ZYXEL

www.zyxel.com

Коммутаторы серий

Zyxel GS1920 / GS2210 / GS2220 / GS3700 /

XGS1930 / XGS2210 / XGS3700 / XGS4600 /

XS1920 / XS1930 / XS3700 / XS3800

Редакция 2020.1

Справочник

Вход в систему по умолчанию	
IP-адрес порта LAN	https://192.168.1.1
User Name	admin
Password	1234

Содержание

Основы управления сетью

1.1 Как изменить используемый для управления IP-адрес коммутатора чтобы получить доступ именно к нему, а не к другому коммутатору

На следующем примере показано, как администратор может с помощью Web-интерфейса менять IP-адреса коммутаторов для того, чтобы получить доступ к конкретному устройству если в сети есть два коммутатора с одинаковым IP-адресом 192.168.1.1.

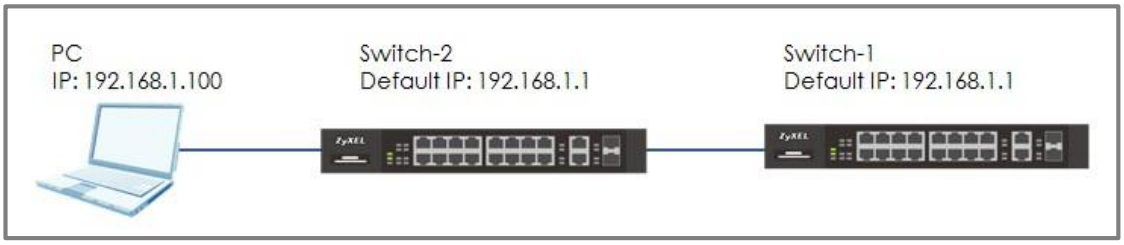


Иллюстрация 1 У двух коммутаторов один и тот же IP-адрес по умолчанию

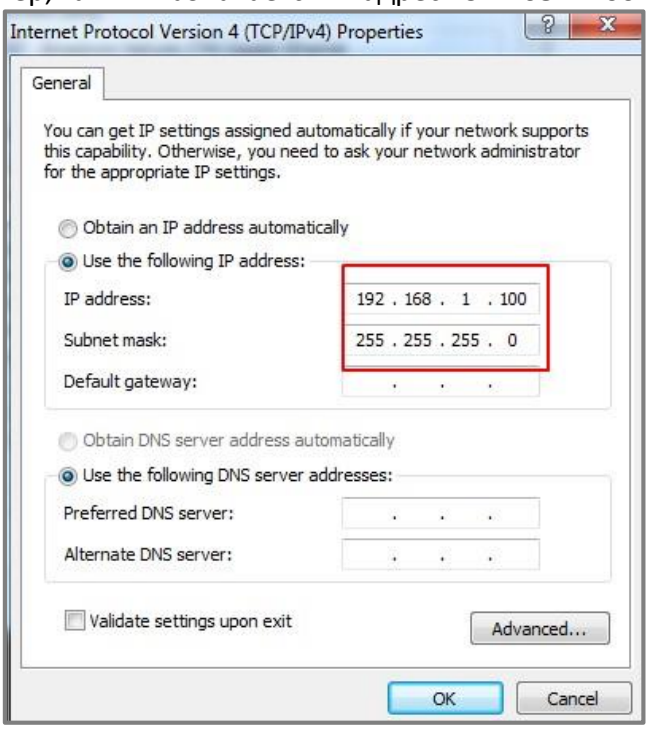
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.1.1 Настройка конфигурации коммутатора 2 (Switch-2)

1 Разорвите соединение между коммутаторами Switch-1 и Switch-2.

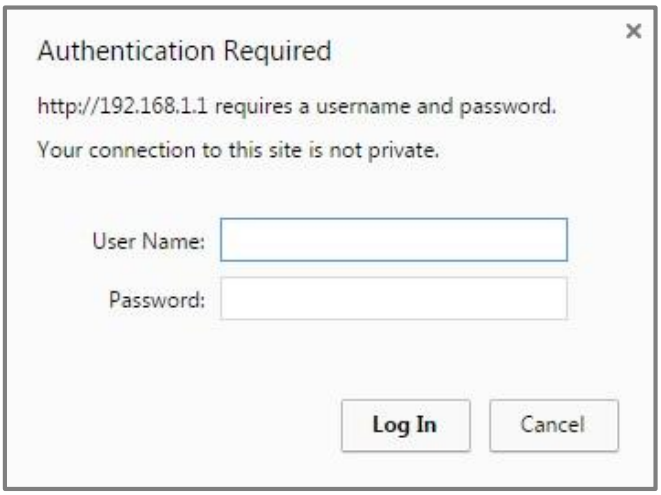
2 Задайте у ПК IP-адрес в той подсети, к которой относятся коммутаторы.

Например, так ПК назначается IP-адрес **192.168.1.100**.



3 Запустите браузер (IE, Chrome, Safari, Firefox и т.п.). Введите в его адресной строке **http://192.168.1.1** (IP-адрес управления по умолчанию).

Введите “**username: admin**; **password: 1234**” и щелкните **Log In**.

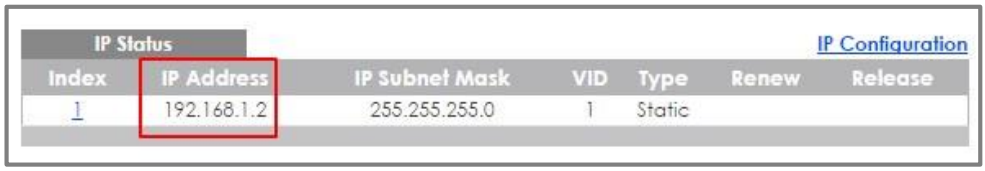


4 На открывшейся web-странице перейдите **Menu > Basic Setting > IP Setup > IP Configuration**. Введите предпочтительный IP-адрес, например, **192.168.1.2**, и затем щелкните **Add**.

5 Заново зайдите в систему по новому IP-адресу **192.168.1.2**. После входа в систему щелкните пиктограмму **Save** для сохранения новой конфигурации.

1.1.2 Проверьте новую конфигурацию

1 Зайдите с помощью web-интерфейса и перейдите **Menu > Basic Setting > IP Setup > IP Configuration**. Убедитесь, что в поле IP-адреса стоит **192.168.1.2**.



1.2 Как настроить имя устройства для коммутатора чтобы получить доступ к нему, а не к другому коммутатору

На следующем примере показано, как администратор может с помощью Web-интерфейса изменить имя устройства у коммутатора для того, чтобы получить доступ к конкретному устройству. В этом примере ПК через сеть подключен к коммутатору Switch-1. По умолчанию имя устройства (System Name) – это названием модели (в данном примере XGS4600).

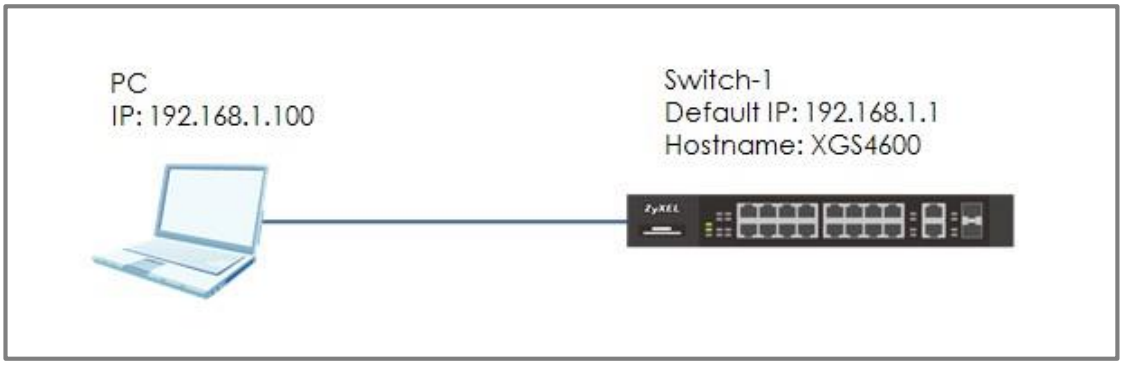
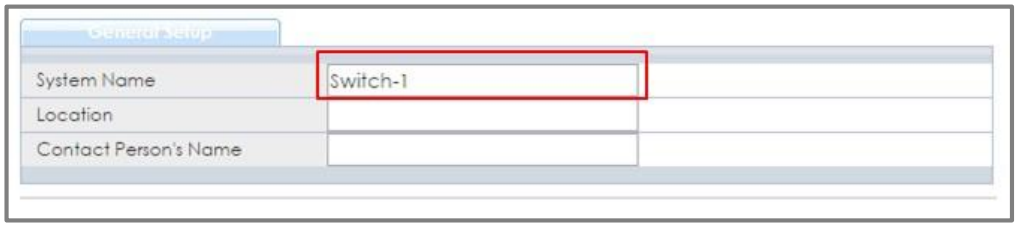


Иллюстрация 2 Изменение имени устройства у коммутатора

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.2.1 Настройка конфигурации коммутатора Switch-1

1 Откройте web-интерфейс и перейдите в **Menu > Basic Setting > General Setup**. Измените System Name (Switch-1 в данном примере) и щелкните **Apply**.



2 Щелкните “**Save”** чтобы сохранить конфигурацию.

1.2.2 Проверьте новую конфигурацию

Откройте web-интерфейс и перейдите на страницу с информацией о коммутаторе. В поле **System Name** должно стоять новое имя коммутатора (в данном случае **Switch-1**).

1.3 Как настроить синхронизацию часов коммутатора с сервером NTP

В следующем примере показано, как администратор может настроить синхронизацию внутренних часов коммутатора с сервером точного времени NTP. В этом примере ПК через сеть подключен к Коммутатору, а Коммутатор подключен к межсетевому шлюзу USG.

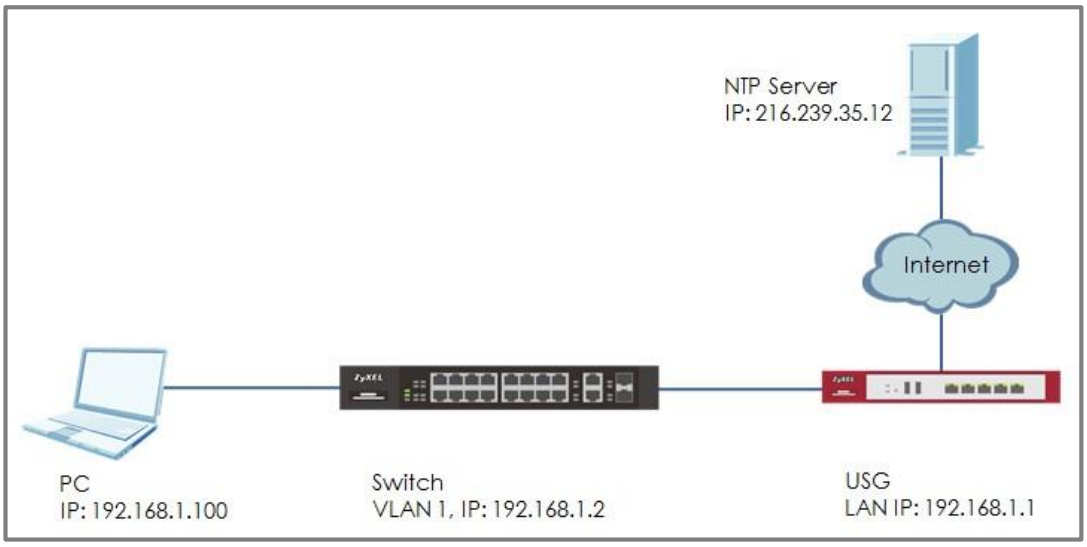


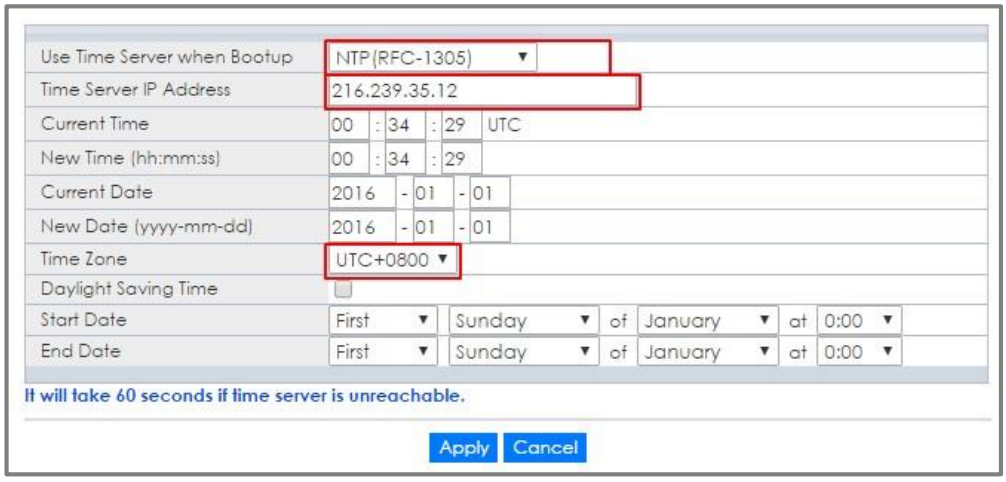
Иллюстрация 3 Настройка синхронизации часов коммутатора с сервером NTP

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50). В качестве сервера NTP использует бесплатный открытый сервер google NTP (216.239.35.12). вместо него вы может использовать другой доступный для вас сервер NTP. Для некоторых моделей коммутаторов интерфейс настройки маршрутизации может немного отличаться от показанного в этом примере.

1.3.1 Настройка конфигурации коммутатора

1 Откройте web-интерфейс и перейдите в **Menu > Basic Setting > IP Setup > IP Configuration**. Введите в поле default Gateway IP-адрес USG: **192.168.1.1**. Затем щелкните “**Apply**”.

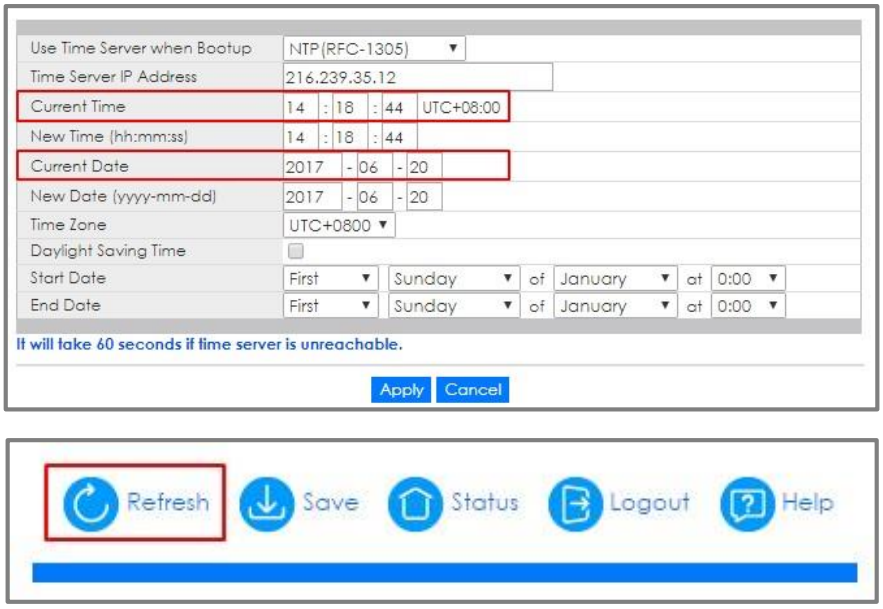
2 Перейдите в **Menu > Basic Setting > General Setup**. В “Use Time Server when Bootup” поставьте **NTP(RFC-1305)** и задайте “Time Server IP Address”. В этом примере используется бесплатный открытый сервер google NTP (**216.239.35.12**). Укажите ваш часовой пояс в поле “Time Zone” и затем щелкните “**Apply**”.



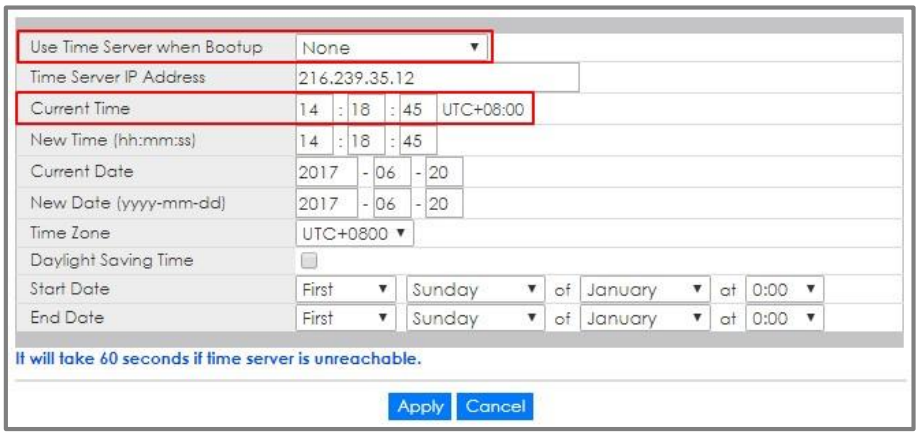
3 Щелкните **Save** для сохранения конфигурации.

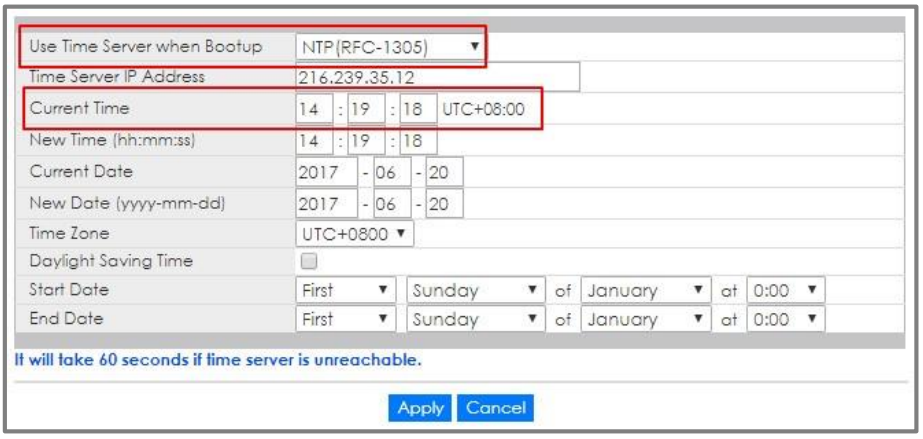
1.3.2 Проверка правильности настройки часов коммутатора

1 Перейдите в **Menu > Basic Setting > General Setup**. Значения Current Time и Current Date должны соответствовать вашему местному времени. Если Current Time не соответствует местному времени, то щелкните “**Refresh**”.



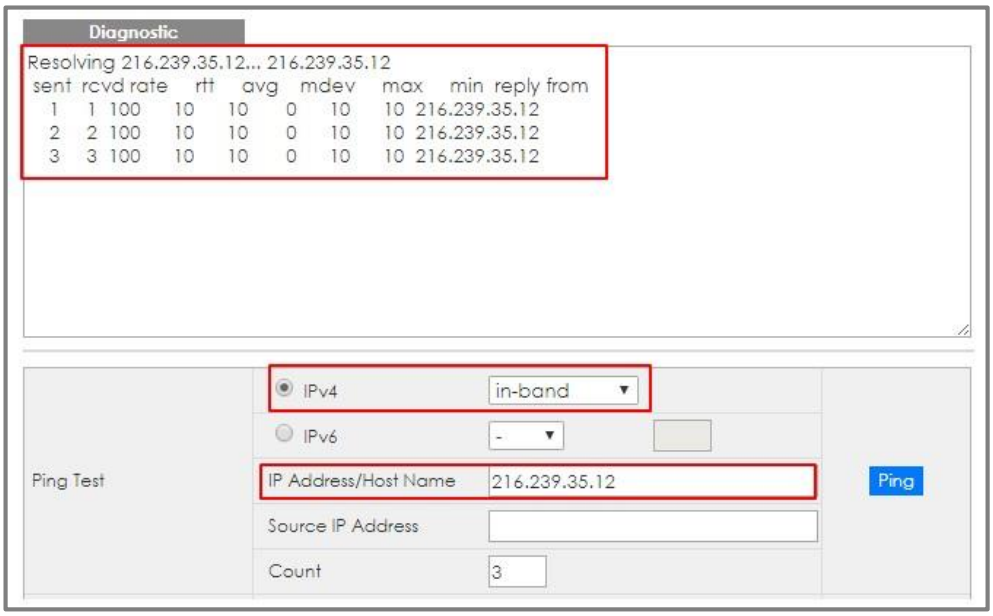
2 Попробуйте поставить **None** в “User Time Server when Bootup” и через несколько секунд обратно поменяйте это поле на **NTP(RFC-1305)**. Время на часах будет синхронизировано с текущим временем.


Use Time Server when Bootup
None
Time Server IP Address
216.239.35.12
Current Time
14 : 18 : 45 UTC+08:00
New Time (hh:mm:ss)
14 : 18 : 45
Current Date
2017 - 06 - 20
New Date (yyyy-mm-dd)
2017 - 06 - 20
Time Zone
UTC+0800
Daylight Saving Time
Start Date
First Sunday of January at 0:00
End Date
First Sunday of January at 0:00
It will take 60 seconds if time server is unreachable.
Apply
Cancel


Use Time Server when Bootup
NTP(RFC-1305)
Time Server IP Address
216.239.35.12
Current Time
14 : 19 : 18 UTC+08:00
New Time (hh:mm:ss)
14 : 19 : 18
Current Date
2017 - 06 - 20
New Date (yyyy-mm-dd)
2017 - 06 - 20
Time Zone
UTC+0800
Daylight Saving Time
Start Date
First Sunday of January at 0:00
End Date
First Sunday of January at 0:00
It will take 60 seconds if time server is unreachable.
Apply
Cancel

1.3.3 Почему не работает синхронизация часов коммутатора?

1 Возможно, у коммутатора нет доступа к серверу NTP. Выполните следующую процедуру для проверки доступности сервера NTP. Перейдите в **Menu > Management > Diagnostic**. Выберите IPv4 в поле **in-band** и введите IP-адрес сервера NTP (216.239.35.12) в поле IP Address. Щелкните “**Ping**”.



1.4 Как настроить сервер на сохранение резервной копии журнала событий на сервере SYSLOG

В этом примере объясняется, как можно настроить коммутатор на пересылку копии журнала событий системы на удаленный сервер syslog.

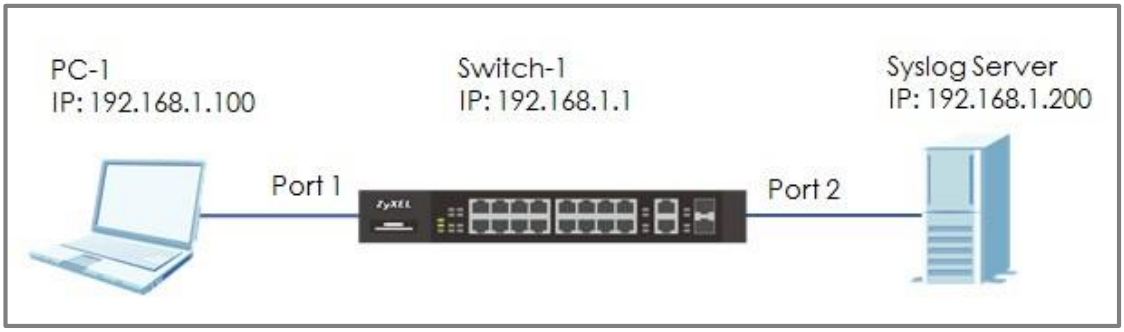


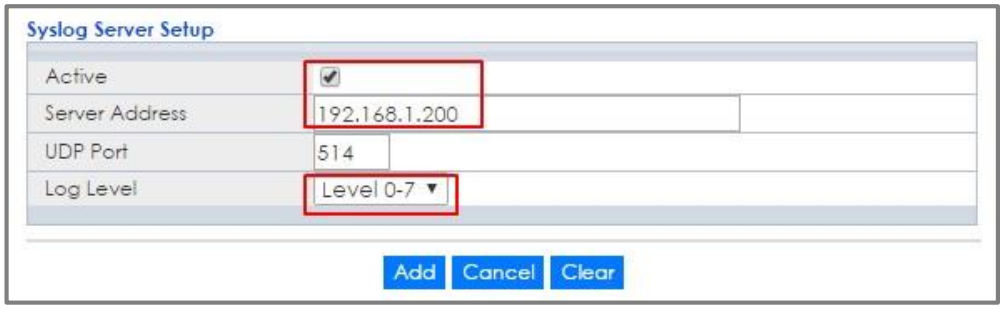
Иллюстрация 4 Автоматическая загрузка журнала событий на сервер

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.4.1 Настройка конфигурации коммутатора Switch-1

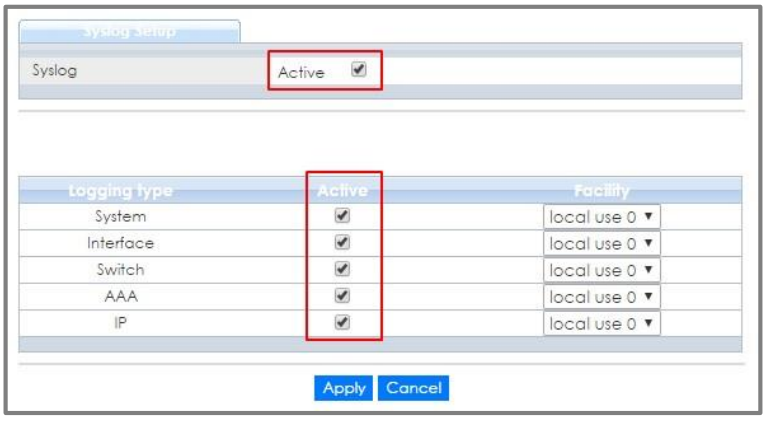
1 Откройте web-интерфейс и перейдите в **Menu > Management > Syslog Setup > Syslog Server Setup**. Поставьте галочку в **Activate** чтобы включить сервер syslog server и введите IP-адрес этого сервера (в данном примере **192.168.1.200**). Выберите предпочитаемый уровень

Log Level (в данном примере **Level 0-7**). Чем шире диапазон, то больше информации будет записываться в журнал. Щелкните “**Add**”.



Примечание:
Log Level определяет, какого уровня важности события будут фиксироваться на сервере Syslog. Важность событий может быть: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7).

2 На этой же странице нужно поставить галочку в поле activate напротив **Syslog** и напротив предпочитаемых типов регистрации событий logging и затем щелкнуть “**Apply**”.

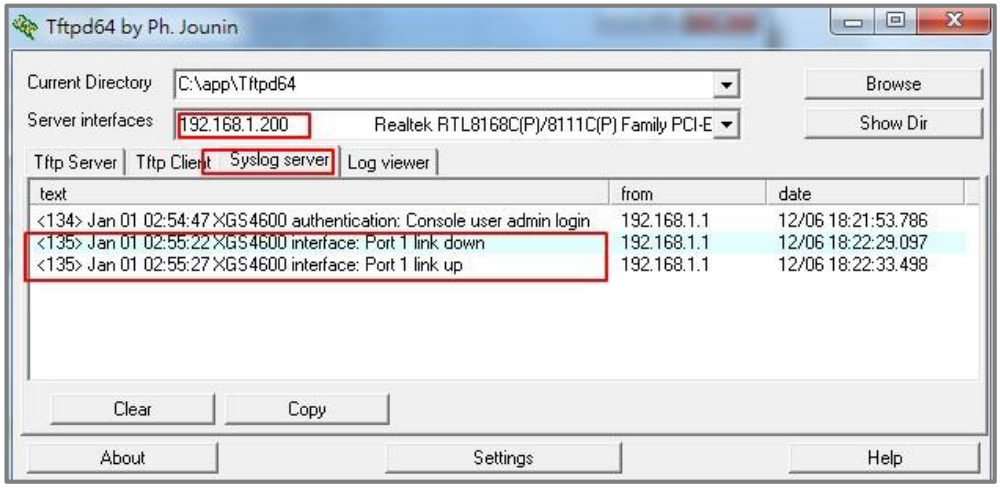


3 Щелкните **Save** для сохранения конфигурации.

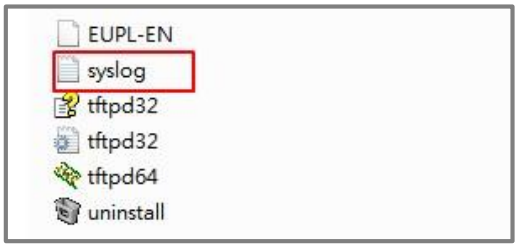
1.4.2 Проверка правильности настройки

1 Отключите и снова подключите ПК PC-1 к коммутатору.

2 Сервер Syslog должен получить от коммутатора журнал событий с такими записями.



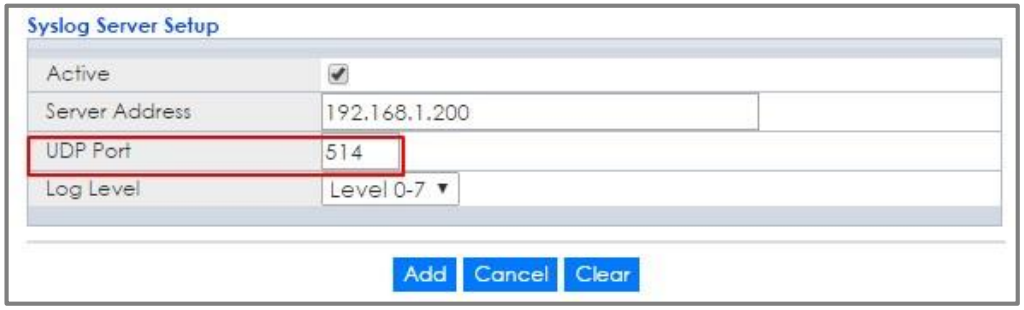
3 Также можно проверить папку **directory** (в данном примере “C:\app\Tftpd64”) чтобы убедиться, что на сервере Syslog создан текстовый файл syslog.



1.4.3 Почему не получается настроить пересылку журнала событий на сервер Syslog?

1 Если коммутатор Switch-1 и сервер Syslog находятся в разных подсетях, то нужно настроить шлюз по умолчанию **default gateway** так, чтобы Switch-1 и Syslog могли обмениваться данными.

2 Убедитесь, что у коммутатора Switch-1 и сервера Syslog совпадают номера порта, используемого для сервиса. (По умолчанию для сервиса Syslog на Switch-1 используется порт **514**).



1.5 Как настроить коммутатор так, чтобы можно было сразу идентифицировать устройства, напрямую подключенные к его порту

В этом примере объясняется, как настроить коммутатор так, чтобы можно было легко идентифицировать устройство или сегмент сети, подключенные к его порту.

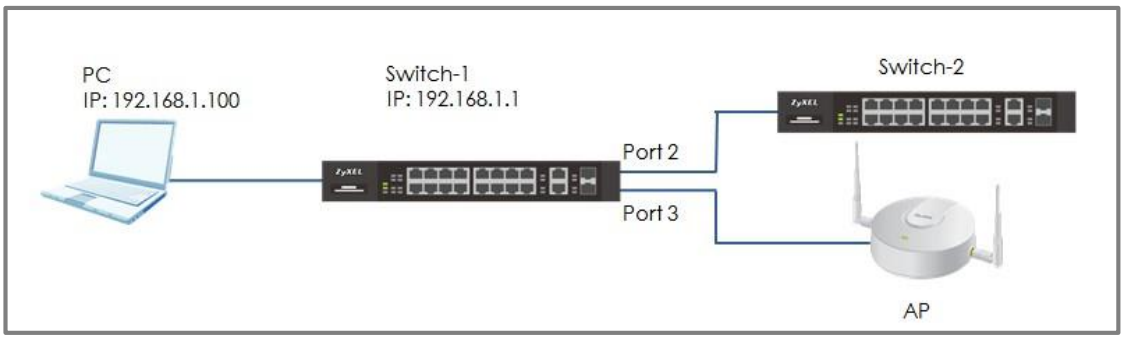
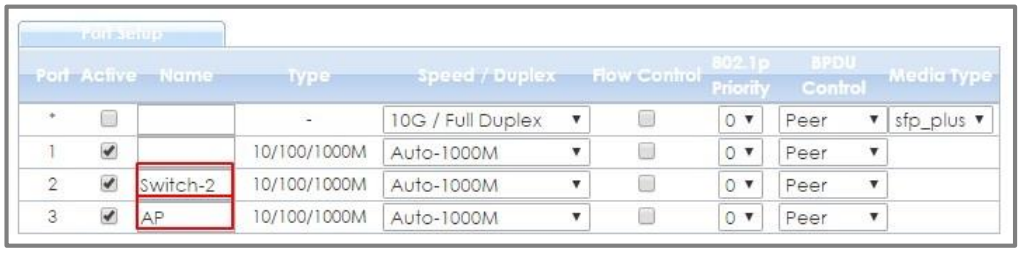


Иллюстрация 5 Настройка имени порта коммутатора

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.5.1 Настройка конфигурации коммутатора Switch-1

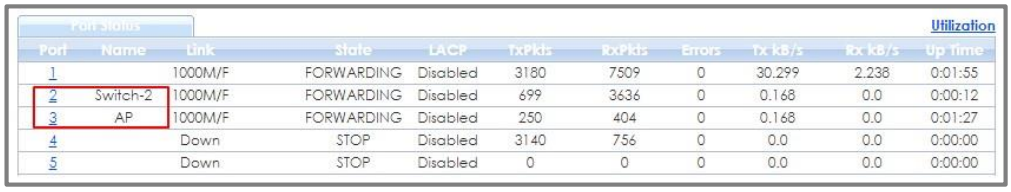
1 Откройте Web-интерфейс и перейдите в **Menu > Basic Setting > Port Setup**. Напротив имени каждого порта введите имя подключенного к нему устройства, например, Switch2 напротив порта port 2 и AP напротив порта port 3. Щелкните “**Apply**”.



2 Щелкните **Save** для сохранения конфигурации.

1.5.2 Проверка правильности конфигурации

1 Перейдите в **Menu > Maintenance > Port Status**. В колонке Name должны стоять введенные вами имена.



Port Status — Utilization

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx kB/s	Rx kB/s	Up Time
1		1000M/F	FORWARDING	Disabled	3180	7509	0	30.299	2.238	0:01:55
2	Switch-2	1000M/F	FORWARDING	Disabled	699	3636	0	0.168	0.0	0:00:12
3	AP	1000M/F	FORWARDING	Disabled	250	404	0	0.168	0.0	0:01:27
4		Down	STOP	Disabled	3140	756	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

1.6 Как получить диагностическую информацию

В этом примере объясняется, как с помощью web-интерфейса получить диагностическую информацию. Диагностическая информация Diagnostic Info – это набор журналов, куда заносится полезная информация, включая информацию о системе System Information, историю использования центрального процессора CPU utilization history, журналы событий системы и отчеты об отладке. С помощью этой информации можно анализировать проблемы в работе коммутатора и сети.

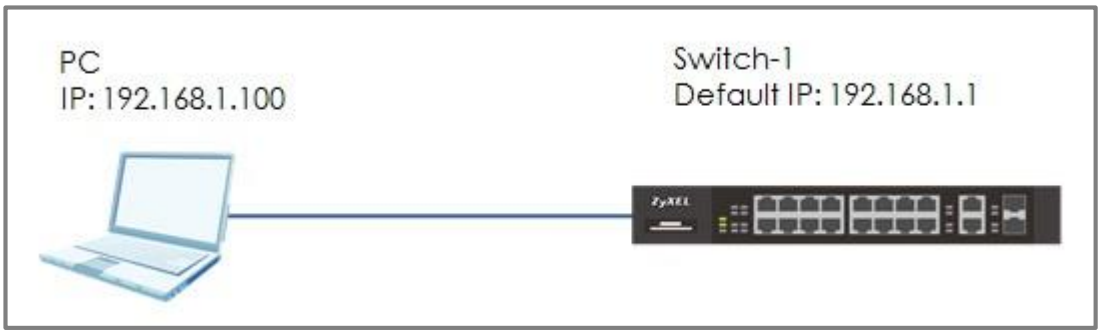
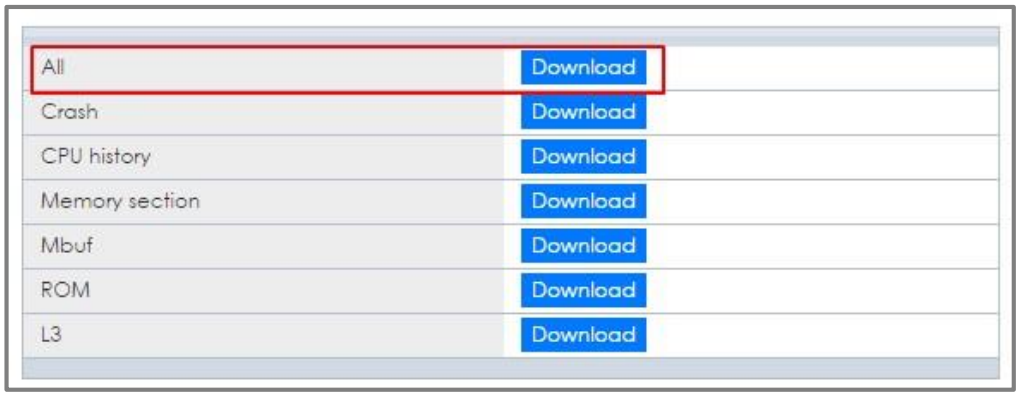


Иллюстрация 6 Получение диагностической информации с помощью web-интерфейса

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

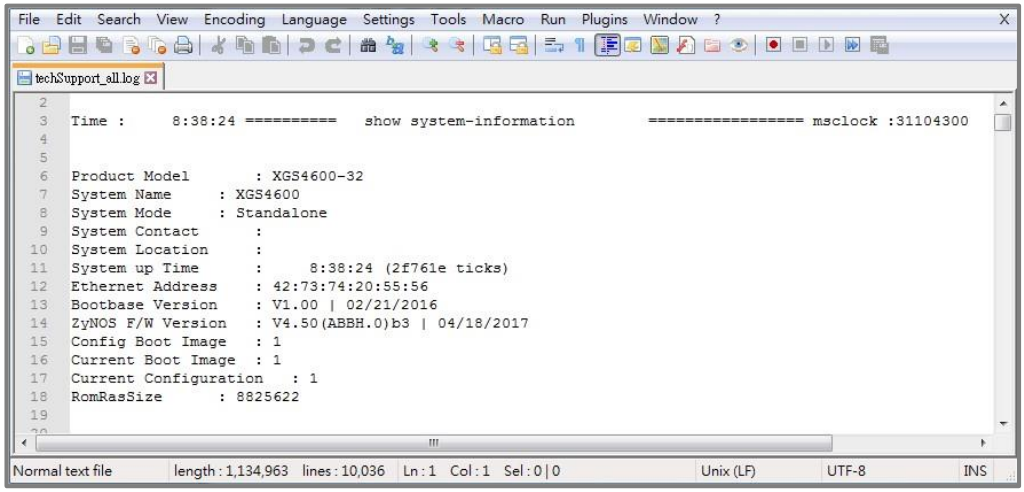
1.6.1 Получение диагностической информации с помощью web-интерфейса

1 Откройте web-интерфейс и перейдите в **Menu > Management > Maintenance > Tech-Support > Click Here**. Щелкните кнопку Download напротив **All**. Также можно выбрать диагностическую информацию определенного типа, например, Crash или ROM.



