Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Аппаратное обеспечение компьютерных сетей

ОТЧЕТ

по лабораторной работе № 2

ВАРИАНТ № 814

Студенты: А.В. Гуринович

Проверил: И.И. Глецевич

МИНСК 2022

**СОДЕРЖАНИЕ**

[1 ЗАДАНИЕ 2](#_Toc117905707)

[2 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ 3](#_Toc117905708)

[2.1 Выбор из маршрутизатора и L3-коммутатора 3](#_Toc117905709)

[2.2 VTP 3](#_Toc117905710)

[2.3 Агрегация каналов 3](#_Toc117905711)

[2.4 Port Security 4](#_Toc117905712)

[3 ХОД РАБОТЫ 5](#_Toc117905713)

[3.1 Выбор Root 5](#_Toc117905714)

[3.2 Настройка агрегации каналов 5](#_Toc117905715)

[3.3 Настройка виланов 5](#_Toc117905716)

[3.3.1 Настройка VTP 5](#_Toc117905717)

[3.3.2 Создание виланов 5](#_Toc117905718)

[3.3.3 Настройка портов 6](#_Toc117905719)

[3.4 PVST 6](#_Toc117905720)

[3.4.1 Назначение Root корневым мостом 6](#_Toc117905721)

[3.4.2 Настройка PortFast 6](#_Toc117905722)

[3.4.3 Настройка BPDU Guard 6](#_Toc117905723)

[3.4.4 Проверка работоспособности PVST+ 7](#_Toc117905724)

[3.5 Настройка маршрутизации 7](#_Toc117905725)

[3.6 Настойка SSH 7](#_Toc117905726)

[3.7 Последний шаг 8](#_Toc117905727)

[4 РАБОЧИЕ КОФИГУРАЦИИ 9](#_Toc117905728)

[4.1 N1 9](#_Toc117905729)

[4.2 N2 10](#_Toc117905730)

[3.3 N3 11](#_Toc117905731)

[4.4 N4 12](#_Toc117905732)

[4.5 N5 13](#_Toc117905733)

[4.6 N6 14](#_Toc117905734)

[4.7 N7 15](#_Toc117905735)

[4.8 N8 16](#_Toc117905736)

[4.9 PC1 16](#_Toc117905737)

[4.10 PC2 17](#_Toc117905738)

[4.11 PC3 17](#_Toc117905739)

[4.12 Laptop1 17](#_Toc117905740)

[4.13 Laptop2 18](#_Toc117905741)

[4.14 Laptop3 18](#_Toc117905742)

# 1 ЗАДАНИЕ

1. Взять за основу лабораторную работу No1. Использовать Cisco Packet Tracer.

2. Изучить команды: vlan, switchport mode, switchport access, switchport trunk, vtp, show vlan, show vtp. Изучить как хранится информация о виланах.

3.Среди коммутаторов выбрать один -- Root. Дополнительно подключить к Root маршрутизатор либо заменить Root -- коммутатор заменить L3-коммутатором. В качестве маршрутизатора использовать 2811, 2901 либо 4331; в качестве L3-коммутатора использовать 3560 либо 3650. Учесть топологию и следующие пункты задания. Маршрутизатор можно подключить посредством более чем одного канала.

4. Реализовать концепцию виланов 802.1Q. Можно с помощью VTP. Одну из станций включить в административный вилан для управления всеми устройствами-посредниками. Оставшиеся станции распределить между двумя пользовательскими виланами, так чтобы к каждому из крайних коммутаторов были подключены станции из обоих виланов. Предусмотреть вилан для оригинально трафика (native) с идентификатором, отличным от идентификатора по умолчанию. Запретить передачу по транкам пакетов из неизвестных виланов. Использовать CLI.

5. Изучить команды: speed, duplex, mdix, channel-group, interface port-channel, show etherchannel.

6.Соединить Root с каждым из соседних коммутаторов минимум двумя физическими каналами. Настроить статическую либо динамическую агрегацию каналов. Параметры задействованных физических соединений (скорость и режим) задать вручную. Использовать CLI.

