Инв. №	Подп. и дата	Взам.	Инв.№	Подп. и дата

Коммутатор уровня доступа

QSW-3750

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ 4
2 ОСНОВНЫЕ НАСТРОЙКИ ПРОГРАММЫ 5
2.1 Настройка SNMP 5
2.1.1 Введение в SNMP 5
2.1.2 Введение в MIB 6
2.1.3 Типичные примеры настройки SNMP 7
2.2 Модернизация системы 7
2.2.1 Системные файлы программы 8
2.2.2 Введение в FTP/TFTP 8
2.2.3 Пример обновления прошивки через FTP/TFTP 10
2.3 КОНФИГУРИРОВАНИЕ ПОРТОВ 12
2.3.1 ВВЕДЕНИЕ 12
2.4 КОНФИГУРАЦИЯ ФУНКЦИИ ИЗОЛЯЦИИ ПОРТОВ 15
2.4.1 ВВЕДЕНИЕ В ФУНКЦИЮ ИЗОЛЯЦИИ ПОРТОВ 15
2.4.2 ТИПОВЫЕ ПРИМЕРЫ ФУНКЦИИ ИЗОЛЯЦИИ ПОРТОВ. 15
2.5 КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ 16
2.5.1 ВВЕДЕНИЕ В ФУНКЦИЮ РАСПОЗНАВАНИЯ ПЕТЛИ 16
2.5.2 ПРИМЕРЫ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ. 17
2.6 НАСТРОЙКА PORT CHANNEL 18
2.6.1 ОБЩИЕ СВЕДЕНИЯ О PORT CHANNEL 18
2.6.2 ОБЩИЕ СВЕДЕНИЯ О LACP 19
2.6.3 ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ PORT CHANNEL 21
2.7 БЕЗОПАСНОСТЬ ПОРТОВ 22
2.7.1 Введение в 802.1x 22
2.8 НАСТРОЙКА ТАБЛИЦЫ MAC АДРЕСОВ 25
2.8.1 ОБЩИЕ СВЕДЕНИЯ О ТАБЛИЦЕ MAC АДРЕСОВ 25
2.8.2 ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ ТАБЛИЦЫ MAC АДРЕСОВ. 28
2.9 НАСТРОЙКА QOS 29
2.9.1 ОБЩИЕ СВЕДЕНИЯ О QOS 29

2.9.2 ПРИМЕР НАСТОРОЙКИ QOS 35
2.11.1 ВВЕДЕНИЕ В DHC/ARP SNOOPING 38
2.11.2 ТИПОВОЕ ПРИМЕНЕНИЕ DHCP SNOOPING 39
2.13 Конфигурирование SYSLOG 41
2.14 КОНФИГУРИРОВАНИЕ ACL 43
2.14.1 Введение в ACL 43
2.14.2 Примеры конфигурирования ACL 44
3 УПРАВЛЕНИЕ ПРОГРАММОЙ 45
3.1 Варианты управления 45
3.1.1 Внеполосное управление 45
3.1.2 Внутриполосное управление 48
3.1.2.1 Управление по Telnet/SSH 48
3.1.2.2 Управление через HTTP 52
3.1.2.3 Управление программой через сетевое управление SNMP **Ошибка! Закладка не определена.**
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 57

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Программное обеспечение устанавливается на коммутатор.

Коммутатор — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В отличие от концентратора (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется. Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса.

Для временного хранения фреймов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки фреймов: буферизация по портам и буферизация с общей памятью. При буферизации по портам пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передаётся на выходной порт только тогда, когда все фреймы, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные фреймы могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти все фреймы хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого фреймы, находившиеся в буфере,

динамически распределяются выходным портам. Это позволяет получить фрейм на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить фреймы. Очистка этой карты происходит только после того, как фрейм успешно отправлен.

2 ОСНОВНЫЕ НАСТРОЙКИ ПРОГРАММЫ

2.1 Настройка SNMP

2.1.1 Введение в SNMP

SNMP (Simple Network Management Protocol) является стандартным протоколом сетевого управления, который широко используется в управлении компьютерными сетями. SNMP является развивающимся протоколом. SNMP v1 [RFC1157] является первой версией протокола SNMP, которая адаптирована к огромному числу производителей своей простотой и легкостью внедрения; SNMP v2c является улучшенной версией SNMP v1.

SNMP-протокол обеспечивает простой способ обмена информацией управления сетью между двумя точками в сети. SNMP использует механизм запросов и передает сообщения через UDP (протокол без установления соединения транспортного уровня), поэтому он хорошо поддерживается существующим компьютерными сетями.

SNMP-протокол использует режим станции-агента. В этой структуре есть две составляющие: NMS (Network Management Station) и агент. NMS является рабочей станцией, на которой стоит клиентская программа SNMP. Это ядро SNMP-управления сетью. Агент серверного программного обеспечения работает на устройствах, которые нуждаются в управлении. NMS управляет всеми объектами через агентов. Программа поддерживает функции агента.

Связь между NMS и агентом происходит в режиме Клиент-Сервер, обмениваясь стандартными сообщениями. NMS посылает запрос и агент отвечает. Есть семь типов SNMP сообщений:

- Get-Request;
- Get-Response;
- Get-Next-Request;
- Get-Bulk-Request;
- Set-Request;

- Trap;
- Inform-Request.

NMS связывается с агентом с помощью запросов: Get-Request, Get-Next-Request, Get-Bulk-Request and Set-Request, агент, при получении запросов, отвечает сообщением Get-Response. О некоторых специальных ситуациях, таких, как изменения статусов сетевых портов устройства или изменения топологии сети, агенты могут отправлять специальные сообщения об аномальных событиях. Кроме того, NMS может быть также установлен для предупреждения некоторых аномальных событий, активируя RMON функцию. Когда срабатывает определенное правило, агенты отправляют сообщения в журналы событий в соответствии с настройками.

2.1.2 Введение в MIB

Информация управления сетью доступа в NMS корректно определена и организована в информационной базе управления (MIB). MIB это предопределенная информация, которая может быть доступна через протоколы управления сетью, во всей своей многослойности и структурированном виде. Предопределенная информация управления может быть получена путем мониторинга сетевых устройств. ISO ASN.1 определяет древовидную структуру для MID, соответственно каждый MIB организует всю доступную информацию в виде такой структуры. Каждый узел этого дерева содержит OID (идентификатор объекта) и краткое описание узла. OID представляет собой набор целых чисел, разделенных точками и может быть использован для определения местоположения узла в древовидной структуре MID, как показано на рисунке 1:

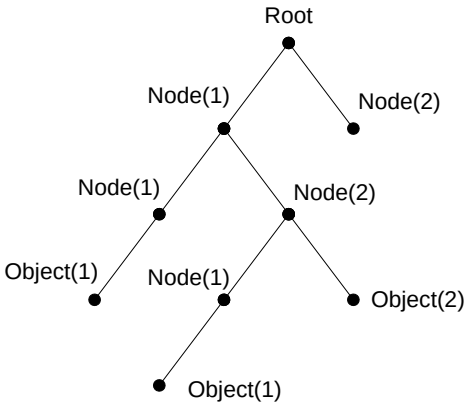

Рисунок 1 – Пример дерева ASN.1

На рисунке 1 OID объекта A является 1.2.1.1. NMS может найти этот объект через этот уникальный OID и получить стандартные переменные объекта. MIB определяет

набор стандартных переменных для мониторинга сетевых устройств, следуя этой структуре.

Если информация о переменных MIB агента должна быть просмотрена, необходим запуск программного обеспечения просмотра MIB на NMS. MIB в агенте обычно состоит из публичного MIB и частного MIB. Публичный MIB содержит открытую информацию управления сетью, которая может быть доступна для всех NMS, частный MIB содержит конкретную информацию, которая может быть просмотрена и контролируется поддержкой производителя.

MIB-I [RFC1156] была первой реализацией публичных MIB SNMP, и была заменена MIB-II [RFC1213]. MIB-II расширяет MIB-I и сохраняет OID для MIB деревьев в MIB-I. MIB-II, содержит вложенные деревья, которые также называются группами. Объекты в этих группах охватывают все функциональные области в управлении сетью. NMS получает информацию об управлении сетью просматривая MIB на SNMP агенте.

Программа может работать в качестве SNMP агента, а также поддерживает SNMP v1/v2c. Также программа поддерживает базовые MIB-II, RMON публичные MIB и другие публичные MID, такие как Bridge MIB. Кроме того, программа поддерживает самостоятельно определенные частные MIB.

2.1.3 Типичные примеры настройки SNMP

IP-адрес NMS 1.1.1.5.

Конфигурация программы, записана ниже:

```
snmp-server sysname "MUEV"
!
snmp-server community "read" ro
snmp-server community "write" rw
snmp-server host 1.1.1.5 traps version 2 "read"
snmp trap link-status all
snmp-server sysname voentelecom
```

NMS может использовать частную строку сообщества для доступа к программе для чтения и записи разрешений или использовать публичную строку сообщества для доступа к программе только для чтения разрешений.

2.2 Модернизация системы

Программа предоставляет два способа обновления: обновление через TFTP и FTP

2.2.1 Системные файлы программы

Файл образа системы включает в себя сжатые файлы аппаратных драйверов, файлы программного обеспечения и т. д., это то, что мы обычно называем «STK file» . STK файл может быть сохранен только в FLASH с определенным названием *****.stk.

Программа предоставляет пользователю два режима обновления TFTP и FTP обновление в режиме Shell.

2.2.2 Введение в FTP/TFTP

FTP (File Transfer Protocol) / TFTP (Trivial File Transfer Protocol) являются протоколами передачи файлов, они оба принадлежат к четвертому уровню (уровню приложений) в TCP / IP стеке протоколов, используемому для передачи файлов между компьютерами, узлами и программами. Оба они передают файлы в клиент-серверной модели. Разница между ними описана ниже.

FTP основан на протоколе TCP для обеспечения надежной связи и транспортировки потока данных. Тем не менее, он не предусматривает процедуру авторизации для доступа к файлам и использует простой механизм аутентификации (передает имя пользователя и пароль для аутентификации в виде простого текста). При использовании FTP для передачи файлов, должны быть установлены два соединения между клиентом и сервером: управляющее соединение и соединение передачи данных. Далее должен быть послан запрос на передачу от FTP-клиента на порт 21 сервера для установления управляющего соединения и согласования передачи данных через управляющее соединение.

Существует два типа таких соединений: активные и пассивные соединения.

При активном подключении клиент передает его адрес и номер порта для передачи данных серверу, управляющее соединение поддерживается до завершения передачи этих данных. Затем, используя адрес и номер порта, предоставленных клиентом, сервер устанавливает соединение на порт 20 (если не занят) для передачи данных, если порт 20 занят, сервер автоматически генерирует другой номер порта для установки соединения.

При пассивном подключении, клиент через управляющее соединение просит сервер установить подключение. Затем сервер создает свой порт для прослушивания данных и уведомляет клиента о номере этого порта, далее клиент устанавливает соединение с указанным портом.

TFTP основан на протоколе UDP, обеспечивающим службу передачи данных без подтверждения доставки и без аутентификации и авторизации. Он обеспечивает правильную передачу данных путем механизма отправки и подтверждения и повторной передачи тайм-аут пакетов. Преимущество TFTP перед FTP в том, что у первый гораздо проще и имеет низкие накладные расходы передачи данных.

Программа может работать как FTP / TFTP клиент или сервер. Когда программа работает как FTP / TFTP клиент, файлы конфигурации и системные файлы можно загрузить с удаленного FTP / TFTP сервера (это могут быть как хосты, так и другие

программы) без ущерба для его нормальной работы. И также может быть получен список файлов с сервера в режиме FTP клиента. Конечно, программа может также загрузить текущие конфигурационные файлы и системные файлы на удаленный FTP / TFTP сервер (это могут быть как хосты, так и другие программы). Когда программа работает как FTP / TFTP сервер, он может обеспечить загрузку и выгрузку файлов для авторизованных FTP / TFTP клиентов.

Вот некоторые термины часто используемые в FTP/TFTP.

ROM: Сокращенно от EPROM, СПЗУ. EPROM заменяет FLASH память в программе.

SDRAM: ОЗУ в программе, которая используется для работы системы и программного обеспечения, а также хранилища последовательности конфигурации.

FLASH: Флэш-память используется для хранения файлов системы и файла конфигурации.

System file: включает в себя образ системы и загрузочный файл.

System image file: файл образа системы включает в себя сжатые файлы аппаратных драйверов, файлы программного обеспечения, это то что мы обычно называем «STK file» . STK файл может быть сохранен только в FLASH. Программа позволяет загрузить файл образа системы через FTP в режиме Shell только с определенным названием nos.stk, другие файлы STK будут отклонены.

Boot file: необходимы для загрузки и запуска программы, это то, что мы обычно называем «ROM file» (могут быть сжаты в STK файлы, если они слишком больших размеров).

Configuration file: включает в себя файл начальной конфигурации и файл текущей конфигурации. Разница в свойствах между этими файлами позволяет облегчить резервное копирование и обновление конфигураций

Start up configuration file: это последовательность команд конфигурации, используемая при запуске программы. Файл начальной конфигурации хранится в энергонезависимой памяти. Если устройство не поддерживает CF, файл конфигурации хранится только во FLASH, Если устройство поддерживает CF, файл конфигурации хранится во FLASH-памяти или CF. Если устройство поддерживает мультиконфигурационный файл, они должны иметь расширение .cfg, имя по умолчанию startup.cfg. Если устройство не поддерживает мультиконфигурационный файл, имя файла начальной конфигурации должно быть startup-config.

Running configuration file: это текущая(running) последовательность команд конфигурации, используемая программой. Текущий конфигурационный файл хранится в оперативной памяти. В процессе работы текущая конфигурация running-config может быть сохранена из RAM во FLASH память командой «write» или «copy running-config startup-config» .

Factory configuration file: файл конфигурации, поставляемый с программой, так называемый factory-config. Для того, чтобы загрузить заводской файл конфигурации и

перезаписать файл начальной конфигурации, необходимо ввести команды erase startup-config, а затем перезагрузить программу.

2.2.3 Пример обновления прошивки через FTP/TFTP

Настройки одинаковы для IPv4 и IPv6 адресов. На рисунке 2 пример загрузки nos.stk файла FTP/TFTP клиентом показан только для IPv4 адреса.

