VLAN по одному интерфейсу, и лишь затем присвоить им IP-адреса.

При настройке VLAN используются следующие команды: Switch(config)#vlan N – создание VLAN N;

Switch(config-vlan)#name <имя> – присвоение имени VLAN. Привязка интерфейса к VLAN осуществляется командой

Switch(config-if)#switchport access vlan 2 – присвоение заданного интерфейса какой-либо VLAN (в данном случае VLAN 2).

Произведем конфигурирование Cisco 3560 с использованием указанных команд и с учетом произведенного в предыдущем разделе разделения адресного пространства.

Просмотр созданных виртуальных частных сетей производится с использованием команды show vlan brief, рисунок 3.1.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    v2                               active    Fa0/1
3    v3                               active    Fa0/2
4    v4                               active    Fa0/3
5    v5                               active    Fa0/4
6    v6                               active    Fa0/5
7    v7                               active    Fa0/6
8    v8                               active    Fa0/7
9    v9                               active    Fa0/8
10   v10                              active    Fa0/9
11   v11                              active    Fa0/10
12   v12                              active    Fa0/11
13   v13                              active    Fa0/12
14   v14                              active    Fa0/13
15   v15                              active    Fa0/14
1002 fddi-default                     active
1003 token-ring-default               active
```

Рисунок 3.1 – Просмотр созданных VLAN

Завершив настройку интерфейсов коммутатора L3, произведем проверку с помощью команды show ip route. На рисунке 3.2 представлена таблица маршрутизации.

```
Switch#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.30.0/28 is subnetted, 14 subnets
C       192.168.30.0 is directly connected, Vlan2
C       192.168.30.16 is directly connected, Vlan3
C       192.168.30.32 is directly connected, Vlan4
C       192.168.30.48 is directly connected, Vlan5
C       192.168.30.64 is directly connected, Vlan6
C       192.168.30.80 is directly connected, Vlan7
C       192.168.30.96 is directly connected, Vlan8
C       192.168.30.112 is directly connected, Vlan9
C       192.168.30.128 is directly connected, Vlan10
C       192.168.30.144 is directly connected, Vlan11
C       192.168.30.160 is directly connected, Vlan12
C       192.168.30.176 is directly connected, Vlan13
C       192.168.30.192 is directly connected, Vlan14
C       192.168.30.208 is directly connected, Vlan15
```

Рисунок 3.2 – Таблица маршрутизации

Настройка коммутаторов второго уровня. Так как интерфейсам этих коммутаторов не нужно присваивать IP-адреса, можно ограничиться только настройкой виртуальных локальных сетей VLAN. Например, в подсети 2 интерфейсы коммутатора должны быть привязаны к vlan 2 с именем VLAN002. Конфигурирование коммутатора второй подсети иллюстрируется рисунком 3.3.

```
Switch#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/1, Gig1/2
2    VLAN0002                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.3 – Настройка коммутатора подсети

Для всех остальных коммутаторов находящихся в сети компании произведём аналогичные настройки. При этом, будем помнить, что на каждом коммутаторе разрешается прохождения трафика только своей Vlan.

Для проверки правильности проведенных настроек используем утилиту ping. Для этого присвоим рабочим станциям двух различных подсетей IP-адреса, и проверим возможность связи этих станций между собой.

Для рабочих станций в подсети 2 присвоим диапазон адресов 192.168.30.0 – 15. Аналогично для других сетей:

Для сокращения записей в каждой подсети поставим по одному компьютеру, и на его примере будем показывать настройки.

Для каждого компьютера подсети необходимо указать маршрут по умолчанию. В качестве них, будем указывать адрес интерфейсов коммутатора L3 к которому подключена та или иная подсеть.

Результаты настройки представлены на рисунке 3.4.