1.6.2 Проверка результатов

1 Откройте полученный текстовый файл с диагностической информации (в данном примере для просмотра этого файла используется текстовый редактор **Notepad++**.)



1.7 Как изменить пароль администратора по умолчанию

В этом примере показано, как можно изменить пароль администратора по умолчанию, используемый для управления коммутатором. Мы настоятельно рекомендуем проделать эту процедуру, поскольку использование пароля администратора по умолчанию создает риск неавторизованного доступа к средствам управления коммутатором.

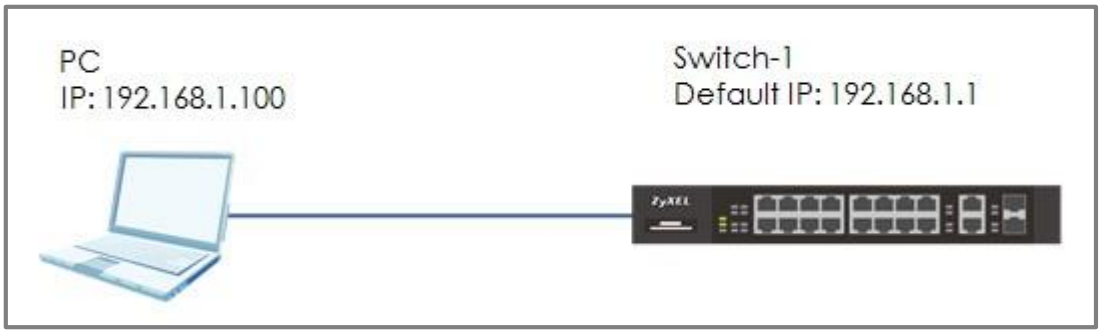
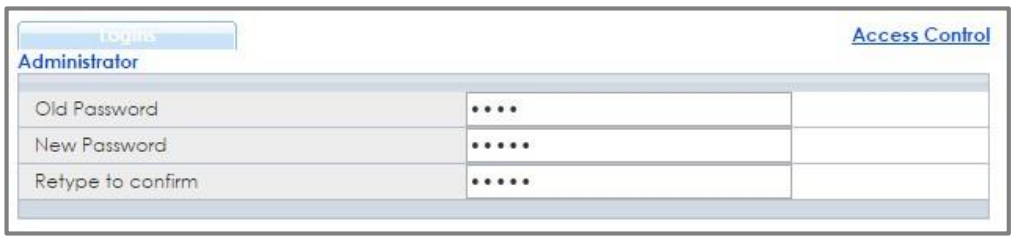


Иллюстрация 7 Изменение пароля администратора по умолчанию

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.7.1 Изменение пароля администратора по умолчанию

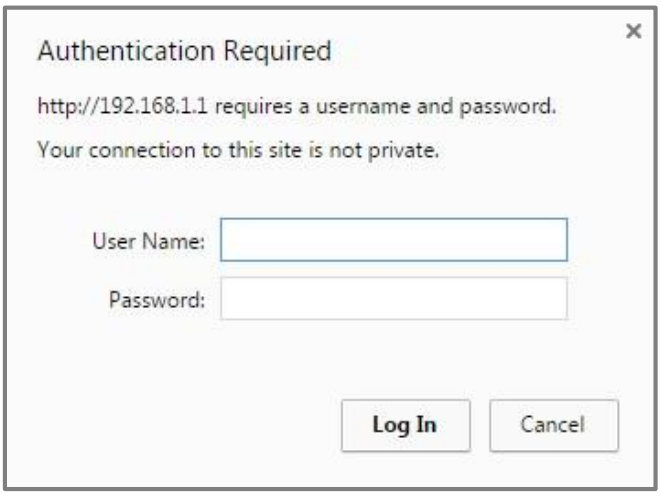
1 Откройте web-интерфейс и перейдите в **Menu > Management > Access Control > Logins > Click Here**. Введите новый и старый пароль (Old Password и New Password), затем щелкните “**Apply**”.



2 После щелчка по “**Apply**” в окне браузера появится такое сообщение или аналогичное.

1.7.2 Проверка результатов изменения пароля администратора

1 Закройте web-интерфейс и зайдите в систему снова по **СТАРОМУ** паролю. Снова откроется окно “Authentication Required”.



2 Введите **новый** пароль для входа в систему. Теперь вы снова сможете открыть web-интерфейс коммутатора Switch-1.

1.8 Как создать «белый список» для удаленного управления чтобы предотвратить неавторизованный доступ

В этом примере показано, как можно создать «белый список» хост-устройств чтобы предотвратить доступ к коммутатору с неавторизованных устройств или подсетей. По этому белому списку проверяются IP-адреса хостов и типы сервисов, с помощью которых они пытаются получить доступ к коммутатору (например, Telnet, FTP, HTTP…..).

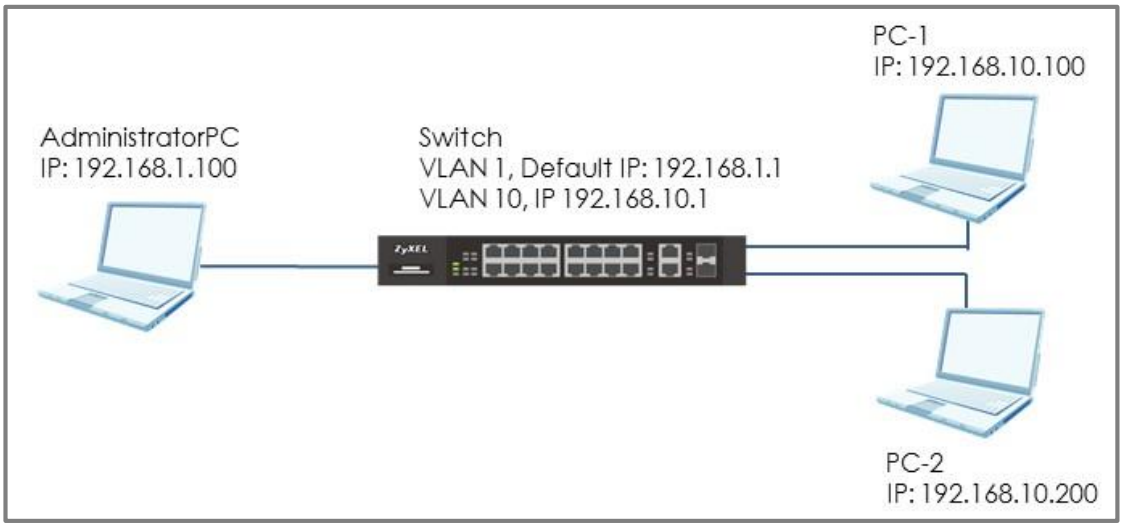


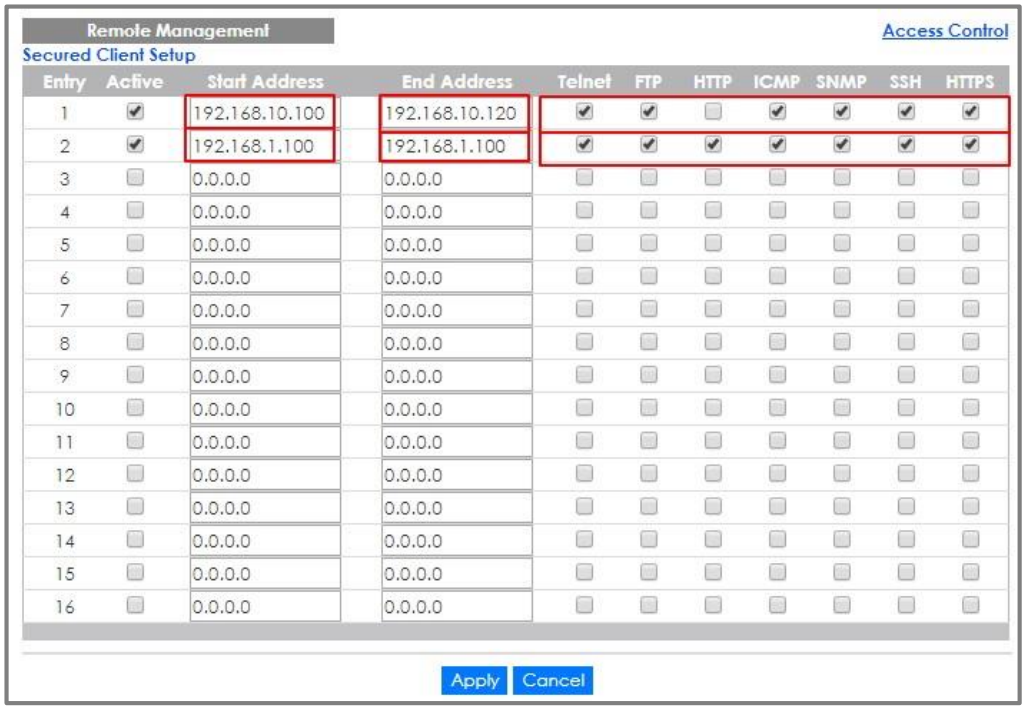
Иллюстрация 8 Создание «белого списка» для удаленного управления

Примечание:

Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

1.8.1 Создание «белого списка» для удаленного управления

1 Откройте web-интерфейс и перейдите в **Menu > Management > Access Control > Remote Management > Click Here** с ПК администратора AdministratorPC. Задайте диапазон IP-адресов и разрешенные им типы сервисов для доступа к коммутатору. Затем щелкните “**Apply**”.



1.8.2 Проверка результатов

1 В этом примере был задан диапазон IP-адресов: **192.168.10.100 - 192.168.10.120**, с которых разрешен доступ к коммутатору для всех протоколов КРОМЕ **HTTP.** Поэтому если использовать ПК PC-1 (192.168.10.100) для доступа к коммутатору по **HTTP**, то коммутатор сбросит соединение, но если попытаться получить доступ к web-интерфейсу по **HTTPS** (ввести **https**://192.168.10.1), то PC-1 сможет подключиться к коммутатору.

2 ПК PC-2 (192.168.10.200) нет в белом списке, поэтому он не может получить доступ к IP-адресу управления коммутатором и коммутатор не отвечает на ping с этого ПК.

3 С ПК AdministratorPC можно получить доступ к коммутатору с помощью **любого** типа сервиса.

8.1.3 Ошибки при создании «белого списка»

1 Если по ошибке один и тот же IP-адрес дважды внесен в белый список, то правила для обоих записей в списке объединяются (логическое **ИЛИ**).

В этом примере IP-адрес **192.168.10.120** дважды внесен в список и в результате для него разрешен доступ к коммутатору с использованием **ЛЮБОГО** из сервисов.

2 Если администратор забыл или потерял белый список IP-адресов, то он не сможет получить доступ к коммутатору. В этом случае посмотреть белый список можно только с помощью консоли **Console**, выведя используемую конфигурацию.

```
XGS4600# show run
  Building configuration...

  Current configuration:

no remote-management 1 service telnet ftp snmp ssh
vlan 1
  name 1
  normal ""
  fixed 1-32
  forbidden ""
  untagged 1-32
  ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
remote-management 1 start-addr 192.168.1.100 end-addr 192.168.1.200 service http icmp https
```

Примечание:

Если коммутатор **не поддерживает Console**, то нужно восстановить его заводские настройки по умолчанию как этому описано в Руководстве пользователя этой модели коммутатора.

Настройка параметров локальной сети

2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN

В этом примере показано, как настроить коммутатор для изоляции трафика разных отделов. При использовании **Static VLAN** хосты могут обмениваться данными только если они находятся в одной и той же VLAN.

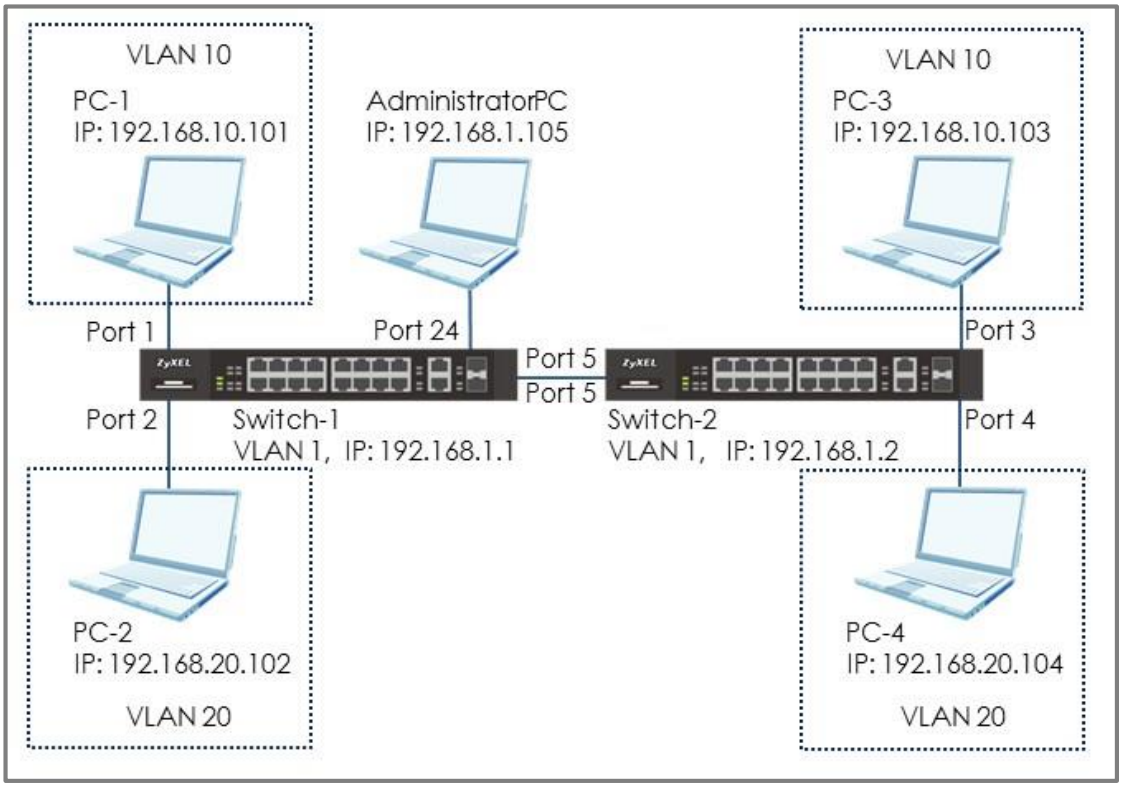


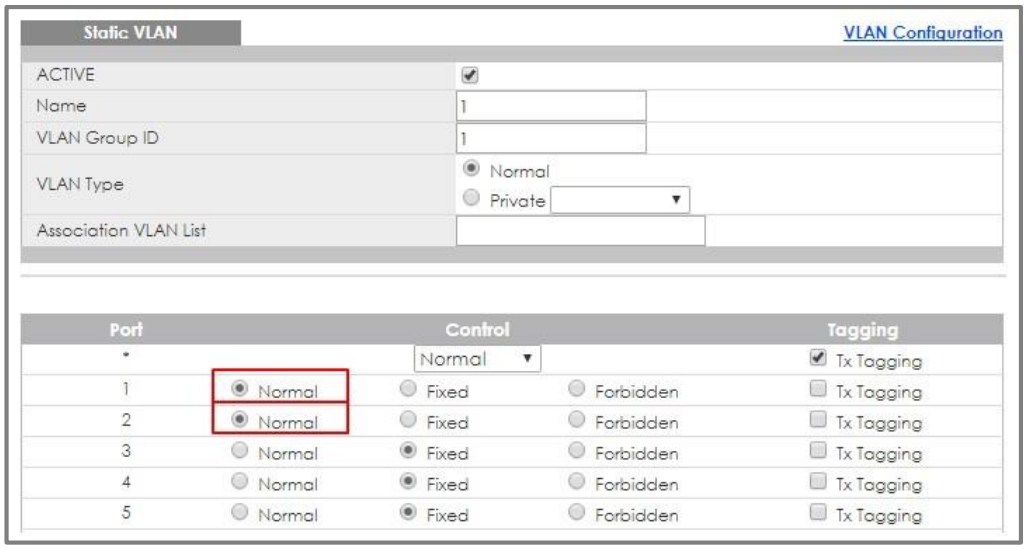
Иллюстрация 9 Настройка VLAN для изоляции трафика разных отделов

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

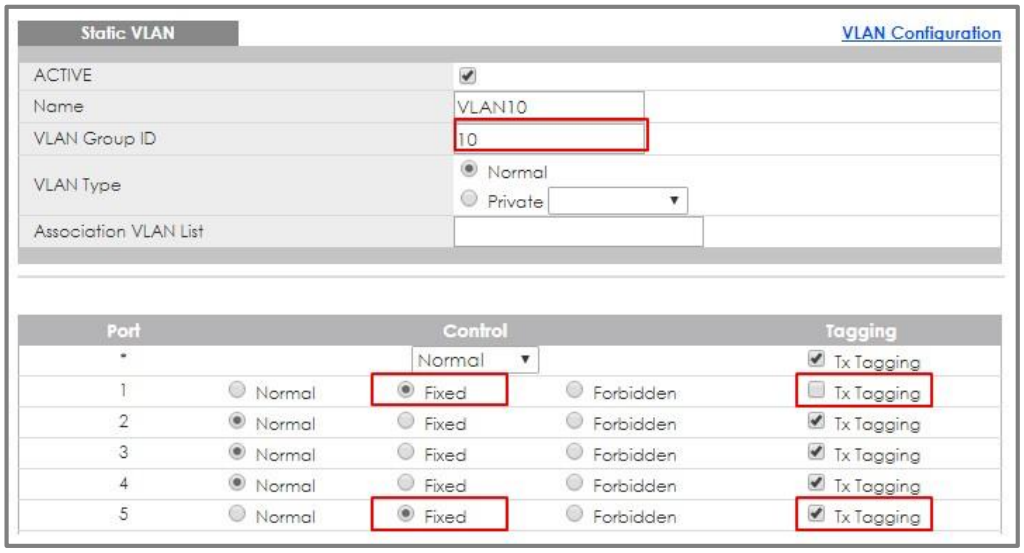
2.1.1 Настройка конфигурации коммутатора Switch-1

1 С ПК AdministratorPC настройте **VLAN 1** на коммутаторе **Switch-1**: Port 1 и 2 как обычный порт **Normal** (чтобы VLAN 1 не транслировала пакеты

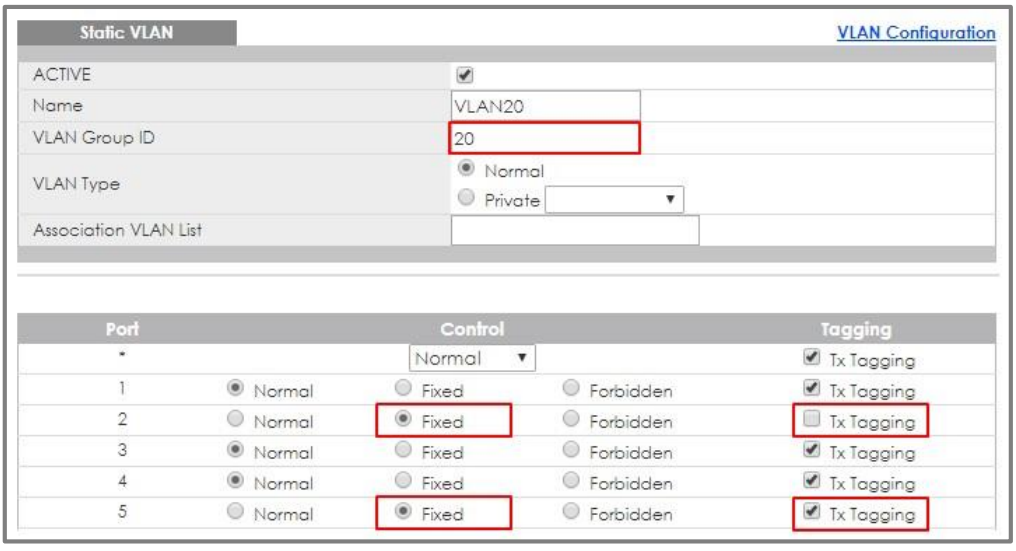
на порты 1 и 2). Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Выберите порт 1, 2 как **Normal**. Щелкните “**Add**”.



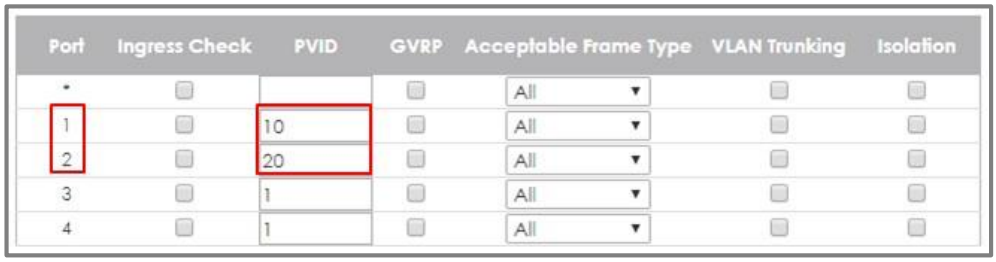
2 С ПК AdministratorPC создайте **VLAN 10** на **Switch-1**: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в “ACTIVE”. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**10**. Выберите порты **1** и **5** как **Fixed** и уберите галочку в Tx Tagging (**Untagged**) для порта **1** и поставьте галочку в Tx Tagging (**Tagged**) для порта **5**. Щелкните “**Apply**”.



3 С ПК AdministratorPC создайте **VLAN 20** на **Switch-1**: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в “ACTIVE”. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**20**. Выберите порты **2** и **5** как **Fixed** и уберите галочку в Tx Tagging (он станет **Untagged**) для порта **2** и поставьте галочку в Tx Tagging (он станет **Tagged**) для порта **5**. Щелкните “**Apply**”.



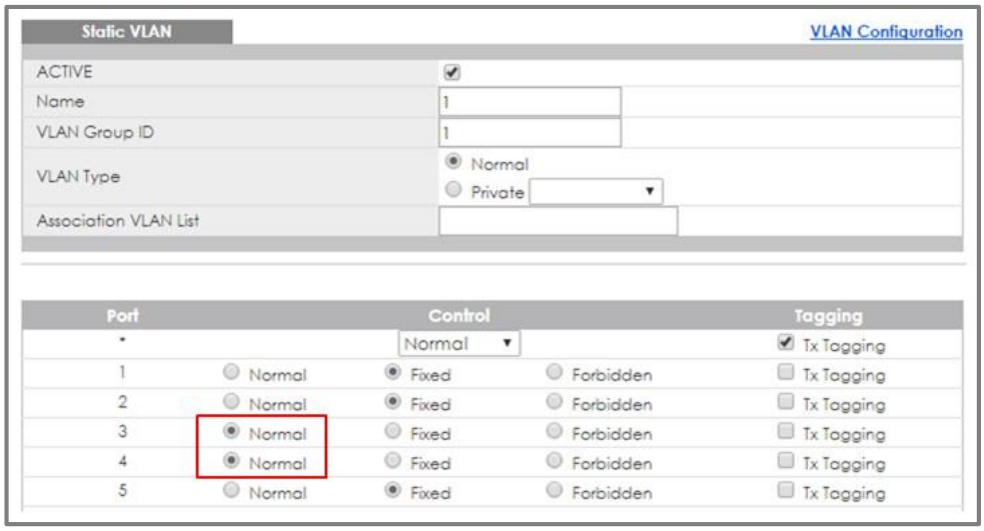
4 Настройка PVID в **Switch-1**: Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Задайте для порта port 1 PVID=**10** (VLAN 10) и для port 2 PVID=**20** (VLAN 20).



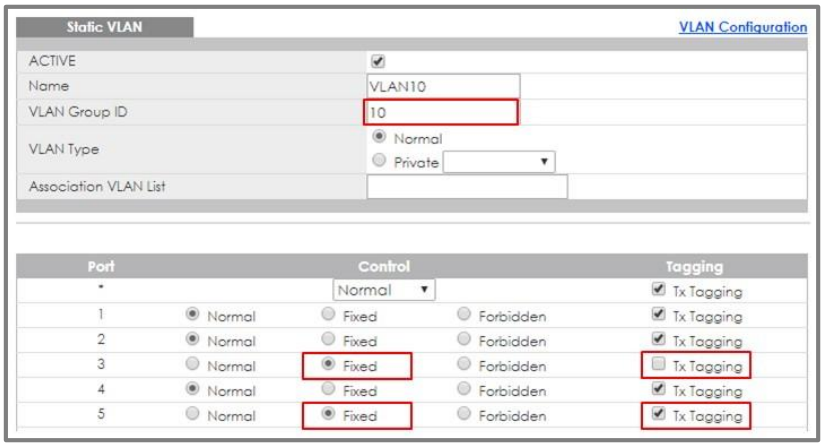
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	10	☐	All	☐	☐
2	☐	20	☐	All	☐	☐
3	☐	1	☐	All	☐	☐
4	☐	1	☐	All	☐	☐

2.1.2 Настройка конфигурации коммутатора Switch-2

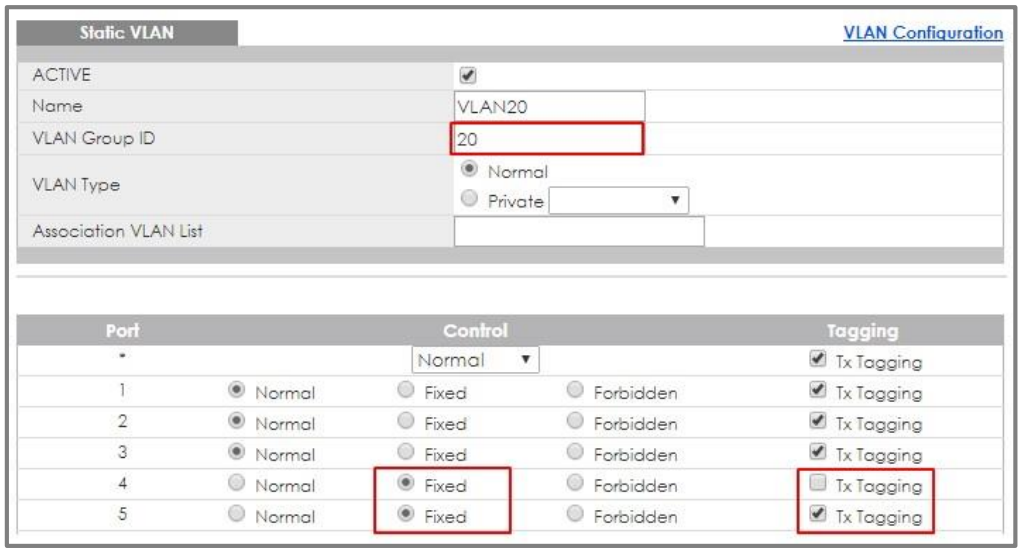
1 С ПК AdministratorPC настройте **VLAN 1** на **Switch-2**: порты Port 3, 4 настройте как **Normal** port (чтобы VLAN 1 не транслировала пакеты на порты port 3 и 4). Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup > VID > 1**. Выберите порты port 3, 4 как **Normal**. Щелкните “**Add**”.



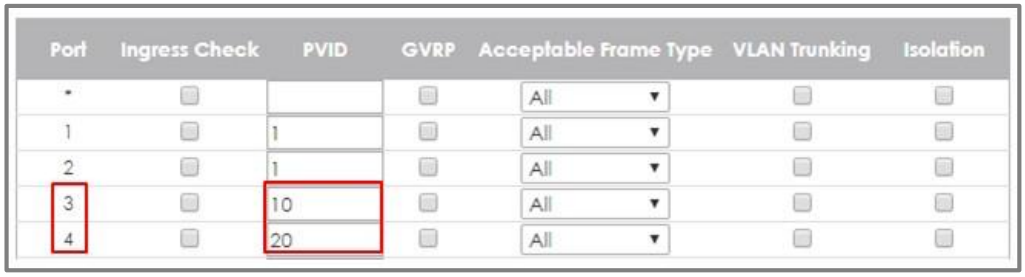
2 С ПК AdministratorPC создайте **VLAN 10** на коммутаторе **Switch-2**. Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в “ACTIVE”. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**10**. Выберите порты port 3, 5 как **Fixed** и уберите галочку в Tx Tagging (**Untagged**) для порта port 3 и поставьте галочку в check Tx Tagging (**tagged**) для порта port **5**. Щелкните “**Apply**”.



3 С помощью ПК AdministratorPC создайте VLAN 20 in **Switch-2**. Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в “ACTIVE”. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**20**. Выберите порты port 4, 5 как **Fixed**, уберите галочку в Tx Tagging (**Untagged**) для порта port 4 и поставьте галочку в Tx Tagging (**tagged**) для порта port 5. Щелкните “**Apply**”.



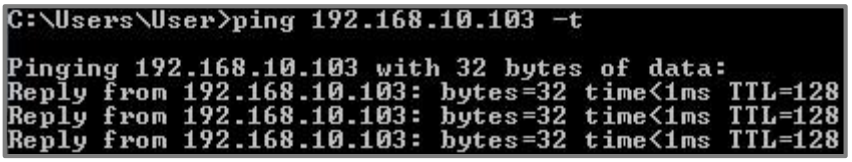
4 Настройте PVID на коммутаторе **Switch-2**: Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Задайте для порта port 3 PVID=**10** (VLAN 10) и для порта port 4 PVID=**20**.



Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All	☐	☐
1	☐	1	☐	All	☐	☐
2	☐	1	☐	All	☐	☐
3	☐	10	☐	All	☐	☐
4	☐	20	☐	All	☐	☐

2.1.3 Проверка правильности настройки

1 ping должен проходиться между двумя ПК, находящимися в одной VLAN. От PC-1 ping успешно доходит до PC-3, но ping от PC-1 не доходит до PC-2.



```
C:\Users\User>ping 192.168.10.103 -t

Pinging 192.168.10.103 with 32 bytes of data:
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
Reply from 192.168.10.103: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.20.102

Pinging 192.168.20.102 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

2 От PC-2 ping успешно доходит до PC-4, но ping от PC-2 не доходит до PC-3.

```
C:\Users\User>ping 192.168.20.104 -t

Pinging 192.168.20.104 with 32 bytes of data:
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
Reply from 192.168.20.104: bytes=32 time<1ms TTL=128
```

```
C:\Users\User>ping 192.168.10.103

Pinging 192.168.10.103 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

2.2 Как настроить коммутатора для маршрутизации трафика между двумя VLAN

VLAN изолирует между собой домены broadcast, поэтому для обмена трафиком между разными VLAN нужно настроить на коммутаторе его маршрутизацию как показано в этом примере.

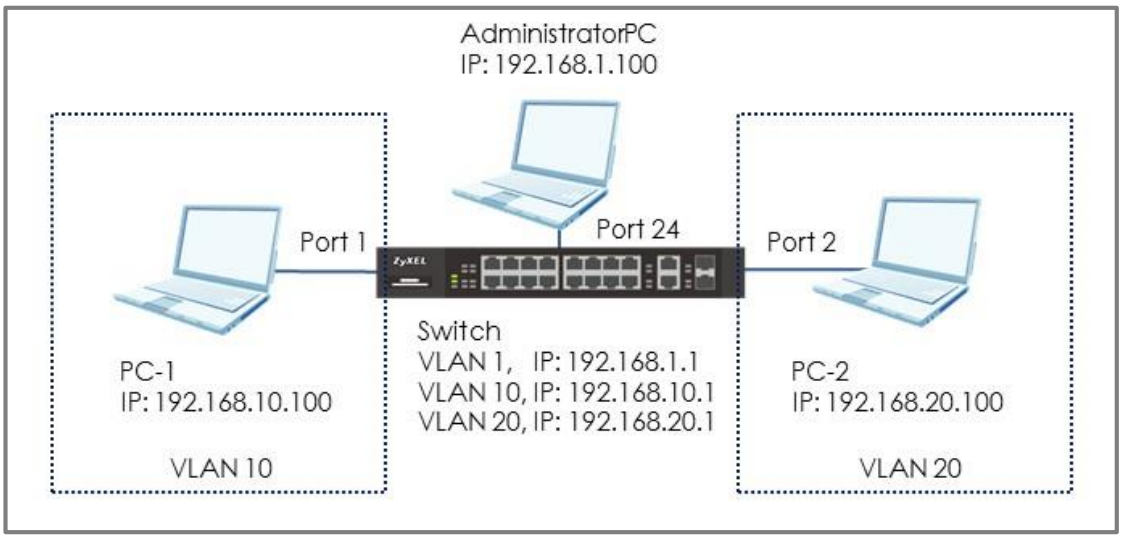


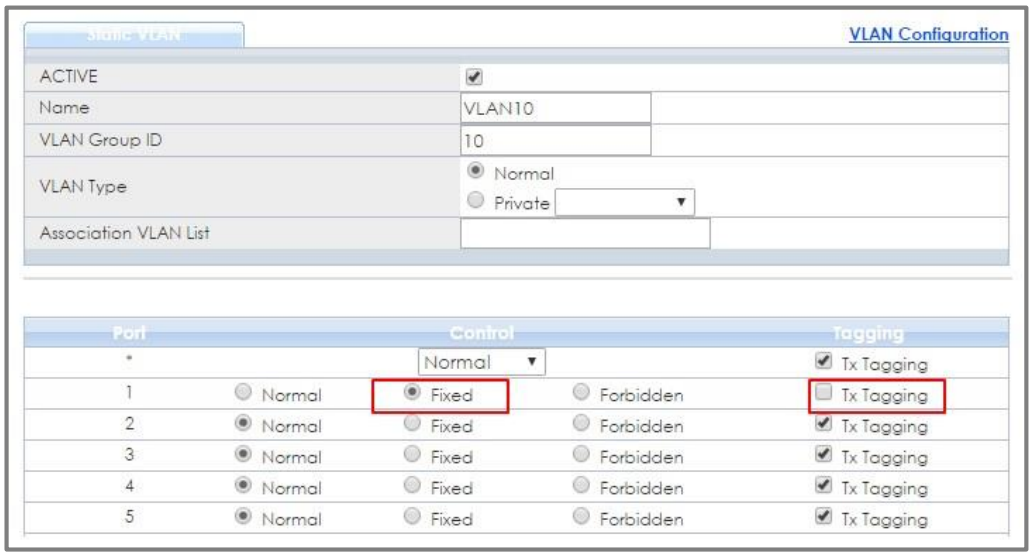
Иллюстрация 10 Настройка коммутатора для маршрутизации трафика между двумя VLAN

Примечание:

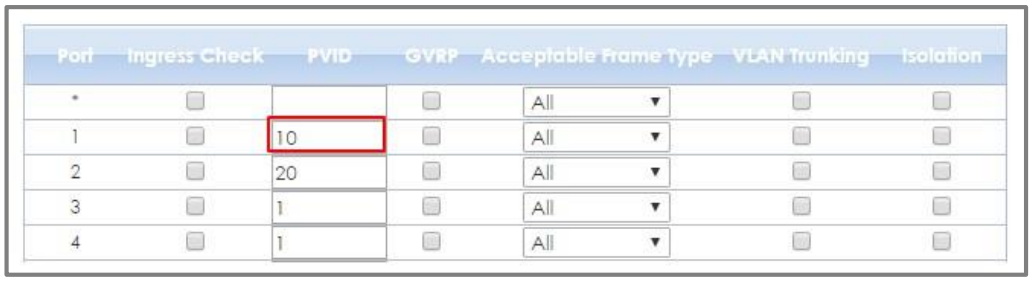
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

2.2.1 Настройка конфигурации VLAN 10

1 С ПК AdministratorPC создайте VLAN 10. Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**10**. Выберите порт port **1** как **Fixed** и уберите галочку в Tx Tagging (Untagged). Щелкните “**Apply**”.



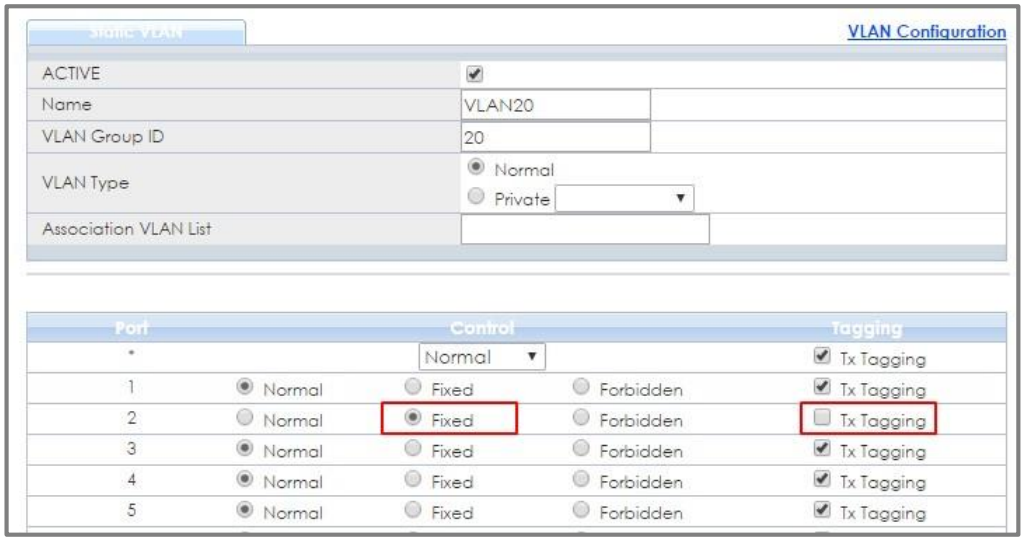
2 Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте PVID. Задайте для порта port **1** PVID=**10** (VLAN 10). Щелкните “**Apply**”.



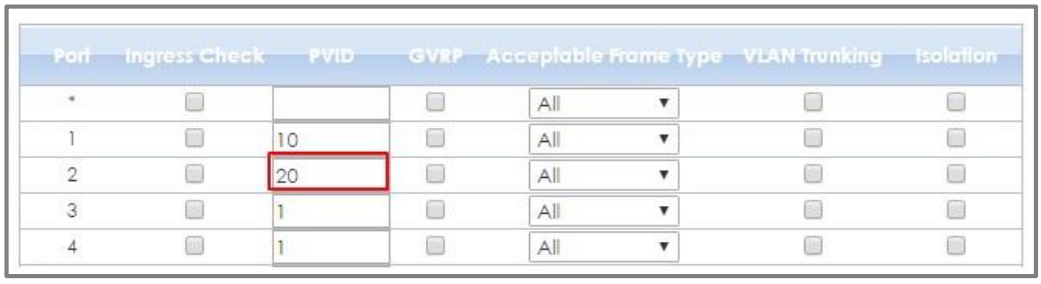
3 Создайте статический IP-адрес для коммутатора в in **VLAN 10** (чтобы он был шлюзом в VLAN 10): Перейдите в **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Настройте статический IP-адрес: **192.168.10.1** для коммутатора в VLAN 10. Щелкните “**Add**”.