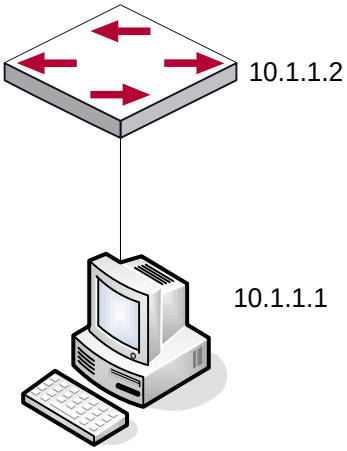

Рисунок 2 - Загрузка nos.stk файла FTP/TFTP клиентом

Сценарий 1: Использование программы в качестве FTP/TFTP клиента. Программа соединяется одним из своих портов с компьютером, который является FTP/TFTP сервером с IP-адресом 192.168.1.2, программа действует как FTP/TFTP клиент, IP-адрес интерфейса VLAN1 программы 192.168.1.2. Требуется загрузить файл "nos.stk" с компьютера в программу.

Далее описана процедура обновления программы:

switch#copy tftp://192.168.1.2/nos.stk backup

Mode..... TFTP

Set Server IP..... 192.168.1.2

Path..... ./

Filename..... nos.stk

Data Type..... Code

Destination Filename..... backup

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) – для FTP

switch#copy ftp://switch@192.168.1.2/nos.stk backup
Remote Password:*****

Mode..... FTP
Set Server IP..... 192.168.1.2
Path..... ./
Filename..... nos.stk
Data Type..... Code
Destination Filename..... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) - для TFTP

switch #boot system backup
Activating image backup .. – выбираем next-active stk файл

switch#show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	8.1.0.3	8.1.0.4	8.1.0.3	8.1.0.4

2.3 Конфигурирование портов

2.3.1 Введение

В программе существуют кабельные и комбо порты. Комбо порт может быть сконфигурирован как 1000GX-TX порт, так и как оптический SFP Gigabit порт.

Если пользователь хочет сконфигурировать сетевой порт, он может ввести команду «interface ethernet <interface-list>«для входа в соответствующий режим конфигурации порта, где <interface-list> содержит один или несколько портов. Если <interface-list> содержит несколько портов, номера портов разделяются специальными символами «,» и «-», где «,» используется для перечисления портов, а «-» - для указания диапазона номеров портов. Положим, операция должна быть выполнена над портами 2,3,4,5. Тогда команда будет выглядеть так «interface ethernet 1/0/2-1/0/5» . В режиме конфигурации порта можно изменять скорость, режим дуплекса и настраивать управление траффиком, при этом данные изменения требуют соответствующих изменений на ответных сетевых портах.

2.3.2 Пример конфигурирования порта

(Config)#interface 1/0/2

(Interface 1/0/2)# bandwidth-control 1024 both / ограничение полосы пропускания интерфейса в kbps

Включение функционала storm-control :

(Switch) (Config)#interface 1/0/1

(Switch) (Interface 1/0/11)#storm-control broadcast

(Switch) (Interface 1/0/11)#storm-control broadcast rate 64

(Switch) (Interface 1/0/11)#storm-control multicast

(Switch) (Interface 1/0/11)#storm-control multicast rate 64

(Switch) (Interface 1/0/11)#storm-control unicast

(Switch) (Interface 1/0/11)#storm-control unicast rate 64

(Switch) (Interface 1/0/11)#exit

(Interface 1/0/2)#speed 100 full-duplex /конфигурирование скорости и дуплекса интерфейса

2.4 Конфигурирование VLAN

2.4.1 Начальные сведения о VLAN

VLAN (Virtual Local Area Network – виртуальная локальная сеть) – технология, разделяющая логические адреса устройств в сети для отделения сегментов сети в зависимости от функций, выполняемых устройствами, приложений или требований управления. Таким образом, виртуальные локальные группы могут формироваться независимо от физического расположения устройств. IEEE опубликовал протокол IEEE 802.1Q для стандартизации применения VLAN. VLAN на коммутаторе работает в соответствии с этим протоколом. Основная идея технологии VLAN в том, чтобы разделить динамически большую локальную сеть на несколько независимых широковещательных доменов в соответствии с требованиями, предъявляемыми к сети.

Каждый широковещательный домен на рисунке является VLAN. VLANы имеют те же свойства, что и физические сети, за исключением того, что VLAN – логическое объединение, а не физическое. Поэтому объединение VLANов может создаваться вне зависимости от физического расположения устройств и широковещательный, многопользовательский и однопользовательский трафик внутри VLAN отделен от других VLANов. Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает следующие преимущества:

- Улучшается производительность сети;
- Экономятся сетевые ресурсы;
- Упрощается управление сетью;
- Снижается стоимость сети;
- Улучшается безопасность сети;

Ethernet порты коммутатора могут работать в трех различных режимах: Access, Hybrid и Trunk. Каждый режим имеет свой способ пересылки пакетов, с меткой или без. Порты типа Access принадлежат только одному VLAN. Обычно они используются для подключения к компьютеру. Порты типа Trunk позволяют пересылать пакеты нескольких VLANов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств. Порты типа Hybrid также позволяют пересылать пакеты нескольких VLANов. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств. Порты типов Hybrid и Trunk принимают данные по одному алгоритму, но методы отправки данных отличаются: порты типа Hybrid могут отправлять пакеты в различные VLANы без метки VLANa, тогда

как порты типа Trunk отправляют пакеты различных VLAN только с меткой VLANa, за исключением VLAN, прописанного на порту как native.

2.4.2 Пример конфигурирования VLAN

(Switch) #vlan database

(Switch) (Vlan)#vlan 1-100

(Switch) (Vlan)#

(Switch) (Vlan)#exit

(Switch) #configure

(Switch) (Config)#interface 1/0/1

(Switch) (Interface 1/0/1)#switchport mode trunk

(Switch) (Interface 1/0/1)#switchport trunk allowed vlan 1-100

2.5 Конфигурирование функции изоляции портов

2.5.1 Начальные сведения о функции изоляции портов

Изоляция портов — это независимая порто-ориентированная функция, работающая между портами, которая изолирует потоки различных портов друг от друга. С помощью этой функции пользователь может изолировать порты в пределах VLAN для сохранения ресурсов VLAN и усиления секретности сети. После того, как эта функция будет сконфигурирована, порты в группе изолированных портов будут изолированы друг от друга, в то время как порты из различных групп изоляции или неизолированных могут пересылать данные друг другу совершенно нормально. На коммутаторе может быть сконфигурировано не более 3 групп изоляции портов.

2.5.2 Пример конфигурации функции изоляции портов

(Switch) (Config)#switchport protected 0 name group_1

(Switch) (Config)#interface 1/0/1-1/0/10

(Switch) (Interface 1/0/1-1/0/10)#switchport protected 0

2.4 Конфигурация функции изоляции портов

2.4.1 Введение в функцию изоляции портов

Изоляция портов — это независимая портоориентированная функция, работающая между портами, которая изолирует потоки различных портов друг от друга. С помощью этой функции пользователь может изолировать порты в пределах VLAN для сохранения ресурсов VLAN и усиления секретности сети. После того, как эта функция будет сконфигурирована, порты в группе изолированных портов будут изолированы друг от друга, в то время как порты из различных групп изоляции или неизолированных могут пересылать данные друг другу совершенно нормально. В программе может быть сконфигурировано не более 3 групп изоляции портов.

2.4.2 Типовые примеры функции изоляции портов показан на рисунке 3.

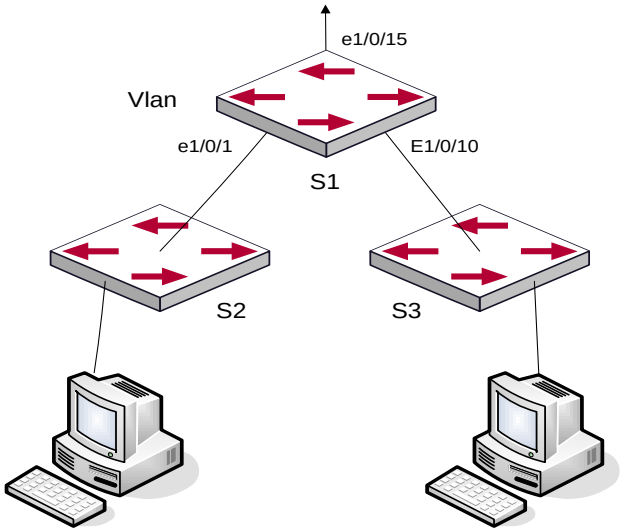

Рисунок 3 – Типовые примеры функции изоляции портов

Порты e1/0/1, e1/0/10 и e1/0/15 все принадлежат к VLAN 100. Требование заключается в том, чтобы после включения функции изоляции портов в программе switch1 порты e1/0/1 и e1/0/10 в программе не могли связываться друг с другом и оба могли связываться с портом e1/0/15, смотрящим в сеть. То есть, связи между любыми парами низ лежащих портов нет, и в то же время связь между любым низ лежащим и вышестоящим портом работает. Вышестоящий порт может работать с любым портом нормально.

Конфигурация программы S1:

(Config)#switchport protected 0

(Config)#interface 1/0/2-1/0/10

(Interface 1/0/2-1/0/10)#switchport protected 0

(switch) #show switchport protected 0

Name.....

Member Ports :

1/0/2, 1/0/3, 1/0/4, 1/0/5, 1/0/6, 1/0/7, 1/0/8, 1/0/9,

1/0/10

2.5 Конфигурация функции распознавания петли на порту

2.5.1 Введение в функцию распознавания петли

С развитием сетевых устройств, все больше и больше пользователей подключаются к сети через Ethernet-программы. В промышленных сетях пользователи получают доступ через программы 2-го уровня, что предъявляет строгие требования к взаимодействию между устройствами как внешней, так и внутренней сети. Когда требуется взаимодействие на 2-ом уровне, сообщение должно отправляться точно в соответствии с MAC адресом для корректной работы между пользователями. Устройства второго уровня запоминают MAC адреса, изучая входящие MAC адреса источников пакетов, и при поступлении пакета с неизвестным адресом источника они записывают его MAC адрес в таблицу, закрепляя его за портом, откуда пришел этот пакет. Таким образом, следующий пакет с данным MAC адресом в качестве порта назначения будет отправлен сразу на этот порт. То есть адрес сразу фиксируется на порту для отправки всех пакетов.

Когда пакет с MAC адресом источника, уже запомненным программой, приходит через другой порт, запись в таблице MAC адресов изменяется таким образом, чтобы пакеты с данным MAC адресом направлялись через новый порт. В результате, если на участке между двумя адресатами существует какая-либо петля, все MAC адреса из сети второго уровня будут пересылаться на тот порт, где существует петля (обычно MAC адреса в этом случае с высокой частотой переключаются с одного порта на другой), что вызывает перегрузку и потерю работоспособности сети 2-го уровня. Вот почему

необходимо проверять наличие петли на сетевых портах. Когда на порту определяется петля, обнаружившее ее устройство должно послать предупреждение в систему управления сетью, позволяя сетевому администратору обнаружить, локализовать и решить проблему в сети.

Поскольку, система обнаружения петель может автоматически принимать решения о наличии петли в соединении и ее исчезновении, устройства с функциями контроля на портах (таких, как изоляция портов и контроль за запоминанием MAC адресов) могут значительно снизить нагрузку с сетевого администратора, а также уменьшить время реакции на проблему, минимизируя воздействие петли на сеть.

2.5.2 Примеры функции распознавания петли на порту показаны на рисунке 4.

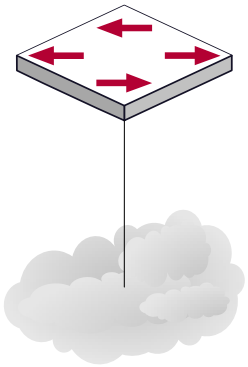

Рисунок 4 – Типичный пример подключения

В приведенной ниже конфигурации, программа определяет существование петли в топологии сети. После включения функции распознавания петли на порту, смотрящем во внешнюю сеть, программа будет уведомлять подсоединенную сеть о существовании петли и контролировать порт программы для обеспечения нормальной работы данной сети.

Последовательность конфигурации программы:

(switch) (Config)#spanning-tree

(switch) (Config)#errdisable recovery cause bpdustorm

(switch) (Config)#errdisable recovery interval 300

(switch) (Config)#show errdisable recovery

Errdisable Reason Auto-recovery Status

---------- ----------

dhcp-rate-limit Disabled

udld Disabled

bcast-storm Disabled

mcast-storm Disabled
ucast-storm Disabled
bpduguard Disabled
bpdustorm Enabled
sfp-mismatch Disabled

Timeout for Auto-recovery from D-Disable state 300

2.6 Настройка Port channel

2.6.1 Общие сведения о Port channel

Для понимания термина порт-канала (Port channel) надо ввести понятие группы портов. Группа портов – это группа физических портов на конфигурационном уровне. Только физические порты в группе портов могут быть частью объединенного канала и стать членами Port channel. Логически группа портов является не портом, а набором портов. При определенных условиях физические порты в группе портов позволяют посредством объединения портов сформировать Port channel, который обладает всеми свойствами логического порта и таким образом становится независимым логическим портом. Агрегация портов — это абстрактное понятие, подразумевающее по собой объединение набора портов с одинаковыми свойствами в логический порт. Port channel — это набор физических портов, который логически используется как один физический порт. Он может использоваться пользователем как обычный порт. Он не может не только добавить пропускной способности на сеть, но и способен обеспечить резервирование соединений. Обычно объединение портов используется, когда программа подключена к маршрутизатору, клиентской станции или другим программам. На рисунке 5 показано агрегирование портов.

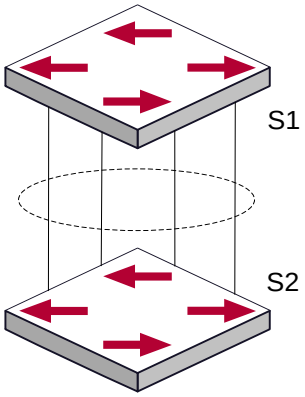

Рисунок 5 – Агрегирование портов

Как показано выше, программа S1 объединил порты в Port channel. Пропускная полоса Port channel равна сумме пропускных способностей четырех портов. Когда необходимо передать трафик с программы S1 на S2, распределение трафика будет определяться на основе MAC адреса источника и младшего бита MAC адреса приемника. В результате вычислений определяется, какой порт будет передавать трафик. Если один порт в Port channel неисправен, трафик будет перераспределяться на другие порты посредством алгоритма распределения. Данный алгоритм поддерживается аппаратно.

Для правильной работы Port channel необходимо соблюдать следующие условия:

1) Все порты работают в режиме полного дуплекса.

2) Все порты имеют одинаковую скорость.

3) Все порты являются портами доступа и принадлежат одному VLAN, или все они являются транковыми портами или они все гибридные порты.

4) Если все порты являются транковыми или гибридными, тогда сконфигурированные на них допустимые VLAN и основной VLAN должны быть у всех одинаковыми.