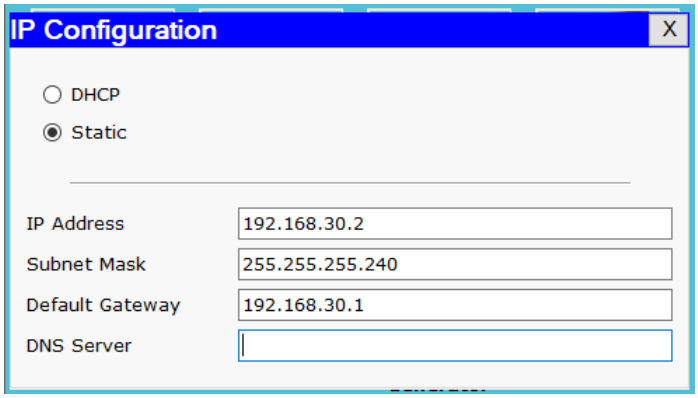

Рисунок 3.4 – Результаты настройки компьютеров

Полученные после выполнения утилиты ping результаты представлены на рисунке 3.5.

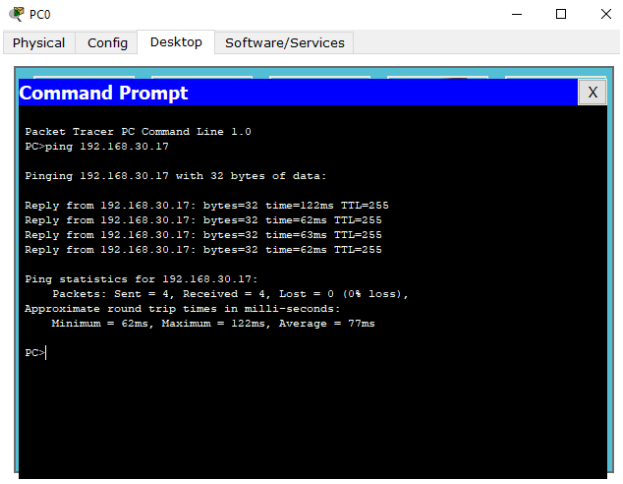

Рисунок 3.5 – Результат выполнения утилиты ping

Из рисунка следует, что все настройки произведены правильно, и пакеты

успешно передаются между двумя подсетями. Аналогичная проверка проведена и с остальными подсетями.

4 Настройка маршрутизации междуподсетями

В сети компании оконечные узлы всех подсетей могут обмениваться информацией друг с другом. Однако на практике чаще всего трафик различных подсетей должен быть изолирован друг от друга. В соответствии с исходными данными на проектирование, данными могут обмениваться только подсеть 4 (Vlan 5) с подсетью 9 (Vlan 10), а также подсеть 1 (Vlan 2) с подсетью 7 (Vlan 8), трафик остальных подсетей должен быть изолирован друг от друга.

Для разграничения трафика между Vlan будем использовать возможность настройки списков доступа Access List (ACL).

В общем случае, для принятия решения о пропуске в IP-пакете анализируется только адрес источника сообщения, чтобы принять решение о фильтрации или продвижении пакета далее по сети. Список доступа производит фильтрацию пакетов по порядку, поэтому в строках списков следует задавать условия фильтрации, начиная от специфических условий и заканчивая общими. Условия списка доступа обрабатываются последовательно от вершины списка к основанию, пока не будет найдено соответствующее условие.

Если никакое условие не найдено, тогда пакет отклоняется и уничтожается, поскольку неявное условие deny any (запретить все остальное) есть неявно в конце любого списка доступа. Не удовлетворяющий списку доступа пакет протокола IP будет отклонен и уничтожен, при этом отправителю будет послано сообщение ICMP. Каждая новая запись (линии) всегда будет добавляться в конец списка доступа.

Для того, чтобы создать список доступа необходимо выполнить следующие действия:

- создать список доступа в режиме глобального конфигурирования устройства;

- привязать созданный список доступа к интерфейсу в режиме детального

конфигурирования интерфейса.

Формат команды создания стандартного списка доступа следующий: Router(config)#access-list {№} {permit или deny} {адрес источника}.

Списки доступа могут фильтровать как трафик, входящий в маршрутизатор (in), так и трафик, исходящий из маршрутизатора (out). Направление трафика указывается при привязке списка доступа к интерфейсу. Формат команды привязки списка к интерфейсу следующий:

Router(config-if)#{протокол} access-group {номер} {in или out}

После привязки списка доступа его содержимое не может быть изменено. Не удовлетворяющий администратора список доступа должен быть удален командой no access-list и затем создан заново.

