ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»

А. В. Бородко

ДИСЦИПЛИНА

КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ЛАБОРАТОРНЫМ РАБОТАМ С ИСПОЛЬЗОВАНИЕМ КОММУТАЦИОННОГО ОБОРУДОВАНИЯ ZYXEL

СПбГУТ)))

САНКТ-ПЕТЕРБУРГ
2012

УДК 681.326(075)
ББК 3.8.8стд1-01.4

Рецензент:
Н. В. Савищенко – доктор технических наук, профессор военной академии связи имени С. М. Буденного.

Бородко А.В.
Методическое пособие по лабораторным работам дисциплины КСПД с использованием коммутационного оборудования Zyxel для специальности 210700 / ГОУВПО СПбГУТ. – СПб, 2012.
Излагаются теоретические основы, приводятся конкретные задания для лабораторных работ по дисциплине Компьютерные сети передачи данных. Рассмотрен порядок выполнения семи лабораторных работ, которые можно выполнить с использованием стенда коммутационного оборудования ZyXEL.
Предназначено для студентов, бакалавров специальности 210700, а также магистров и специалистов в области телекоммуникаций.

СОДЕРЖАНИЕ

1 МЕТОДИКА ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

1.1 Лабораторная работа №1
Управление коммутатором ZyXEL

Управление сетевыми коммутаторами ZyXEL осуществляется через Web-интерфейс и интерфейс командной строки (CLI – Command Line Interface). Интерфейс командной строки доступен через коммуникационную программу (например, HyperTerminal), а также через сетевые протоколы telnet и ssh (защищенный командный интерпретатор).

Интерфейс командной строки через коммуникационную программу является полезным средством настройки коммутатора, если тот недоступен по сети (отсутствует информация об IP-адресах на интерфейсе Management и остальных портах). В этом случае осуществляется подключение компьютера к коммутатору через выбранный последовательный порт, производится запуск программы HyperTerminal с параметрами: битовая скорость – **9600** бит/с, бит в слове – **8**, четность – **Нет**, стоповый бит – **1**, управление потоком – **Нет**) и ввода логина **admin**, пароля **1234**.

В зависимости от версии микропрограммы и модели устройства запустится либо привилегированный, либо непривилегированный режим управления. Режимы внешне отличаются символом перед вводом команды ('#'–привилегированный или '>'–непривилегированный). Переключение между режимами управления осуществляется с помощью команд **enable** (переход из '>' в '#') и с помощью команды **disable** (переход из '#' в '>').

Сброс текущей конфигурации осуществляется командой **erase running-config**. После этого IP-адрес для управления коммутатором на интерфейсе Management устанавливается **192.168.0.1**, а через рабочие порты он доступнен по адресу **192.168.1.1**. При этом IP-адрес на интерфейсе Management задается командой **ip address**. Для сохранения конфигурации используется команда **write memory**.

Методика выполнения лабораторной работы

1. Получить от преподавателя IP-адрес интерфейса Management одного из трех коммутаторов (коммутаторы предварительно подключены к сети через интерфейсы Management):
- 172.16.100.161
- 172.16.100.162
- 172.16.100.163

2. Запустить на компьютере командную строку и подключиться к коммутатору при помощи команды **telnet [IP-адрес]**. Логин **admin**, пароль **1234**.

3. Наберите символы **show ha**, нажмите [tab], [enter]. Почему команда выдала ошибку? Введите команду правильно (чтобы узнать правильный

формат команды, введите **help**). Команда **show hardware-monitor** показывает аппаратные измерения: температуру, напряжение, скорости вращения вентиляторов. Если на коммутаторе моргает красный светодиод ALM, с помощью этой команды Вы всегда сможете узнать причину неисправности.

4. Произвести переключение между режимами управления коммутатором (рис. 1). Найти команды и воспользоваться ими:

- *show hardware-monitor*
- *show ip*
- *show running-config*
- *ping*
- *traceroute*

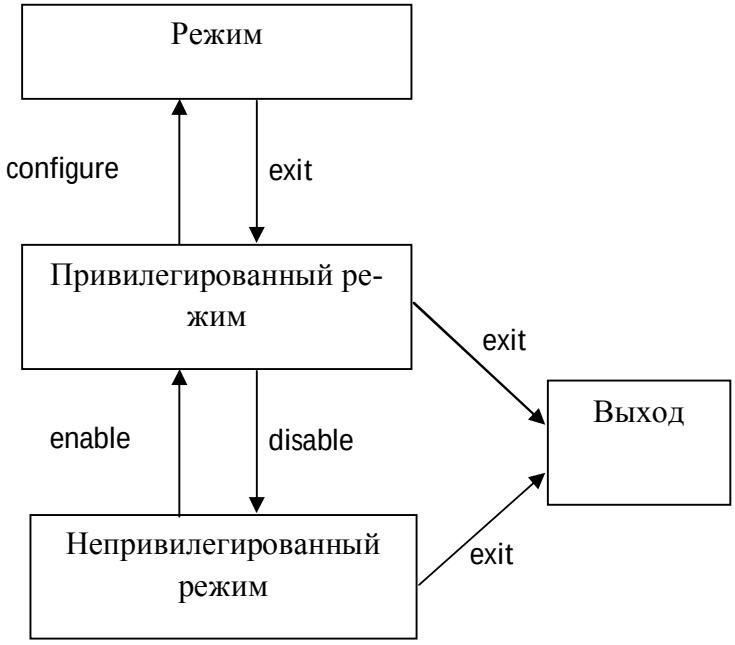


Рис. 1. Переключение между режимами управления коммутатора

5. Осуществить выход из интерфейса командной строки. Подключиться к коммутатору через Web-интерфейс. Набрать в адресной строке web-браузера адрес коммутатора **http://**[**IP-адрес**]. Логин **admin**, пароль **1234**.

6. Получить от преподавателя IP-адрес для подключения через рабочие порты коммутатора:

- 172.16.100.171
- 172.16.100.172
- 172.16.100.173

Зайти в раздел конфигурации сетевых настроек. Задать IP-адрес на интерфейсе Management **192.168.0.1**, IP-адрес для подключения через рабочие порты коммутатора, полученный от преподавателя, применить настройки. Управление над коммутатором через Web-интерфейс будет потеряно.

7. Извлечь сетевой кабель из порта Management и подключить в порт **1** из рабочего набора портов. Подключиться к коммутатору через Web-интерфейс.

Контрольные вопросы

Как можно узнать информацию о температуре процессора в коммутаторе?
В чем назначение порта Management?
В чем назначение команды ping?
В чем назначение команды traceroute?
Как определить текущий IP-адрес коммутатора?

1.2 Лабораторная работа №2
Широковещательный шторм

Loop Guard - функция защиты Ethernet-коммутатора от образования петлевых, т.е. замкнутых маршрутов (петель). Функция защиты от образования петель позволяет настроить на коммутаторе отключение определенного порта при обнаружении ситуации, когда отправляемые через этот порт пакеты возвращаются на коммутатор. Как правило, петля образуется в результате человеческой ошибки, она возникает, когда два порта коммутатора оказываются соединенными одним кабелем. При рассылке коммутатором с петлевым маршрутом широковещательных сообщений они возвращаются на коммутатор и повторно ретранслируются снова и снова, вызывая широковещательный шторм. При подключении коммутатора (без петли) к коммутатору с петлевым маршрутом проблемы последнего отражаются на первом следующим образом:

- он будет принимать широковещательные сообщения, рассылаемые коммутатором с петлей.
- он будет получать собственные широковещательные сообщения, так как они будут возвращаться по петле к нему. После этого эти сообщения будут ретранслироваться коммутатором повторно.

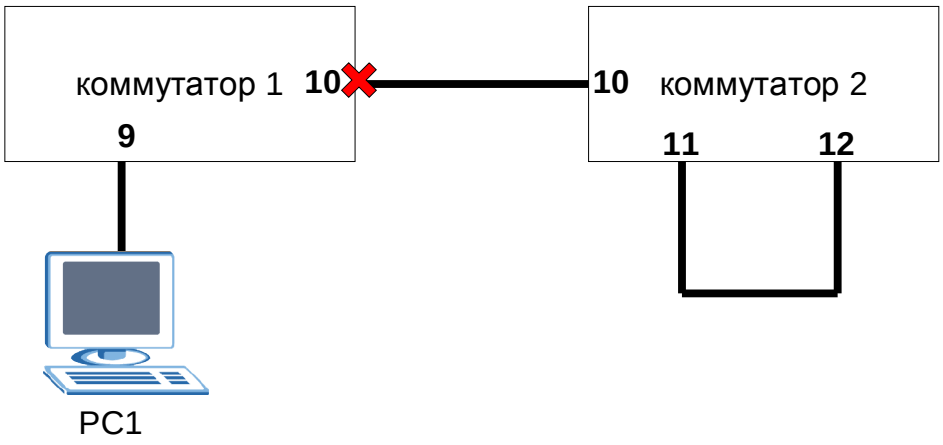


Рис. 2. Образование петли на коммутаторе 2

Работа выполняется на коммутаторах ES-3124 (рис. 2).

Не соединяйте 11 и 12 порт коммутатора 2 между собой, пока не настроите функцию Loop Guard на коммутаторе 1, в противном случае возможно возникновение широковещательных штормов.

Методика выполнения лабораторной работы

1. Предварительно присвоить IP-адреса оборудованию:
   - для подключения через рабочие порты к коммутатору 1 – 192.168.1.1
   - для подключения через рабочие порты к коммутатору 2 – 192.168.1.2
   - компьютер PC1 – 192.168.1.3
2. Подключить PC1 к порту 9 коммутатора 1 и соединить 10 порт коммутатора 1 с 10-ым портом коммутатора 2.
3. Подключиться к коммутатору 1 по Web-интерфейсу. Зайти в меню Advanced Application > Loop Guard и активировать данную функцию на коммутаторе, а также на 10 порту. Применить и сохранить настройки.
4. Соединить 11 и 12 порты коммутатора 2, тем самым искусственно создав шторм (индикаторы состояния портов на коммутаторе 2 будут непрерывно мигать).
5. Проверить доступность коммутатора 1 (с помощью команды ping).
6. На коммутаторе 1 зайти в меню Basic Settings > Port Setup. Флаг Active напротив порта 10 должен отсутствовать. Это результат работы функции Loop Guard, которая отключила порт 10, чтобы избежать распространения шторма.

Контрольные вопросы

Что происходит с коммутатором 2 (рис. 2) при образовании на нем петли?

Что произойдет с коммутатором 1 (рис. 2), если на нем не включить функцию Loop Guard?

Что делать с коммутаторами при возникновении на них широковещательного шторма?

1.3 Лабораторная работа №3
Ограничение полосы пропускания

Данная работа выполняется на коммутаторах ES-3124 или GS-4024. Схема стенда приведена на рисунке 3.

Методика выполнения лабораторной работы.

1. Подключите Ваши компьютеры PC1 и PC2 к коммутатору – к портам 9 и 10 соответственно (см. рис. 3).

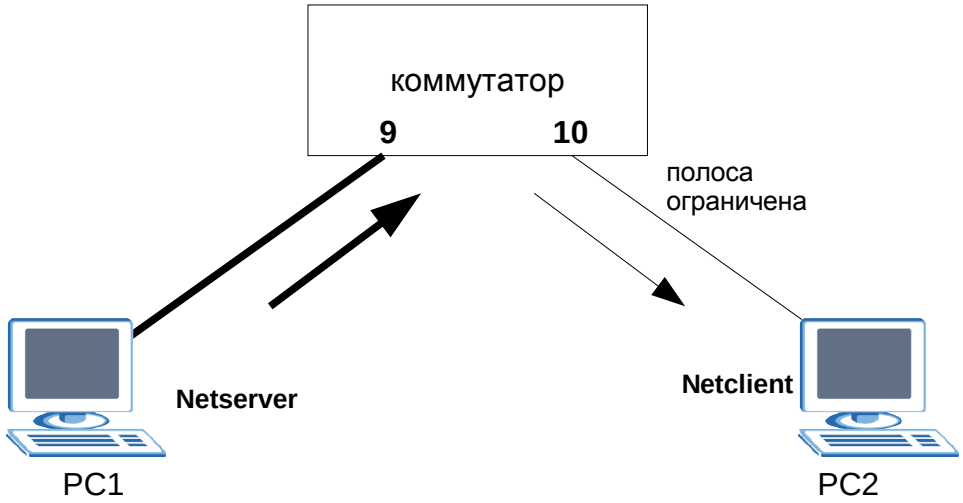


Рис. 3. Стенд для измерения полосы пропускания каналов

2. Назначьте компьютерам PC1 и PC2 следующие IP-адреса:

   PC1 – **192.168.1.101**
   PC2 – **192.168.1.102**
3. Убедитесь, что на PC1 запущен *Netclient* (*см. Приложение 1*).
4. Сейчас Вы будете измерять пропускную способность с помощью программы *Netclient*. На PC2 запустите программу *Netserver*.
5. На компьютере PC1 запустите *Netclient -H <адрес PC2>* для определения пропускной способности.
6. Откройте Web-браузер. В строке адреса наберите **192.168.1.1** (адрес коммутатора).
7. Войдите в настройки коммутатора (логин **admin**, пароль **1234**).
8. Зайдите в меню Advanced Application > Bandwidth Control.
9. Установите выходную пропускную способность (Eggress) порта 10 равную 1 Мбит/с.
10. Измерьте полосу пропускания PC1—PC2 с помощью *Netclient*. При этом можно динамически менять выходную пропускную способность порта 10 и наблюдать за изменениями графика скорости передачи данных.

Контрольные вопросы

Что означает понятие – «Пропускная способность линии»?

Каким образом программа *Netclient* измеряет пропускную способность канала связи, какие факторы на оконечном оборудовании могут исказить результат измерений?

1.4 Лабораторная работа №4
Резервирование линий

RSTP (Rapid Spanning Tree Protocol) – протокол, обеспечивающий восстановление связи при разрыве сетевых соединений за счет резервирования линий.