7. Изучить команды: spanning-tree vlan, spanning-tree portfast, spanning-tree bpduguard, show spanning-tree.

8. Убедиться в работоспособности PVST+. В каждом из виланов Root принудительно назначить корневым мостом. Использовать PortFast и BPDU Guard. Использовать CLI.

9.Изучить команды для создания SVI и подинтерфейсов (на маршрутизаторе), команду encapsulation dot1q (на маршрутизаторе).

10.Настроить маршрутизацию между виланами и тем самым обеспечить достижимость всех сетевых интерфейсов. Для адресации в виланах использовать соответствующее количество подсетей из указанных в варианте задания. Использовать CLI (коммутаторы, маршрутизатор) и графический интерфейс (ПК, ноутбуки).

11. Изучить команду switchport port-security.

12. С помощью Port Security защитить физический порт, к которому подключена станция для администрирования, от несанкционированного доступа (по своему усмотрению). Административно выключить все незадействованные порты коммутаторов. Использовать CLI. Подумать о том, как можно защитить административный вилан.

# 2 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## 2.1 Выбор из маршрутизатора и L3-коммутатора

Для осуществления IP-маршрутизации выбран L3-коммутатор. Причинами этого послужили – отсутствие необходимости в подключении внешних связей в топологию, отсутствие необходимости в функциях доступных только в маршрутизаторах, таких как VPN, NAT и иных.

Использование L3-коммутатора, который устанавливается вместо L2-коммутатора, а не установка маршрутизатора «на палочке», подключённого только к одному коммутатору, позволяет подключить к осуществляющему маршрутизацию устройству сразу несколько коммутаторов, то есть трафик проходит через большее количество каналов, увеличивается пропускная способность. Такое решение сократит количество переходов между коммутаторами для маршрутизации, в случае установки маршрутизатора «на палочке», коммутатор, к которому он был бы подключён столкнулся с большим количеством транзитного трафика.

## 2.2 VTP

Для обмена информацией о виланах между коммутаторами используется VLAN Trunking Protocol. Протокол позволяет централизованно управлять виланами, то есть вилан, созданный на коммутаторе в режиме VTP-сервера, автоматически будет добавлен и на всех остальных коммутаторах, которые работаю в режиме VTP-клиента. Удаление вилана на VTP-сервере приведёт также к его автоматическому удалению на всех VTP-клиентах.

При выполнении лабораторной работы виланам были присвоены названия, которые позволяют понять назначение вилана прямо на коммутаторе, названия также автоматически переносятся.

Таким образом, настройка VTP-клиента и -сервера является менее затратой с точки зрения общего количества команд: требуется выполнение только трёх команд на каждом коммутаторе, после чего информация о виланах заносится только в VTP-сервер.

## 2.3 Агрегация каналов

Агрегация каналов позволяет увеличить пропускную способность соединения между коммутаторами. Согласно заданию, агрегированные каналы должны быть организована на соединении Root с каждым соседним коммутатором.

Root имеет три соседних коммутатора: N1, N4 и N6 – каждый из которых не является конечным. Рассматривая соединение с всеми соседними коммутаторами можно сделать вывод, что создание более двух физических каналов не имеет смысла, так как к каждому из соседних коммутаторов подключено только два других коммутатора, эти коммутаторы подключены одним физическим каналом. То есть продолжение сети от соседних с Root коммутаторов не может создать трафик на более чем два физических канала.

Если бы к соседним к Root коммутаторам были подключены пользовательские станции или более двух коммутаторов с одними физическим соединением, то создание более двух физических каналов между Root и соседом имело бы смысл.

## 2.4 Port Security

Защита с помощью Port Security обеспечена на соединяющих коммутаторы N3 и N5 со станциями портах, каждому из них в Port Security присвоен единственный разрешённый статический MAC-адрес, который соответствует MAC-адресу порта станции. Режимом реагирования на нарушение назначен shutdown.