2.2.2 Настройка конфигурации VLAN 20

1 Создайте VLAN 20. Выполните те же шаги. Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**20**. Выберите порт port **2** как **Fixed** и уберите галочку в Tx Tagging (Untagged). Щелкните “**Apply**”.



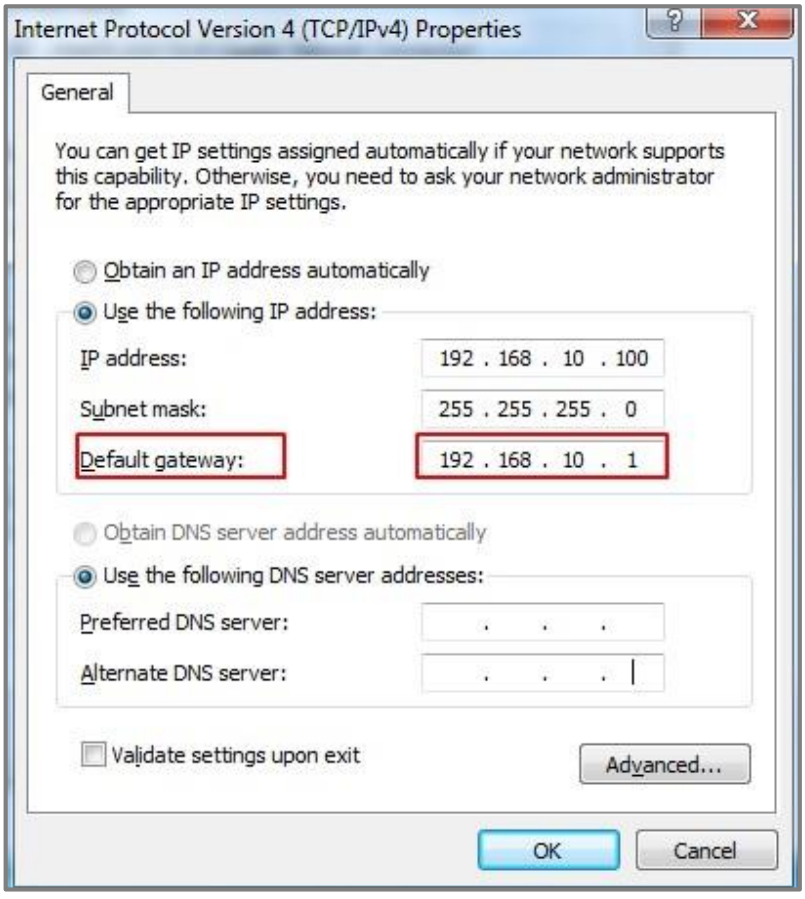
2 Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте PVID. Задайте для порта port **2** PVID=**20** (VLAN 20). Щелкните “**Apply**”.



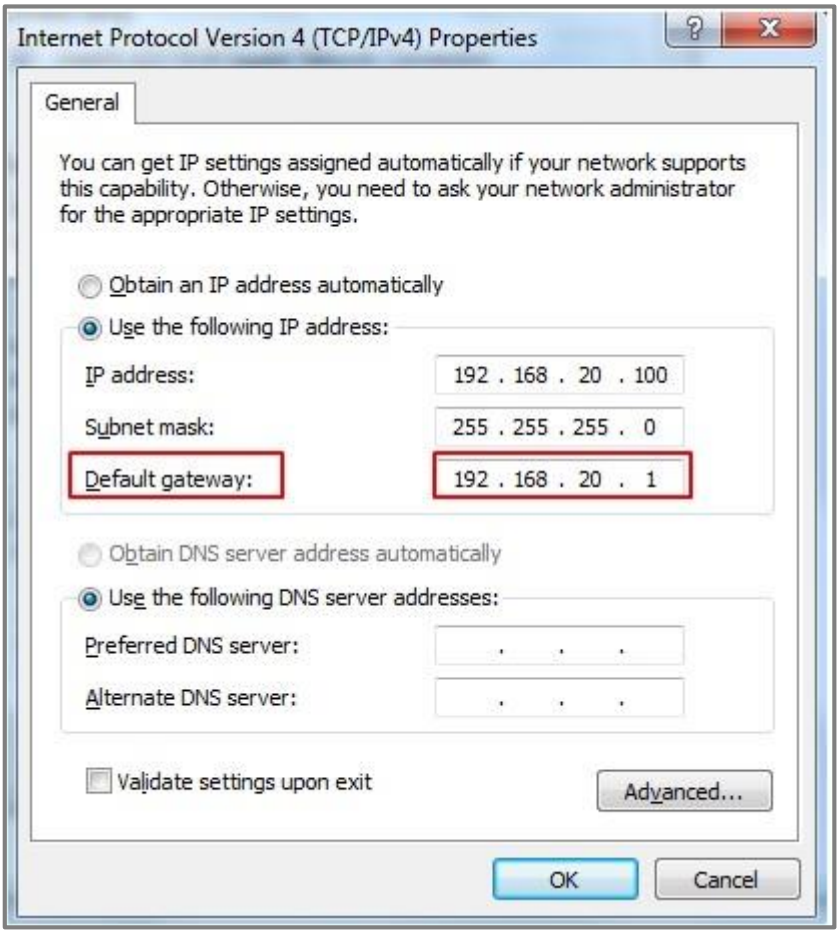
3 Создайте статический IP-адрес для коммутатора в VLAN 20 (адрес для шлюза в VLAN 20). Перейдите в **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Настройте статический IP-адрес: **192.168.20.1** для коммутатора в **VLAN 20**. Щелкните “**Add**”.

2.2.3 Настройте шлюз на PC-1 и PC-2

1 Настройте шлюз на **PC-1** как **192.168.10.1** (Статический IP-адрес для коммутатора в **VLAN 10**).



2 Настройте шлюз на PC-2 как **192.168.20.1** (Статический IP-адрес для коммутатора в **VLAN 20**).