Если Port channel сконфигурирован на программе вручную иди динамически, система автоматически назначает порт с наименьшим номером мастер-портом Port channela. Если в программе активирован протокол spanning tree, протокол построения дерева воспринимает Port channel как логический порт и посылает BPDU пакеты через мастер-порт.

Объединение портов жестко связано с аппаратной частью программы. Программа позволяет агрегировать соединения между любыми двумя программами.

После того, как порты агрегированы, их можно использовать, как обычный порт. Программа имеет встроенный режим конфигурирования интерфейса агрегации, пользователь может создавать соответствующую конфигурацию в этом режиме точно так же, как при конфигурировании VLAN или физического интерфейса.

2.6.2 Общие сведения о LACP

LACP – протокол, базирующийся на стандарте IEEE 802.3ad, и реализующий механизм динамического объединения каналов. Протокол LACP использует пакеты LACPDU (Link Aggregation Control Protocol Data Unit) для обмена информацией с ответными портами.

После того, как протокол LACP включен на порту, данный порт посылает пакеты LACPDU на ответный порт соединения, уведомляя о приоритете системы, MAC адресе системы, приоритете порта, идентификаторе порта и ключе операции. Когда ответный порт получает эту информацию, она сравнивается с информацией о других портах,

которые могут быть объединены. Соответственно, обе стороны соединения могут достичь соглашения о включении или исключении порта из динамической объединенной группы.

Ключ операции создается протоколом в соответствии с комбинацией параметров конфигурации (скорость, дуплекс, базовая конфигурация, ключ управления) портов, которые будут объединяться.

После включения протокола динамического объединения портов (LACP), ключ управления по умолчанию равен 0. После статического объединения портов посредством LACP, ключ управления порта такой же, как ID объединенной группы.

При динамическом объединении портов все члены одной группы имеют одинаковый ключ операции. При статическом объединении только активные порты имеют одинаковый ключ операции.

2.6.2.1 Статическое объединение LACP

Статическое объединение выполняется путем конфигурирования пользователем и не требует протокола LACP. При конфигурировании статического LACP объединения, используется режим «on» для включения порта в группу агрегации.

2.6.2.2 Динамическое объединение LACP

1) Общие положения динамического объединения LACP

Динамическое объединение — это объединение, создаваемое/удаляемое системой автоматически. Оно не позволяет пользователям самостоятельно добавлять или удалять порты из динамического объединения LACP. Порты, которые имеют одинаковые параметры скорости и дуплекса, подключенные к одним и тем же устройствам, имеющие одинаковую конфигурацию могут быть динамически объединены в группу. В случае, если только один порт может создавать динамическое объединение, это называется однопортовым объединением. При динамическом объединении LACP протокол на порту должен быть включен.

2) Режимы портов в динамической группе объединения

В динамической группе объединения порты имеют два статуса — выбранный (selected) или «в ожидании» (standby). Оба типа портов могут посылать и принимать пакеты протокола LACP, но порты в статусе «ожидания» не могут пересылать данные.

Поскольку существует ограничение на максимальное количество портов в группе агрегации, если текущий номер порта превышает предел в группе, тогда устройство на одном конце соединения договаривается с устройством на другом конце для определения статуса порта в соответствии с идентификатором порта.

Этапы согласования следующие:

Сравнение идентификаторов (ID) устройств (приоритет системы и MAC адрес системы). Сначала сравниваются приоритеты систем. Если они одинаковые, тогда сравниваются MAC адреса устройств. Устройство с меньшим идентификатором имеет высший приоритет.

Затем идет сравнение идентификаторов портов (приоритет порта и идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сначала сравниваются приоритеты портов. Если приоритеты одинаковые, тогда сравниваются идентификаторы портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные становятся в режим «ожидание» (standby).

В группе объединения порт с наименьшим идентификатором и статусом «выбранный» становится мастер-портом. Другие порты со статусом «выбранный» становятся членами группы.

2.6.3 Примеры использования Port channel

Вариант 1 – Настройка Port channel для протокола LACP. На рисунке 6 показана конфигурация порта-канала в LACP.

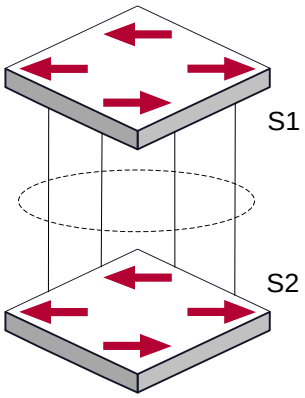

Рисунок 6 – Конфигурация порта-канала в LACP

Имеется две программы S1 и S2. Порты 1, 2, 3, 4 на программе S1 - порты доступа и добавлены в группу 1 в активном режиме. Порты 6, 8, 9, 10 на программе S2 – тоже порты доступа и добавлены в группу 2 в пассивном режиме. Все порты соединены кабелями.

Этапы конфигурации показаны ниже:

Switch1 (Config)#interface 1/0/1-1/0/4

Switch1 (Interface 1/0/1-1/0/4)#addport lag 1

Switch1 (Interface 1/0/1-1/0/4)#interface lag 1

Switch1 (Interface lag 1)#no port-channel static

Switch2 (Config)#interface 1/0/6-1/0/10

Switch2 (Interface 1/0/6-1/0/10)#addport lag 2

Switch2 (Interface 1/0/6-1/0/10)#lacp actor admin state passive

Switch2 (Interface 1/0/6-1/0/10)#interface lag 2

Switch2 (Interface lag 2)#no port-channel static

Switch2 (Interface lag 2)#lacp actor admin state passive

2.7 Безопасность портов

2.7.1 Введение в 802.1x

Протокол IEEE 802.1x реализует метод управления доступом к сети на основе портов, он управляет аутентификацией и устройствами доступа на физическом уровне доступа к сетевым устройствам. На физическом уровне доступа в данном случае находятся порты программы. Если пользовательские устройства, подключенные к этим портам, удается идентифицировать, они получают доступ к ресурсам локальной сети, в противном случае доступ будет запрещен, что во многом эквивалентно физическому выключению. Стандарты IEEE 802.1x определяют протокол управления доступом к сети на основе портов. Протокол применим к соединению точка-точка между устройством доступа и портом доступа, при этом порт может быть логическим или физическим. В типичном случае один физический порт программы присоединен только к одному терминирующему устройству (имеющему физические порты).

Архитектура IEEE 802.1x показана на рисунке 7.

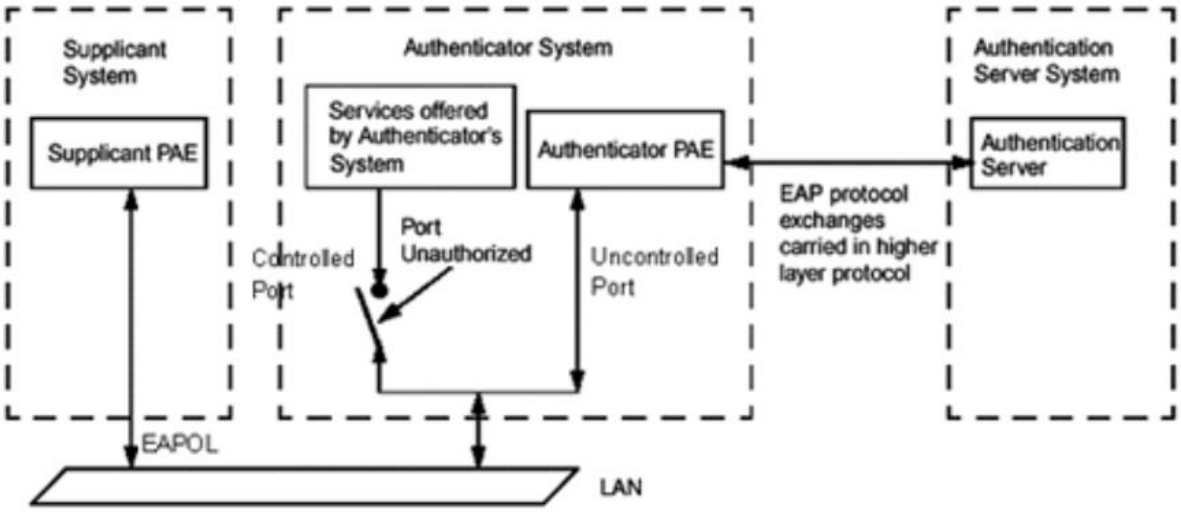

Рисунок 7 – Архитектура IEEE 802.1x показана на рисунке ниже.

Надписи на рисунке 7:

– Supplicant System – клиентская система;

– Supplicant PAE – PAE клиентской системы;

– Autenthicator system – система аутентификатора;

– Autenthicator PAE – PAE аутентификатора;

– Services offered by Autenthicator’s system – услуги, предоставляемые системой аутентификатора;

– Controlled Port – управляемый порт;

– Uncontrolled port – неуправляемый порт;

– EAP protocol exchanges carried in higher layer protocol – обмен сообщениями протокола EAP происходит через протокол более высокого уровня;

– Authentication Server system – система сервера аутентификации;

– Authentication Server – сервер аутентификации.

Архитектура IEEE 802.1x состоит из трех частей:
– клиентской системы (пользовательское устройство доступа);

– аутентифицирующей системы (устройство управления доступом);

– сервера аутентификации.

Взаимодействие пользовательского устройства доступа (PC) и устройства управления доступом (программа доступа) происходит по протоколу EAPOL, определенного стандартами IEEE 802.1x. Взаимодействие сервера аутентификации с устройством управления доступом происходит по протоколу EAP. Данные аутентификации инкапсулируются в пакеты EAP. Пакет EAP передается в пакетах протоколов более высоких уровней, например, RADIUS и, пройдя через сложную сеть, попадает на сервер аутентификации.

Порты, которые предоставляет устройство управления доступом на уровне порта, могут быть виртуальными портами двух типов: управляемые порты и неуправляемые порты. Неуправляемый порт всегда находится во включенном состоянии в обоих направлениях передачи пакетов аутентификации EAP. Управляемый порт, когда он авторизован на передачу трафика с коммутацией пакетов, всегда будет в подключенном состоянии. Если порт не авторизован, то он выключен и передача пакетов невозможна.

При IEEE 802.1x, программа используется как устройство управления доступом; подключаемое пользовательское устройство — это устройство с клиентским ПО, поддерживающим 802.1x. Сервер аутентификации обычно находится в AAA-центре оператора и обычно является RADIUS-сервером.

Для улучшения безопасности и управления в программе реализовано различие между пользовательским доступом и аутентификацией IEEE 802.1x на основе MAC-адресов. Только аутентифицированные пользовательские устройства доступа, подключенные к одному и тому же физическому порту, могут получать доступ к сети. Неавторизованные устройства не получат доступа в сеть. Таким образом, даже если к одному физическому порту подключено много терминалов, программа может аутентифицировать их и управлять каждым пользовательским устройством доступа индивидуально.

На основе функции аутентификации 802.1x по MAC-адресам реализована пользовательская аутентификация 802.1x (IP-адрес + MAC-адрес + порт). Это позволяет пользователям до прохождения ими аутентификации получать доступ к ограниченным ресурсам. При пользовательском управлении доступом имеется два режима: стандартное управление и расширенное управление. При стандартном пользовательском управлении доступ к ограниченным ресурсам не ограничивается, все пользователи порта имеют к ним доступ до аутентификации. После аутентификации пользователи получают доступ ко всем ресурсам. При расширенном пользовательском управлении доступом только специальные пользователи до аутентификации получат доступ к ограниченным ресурсам. После прохождения аутентификации эти специальные пользователи получат доступ ко всем ресурсам.

2.7.2 Пример конфигурации 802.1x + RADIUS.

Конфигурация 802.1x + RADIUS показана на рисунке 8.

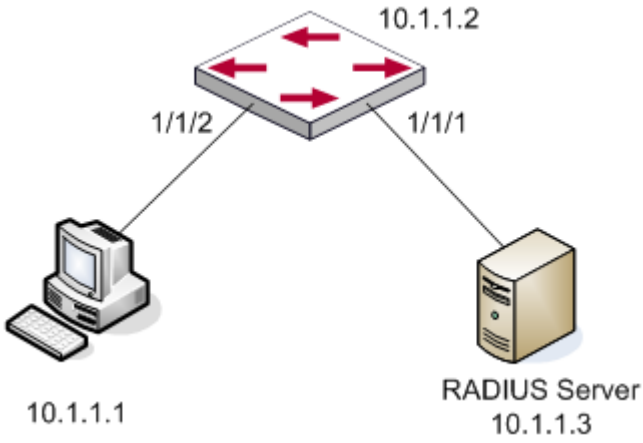

Рисунок 8 – Конфигурация 802.1x + RADIUS

Компьютер подключен к порту 2 программой. На порту включена функция аутентификации IEEE802.1, в качестве метода доступа по умолчанию используется аутентификация на основе MAC-адресов. IP-адрес программы 10.1.1.1. По умолчанию портами аутентификации и учета сетевых сервисов являются соответственно порт 1812 и порт 1813. Для выполнения аутентификации IEEE802.1x в компьютере установлено клиентское ПО.

```
(Switch) (Config)#radius server host auth "10.1.1.3" name "Default-RADIUS-Server"
(Switch) (Config)#radius server key auth "10.1.1.3" encrypted
1941ca8d99fc9209eade226bd848b3b7050129ecc6f67cc6efb138dde1b408b7dedb295c1991feb
b897813fab859d6d538d52015eb26e45a87b3f1148bbd8686
(Switch) (Config)#interface 1/0/1
(Switch) (Interface 1/0/1)#dot1x port-control force-authorized
(Switch) (Interface 1/0/1)#description RADIUS_SERVER
(Switch) (Interface 1/0/1)#exit
```

```
(Switch) (Config)#dot1x system-auth-control
(Switch) (Config)#aaa authentication dot1x default radius

(Switch) (Config)#show dot1x authentication-history 1/0/2
Time Stamp          Interface    MAC-Address       VLANID  Auth Status
------------------- ---------    ----------------  ------  ------------
Jan 01 1970 00:23:04  1/0/1    AC:22:0B:E7:BD:D9   3       Authorized
Jan 01 1970 00:22:41  1/0/1    AC:22:0B:E7:BD:D9   3       Authorized
Jan 01 1970 00:19:08  1/0/1    AC:22:0B:E7:BD:D9   3       Authorized
Jan 01 1970 00:15:48  1/0/1    AC:22:0B:E7:BD:D9   3       Authorized
Jan 01 1970 00:14:39  1/0/1    AC:22:0B:E7:BD:D9   3       Authorized

(Switch) (Config)#show dot1x clients 1/0/1
Logical Interface..... 0
Interface..... 1/0/2
User Name..... dot1xuser
Supp MAC Address..... AC:22:0B:E7:BD:D9
Session Time..... 630
VLAN Id..... 3
VLAN Assigned..... Default
Session Timeout..... 0
Session Termination Action..... Default
```

2.8 Настройка таблицы MAC адресов

2.8.1 Общие сведения о таблице MAC адресов

Таблица MAC-адресов — это таблица соответствий MAC-адресов устройств назначения портам программы. MAC адреса делятся на статические и динамические. Статические MAC адреса вручную сконфигурированы пользователем, имеют наивысший приоритет и действуют постоянно (они не могут быть замещены динамическим MAC адресами). Динамические адреса запоминаются программой при передаче пакетов данных, и они действуют ограниченное время. Когда программа получает фрейм данных для пересылки, он сохраняет MAC адрес источника фрейма и соответствующий ему порт назначения. Когда таблица MAC адресов опрашивается на предмет MAC адреса приемника, при нахождении нужного адреса, пакет данных отправляется на соответствующий порт, в противном случае программа пересылает пакет на свой

широковещательный домен. Если динамический MAC адрес не встречается в пакетах для пересылки длительное время, запись о нем удаляется из таблицы MAC адресов программы.