Таким образом доступ в сеть через конкретный порт может получить только один соответствующий этому порту компьютер. К примеру, если рассматривать коммутатор N5 и станции Laptop1 и Laptop2, если поменять ноутбуки местами, то есть подключить Laptop1 к порту коммутатора Fa0/2 и Laptop2 к порту коммутатора Fa0/1, то оба порта будут сразу же перейдут в состояние error-disabled, так как MAC-адрес станций не будет включён в список разрешённых на соответствующих портах.

Данная реализация имеет недостаток: даже в случае смены станций, которые предназначены для подключения к одному и тому же вилану, необходимо будет перенастраивать Port Security на соответствующих портах.

# 3 ХОД РАБОТЫ

Это не нужно писать в отчёте, это только для вас, котики-собачки...

## 3.1 Выбор Root

Root-коммутатором выбран коммутатор N2, который максимально равноудалён от остальных коммутаторов, аналогичными свойствами обладают и коммутаторы N1 и N4.

В качестве L3-коммутатора используется 3650.

### 3.2 Настройка агрегации каналов

Для организации статической агрегации каналов соединяем коммутаторы двумя и более физическими соединениями. На обоих коммутаторах настраиваем эти интерфейсы через interface range. Используя команду channel-group, создаём группу интерфейсов и присваиваем им режим active.

## 3.3 Настройка виланов

Для настройки виланов необходимо выполнить три группы действий.

### 3.3.1 Настройка VTP

Для настройки VTP необходимо выбрать VTP-сервер. Логично будет расположить его в Root. Для настройки воспользуемся следующими командами:

1. VTP mode выбираем server,

2. VTP domain – задаём название VTP-серверу,

3. VTP password – задаём пароль VTP-серверу.

На остальных коммутаторах выполняются следующие команды:

1. VTP mode выбираем client,

2. VTP domain – указываем название сервера, к которому необходимо подключиться,

3. VTP password – указываем соответствующий пароль.

### 3.3.2 Создание виланов

На VTP-сервере создаём четыре вилана используя команду vlan. Каждому из них присваиваем номер. В данной лабораторной использованы следующие номера виланов: 10 – первый пользовательский, 20 – второй пользовательский, 100 – нативный, 101 – административный. Каждому из них присваиваем соответствующие название командой name.

### 3.3.3 Настройка портов

Все соединяющие коммутаторы между собой порты командой switchport mode необходимо перевести в режим trunk. Каждому из них нужно командой switchport trunk allowed назначить разрешённые виланы, разрешёнными должны быть все четыре вилана. Также необходимо задать нативный вилан командой switchport trunk native.

Все порты, которые соединяют станции и коммутаторы командой switchport mode необходимо перевести в режим access. Каждому порту командой switchport access назначается вилан, который будет использоваться на этом порте. В данной лабораторной первый пользовательский вилан назначен PC2 и Laptop1, второй – PC1, Laptop2, Laptop3, административный – PC3.

## 3.4 PVST

Per VLAN Spanning Tree по умолчанию включён на коммутаторах, явная активация не требуется.

## 3.4.1 Назначение Root корневым мостом

Для назначения Root корневым мостом на Root необходимо выполнить команду spanning-tree vlan [номера вланов] root, что обозначит его данный коммутатор как корневой мост.

### 3.4.2 Настройка PortFast

PortFast рекомендуется только на портах подключённых к конечному оборудованию. PortFast позволяет миновать стадии listening и learning и сразу же перейти в состояние forwarding. В случае использования PortFast на truck портах могут возникать петли.

Для настройки PortFast необходимо на всех интерфейсах выполнить команду spanning-tree portfast.

### 3.4.3 Настройка BPDU Guard

BPDU Guard гарантирует, что при получении BPDU на порт он будет сразу же отключен. Это необходимо для защиты от атак по типу «человек в центре», которые можно осуществить, претворившись коммутатором с превосходящим ID моста, что сделало бы его корневым, в таком случае пакеты для обхода петли будут проходить именно через этот подставной корневой мост.