2.2.4 Проверьте результат

1 Ping от PC-1 доходят до PC-2.

```
C:\Users\User>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128
Reply from 192.168.20.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.2.5 Почему это не работает

1 У PC-1 нет доступа к PC-2:

a. Убедитесь, что PC-1 и PC-2 находятся в разных подсетях.

b. Убедитесь, что шлюз по умолчанию PC-1 и PC-2 соответствуют IP-интерфейсу коммутатора в соответствующих VLAN.

c. Убедитесь, что нет политик маршрутизации, в которых подсеть PC-1 или PC-2 является критерием IP-адреса получателя (destination IP criteria).

2.3 Как настроить коммутатор на предоставление сервиса DHCP для VLAN

В этом примере показано настройка конфигурации коммутатора на выделение динамических IP-адресов хостам в каждой VLAN.

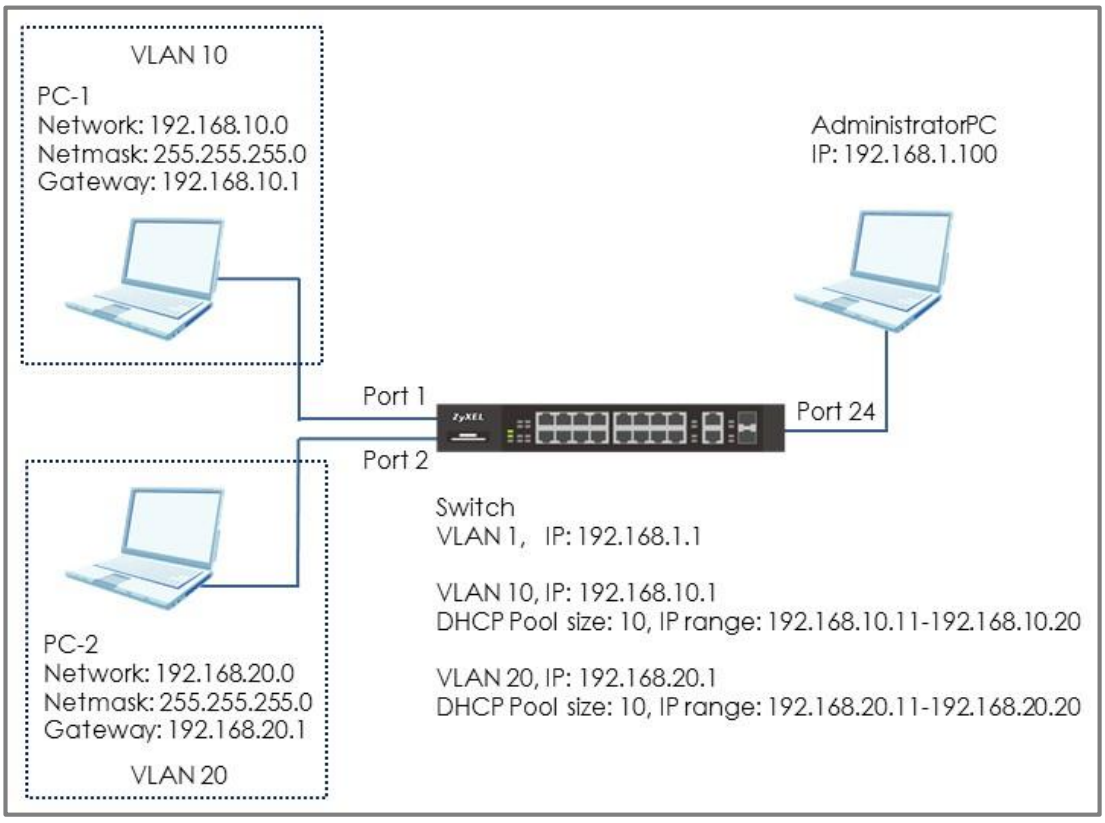


Иллюстрация 11 Предоставление сервиса DHCP в разных VLAN

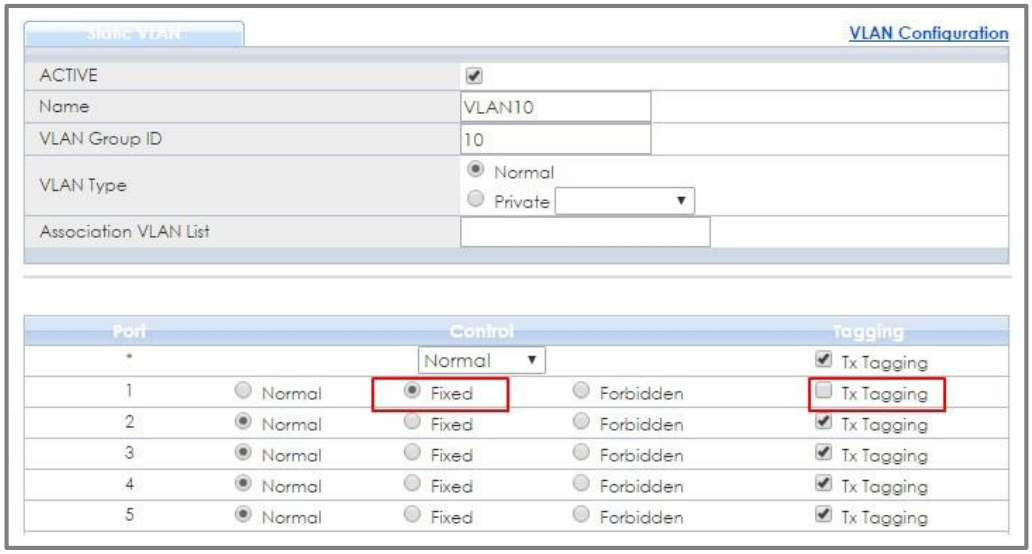
Примечание:

Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

Только коммутаторы третьего уровня (L3) могут выполнять функцию сервера DHCP (это модели коммутаторов серий 3700, 4500 и 4600)

2.3.1 Настройка VLAN 10

1 С помощью ПК AdministratorPC создайте VLAN 10. Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**10**. Выберите порт **1** как **Fixed** и уберите галочку в Tx Tagging (Untagged). Щелкните “**Apply**”.



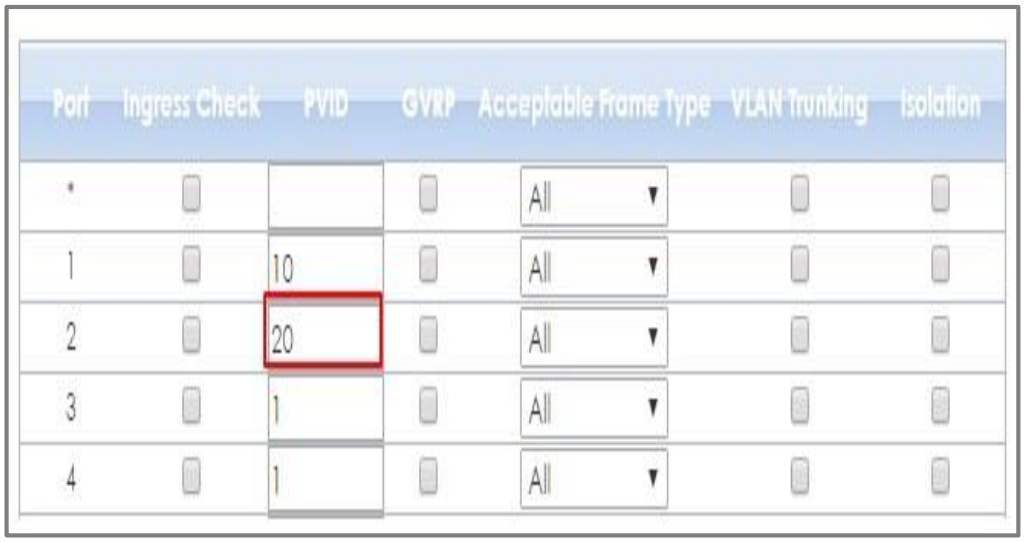
2 Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Задайте PVID. Задайте для порта port **1** значение PVID=**10** (VLAN 10). Щелкните “**Apply**”.

2

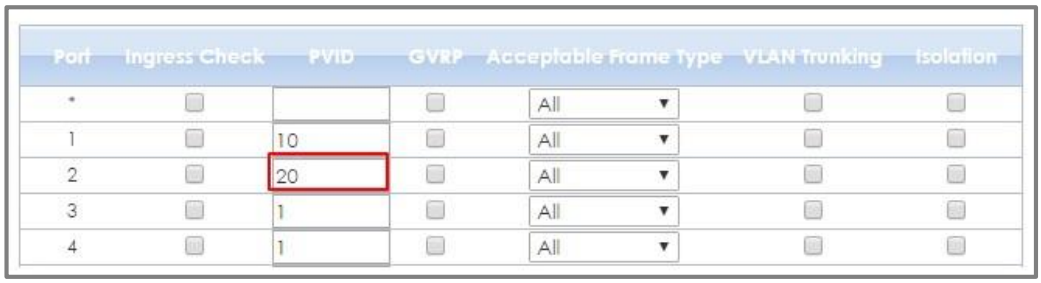
3 Создайте статический IP-адрес для коммутатора в **VLAN 10** (IP-адрес для сервера DHCP в VLAN 10): Перейдите в **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Настройте статический IP-адрес Static IP Address: **192.168.10.1** для коммутатора в VLAN 10. Щелкните “**Add**”.

2.3.2 Настройка конфигурации VLAN 20

1 Создайте VLAN 20. Выполните аналогичную процедуру. Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE. Введите имя виртуальной сети Name и идентификатор VLAN Group ID=**20**. Выберите порт **2** как **Fixed** и уберите галочку в Tx Tagging (Untagged). Щелкните “**Apply**”.

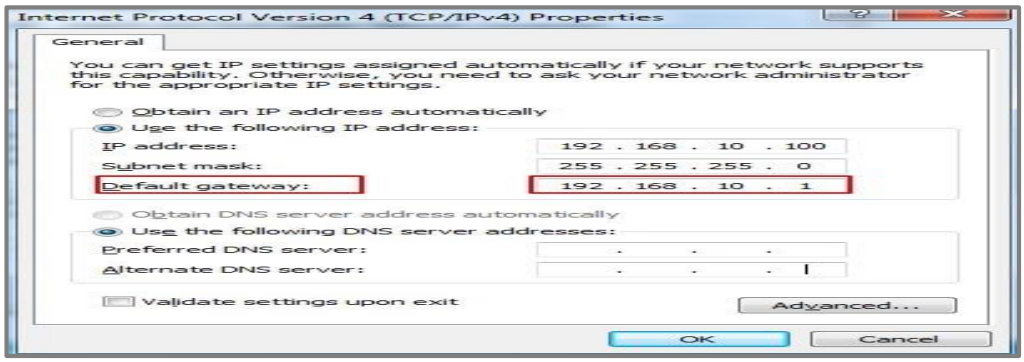


2 Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Задайте PVID. Задайте для порта port **2** значение PVID=**20** (VLAN 20). Щелкните “**Apply**”.



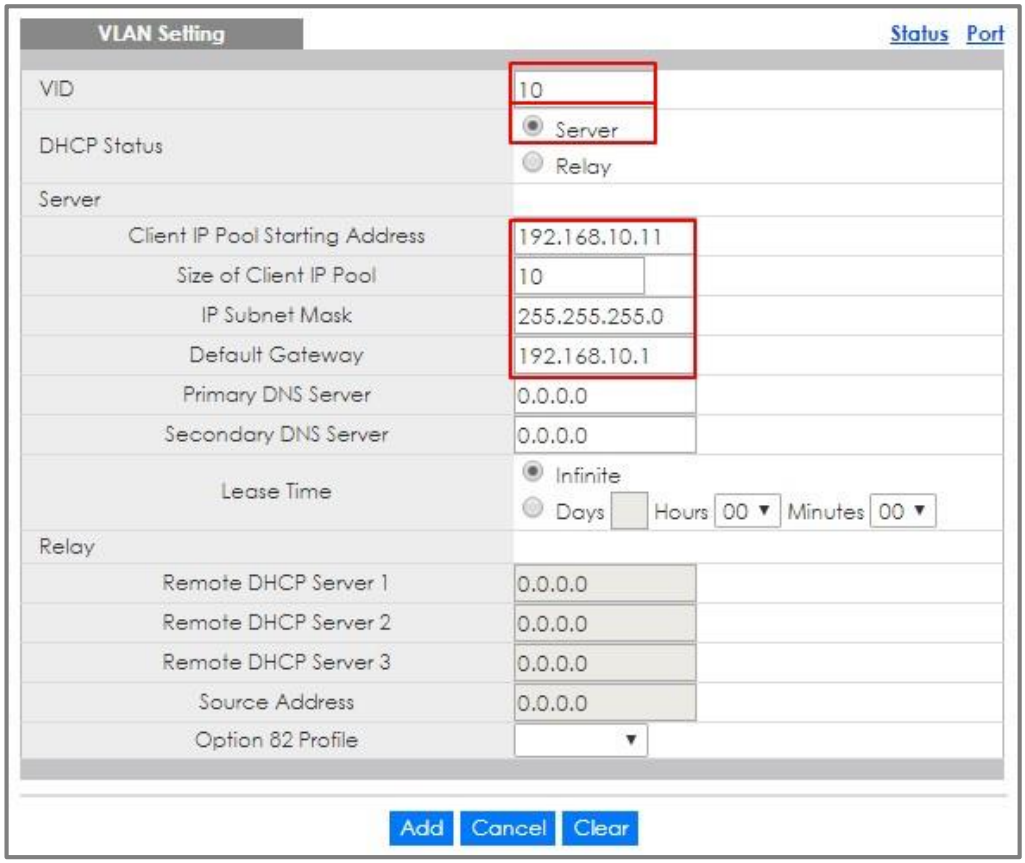
2

3 Создайте статический IP-адрес Static IP Address для коммутатора в VLAN 20 (это IP-адрес сервера DHCP в VLAN 20): Перейдите в **Menu > Basic Setting > IP Setup > IP Configuration > IP Interface**. Задайте статический IP-адрес Static IP Address: **192.168.20.1** для коммутатора в **VLAN 20**. Щелкните “**Add**”.



2.3.3 Настройка конфигурации коммутатора и ПК

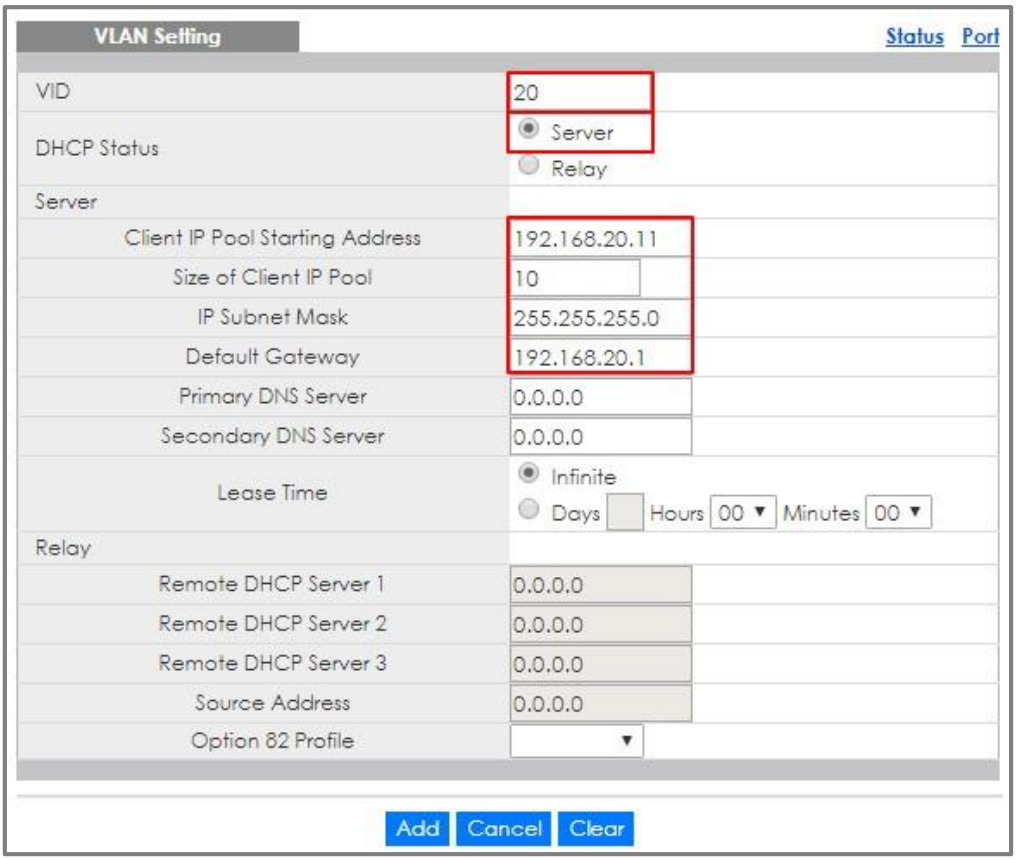
1 Настройте сервер DHCP в **VLAN 10**: Перейдите в **Menu > IP Application > DHCP > DHCPv4 > Click Here > VLAN**. Настройте VID (VLAN для PC-1) и DHCP Status как **Server**. Client IP Pool Starting Address – это первый IP-адрес, который коммутатор назначит клиентам DHCP. Size of Client IP Pool – это максимальное число IP-адресов, которые может предоставить коммутатор. Задайте для шлюза IP-адрес коммутатора в VLAN 10 (**192.168.10.1**). Щелкните “Add”.



Примечание:
В этом примере размер пула pool size равен 10, а начальный IP-адрес 192.168.10.11, поэтому сервер DHCP может назначать динамические адреса в диапазоне от 192.168.10.11 до 192.168.10.20.

2 Настройте сервер DHCP в **VLAN 20**: Перейдите в **Menu > IP Application > DHCP > DHCPv4 > Click Here > VLAN**. Настройте VID (VLAN для PC-2) и DHCP Status как **Server**. Client IP Pool Starting Address – это первый IP-адрес, который коммутатор назначит клиентам DHCP. Размер пула IP-адресов клиентов Size of Client IP Pool – это максимальное число IP-адресов, которые может предоставить коммутатор. Задайте для шлюза IP-адрес коммутатора в VLAN 10 (**192.168.20.1**). Щелкните “Add”.

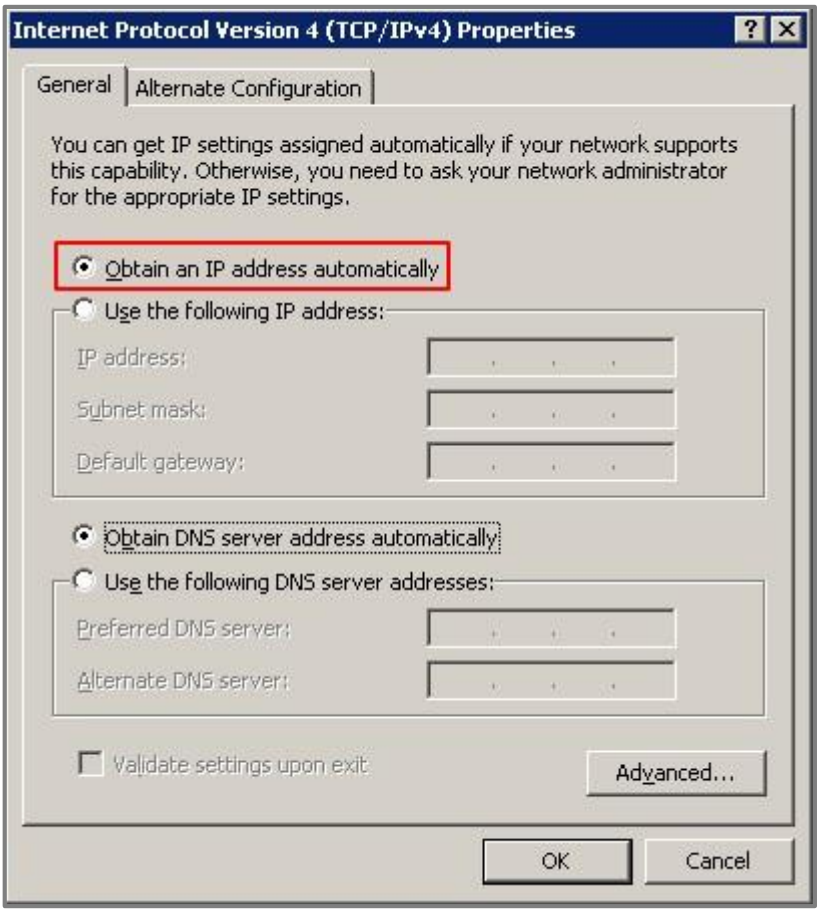
2



Примечание:

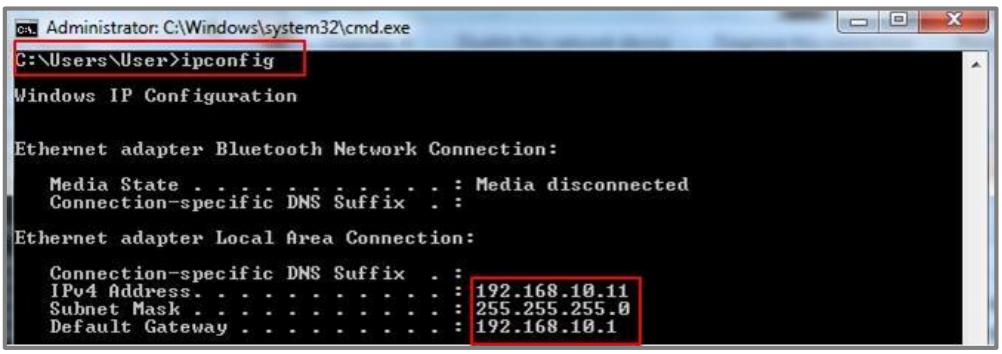
В этом примере размер пула 10 адресов и первый IP-адрес 192.168.20.11, поэтому DHCP может назначать адреса от 192.168.20.11 и до 192.168.20.20.

3 Настройте PC-1 и PC-2 чтобы они работали как клиенты DHCP. Для нужно настроить IPv4 на “**Obtain an IP Address automatically**”.

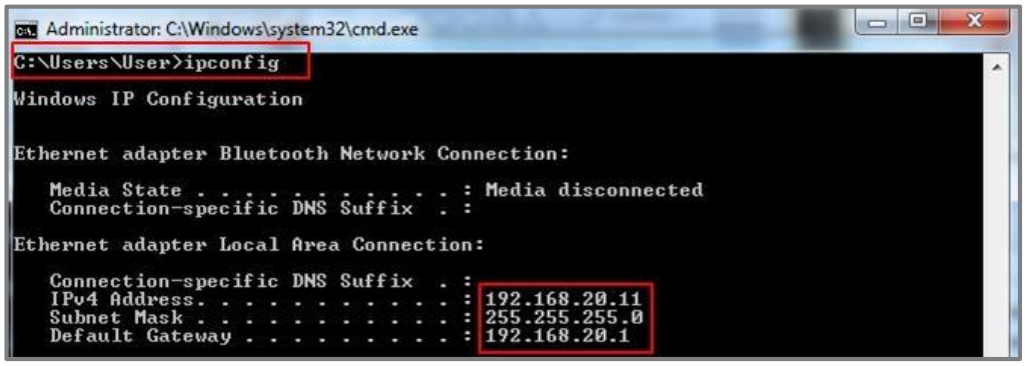


2.3.4 Проверка результатов

1 Чтобы проверить, PC-1 может получить IP-адрес от коммутатора, нужно ввести в командной строке “**ipconfig**”. PC-1 получит IP-адрес в диапазоне **192.168.10.11-192.168.10.20** и адрес шлюза **192.168.10.1.**



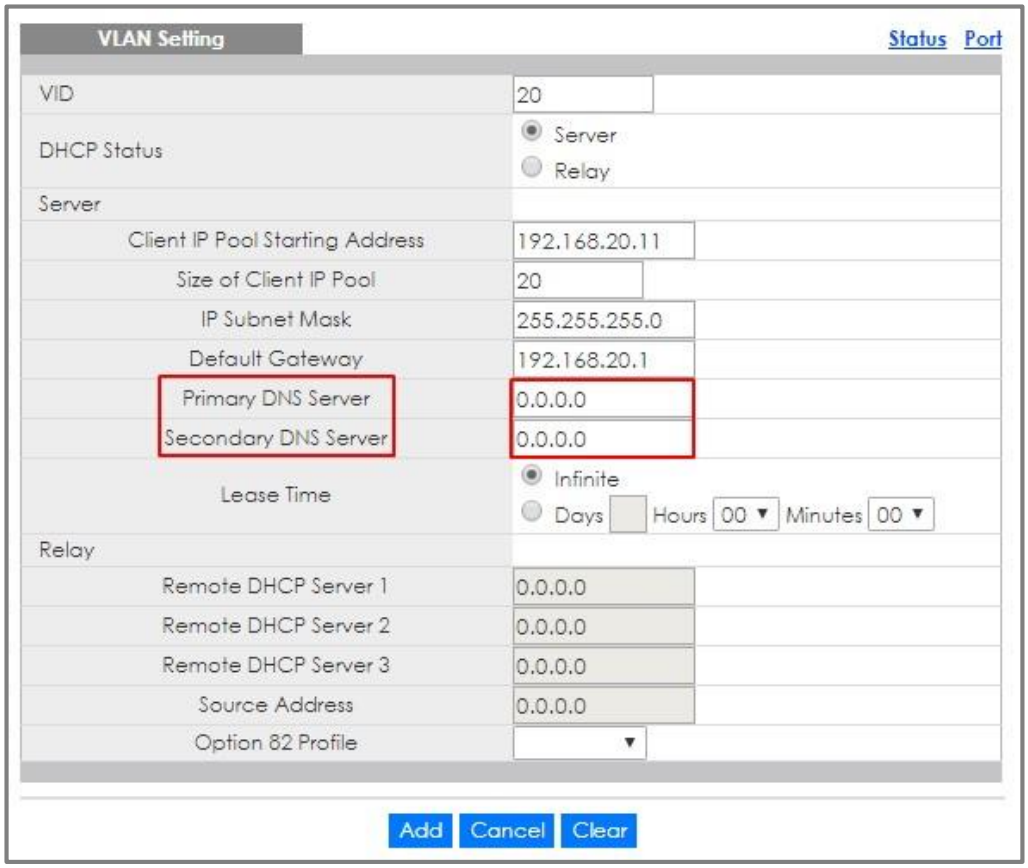
2 Чтобы проверить, PC-2 может получить IP-адрес от коммутатора, нужно ввести в командной строке “**ipconfig**”. PC-2 получит IP-адрес в диапазоне **192.168.20.11-192.168.20.20** и адрес шлюза **192.168.20.1.**



2.3.5 Почему это не работает

1 Если некоторые устройства не могут получить динамический IP-адрес от сервера DHCP, то попробуйте увеличить размер пула IP-адресов клиентов Size of Client Pool.

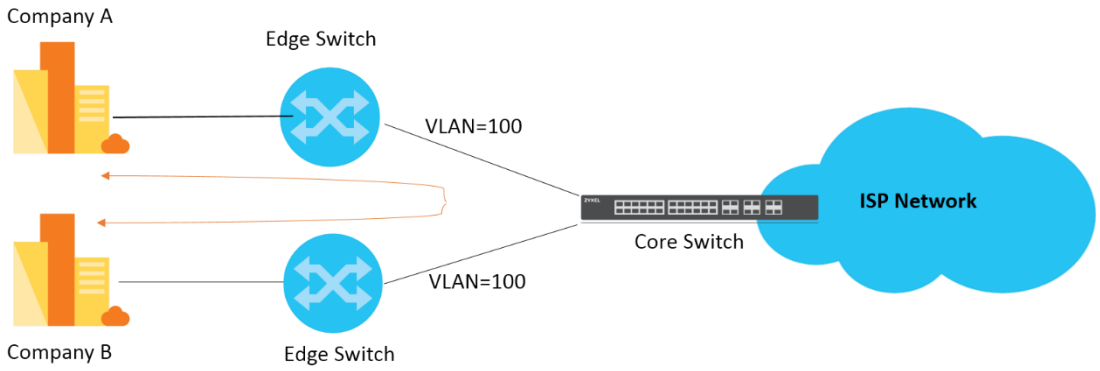
2 Если вы хотите просматривать сайты в Интернете по их URL или имени домена, то нужно настроить **DNS Server**.



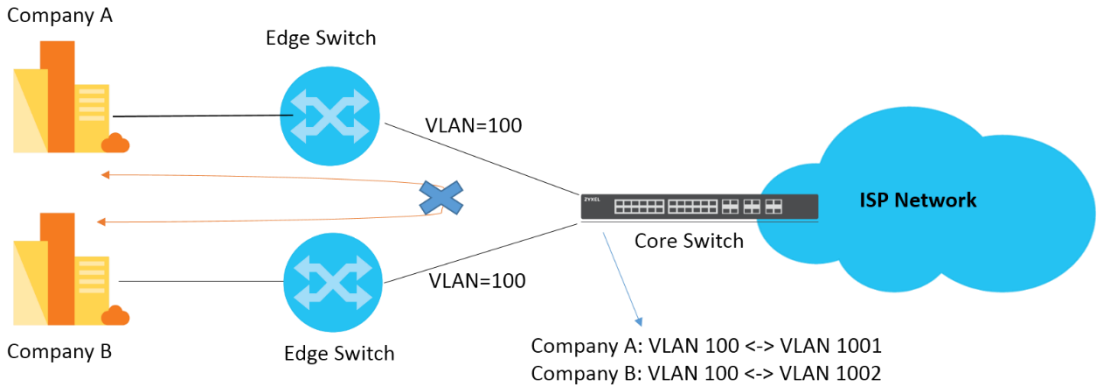
2.4 Как настроить коммутатор на трансляцию VLAN клиента в VLAN сервис-провайдера

VLAN Mapping – это механизм трансляции VLAN клиента в VLAN сервис-провайдера (Translated-VLAN). Пакеты, которые приходят на порт, будут пересылаться в Translated VLAN на основе ID порта и ID-идентификатора VLAN, который указан в пакете.

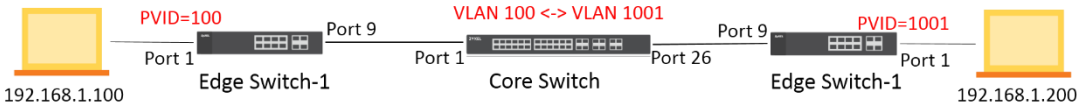
VLAN Mapping позволяет разделить трафик разных клиентов, которые используют одну и ту же VLAN в одной сети. В следующем примере компании A и B используют одну и ту же VLAN 10. Когда компания A sends посылает трафик в сеть провайдера, то он может пересылаться через коммутатор ядра компании B, потому что обе компании используют VLAN 10.



Если настроить VLAN Mapping на коммутаторах границы сети, то они будут транслировать VLAN клиентов компании A и B в разные соответствующие VLAN, поэтому трафик не будет идти между компаниями A и B, так они находятся в разных VLAN после выполнения трансляции VLAN на коммутаторах границы сети.



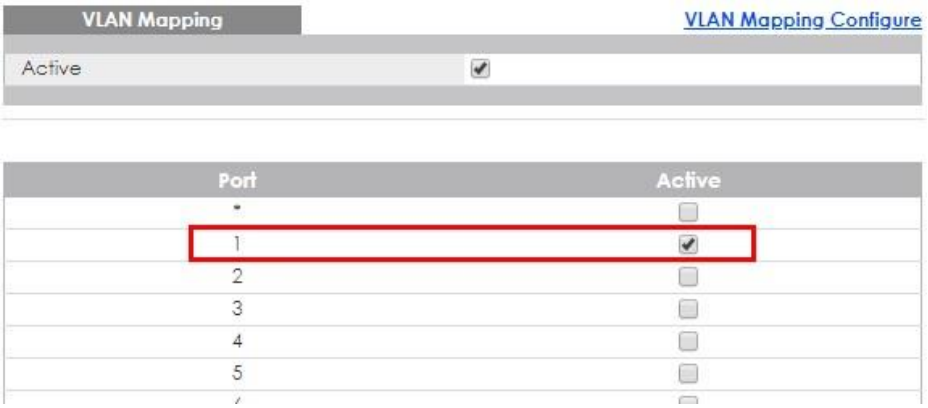
В следующем примере показано, как настроить коммутатор на трансляцию VLAN.



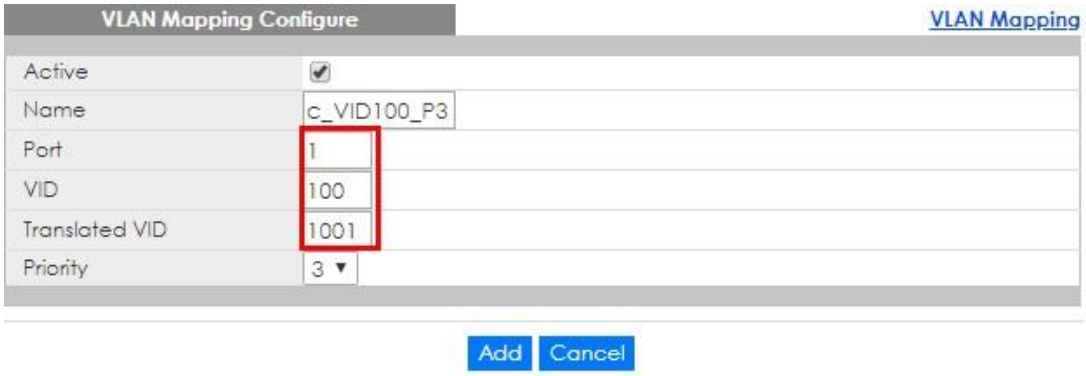
Примечание:
В этом примере коммутаторы границы сети – это два GS2210, а коммутатор ядра сети – один XGS4600.

2.4.1 Настройка конфигурации коммутатора ядра сети

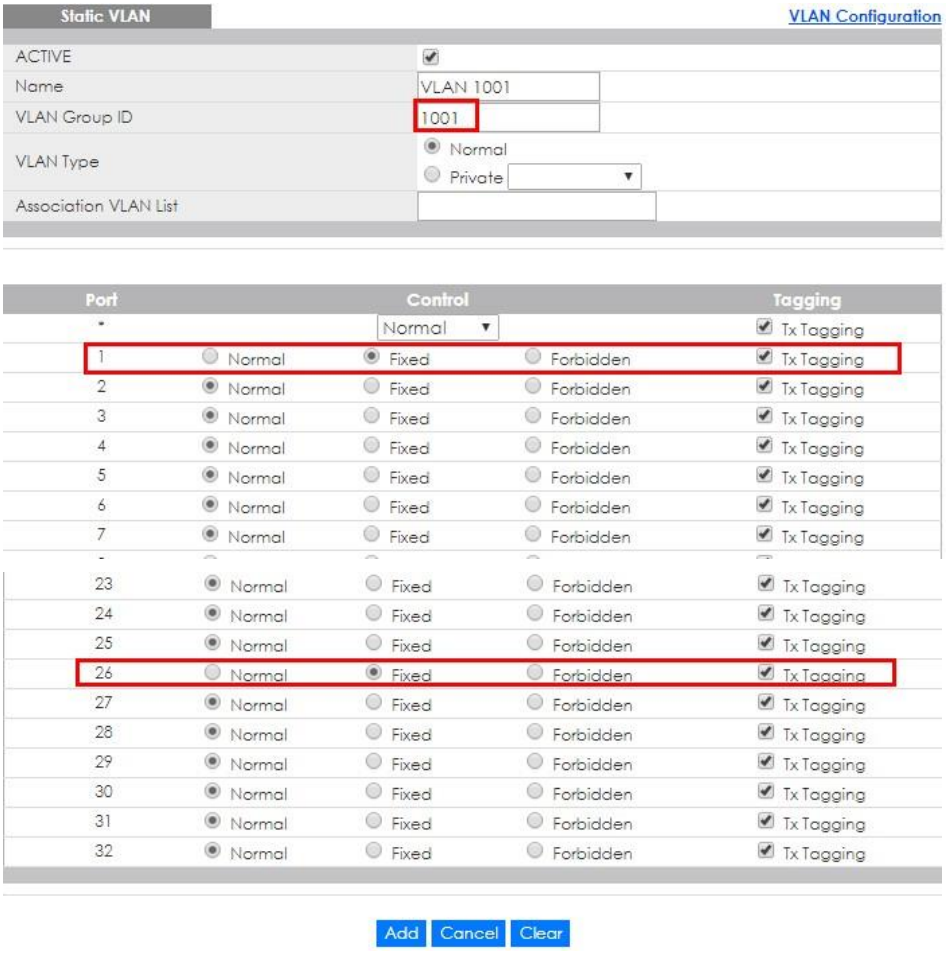
1 Откройте web-интерфейс, перейдите в **Menu > Advanced Application > VLAN Mapping.** Поставьте галочку в ACTIVE чтобы включить порт port **1**.



2 Перейдите в **Menu > Advanced Application > VLAN Mapping > Configure**. Поставьте галочку в ACTIVE и введите **Name**. Настройте порт Port в **1**, VID в **100** и Translated VID в **1001**. Назначьте приоритет Priority value равным 3 (опция) и щелкните “Apply”.



3 Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE, Введите имя виртуальной сети Name и идентификатор VLAN Group ID= как **1001**. Выберите порт **1, 26** как **Fixed** и щелкните “**Apply**”.



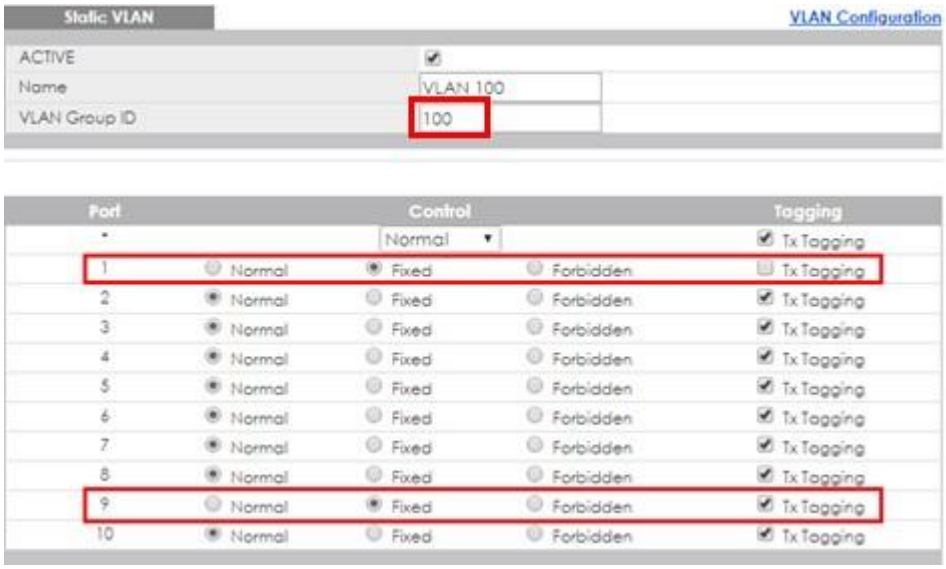
Примечание:

Создайте Static VLAN только для Translated VLAN, и настройте оба порта как члены Translated VLAN. В противном случает пакеты от Translated VLAN, которые приходят на порт port 26, НЕ будет пересылаться на порт port 1.

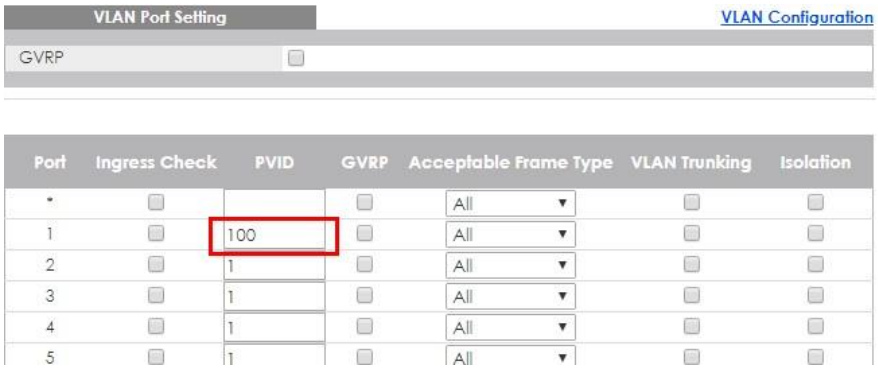
2.4.2 Настройка конфигурации коммутатора границы сети

1 Настройте коммутатор **Customer Switch-1:** Откройте web-интерфейс коммутатора. Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE, Введите имя виртуальной сети Name и идентификатор VLAN

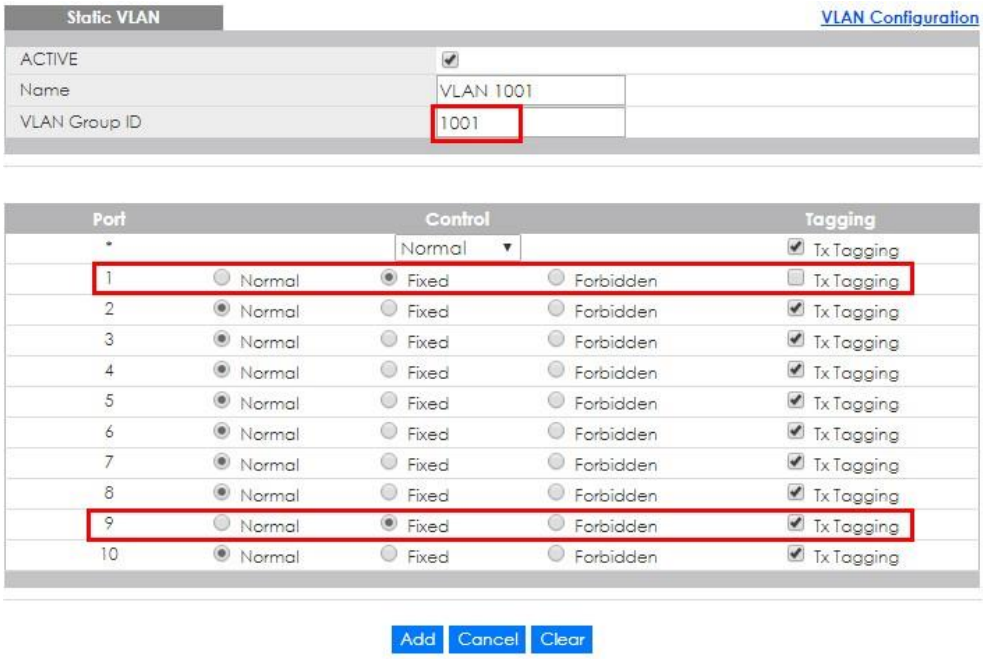
Group ID= as **100**. Выберите порт **1** as **Fixed** и уберите галочку в Tx Tagging (Untagged). Выберите порт **9** как **Fixed** и щелкните “**Apply**”.



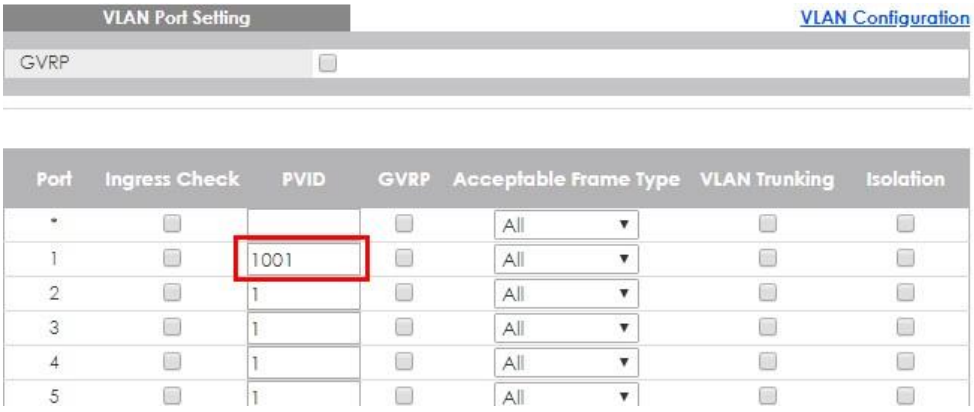
2 Настройка **Customer Switch-1:** Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте port **1** PVID**=** как **100** (VLAN 100) и щелкните “**Apply**”.



3 Настройка **Customer Switch-2:** Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**. Поставьте галочку в ACTIVE, введите **Name** и VLAN Group ID**=** as **1001**. Выберите порт **1** как **Fixed** и уберите галочку в Tx Tagging (Untagged). Выберите порт **9** как **Fixed** и щелкните “**Apply**”.

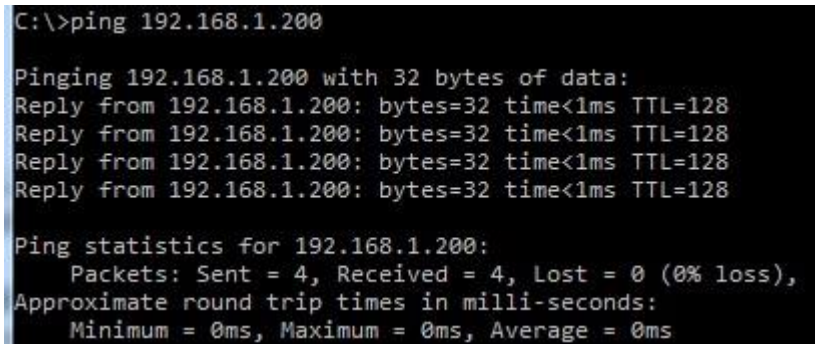


4 Настройка **Customer Switch-2:** Перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте port **1** PVID= как **1001** (VLAN 1001) и щелкните “**Apply**”.

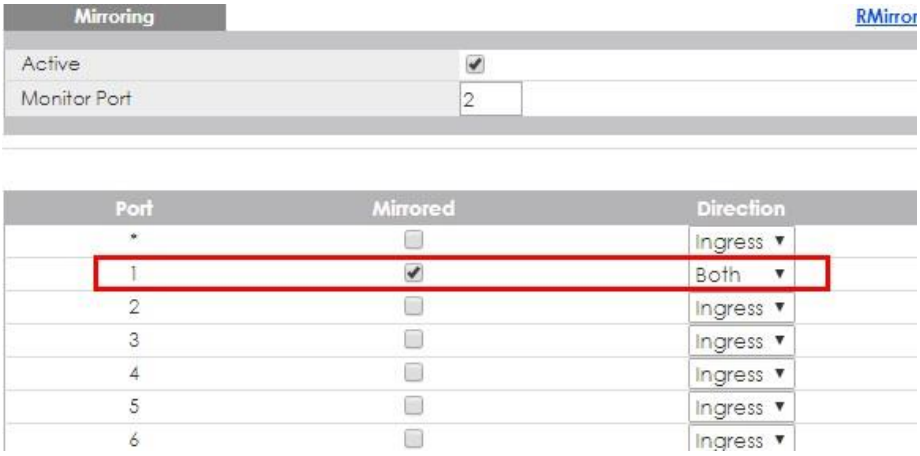


2.4.3 Test the Results

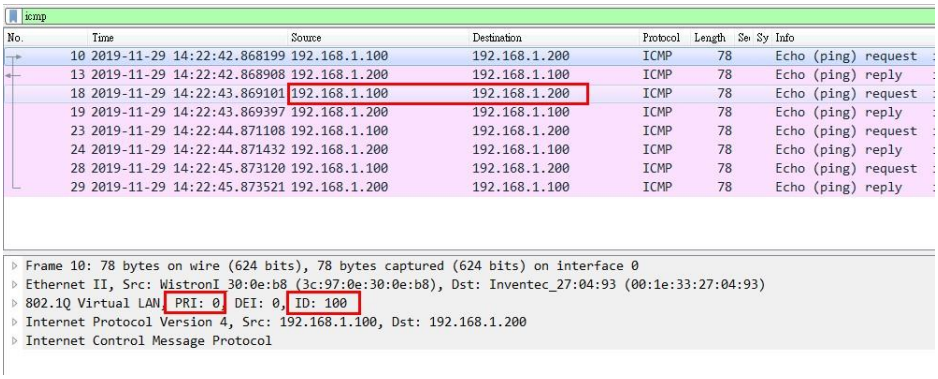
1 От PC-1 ping доходят до PC-2.



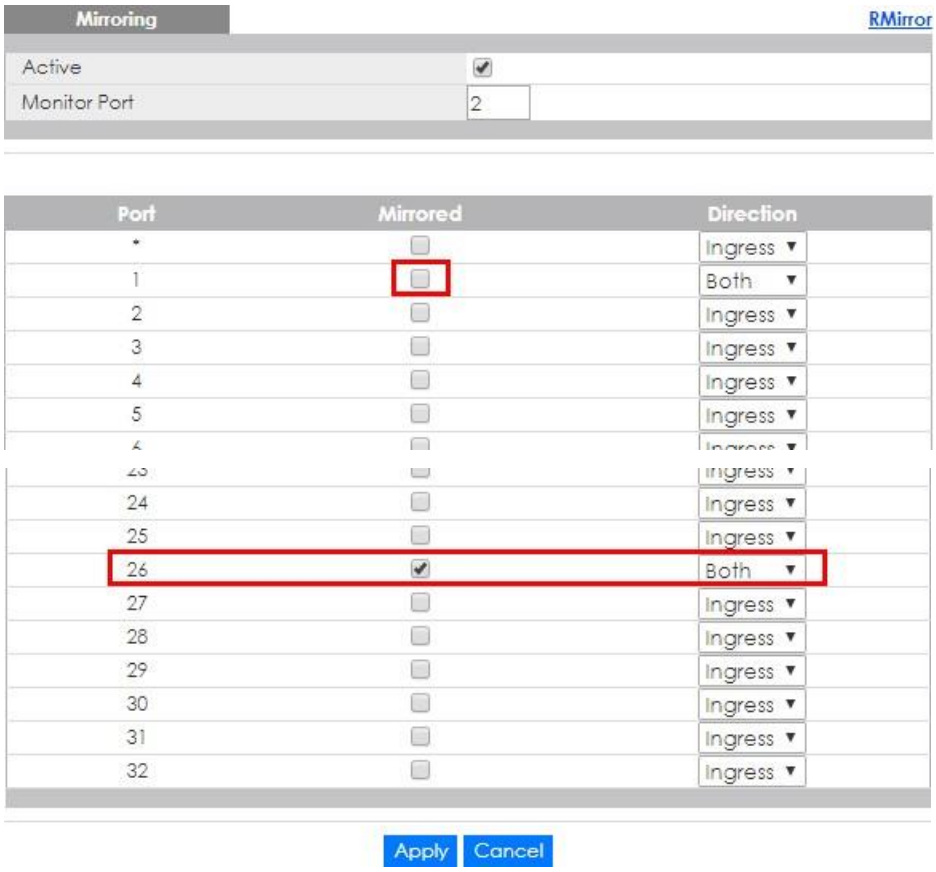
2 Настройте Mirroring для проверки значений VLAN ID/Priority в пакетах, которые приходят на порт **port 1** коммутатора ядра сети чтобы убедиться, что это значение совпадает с исходным (**VLAN=100/Priority=0**). Откройте Web-интерфейс и перейдите в **Menu > Advanced Application > Mirroring**. Поставьте галочку в “**Active**”. Настройте Monitor port как port **2**, который будет использоваться для мониторинга трафика и поставьте галочку в порте-получателе (в данном примере **port 1**). В Direction выберите “Both” и щелкните “**Apply**”.



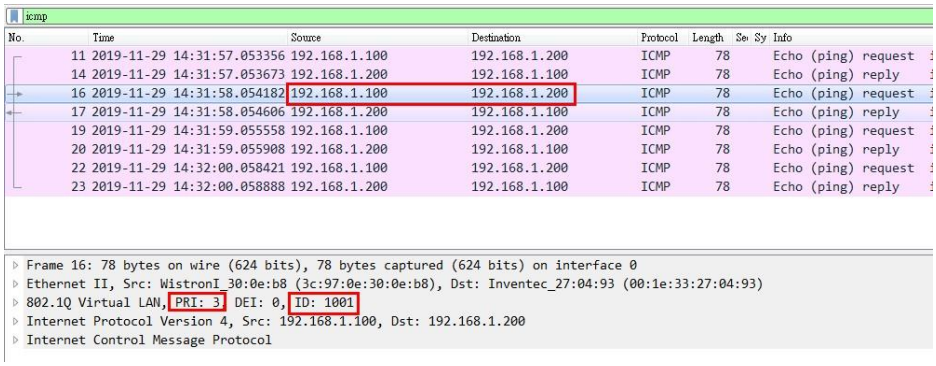
3 Соедините другой ПК с портом port 2 коммутатора ядра сети. Откройте **wireshark** для мониторинга пакетов и настройте фильтр на “**icmp**”.



4 Настройте Mirroring для проверки значений VLAN ID/Priority в пакетах, которые идут от порта **port 26** коммутатора ядра чтобы убедиться, что у них будет транслированные значения (**VLAN=1001/Priority=3**). Перейдите в **Menu > Advanced Application > Mirroring**. Сбросьте галочку в port 1 и поставьте галочку в **port 26**. Выберите в Direction “Both” и щелкните “**Apply**”.



5 Соедините другой ПК к порту port 2 коммутатора ядра. Откройте **wireshark** для мониторинга пакетов и настройте фильтр на “**icmp**”.



Улучшение надежности сети

3.1 Как настроить стек коммутаторов для обеспечения высокой доступности сервера

В этом примере для обеспечения высокой доступности сервера два коммутатора Switch-1 и Switch-2 объединяются в стек и работают как один логический коммутатор. Если один из этих коммутаторов выйдет из строя, то у клиентов сохранится доступ к серверу. Перед настройкой коммутаторов нужно отсоединить их от сети чтобы не возник «шторм» широковещательной рассылки broadcast storm.

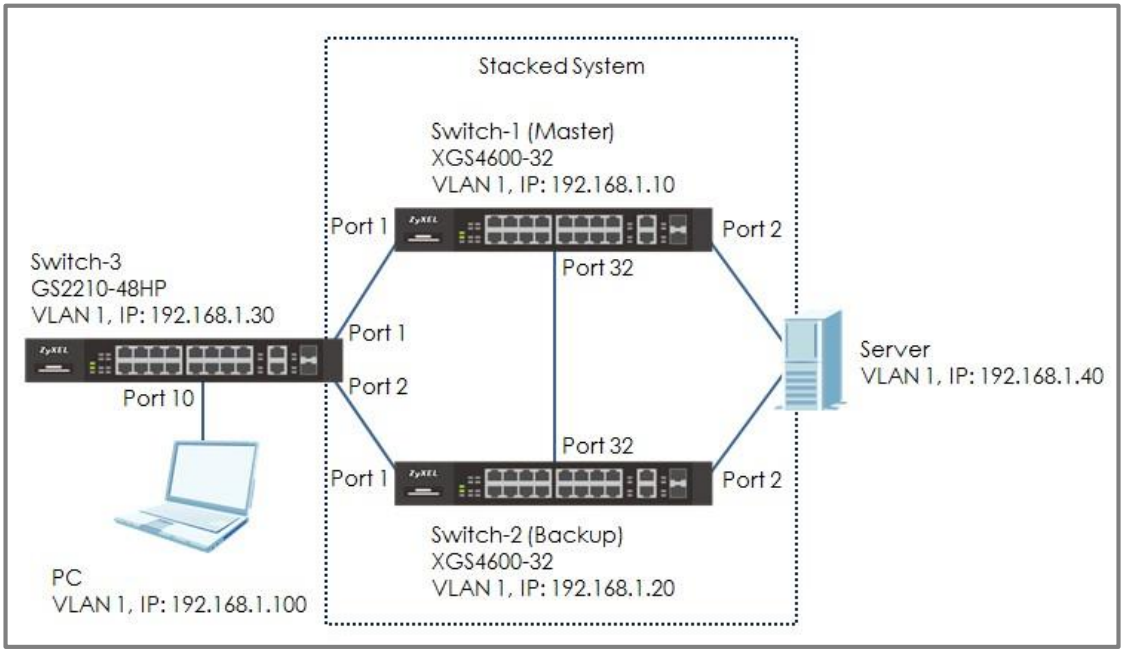


Иллюстрация 12 Настройка стека коммутаторов

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

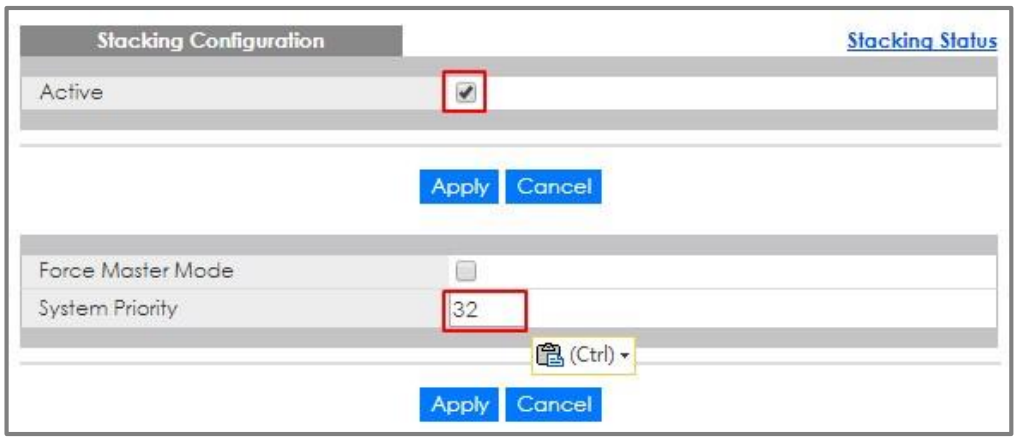
3.1.1 Настройка коммутаторов Switch-1 и Switch-2 для построения стека

1 Настройте **Switch-1**: Откройте web-интерфейс и перейдите в **Menu > Basic Setting > Stacking > Configuration**. Введите номер приоритета в

поле System Priority («мастером» стека будет тот коммутатор, у которого выше приоритет) и щелкните “Apply”. Поставьте галочку в поле “Active” и щелкните “Apply”. Коммутатор Switch-1 перезагрузится.

Примечание:
В этом примере мы назначили коммутатору Switch-1 более высокий приоритет, чем коммутатору Switch-2, поэтому Мастером будет Switch-1.

2 Настройте **Switch-2**: Откройте web-интерфейс и перейдите в **Menu > Basic Setting > Stacking > Configuration**. Введите номер приоритета в поле System Priority («Мастером» стека будет тот коммутатор, у которого выше приоритет) и щелкните “Apply”. Поставьте галочку в “Active” и щелкните “Apply”. Switch-2 перезагрузится.



3 Соедините Switch-1 и Switch-2 через порт 32 используя трансивер 10Gigabit.

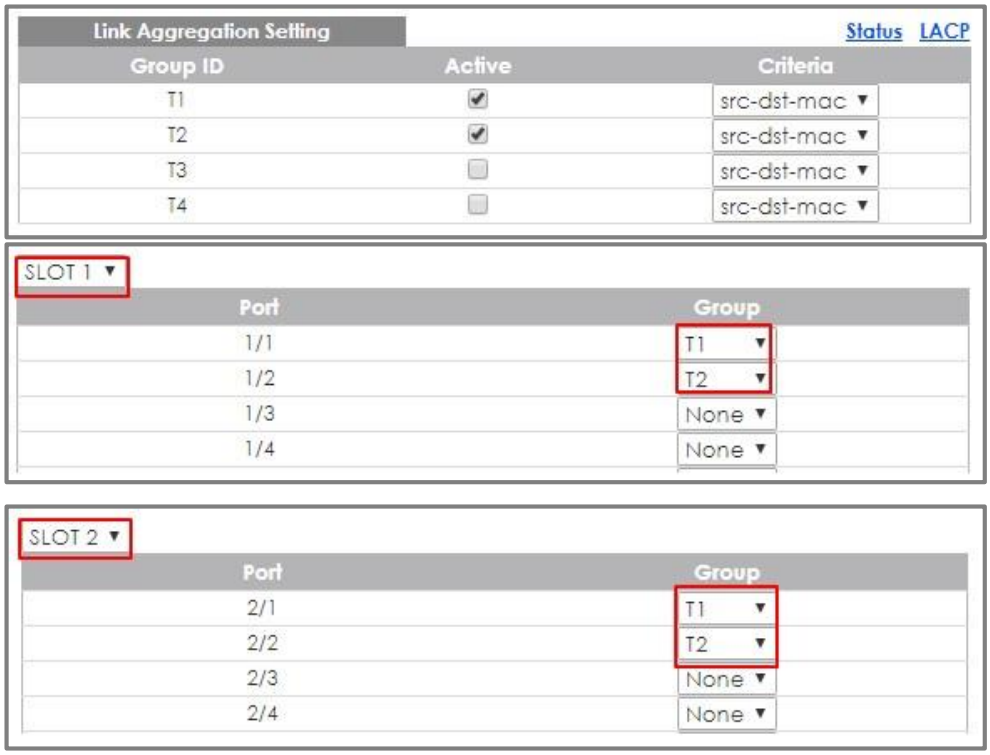
Примечание:
Обычно последние два порта коммутатора резервируются для стекирования. В коммутаторе XGS460032 это порты 31 и 32 (у других моделей эти порты для стекирования указаны в руководстве пользователя).

4 Теперь Switch-1 и Switch-2 объединены в стек. В индикаторе стекирования Stack ID на передней панели у них должно стоять “1” и “2”.

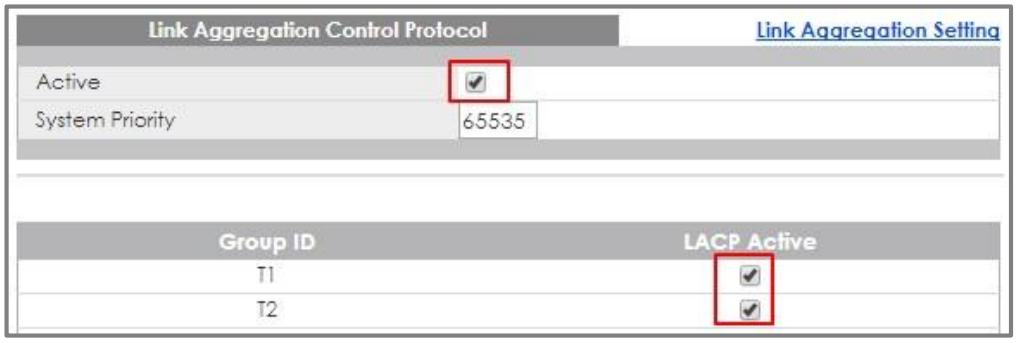
5 Сохраните конфигурацию.

3.1.2 Настройке Link Aggregation в коммутаторе, который входит в стек

1 Подключитесь к коммутатору, который входит в стек. Откройте web-интерфейс и перейдите **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting**. Активируйте T1 и T2. Выберите SLOT 1 и назначьте Group для портов port 1/1 и 1/2 соответственно как T1 и T2. Щелкните “Apply”. Выберите SLOT 2 и назначьте Group для портов 2/1 и 2/2 соответственно как T1 и T2. Щелкните “Apply”.



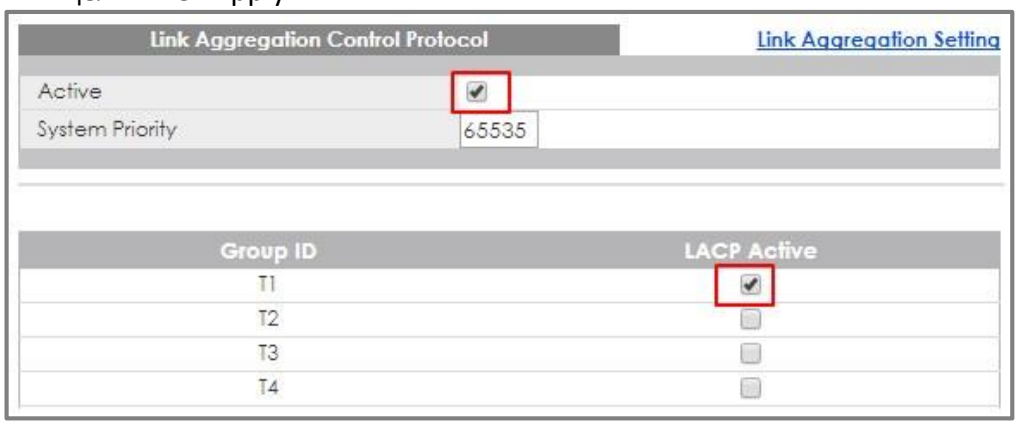
2 Перейдите в **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting >LACP**. Поставьте галочку в поле “Active”, а также для T1 и T2.



3.1.3 Настройка Link Aggregation в Switch-3

1 Перейдите в **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting**. Поставьте галочку в ACTIVE для T1 и выберите port 1 и 2 как Group T1. Щелкните “Apply”.

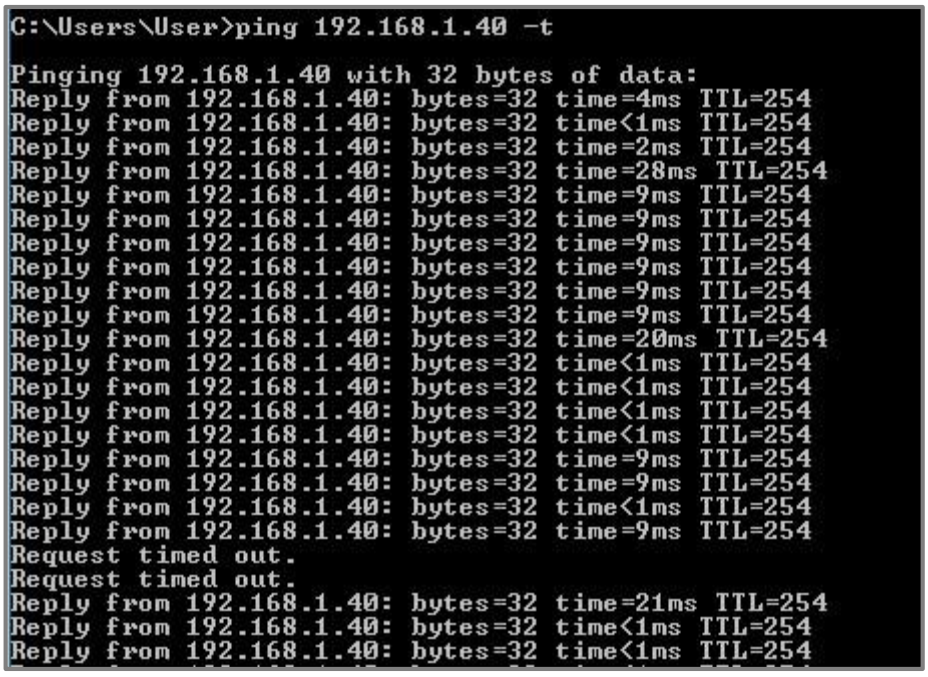
2 Перейдите в **Menu > Advanced Application > Link Aggregation > Link Aggregation Setting >LACP**. Поставьте галочку в “Active” напротив T1. Щелкните “Apply”.



3.1.4 Проверка

1 Настройте Link Aggegation между двумя сетевыми картами (NIC) сервера и соедините эти порты к портам port 1/2 и 2/2 коммутатора в стеке.

2 Запустите ping с ПК на сервер (192.168.1.40). После нескольких ping попробуйте выключить Switch-1 (Master down). Сначала ping выдаст несколько раз сообщение “timed out” и затем снова начнут приходить ответы от сервера, что означает, что резервный коммутатор Switch-2 (Backup) стал новым Мастером.



3.1.5 Почему не получается объединить коммутаторы в стек

1 Обычно для стекирования используются последние два порта коммутатора. Если для стекирования использовать другие порты, то коммутаторы не смогут работать в стеке.

2 Перед тестированием обязательно сохраните конфигурацию иначе вам не удастся ее восстановить после перезагрузки и надо будет заново настроить Link Aggregation.

3.2 Как настроить RSTP в топологии ring

В этом примере показано как настроить RSTP (Rapid Spanning Tree Protocol) в топологии ring ля резервирования сетевых соединений.

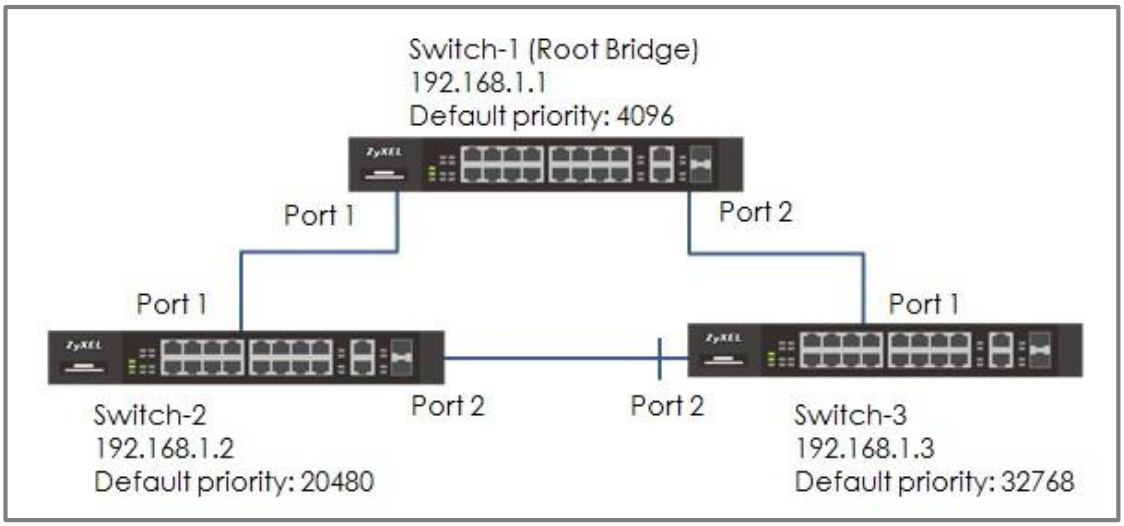


Иллюстрация 13 Настройка RSTP в топологии ring

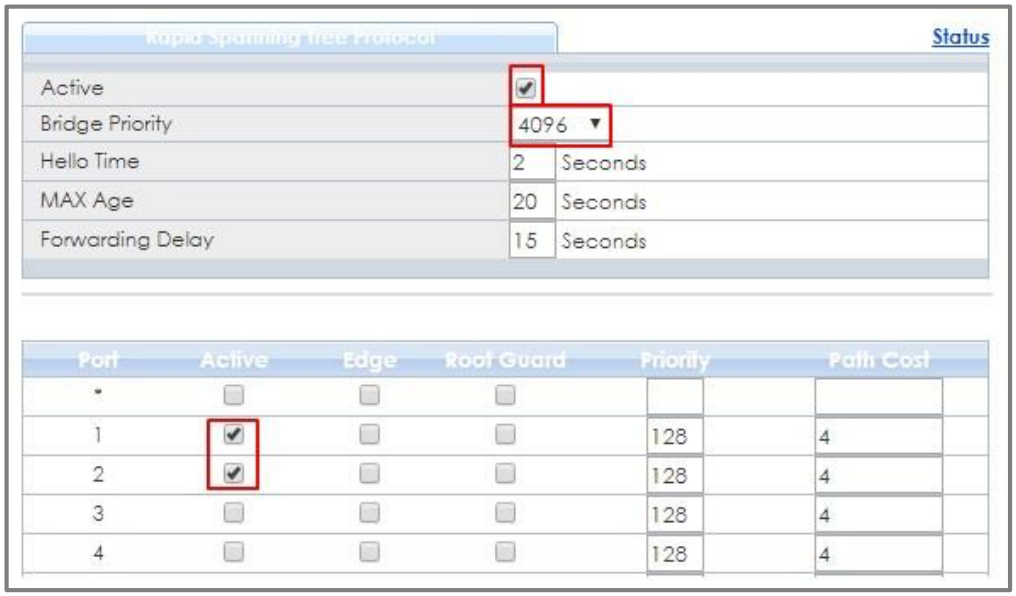
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

3.2.1 Настройка конфигурации коммутатора

1 Убедитесь, что нет соединения между **Switch-2** и **Switch-3** иначе до завершения настойки RSTP в сети образуются ненужные петли.

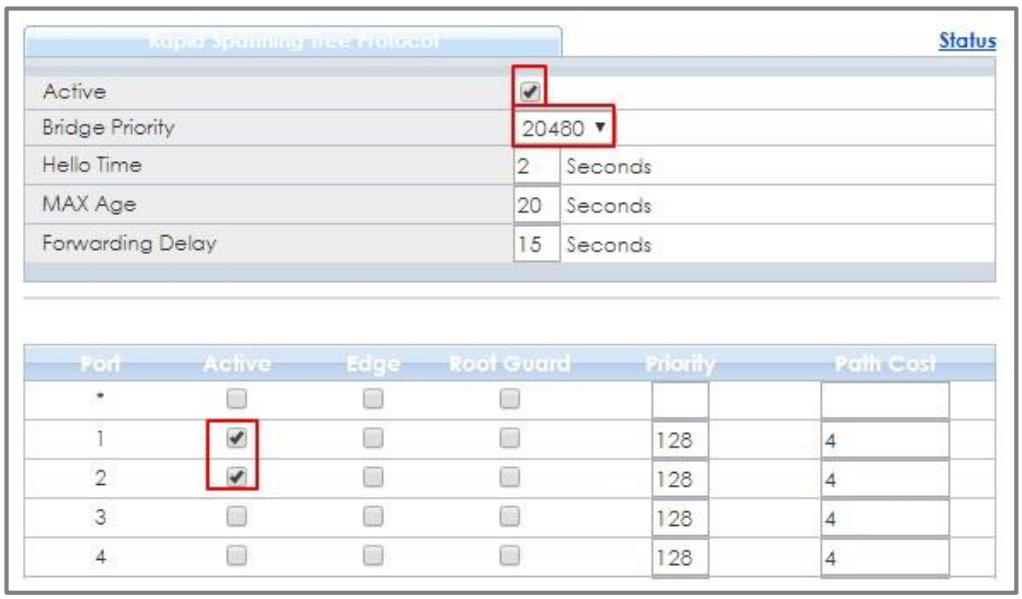
2 Настройте Switch-**1**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Убедитесь, что в Spanning Tree Configuration выбрана **Rapid Spanning Tree**. Если нет, то выберите ее и щелкните “Apply”.

3 Настройте Switch-**1**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Поставьте галочку в “**Active**”. Назначьте Bridge Priority = **4096**. Активируйте порты port **1**, **2**. Щелкните “Apply”.



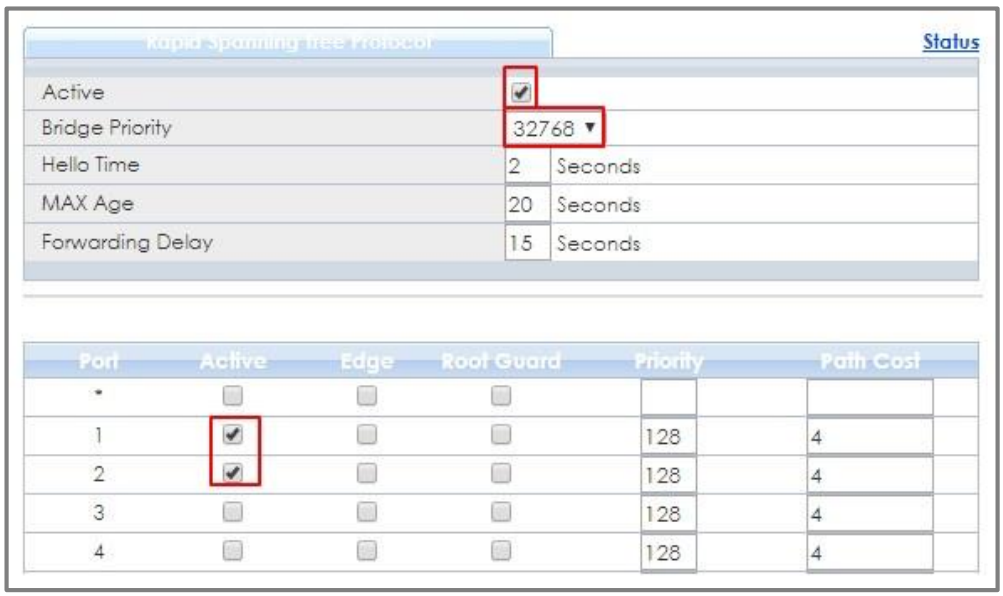
4 Настройте Switch-**2**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Убедитесь, что в Spanning Tree Configuration выбрана **Rapid Spanning Tree**. Если нет, то выберите ее и щелкните “Apply”.

5 Настройте Switch-**2**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Поставьте галочку в “**Active**”. Назначьте Bridge Priority = **20480**. Активируйте порты port **1**, **2**. Щелкните “**Apply**”.



6 Настройте Switch-**3**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Убедитесь, что в Spanning Tree Configuration выбрана **Rapid Spanning Tree**. Если нет, то выберите ее и щелкните “Apply”.

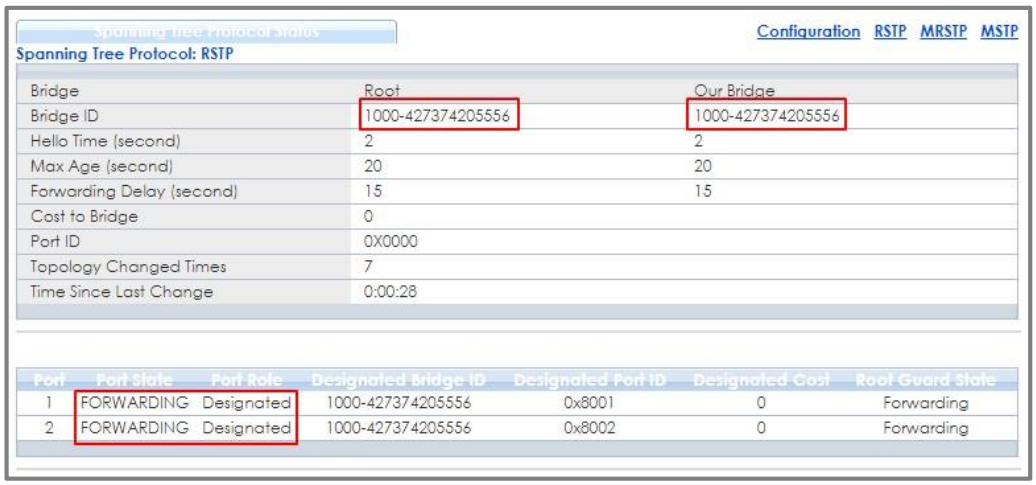
7 Настройте Switch-**3**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Поставьте галочку в “**Active**”. Назначьте Bridge Priority = **32768**. Активируйте порты **1**, **2**. Щелкните “Apply”.



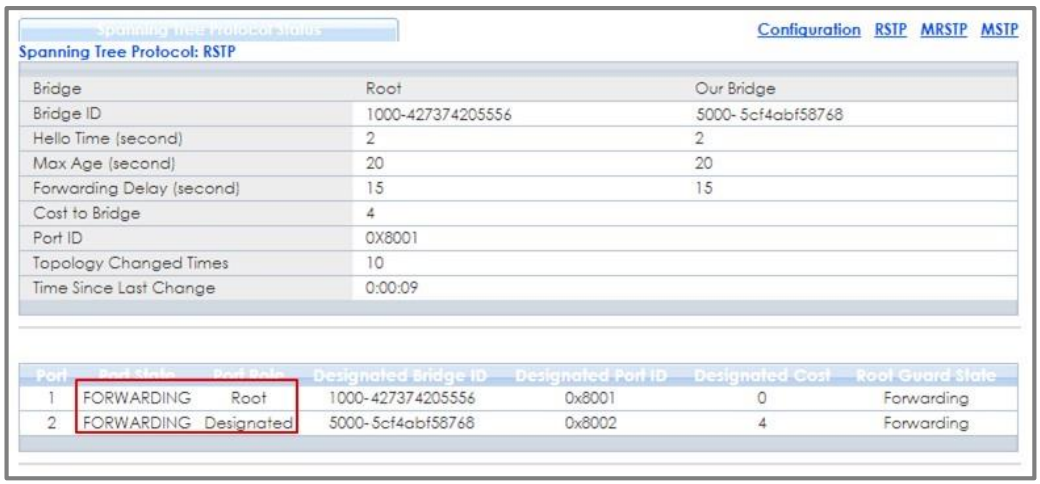
8 Наконец, соедините коммутаторы **Switch-2** и **Switch-3**.

3.2.2 Проверка результатов

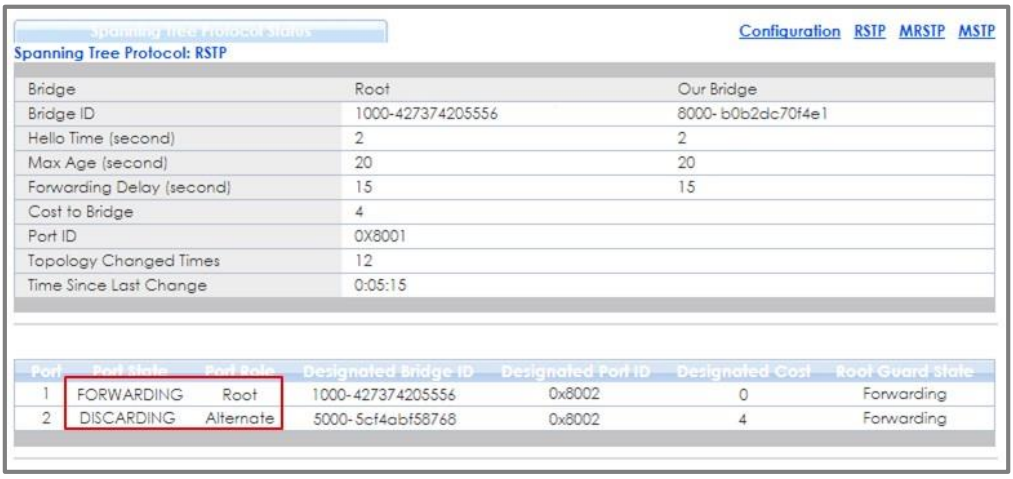
1 Проверьте состояние коммутатора **Switch-1**: Перейдите в **Menu > Advanced Application > Spanning Tree Protocol**. Идентификаторы Root Bridge ID и Our Bridge ID должны совпадать. Это означает, что Switch1 в Root Bridge. Порты port 1 и 2 должны быть в состоянии **FORWARDING**, а их роли Port Role - **Designated Ports**.



2 Проверьте состояние коммутатора **Switch-2**: Перейдите в **Menu > Advanced Application > Spanning Tree Protocol.** Проверьте состояние портов коммутатора Switch-2. Port 1 должен быть **Root Port** в состоянии **FORWARDING**, а port 2 - **Designated Port** также в состоянии **FORWARDING**.



3 Проверьте состояние коммутатора **Switch-3**: Перейдите в **Menu > Advanced Application > Spanning Tree Protocol.** Проверьте состояние портов коммутатора Switch-3. Port 1 должен быть **Root Port** в состоянии **FORWARDING**, а Port 2 - **Alternate Port** в состоянии **DISCARDING**.



3.2.3 Почему это не работает

1 Если Root Bridge оказался не тот коммутатор, который вам нужен:

a. Нужно уменьшить приоритет Spanning Tree этого устройства.

b. Нужно увеличить приоритет Spanning Tree другого устройства.

Коммутатор с **САМЫМ НИЗКИМ** приоритетом будет Root Bridge. Если приоритеты у двух коммутаторов совпадают, то Root Bridge будет коммутатор с **НАИМЕНЬШИМ MAC-адресом**.

2 Если у вас нет доступа к управлению коммутатором и светодиоды его портов постоянно мигают, то нужно разорвать топологию ring, разорвав любое дублирующее соединение для восстановления доступа к управлению. Такая ситуация часто возникает до того, как Spanning Tree сконфигурирована на устройствах или при ошибках в конфигурации Spanning Tree.

3.3 Как настроить VRRP чтобы предоставить хостам резервированный шлюз

Этот пример объясняет, как настроить резервирование шлюза redundancy. Протокол **Virtual Router Redundancy Protocol (VRRP)** позволяет двум шлюзам использовать один и тот же IP-адрес и в случае выхода из строя одного из этих шлюзов Интернет по-прежнему будет доступен из локальной сети.

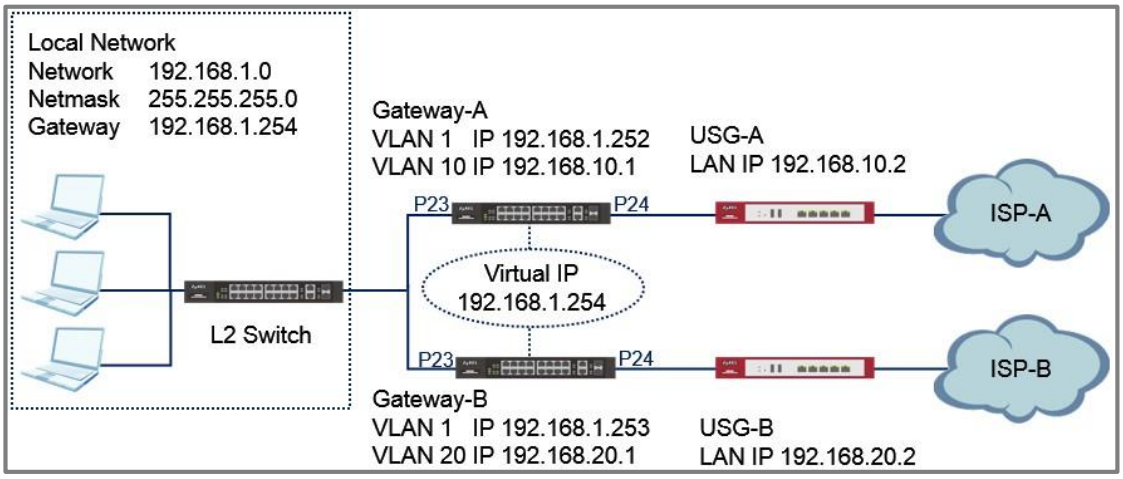


Иллюстрация 14 Два шлюза используют VRRP в одной LAN

Примечание:

Все сетевые IP-адреса и маски подсети относятся только к этому примеру.

Их нужно заменить на реальные IP-адреса и маски подсети вашей сети.

VRRP поддерживают только коммутаторы серий GS/XGS/XS3700 и XGS4600.

Коммутатором L2 Switch может быть любой коммутатор Zyxel, использующий конфигурацию по умолчанию.

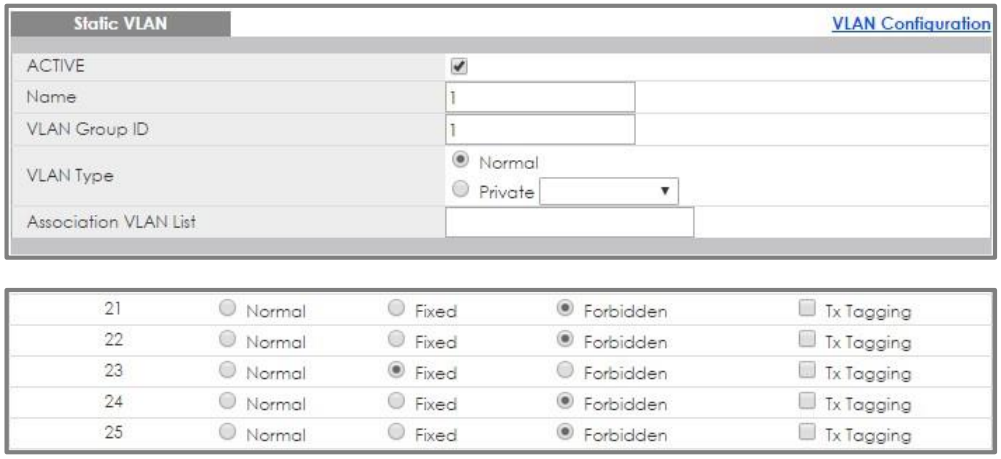
В этом примере для доступа к Интернету используются каналы двух разных провайдеров Internet Service Provider (ISP).

Интерфейс пользователя (UI) в этом примере относятся к коммутатору XGS4600.

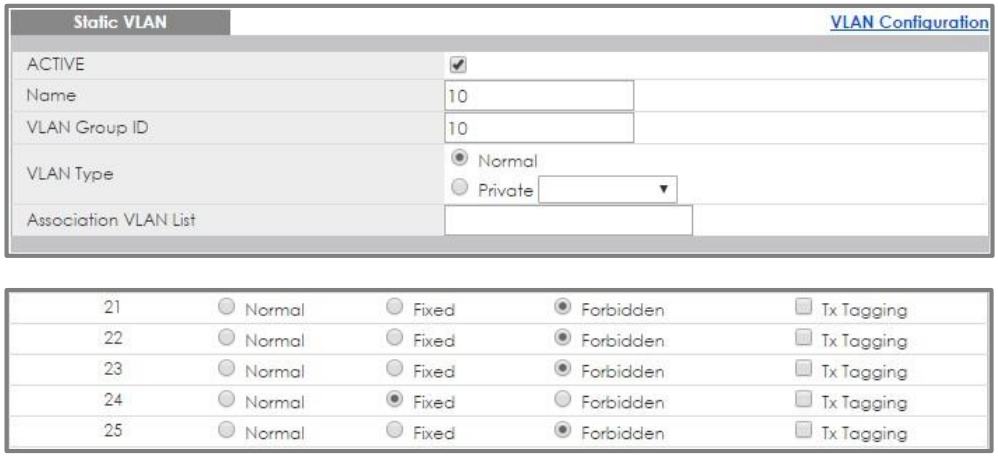
3.3.1 Настройка шлюза Gateway-A

1 Откройте web-интерфейс шлюза Gateway-A.

2 Перейдите в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Создайте/отредактируйте VLAN чтобы только порт Port 23 был fixed port. Щелкните **Add**.

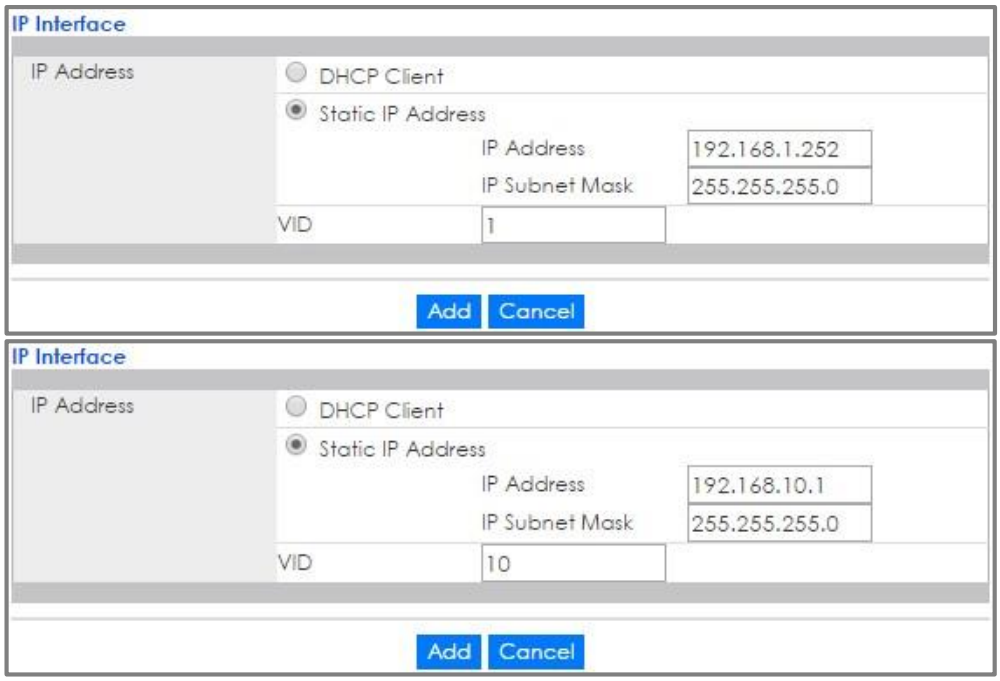


3 Перейдите в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Создайте/отредактируйте VLAN чтобы только порт Port 24 был fixed port. Щелкните **Add**.



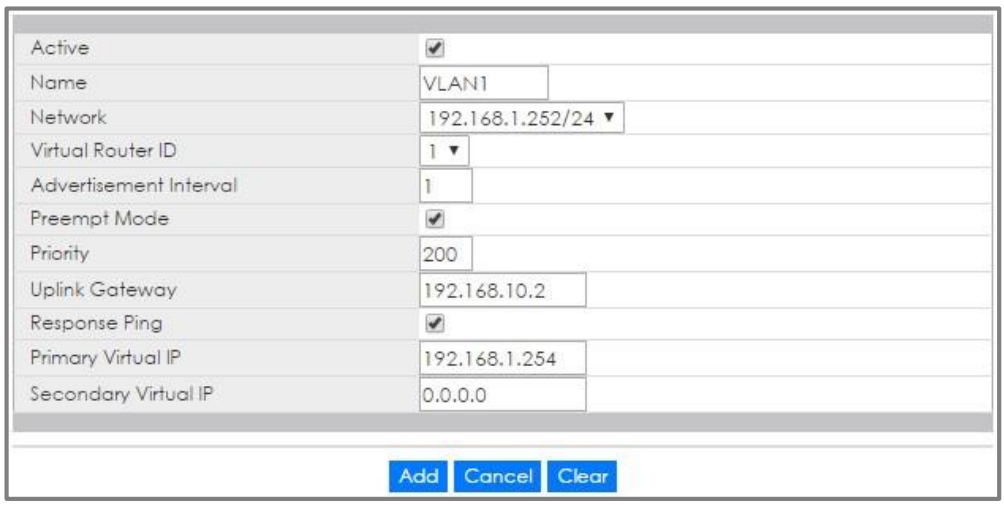
4 Перейдите в **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте port 24 на PVID 10. Щелкните **Apply**.

5 Перейдите в **Basic Setting > IP Setup**. Задайте IP-адрес для VLAN 1. Щелкните **Add** и выполните ту же операцию для VLAN 10.



6 Перейдите в **Basic Setting > IP Setup**. Настройте шлюз In-band Default Gateway. Щелкните **Apply**.

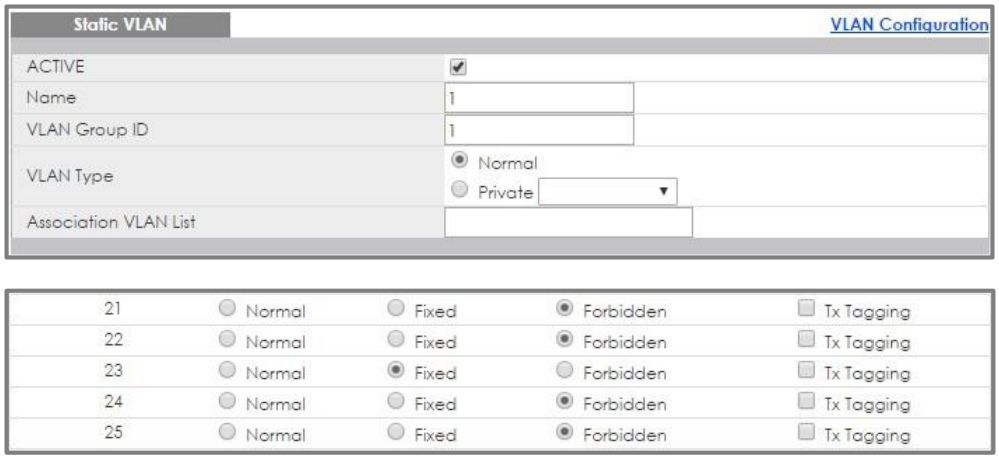
7 Перейдите в **IP Application > VRRP > Configuration**. Включите VRRP для сети “192.168.1.252/24”. Убедитесь, что приоритет priority - “200”. Щелкните **Add**.



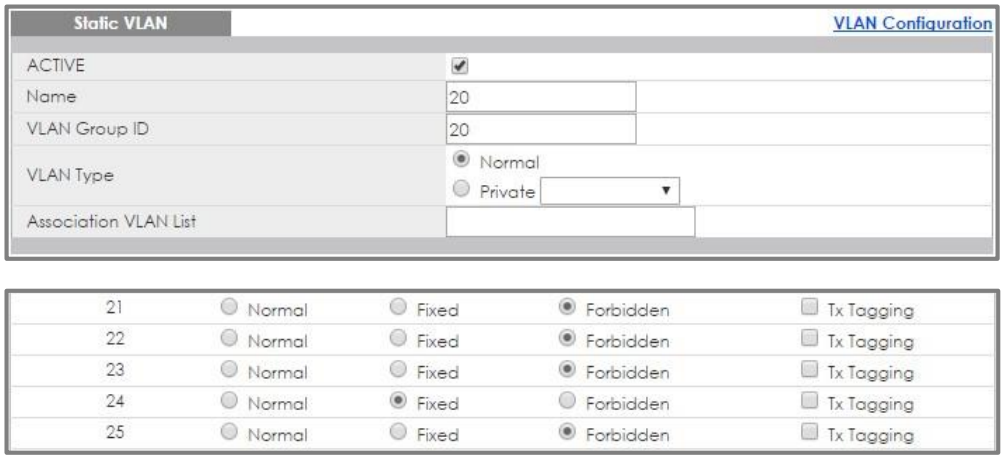
3.3.2 Настройка шлюза Gateway-B

1 Откройте web-интерфейс шлюза Gateway-B.

2 Перейдите в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Создайте/отредактируйте VLAN чтобы только порт Port 23 был fixed port. Щелкните **Add**.

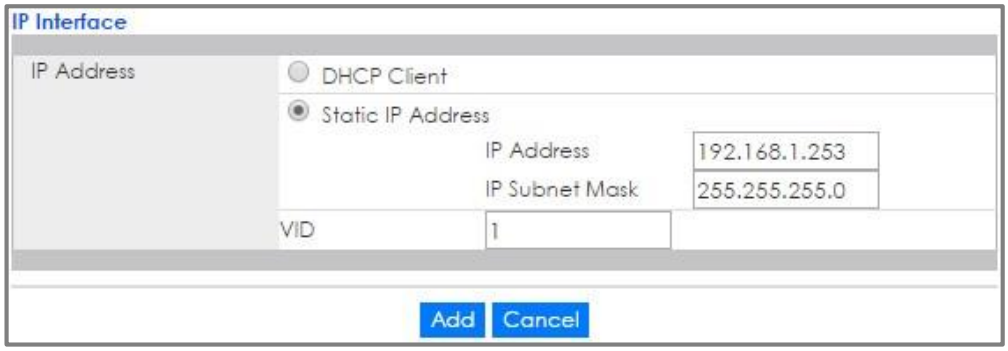


3 Перейдите в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. Создайте/отредактируйте VLAN чтобы только порт Port 24 был fixed port. Щелкните **Add**.



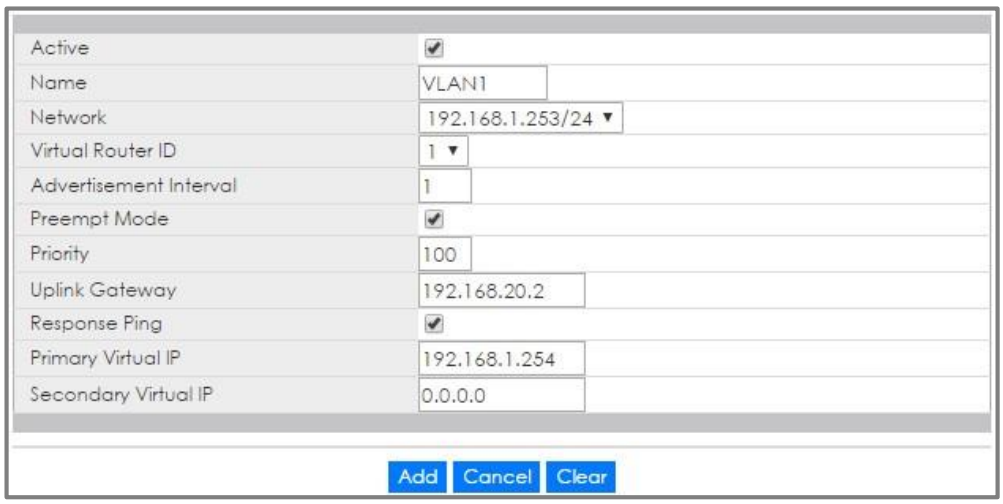
4 Перейдите в **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте port 24 на PVID 20. Щелкните **Apply**.

5 Перейдите в **Basic Setting > IP Setup**. Задайте IP-адрес для VLAN 1. Щелкните **Add** и выполните ту же операцию для VLAN 20.



6 Перейдите в **Basic Setting > IP Setup**. Настройте шлюз по умолчанию Default Gateway. Щелкните **Apply**.

7 Перейдите в **IP Application > VRRP > Configuration**. Включите VRRP для сети “192.168.1.252/24”. Щелкните **Add**.



3.3.3 Проверка результатов настройки

1 Убедитесь, что шлюз Gateway-A - это Master VRRP Router. Перейдите в **IP Application > VRRP**. VR Status должен быть **Master**.

2 Убедитесь, что шлюзы Gateway-B is the Backup VRRP Router. Перейдите в **IP Application > VRRP**. VR Status должен быть **Backup**.

3 Убедитесь, что шлюзы Gateway-A and Gateway-B записаны как default route (маршрут по умолчанию) в таблице **Maintenance > Routing Table** соответствующих USG.

Routing Table Status

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.1.0/24	192.168.1.252	192.168.1.252	1	LOCAL	0:00:54
2	192.168.10.0/24	192.168.10.1	192.168.10.1	1	LOCAL	0:00:44
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	138:42:02
4	default	192.168.10.2	192.168.10.1	1	STATIC	0:00:23

Routing Table Status

Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.1.0/24	192.168.1.253	192.168.1.253	1	LOCAL	0:04:41
2	192.168.20.0/24	192.168.20.1	192.168.20.1	1	LOCAL	0:04:29
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	139:13:20
4	default	192.168.20.2	192.168.20.1	1	STATIC	0:03:45

4 Настройте хост со статическим IP-адресом. С хоста должны доходить ping на виртуальный IP-адрес **192.168.1.254**.