Протокол RSTP обнаруживает и разрывает сетевые петли и обеспечивает наличие запасных каналов между коммутаторами, мостами или маршрутизаторами. Он позволяет коммутатору взаимодействовать с другими устройствами, поддерживающими протокол RSTP, благодаря чему достигается наличие только одного пути между любыми двумя станциями в сети. При использовании RSTP информация об изменении топологии непосредственно распространяется по всей сети от устройства, вызвавшего изменение топологии.

Работа выполняется на коммутаторах ES-3124 и GS-4024 (рис. 4 и 5).

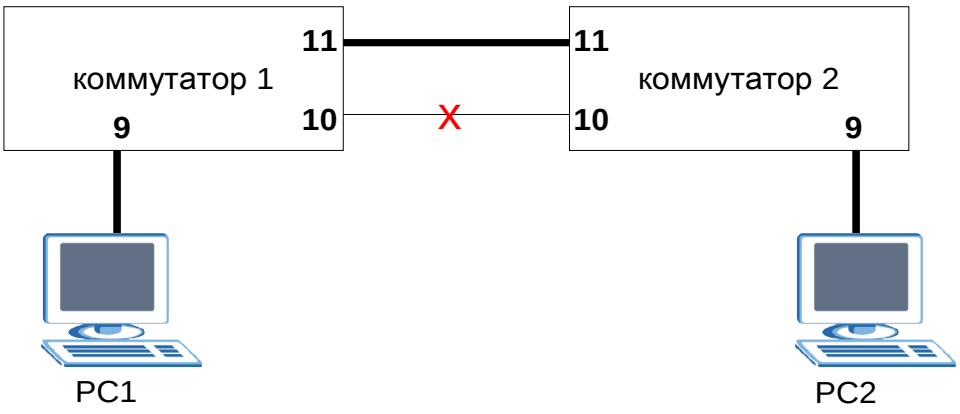


Рис.4. Вариант использования RSTP с двумя коммутаторами

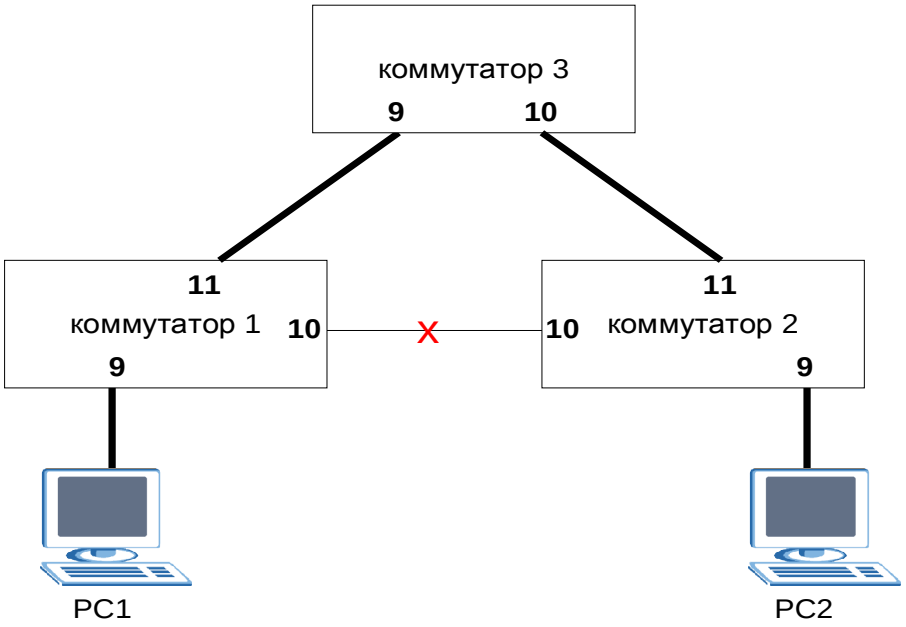


Рис. 5. Вариант использования RSTP с тремя коммутаторами

Не соединяйте 10 порты коммутаторов между собой, пока не включите протокол RSTP, в противном случае возникнет широковещательный шторм.

Методика выполнения лабораторной работы.

1. Предварительно присвоить IP-адреса оборудованию:
- для подключения через рабочие порты к коммутатору 1 (ES-3124) – 192.168.1.1
- для подключения через рабочие порты к коммутатору 2 (ES-3124) – 192.168.1.2
- для подключения через рабочие порты к коммутатору 3 (GS-4024) – 192.168.1.3
- компьютер PC1 – 192.168.1.4
- компьютер PC2 – 192.168.1.5

2. Подключиться ко всем коммутаторам по Web-интерфейсу и зайти в меню Advanced Application > Spanning Tree Protocol > Configuration. Активировать протокол STP, поставив флаг вверху страницы, а также напротив тех портов, которые соединяют каждый коммутатор с соседними коммутаторами. Применить и сохранить настройки.
3. Собрать сеть согласно варианту 1 (рис. 4). Проверить связь между компьютерами (утилита *ping*).
4. Поочередно отключить одно из соединений между коммутаторами, проверяя наличие связи (утилита *ping*).
5. Собрать сеть согласно варианту 2 (рис. 5). Проверить связь между компьютерами (утилита *ping*).
6. Поочередно отключить одно из соединений между двумя коммутаторами, проверяя наличие связи (утилита *ping*).

Контрольные вопросы

С какой целью на коммутаторах включается протокол RSTP?
Что делать при возникновении в сети широковещательного шторма?
Как проверить наличие связи между компьютерами?
Как проверить наличие связи между коммутаторами?

1.5 Лабораторная работа №5
Настройка IP-доменов и разграничения доступа по технологии VLAN в коммутаторе 3-го уровня

Выполняется коммутаторе GS-4024. Соберите стенд по схеме, приведенной на рисунке 6.

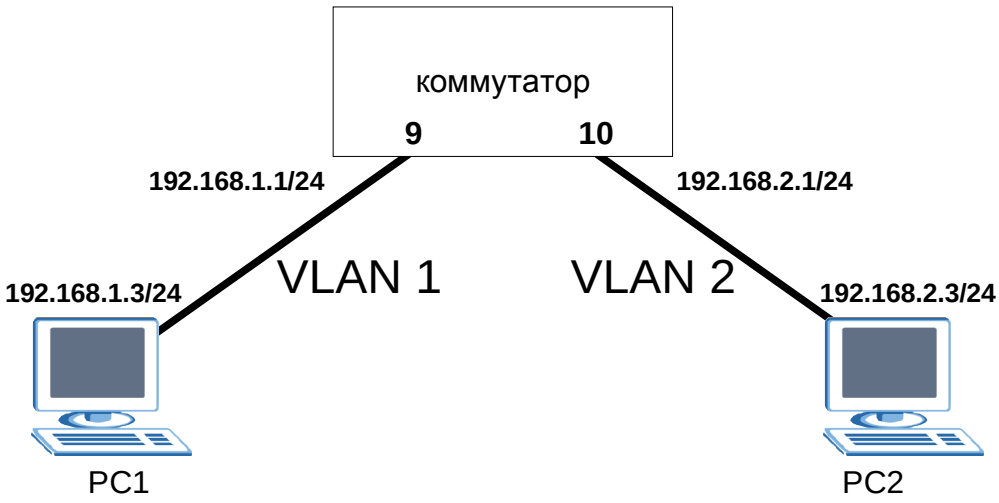


Рис. 6. Стенд для настройки IP-доменов и разграничения доступа по технологии VLAN в коммутаторе 3-го уровня

Методика выполнения лабораторной работы.

1. Зайдите в меню Advanced Application > VLAN > Static VLAN, введите
Active−**Вкл.**
Name−**second**
VLAN Group ID−**2**
Порт 9−**forbidden;**Tx Tagging–**Откл.**
Порт 10−**fixed;**Tx Tagging–**Откл.**
2. Нажмите **Add**.
3. Выберите из списка (внизу) настройки VLAN VID 1.
4. Переведите порт 10 в состояние forbidden, нажмите Add.
5. Зайдите в меню Advanced Application > VLAN > VLAN Port Setting. Установите PVID **2** на порт **10**.
6. IP-домен 192.168.1.1/24 присутствует в коммутаторе по умолчанию. Зайдите в меню Basic Setting > IP Setup, введите:
IP Address−**192.168.2.1**
IP Subnet Mask−**255.255.255.0**
VID−**2**
7. Нажмите **Add**.
8. Задайте компьютеру PC2 адрес 192.168.2.3, маску 255.255.255.0 и адрес шлюза по умолчанию 192.168.2.1.
9. Задайте компьютеру PC1 адрес 192.168.1.3, маску 255.255.255.0 и адрес шлюза по умолчанию 192.168.1.1.
10. Проверьте связь PC1 и PC2 с помощью утилиты *ping*.

Настройка IP-доменов в коммутаторе 3-го уровня с доступом через коммутатор 2-го уровня и разграничением доступа по технологии VLAN

Выполняется на коммутаторе GS-4024 в качестве коммутатора 3-го уровня (L3) и коммутаторе ES-3124 в качестве коммутатора 2-го уровня (L2). Соберите стенд по схеме, приведенной на рисунке 7.

Методика выполнения лабораторной работы.

1. Установите между коммутатором 3 уровня и рабочими станциями коммутатор 2 уровня.
2. Настройте на коммутаторе 2 уровня VLAN следующим образом:

VLAN 1
Порт 9–**fixed**; Tx Tagging–**Откл.**
Порт 10–**forbidden**; Tx Tagging–**Откл.**
Порт 11–**fixed**; Tx Tagging–**Вкл.**
VLAN 2
Порт 9–**forbidden**; Tx Tagging – **Откл.**
Порт 10–**fixed**; Tx Tagging – **Откл.**
Порт 11–**fixed**; Tx Tagging – **Вкл.**

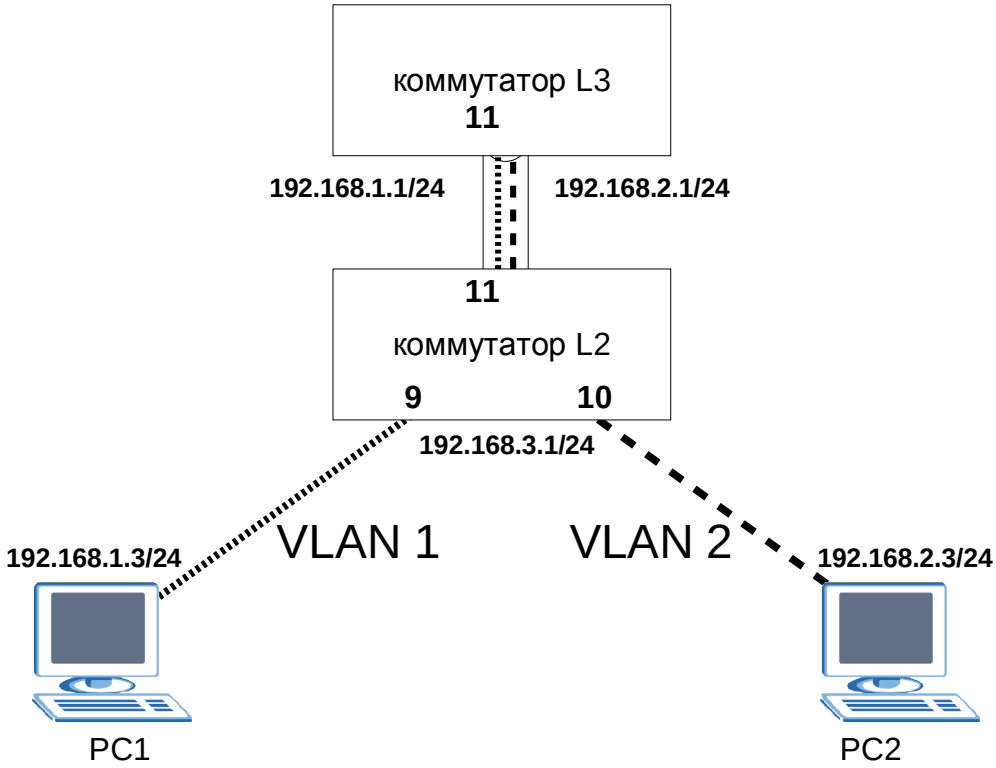


Рис. 7. Стенд для создания IP-доменов в коммутаторе 3-го уровня с доступом через коммутатор 2-го уровня и разграничением доступа по технологии VLAN

3. В меню **VLAN Port Setup** поставьте на 9 порту **PVID=1**, на 10 порту

PVID=2.
4. Настройте на коммутаторе 3 уровня VLAN следующим образом:
VLAN 1 Порт 11–**fixed**; Tx Tagging–**Вкл.**
VLAN 2 Порт 11–**fixed**; Tx Tagging–**Вкл.**
5. Проверьте связь между PC1 и PC2 с помощью утилиты *ping*.

Контрольные вопросы

Зачем нужны логические локальные сети (VLAN)?
Какую технологию организации VLAN рациональнее использовать если узлы, которые должны быть в разных VLAN физически подключены к разным коммутаторам?
Чем тегированный порт коммутатора отличается от нетегированного?
Какие существуют протоколы автоматической настройки VLAN?

1.6 Лабораторная работа №6
Использование классификатора и политики экранирования сетевых протоколов

Данная лабораторная работа выполняется на коммутаторах ES-3124 и GS-4024. В задании требуется с помощью классификатора и политики запретить прохождение через коммутатор пакетов ICMP.

Методика выполнения лабораторной работы.

1. Подключите Ваши компьютеры PC1 и PC2 к коммутатору – к портам 9 и 10 соответственно (см. рис. 8).
2. Назначьте компьютерам следующие IP-адреса:

PC1 – **192.168.1.101**
PC2 – **192.168.1.102**

2. Войдите в меню **Advanced Application** > **Classifier**.