Для рассматриваемой сети необходимо установить стандартный ACL на порт fa0/4 и fa0/9 коммутатора L3, разрешающий продвижение пакетов в подсети 192.168.30.48 и 192.168.20.128. Таким образом, задаётся возможность ограничить общение только оборудования подсети 4 (Vlan 5) и подсети 9 (Vlan 10), а также создать возможность обращения к необходимым серверам.

Также необходимо на порт fa0/1 и fa0/7 коммутатора L3, разрешающий продвижение пакетов в подсети 192.168.20.0 и 192.168.20.96. Таким образом, задаётся возможность ограничить общение только оборудования подсети 1 (Vlan 2) и подсети 7 (Vlan 8), а также создать возможность обращения к необходимым серверам.

В списке доступа имеются адреса сети, а не отдельного узла, поэтому необходимо использовать маску. Нулевые значения маски означают требование обработки соответствующих разрядов адреса, а единичные – игнорирование соответствующих разрядов адреса при функционировании списка доступа.

Таким образом, маска 0.0.0.0 предписывает анализ и обработку всех разрядов адреса, т.е. в этом случае будет обрабатываться адрес каждого узла. Маска

0.0.0.255 показывает, что обрабатываться будет только сетевая часть

адреса класса С.

Таким образом, для решения задачи необходимо в маршрутизаторе прописать следующие команды:

Switch(config)#access-list <номер> permit <адрес сети> <обратная маска >
Switch (config)#int vlan <номер влан>

Switch (config-if)#ip access-group <номер списка> out Результаты настройки представлены на рисунке 4.1.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list 2 permit 192.168.30.48
Switch(config)#access-list 2 permit 192.168.30.128
Switch(config)#access-list 2 permit 192.168.30.96
Switch(config)#access-list 2 permit 192.168.30.112
Switch(config)#access-list 3 permit 192.168.30.0
Switch(config)#access-list 3 permit 192.168.30.96
Switch(config)#access-list 3 permit 192.168.30.112
Switch(config)#
Switch(config)#int vlan 5
Switch(config-if)#ip access-group 2 out
Switch(config-if)#int vlan 10
Switch(config-if)#ip access-group 2 out
Switch(config-if)#int vlan 2
Switch(config-if)#ip access-group 3 out
Switch(config-if)#int vlan 8
Switch(config-if)#ip access-group 3 out
```

Рисунок 4.1 – Результаты настройки листов доступа

Просмотреть созданные списки можно с помощью команды show access-list. Для того, чтобы обеспечить доступ Vlan 2, 5, 8, 10 к серверам, добавим их в ACL. Произведём настройку списков доступа необходимым образом, с учётом ранее указанного подхода. После полной настройки листов доступа получим список показанный на рисунке 4.2.

```
show acc
Standard IP access list 2
    permit host 192.168.30.48
    permit host 192.168.30.128
    permit host 192.168.30.96
    permit host 192.168.30.112
Standard IP access list 3
    permit host 192.168.30.0
    permit host 192.168.30.96
    permit host 192.168.30.112
Switch#
```

Рисунок 4.2 – Результаты составления списков доступа

5 Настройка службы динамической маршрутизации DHCP

Протокол DHCP — это протокол клиента или сервера, который автоматически предоставляет узел протокола IP с его IP-адресом и другие связанные сведения о конфигурации, такие как маска подсети и шлюз по умолчанию.

Для настройки DHCP на Коммутаторе L3 воспользуемся командами:

ip dhcp excluded-address 192.168.30.0 – исключение ip из пула адресов;

ip dhcp pool vlan2 – настройка пула адресов для vlan2;

default-router 192.168.30.1 – настройка DG для DHCP vlan2;

network 192.168.30.0 255.255.255.240 – сеть и маска для DHCP;

dns-server 192.168.30.144 – ДНС сервер;

do wr – запись настроек.

На рисунке 5.1 показан сконфигурированный DHCP.