Для настройки BPDU Guard необходимо на всех интерфейсах, которые направлены соединены со станциями, выполнить команду spanning-tree bpduguard enable.

Для проверки BPDU Guard необходимо к одному из настроенных для станций портов, предварительно отключив Port Security, подключить коммутатор. После этого порт сразу же будет переведён в состояние error-disabled.

### 3.4.4 Проверка работоспособности PVST+

Чтобы проверить работоспособность PVST+ отключим активное соединение в районе петли, после этого ранее выключенное для исключения возможности появления петель соединение должно перейти в режим forwarding.

Чтобы проверить PortFast отключим и сразу включим один из портов, соединяющих коммутатор и станцию, порт сразу же должен перейти в состояние forwarding (загорится зелёным), что свидетельствует о пропуске состояний listening и learning.

## 3.5 Настройка маршрутизации

Для настройки маршрутизации в Root используем команду ip routing. Создаём виртуальные интерфейсы командой interface vlan для каждого вилана, после чего назначаем им IP-адреса из выбранных подсетей. На каждом коммутаторе создаём виртуальный интерфейс с административным виланом, после чего назначаем IP-адрес из административной подсети.

На каждой станции прописываем IP-адрес, маску подсети, Root указываем шлюзом по умолчанию. Однако прописывать шлюз по умолчанию для станции, которая подключена к административному вилану не нужно.

## 3.6 Настойка SSH

Для настройки SSH нужно выполнить следующие действия на каждом коммутаторе. Задать названия коммутаторов, для этого выполняем команды hostname и ip domain-name. Также необходимо установить пароль на вход в привилегированный режим, для чего используем команду enable password. После этого можно создать криптографический ключ длинной 1024 бита, для чего используется команда crypto key generate rsa.

Теперь создаётся имя пользователя и соответствующий пароль, для этого используется команда username [имя пользователя] password [пароль]. Переходим в режим конфигурации линии командой line vty 0 15 и выполняем команду transport input ssh, тем самым наставая разрешённый протокол подключения к линии. Тут же прописываем команду login local, чтобы при аутентификация производилась посредством локального пароля.

Теперь с административной станции можно подключиться к коммутатору можно с помощью команды sh -l [имя пользователя] [IP-адрес].

## 3.7 Последний шаг

Последним шагом выполнения данной лабораторной работы является установка звезды (star) на мой [репозиторий](https://github.com/andrejHurynovic/bsuirLabs) в GitHub, откуда вы, собственно, и взяли этот документ…

# 4 РАБОЧИЕ КОФИГУРАЦИИ

## 4.1 N1

hostname N1

ip domain-name N1

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface Port-channel2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 2 mode active

interface FastEthernet0/2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 2 mode active

interface FastEthernet0/3

shutdown

interface FastEthernet0/4

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/5-6

interface FastEthernet0/7

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/8-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.1 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.2 N2

hostname N2

ip domain-name N2

enable password 123

username cisco password 0 123

ip routing

spanning-tree mode pvst

spanning-tree vlan 10,20,100-101 priority 24576

interface Port-channel1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface Port-channel4

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface Port-channel6

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface GigabitEthernet1/0/1-2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/3-4

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 4 mode active

interface GigabitEthernet1/0/5-6

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/7-24

shutdown

interface GigabitEthernet1/1/1-4

shutdown

interface Vlan10

mac-address 00e0.f784.ac01

ip address 47.57.196.100 255.255.254.0

interface Vlan20

mac-address 00e0.f784.ac02

ip address 98.46.233.100 255.255.255.128

interface Vlan100

mac-address 00e0.f784.ac03

ip address 183.171.210.1 255.255.255.0

interface Vlan101

mac-address 00e0.f784.ac04

ip address 199.216.215.2 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 3.3 N3

hostname N3

ip domain-name N3

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface FastEthernet0/1

switchport access vlan 20

switchport mode access

switchport port-security

switchport port-security mac-address 0001.424A.9360

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 10

switchport mode access

switchport port-security

switchport port-security mac-address 0003.E46C.B1DA

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

switchport access vlan 101

switchport mode access

switchport port-security

switchport port-security mac-address 0007.EC60.6AB8

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/4-6

shutdown

interface FastEthernet0/7

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/8-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.3 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.4 N4

hostname N4

enable password 123

ip domain-name N4

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface Port-channel2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/2-3