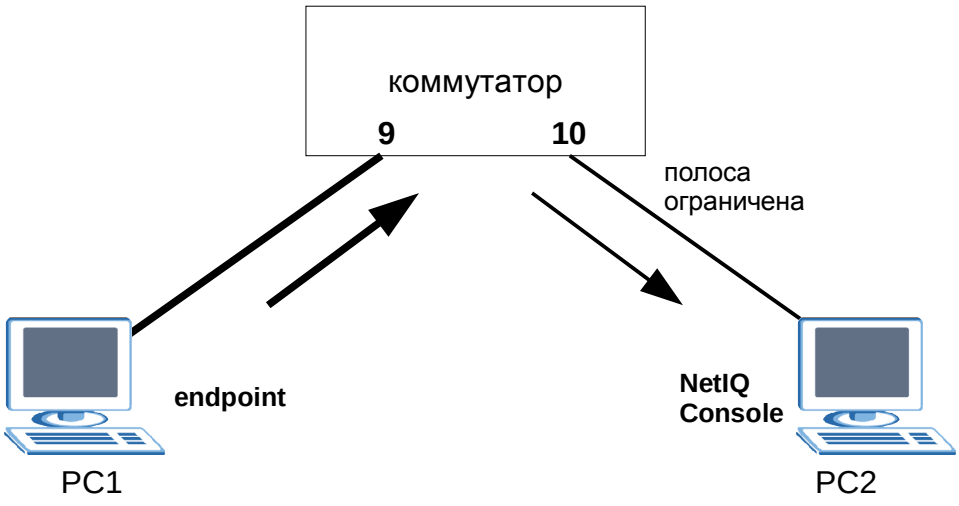


Рис. 8. Стенд для запрета ICMP трафика с помощью политики

3. Поставьте флаг **Active**, имя **icmp**, IP Protocol–**ICMP**, Source IP address **192.168.1.0/24** остальные поля оставьте по умолчанию.
4. Нажмите **Add**.
5. Зайдите в меню **Advanced Application** > **Policy**.
6. Активизируйте политику, назовите ее **noicmp**, выберите из списка классификаторов **icmp**, установите действие Action–**Discard the packet**.
7. Нажмите **Add**.
8. Проверьте, что утилита *ping* не может передать пакет через коммутатор.
9. Проверьте, что компьютер PC2 «виден» с компьютера PC1, если зайти в меню **Пуск > Выполнить...** и набрать в командной строке две обратные косые черты и IP-адрес PC2:
\\192.168.2.3

Контрольные вопросы

Для чего используется протокол ICMP?
К какому уровню стека протоколов TCP/IP принадлежит ICMP?
Как сгенерировать пакет ICMP?
Как узнать доступность узла без использования протокола ICMP?

1.7 Лабораторная работа №7
Трансляция сообщений DHCP (DHCP Snooping) и защита клиентских портов (IP Source Guard)

Подключите компьютер PC1 и DHCP сервер к коммутатору – к портам 9 и 11 соответственно (рис. 9).

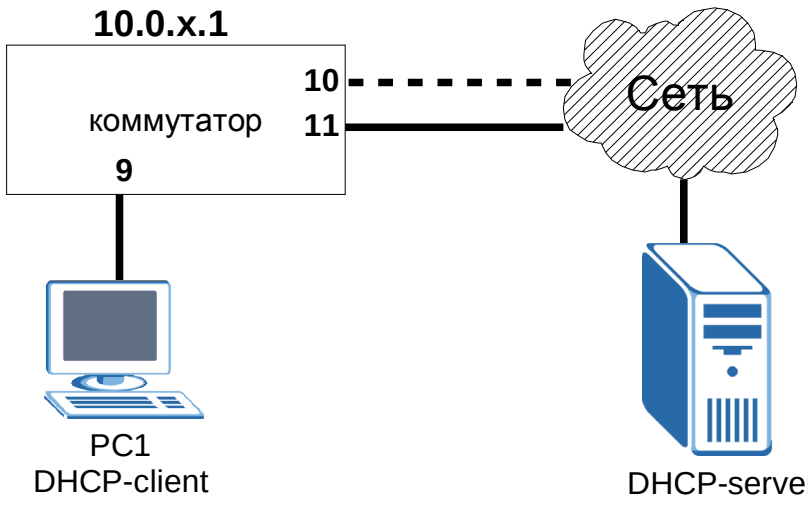


Рис. 9. Стенд для изучения работы коммутатора с DHCP сервером

Методика выполнения лабораторной работы.

1. Подключитесь к коммутатору по консольному порту.
2. Назначьте коммутатору IP-адрес 10.0.x.1 маска 255.255.0.0 (где x – номер рабочего места + 100)

3. Назначьте рабочей станции IP-адрес 10.0.x.2, маска 255.255.0.0 (где x – номер рабочего места + 100)
4. Подключите PC1 к порту 9 коммутатора 1.
5. Зайдите в меню Advanced Application -> IP Source Guard -> DHCP Snooping -> Configure и активизируйте функцию **DHCP Snooping**.
6. Зайдите в меню Advanced Application -> IP Source Guard -> DHCP Snooping -> Configure -> VLAN, добавьте диапазон VLAN **1-1** и активизируйте **DHCP Snooping** в указанном диапазоне VLAN.
7. Зайдите в меню Advanced Application -> IP Source Guard -> DHCP Snooping -> Configure -> Port, присвойте порту **11** значение **trusted,** а порту **10** – значение **untrusted.**
8. Подключите коммутатор к сети учебной лаборатории через порт 10.
9. Настройте PC1 в качестве DHCP-клиента.
10. Ответьте на вопрос: – Удалось ли получить IP-адрес в случае, если DHCP-сервер подключен к недоверенному (untrusted) порту?
11. Переключите сеть учебной лаборатории из порта 10 в порт 11.
12. Попробуйте снова получить IP-адрес, для этого в командной строке сначала наберите **ipconfig /release**, а затем **ipconfig /renew**
13. Теперь, если DHCP Snooping настрен правильно, PC1 сможет получить адрес от DHCP-сервера, и в меню **Advanced Application** -> **IP Source Guard** вы увидите запись с MAC/IP-адресами PC1.

Контрольные вопросы

Что представляет собой протокол DHCP?
Опишите механизм выделения IP-адресов с помощью сетевого сервиса DHCP, что в него вносит посредник в виде коммутатора?
Какие параметры получает рабочая станция от сервера DHCP?

Защита клиентских портов (ARP-Spoofing)

Все настройки коммутатора, касающиеся DHCP Snooping, сделанные в предыдущей лабораторной работе необходимо сохранить. Подключите компьютер PC1 и DHCP сервер к коммутатору – к портам 9 и 11 соответственно (рис. 10).

Методика выполнения лабораторной работы.

1. Проверьте доступность узла 10.0.0.1. с помощью команды *ping*.
2. Зайдите в меню Advanced Application -> IP Source Guard -> Arp Inspection -> Configure и активизируйте функцию **Arp Inspection**
3. Зайдите в меню Advanced Application -> IP Source Guard -> Arp Inspection -> Configure -> VLAN, добавьте диапазон VLAN **1-1** и активизируйте **Arp Inspection** в указанном диапазоне VLAN.

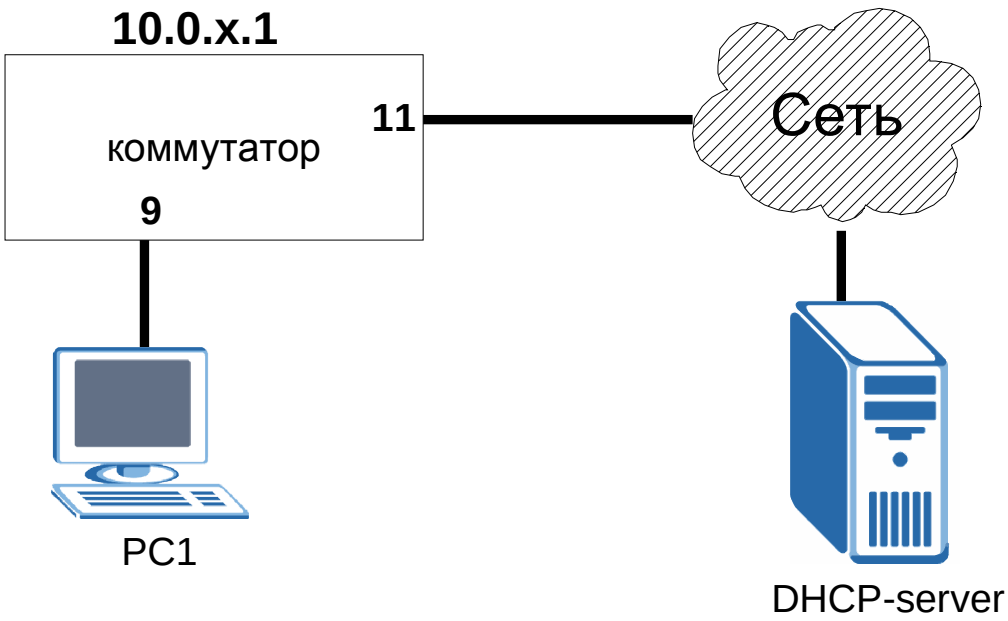


Рис. 10. Стенд для изучения механизма защиты клиентских портов

4. Проверьте доступность узла 10.0.0.1. с помощью команды *ping*. При таких настройках ICMP-запросы, отправляемые рабочей станцией, будут передаваться коммутатором, так как запись об узле с MAC и IP адресом рабочей станции была добавлена в таблицу IP-MAC Binding Table функцией DHCP Snooping. Однако, ICMP-ответы от узла 10.0.0.1 коммутатор через себя пропускать не будет, так как информация об этом узле не содержится в таблице IP-MAC Binding Table.
5. Зайдите в меню Advanced Application -> IP Source Guard -> Static Binding и создайте статическую запись в таблице IP-MAC Binding Table для следующего вида:
MAC Address: **MAC адрес DHCP сервера**
IP Address: **10.0.0.1**
VLAN: **1**
Port: **Any**
6. В меню Advanced Application -> IP Source Guard -> Arp Inspection удалите динамическую запись с MAC-адресом DHCP сервера, если она там есть.
7. Проверьте доступность узла 10.0.0.1. с помощью команды ping, теперь ответы узла 10.0.0.1 будут доходить до PC1.
8. Назначьте PC1 ip-адерс 10.0.x.2 и проверьте доступность узла 10.0.0.1. Теперь узел 10.0.0.1 будет недоступен, так как в таблице существует запись с MAC-адресом PC1, но при этом ip-адресом, полученным от DHCP-сервера, а не 10.0.x.2
9. Настройте PC1 в качестве DHCP-клиента и в меню Advanced Application -> IP Source Guard -> Arp Inspection удалите динамическую запись с MAC-адресом PC1 (MAC-адрес PC1 можно просмотреть с

помощью команды **ipconfig /all**)
10. Проверьте, что узел 10.0.0.1 снова доступен.
11. Удалите статическую запись об узле с MAC-адресом DHCP сервера и IP-адресом: 10.0.0.1.
12. Проверьте доступность узла 10.0.0.1. с помощью команды *ping*, через некоторое время ответы от 10.0.0.1 доходить до рабочей станции уже не будут.
13. Зайдите в меню Advanced Application -> IP Source Guard -> ARP Inspection -> Configure -> Port и присвойте порту **11** значение **trusted.**
14. В меню Advanced Application -> IP Source Guard -> Arp Inspection удалите динамическую запись с MAC-адресом DHCP сервера.
15. Проверьте доступность узла 10.0.0.1. с помощью команды ping.
16. Таким образом, при использовании функции **Arp Inspection** все узлы сети должны быть:
- либо подключены к trusted порту
- либо в таблице **IP-MAC Binding Table** должна быть динамическая (DHCP Snooping) или статическая (Static Binding) запись об узле.

Контрольные вопросы

Как злоумышленник может использовать отсутствие механизма защиты клиентских портов коммутатора Ethernet?
С помощью каких методов можно защитится от DHCP и ARP атак?
От атак какого уровня мы защищались в этой лабораторной работе?

2. УПРАВЛЕНИЕ КОММУТАТОРАМИ ZYXEL

2.1 Стенд «коммутационное оборудование Zyxel»

Стенд для проведения лабораторных работ состоит из двух управляемых коммутаторов второго уровня Zyxel ES-3124 и одного управляемого коммутатора третьего уровня Zyxel GS-4024. На каждом коммутаторе имеется 24 10/100 Мбит/с порта (RJ-45) и два порта для скоростей до 1 Гбит/с (100/1000), позволяющие осуществлять как подключения с использованием медного кабеля, так и оптического волокна для соединения их друг с другом, с коммутационным оборудованием других фирм производителей и оконечными терминалами, в качестве которых предполагается использовать портативные персональные компьютеры Apple Macbook 13.

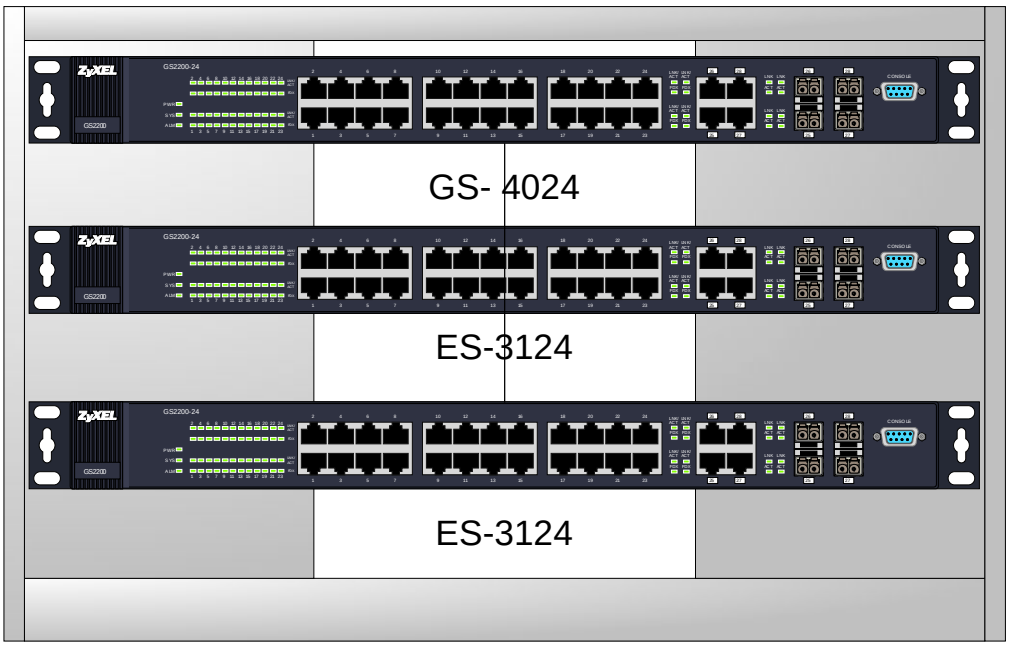


Рис. 1. Стенд «коммутационное оборудование Zyxel»

Стенд комплектуется набором коммутационных кабелей UTP пятой категории с разъемами RJ45 для коммутации с оконечными терминалами.