```
ip dhcp pool vlan2
 network 192.168.30.0 255.255.255.240
 default-router 192.168.30.1
 dns-server 192.168.30.114
ip dhcp pool vlan3
 network 192.168.30.16 255.255.255.240
 default-router 192.168.30.17
 dns-server 192.168.30.114
ip dhcp pool vlan4
 network 192.168.30.32 255.255.255.240
 default-router 192.168.30.33
 dns-server 192.168.30.114
ip dhcp pool vlan5
 network 192.168.30.48 255.255.255.240
 default-router 192.168.30.49
 dns-server 192.168.30.114
ip dhcp pool vlan6
 network 192.168.30.64 255.255.255.240
 default-router 192.168.30.65
 dns-server 192.168.30.114
ip dhcp pool vlan7
 network 192.168.30.80 255.255.255.240
 default-router 192.168.30.81
 dns-server 192.168.30.114
ip dhcp pool vlan8
 network 192.168.30.96 255.255.255.240
 default-router 192.168.30.97
 dns-server 192.168.30.114
ip dhcp pool vlan10
 network 192.168.30.128 255.255.255.240
 default-router 192.168.30.129
 dns-server 192.168.30.114
ip dhcp pool vlan11
 network 192.168.30.144 255.255.255.240
 default-router 192.168.30.145
 dns-server 192.168.30.114
ip dhcp pool vlan12
 network 192.168.30.160 255.255.255.240
 default-router 192.168.30.161
 dns-server 192.168.30.114
ip dhcp pool vlan13
 network 192.168.30.176 255.255.255.240
 default-router 192.168.30.177
 dns-server 192.168.30.114
ip dhcp pool vlan14
 network 192.168.30.192 255.255.255.240
 default-router 192.168.30.193
 dns-server 192.168.30.114
ip dhcp pool vlan15
 network 192.168.30.208 255.255.255.240
 default-router 192.168.30.209
 dns-server 192.168.30.114
ip routing
```

Рисунок 5.1 – Конфигурация DHCP для чётных подсетей

Далее необходимо на компьютерах отключить статический IP, который был настроен раннее, и включить службу DHCP. Если полученный адрес и маска соответствуют сегменту сети – настройка произведена успешно.

Настроенный DHCP на компьютере 1 показан на рисунке 5.2.

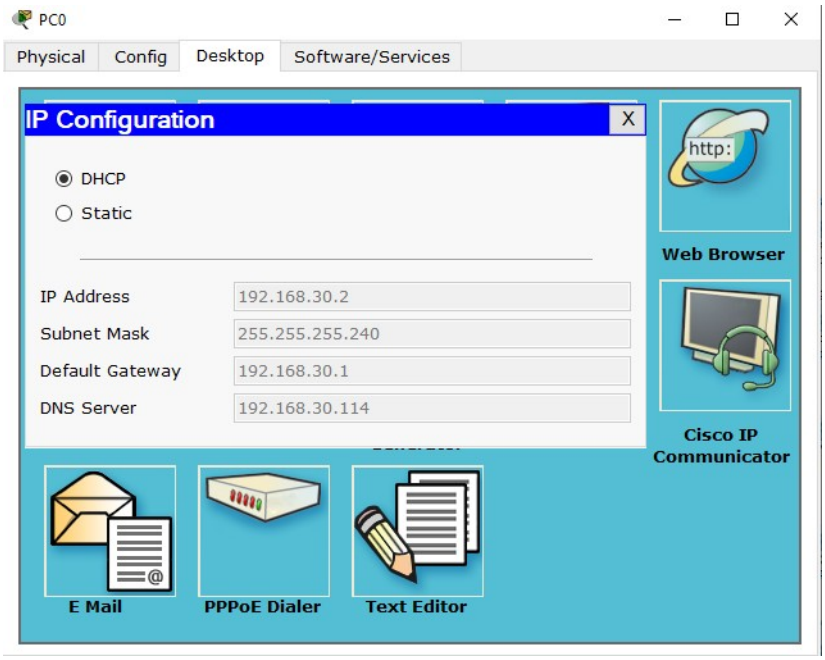