```
C:\Windows\system32>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=254
Reply from 192.168.1.254: bytes=32 time<1ms TTL=254
Reply from 192.168.1.254: bytes=32 time<1ms TTL=254
Reply from 192.168.1.254: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5 Отсоедините порт port 23 или port 24 шлюза Gateway-A. С хостов должны по-прежнему проходить ping на виртуальный IP-адрес **192.168.1.254**.

3.3.4 Почему это не работает

1 Если у хостов нет доступа к Интернету когда шлюз Gateway-A отключен от сети, то нужно проверить:

a. IP-интерфейсы хостов и шлюза Gateway-B относятся к одной подсети и VLAN.

b. Подключение порта port 23 или port 24 шлюза Gateway-B.

c. Шлюз Gateway-B является default route для USG-B.

3.4 Как настроить контроль полосы пропускания для ограничения скорости входящего или исходящего трафика

В этом примере объясняется, как настроить контроль полосы пропускания для ограничения скорости входящего и/или исходящего трафика. В этом примере используются два компьютера: клиент FTP Client (PC) и сервер FTP Server (FTPServer). PC может загружать файлы с/на FTP Server.

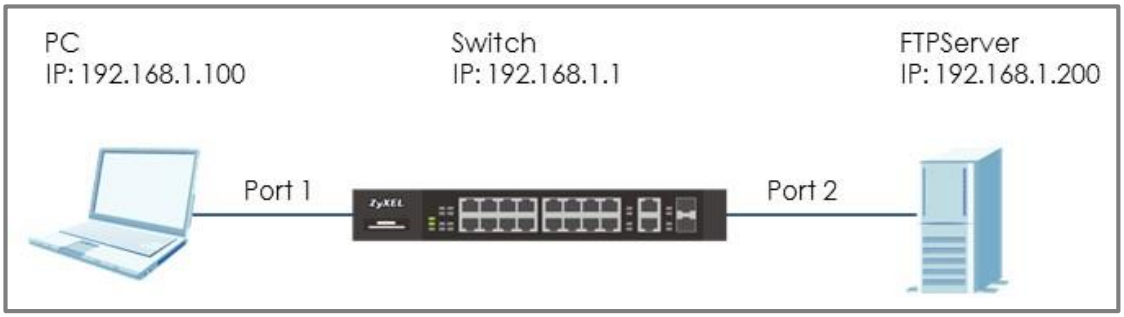
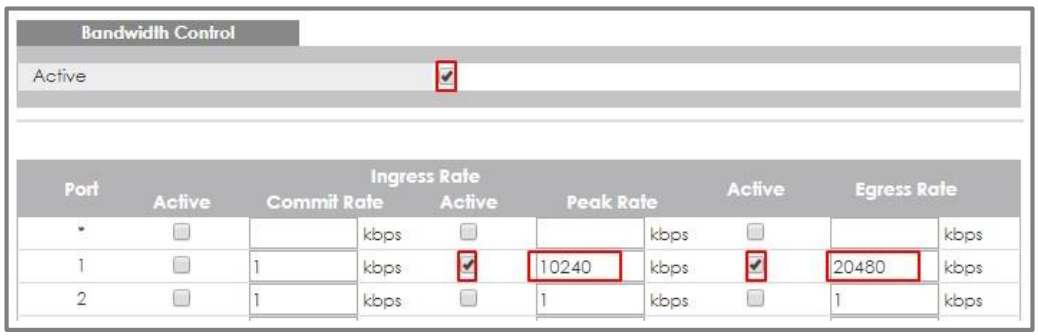


Иллюстрация 15 Настройка контроль полосы пропускания для ограничения скорости трафика

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

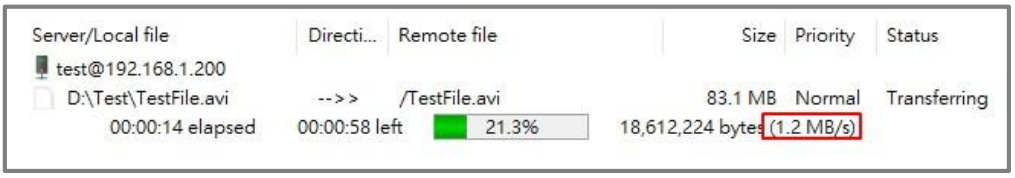
3.4.1 Настройка конфигурации коммутатора

1 Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Bandwidth Control**. Поставьте галочку в “**Active**”. Введите скорость в **Ingress Rate** (PC **Upload rate**) = **10240 kbps** и **Egress Rate** (PC **Download rate**) = **20480 kbps**. Также надо поставить галочку в “**Active**” для порта. Щелкните “**Apply**”.

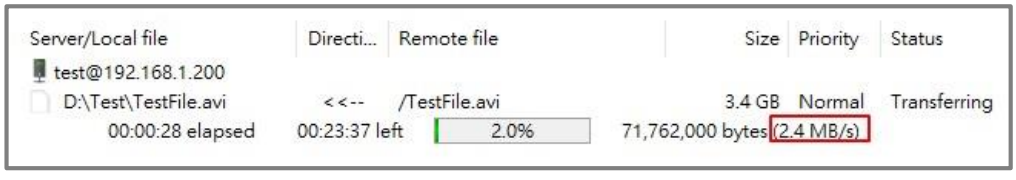


3.4.2 Проверка результатов

1 Попробуйте загрузить файл с PC на FTP Server. Скорость передачи должна быть около 1.2 MB/s (или 10240 Mb/s).



2 Попробуйте загрузить файл с FTP Server на PC. Скорость передачи должна быть около 2.4 MB/s (or 20480 Mb/s).



3.5 Как настроить ACL для ограничения скорости трафика IP

Иногда требуется ввести ограничения скорости для отдельных VLAN локальной сети, например, если в компании VLAN 10 предназначена для персонала, а VLAN 20 - для гостей, то ограничив скорость в VLAN 20, мы обеспечим больше полосы пропускания для пользователей в VLAN 10. В этом примере показывается, как настроить ACL на ограничение скорости трафика VLAN. Для проверки результатов этой настройки нужно сравнить скорости входящего/исходящего трафика в VLAN 10 и VLAN 20.

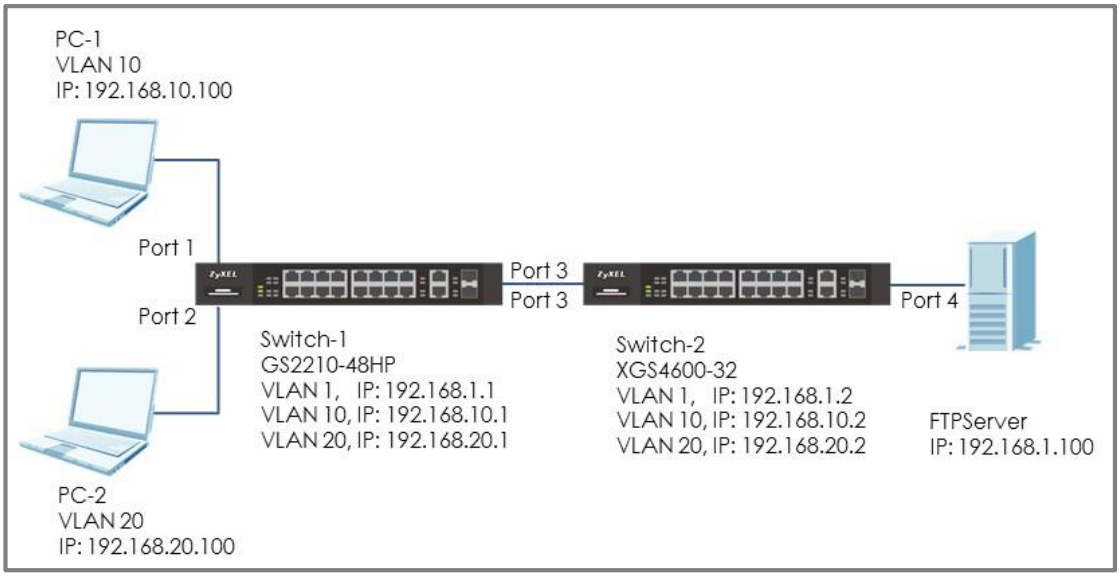


Иллюстрация 16 Настройка ACL для ограничения трафика VLAN

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

3.5.1 Настройка VLAN и маршрутизации трафика Route Traffic

1 Настройте параметры VLAN (VLAN 10 и VLAN 20) на коммутаторах Switch1 и Switch-2 (См. **2.1 Как настроить коммутатор на изоляцию трафика между отделами**).