2.2 Коммутационное оборудование фирмы ZyXEL.

Вся линейка Ethernet-коммутаторов компании ZyXEL разделена на 4 серии:

100 и **1000** серия - неуправляемые коммутаторы 2 уровня

2000 серия - управляемые коммутаторы 2 уровня (L2) для пользователей класса SOHO (небольшие и домашние офисы). Поддерживают VLAN,

управление полосой пропускания, предотвращение широковещательных штормов, [Stacking, аутентификацию 802. lx, LACP.

3000 серия - управляемые коммутаторы 2 уровня (L2+) для пользователей класса SMB (малый и средний бизнес). Расширяют функциональность серии 2000: большая таблица MAC-адресов, дополнительный разъем питания, стекирование VLAN, гарантия полосы пропускания ("трехцветный" алгоритм) и многое другое. Основное отличие от серии 2000 в том, что многие функции реализованы аппаратно и не снижают скорости передачи данных.

4000 серия - коммутаторы третьего уровня. Расширяют функциональность серии 3000: IP-домены, DHCP-server, RIP, VRRP, DVMRP, OSPF, IGMP-server.

Расшифровка названий коммутаторов:

ES (Ethernet Switch) — коммутатор со 100 Мбит/с портами и гигабитными uplink

GS (Gigabit Switch) — полностью гигабитный коммутатор

MES/MGS (Metro Ethernet/Gigabit Switch) - коммутаторы Metro Ethernet

PWR (Power) - означает, что данный коммутатор является источником питания по стандарту PoE (Power over Ethernet)

2.3 Доступ к коммутаторам Zyxel

Получим доступ к коммутатору, используя Web браузер. Для этого на ПК необходимо настроить адрес сетевого адаптера 192.168.0.2/24 и подключили кабель к порту MGMT. По умолчанию доступ к устройству можно получить либо с порта MGMT по адресу 192.168.0.1/24, либо с коммутируемых портов по адресу 192.168.1.1/24. При входе на устройство по протоколу HTTP или HTTPS необходимо ввести имя пользователя и пароль в окне авторизации (рис. 2). Стандартное имя пользователя (UserName): admin. Стандартный пароль (Password): 1234.

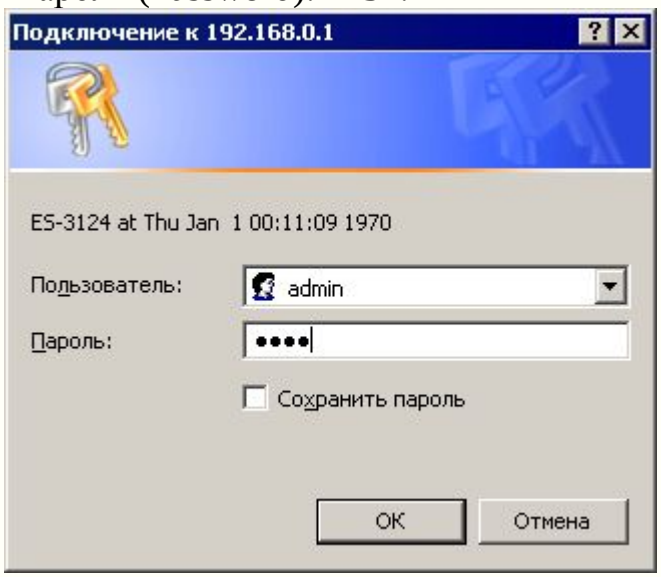


Рис. 2. Окно авторизации

Основное окно отображает текущую статистику по каждому порту (активен ли порт, LACP, количество переданных/принятых пакетов, количество ошибок приема/передачи, текущая скорость передачи/приема в Кб/с, время работы порта). Слева в окне выводится основное меню и под ним меню текущих настроек (рис. 3).

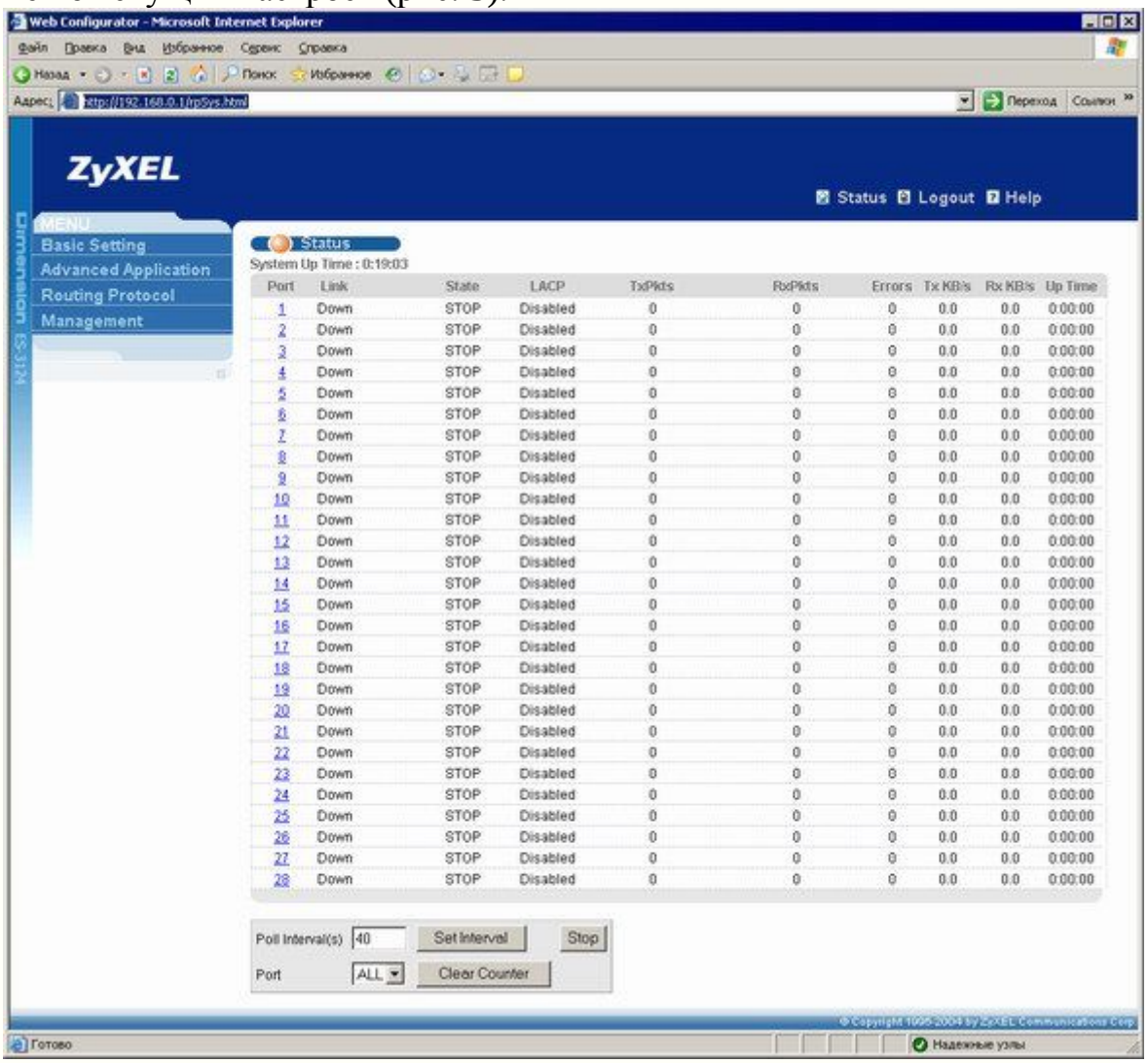


Рис. 3.Основное окно Web-интерфейса коммутаторов ZyXEL

Меню System Info отображает информацию о системе, а именно: наименование системы, версию ПО, MAC-адрес и пр. В General Setup возможно задать имя устройства, местоположение и ответственного, а также параметры синхронизации с внешним сервером времени. Поддерживаются следующие форматы: Daytime (RFC 867), Time (RFC-868) и NTP (RFC-1305).

В Switch Setup определяются общие настройки коммутатора – тип VLAN (port-based или 802.1Q), поддержка IGMP Snooping, время старения динамических записей в таблице MAC, интервалы задержек для протокола GARP и распределение приоритетов 802.1p по очередям.

В IP Setup определяются настройки IP-адреса для управления коммутатором (статический или DHCP Client) и Management VLAN (идентификатор VLAN), с которого разрешено управление устройством. Можно ввести несколько IP-адресов в различных VLAN для управления коммутатором из разных подсетей.

Основное меню содержит следующие разделы:

- Basic Settings – системная информация и основные настройки, такие как режим работы VLAN, распределение приоритетов 802.1p по очередям и т.д.
- Advanced Application – дополнительный настройки, такие как VLAN, Link Aggregation, STP/RST/MSTP, IP Source Guard и т.д.
- IP Application – настройка протоколов маршрутизации (для коммутаторов L3), статических маршрутов, DHCP Server/Relay и т.д.
- Management – обновление микропрограммы, сохранение/восстановление конфигурации, просмотр таблиц MAC/ARP и т.д.

Управление коммутатором через консоль

Оборудование имеет или выведенный на корпус консольный порт RS-232.

Через консоль возможно получить доступ к SMT управлению, которое может содержать командную строку или текстовую систему меню. Используется для локального управления, обновления программного обеспечения по Bootp/TFTP в ОС Zyxel ATMOS. Это наиболее безопасный способ управления оборудованием.

Управление коммутатором через Telnet

Данный способ управления оборудованием аналогичен по функционалу управлению по консоли, однако управление возможно удаленное через Ethernet. Недостаток – данные, в том числе и пароль, передаются в открытом виде.

Управление коммутатором через FTP

В данном случае оборудование выступает в качестве FTP сервера. Пароль аналогичен паролю для консоли и telnet. Это наиболее удобный способ обновления и сохранения конфигурации, он может быть использован для специализированных программ, которые по расписанию сохраняют конфигурацию с оборудования и автоматически обновляют ПО при выходе новой версии.

2.4 Широковещательные штормы

Если в сети по какой-либо причине возникает широковещательный шторм, полезные данные не будут проходить через коммутатор из-за переполнения буферов ненужными пакетами (рис. 4). Функция Broadcast Storm Control позволяет ограничить количество широковещательных (Broadcast),

и групповых (Multicast) пакетов, а также пакетов DLF (Destination Lookup Failure). DLF пакеты генерируются коммутатором, когда происходит обращение по MAC-адресу, присутствующему в таблице фильтрации MAC при отключенном порту назначения.

Ограничение устанавливается на количество принятых пакетов в секунду. Если пакеты указанного типа превышают ограничение, они отбрасываются.

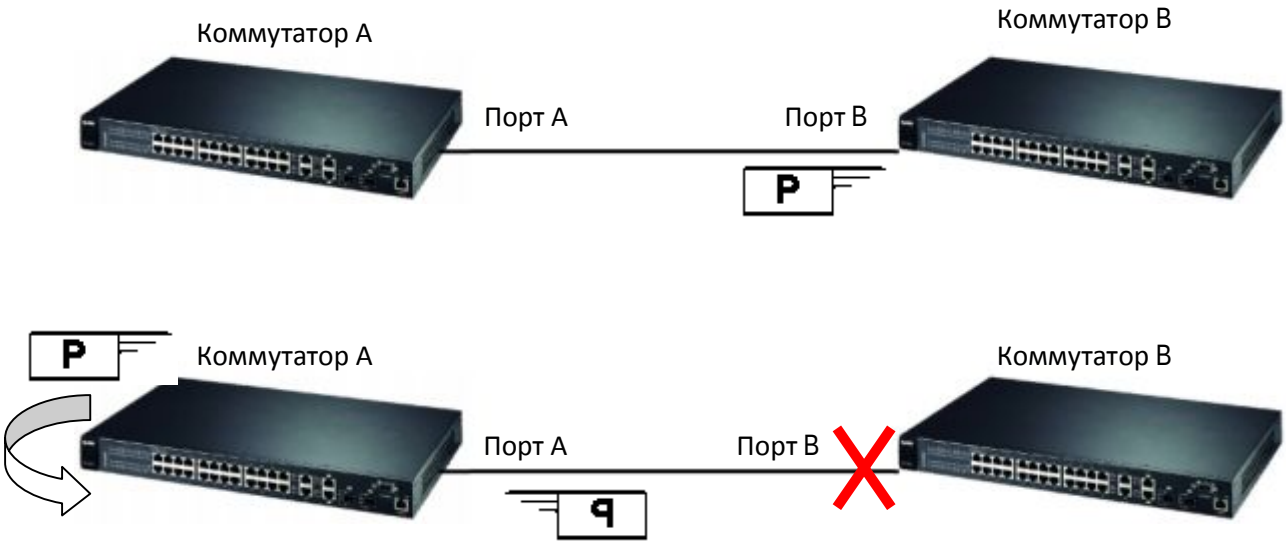


Рис.4. Работа функции предотвращения распространения шторма (Loop Guard)

Loop Guard – функция, которая позволяет предотвращать распространение шторма.

Алгоритм работы функции следующий:

- Коммутатор B, на котором включена функция Loop Guard на порте B, с некоторой периодичностью отправляет в этот порт специальный тестовый (probe) пакет, имеющий широковещательный (multicast) адрес назначения.
- В случае, если на коммутаторе A нет шторма, полученный probe-пакет будет отправлен на все порты, за исключением порта, на который пакет был получен.
- В случае, если коммутатор A находится в состоянии шторма, пакет будет отправлен на все порты.

Таким образом, если коммутатор получил тестовый пакет, им же отправленный, значит коммутатор A находится в состоянии шторма и порт B выключается. После устранения причины шторма, порт необходимо будет включить вручную, автоматически этого не произойдет.