Для таблицы MAC адресов определены две операции:

1) Получение MAC адреса;

2) Отправка или фильтрация пакета данных в соответствии с таблицей MAC адресов.

Получение таблицы MAC адресов

Таблица MAC адресов может быть построена статически или динамически. Статическим конфигурированием настраивается соответствие между MAC адресами и портами. Динамическое обучение – это процесс, когда программа изучает связи между MAC адресами и портами и регулярно обновляет таблицу MAC адресов. В этой секции мы остановимся на процессе динамического построения таблицы MAC адресов, показанного на рисунке 9.

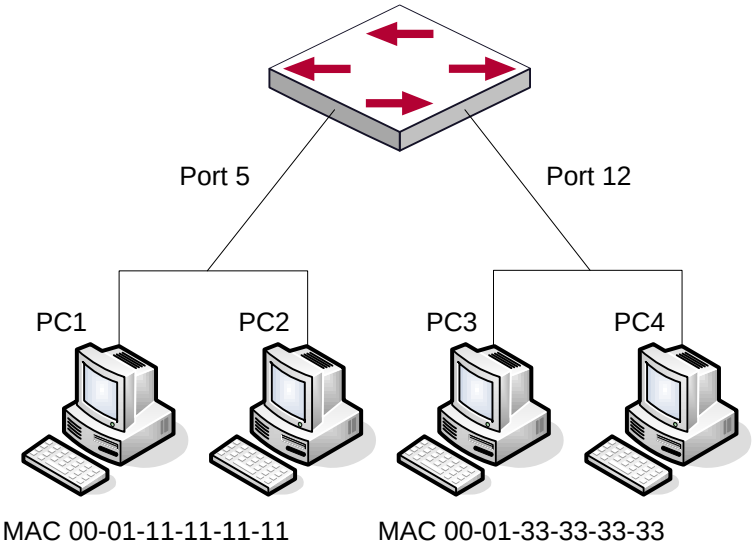

Рисунок 9 – Динамическое построение таблицы MAC адресов

Топология на рисунке 9: 4 компьютера подключены к программе, где PC1 и PC2 принадлежат одному физическому сегменту(домену коллизий), физический сегмент подключен к порту 1/0/5 программы, PC3 и PC4 принадлежат к другому физическому сегменту, подключенному к порту 1/0/12 программы.

Начальная таблица MAC адресов не содержит никаких значений. Возьмем для примера процесс связи между PC1 и PC3. Процесс обучения MAC адресам следующий:

1) Когда PC1 посылает сообщение к PC3, MAC адрес источника 00-01-11-11-11-11 и порт 1/0/5 из этого сообщения заносятся в таблицу MAC адресов программы.

2) В то же время программу надо понять, как доставить сообщение на адрес 00-01-33-33-

33-33. Так как таблица содержит запись только для адреса 00-01-11-11-11-11 и порта 1/0/5, а для адреса 00-01-33-33-33-33 никаких записей нет, программа рассылает данное сообщение на все свои порты (предполагаем, что все порты принадлежат по умолчанию VLAN1).

3) PC3 и PC4 получают сообщение, посланное PC1, но PC4 не отвечает на это сообщение, так как адрес приемника 00-01-33-33-33-33, и отвечать на него будет только PC3. Когда порт 1/0/12 получает сообщение, отправленное PC3, в таблицу MAC адресов добавляется запись о MAC адресе 00-01-33-33-33-33 и соответствующем ему порте 1/0/12.

4) Теперь таблица MAC адресов имеет две динамические записи: MAC адрес 00-01-11-11-11-11 – порт 1/0/5 и 00-01-33-33-33-33 – порт 1/0/12.

5) После обмена пакетами между PC1 и PC3, программа больше не получает пакетов, отправленных PC1 и PC3. И записи в таблице MAC адресов, соответствующие этим устройствам удаляются через 300 или 2*300 секунд (т.е. простое или двойное время жизни). 300 секунд здесь это время жизни по умолчанию для записей в таблице MAC адресов. Время жизни может быть изменено на программе.

Пересылка или фильтрация кадров

Программа посылает или отфильтровывает принимаемые пакеты данных в соответствии с таблицей MAC адресов. Рассматривая для примера рисунок выше, предполагаем, что программа изучил адреса PC1 и PC3, и пользователь вручную настроил соответствие портов для PC2 и PC4.

MAC адреса программы показаны в таблице 1.

Таблица 1 – MAC адреса программы

MAC адрес	Номер порта	Кем добавлена запись
00-01-11-11-11-11	1/0/5	Динамическое обучение
00-01-22-22-22-22	1/0/5	Статическая конфигурация
00-01-33-33-33-33	1/0/12	Динамическое обучение
00-01-44-44-44-44	1/0/12	Статическая конфигурация

1) Отправка пакетов в соответствии с таблицей MAC адресов

Если PC1 посылает пакет к PC3, программа отправляет данные, полученные с порта 1/0/5 на порт 1/0/12

2) Фильтрация данных в соответствии с таблицей MAC адресов

Если PC1 посылает сообщение PC2, программа, проверив таблицу MAC адресов, находит PC2 и PC1 в одном физическом сегменте и отфильтровывает это сообщение (то есть сбрасывает это сообщение).

Программой могут пересылаться три типа фреймов:

– широковещательные фреймы;

– многопользовательские фреймы;

– однопользовательские фреймы.

Далее описывается, как программа работает со всеми тремя типами пакетов:

1) Широковещательный фрейм: Программа может определять коллизии в домене, но только не для широковещательных доменов. Если VLAN не установлены, все устройства, подключенные к программау считаются находящимися в одном широковещательном домене. Когда программа получает широковещательный фрейм, он пересылает его во все порты. Если VLANы сконфигурированы, таблица MAC адресов адаптируется в соответствии с дополнительной информацией о VLANax. В этом случае программа отправляет фрейм только на порты, находящиеся в том же VLANe.

2) Многопользовательский фрейм: Если многопользовательский домен неизвестен, программа рассылает фрейм в том же VLANe, но если включена функция IGMP snooping или сконфигурирована статическая многопользовательская группа, программа будет посылать этот фрейм в порты многопользовательской группы.

3) Однопользовательский фрейм: если VLANы не сконфигурированы, то, если MAC адрес приемника есть в таблице MAC адресов программы, программа напрямую пересылает пакет в соответствующий порт. Если же адрес приемника в таблице не найден, программа делает широковещательную рассылку этого фрейма. Если VLANы сконфигурированы, программа рассылает однопользовательский фрейм только внутри одного VLANa. Если MAC адрес найден в таблице, но принадлежит другому VLANy, программа делает широковещательную рассылку фрейма в том VLANe, к которому принадлежит фрейм.

2.8.2 Дополнительные функции таблицы MAC адресов.

Большинство программ поддерживают режим обучения MAC адресам. Каждый порт может динамически запомнить несколько MAC адресов, таким образом, возможна передача потоков данных между известными MAC адресами внутри порта. Если срок жизни MAC адреса истек, пакет, направленный на этот адрес, будет разослан широковещательно.

Другими словами, MAC-адрес, которому обучился порт, будет использоваться для передачи пакетов к этому порту. Если соединение переключено на другой порт,

программа снова выполнит обучение MAC-адресу и будет передавать данные новому порту.

Однако, в некоторых случаях политика управления или секретности может требовать, чтобы MAC адреса были прикреплены к портам, и только потоки с привязанных MAC адресов будут пропускаться к пересылке на порт. То есть, после привязки MAC адреса к порту, в этот порт могут передаваться только данные, предназначенные для данного MAC адреса. Потоки данных, предназначенные для других MAC адресов, не привязанных к данному порту, не будут пропускаться через порт.

Пример конфигурирования привязки и ограничения MAC адресов.

(Switch) (Interface 1/0/17)#port-security mac-address 00:01:00:00:00:01 1 - привязка MAC адреса к интерфейсу.

(Switch) (Interface 1/0/17)#port-security max-static X – где X максимальное количество mac адресов на порту.

(Switch) (Interface 1/0/17)#interface 1/0/10

(Switch) (Interface 1/0/10)#port-security max-dynamic 10

(Switch) (Config)#show mac-addr-table

VLAN ID	MAC Address	Interface	IfIndex	Status
1	00:01:00:00:00:01	1/0/17	17	Static

(Switch) (Config)#show mac-addr-table count

Dynamic Address count..... 1

Static Address (User-defined) count..... 1

Total MAC Addresses in use..... 2

Total MAC Addresses available..... 16384

2.9 Настройка QoS

2.9.1 Общие сведения о QoS

QoS (Quality of Service – качество сервиса) - набор возможностей, которые позволяют создавать разделенные полосы для передаваемых по сети данных, тем самым обеспечивая лучший сервис для выбранного сетевого трафика. QoS - гарантия качества последовательной и предсказуемой передачи данных для обеспечения требований программ. QoS не создает дополнительной полосы передачи, но обеспечивает более

эффективное управление полосой в соответствии с требованиями приложений и политикой управления сетью.

QoS: Качество сервиса, обеспечение гарантированного качества сервиса для последовательной и предсказуемой передачи данных и выполнения требований программ.

Домен QoS: Домен QoS поддерживает устройства с QoS для формирования сетевой топологии, которая обеспечит качество сервиса. Такая топология называется доменом QoS.

CoS: Класс сервиса - классификационная информация, передаваемая фреймами 802.1Q на втором уровне. Занимает три бита поля Tag в заголовке фрейма и называется уровнем пользовательского приоритета в диапазоне от 0 до 7.

На рисунке 10 показаны приоритеты Класса сервиса.

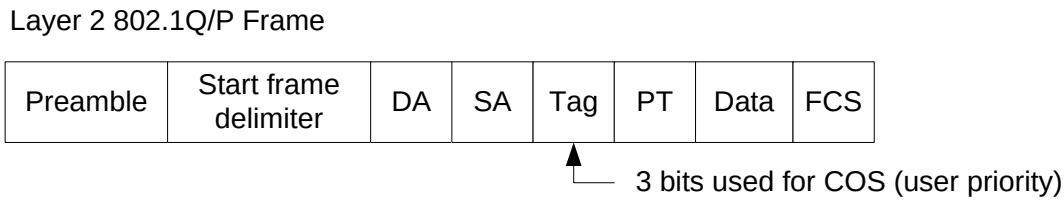

Рисунок 10 – Приоритеты Класса сервиса

ToS: Тип сервиса. Однобайтовое поле, передаваемое в заголовке пакета IPv4 на третьем уровне для объявления типа сервиса IP пакета. Значением поля ToS может быть приоритет IP (IP Precedence) или значение DSCP.

На рисунке 11 показан приоритет ToS.

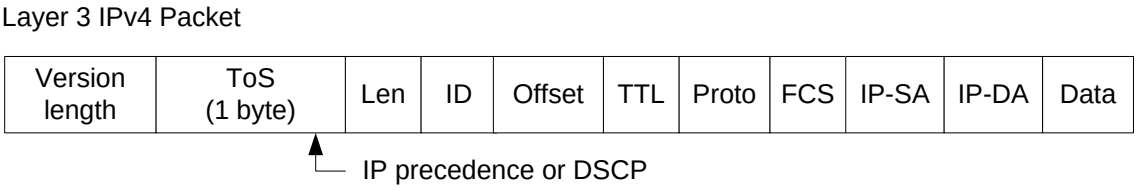

Рисунок 11 – Приоритет ToS

IP Precedence: Приоритет IP. Классификационная информация передающаяся в заголовке пакета третьего уровня, занимающая 3 бита и могущая принимать значения от 0 до 7.

DSCP (Differentiated Services Code Point): коды разделенных сервисов, классификационная информация, передающаяся в заголовке IP пакета третьего уровня, занимает 6 бит, имеет значение от 0 до 63 и обратно совместима с приоритетом IP.

MPLS TC(EXP) :

Поле MPLS означает класс обслуживания, имеет 3 бита для диапазона от 0 до 7. На рисунке 12 изображено поле MPLS.

Рисунок 12 – Поле MPLS

Internal Priority: Внутренний приоритет, устанавливаемый процессором программаа. Возможный диапазон значений зависит от типа процессора. Сокращенно - Int-Prio или IntP.

Drop Precedence: Приоритет сброса. При обработке пакетов первыми сбрасываются пакеты с большим приоритетом сброса. Имеет значение 0 или 1. Сокращенно обозначается Drop-Prec или DP.

Classification: основное назначение механизма QoS, классифицирует передаваемые пакеты в соответствии с классификационной информацией, содержащейся в пакетах и списками контроля доступа(ACL).

Policing: действие механизма QoS на входе, которое устанавливает политики трафика и управляет классифицированными пакетами.

Remark: действие механизма QoS на входе, выполняющее пропуск, остановку или сброс пакета в соответствии с политиками трафика.

Scheduling: действие механизма QoS на выходе. Добавляет пакеты в соответствующие исходящие очереди основываясь на внутреннем приоритете. И принимает решение о посылке или сбросе пакетов в соответствии с приоритетом сброса, алгоритмом посылки и важностью соответствующей очереди в исходящем потоке.

In-Profile: Траффик в рамках политики QoS(полоса пропускания или дополнительной полосой) называется In-Profile.

Out-of-Profile: Траффик в рамках политики QoS(полосы пропускания или дополнительной полосы) называется Out-of-Profile.

Для выполнения в программе программного QoS необходимо рассмотреть основную базовую модель. QoS не создает новой полосы в канале, но может максимально подстраивать конфигурацию текущих канальных ресурсов. Полная реализация QoS дает возможность полностью управлять сетевым трафиком. Ниже, как можно точнее, описывается сам принцип QoS.