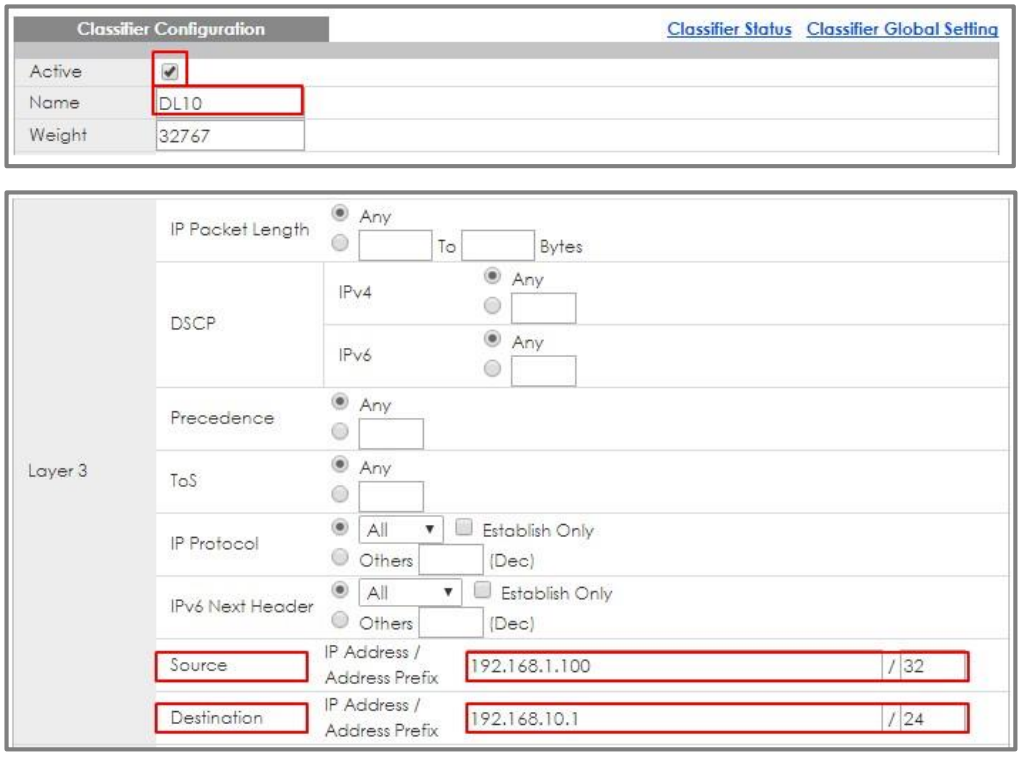
2 Настройте маршрутизацию трафика route traffic на Switch-1 и Switch-2 (см. **2.2 Как настроить коммутатор на маршрутизацию трафика через VLAN**)

3.5.2 Настройка Classifier

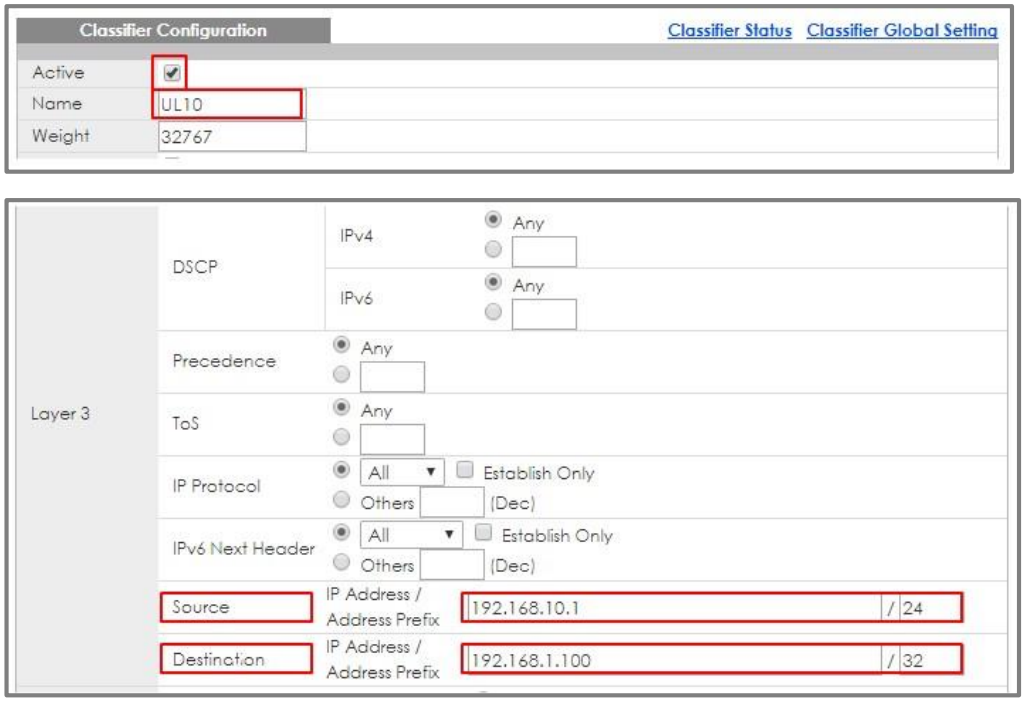
1 Настройте **Classifier** на коммутаторе Switch-2: Перейдите в **Menu > Advanced Application > Classifier > Classifier Configuration**. Настройте четыре 4 Classifier (по два Classifier для трафика download и upload в VALN 10 и в VLAN 20)

> Примечание:
> Если трафик соответствует **Classifier**, то ACL применяет к нему соответствующее правило **Policy Rule**.

2 Настройка Classifier для трафика download в VLAN 10: поставьте галочку в “Active” и введите имя в поле Name. Настройте **Layer 3 > Destination** как **192.168.10.0/24** (это означает, что получатель в VLAN 10) и **Source** как **92.168.1. 100/32** (это означает, что отправитель - FTPServer). Нажмите “Add”.



3 Настройка Classifier для трафика upload в VLAN 10: Поставьте галочку в “Active” и введите имя в поле Name. Настройте **Layer 3 > Destination** как **192.168.1.100/32** (это означает, что получатель FTPServer) и **Source** как **192.168.10.0/24** (это означает, что источник в VLAN 10). Нажмите “Add”.



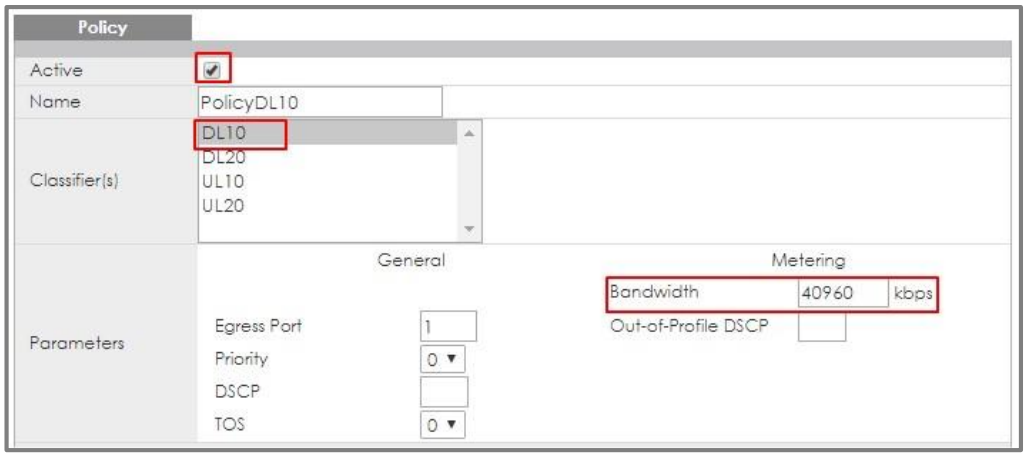
4 Настройка Classifier для трафика download в VLAN 20: поставьте галочку в “Active” и введите имя в поле Name. Настройте **Layer 3 > Destination** как **192.168.20.0/24** (это означает, что получатель VLAN 20) и **Source** как 192.168.1.100/32 (это означает, что источник FTPServer). Нажмите “Add”.

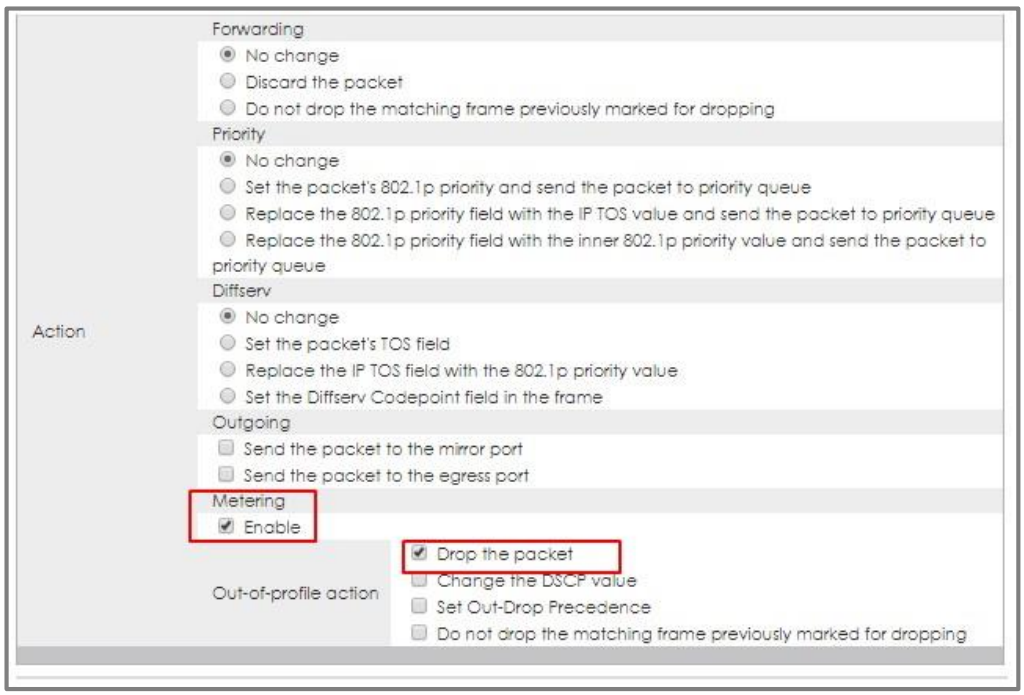
5 Настройка Classifier для трафика upload в VLAN 20: поставьте галочку в “Active” и введите имя в поле Name. Настройте **Layer 3 > Destination** как **192.168.1.100/32** (это означает, что получатель FTPServer) и **Source** как **192.168.20.0/24** (это означает, что источник VLAN 20). Нажмите “Add”.

3.5.3 Настройка the ACL (правило политики Policy Rule)

1 Настройка **Policy Rule** на Switch-2: в разделе 3.5.2 мы создали четыре Classifier. Чтобы найти их в окне Policy Rule перейдите в **Menu > Advanced Application > Policy Rule**.

2 Для Policy Rule трафика download в VLAN 10: Поставьте галочку в “Active” и введите имя в поле Name. Выберите Classifier для трафика download в VLAN 10 (DL10). Настройте действия при соответствии этому Classifier: **Bandwidth Metering**=40960 kbps. Включите **Metering** и настройте действие **Out-of-profile action** (оно будет выполняться если скорость больше полосы пропускания) на “**Drop the packet**” (Switch-2 будет отбрасывать трафик, который превышает полосу пропускания). Нажмите “Add”.





3 Для Policy Rule трафика upload в VLAN 10: Поставьте галочку в “Active” и введите имя в поле Name. Выберите Classifier для трафика upload в VLAN 10 (UP10). Настройте действия при соответствии этому Classifier: **Bandwidth Metering**=20480 kbps. Включите **Metering** и настройте действие **Out-of-profile action** на “**Drop the packet**”. Нажмите “Add”.

4 Для Policy Rule трафика download в VLAN 20: Поставьте галочку в “Active” и введите имя в поле Name. Выберите Classifier для трафика download в VLAN 20 (DP20). Настройте действия при соответствии этому Classifier: **Bandwidth Metering**=20480 kbps. Включите **Metering** и настройте действие **Out-of-profile action** на “**Drop the packet**”. Нажмите “Add”.

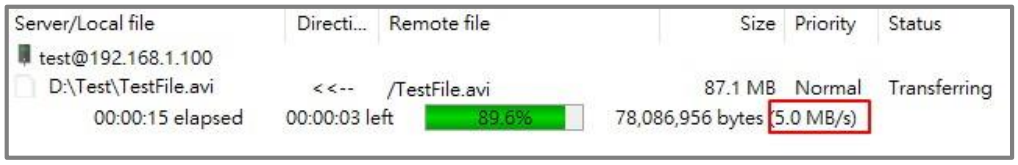
5 Для Policy Rule трафика upload в VLAN 20: Поставьте галочку в “Active” и введите имя в поле Name. Выберите Classifier для трафика download в VLAN 20 (UP20). Настройте действия при соответствии этому Classifier:

Bandwidth Metering=10240 kbps. Включите **Metering** и настройте действие **Out-of-profile action** на “**Drop the packet**”. Нажмите “Add”.

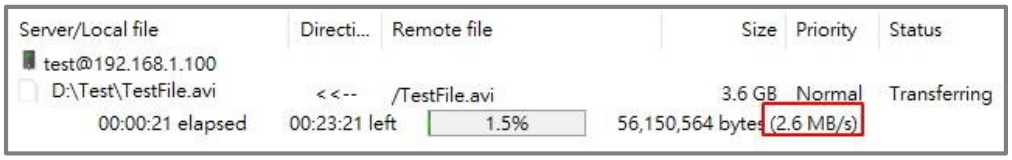
3.5.4 Проверка результатов

1 Перейдите в **Menu > Advanced Application > Classifier**. Проверьте значение “Count”. Если трафик соответствует classifier, то Match Count для этого classifier будет увеличиваться при каждом обновлении web-страницы.

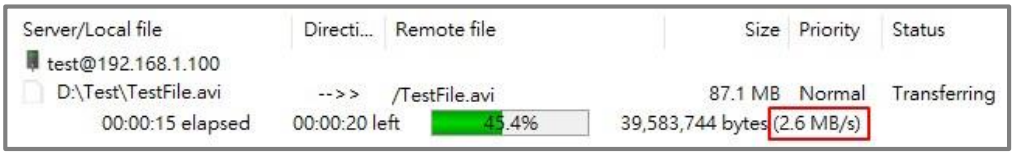
2 Загрузить на PC-1 файл с FTP Server. Скорость передачи данных должна быть около 5 MB/s (или 40960 Mb/s).



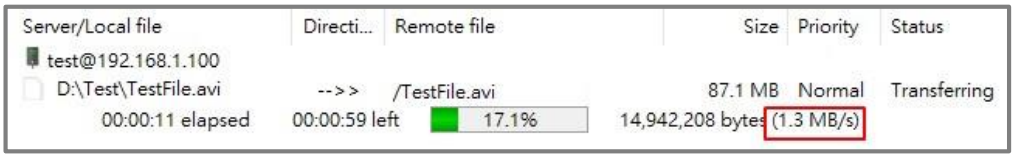
3 Загрузить с PC-1 файл на FTP Server. Скорость передачи данных должна быть около 2.6 MB/s (или 20480 Mb/s).



4 Загрузить на PC-2 файл с FTP Server. Скорость передачи данных должна быть около 2.6 MB/s (или 20480 Mb/s).



5 Загрузить с PC-2 файл на FTP Server. Скорость передачи данных должна быть около 1.2 MB/s (или 10240 Mb/s).

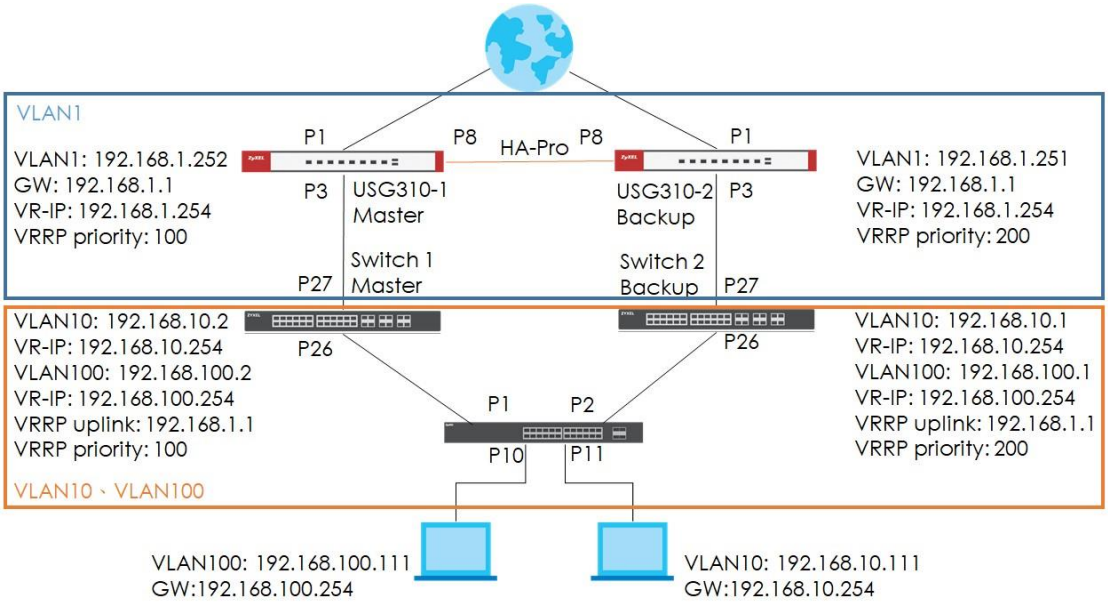


3.5.5 Почему это не работает

1 При настройке Classifier надо учитывать отправителя и получателя трафика. В этом примере мы настроили отправителя как VLAN 10 (192.168.10.0/24) при загрузке файла на Server, но не задали получателя (Server IP: 192.168.1.150). В результате скорость трафика будет ограничена когда PC будет пытаться послать трафик другим хостам из VLAN 10.

3.6 Как внедрить VRRP с несколькими интерфейсами маршрутизации и HA-pro, используя коммутатор Zyxel корпоративного класса

В предыдущей главе мы рассказали о VRRP и привел пример его настройки для резервирования, но этот пример относился к компании, у которой два интернет-провайдера (ISP). Однако у некоторых компаний только один ISP и один шлюз, подключенный к провайдеру, поэтому при сбое в работе шлюза или повреждении кабеля, соединяющего этот шлюз с провайдером, компания потеряет доступ к Интернету. Чтобы избежать этой ситуации нужно использовать два шлюза и для резервирования комбинировать VRRP с HA-pro.



В этой топологии обычно трафик передается как показано на Иллюстрации 1, но если возникнет проблема в USG310-1 (Master) или у соединения link 1 или 2, то у коммутатора Switch-1 (Master) не будет доступа к Интернету. В этой ситуации для резервирования следует использовать комбинацию VRRP и Device HA-Pro. USG310-2 (Backup) и Switch-2 (Backup) станут работать как Master и через них все хосты будут подключены к Интернету (см. Иллюстрацию 2).

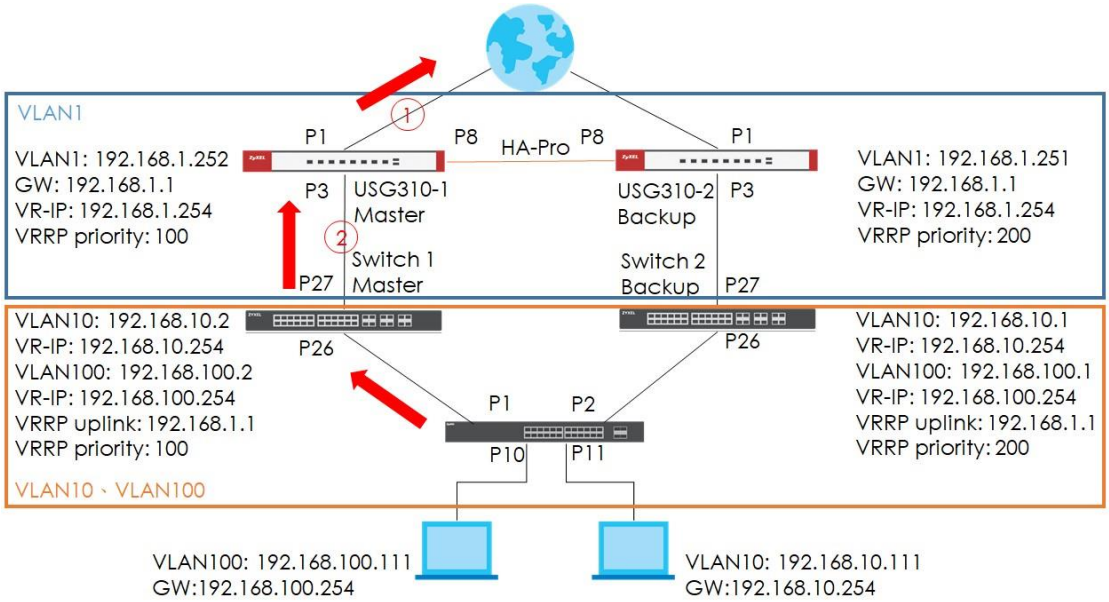


Иллюстрация 1

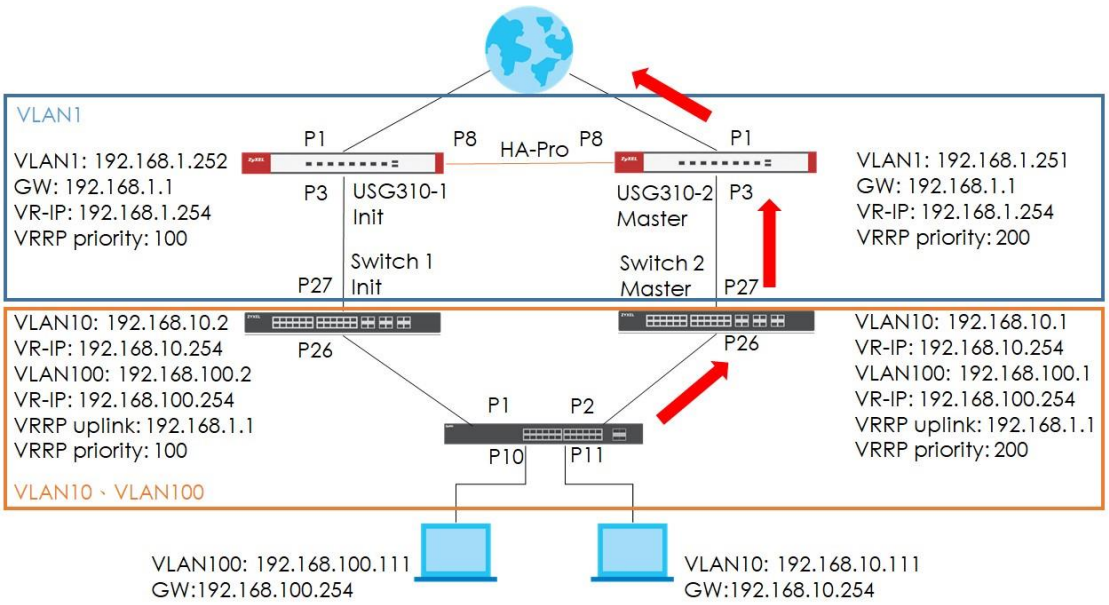


Иллюстрация 2

Примечание:

Все сетевые IP-адреса и маски подсети относятся только к этому примеру.

Их нужно заменить на реальные IP-адреса и маски подсети вашей сети.

3.6.1 Настройка конфигурации

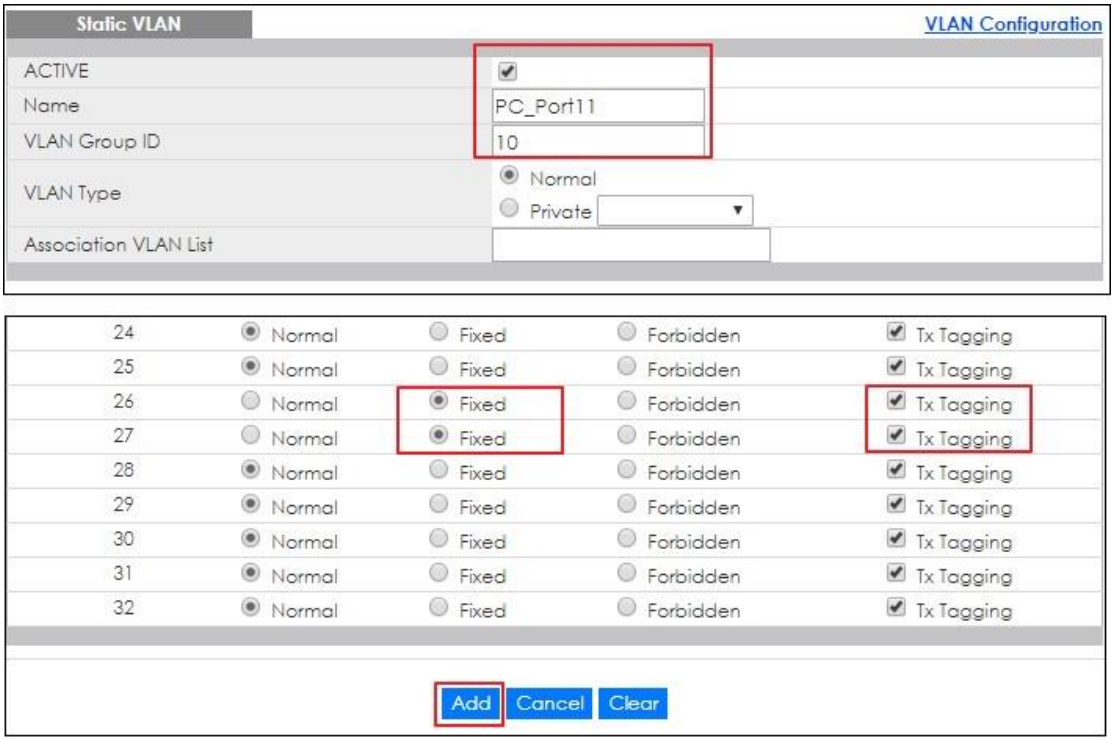
Коммутатор L3 Switch:

1. Откройте web-интерфейс switch-1 (Master)

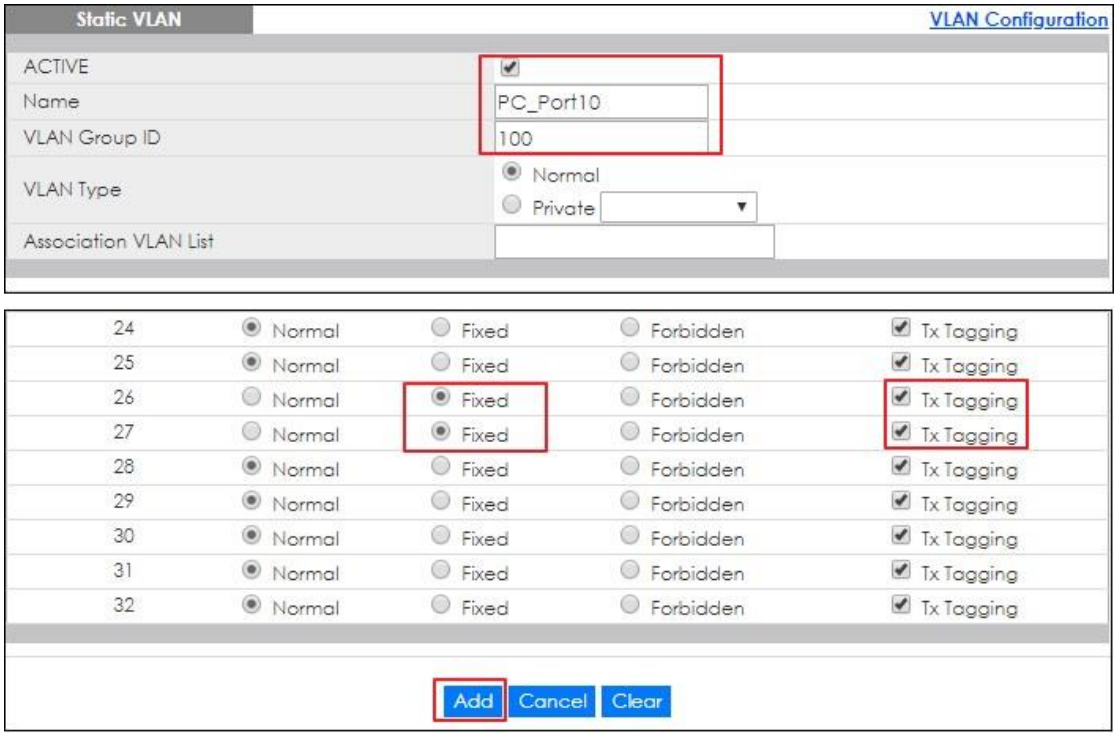
2. Перейдите в **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup**

3. Создайте VLAN 10 и VLAN 100 для хостов.

VLAN 10:

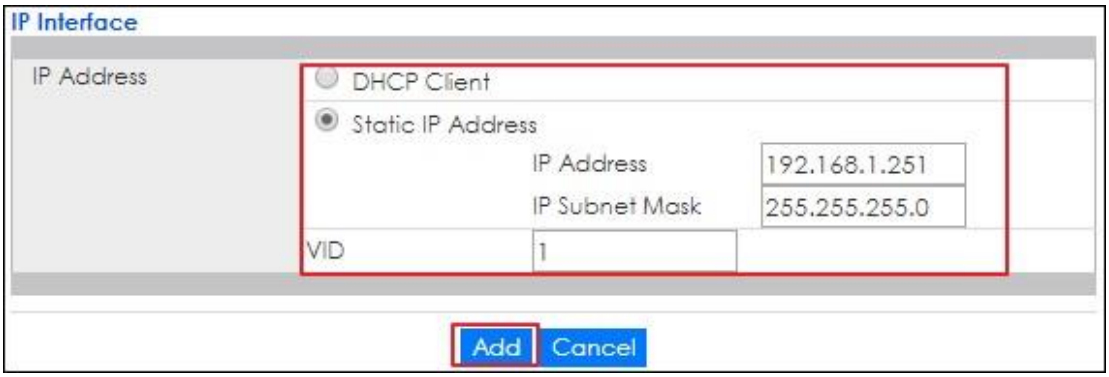


VLAN 100:



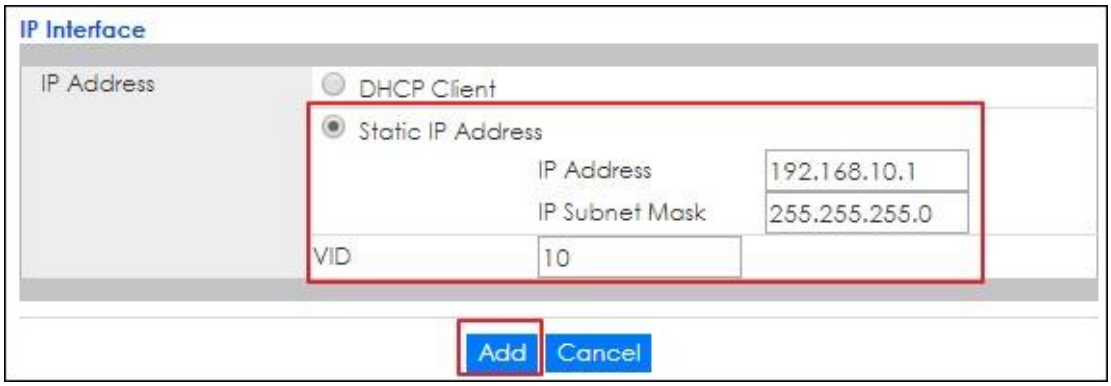
4. Перейдите к **Basic Setting > IP Setup > IP Configuration**

5. Настройте IP-интерфейс в VLAN 1 для uplink.



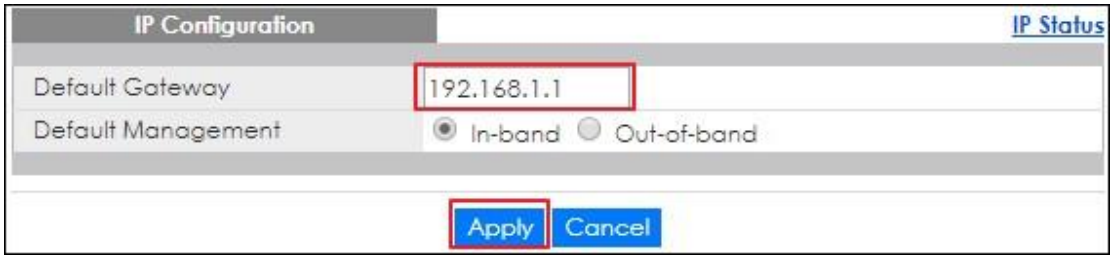
6. Настройте IP-интерфейс в VLAN 10 и VLAN 100 для хостов.

VLAN 10:



VLAN 100:

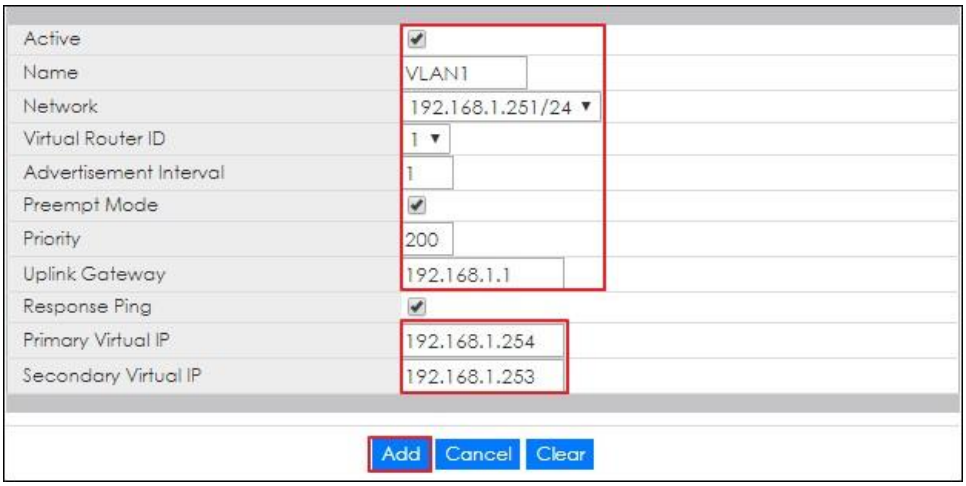
7. Настройте шлюз по умолчанию IP default gateway для интерфейса VLAN 1.



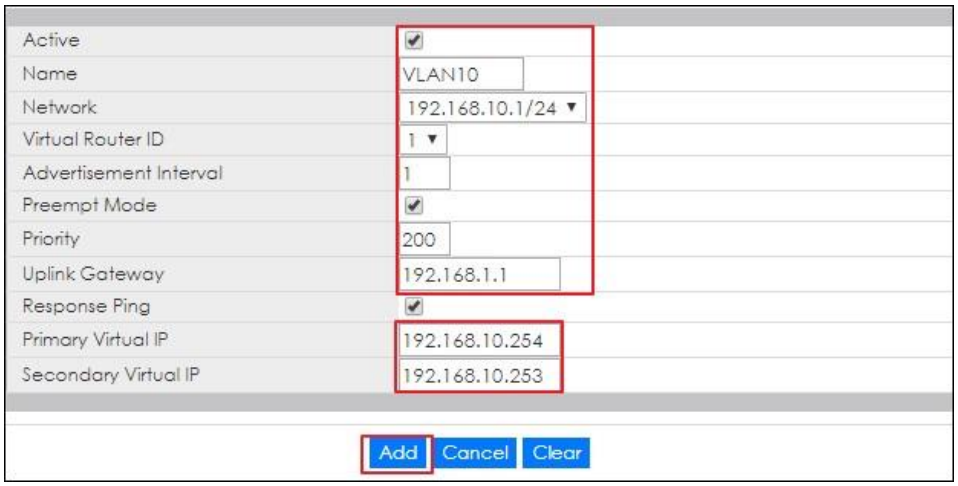
8. Перейдите в **IP Application > VRRP > Configuration**

9. Настройте VRRP на всех интерфейсах VLAN. “Response Ping” является опцией, но если Response Ring не включен, то вы сможете посылать ping на виртуальный IP-адрес.

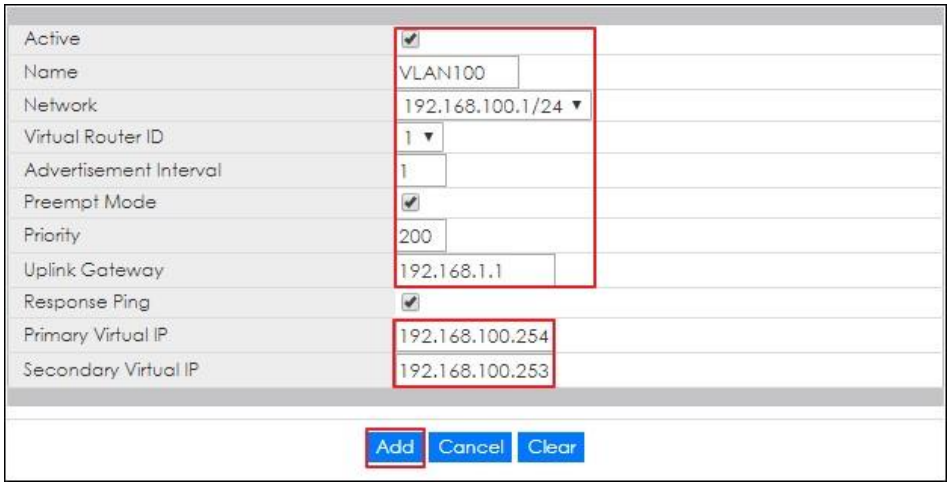
VLAN 1:



VLAN 10:



VLAN 100:

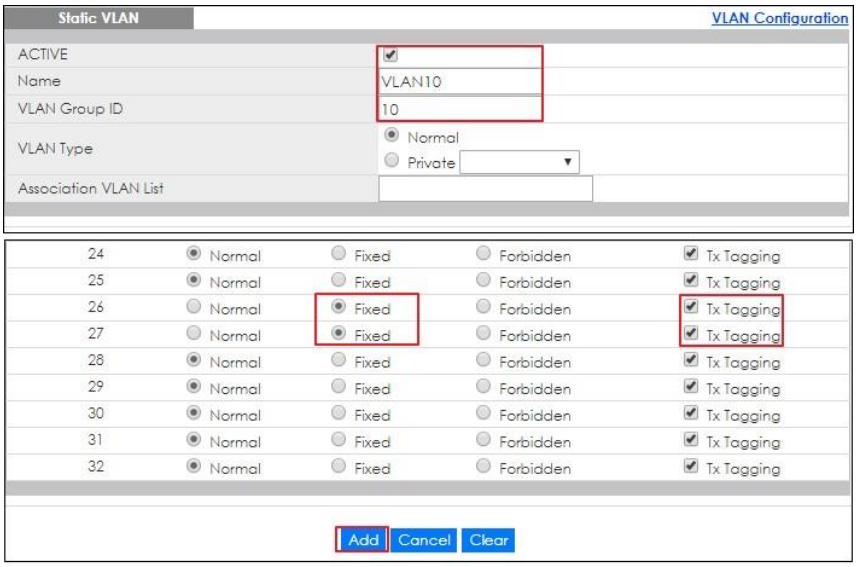


10. Откройте web-интерфейс коммутатора Switch-2 (Backup).