Рис. 5. Страница активации LoopGuard

Команды CLI
loopguard <cr>
interface port-channel <port-list> loopguard

2.5 Управление полосой пропускания

Для настройки полосы пропускания необходимо войти в меню **Advanced Application** -> **Bandwidth Control**.

По каждому порту можно задать ограничение входящего и исходящего потока данных.

Для входящего потока (Ingress Rate) указывается два параметра: Commit Rate и Peak Rate. Пакеты, превышающие порог Peak Rate, отбрасываются.

В выходной порт может поступать сразу несколько потоков данных из разных входных портов, однако его полоса пропускания ограничена либо физическими возможностями выходного канала, либо принудительно - с

помощью параметра Eggress Rate. Если скорость выходного порта не позволяет обслужить все пакеты, то в первую очередь будут отброшены те, которые при входе в коммутатор превысили порог Commit Rate (рис. 6).

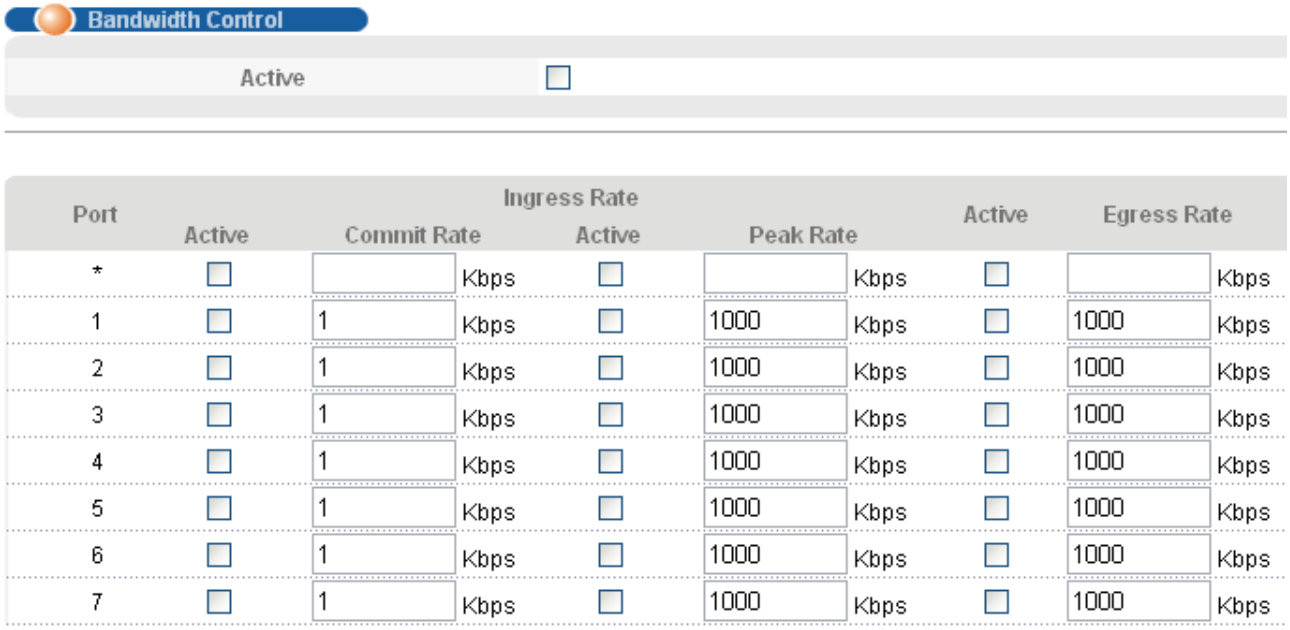


Рис. 6. Управление полосой пропускания через WEB интерфейс

Команды для управления через CLI

bandwidth-control <cr>
interface port-channel <port-list> bandwidth-limit cir <Kbps>
interface port-channel <port-list> bandwidth-limit cir <cr>
interface port-channel <port-list> bandwidth-limit pir <Kbps>
interface port-channel <port-list> bandwidth-limit pir <cr>
interface port-channel <port-list> bandwidth-limit egress <Kbps>
interface port-channel <port-list> bandwidth-limit egress <cr>

2.6 Классификаторы и политики для управления трафиком

Классификатор служит для того, чтобы выделять из общего потока группы пакетов с определенными признаками, и затем с помощью **политик** применять к этим группам пакетов определенные действия.

В зависимости от коммутатора (2-го или 3-го уровня) в классификаторе будут присутствовать признаки, либо относящиеся только к заголовку Ethernet, либо к заголовкам Ethernet+TCP/IP, страница для создания классификатора через Web-интерфейс показана на рисунке 7. Коммутаторы серии 3000 позволяют классифицировать пакеты на 3-м уровне и применять те же политики, что и коммутаторы 3-го уровня 4000-й серии, поэтому их называют коммутаторами уровня 2+.

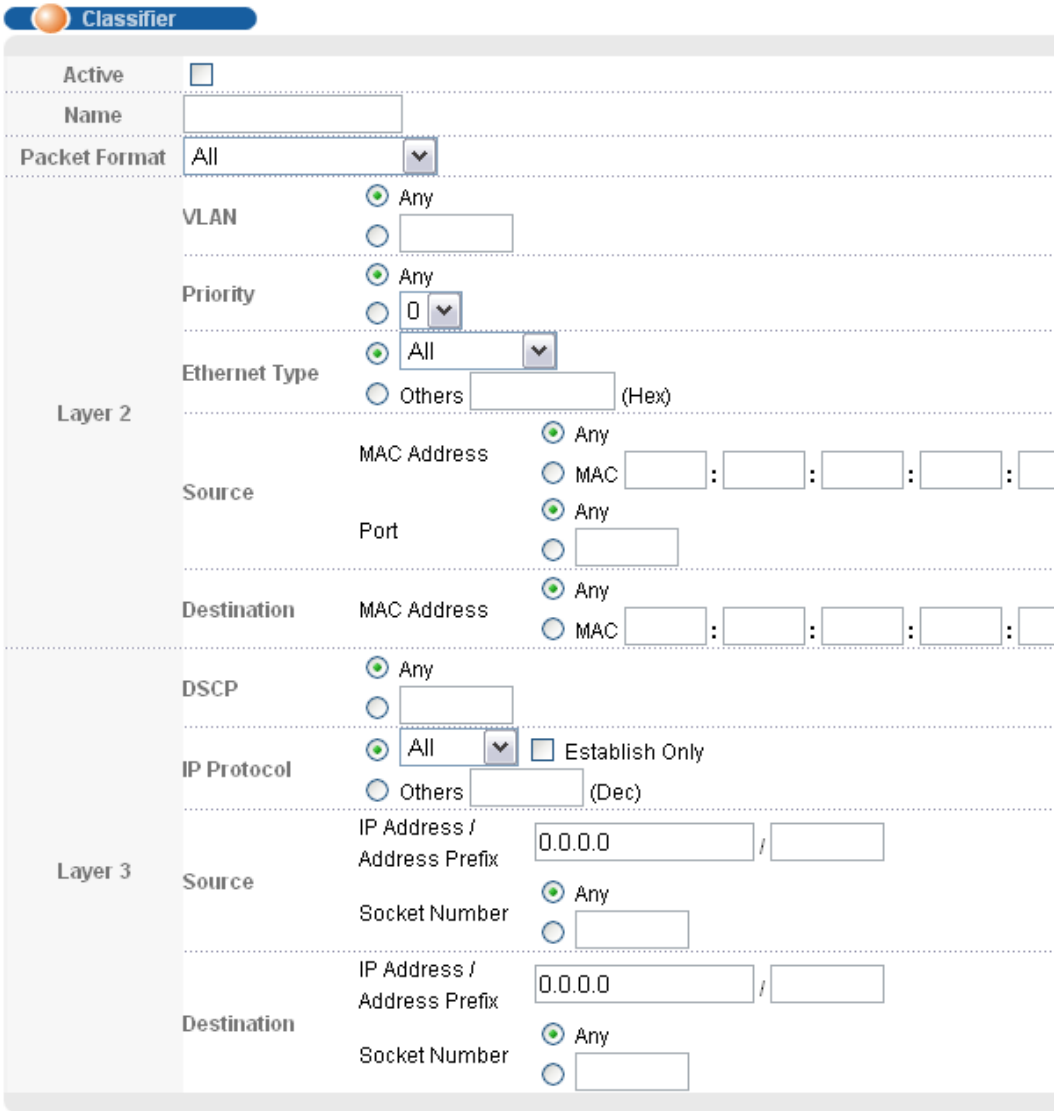


Рис. 7. Добавление классификатора через WEB интерфейс

В полях, относящихся ко второму уровню, указывается тип кадра Ethernet **(Packet Format),** идентификатор **VLAN** 802.1Q, приоритет 802.1p **(Priority),** поле типа в заголовке Ethernet **(Ethernet Type),** MAC-адреса источника и назначения **(Source, Destination)** и порт коммутатора, в который был получен кадр.

На третьем уровне коммутатор проверяет поля заголовка IP-пакета: поле **DCSP,** идентификатор протокола четвертого уровня **(IP Protocol),** IP-адреса источника и назначения, причем можно указать диапазон адресов с помощью маски, например, **192.168.1.0/24.** Кроме того, в случае протоколов TCP и UDP коммутатор может проверять порты источника и назначения **(Socket Number),** а также бит SYN протокола TCP (флаг **Establish only).**

Команда CLI

classifier <name> [vlan<vlan-id>][..] classifier help

Для настройки политики нужно выбрать класс из списка и затем

указать действия **Actions,** применяемые к выбранному классу. Если действие имеет параметр, то этот параметр должен быть установлен в соответствующем поле раздела **Parameters** (рис. 8).

С помощью классификаторов и политик можно решать множество задач, среди которых:

- фильтрация по MAC- и IP-адресам;
- привязка MAC- и IP-адреса к определенному порту;
- фильтрация протоколов по идентификатору в заголовке пакета;
- фильтрация служб по номеру сокета (порта TCP/UDP);
- гибкое управление качеством обслуживания на базе 802.1p, TOS и DSCP;
- зеркалирование определенных типов пакетов;
- изменение идентификатора VLAN, приоритета 802.1p, поля DSCP;
- принудительная пересылка пакета в определенную очередь или на определенный порт.

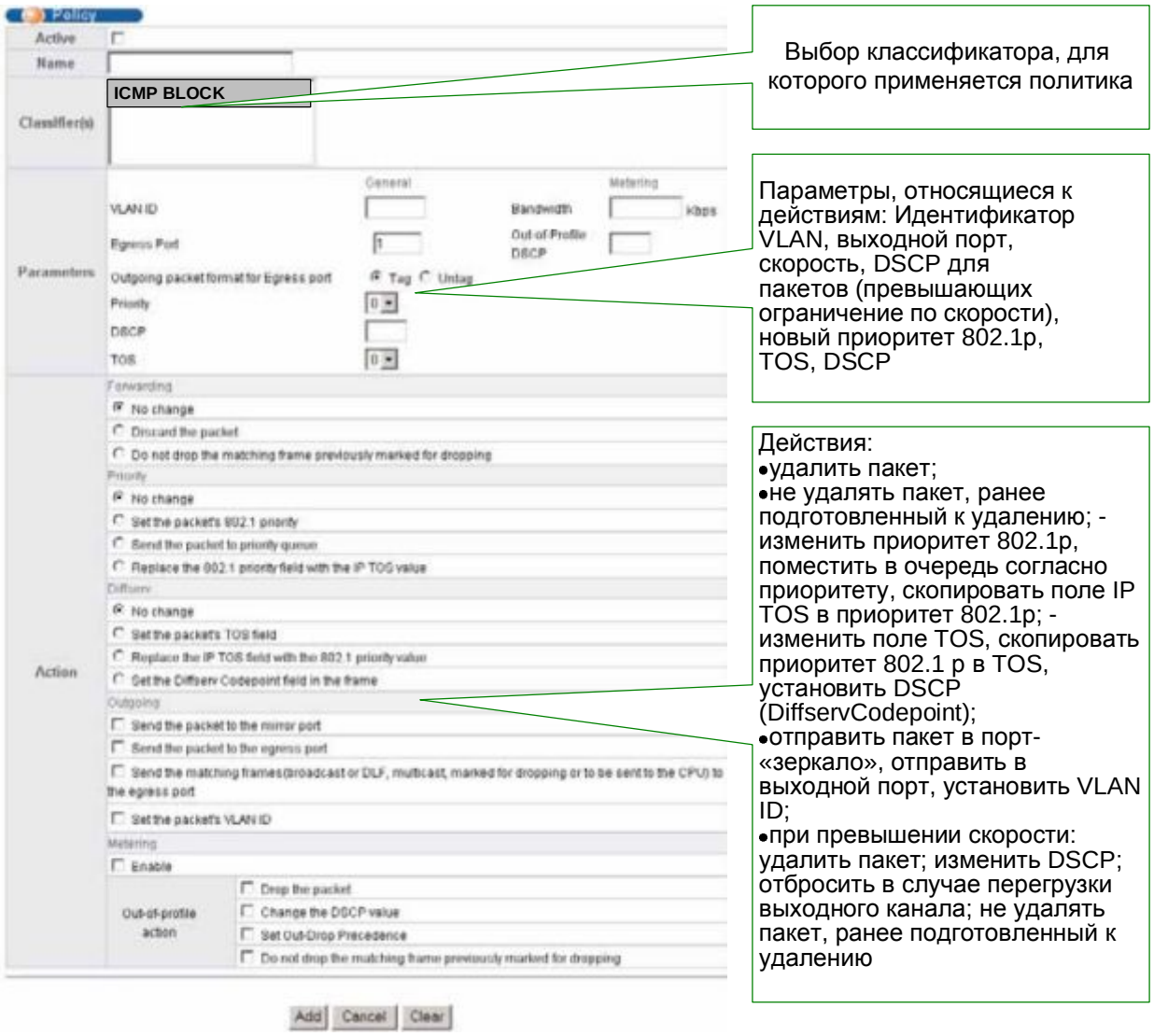


Рис. 8. Добавление политики для выбранного классификатора через WEB интерфейс

Команда в CLI
policy <name> policy help

2.6.1 Управление перегрузками с помощью политики

Гибкий механизм управления перегрузками позволяет ограничивать полосу пропускания, используемую каким-либо типом трафика, при этом ограничение вступает в силу лишь в случае необходимости.