Рисунок 5.2 - Настроенный DHCP на компьютере 1

Аналогично необходимо включить службу DHCP на оставшихся компьютерах.

6 Настройка подключения оборудования удалённого офиса

Для подключения оборудования удалённого офиса подключаемого через сеть Internet потребуется произвести настройку подключения к глобальной сети и настроить сеть компании таким образом, чтобы обеспечить доступ компьютеров сети к удалённому серверу и удалённых компьютеров ко всем устройствам сети.

Для решения этой задачи установим маршрутизатор (который будет имитировать часть сети Internet) и оборудование удалённого офиса. Полученная схема сети показана на рисунке 6.1.

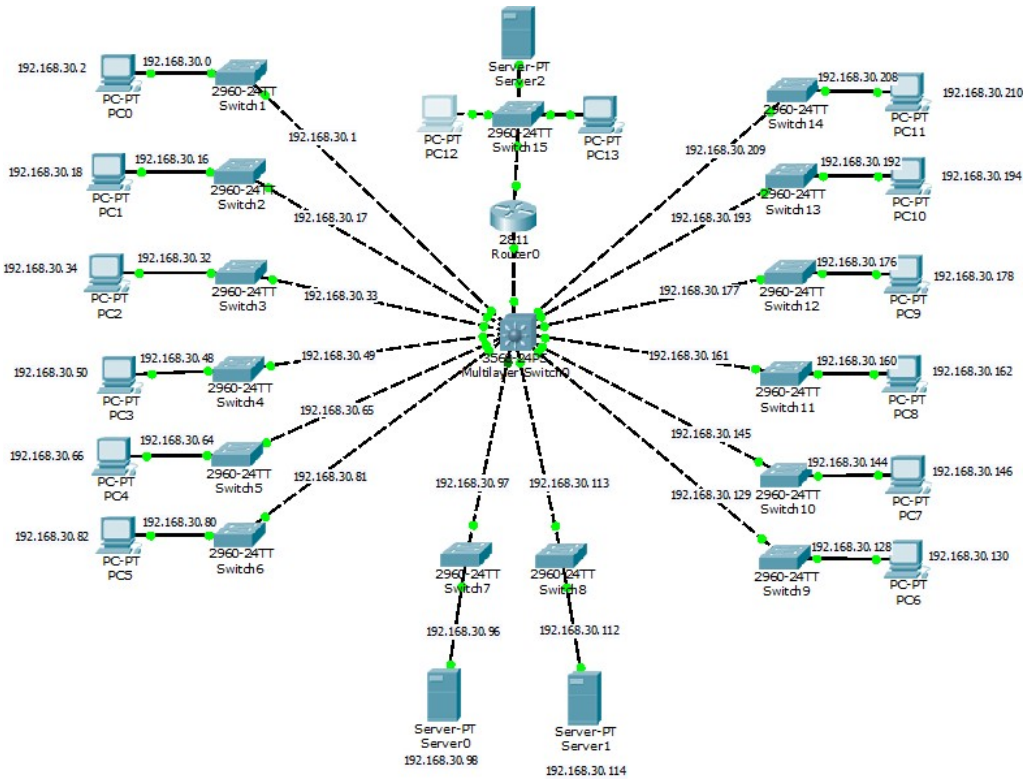

Рисунок 6.1 – Окончательная схема сети

Для присвоения адресации воспользуемся исходными данными для выполнения работы. Так внешняя сеть будет подключаться по интерфейсу с адресом сети 85.76.0.0

Всё оборудование удалённой сети будет находиться в сети с адресом 192.130.30.0.

Для установленных компьютеров и сервера необходимо установить их адреса, маску сети, адрес маршрута по умолчанию. Порядок установки аналогичен тем операциям, которые производились для компьютеров сети компании.

Изначально порты маршрутизатора будут отключены. Исходя из этого, сначала рассмотрим настройку маршрутизатора.

Для этого

На маршрутизаторе для начала необходимо включить интерфейс, к которому подключен коммутатор. Общий синтаксис команд:

Router>enable Router#configure terminal

Router(config)#interface fastEthernet <номерпорта>

Router(config-if)#ip address <IP-адрес> <маска>

Router(config-if)#no shutdown

Router(config-if)#ex

Команды вводятся для каждого порта.

Произведем настройки Vlan и статической маршрутизации на коммутаторе L3, а также настройки статической маршрутизации на роутере удаленного доступа.

Результаты представлены на рисунке 6.2, 6.3, 6.4.