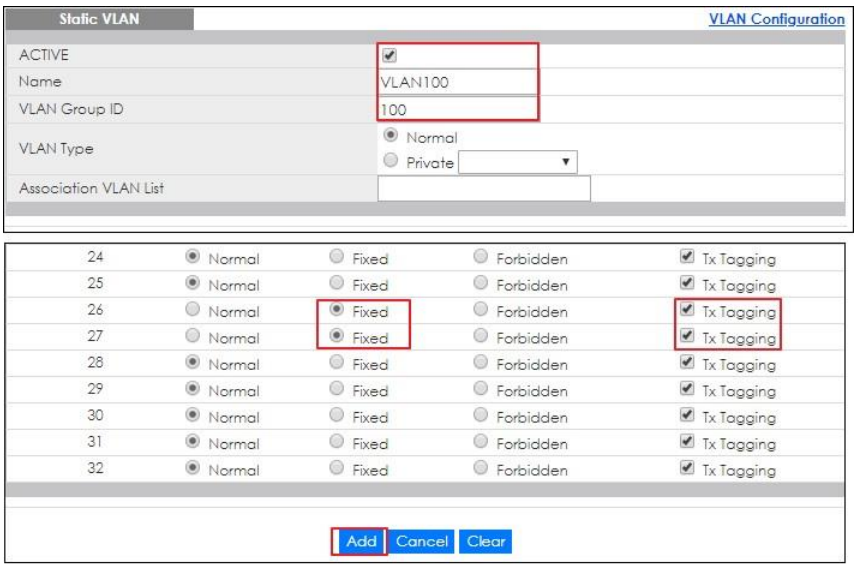
11. Перейдите в **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup**

12. Создайте VLAN 10 и VLAN 100 для хостов.

VLAN 10:



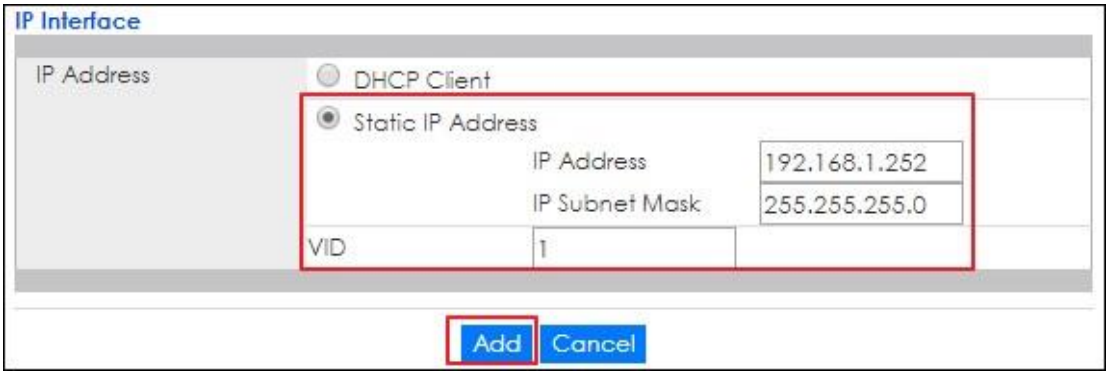
VLAN 100:



13. Перейдите в **Basic Settings > IP Setup > IP Configuration**

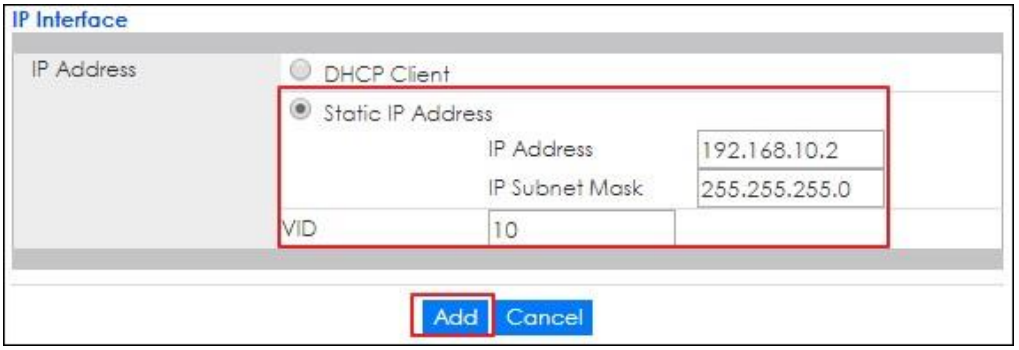
14. Настройте IP-интерфейс в VLAN 1 для uplink.

VLAN 1:

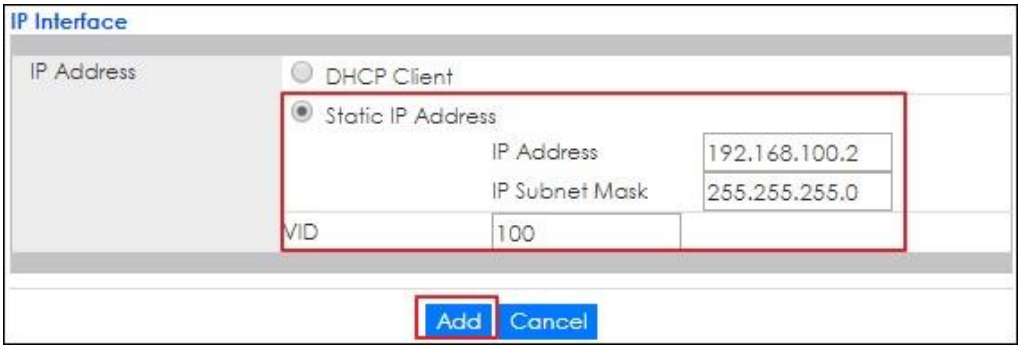


15. Настройте IP-интерфейс в VLAN 10 и VLAN 100 для хостов.

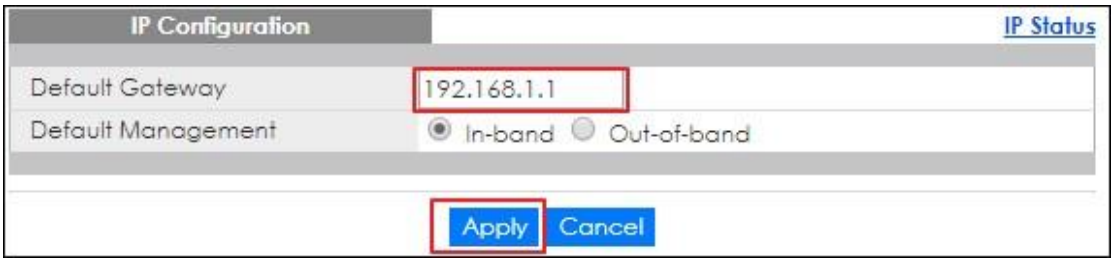
VLAN 10:



VLAN 100:



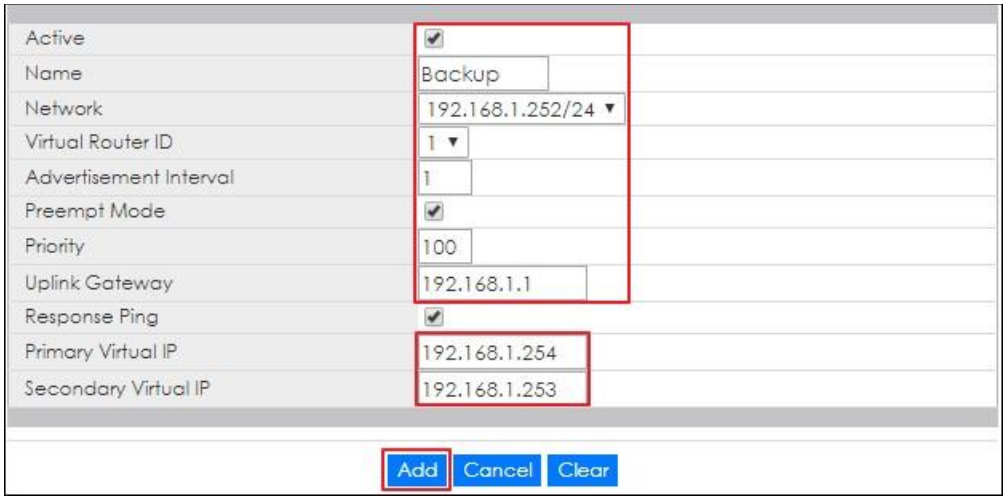
16. Настройте шлюз по умолчанию IP default gateway на VLAN 1 для аплинка.



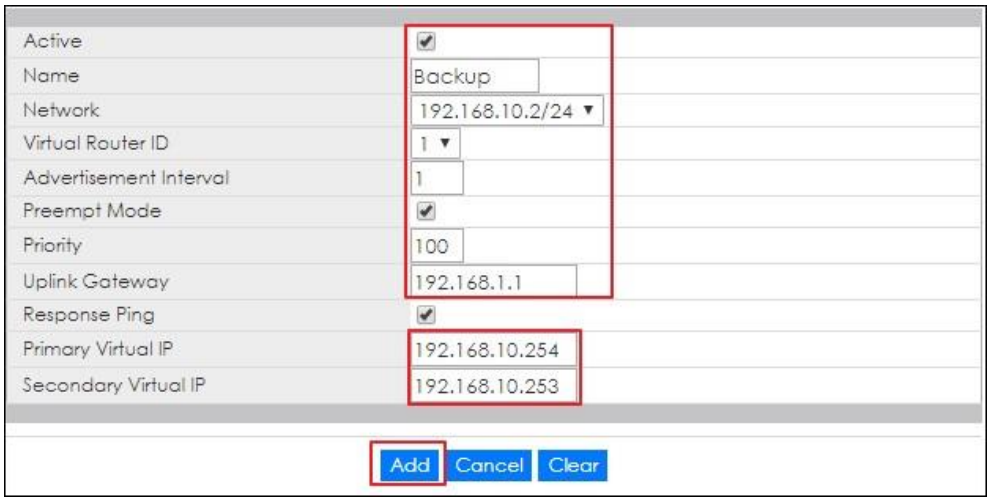
17. Перейдите в **IP Application > VRRP > Configuration**

18. Настройте VRRP на всех интерфейсах VLAN. “Response Ping” является опцией, но если Response Ring не включен, то вы сможете посылать ping на виртуальный IP-адрес.

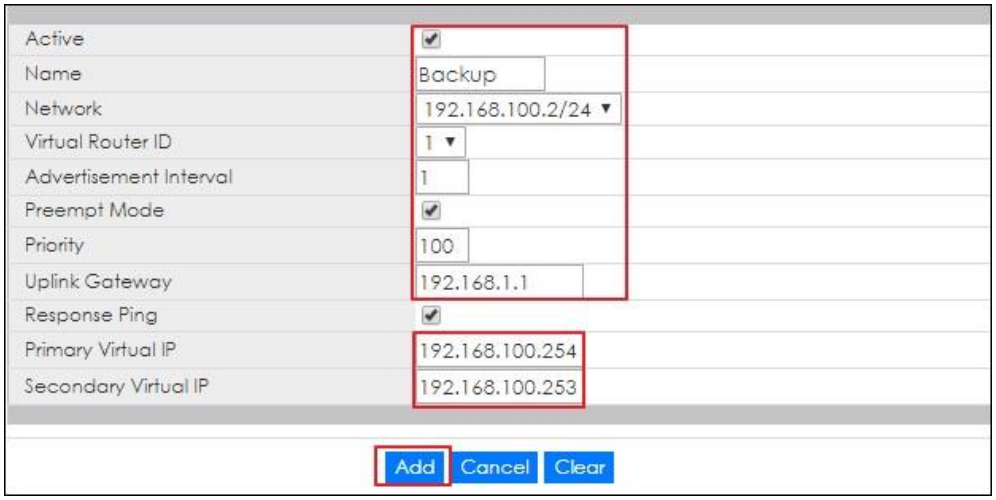
VLAN 1:



VLAN 10:



VLAN 100:



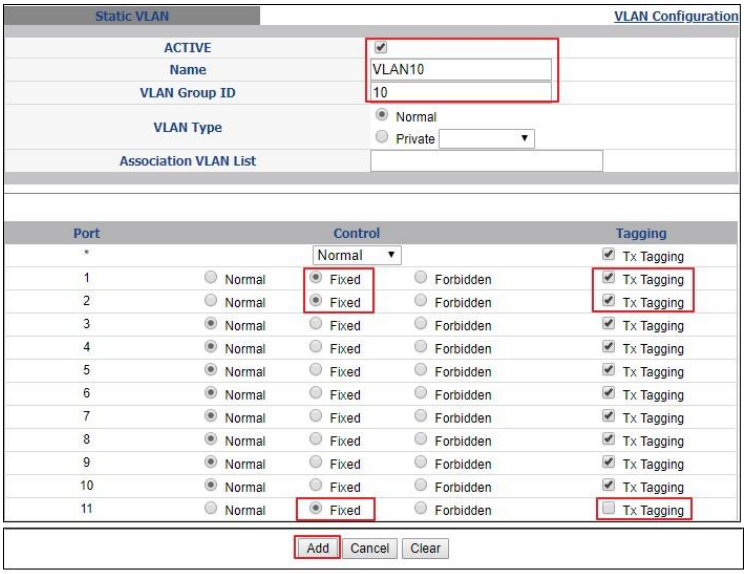
Коммутатор L2 switch:

1. Откройте web-интерфейс коммутатора layer 2 switch.

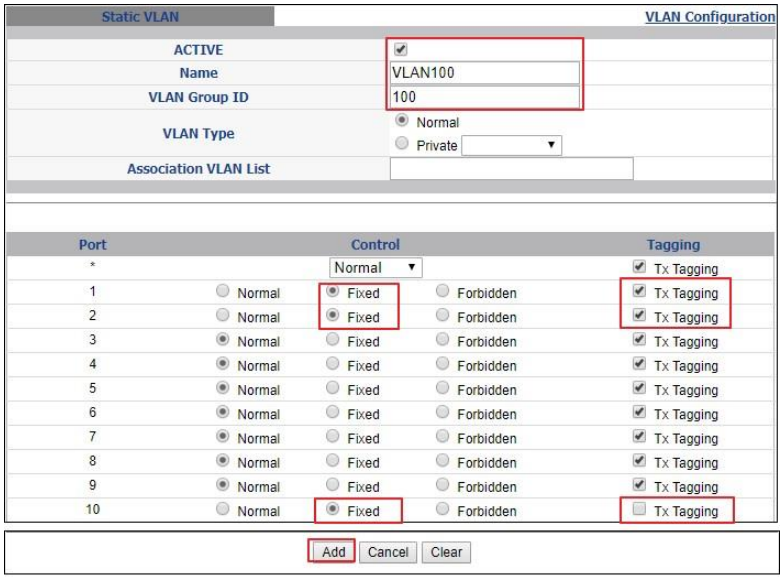
2. Перейдите в **Advanced Application > VLAN > VLAN Configuration >Static VLAN Setup.**

3. Настройте VLAN 10 и VLAN 100 для хостов.

VLAN 10:



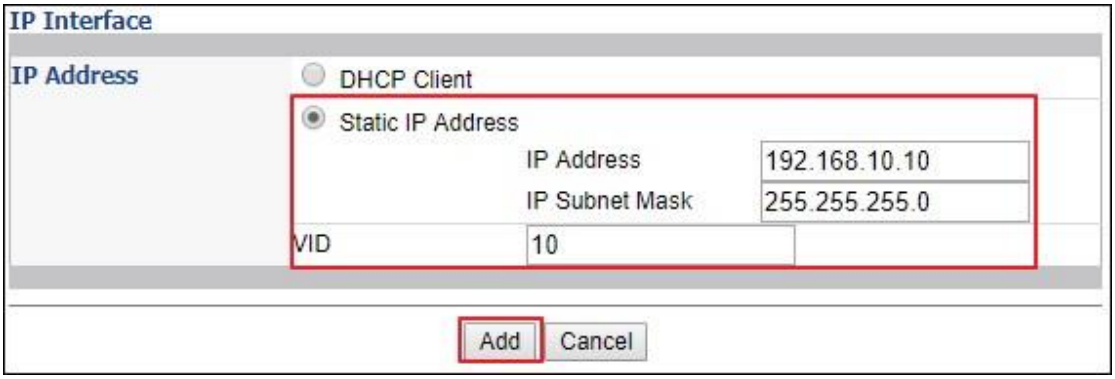
VLAN 100:



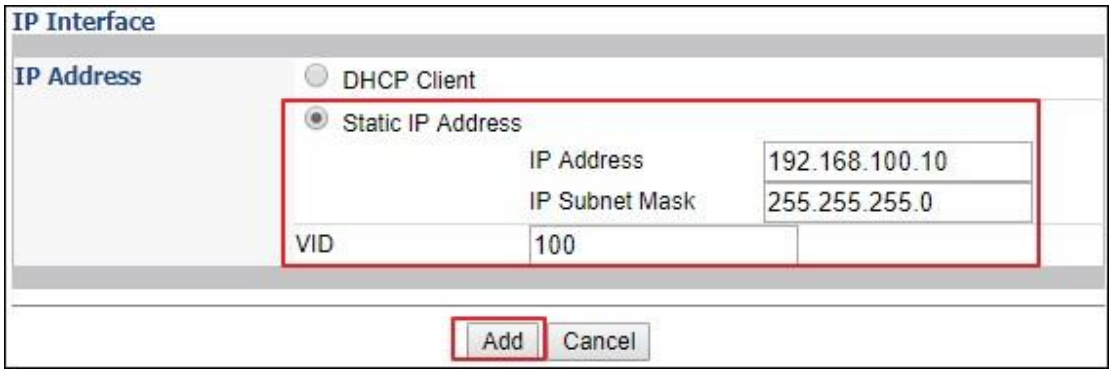
4. Перейдите в **Basic Setting > IP Setup > IP Configuration**

5. Настройте IP-интерфейс для VLAN 10 иVLAN 100

VLAN 10:

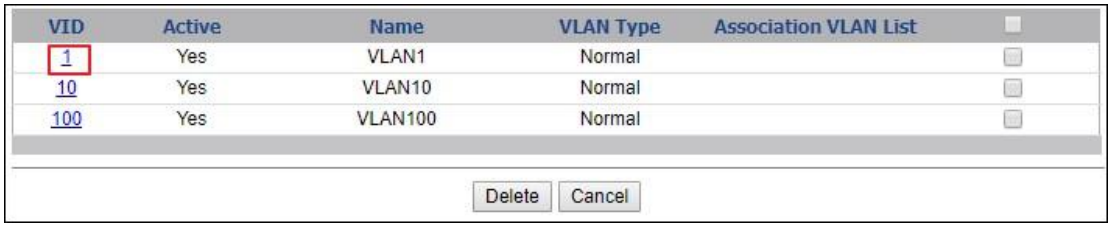


VLAN 100:

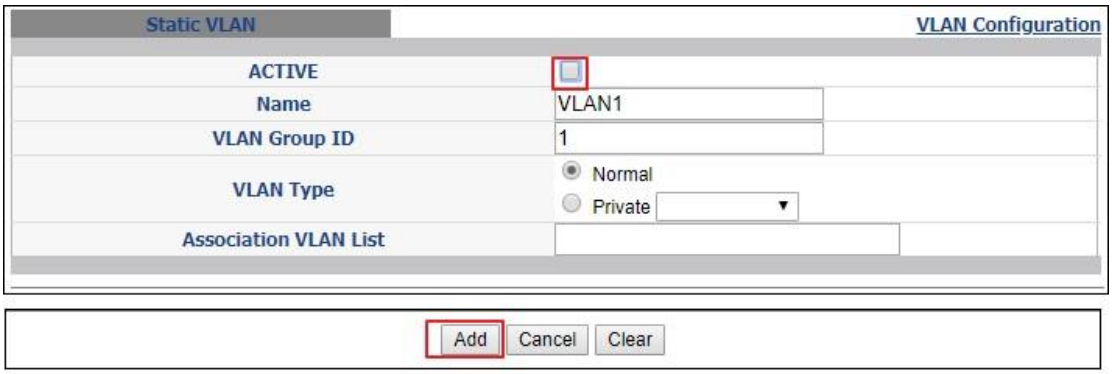


6. Перейдите в **Advanced Application > VLAN > VLAN Configuration> Static VLAN Setup**

7. Введите VLAN 1 чтобы отключить VLAN.

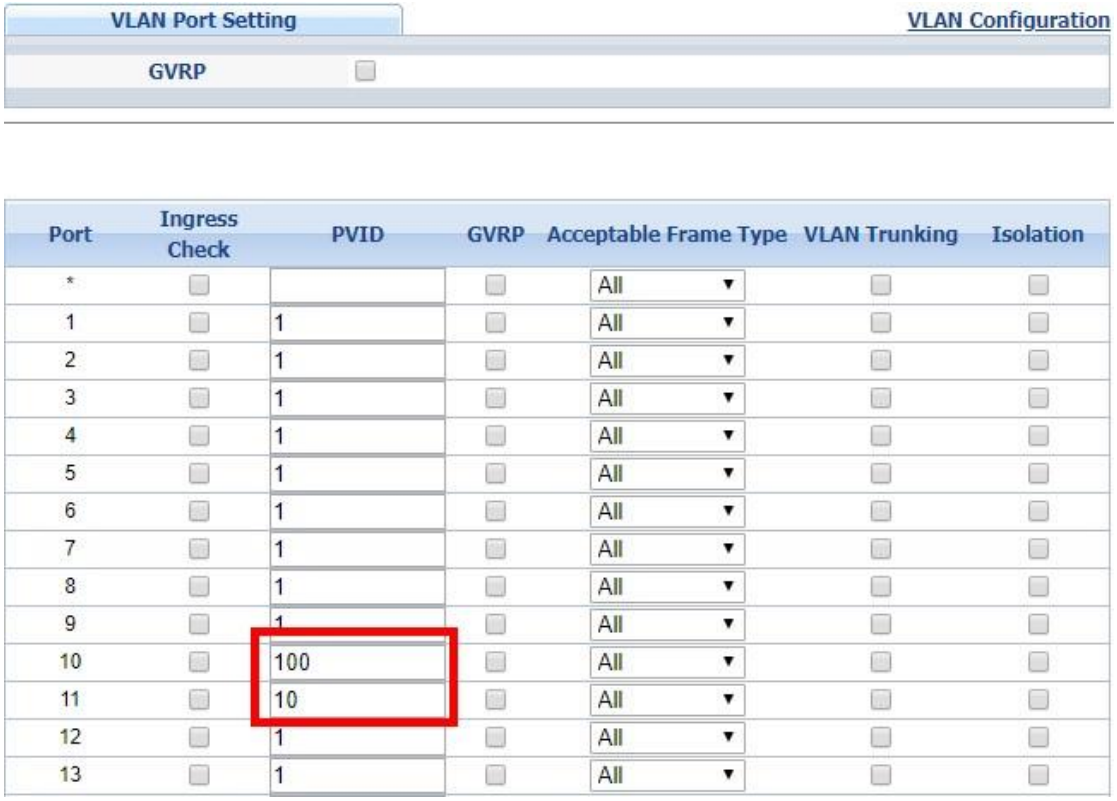


8. Уберите галочку в поле “Active” чтобы включить VLAN 1, затем щелкните Add.



9. Перейдите в **Advanced Application > VLAN > VLAN Configuration> VLAN Port Setting**

10. Настройте PVID на портах port 10 и 11

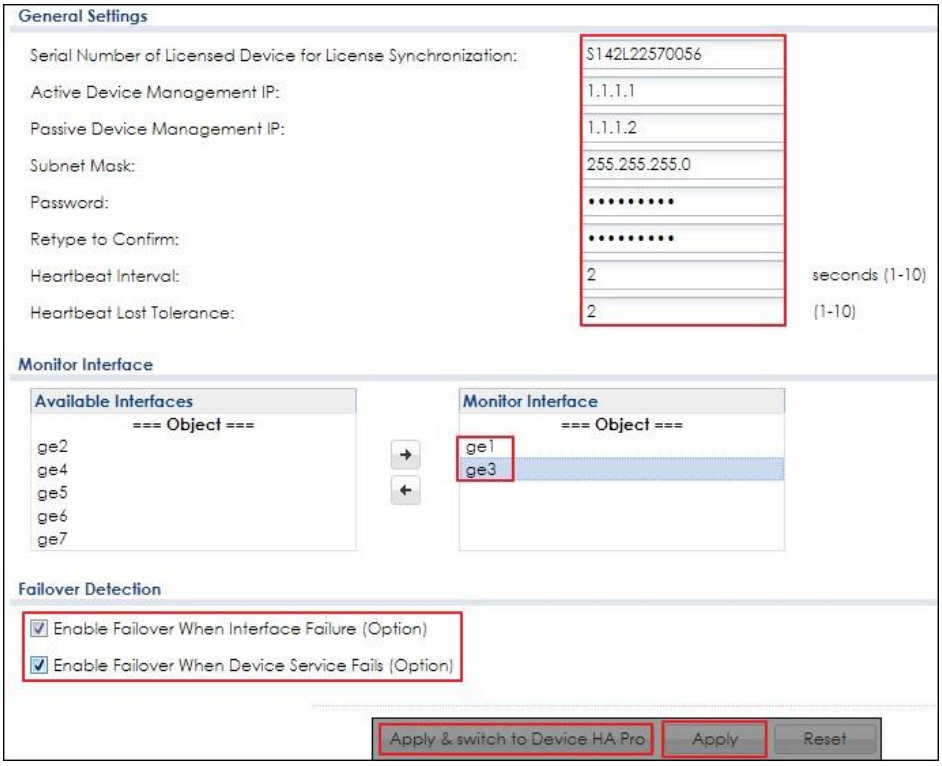


Шлюз Gateway:

1. Откройте Web-интерфейс USG310-1 (Master).

2. Перейдите в **Configuration > Device HA > Device HA Pro**

3. Настройте device HA-pro на USG310-1, Active/Passive device management IP и пароль можно менять в зависимости от ваших настроек. Щелкните “Apply & switch to Device HA pro“, затем щелкните Apply.



4. Перейдите в **Configuration > Device HA > General.**

5. Включите Device HA в General Settings.

6. Откройте web-интерфейс USG310-2 (Backup).

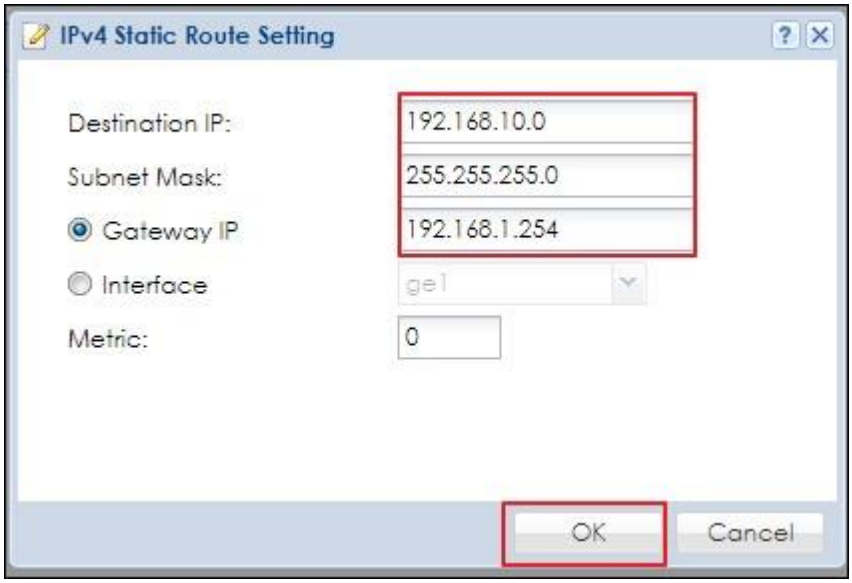
7. Перейдите в **Configuration > Device HA > General.**

8. Включите Device HA в General Settings.

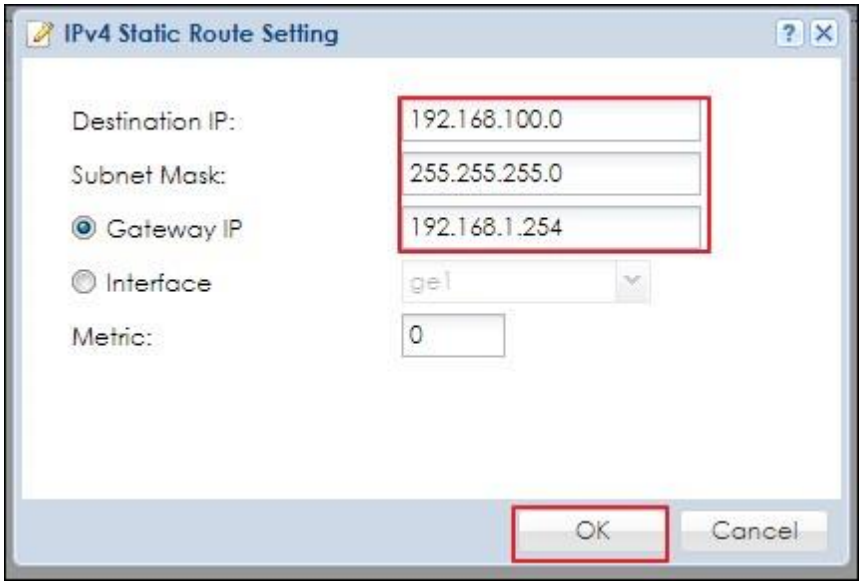
9. Перейдите в **Configuration > Routing > Static Route**

10. Настройте маршрут routing path для получателя destination 192.168.100.0/24 и 192.168.10.0/24.

192.168.10.0/24



192.168.100.0/24



Примечание:

Подключать к USG нужно только когда вы завершите всю настройку конфигурации, иначе настройки не будут полностью синхронизированы.

3.6.2 Проверка

Коммутатор L3 Switch (VRRP):

1. Откройте web-интерфейс Switch-1 (Master).

2. Перейдите в **IP Application > VRRP**, на следующей иллюстрации показано, что VRRP работает, потому что у коммутатора switch-1 есть доступ к IP-интерфейсу шлюза.

VRRP Status — Configuration

Index	Network	VRID	VR Status	Uplink Status
1	192.168.100.1/24	1	Master	Alive
2	192.168.10.1/24	1	Master	Alive
3	192.168.1.251/24	1	Master	Alive

3. Откройте web-интерфейс Switch-2 (Backup).

4. Перейдите в **IP Application > VRRP**,

5. На следующей иллюстрация VRRP успешно работает. В status выводится “Init” потому что USG310-2 все еще в состоянии in backup, поэтому шлюз недоступен.

VRRP Status — Configuration

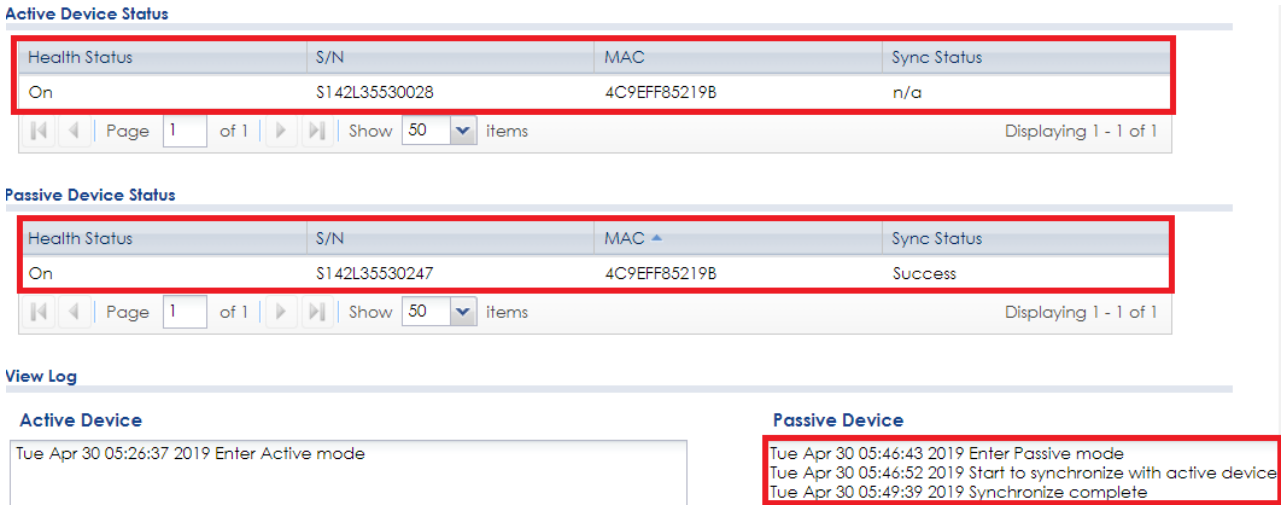
Index	Network	VRID	VR Status	Uplink Status
1	192.168.100.2/24	1	Init	Dead
2	192.168.10.2/24	1	Init	Dead
3	192.168.1.252/24	1	Init	Dead

Примечание: “Init” VR status means that the gateway is not reachable.

Gateway (Device HA-Pro):

1. Откройте web-интерфейс USG310-1 (Master).

2. Перейдите в **Configuration > Device HA**, следующая иллюстрация относится к успешной настройке Device HA Pro.



Примечание:

1. Чтобы USG пересылал трафик обратно на хост он должен быть настроен на “Static route”.
2. Для всех хостов (ПК) шллюз по умолчанию default gateway должен быть настроен с VRRP primary

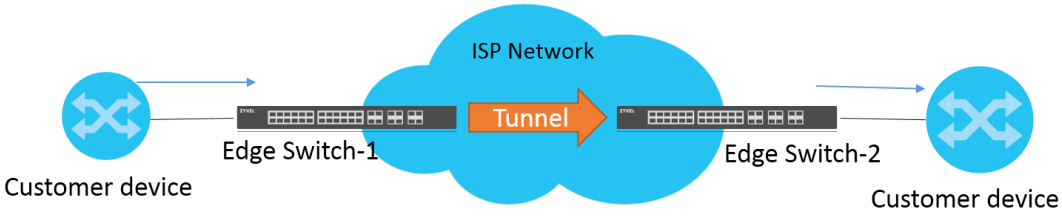
3.6.3 Почему это не работает?

1. У коммутатора в VRRP uplink gateway должен стоять IP-адрес USG.
2. Нужно задать VLAN member для коммутатора downlink switch.

3.7 Как настроить коммутатор чтобы пакеты шли по туннелю Tunnel Layer 2 Protocol через сеть провайдера

Коммутаторы Zyxel поддерживают технологию Layer-2 Protocol Tunneling (L2PT), позволяющую пакетам на границе сети передавать пакеты через сеть провайдера по туннелю tunnel layer-2 protocol. Это может понадобиться если у заказчика коммутаторы установлены на разных площадках, и передача данных между ним идет через сеть провайдера.

В этом случае заказчик может внедрить в своих сетях независимое решение layer 2 protocol, например, единый независимым домен spanning tree domain для своих сетей в сети провайдера.

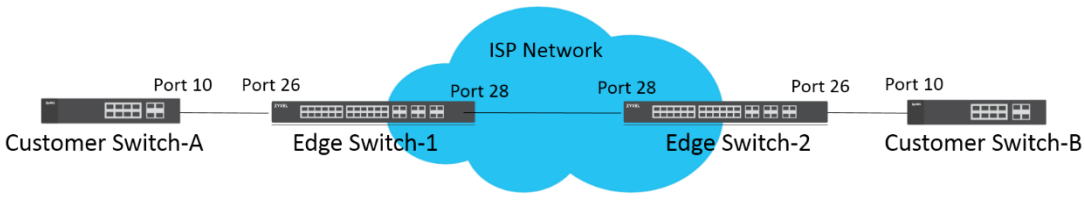


Когда коммутатор границы сети Edge switch-1 получает пакеты Layer-2 protocol, он их инкапсулирует и вместо MAC-адреса получателя записывает определенный MAC-адрес. Все коммутаторы внутри сети провайдера обрабатывают эти инкапсулированные пакеты как пакеты с данными и пересылают их на другую сторону. Когда коммутатор границы сети Edge switch-2 получает эти инкапсулированные пакеты, то он извлекает их восстанавливает их первоначальный MAC-адрес получателя и затем пересылает их коммутатору получателю.

Каждый порт коммутатора границы сети edge switch может работать в двух режимах:

- **Access** Port: в портах ingress коммутатор edge провайдера, подключенных к коммутатору заказчика, входящие пакеты layer 2 protocol инкапсулируются и пересылаются портам туннеля.
- **Tunnel** Port: в портах egress коммутатор edge провайдера, подключенных к коммутатору заказчика, входящие пакеты layer 2 protocol извлекаются и пересылаются на порт access port.

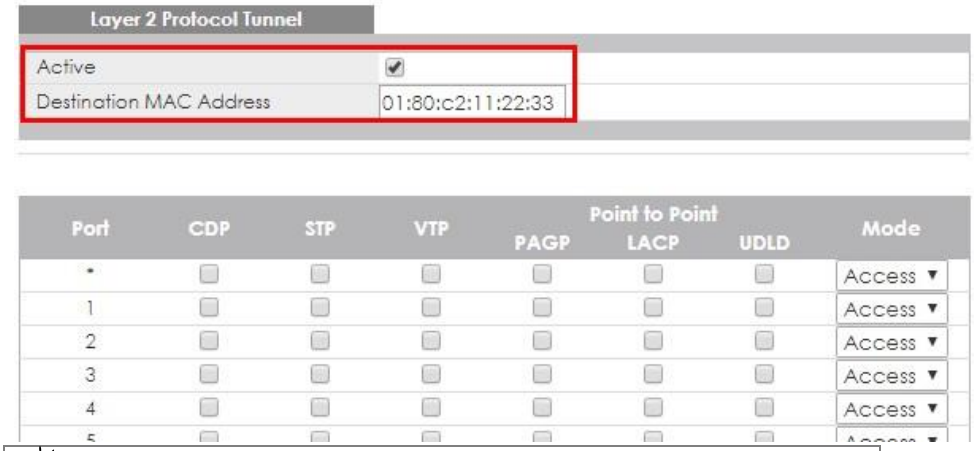
На следующем примере показано, как настроить коммутатор на пересылку пакетов по туннелю STP через сеть провайдера.



Примечание:
В этом примере два XGS4600 – это коммутаторы edge, а два GS2210 – коммутаторы заказчика.

3.7.1 Настройка конфигурации коммутатора Edge

1 Настройте **Edge Switch-1**: Откройте web-интерфейс. Перейдите в **Advanced Application > Layer 2 Protocol Tunneling**. Поставьте галочку в “**Active**” и задайте “**Destination MAC Address**”.



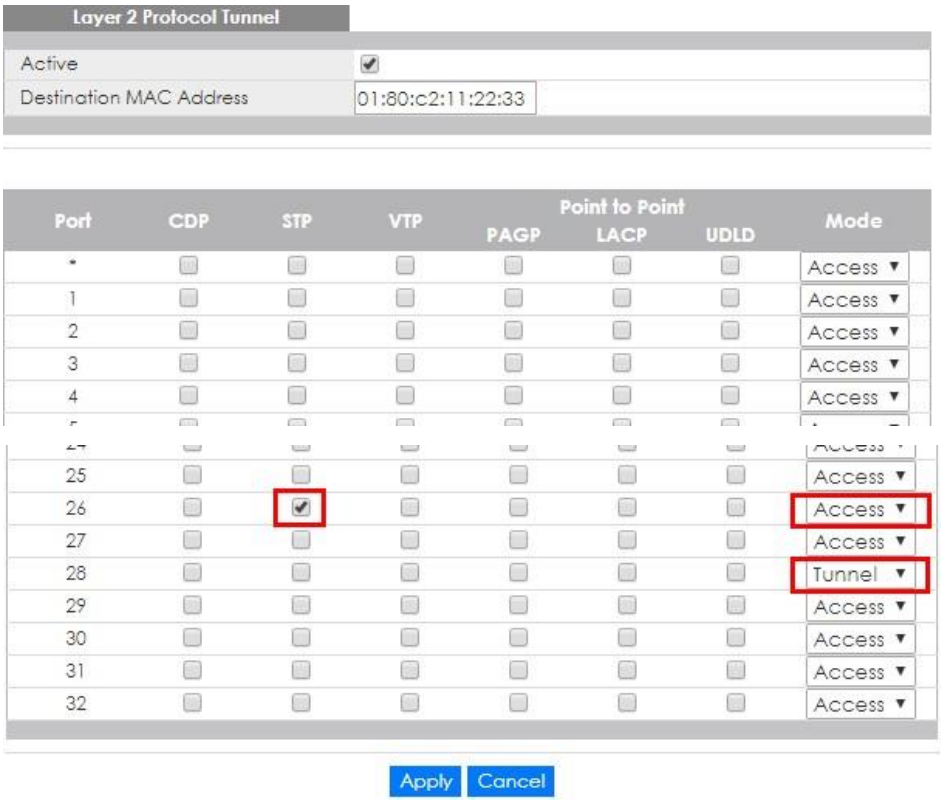
Примечание:
Destination MAC Address может быть MAC-адресом unicast или multicast.