Рассмотрим следующий пример: коммутатор получает трафик по протоколу FTP от PC A и трафик HTTP от PC B. На коммутаторе с помощью классификаторов и политик установлено ограничение пропускной способности для HTTP трафика 512 Kbps, а также указано, что трафик отбрасывать только в случае перегрузки выходного канала.

Пусть трафик HTTP превышает 512 Kpbs, однако полосы пропускания второго порта хватает для отправки и FTP трафика и HTTP. В этом случае полоса пропускания под HTTP уменьшаться не будет. Если же трафик HTTP превышает 512 Kbps и полосы пропускания выходного порта не хватает, то только в этом случае часть трафика будет отбрасываться.

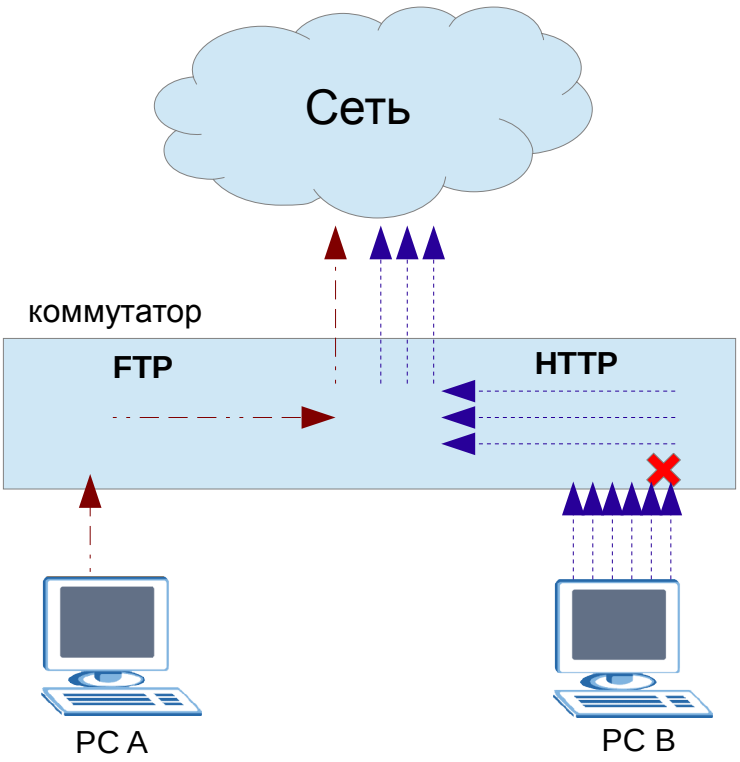


Рис.9. Защита от перегрузки выходного канала

Для настройки механизма управления перегрузками следует создать политику, (рис.10), в действиях которой следует выбирать действия из раздела Исходящие (**Outgoing**), а в качестве параметра трафика – Пропускную способность (**Bandwidth**).

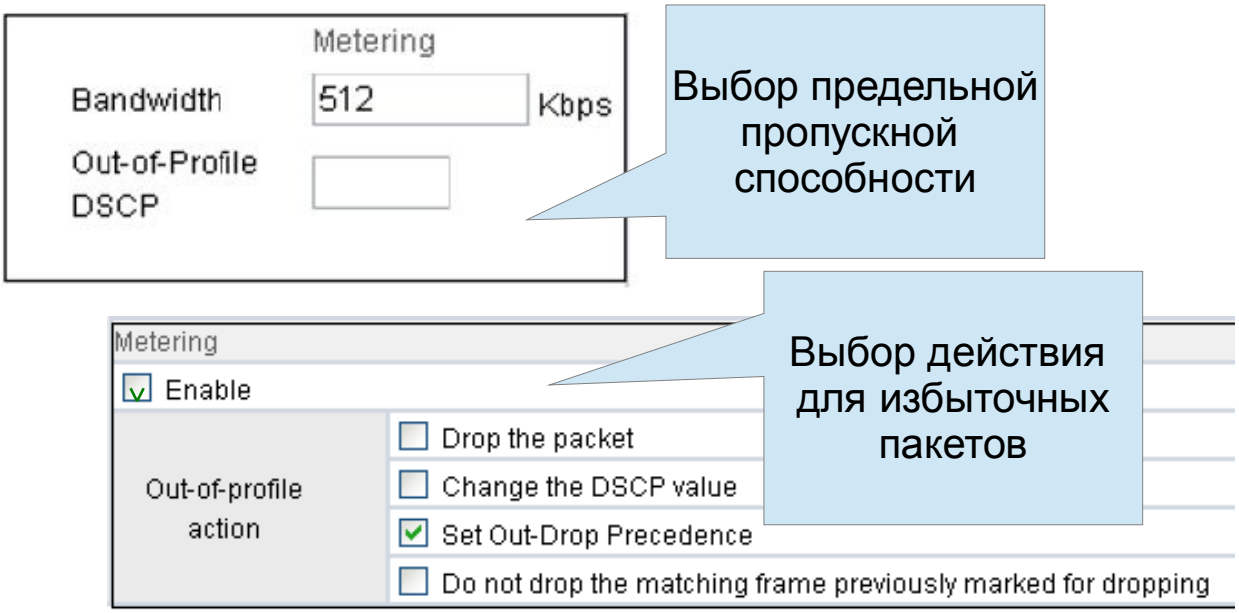


Рис.10. Управление перегрузками через WEB интерфейс

2.7 Link Aggregation

Link Aggregation это - объединение нескольких физических линий в одну логическую до 6 групп, до 8 портов в группе с поддержкой LACP.

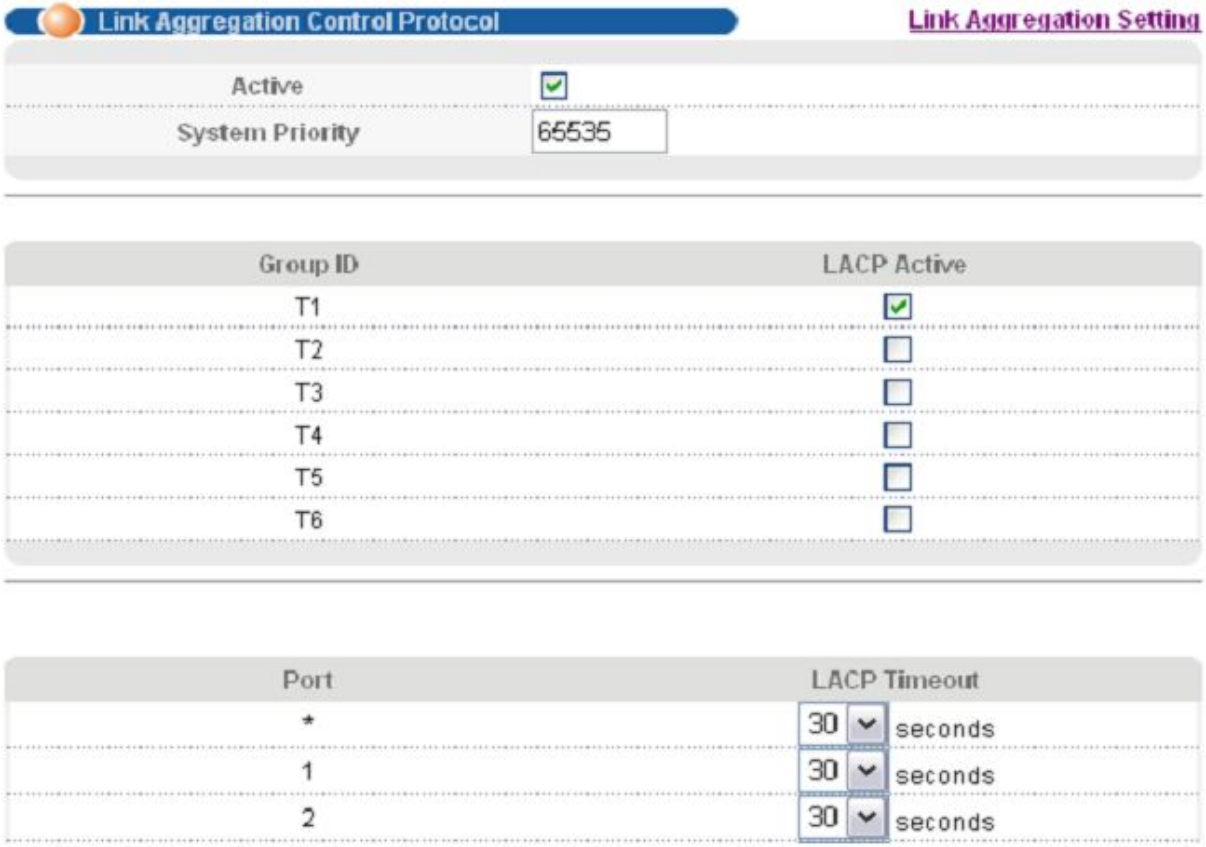


Рис. 11. Страница настройки LACP

Агрегирование (trunk или link aggregation) – это объединение нескольких физических портов в один логический для увеличения пропускной способности и для обеспечения повышенной отказоустойчивости.

В коммутаторах ZyXEL (как и в коммутаторах большинства мировых производителей), Link Aggregation отвечает за разделение нагрузки, но не за балансировку нагрузки (Load Sharing vs. Load Balancing). Load Sharing равномерно распределяет таблицу MAC- адресов междувсеми портами, входящими в агрегированный канал. Таким образом, кадры с определенным MAC-адресом назначения пойдут только по одному физическому каналу без увеличения скорости. Принцип Load Sharing дает увеличение скорости передачи только в том случае, когда по агрегированному каналу передаются кадры с различными MAC-адресами назначения. В каждую группу агрегирования можно включить не более 8-ми портов (рис. 11).

Команды CLI
Trunk <T1|T2|T3|T4|T5|T6> <cr>
Trunk <T1|T2|T3|T4|T5|T6> interface <port-list>

Link Aggregation Control Protocol (LACP) описан в спецификации IEEE 802.3ad, в которой определена возможность объединения нескольких физических линий в один логический канал. В каждой группе можно включить или отключить LACP (Link Aggregation Control Protocol). Ограничение: для каждого порта группы должно быть установлено одно и тоже время задержки LACP (возможно задать 30 сек или 1 сек) – это время, в течение которого коммутатор будет использовать текущую конфигурацию как работоспособную. Если за это время одно из физических соединений станет недоступным для передачи данных, часть передаваемых кадров будет потеряна.

LACP позволяет обеспечить отказоустойчивость соединения. Так, если передача по одной из линий невозможна, все данные будут передаваться по работоспособным линиям. LACP работает только на линиях с полнодуплексным режимом.

Команды CLI
lacp <cr>
lacp system-priority <1-65535>

2.8 Зеркалирование портов

Port mirroring (зеркалирование портов) позволяет копировать трафик на порт мониторинга, к которому необходимо подключить сетевой анализатор трафика (sniffer). Возможно копирование как одного из потоков (входящего/исходящего), так и обоих потоков, с одного или нескольких портов.

Для настройки этой функции необходимо включить функцию зеркалирования в соответствующем меню, выбрать порт, на который будут дублироваться кадры (Monitor Port), и выбрать направления. После этого необходимо выбрать зеркалируемые т.е. отслеживаемые порты (Mirrored), данные с которых будут дублироваться на порт Monitor. Порт, который выбран как Monitor Port, нельзя указать как Mirrored.

Следует учитывать, что зеркалирование удобнее выполнять с помощью классификатора и политики, т.к. в этом случае можно анализировать не весь подряд трафик, а только пакеты определенного типа.

Команды CLI

mirror-port <cr>
mirror-port <port num>
interface port-channel <port-list> mirror <cr>
interface port-channel <port-list> mirror dir <ingress|egress|both>

2.9 Разграничение доступа с использованием виртуальных сетей (VLAN)

В современных сетях логические сети - VLAN (Virtual Local Area Network) — главный механизм для создания логической топологии сети, не зависящей от её физической топологии.

VLAN— группа узлов сети, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам, и наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях. За каждым портом коммутатора может быть закреплена конкретная VLAN, которая может быть логически сегментирована в соответствии с ее функциями и задачами. Порты одной VLAN имеют общий домен циркулярной рассылки. Порты, относящиеся к различным VLAN, не могут осуществлять циркулярную рассылку.

Цели разделения локальной сети на логические подсети:

- Разделение физической ЛВС на несколько логических подсетей
- Изолирование каждого порта для увеличения безопасности
- Изолирование широковещательного трафика

Можно повысить уровень безопасности путем сегментирования сети на отдельные домены циркулярной рассылки. Кроме того, можно регулировать размер и структуру домена путем регулирования размера и структуры VLAN.

VLAN позволяют группировать порты коммутатора таким образом, чтобы трафик ограничивался только членами той или иной группы. Данная функция ограничивает циркулярную, одноадресную и многоадресную рас-

сылку (лавинная адресация) только портами, включенными в конкретную VLAN, что делает возможным эффективное разделение трафика, тем самым, обеспечивая более высокую пропускную способность.

2.9.1 Виртуальная локальная сеть на основе группировки портов (Port-based)

VLAN на основе группировки портов позволяет создавать VLAN из различных портов одного моста или коммутатора.