```
interface FastEthernet0/15
 switchport access vlan 16
!
interface Vlan16
 ip address 85.76.0.1 255.0.0.0
 ip access-group 2 out
!
```

Рисунок 6.2 – Настройки VLAN на коммутаторе L3

```
!
interface FastEthernet0/0
 ip address 85.76.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.130.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.130.30.0 255.255.255.0 85.76.0.1
ip route 192.168.30.0 255.255.255.0 85.76.0.1
!
```

Рисунок 6.3 – Настройки на роутере удаленного доступа

```
ip classless
ip route 192.130.30.0 255.255.255.0 85.76.0.2
!
```

Рисунок 6.4 – Настройки маршрутизации на коммутаторе L3

Аналогичные настройки маршрутизации необходимо произвести у коммутатора второго уровня. Синтаксис команд остаётся тем же. Просмотреть произведённые настройки можно с помощью команды show ip rout. Результат представлен на рисунке 6.5

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    85.0.0.0/8 is directly connected, Vlan16
S    192.130.30.0/24 [1/0] via 85.76.0.2
     192.168.30.0/28 is subnetted, 14 subnets
C       192.168.30.0 is directly connected, Vlan2
C       192.168.30.16 is directly connected, Vlan3
C       192.168.30.32 is directly connected, Vlan4
C       192.168.30.48 is directly connected, Vlan5
C       192.168.30.64 is directly connected, Vlan6
C       192.168.30.80 is directly connected, Vlan7
C       192.168.30.96 is directly connected, Vlan8
C       192.168.30.112 is directly connected, Vlan9
C       192.168.30.128 is directly connected, Vlan10
C       192.168.30.144 is directly connected, Vlan11
C       192.168.30.160 is directly connected, Vlan12
C       192.168.30.176 is directly connected, Vlan13
C       192.168.30.192 is directly connected, Vlan14
C       192.168.30.208 is directly connected, Vlan15
```

Рисунок 6.5 – Таблица маршрутизации коммутатора L3

Для того, чтобы трафик мог продвигаться по необходимым Vlan произведём дополнения к уже сформированным спискам доступа. Смысл дополнений будет таковым, что необходимо разрешить передачу трафика в ранее описанных направлениях. Синтаксис команд аналогичен выполняемому ранее. Результаты настройки представлены на рисунке 6.6.

```
Standard IP access list 2
    permit host 192.168.30.48
    permit host 192.168.30.128
    permit host 192.168.30.96
    permit host 192.130.30.2
    permit host 192.130.30.3
    permit host 192.130.30.4
Standard IP access list 3
    permit host 192.168.30.0
    permit host 192.168.30.96
    permit host 192.168.30.112
    permit host 192.130.30.2
    permit host 192.130.30.3
    permit host 192.130.30.4
```

Рисунок 6.6 – Таблица маршрутизации маршрутизатора и список доступа коммутатора L3

Проверим доступность устройств с помощью команды ping. Результат представлен на рисунке 6.7.

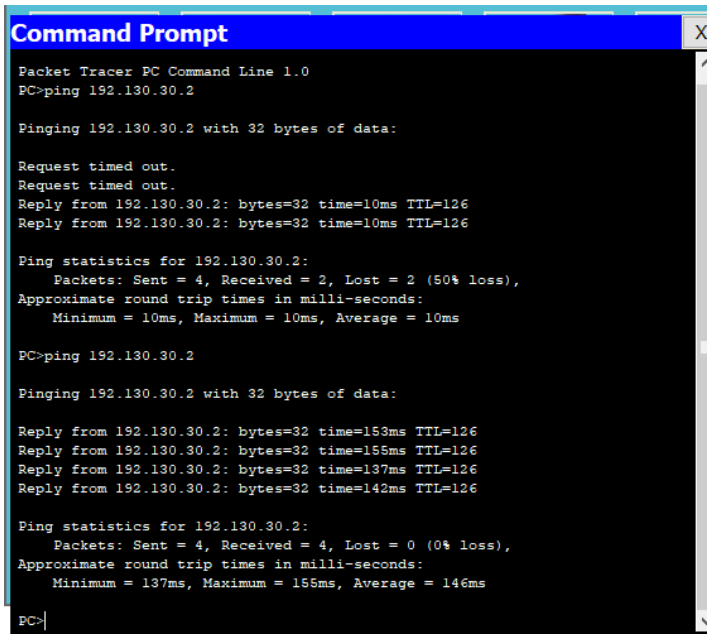

Рисунок 6.7 –Доступность проектируемой

Таким образом, необходимые настройки выполнены. Проверка доступности устройств показала правильность произведённых настроек.