Спецификация передачи данных в IP покрывает только адресацию и сервисы источника и приемника и, конечно, коррекцию передачи пакетов с помощью протоколов 4 уровня модели OSI и выше, таких как TCP. Однако, в большинстве случаев протокол IP использует максимально возможную пропускную способность вместо механизма поддержки и защиты полосы пакетной передачи. Это применимо для таких сервисов как почта и FTP, но при увеличении передачи мультимедийных коммерческих данных и электронных бизнес-сервисов, метод максимальной загрузки не может удовлетворить требования необходимой полосы и низких задержек.

Базируясь на различных методах, QoS определяет приоритет для каждого входящего пакета. Классификационная информация содержится в заголовках IP пакетов третьего уровня и в заголовках фреймов 802.1Q второго уровня. QoS обеспечивает одинаковый сервис для пакетов одинакового приоритета, в то время как для пакетов с различающимися приоритетами предлагаются различающиеся операции. Маршрутизатор или программа, поддерживающие сервис QoS, могут обеспечивать различную полосу передачи в соответствии с классификацией пакетов, помечать пакеты в соответствии с сконфигурированными политиками, а также сбрасывать некоторые низкоприоритетные пакеты в случае перегрузки полосы передачи.

Конфигурация QoS является гибкой, более простой или сложной в зависимости от топологии сети и устройств и глубины анализа входящего/исходящего трафика.

Базовая модель QoS, показанная на рисунке 13, состоит из 4 частей: Классификация, Применение политик, Пометка и Планирование, где классификация, применение политик и пометки – последовательные действия на входе, а работа с очередями и планирование – действия QoS на выходе.

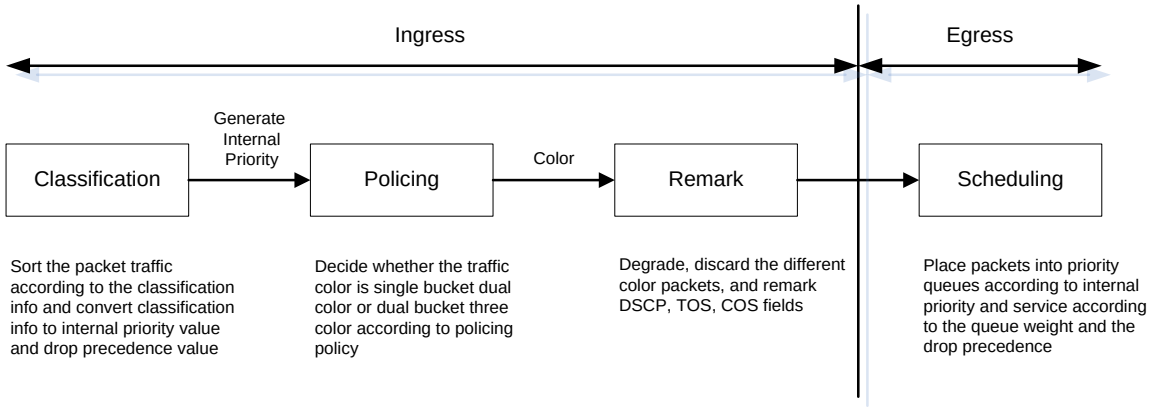

Рисунок 13 – Базовая модель QoS

Классификация: классифицирует трафик в соответствии с классификационной информацией пакетов и генерирует значение внутреннего приоритета, основанное на классификационной информации. Для различных типов пакетов классификация обеспечивается различным образом. На рисунке 14 показана схема процесса классификации.

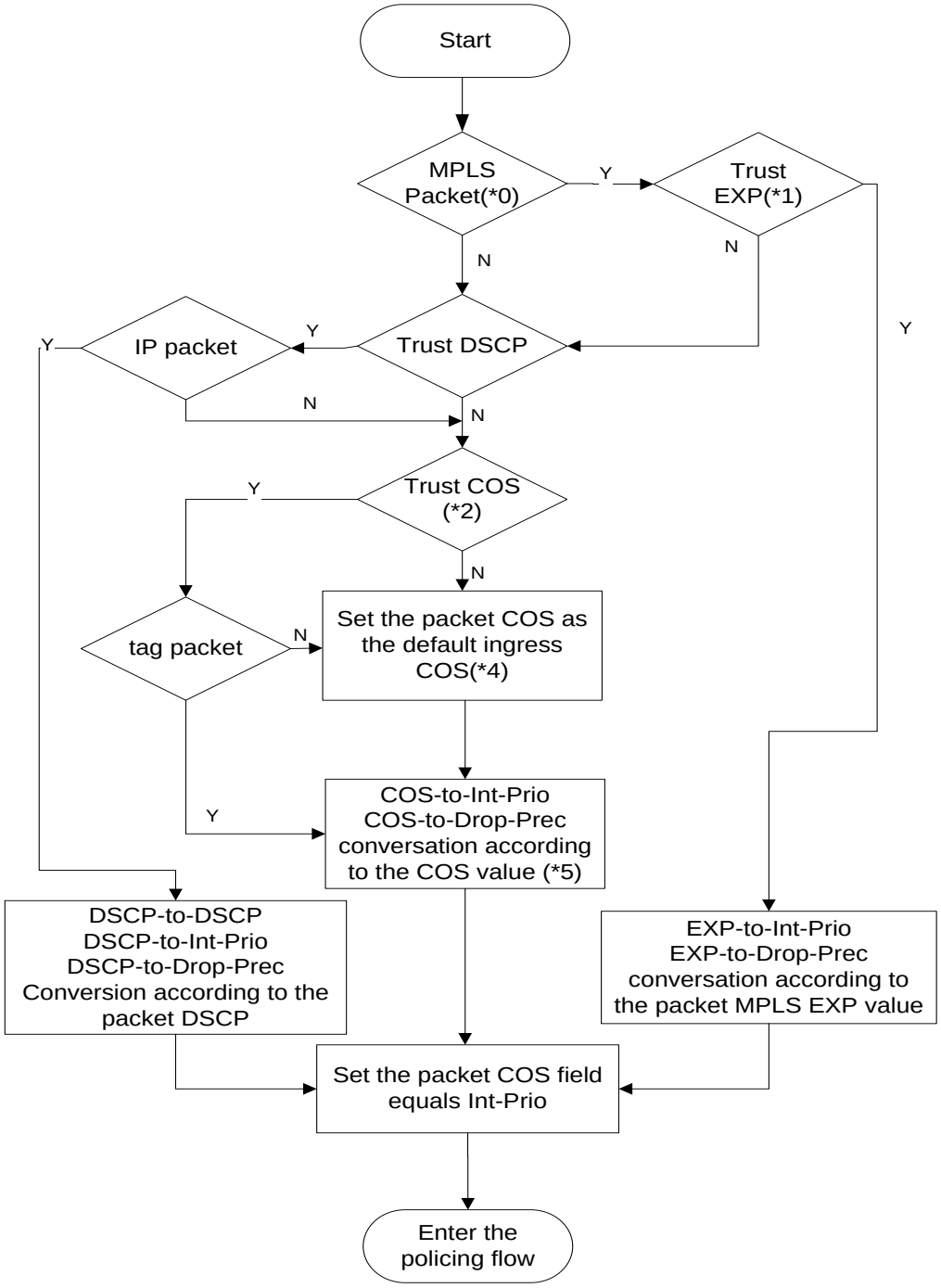

Рисунок 14 – Схема процесса классификации

Замечание 1: Значение CoS рассчитывается, исходя из свойств пакета, и никак не связано со значением внутреннего приоритета, полученным для потока.

Замечание 2: Если одновременно сконфигурированы проверка DSCP и CoS, то приоритет DSCP важнее COS.

Применение политик и пометка: Каждый пакет в классифицированном входящем трафике получает значение внутреннего приоритета и может далее подвергаться действию политик и помечаться.

Применение политик может быть выполнено на потоке данных для обеспечения различной полосы пропускания для различных классов трафика. Назначенная пропускная политика может быть «одна корзина-два цвета» (single bucket dual color) или «две корзины-три цвета» (dual bucket three color). Трафику присваиваются различные цвета, и в соответствии с ними он может сбрасываться или пропускаться. К пропущенным пакетам применяется действие пометки, когда пакету назначается новый, более низкий внутренний приоритет для замены существовавшего ранее более высокого внутреннего приоритета. Процессы регулирования и пометки показаны на рисунке 15.

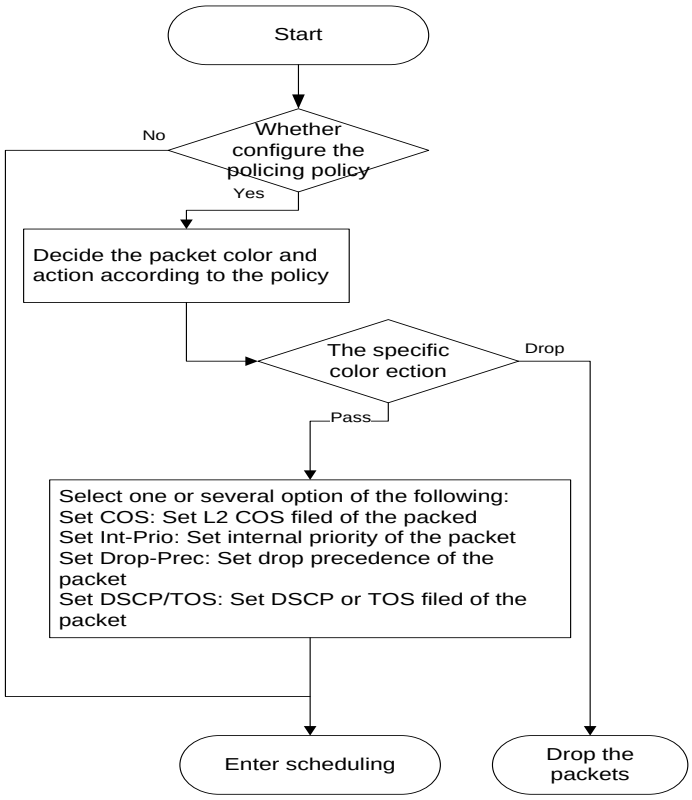

Рисунок 15 – Процессы регулирования и пометки

Замечание 1. Внутренний приоритет будет скрыт после установки. Установка внутреннего приоритета, установленного на трафик с определенным цветом, покрывает установку внутреннего приоритета на трафик, не связанного с цветом.

Замечание 2. Сброс внутреннего приоритета пакетов осуществляется в соответствии с картой преобразования «внутренний приоритет - внутренний приоритет»

(IntP-to-IntP). При классификации потока внутренний приоритет берется от источника или устанавливается действиями, не связанными с цветом.

Работа с очередями и планирование: существует внутренний приоритет для исходящих пакетов, в соответствии с ним планируется распределение пакетов по очередям с различным приоритетом и пакеты посылаются в соответствии с весовым приоритетом очереди и приоритетом сброса. На рисунке 16 показана схема планировки и управления очередями.

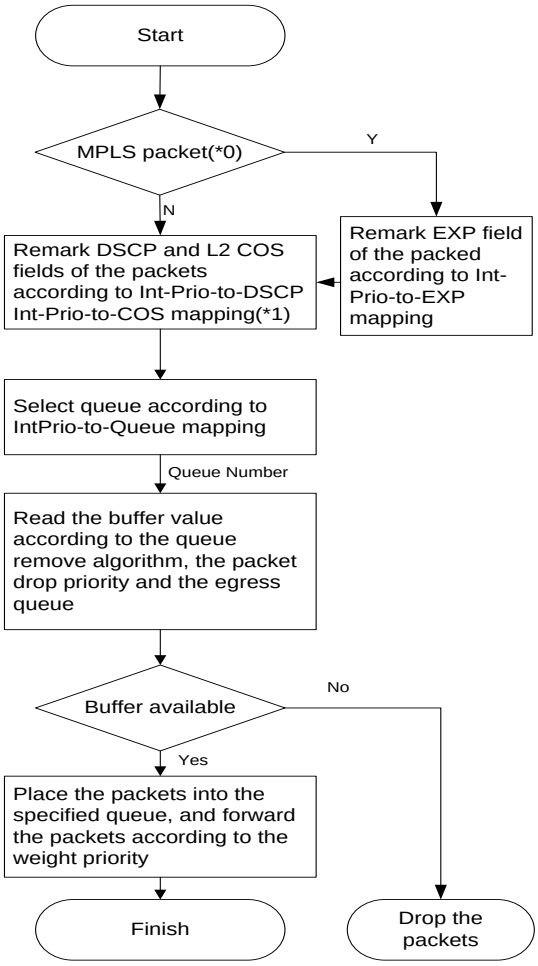

Рисунок 16 – Схема планировки и управления очередями

2.9.2 Пример насторойки QoS

Необходимо включить функцию QoS и установить на порту режим доверительного CoS без изменения значения DSCP

Этапы конфигурирования описаны ниже:

(Config)#interface 1/0/2

(Interface 1/0/2)#classofservice trust dot1p

(Config)#interface 1/0/2

(Interface 1/0/3)#classofservice trust ip-dscp

(Interface 1/0/3)#classofservice dot1p-mapping 5 7

(Config)#classofservice ip-dscp-mapping af41 4

switch# show classofservice dot1p-mapping 1/0/2

User Priority	Traffic Class
0	0
1	0
2	1
3	2
4	3
5	4
6	5
7	6

switch# show classofservice ip-dscp-mapping

IP DSCP	Traffic Class
0(be/cs0)	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8(cs1)	0
.....	
58	3
59	3
60	3

61 3

62 3

63 3

Пример конфигурирования алгоритма обработки очередей

(switch) (Interface 1/0/3)#cos-queue strict 6

(switch) (Interface 1/0/3)#cos-queue min-bandwidth 0 0 0 0 0 0 0

(switch) (Interface 1/0/3)#show interfaces cos-queue 1/0/3

Interface..... 1/0/3

Interface Shaping Rate..... 0

Queue ID	Min. Bandwidth	Scheduler Type	Queue Management Type
0	0	Weighted	Tail Drop
1	0	Weighted	Tail Drop
2	0	Weighted	Tail Drop
3	0	Weighted	Tail Drop
4	0	Weighted	Tail Drop
5	0	Weighted	Tail Drop
6	0	Strict	Tail Drop

2.10 Конфигурирование зеркалирования портов

2.10.1 Введение в зеркалирование портов

Функция зеркалирования включает в себя зеркалирование портов и зеркалирование потоков. Зеркалирование портов представляет собой дублирование кадров данных, посылаемых/принимаемых одним портом, на другом порту. Дублированный порт — это порт-источник зеркального порта, дублирующий его порт — это зеркальный порт (порт назначения). К зеркальному порту обычно подключают анализатор протоколов (например, Sniffer) или средства мониторинга RMON, осуществляющие мониторинг, диагностику и управление сетью.