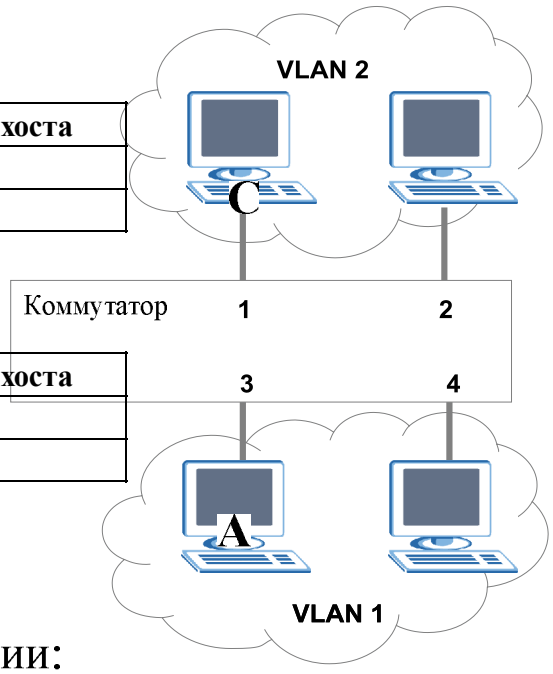
Каждый порт коммутатора приписывается к той или иной виртуальной сети, то есть порты группируются в виртуальные сети. Решение о продвижении сетевого пакета в этой сети основывается на MAC-адресе получателя и ассоциированного с ним порта. Если к порту, которому назначена принадлежность к определенной виртуальной сети, например к VLAN 1, подключить ПК пользователя, то этот ПК автоматически будет принадлежать сети VLAN 1. Если же к данному порту подключается коммутатор, то все порты этого коммутатора также будут принадлежать VLAN 1 (рис. 12). Технология VLAN на основе группировки портов в коммутаторах ZyXEL L2+ и L3+ позволяет управлять только исходящим трафиком. Таблицы коммутации при построении VLAN на основе группировки портов показаны на рисунке 12.

Для VLAN'a 1:

Порт коммутатора	MAC-адрес хоста
1	A
2	B

Для VLAN'a 2:

Порт коммутатора	MAC-адрес хоста
3	C
4	D



Реальная таблица коммутации:

Порт коммутатора	VLAN	MAC-адрес хоста
1	1	A
2	1	B
3	2	C
4	2	D

Рис.12. Построение VLAN на основе группировки портов в коммутаторе

При использовании технологии группировки портов один и тот же порт может быть одновременно приписан к нескольким виртуальным сетям, что позволяет реализовывать разделяемые ресурсы между пользователями различных виртуальных сетей. Например, чтобы реализовать совместный доступ к сетевому принтеру или к файл-серверу пользователей виртуальных сетей VLAN 1 и VLAN 2, тот порт коммутатора, к которому подключается сетевой принтер или файл-сервер, нужно приписать одновременно к сетям VLAN 1 и VLAN 2. Настройка VLAN на основе группировки портов в коммутаторах ZyXEL представляет из себя матрицу, показанную на рисунке 13, ячейки которой говорят о наличии связи между соответствующими портами.

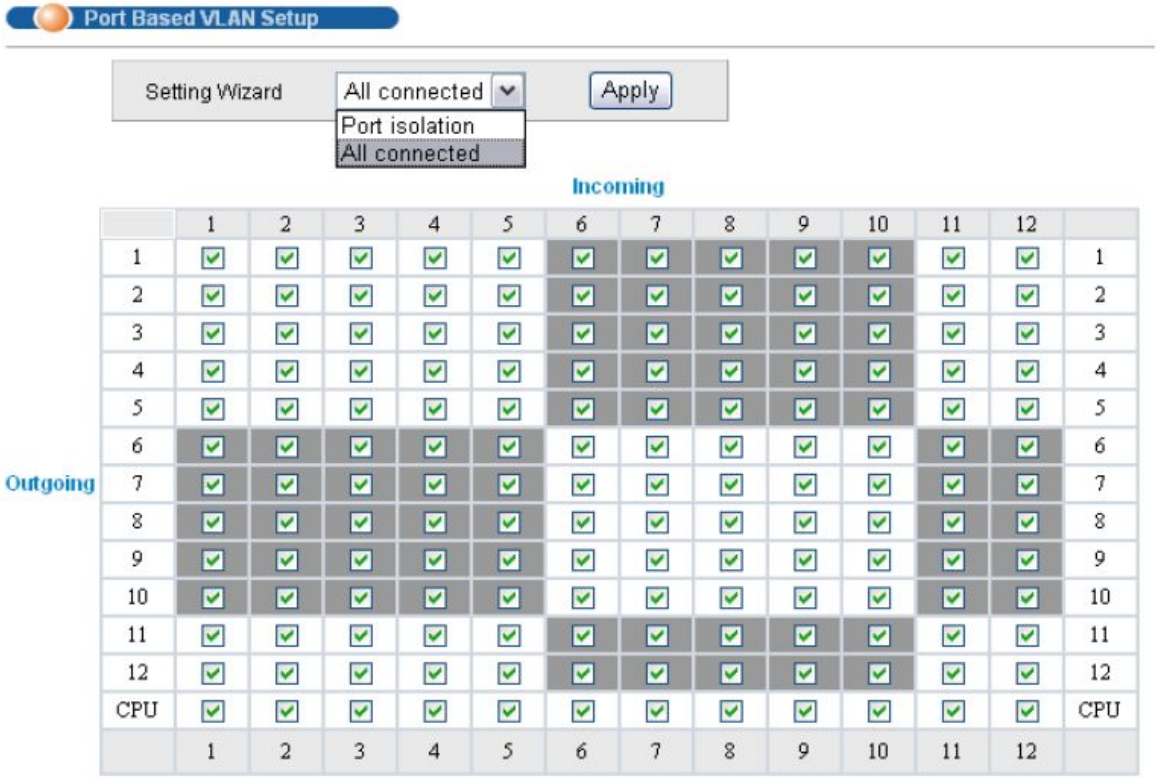


Рис. 13. Настройка VLAN на основе группировки портов в коммутаторах ZyXEL

2.9.2 Виртуальная локальная сеть на основе стандарта IEEE 802.1Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети, т.е. информация о принадлежности передаваемых Ethernet-кадров к той или иной виртуальной сети встраивается в сам передаваемый кадр (рис.14).

До появления общепризнанного стандарта по организации виртуальных сетей IEEE 802.1Q каждый производитель сетевого оборудования использовал собственную технологию организации VLAN. Такой подход

имел существенный недостаток — технологии одного производителя были несовместимы с технологиями других фирм. Поэтому при построении виртуальных сетей на базе нескольких коммутаторов необходимо было использовать только оборудование от одного производителя. Принятие стандарта виртуальных сетей IEEE 802.1Q позволило преодолеть проблему несовместимости, однако до сих пор существуют коммутаторы, которые либо не поддерживают стандарт IEEE 802.1Q, либо, кроме возможности организации виртуальных сетей по стандарту IEEE 802.1Q, предусматривают и иные технологии.

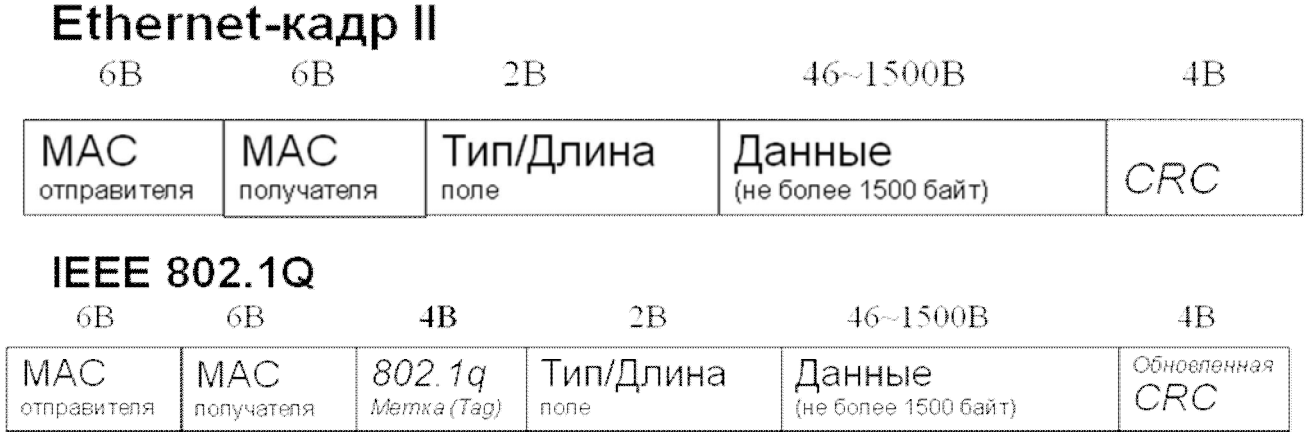


Рис. 14. - Кадр Ethernet и кадр 802.1Q содержащий принадлежность к VLAN

К кадру Ethernet добавляются 4 байта. TPID (Tag Protocol Identifier) – 2 байта, которые содержат информацию о принадлежности кадра Ethernet к протоколу 802.1Q и TCI (Tag Control Information). Добавление четырех байтов к максимальному размеру кадра Ethernet ведет к возникновению проблем в работе многих коммутаторов, обрабатывающих кадры Ethernet аппаратно. Чтобы избежать их, группы по стандартизации предложили сократить на два байта максимальный размер полезной нагрузки в кадре. Спецификация IEEE 802.1p, создаваемая в рамках процесса стандартизации 802.1Q, определяет метод передачи информации о приоритете сетевого трафика. Стандарт 802.1p специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка чувствительного к временным задержкам трафика.

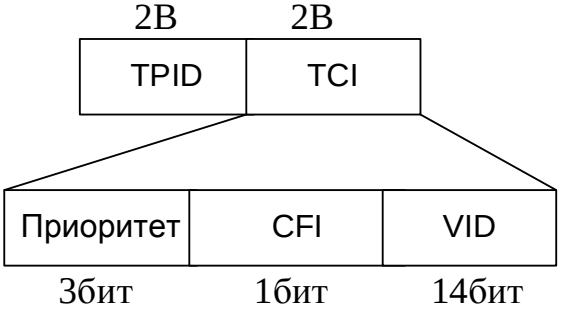


Рис. 15. - Структура метки (Tag)

Метка IEEE 802.1Q (рис. 15) имеет следующие поля:
TPID: Признак идентификатора протокола, для 802.1Q TPID принимает значение 8100_{16}

TCI содержит три поля:

- Поле Приоритета (User Priority) – Первые три бита TCI используется под приоритет. Возможно восемь значений (2^3) приоритета. Устройства, реализующие протокол IEEE 802.1P работает именно с этими 3 битами приоритета.
- CFI – Canonical Format Indicator однобитовый флаг, который всегда равен 0 для кадров Ethernet. CFI для идентификации, если в поле данные находятся данные других стандартов, не Ethernet, например Token Ring. В этом случаи этот бит будет равен 1. Если кадр был получен с Ethernet порта и CFI равен 1, то этот кадр должен быть перенаправлен на untagged порт.
- VID – VLAN ID идентификатор VLAN, который и используется в стандарте 802.1Q. Это поле состоит из 12 бит и позволяет закодировать значения 4096 (2^{12}) VLAN-ов. Из 4096 возможных значений, VID равное 0 и 4095 (FFF) зарезервированы, поэтому максимальное количество VLAN, которые работают в сети равно 4094. VID = 0 определяет, что данный кадр не несет информации о VLAN, а несет только информацию о приоритете. VID = 4095 в оборудовании используется для внутренней коммутации. 802.1Q Tag VLAN:

Сетевые устройства, подключенные к портам с одинаковыми VID могут взаимодействовать друг с другом и обмениваться кадрами.

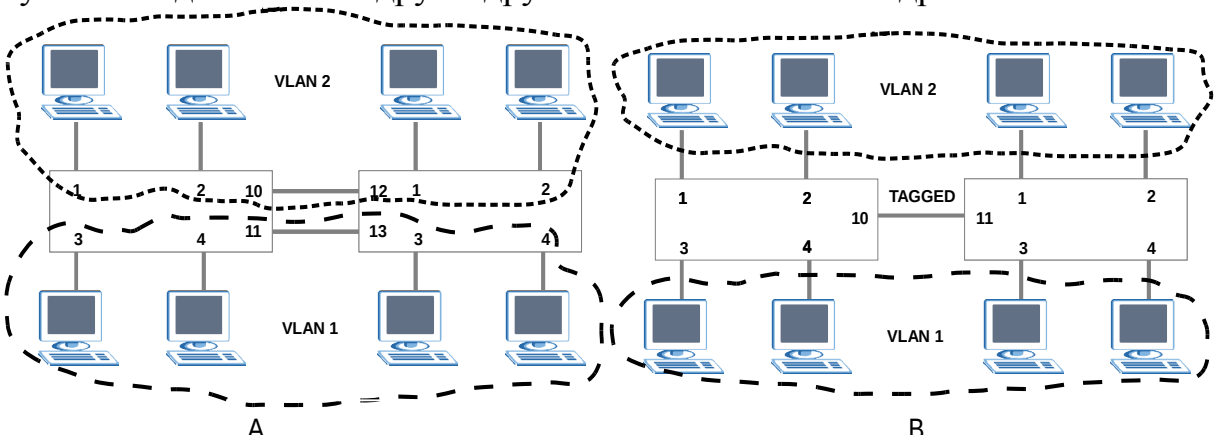


Рис. 16. Объединение узлов в разных VLAN на разных коммутаторах

Когда необходимо передать трафик одного-двух VLAN-ов между коммутаторами, то схема, которая использовалась выше выглядит нормально. Однако, когда количество VLAN возрастает, то схема явно становится очень неудобной, так как для каждого VLAN надо будет добавлять линк между коммутаторами для того чтобы объединить хосты в один широковещательный сегмент (рис. 16а), еще более усложняет схему организа-

ция VLAN в сети с несколькими коммутаторами.

Для решения этой проблемы используются тегированные порты, которые позволяют коммутатору передать трафик нескольких VLAN-ов через один порт и сохранить при этом информацию о том, в пределах какого именно VLAN-а передается кадр (рис. 16б).

Для присвоения портам идентификаторов VLAN согласно протоколу 802.1Q используется страница показанная на рисунке 17.