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 2 mode active

interface FastEthernet0/4-6

shutdown

interface FastEthernet0/7

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/8-24

shutdown

interface GigabitEthernet0/1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,101

switchport mode trunk

interface GigabitEthernet0/2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,101

switchport mode trunk

interface Vlan101

ip address 199.216.215.4 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.5 N5

hostname N5

ip domain-name N5

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface FastEthernet0/1

switchport access vlan 10

switchport mode access

switchport port-security

switchport port-security mac-address 000B.BE44.56D9

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 20

switchport mode access

switchport port-security

switchport port-security mac-address 000A.F38D.BE67

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

switchport access vlan 20

switchport mode access

switchport port-security

switchport port-security mac-address 0010.1100.93B8

duplex full

speed 100

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/4-5

shutdown

interface FastEthernet0/6

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/7-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.5 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.6 N6

hostname N6

ip domain-name N6

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface Port-channel2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 2 mode active

interface FastEthernet0/2

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

channel-group 2 mode active

interface FastEthernet0/3-4

shutdown

interface FastEthernet0/5

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/6-7

shutdown

interface FastEthernet0/8

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/9-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.6 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.7 N7

hostname N7

ip domain-name N7

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface FastEthernet0/1

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/2

shutdown

interface FastEthernet0/3

switchport access vlan 10

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,101

switchport mode trunk

interface FastEthernet0/4

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/5-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.7 255.255.255.0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