При зеркалировании потоков программа точно копирует полученные пакеты или передаваемые в рамках правил от одного порта к другому. Эффективность зеркалирования потоков возможна в случае задания специальных правил.

В настоящее время каждый программа может устанавливать множество зеркалированных сессий. Число портов-источников для зеркального порта не ограничено, может использоваться как один порт, так и несколько. Порты-источники могут принадлежать как одной и той же VLAN, так и разным VLAN. Порт назначения и порты-источники могут принадлежать разным VLAN.

2.10.2 Пример конфигурации зеркалирования портов:

Конфигурация следующая: для мониторинга на интерфейсе 1/0/1 фреймы с данными рассылаются интерфейсом 1/0/3 и получаются интерфейсом 1/0/2.

1) Настройте интерфейс 1/0/1 как интерфейс зеркалирования пункта назначения.

2) Настройте интерфейс 1/0/3 как интерфейс входящего потока и интерфейс 1/0/2 как интерфейс исходящего потока для источника зеркалирования.

Шаги конфигурации следующие:

```
(Config)#monitor session 1 destination interface 1/0/1
(Config)#monitor session 1 source interface 1/0/3
(Config)#monitor session 1 mode
```

2.11 Конфигурация DHCP/ARP Snooping

2.11.1 Введение в DHCP/ARP Snooping

DHCP Snooping означает, что программа наблюдает за процессом присвоения IP адресов по протоколу DHCP. Это предотвращает появление нелегальных DHCP серверов и DHCP атаки путем настройки доверенных и недоверенных портов. DHCP сообщение с доверенных портов передается без проверки. При типичной конфигурации доверенные порты используются для подключения DHCP сервера или DHCP ретранслятора, а к недоверенным портам подключаются клиенты. С недоверенных портов программа будет

пересылать только DHCP запросы, но не ответы. Если с недоверенного порта получено сообщение DHCP ответа, программа поднимет тревогу и предпримет определенные действия с портом, согласно настройкам, например выключение или создание «черной дыры».

Если включена привязка DHCP Snooping, программа сохранит в соответствующей таблице связующую информацию о каждом DHCP клиенте с не доверенного порта (включая MAC адрес, IP адрес, аренду IP, номера VLAN и порта). Имея такую информацию DHCP Snooping можно комбинировать с другими модулями, такими, как dot1x и ARP, или самостоятельно реализовать контроль доступа пользователей

2.11.2 Типовое применение DHCP Snooping

Типовое применение DHCP Snooping показано на рисунке 17.

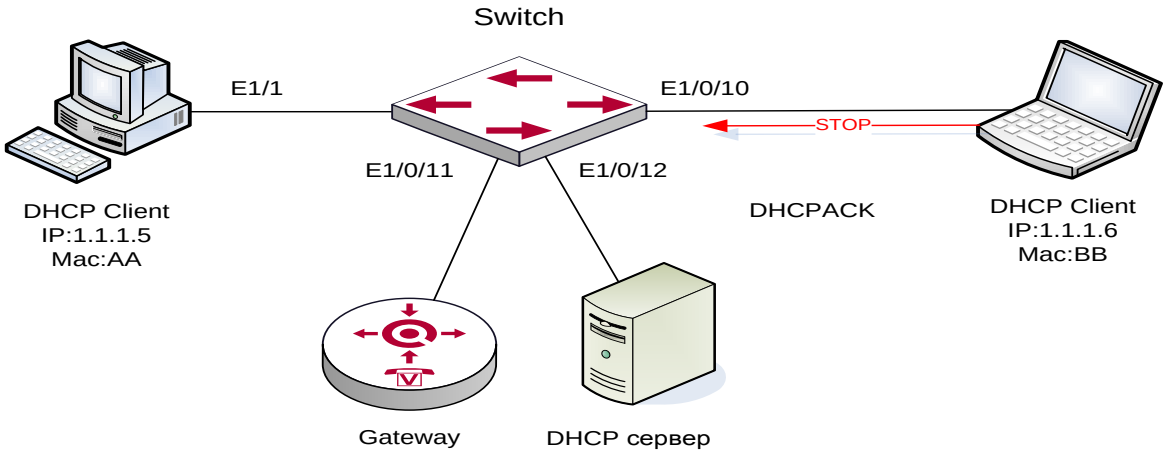

Рисунок 17 – Типовое применение

Как показано на рисунке 17, устройство Mac-AA – обычный пользователь, подключенный к недоверенному порту 1/0/1 программы, получает IP настройки через DHCP, IP адрес клиента 1.1.1.5. DHCP сервер и шлюз подключены к доверенным портам программы, 1/0/11 и 1/0/12 соответственно. Злоумышленник Mac-BB, подключенный к недоверенному порту 1/0/1 программы, пытается подделать DHCP сервер (посылая пакеты DHCPACK). Функция DHCP Snooping на программе эффективно обнаружит и блокирует такой тип сетевой атаки.

Последовательность настройки:

switch#

switch#config

switch(config)#ip dhcp snooping

switch(config)# ip dhcp snooping vlan 1

switch(config)#ip arp inspection vlan 1

switch(config)#interface ethernet 1/0/11

```
switch(Config-If-Ethernet1/1/0/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/1/0/11)# ip arp inspection trust
switch(Config-If-Ethernet1/0/11)#exit
```

2.12 Конфигурирование NTP

2.12.1 Введение в NTP

Протокол NTP (Network Time Protocol) выполняет синхронизацию хронометража в LAN/WAN сетях между распределёнными серверами времени и клиентами с точностью до миллисекунд. Реализация протокола описывается стандартом RFC 1305.

Целью использования протокола NTP является сохранение постоянного хронометража на всех сетевых устройствах для обеспечения эффективного функционирования различных приложений, использующих точную синхронизацию времени.

2.12.2 Пример использования NTP

Клиентская программа синхронизирует время с сетевым сервером времени, которых в локальной сети находится двое. Один сервер времени используется в качестве хоста, другой находится в режиме ожидания. На рисунке 18 показан процесс синхронизации программы.

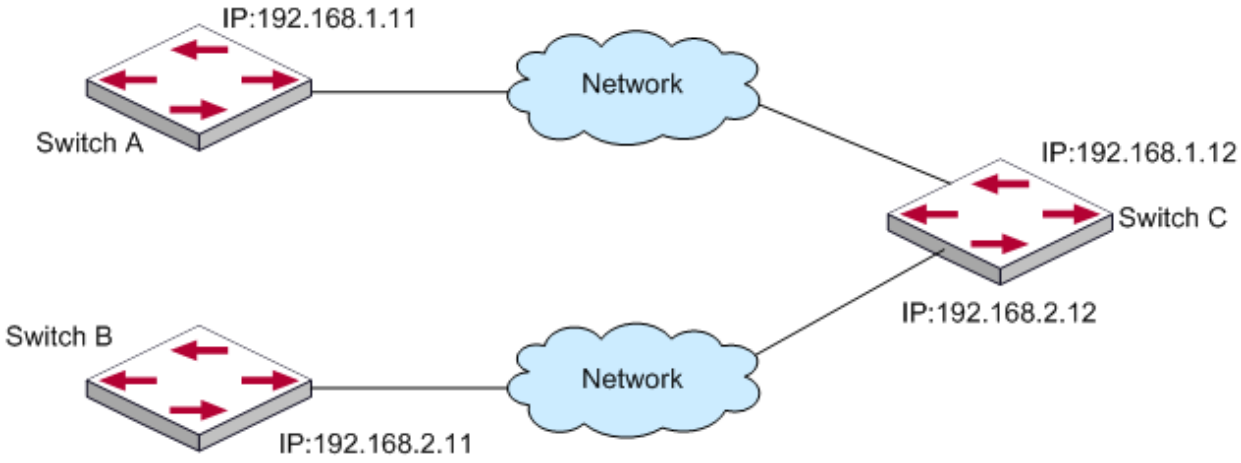

Рисунок 18 – Процесс синхронизации программы

Шаги конфигурации следующие:

```
(Switch) (Config)#sntp client mode unicast
(Switch) (Config)#sntp server 192.168.1.12
(Switch) (Config)#clock timezone 3 minutes 0
```

2.13 Конфигурирование SYSLOG

2.13.1 Введение в SYSLOG

Системные сообщения обеспечивают управляемый вывод наиболее важной информации, которая может быть эффективно отфильтрована за счет использования развитых средств классификации информации. В сочетании с программой отладки, вывод системных сообщений обеспечивает для администраторов и разработчиков всестороннюю поддержку по мониторингу и диагностике проблем в сети.

Вывод системных сообщений программы позволяет:

– передавать системные сообщения по четырем направлениям: на консоль, терминал Telnet, Dumb-терминал (монитор), logbuf и loghost;

– разделять информацию системных сообщений в зависимости от ее значимости на четыре уровня и осуществлять фильтрацию информации по уровням;

– структурировать информацию системных сообщений по различным модулям-источникам и осуществлять фильтрацию информации по модулям.

В настоящее время системные сообщения программаа можно выводить по пяти направлениям (логическим каналам):

– на локальную консоль через порт Console;

– на удаленный терминал Telnet или Dumb-терминал, используемые для удаленной эксплуатации и обслуживания;

– на закрепленный буфер отчетов или в буферную память программы, размер которой достаточен для хранения информации системных сообщений.

– на сконфигурированный хост системных сообщений (loghost). Система создания системных сообщений будет напрямую отправлять системные сообщения на loghost и сохранять их на этом хосте в виде файла, из которого по требованию информация может быть извлечена для просмотра.

2.13.2 Пример настройки вывода системных сообщений на удаленный SYSLOG сервер

Пусть при управлении VLAN IPv4-адрес программы равен 100.100.100.5, а IPv4-адрес удаленного сервера системных сообщений равен 100.100.100.1. Требуется послать системные сообщения на этот сервер и сохранить их в оборудовании записи системных сообщений.

```
switch(config)# logging syslog
switch(config)# logging host "100.100.100.1" ipv4 514 info
```

2.14 КОНФИГУРИРОВАНИЕ ACL

2.14.1 Введение в ACL

Списки управления доступом ACL (Access Control List) — это механизм фильтрации пакетов, используемый программой для управления сетевым трафиком путем разрешения или запрета прохождения его через программа, что значительно повышает безопасность сети. Пользователь может задать набор правил обработки пакетов, несущих ту или иную конкретную информацию, в каждом правиле указаны операции (разрешить или запретить прохождение пакета), которые необходимо применить, если обнаружено, что пакет содержит соответствующую информацию. Пользователь может применять эти правила к входящим и исходящим потокам портов, при этом потоки данных соответствующих направлений в заданном порту будут удовлетворять назначенным для них правилам ACL.

Список доступа — это последовательность условий, соответствующих конкретному правилу. Каждое правило содержит фильтрующую информацию и выполняемую операцию. Информация правила представляет собой комбинацию условий воздействия, например, IP-адреса источника и назначения, номер IP-протокола и TCP порта. Списки доступа могут быть классифицированы по следующим критериям:

Критерий на основе фильтрующей информации: Список доступа по IP-адресам (информация уровня 3 и более высоких уровней), список доступа по MAC-адресам (информация уровня 2), список доступа на основе MAC- IP- адресов (уровни 2 или 3, либо более высокие уровни).

Критерий сложности настройки: стандартная, расширенная настройка. При расширенной настройке применяется более специфическая фильтрующая информация.

Критерий на основе номенклатуры: По номерам, по именам.

В содержании списка доступа должны быть отражены три аспекта, перечисленные выше.

Имеется всего две операции списков доступа (они же являются операциями, назначенными по умолчанию): “permit” (разрешить) и “deny” (запретить). Применяются следующие правила:

Список доступа может содержать несколько правил. При фильтрации пакеты проверяются на соответствие условиям правил, начиная с первого. Если при проверке определенного правила достигается соответствие, остальные правила не обрабатываются, они игнорируются.

Операции, определенные глобально, применяются в портах только к входящим IP-пакетам. Для IP-пакетов, не являющихся входящими, а также для всех исходящих пакетов, операцией, назначенной по умолчанию, является “permit”.

2.14.2 Примеры конфигурирования ACL

Пользователь предъявляет следующие требования к конфигурированию: порт 1/10 программы присоединен к сегменту 10.0.0.0/24, использование FTP-протокола нежелательно.

Шаги конфигурации следующие:

1) Создать соответствующий список доступа ACL.

2) Настроить функцию фильтрации пакетов.

3) Привязать список доступа ACL к порту.

Примеры настройки:

запретить передачу FTP пакетов принимаемых на порт 1/0/2

```
(Switch) (Config)#ip access-list ftp
(Switch) (Config-ipv4-acl)#deny tcp any eq ftp any
(Switch) (Config-ipv4-acl)#exit
(Switch) (Config)#interface 1/0/2
(Switch) (Interface 1/0/2)#ip access-group ftp in 1
(Switch) (Interface 1/0/2)#exit
```

запретить передачу любых пакетов с адресом источника 00:11:22:33:00:01 принимаемых на порт 1/0/1

```
(Switch) (Config)#mac access-list extended src_mac
(Switch)  (Config-mac-access-list)#deny  00:11:22:33:00:01
00:00:00:00:00:00 any
(Switch) (Config-mac-access-list)#permit any any
(Switch) (Config-mac-access-list)#exit
(Switch) (Config)#interface 1/0/1
(Switch) (Interface 1/0/1)#mac access-group src_mac in 1
(Switch) (Interface 1/0/1)#exit
```

запретить передачу пакетов с IP адресом назначения 10.1.1.10 принимаемых на порт 1/0/10

```
(Switch) (Config)#ip access-list dest_ip
(Switch) (Config-ipv4-acl)#deny ip any host 10.1.1.10
(Switch) (Config-ipv4-acl)#permit ip any any
(Switch) (Config-ipv4-acl)#exit
(Switch) (Config)#interface 1/0/10
```

```
(Switch) (Interface 1/0/10)#ip access-group dest_ip in 1
(Switch) (Interface 1/0/10)#exit
```

1. УПРАВЛЕНИЕ ПРОГРАММОЙ

1.1. Варианты управления

Для управления необходимо настроить программу. Программа обеспечивает два варианта управления: внеполосное (out-of-band) или внутриполосное (in-band).

3.1.1 Внеполосное управление

Внеполосное управление — это управление через консольный интерфейс. Внеполосное управление, в основном используется для начального конфигурирования программы, либо когда внутриполосное управление недоступно. Например, пользователь может через консольный порт присвоить программе IP-адрес для доступа по Telnet.

Процедура управления программой через консольный интерфейс, описана ниже:

Шаг 1: Подключить персональный компьютер к консольному (серийному) порту программы.

Подключение ПК к консольному порту программы показано на рисунке 19.