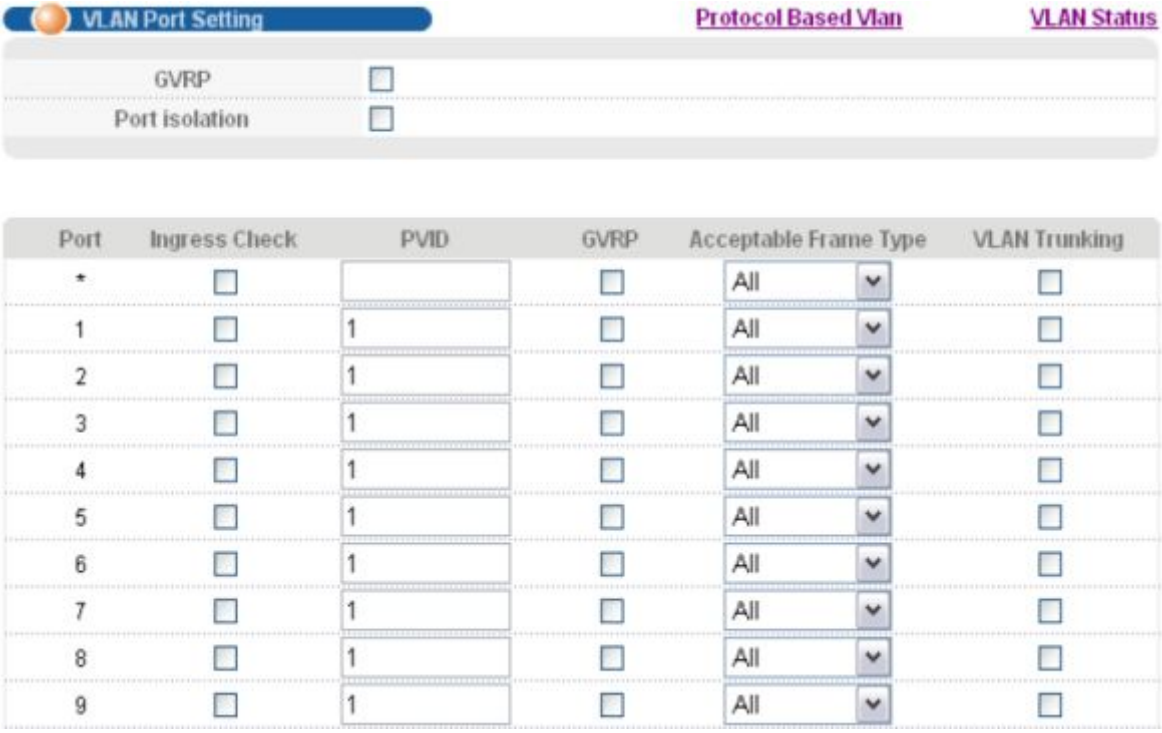


Рис. 17. Настройка портов для организации VLAN в коммутаторах ZyXEL

Для каждого порта имеется набор полей (см. рис. 17):

1. PVID – идентификатор VLAN.
2. Acceptable Frame Type - типы принимаемых кадров: все или только тегированные.
3. VLAN Trunking - когда опция включена, все исходящие кадры выходят из этого порта тегированными, если явно не указано обратное. В коммутаторе, особенно если он работает где-то в центре сети, могут регистрироваться динамические VLAN, которые нужно «проводить» прозрачно в другие участки сети. В этом случае и требуется включить опцию VLAN Trunking. В противном случае пришлось бы в явном виде вводить все возможные VLAN в таблицу.
4. Ingress check - если опция включена, то на порт принимаются только кадры с идентификаторами.
5. VLAN ID, для которых указанный порт является выходным.
6. GVRP - протокол передачи информации о VLAN по сети с одного коммутатора на другой. Если требуется поддержка передачи информации о

VLAN между коммутаторами, его нужно включить как на всем коммутаторе, так и на портах, идущих к соседним коммутаторам.

7. Port Isolation – если опция включена, то данные не могут передаваться с одного порта на другой. Разрешен только обмен данными между портами и коммутатором (CPU) для настройки.

Команды CLI

interface port-channel <port-list> pvid <1-4094>
interface port-channel <port-list> ingress-check
interface port-channel <port-list> gvrp
interface port-channel <port-list> frame-type <all|tagged|untagged>
interface port-channel <port-list> name <port-name-string>
interface port-channel <port-list> vlan-trunking
interface port-channel <port-list> flow-control

ПРИЛОЖЕНИЕ 1 УТИЛИТА NETPERF

Netperf это свободно распространяемая утилита, которая была разработана компанией Hewlett-Packard. Она позволяет получить мгновенную информацию о пропускной способности сети. Обновленная информация об утилите Netperf предоставляется на сайте утилиты по адресу **netperf.org**, где можно получить версию утилиты для операционных систем Linux, Windows (см рис. 11), Mac OS X, так же версию утилиты можно загрузить с сайта кафедры ОПДС **www.opds.sut.ru.**

Рис. 11. Netperf 2.4.5 для windows xp/2003/7 - 32 бит

Netperf - это инструмент, который быстро даст количественный ответ о пропускной способности сети между двумя точками. Он не только прост в использовании, но и очень компактен для размещения на любом носителе, что позволяет переносить его на удаленные компьютеры и сайты.

Утилита состоит из двух исполняемых файлов: Netserver и Netclient. Для выполнения теста пропускной способности необходимо запустить Netserver на одном компьютере, а Netclient на другом компьютере. Программа Netclient предоставляет множество параметров собственного запуска. Вот синтаксис этой команды:

Netclient -H <удаленный_узел> [-a <send,recv>] [-A <send,recv>] [-c] [-C] [-d] [-f <G | M | K | g | m | k>] [-F <файл_заполнения>] [-i <max,min>] [-I <lvl>] [-l <секунд>] [-o <send,recv>] [-O <send,recv>] [-n <numcpu>] [-p <порт>] [-P < 0 | 1 >] [-t <testname>] [-v <уровень_сообщений>] [-W <send,recv>]

Параметры утилиты Netclient рассматриваются в таблице 1.

Табл. 1 Параметры команды Netclient

Параметр	Использование
-H <удаленный_узел>	Имя или адрес IP системы, которая поддерживает работу Netserver
-a <send,recv>	Устанавливает отношение локального буфера приема/отправки
-A <send,recv>	Устанавливает отношение удаленного буфера приема отправки

-c	Сообщает статистику использования центрального процессора на локальном компьютере
-C	Сообщает статистику использования центрального процессора на удаленном компьютере
-d	Увеличивает избыточность отладочной информации
-f <G|M|K|g|m|k>	Устанавливает единицу изменения для указания пропускной способности. По умолчанию пропускная способность указывается в мегабайтах (M).
-F <файл_заполнения>	Наполняет буфер данными из указанного файла
-i <max,min>	Указывает максимум и минимум выполняемых итераций. По умолчанию используются значения 15 и 1.
-I <lvl>	Указывает уровень уверенности команды. Приемлемыми уровнями являются уровни от 95 до 99 (по умолчанию используется значение 99)
-l <секунд>	Указывает длительность работы Netperf (в секундах)
-o <send,recv>	Устанавливает смещение локального буфера приема/отправки
-O <send,recv>	Устанавливает смещение удаленного буфера приема отправки
-n <cpu>	Устанавливает минимальное количество процессоров, которые можно использовать
-p <порт>	Когда программа Netserver ожидает входящего соединения на порту, отличном от принятого по умолчанию (12865), этот параметр необходимо для указания номера порта, на котором ожидает соединений утилита Netserver
-P <0|1>	Отображает (1) или подавляет (0) вывод заголовков в выводе команды
-t <testname>	Указывает имя теста, который необходимо выполнить
-v <уровень_сообщений>	Указывает уровень подробности сооб-

	щений (1-3) в выводе команды
-W <send,recv>	Устанавливает количество буферов приема/передачи

Утилита *Netserver* предоставляет только один параметр – TCP порт. Вот синтаксис команды *Netserver*:
Netserver [-p <номер_ TCP порта>]

По умолчанию, при запуске утилиты Netserver используется TCP порт номер 12865. Использование параметра *-p* позволяет указать другой порт, на котором утилита будет ожидать входящих соединений. Сразу же после запуска утилита Netserver будет работать, пока с ней не установит связь клиент.

Хотя существует множество параметров, предоставляемых командой Netclient, для тестирования пропускной способности сети необходимы только параметры *-H* и, возможно, *-p*, если тестирование производится сквозь брандмауэр, установленный между двумя точками.

После копирования файлов необходимо выполнить такую последовательность действий для тестирования пропускной способности:

1. На удаленном компьютере откройте приглашение командной строки и запустите утилиту Netserver (команду необходимо давать в той папке, где находится исполнимый файл).
2. На второй системе введите команду *Netclient -H <имя_удаленного_сервера>* из приглашения командной строки.
3. Подождите несколько секунд и система, на которой был запущен Netclient, отобразит пропускную способность сети. Кроме того, выполнение команды Netserver автоматически завершиться на первой системе.

Глоссарий

802.1Q — стандарт VLAN на базе тега.
AC (Alternate Current) — переменный ток.
BPDU (Bridge Protocol Data Unit) — кадр, используемый протоколом STP/RSTP при построении дерева.
CLI (Command Line Interface) — интерфейс командной строки.
DA (Destination Address) — адрес назначения.
DSCP (DiffServ Code Point) — 6-битовое поле в заголовке IP-пакета, обычно используется для приоритезации.
DVMRP (Distance Vector Multicast Routing Protocol) — дистанционно-векторный протокол маршрутизации групповых рассылок (RFC 1075).
EAP (Extensible Authentication Protocol) — расширяемый протокол аутентификации. Известные расширения этого протокола: EAP-MD5, EAP-TLS (со взаимной аутентификацией сторон с помощью сертификатов) и EAP-TTLS (с аутентификацией сервера на основе сертификата и аутентификацией клиента по логину и паролю).
FCS (Frame Check Sum) — контрольная сумма кадра.
GARP (Generic Attribute Registration Protocol) — протокол общего назначения для регистрации атрибутов.
GUI (Graphical User Interface) — графический интерфейс пользователя, например web-браузер.
GVRP (GARP VLAN Registration Protocol) — протокол динамической регистрации VLAN, основанный на GARP.
HDAP (Host Discovery and Address assignment Protocol) — протокол для обнаружения узла и назначения адреса, используется устройствами ZyXEL для централизованного управления iStacking.
IGMP (Internet Group Management Protocol) — протокол управления группами
многоадресных рассылок. (RFC 1112, RFC 2236, RFC 3376).
L/T (Length/Type) — поле Типа/Длины кадра Ethernet.
LACP (Link Aggregation Control Protocol) — протокол управления агрегированными каналами.
MAC (Media Access Control) — управление доступом к среде. **MAC-адрес** — адрес устройства в локальной сети.
MSTP (Multiple Spanning Tree Protocol) — алгоритм покрывающего дерева, работающий внутри VLAN. VLAN в сети может быть несколько, отсюда и название алгоритма (IEEE 802.1s).
MRSTP (Multiple RSTP) — реализация RSTP в некоторых коммутаторах ZyXEL, позволяющая включать один коммутатор в несколько деревьев RSTP. Для этого на коммутаторе указываются группы портов, относящихся к различным экземплярам RSTP.

MTU (Maximum Transfer Unit) — максимальный размер пакета, допустимый к передаче в данном сегменте локальной сети.
MVR (Multicast VLAN Registration) — метод отправки групповых рассылок в отдельном VLAN .
NAT (Network Address Translation) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса проходящих пакетов. (RFC 1631, RFC 3022)
NAPT (Network Address Port Translation) — частный случай механизма NAT, который помимо подмены IP-адресов проходящих пакетов обеспечивает подмену TCP/UDP портов проходящих пакетов. (RFC 3022)
OSPF (Open Shortest Path First) — протокол маршрутизации (RFC 2328).
PEAP (Protected Extensible Authentication Protocol) — защищенный расширяемый протокол аутентификации. Приблизительно то же самое, что EAP-TTLS, инициатива Microsoft и Cisco.
QoS (Quality of Service) — качество обслуживания.
RADIUS (Remote Authentication Dial-In User Service) — служба, отвечающая за аутентификацию пользователей. На сервере RADIUS хранится информация о пользователях и паролях (RFC 2865, RFC 2866).
RIP (Routing Information Protocol) — дистанционно-векторный маршрутизирующий протокол. Из-за медленной сходимости применяется только в небольших сетях (RFC 1058, RFC 2453).
RFC (Request For Comment) — общее название документа-рекомендации комитета IETF (Internet Engineering Task Force).
RSTP (Rapid Spanning Tree Protocol) — улучшенная редакция протокола STP с быстрым восстановлением связности сети при разрывах в активной топологии (IEEE 802.1w).
SA (Source Address) — адрес источника.
SFP (Small Factor Pluggable) — универсальный модуль для подключения оптоволоконного канала к коммутатору.
SPQ (Strict Priority Queueing) — алгоритм обработки очередей на порту коммутатора.
STP (Spanning Tree Protocol) — протокол покрывающего дерева, служит для удаления циклов из сети(IEEE 802.1d).
TCI (Tag Control Information) — управляющая информация, содержащаяся в теге 802.1Q.
TOS (Type of Service) — флаговое поле в заголовке IP-пакета. Флаги отвечают за тип обслуживания - «наилучшее время», «наименьшая стоимость» и т. п.
TPID (Tag Protocol Identifier) — идентификатор протокола тега (маркера) 802.1Q.
VID (VLAN Identifier) — идентификатор VLAN.
VLAN (Virtual Local Area Network) — виртуальная локальная сеть.

VRRP (Virtual Router Redundancy Protocol) — протокол виртуального отказоустойчивого маршрутизатора (RFC 3768).

WDM (Wavelength Division Multiplexing) — метод полнодуплексной передачи данных по одному оптоволоконному кабелю, когда прямой и обратный сигналы передаются на различных длинах волн.

WFQ (Weighted Fair Queuing) — алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и объеме отправляемых данных.

WRR (Weighted Round Robin) — простой циклический алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и количестве отправляемых пакетов.

Бородко Александр Владимирович

ДИСЦИПЛИНА
КОМПЬЮТЕРНЫЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ЛАБОРАТОРНЫМ РАБОТАМ С ИСПОЛЬЗОВАНИЕМ КОММУТАЦИОННОГО ОБОРУДОВАНИЯ ZYXEL

Редактор

План 2012 г., п. 9а

Подписано к печати 1.06.2012
Объем 3,75 усл.-печ. л. Тираж 105 экз. Заказ 145

Издательство СПбГУТ. 191186 СПб., наб. р. Мойки, 61
Отпечатано в