## 4.8 N8

hostname N8

ip domain-name N8

enable password 123

username cisco privilege 1 password 0 123

spanning-tree mode pvst

interface FastEthernet0/1-5

shutdown

interface FastEthernet0/6

switchport trunk native vlan 100

switchport trunk allowed vlan 10,20,100-101

switchport mode trunk

interface FastEthernet0/7-24

shutdown

interface GigabitEthernet0/1-2

shutdown

interface Vlan101

ip address 199.216.215.8 255.255.255.0

line vty 0 4

login local

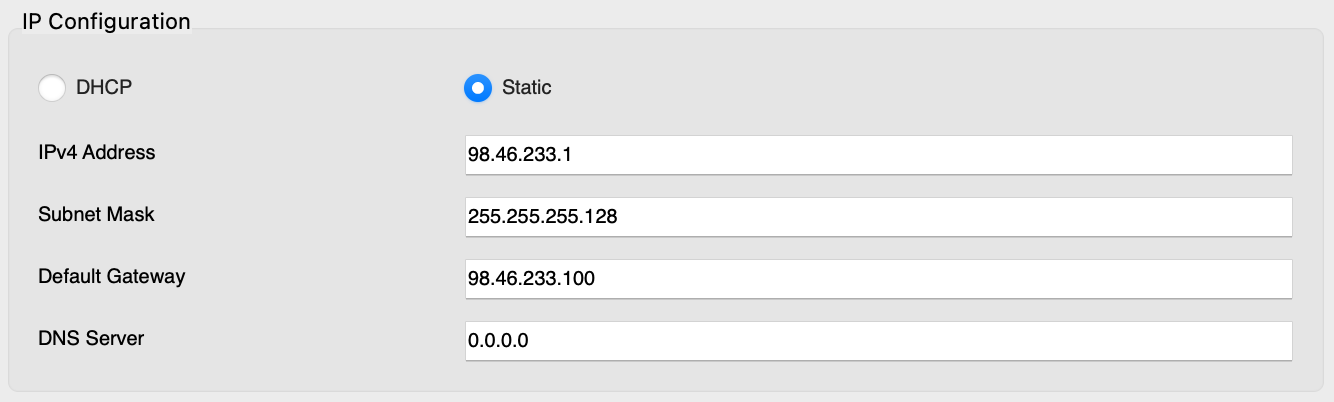
transport input ssh

line vty 5 15

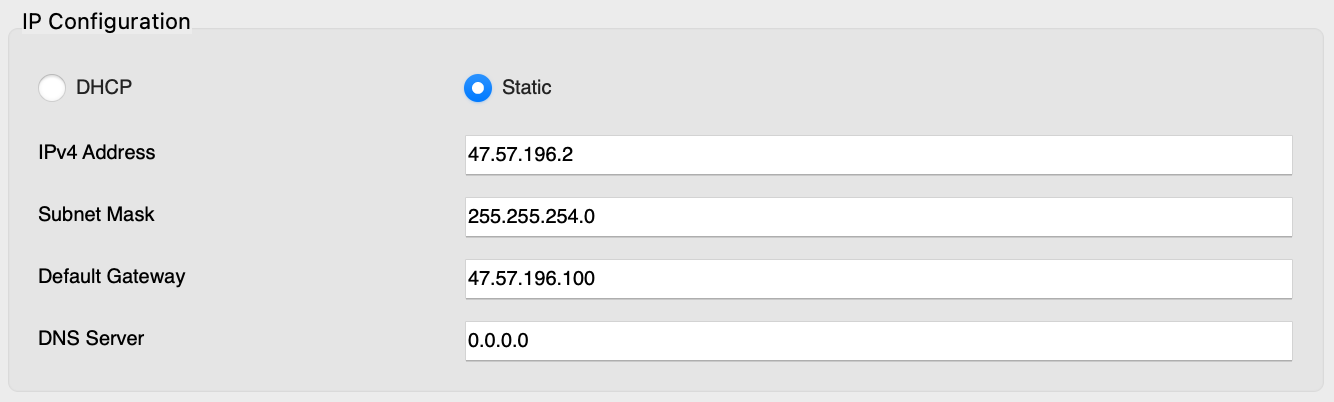
login local

transport input ssh

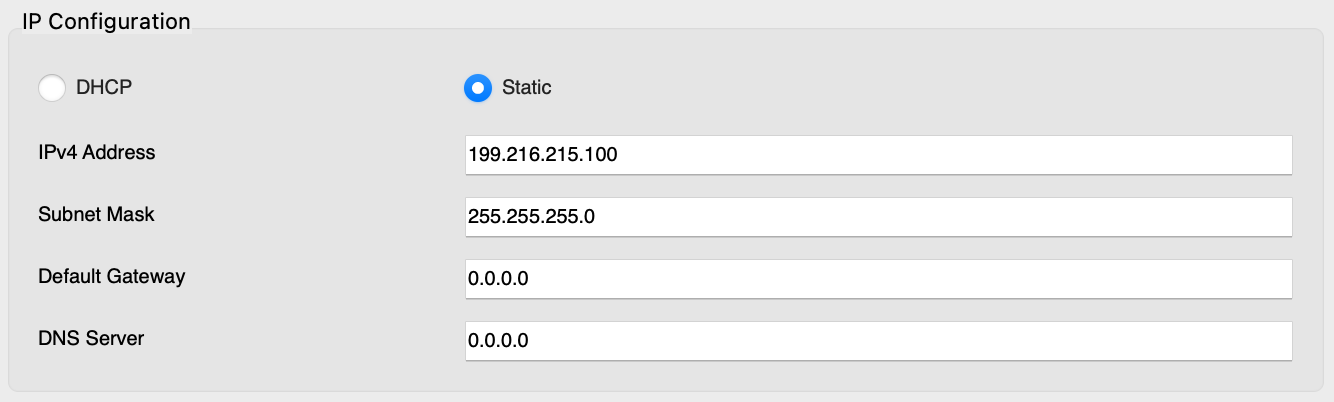
## 4.9 PC1



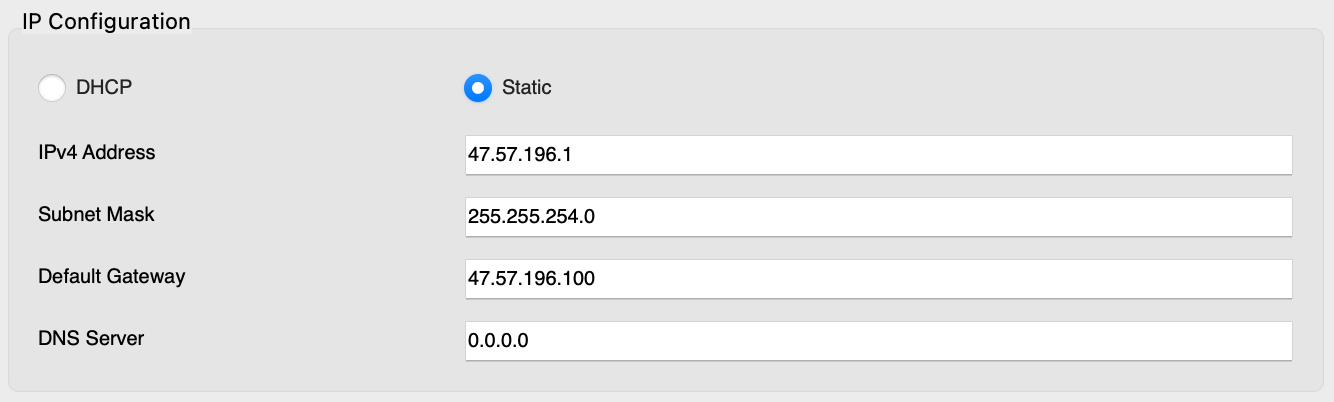
## 4.10 PC2



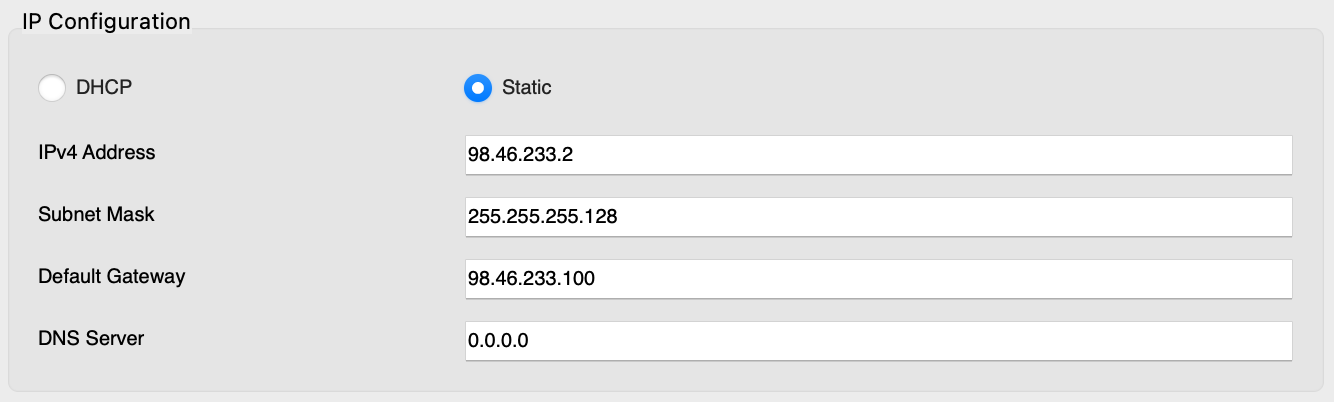
## 4.11 PC3



## 4.12 Laptop1



## 4.13 Laptop2



## 4.14 Laptop3