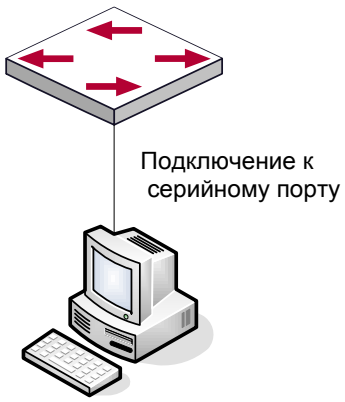

Рисунок 19 – Подключение ПК к консольному порту программы

Как показано выше, серийный порт (RS-232) подключен к программе через серийный кабель. В таблице 2 указаны все устройства, использующийся в подключении.

Таблица 2 – Устройства, использующиеся в подключении

Шаг 2: Включение и настройка HyperTerminal.

После установки соединения, запустите HyperTerminal, входящий в комплект Windows. Пример, приведенный далее, основан на HyperTerminal входящий в комплект Windows XP.

Название устройства	Описание
Персональный компьютер (PC)	Имеет функциональную клавиатуру и порт RS-232, с установленным эмулятором терминала, таким как HyperTerminal, входящий в комплект Windows 9x/NT/2000/XP.
Кабель серийного порта	Один конец подключается к серийному порту RS-232, а другой к порту консоли.
Программа	Требуется работающий консольный порт.

1) Нажмите «Пуск» (Start menu) – Все программы (All Programs) – Стандартные (Accessories) – Связь (Communication) – HyperTerminal.

На рисунке 20 показан запуск HyperTerminal.

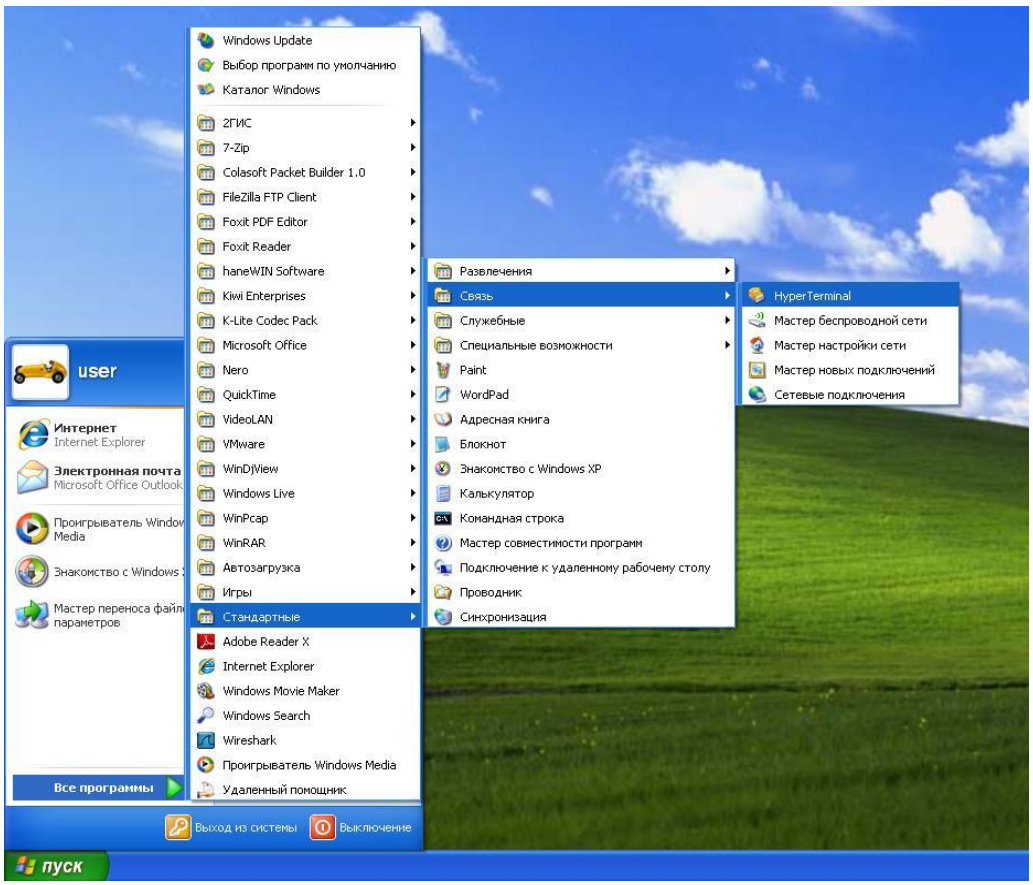

Рисунок 20 – Запуск HyperTerminal

2) Наберите имя для запущенного HyperTerminal, например «Switch».

На рисунке 21 показан запуск HyperTerminal.

Рисунок 21– Запуск HyperTerminal

3) В выпадающем меню «Подключение» выберите, серийный порт RS-232 который используется PC, например, COM1 и нажмите «OK» . На рисунке 22 показан запуск HyperTerminal.

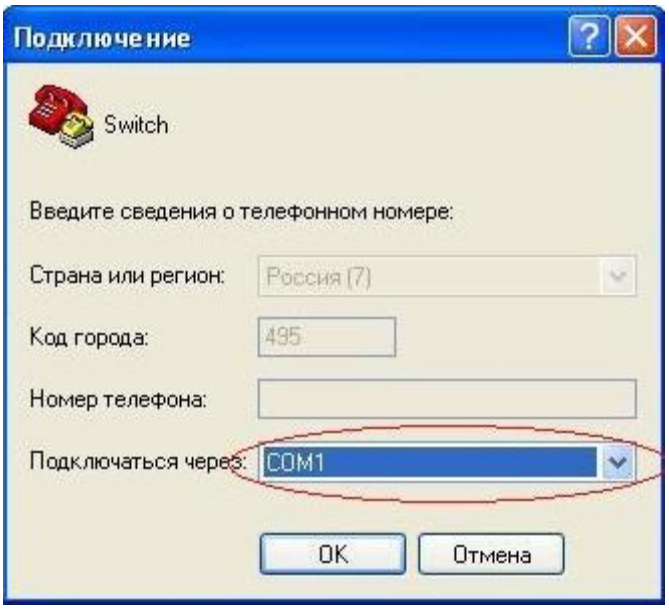

Рисунок 22 – Запуск HyperTerminal

4) Настройте свойства COM1 следующим образом: Выберите скорость «115200» для «Baud rate» ; «8» для» Data bits» ; «none» для «Parity checksum» ; «1» для «stop bit» ; «none» для «traffic control» ; или вы можете нажать» Restore default» , а после нажать «OK» .

На рисунке 23 – показан HyperTerminal.

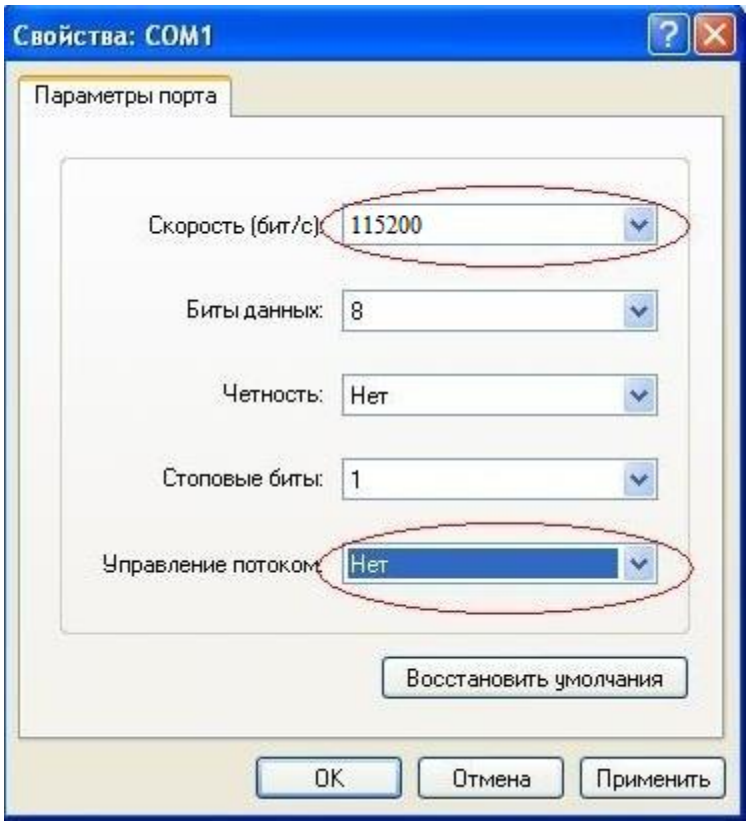

Рисунок 23 – HyperTerminal

Шаг 3: Вызов командного интерфейса (CLI) программы.

Включите программу, после чего следующие сообщения появятся в окне HyperTerminal – это режим конфигурации для программы.

Switch>

Теперь можно вводить команды управления программой. Детальное описание команд приведено в последующих главах.

3.1.2 Внутриполосное управление

Внутриполосное управление относится к управлению посредством доступа к программе с использованием Telnet, или HTTP, а также SNMP. Внутриполосное управление включает функции управления программы для некоторых устройств, подключенных к нему. В тех случаях, когда внутриполосное управление из-за изменений, сделанных в конфигурации программы, работает со сбоями, для управления и конфигурирования программы можно использовать внеполосное управление.

3.1.2.1 Управление по Telnet/SSH

Чтобы управлять программой по Telnet/SSH, должны выполняться следующие условия:

1) Программа должен иметь сконфигурированный IPv4/IPv6 адрес;

2) IP адрес хоста (Telnet/SSH клиент) и VLAN интерфейс программы должны иметь IPv4/IPv6 адреса в одном сегменте сети;

3) Если второй пункт не может быть выполнен, Telnet/SSH клиент должен быть подключен к IPv4/IPv6 адресу программы с других устройств, таких как маршрутизатор.

Последующие шаги описывают подключение Telnet/SSH клиента к интерфейсу VLAN1 программы посредством Telnet/SSH (пример адреса IPv4).
На рисунке 24 показано управление программой по Telnet/SSH.

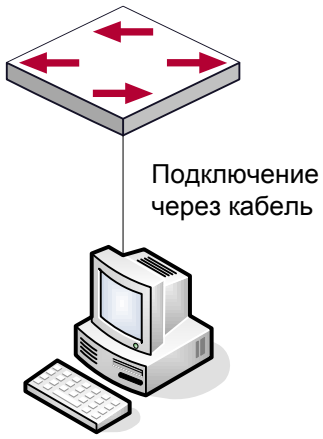

Рисунок 24 – Управление программой по Telnet/SSH

Шаг 1: Настройка IP адресов для программы и запуск функции Telnet/SSH Server в программе:

– первым делом идет настройка IP адреса хоста. Он должен быть в том же сегменте сети, что и IP адрес VLAN1 интерфейса программы. Предположим что IP адрес интерфейса VLAN1 программы 10.1.128.251/24. Тогда IP адрес хоста может быть 10.1.128.252/24. С помощью команды «ping 10.1.128.251» можно проверить доступна программа или нет;

– команды настройки IP адреса для интерфейса VLAN1 указаны ниже. Перед применением внутриполосного управления IP-адрес программы должен быть настроен посредством внеполосного управления (например, через порт Console). Команды конфигурирования следующие (далее считается, что все приглашения режима конфигурирования программы начинаются со слова «switch» , если отдельно не указано иного):

Switch>

Switch>enable

Switch#vlan database

Switch (Vlan)#vlan routing 1

Switch (Vlan)#exi

Switch #configure

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 10.1.128.251 255.255.255.0

Для активации функции Telnet/SSH сервера пользователь должен включить её, как показано ниже:

Switch>enable

Switch# ip telnet server enable

Switch# ip telnet port 23

Switch# show telnetcon

Remote Connection Login Timeout (minutes)..... 5

Maximum Number of Remote Connection Sessions... 4

Allow New Telnet Sessions..... Yes

Telnet Server Admin Mode..... Disable

Telnet Server Port..... 23

(switch) (Config)#crypto key generate rsa

(switch) (Config)#crypto key generate dsa

(switch) (Config)#exit

(switch) #ip ssh server enable

Шаг 2: Запуск программы Telnet Client

Необходимо запустить программу Telnet клиент в Windows с указанием адреса хоста. На рисунке 25 показан запуск программы Telnet клиент в Windows.

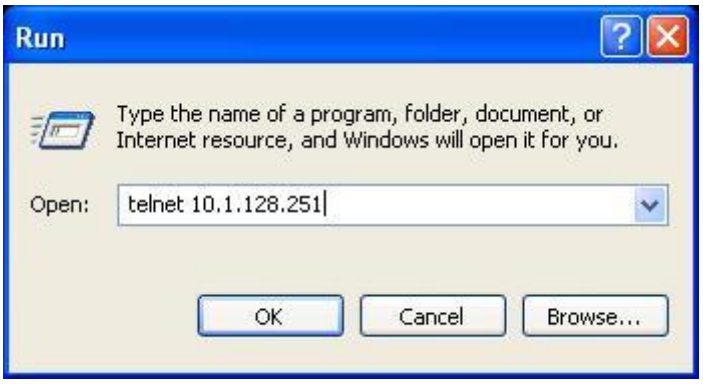

Рисунок 25 – Запуск программы Telnet клиент в Windows.

Шаг 3: Получить доступ к программе.

Для того что бы получить доступ к конфигурации через интерфейс Telnet необходимо ввести достоверный логин (login) и пароль (password). В противном случае в доступе будет отказано. Этот метод помогает избежать неавторизованного получения доступа.

Для доступа в привелигерованный режим необходимо задать уровень привилегий 15.

Допустим, авторизованный пользователь имеет имя «test» и пароль «test» , тогда процедура задания имени и пароля для доступа по Telnet:

Switch>enable

Switch#config

Switch#username test level 15 password

Enter new password:****

Confirm new password:****

После ввода имени и пароля для интерфейса конфигурирования Telnet, пользователь сможет вызвать командный интерфейс CLI настройки программы. Команды, используемые в командном интерфейсе Telnet CLI, которые становятся доступны после ввода имени и пароля — те же самые, что и в консольном интерфейсе. На рисунке 26 показана настройка Telnet интерфейса.

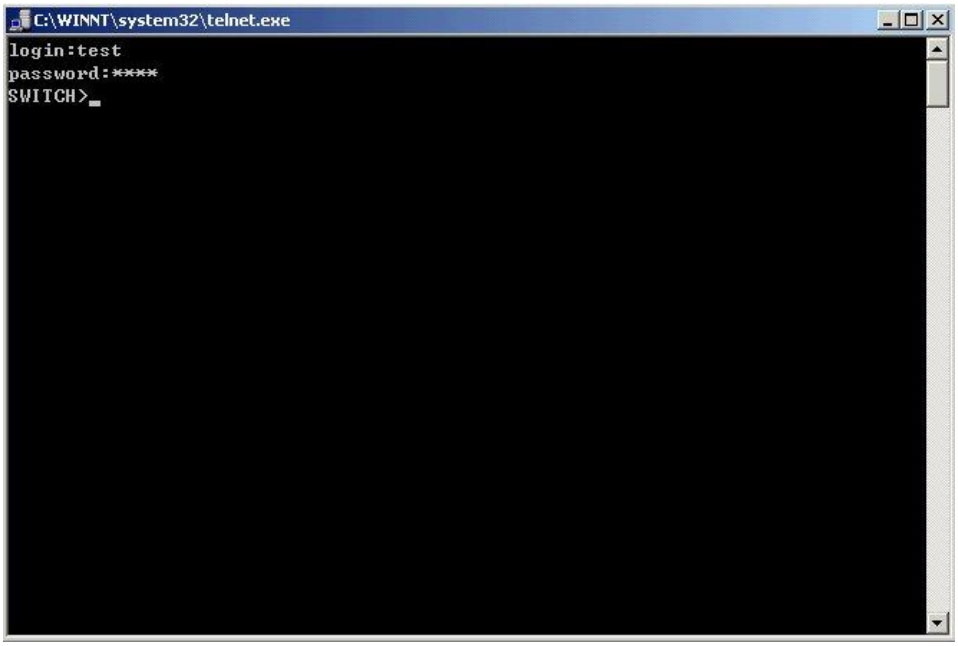

Рисунок 26 – Настройка Telnet интерфейса

3.1.2.2 Управление через HTTP

Чтобы управлять программой через Web-интерфейс должны быть выполнены следующие условия:

1) Программа должен иметь сконфигурированный IPv4/IPv6 адрес.

2) IP адрес хоста (HTTP клиент) и VLAN интерфейс программы, должны иметь IPv4/IPv6 адреса в одном сегменте сети.

3) Если второй пункт не может быть выполнен, HTTP клиент должен быть подключен к IPv4/IPv6 адресу программы с других устройств, таких, как маршрутизатор.

Как и в управлении программой через Telnet, как только удается ping/ping6 хоста к IPv4/IPv6 адресам программы и вводится правильный логин и пароль, возможно получить доступ к программе через HTTP. Ниже описан способ настройки:

Шаг 1: Настройка IP адресов для программы и запуск функции HTTP сервера.

О настройке IP-адреса программы с помощью внеполосного управления, смотри главу о настройке Telnet управления.

Шаг 2: Запуск Web-браузера на хосте.

Необходимо открыть Web-браузер на хосте и ввести IP адрес программы, или непосредственно запустить HTTP протокол в Windows. На рисунке 27 показан запуск HTTP протокола с IP адресом программы «10.1.128.251».

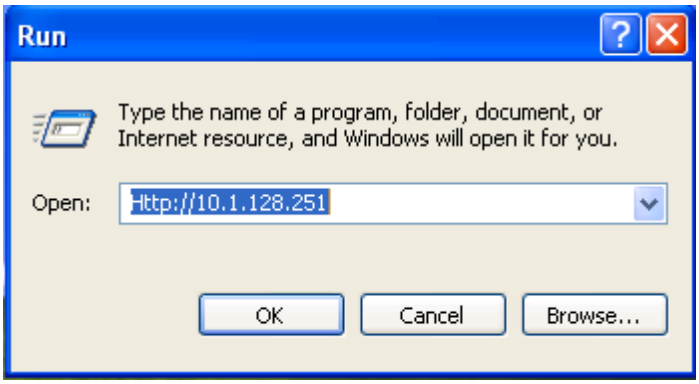

Рисунок 27 – Запуск HTTP протокола

При обращении программы с IPv6 адреса рекомендуется использовать браузер Firefox версии 1.5 или позднее. Например, если адрес программы 3ffe:506:1:2::3. Введите адрес IPv6 программы http:// [3ffe: 506:1:2:: 3], адрес обязательно должен быть заключен в квадратные скобки.

Шаг 3: Получение доступа к программе.

Для того чтобы получить доступ конфигурации с использованием WEB интерфейса, необходимо ввести достоверный логин (login) и пароль (password), в противном случае будет отказано в доступе. Этот метод помогает избежать неавторизованного доступа.

Для доступа в привелигерованный режим необходимо задать уровень привилегий 15.Допустим, авторизованный пользователь имеет имя «admin» и пароль «admin» , тогда процедура настройки следующая:

Switch>enable

Switch#config

Switch#username admin level 15 password

Enter new password:******

Confirm new password:******

Web интерфейс входа показан на рисунке 28.

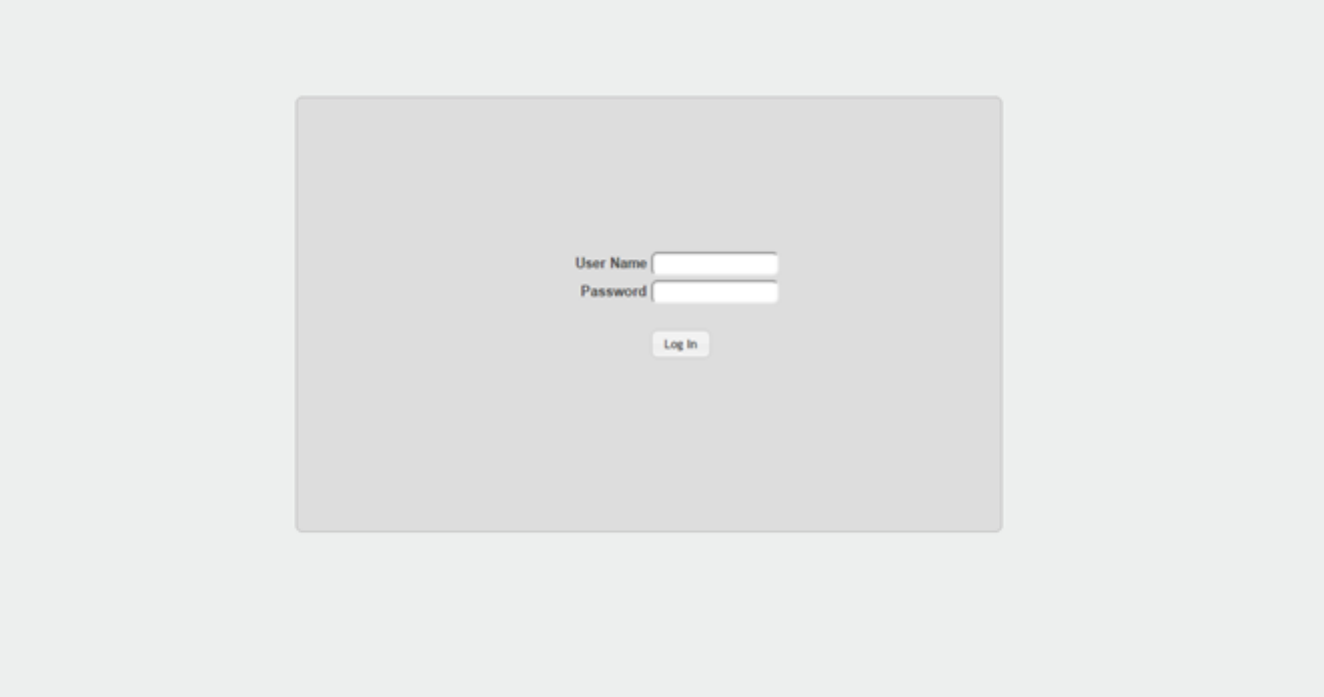

Рисунок 28 – Web интерфейс входа

Введите достоверные имя пользователя и пароль, затем вы попадете в главное меню настройки Web интерфейса.

Web интерфейс настройки порта показан на рисунке 29.

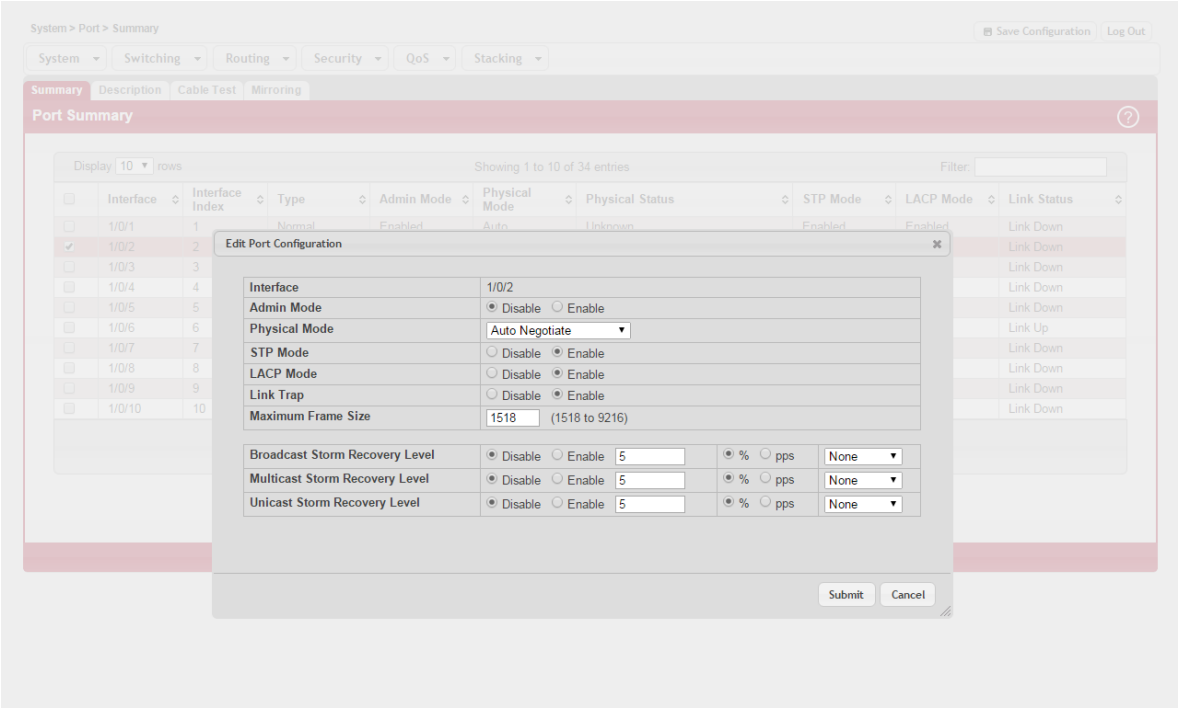

Рисунок 29 – Web интерфейс настройки порта

Примечание: при настройке программы имя программы пишется английскими буквами.

3.1.3 Пример конфигурирования аутентификации и авторизации доступа к управлению с использованием централизованной и локальной базы.

```
(Switch) #enable password
Enter old password:
Enter new password:******
Confirm new password:******
(Switch) #configure
(Switch) (Config)#username admin level 15 password
Enter new password:*****
Confirm new password:*****
(Switch) (Config)#username user level 1 password
Enter new password:****
Confirm new password:****
(Switch) (Config)#radius server host auth 10.1.1.10
(Switch) (Config)#radius server key auth 10.1.1.10
Enter secret (64 characters max):*****
Re-enter secret:*****
(Switch) (Config)#aaa authorization exec default radius local
(Switch) (Config)#aaa authentication login default radius local
(Switch) (Config)#aaa authentication enable default radius enable
(Switch) (Config)#aaa authentication login "networkList" radius local
(Switch) (Config)#show authentication methods
Login Authentication Method Lists
---------------------------------
defaultList       : radius   local
networkList       : radius   local
Enable Authentication Method Lists
---------------------------------
enableList        : radius   enable
```

```
enableNetList      : enable   deny
Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList
HTTPS      :local
HTTP       :local
DOT1X      :

(Switch) (Config)#show authorization methods
Command Authorization Method Lists
-------------------------------------
dfltCmdAuthList             :     none
Line       Command Method List
---------  ---------------------
Console    dfltCmdAuthList
Telnet     dfltCmdAuthList
SSH        dfltCmdAuthList
Exec Authorization Method Lists
-------------------------------------
dfltExecAuthList            :     radius     local
Line       Exec Method List
---------  ---------------------
Console    dfltExecAuthList
Telnet     dfltExecAuthList
SSH        dfltExecAuthList
```

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОЗУ – оперативное запоминающее устройство

ПО – программное обеспечение

ACL – Access Control List (список контроля доступа)

ARP – Address Resolution Protocol (протокол разрешения адресов)

ASN.1 – Abstract Syntax Notation One (язык для описания абстрактного синтаксиса данных)

BPDU – Bridge Protocol Data Unit (фрейм протокола управления сетевыми мостами, IEEE 802.1d)

CLI – Command Line Interface (инструкций ввода-вывода)

CoS – Class of Service (способ управления трафиком)

DHCP – Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)

EPROM – Erasable Programmable Read Only Memory (класс полупроводниковых запоминающих устройств для записи информации)

ID – Идентификатор

IEEE – Institute of Electrical and Electronics Engineers (Институт инженеров по электротехнике и электронике)

IP – Internet Protocol (протокол Интернет)

IPv4 – Internet Protocol version 4 (четвёртая версия интернет протокола (IP))

IPv6 – Internet Protocol version 6 (шестая версия интернет протокола (IP))

ISO – International Organization for Standardization (международная организация п о стандартизации)

LACP – Link Aggregation Control Protocol (протокол для объединения нескольких физических каналов в один логический)

FTP – File Transfer Protocol (протокол передачи файлов)

TFTP – Trivial File Transfer Protocol (простой протокол передачи файлов для первоначальной загрузки бездисковых рабочих станций)

HTTP – HyperText Transfer Protocol (протокол передачи гипертекстовых файлов)

IGMP – Internet Group Management Protocol (межсетевой протокол управления группами)

MAC – Media access control (мандатное управление доступом)

MIB – Management Information Base (база данных информации управления)

MID – встроенная функция обработки строк

MPLS – Multiprotocol label switching (многопротокольная коммутация по меткам)

NMS – Network Management System (система сетевого управления)

NTP – Network Time Protocol (сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью)

QoS – Quality of service (качество обслуживания)

PAE – Physical Address Extension (режим работы встроенного блока управления памятью x86-совместимых процессоров)

PC – персональный компьютер

RAM – Random Access Memory (память с произвольным доступом)

SNMP – Simple Network Management Protocol (простой протокол сетевого управления)

ToS – Type of Service (одно из полей IPv4-пакета)

TCP – Transmission Control Protocol (протокол передачи данных)

UDP – User Datagram Protocol (протокол пользовательских дейтаграмм)

VLAN – Virtual Local Area Network (логическая локальная вычислительная сеть)

WEB – World Wide Web (распределённая система, предоставляющая доступ к связанным между собой документам)