1. Если **unicast** MAC-адрес: убедитесь, что такого MAC-адреса **НЕТ** в таблице MAC-адресов коммутаторов сети провайдера.
2. Если **multicast** MAC-адрес: убедитесь, что такого MAC-адреса **НЕ** используется для определенного протокола, например, STP и VTP.

Примечание:
Все коммутаторы edge сети провайдера должны использовать **один и тот же** MAC-адрес для инкапсуляции.

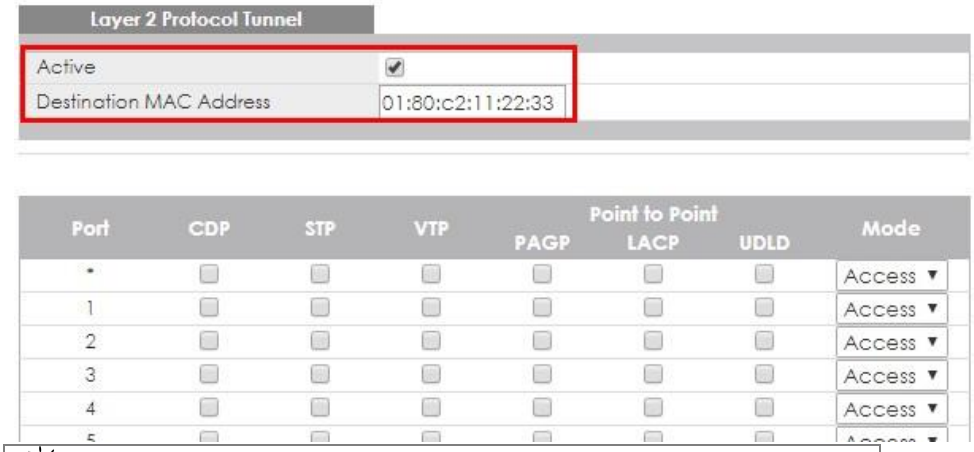
2 Настройте **Edge Switch-1**: На той же странице поставьте галочку в “**STP**” и настройте “**Mode**” на “**Access**” для порта 26, который подключен к коммутатору заказчика.

3 Настройте **Edge Switch-1**: На той же странице настройте “**Mode**” на “**Tunnel**” для порта 28, который подключен к другому коммутатору edge в сети провайдера, и щелкните “**Apply**”.



Примечание:
Сервисы L2PT нужно активировать для поддерживаемых протоколов только для портов access port.

4 Настройте **Edge Switch-2**: Откройте web-интерфейс. Перейдите в **Advanced Application > Layer 2 Protocol Tunneling**. Активируйте Layer 2 Protocol Tunnel и настройте “Destination MAC Address”.



Примечание:

Destination MAC Address может быть MAC-адресом unicast или multicast.

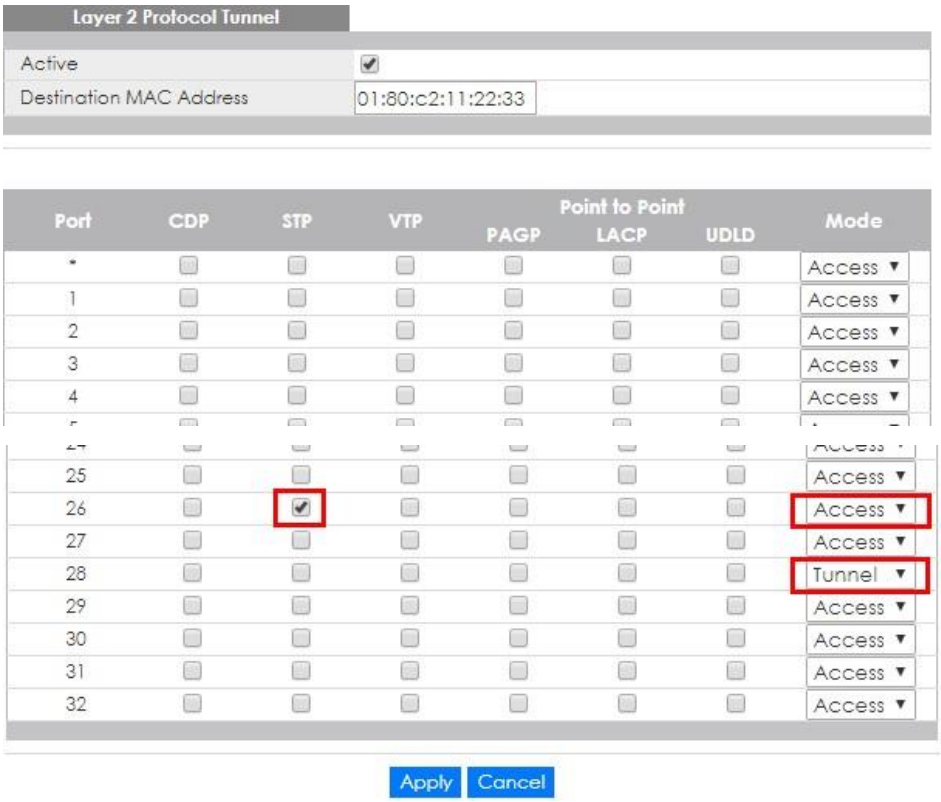
1. Если **unicast** MAC-адрес: убедитесь, что такого MAC-адреса **НЕТ** в таблице MAC-адресов коммутаторов сети провайдера.
2. Если **multicast** MAC-адрес: убедитесь, что такого MAC-адреса **НЕ** используется для определенного протокола, например, STP и VTP.

Примечание:

Все коммутаторы edge сети провайдера должны использовать **один и тот же** MAC-адрес для инкапсуляции.

5 Setup **Edge Switch-2**: On the same page. Activate STP and set mode as “Access” on port 26 which connects to the customer switch.

6 Настройте **Edge Switch-2**: На той же странице настройте “**Mode**” на “**Tunnel**” для порта 28, который подключен к другому коммутатору edge в сети провайдера, и щелкните “Apply”.



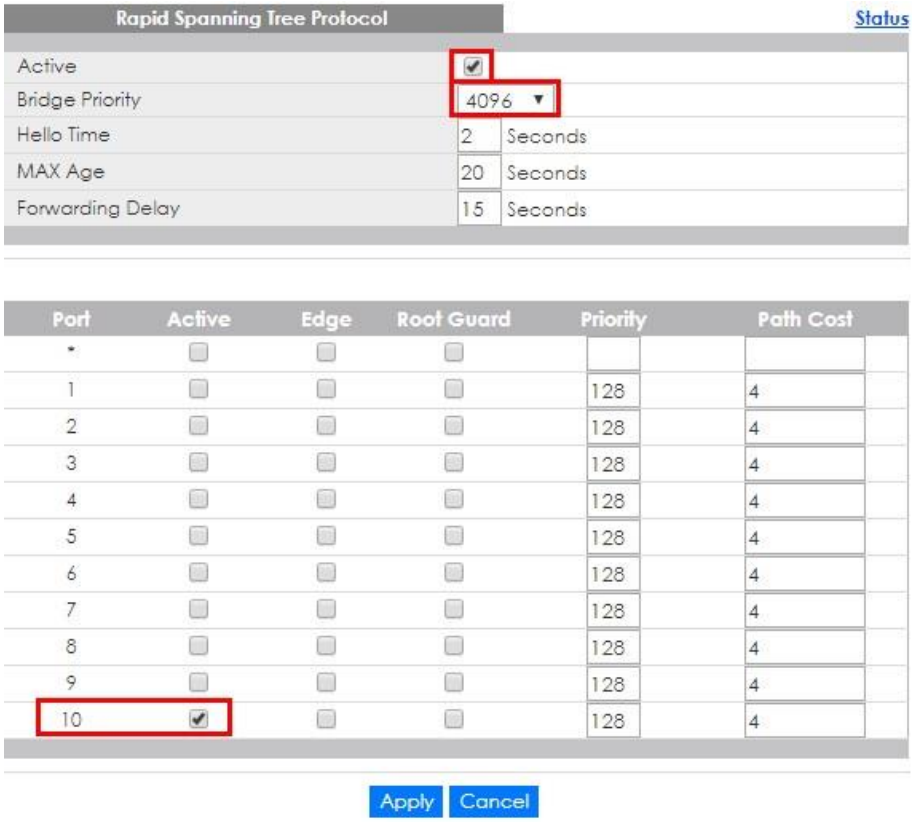
Примечание:
Сервисы L2PT нужно активировать для поддерживаемых протоколов только для портов access port.

3.7.2 Настройка конфигурации коммутатора заказчика

1 Настройте **Customer Switch-A:** Откройте Web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Убедитесь, что в Spanning Tree Configuration выбрано **Rapid Spanning Tree**. Если нет, выберите и щелкните “Apply”.

Примечание:
Необязательно включать STP на коммутаторах потому они только перенаправляют пакеты STP по туннелю.

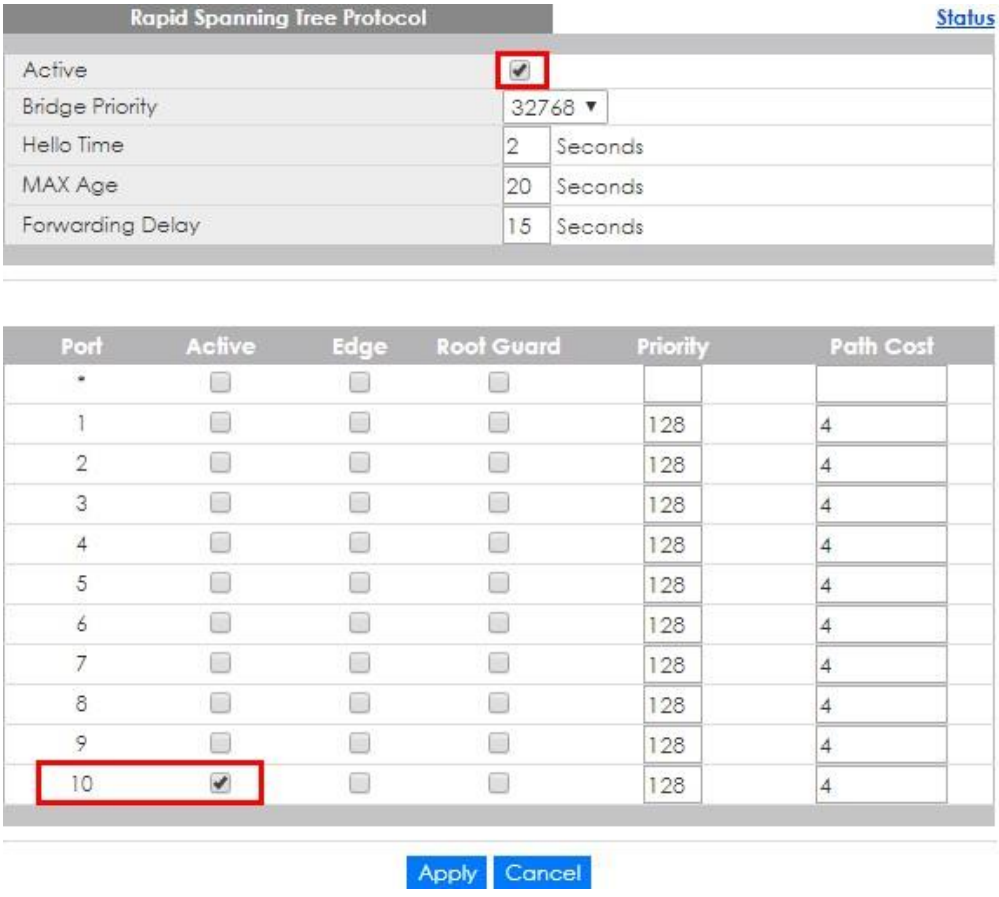
2 Настройте **Customer Switch-A**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > RSTP**. Поставьте галочку в “**Active**” и настройте Bridge Priority = **4096.** Активируйте порт port **10** и щелкните “**Apply**”.



3 Настройте **Customer Switch-B:** Откройте Web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > Configuration**. Убедитесь, что Spanning Tree Configuration - это **Rapid Spanning Tree**. Если нет, выберите это и щелкните “Apply”.

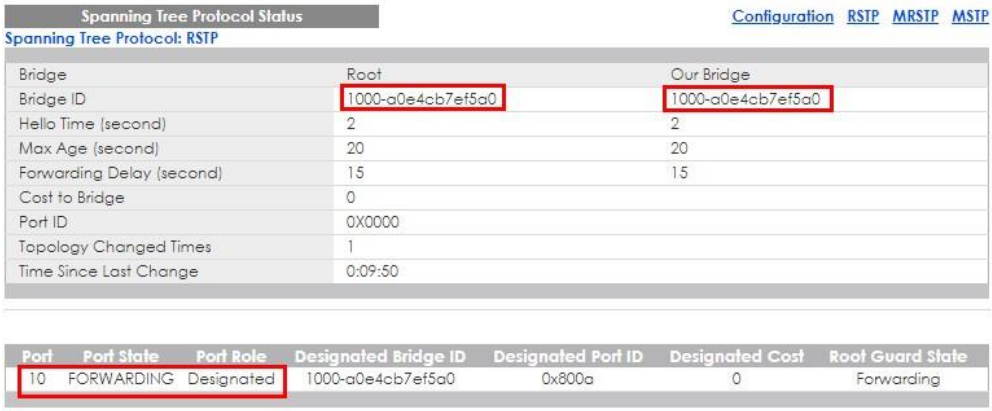
4 Настройка **Customer Switch-B**: Откройте web-интерфейс. Перейдите в **Menu > Advanced Application > Spanning Tree Protocol > RSTP**.

Поставьте галочку в “**Active**”. Активируйте порт port **10** и щелкните “**Apply**”.



3.7.3 Проверка результатов настройки

1 Проверьте состояние **Customer Switch-A**: Перейдите в **Menu > Advanced Application > Spanning Tree Protocol**. Root Bridge ID и Our Bridge ID должны совпадать. Это означает, что Customer Switch-A – это Root Bridge. Port 10 должен быть в состоянии **FORWARDING**, а его Port Role должна быть **Designated Ports**.



Spanning Tree Protocol Status

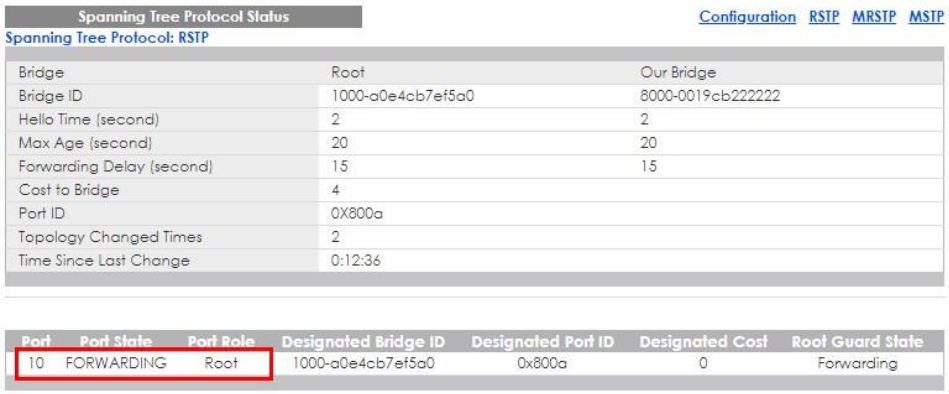
Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-a0e4cb7ef5a0	1000-a0e4cb7ef5a0
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times	1	
Time Since Last Change	0:09:50	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Designated	1000-a0e4cb7ef5a0	0x800a	0	Forwarding

2 Проверьте состояние **Customer Switch-B**: Перейдите в **Menu > Advanced Application > Spanning Tree Protocol.** Проверьте состояние порта в Customer Switch-A. Port 10 должен быть **Root Port** в состоянии **FORWARDING**.



Spanning Tree Protocol Status

Configuration RSTP MRSTP MSTP

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	1000-a0e4cb7ef5a0	8000-0019cb222222
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	4	
Port ID	0X800a	
Topology Changed Times	2	
Time Since Last Change	0:12:36	

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
10	FORWARDING	Root	1000-a0e4cb7ef5a0	0x800a	0	Forwarding

3.7.4 Почему это не работает?

1 Убедитесь, что вы задали один и тот же destination MAC address для Layer-2 Protocol Tunneling на всех коммутаторах edge. В

противном случае инкапсулированные пакеты не будут распознаны при их пересылке между коммутаторами edge.

Развертывание сети IPTV

4.1 Введение в IGMP

Для проектирования сети IPTV важно знать 3 важные концепции Zyxel IGMP (Internet Group Management Protocol) и IGMP Snooping.

4.1.1 Что такое General Queries и Group Specific Queries?

General Query: querier посылает сообщения query клиентам multicast чтобы выяснить, из каких групп multicast сейчас есть в сети активные члены.

Group Specific Query: Когда клиент покидает группу multicast и посылает сообщение leave group, то querier посылает это сообщение query чтобы выяснить, есть ли этой группы другие активные члены, подключенные к порту downlink.

4.1.2 Что такое IGMP Snooping Querier Mode?

Есть 3 режима Querier Mode: Auto, Fixed и Edge.

Fixed: Коммутатор всегда использует этот порт как порт IGMP query port. Этот режим нужно выбрать при подключении к порту сервера IGMP multicast server.

Edge: Коммутатор не может использовать этот порт как IGMP query port и у него не будет записи, о том, что к этому порту подключен маршрутизатор IGMP router. Коммутатор не пересылает на этот порт IGMP join или пакеты leave packet.

Auto: Порт работает как Fixed когда получает запрос IGMP query, а если такие запросы не приходят в течение заданного времени, то работает как порт Edge.

4.1.3 В чем разница между IGMP Snooping fast/normal/immediate leave?

Fast leave:

В режиме fast leave коммутатор посылает сообщение IGMP Group-Specific Query (GSQ) сразу получения сообщения IGMP leave message от хоста, подключенного к

этому порту. Это определяет, должны ли другие подключенные к этом порту хосты оставаться в определенной группе multicast. Это ускоряет процесс leave.

Normal leave:

В режиме normal leave mode коммутатор при получении сообщения IGMP leave message от хоста, подключенного к порту, перенаправляет это сообщение маршрутизатору multicast router. Маршрутизатор multicast router посылает сообщение IGMP Group-Specific Query (GSQ) чтобы определить, должны ли другие подключенные к этом порту хосты оставаться в определенной группе multicast. Коммутатор пересылает сообщение query message всем хостам, подключенным к порту, и ждет отчетов IGMP от хостов чтобы обновить таблицу forwarding table.

Immediate leave:

Если выбрать эту опцию, то коммутатор уберет этот порт из дерева multicast tree как только порт получит сообщение IGMP leave message. Эту опцию следует использовать только если к этому порту подключен только один хост.

4.2 Как настроить IGMP routing для клиентов multicast в разных LAN

В этом примере показано, как настроить IGMP routing в коммутаторе Zyxel Layer 3. Эта настройка требуется если клиенты multicast и сервер streaming находятся в разных LAN или VLAN.

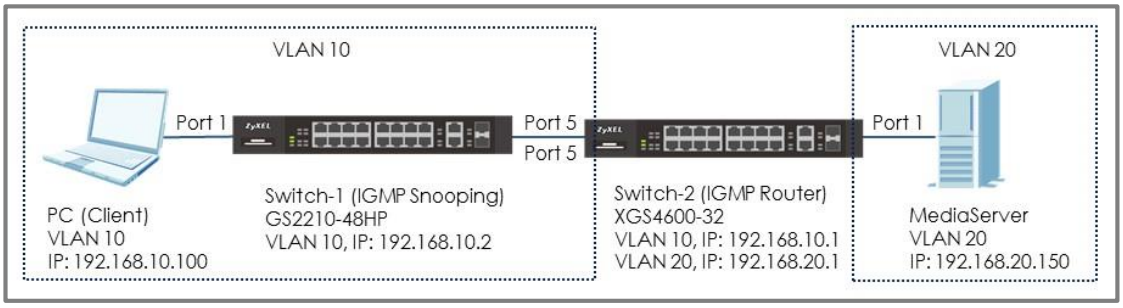


Иллюстрация 17 Настройка IGMP routing для клиентов multicast в разных VLAN

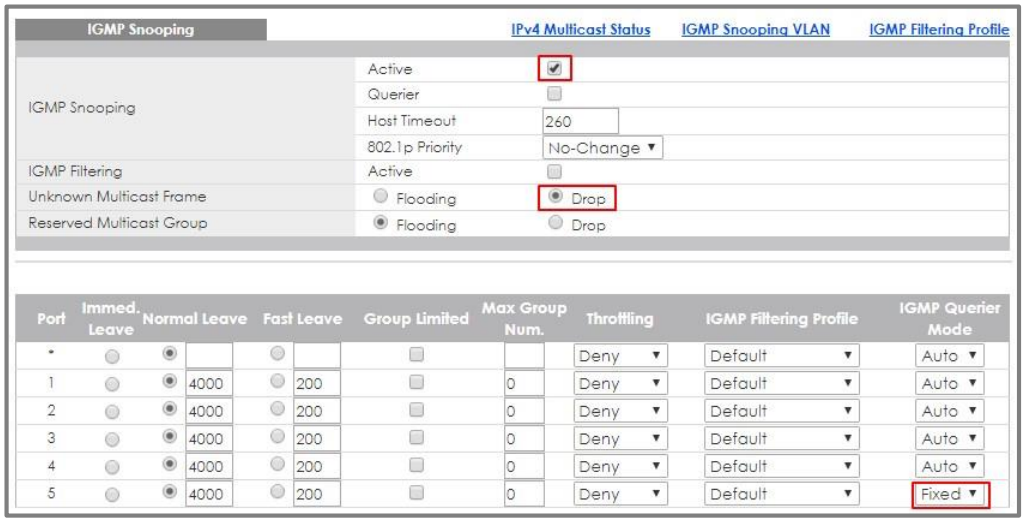
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

4.2.1 Настройка конфигурации коммутатора Switch-1

1 Настройте VLAN 10 на Switch-1. (См. **2.1 Как настроить коммутатор для изоляции трафика между разными отделами**).

2 Настройте IGMP Snooping: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping**. Поставьте галочку в поле the “Active” и выберите в Unknown

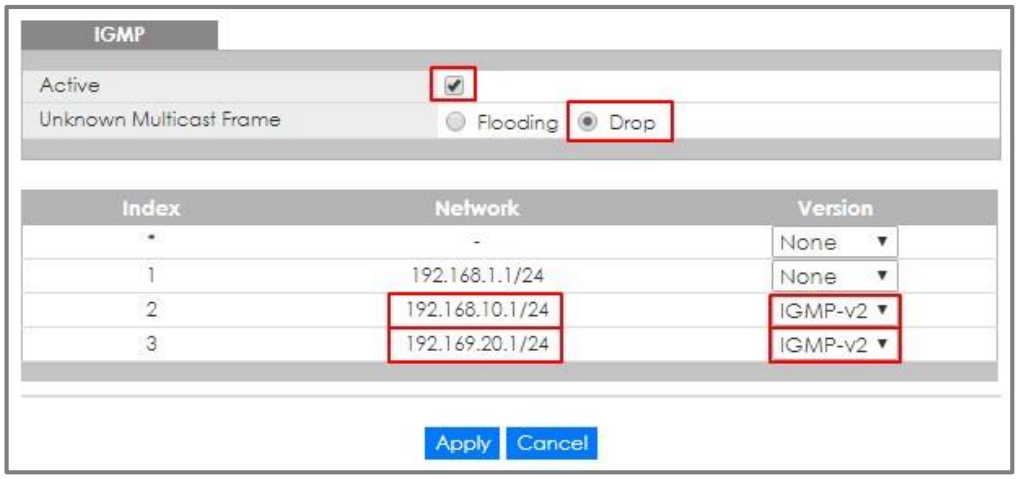
Multicast Frame **Drop**. Выберите порт port 5 как **Fixed**. Щелкните “Apply”.



4.2.2 Настройка конфигурации коммутатора Switch-2

1. Настройте VLAN 10 и VLAN 20 на Switch-2. (См. **2.1 Как настроить коммутатор для изоляции трафика между разными отделами**).
2. Настройте IP-адрес на коммутаторе для VLAN 10 и VLAN 20 как показано на иллюстрации. См. **1.1 Как изменить используемый для управления IP-адрес коммутатора чтобы получить доступ к нему, а не к другому коммутатору**.

3 Настройте IGMP Routing: Откройте web-интерфейс и перейдите в **Menu > IP Application > IGMP**. Поставьте галочку в поле “Active” и выберите VLAN 10 и VLAN 20 как IGMP-v2. Выберите “Unknown Multicast Frame” как “**Drop**”. Щелкните “Apply”.

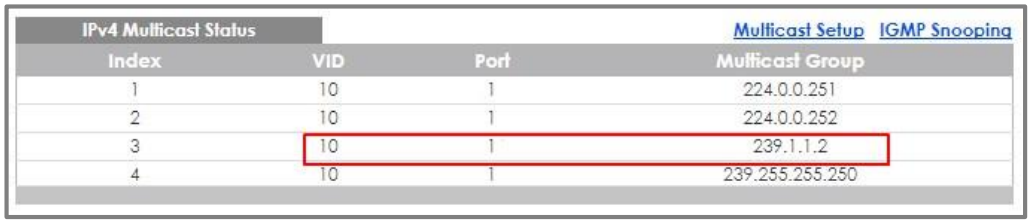


4.2.3 Проверка результатов

1 Запустите поток на сервере MediaServer используя Multicast IP address 239.1.1.2.

2 С PC отправьте сообщение IGMP join message для 239.1.1.2.

3 Перейдите в **Menu > Advanced Application > Multicast > IPv4 Multicast**. PC, подключенный к порту port 10, вступит в группу Multicast Group239.1.1.2.



4.2.4 Почему это не работает

1 Для правильной маршрутизации потока IGMP VLAN коммутатора Switch-2 (IGMP Router) должна содержать как MediaServer (VLAN 20), так и PC (Client) (VLAN 10). Если клиент не получает поток, то проверьте конфигурацию VLAN.

4.3 Как настроить IGMP Snooping для клиентов multicast в одной LAN

В этом примере показано, как настроить IGMP Snooping когда клиенты multicast и серверы steaming находятся в одной VLAN. Когда MediaServer ведет multicast-трансляцию потока, то коммутатор с помощью IGMP snooping может узнать о группах multicast без ручного конфигурирования каждого коммутатора. Этот механизм предотвращает передачи с коммутатора потоков multicast через те порты, где нет членов групп multicast.

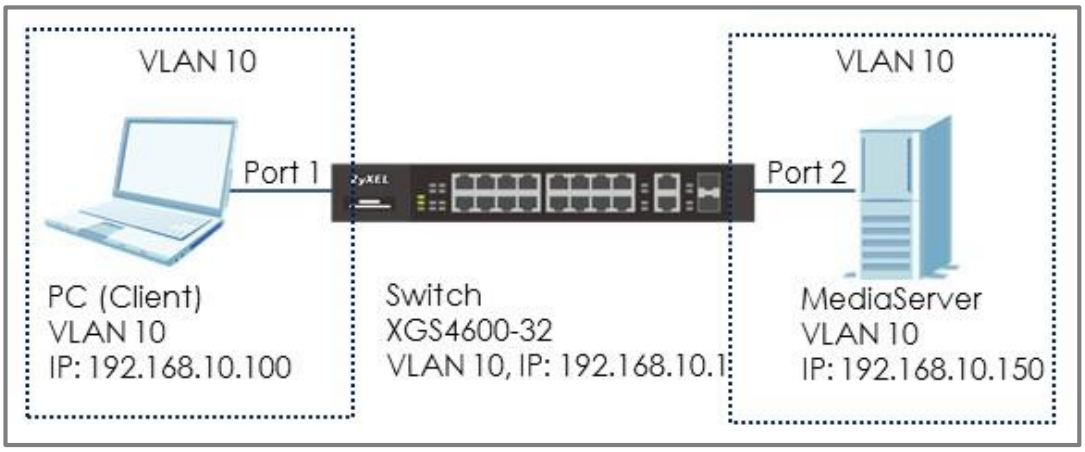


Иллюстрация 18 Настройка IGMP Snooping для клиентов multicast в одной LAN

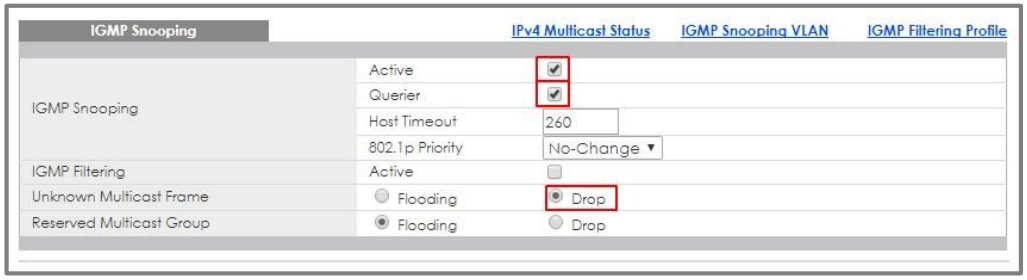
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

4.3.1 Настройка конфигурации коммутатора

1 Настройте VLAN 10 на коммутаторе. (См. **2.1 Как настроить коммутатор для изоляции трафика между разными отделами**).

2 Настройте IGMP Snooping: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > Multicast > IPv4 Multicast > IGMP**

Snooping. Поставьте галочку в поле “Active” и выберите Unknown Multicast Frame as **Drop**. Поставьте галочку в **Querier**. Щелкните “Apply”.

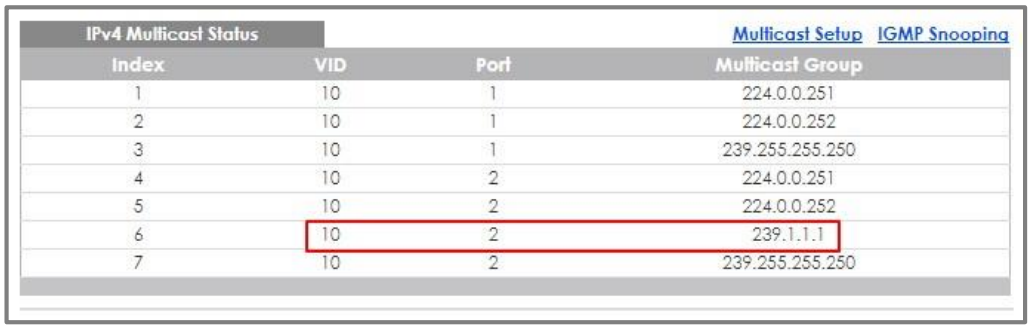


4.3.2 Проверка результатов

1 Запустите поток на MediaServer, используя using Multicast IP address 239.1.1.1.

2 С PC отправьте сообщение IGMP join message на 239.1.1.1.

3 Перейдите в **Menu > Advanced Application > Multicast > IPv4 Multicast**. PC, подключенный к порту port 2, вступил в группу Multicast Group- 239.1.1.1.



Сетевая безопасность

5.1 Как настроить безопасность порта на ограничение числа подключенных к порту устройств

В этом примере показано, как настроить безопасность порта на ограничение числа подключенных к порту устройств. На практике с помощью этой настройки можно ограничить число подключенных к серверу пользователей.

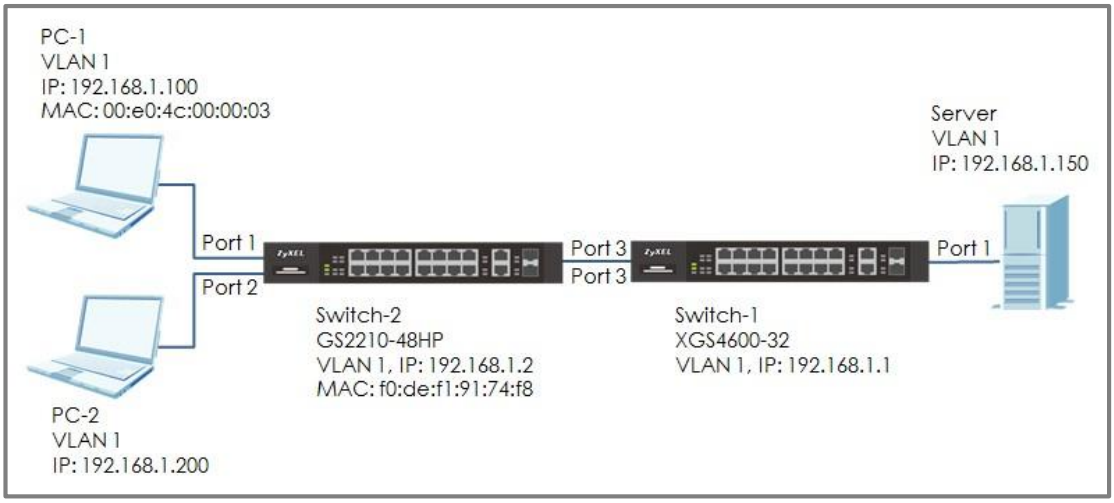
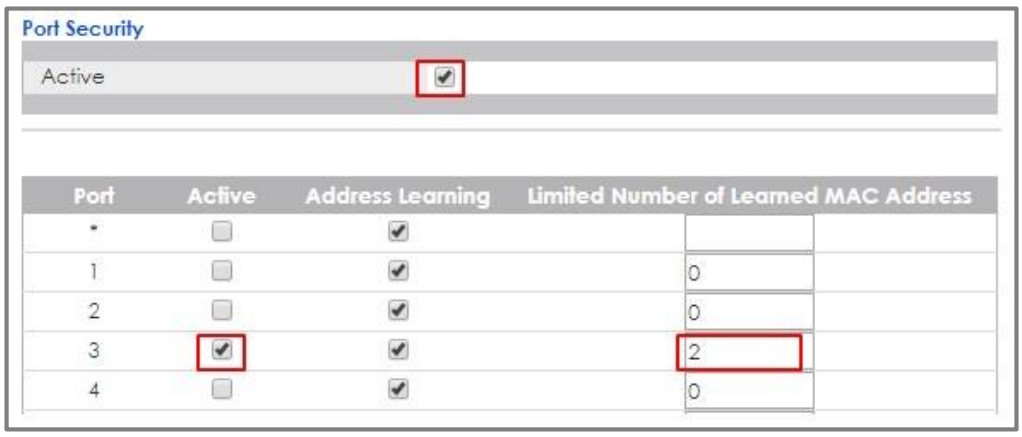


Иллюстрация 19 Настройка безопасности портов для ограничения числа подключенных устройств

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

5.1.1 Настройка конфигурации Switch-1

1 Откройте Web-интерфейс и перейдите в **Menu > Advanced Application > Port Security**. Поставьте галочку напротив порта port 3 и задайте “Limited Number of Learned MAC Address” в 2.



Примечание:
По умолчанию коммутатор Zyxel посылает пакеты Link Layer Discovery Protocol (LLDP) с заданной периодичностью. Если коммутатор Switch-2 не поддерживает LLDP или у него отключена поддержка LLDP, то значение Limited Number of Learned MAC Address будет установлено равным 1, в противном случае 2.

5.1.2 Проверка результатов Result

1 От PC-1 до сервера проходят ping.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.150: bytes=32 time=766ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128
Reply from 192.168.1.150: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 766ms, Average = 191ms
```

2 Подсоедините PC-2 к порту port 2.

3 От PC-2 не доходят ping до сервера.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

4 Откройте web-интерфейс Switch-1. Перейдите в **Menu > Management > MAC Table > Search**. В таблице MAC Address Table должны быть MAC-адреса PC-1 (и Switch-2), но отсутствовать MAC-адрес PC-2.

Index	MAC Address	VID	Port	Type
1	00:23:54:2e:98:b9	1	1	Dynamic
2	00:e0:4c:00:00:03	1	3	Dynamic
3	42:73:74:20:55:56	1	CPU	Static
4	f0:de:f1:91:74:f8	1	3	Dynamic

5.1.3 Почему это не работает

1 MAC-адрес коммутатора Switch-2 должен быть в таблице MAC address table коммутатора Switch-1, поэтому нужно учитывать MAC-адрес коммутатора Switch-2 при задании параметра Limited Number of Learned MAC Address.

5.2 Как сконфигурировать MAC filter для блокировки ненужного трафика

В этом примере объясняется, как настроить фильтр MAC-адресов для блокировки нежелательного трафика. Коммутатор Switch-1 блокирует пакеты, которые приходят от определенного устройства или идут на определенное устройство.

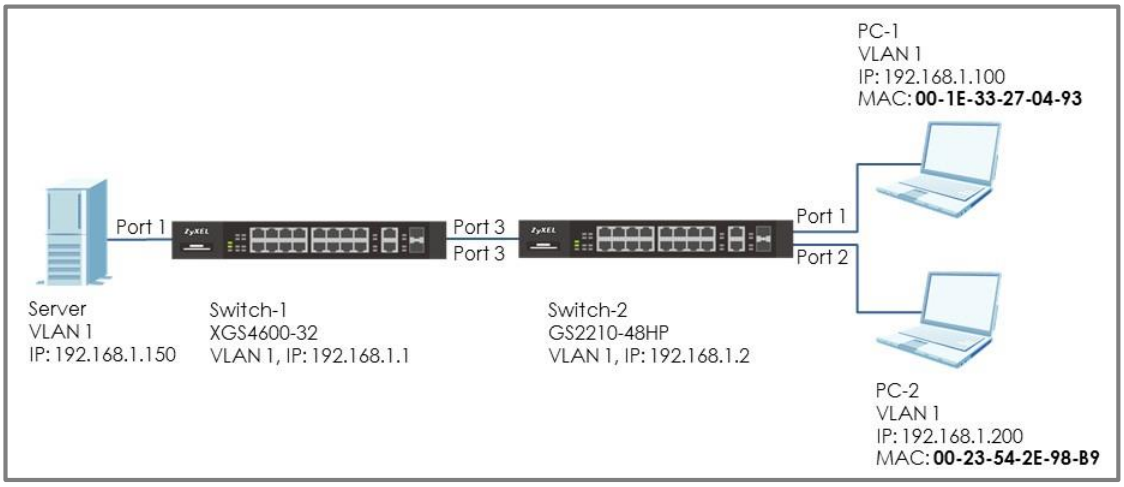
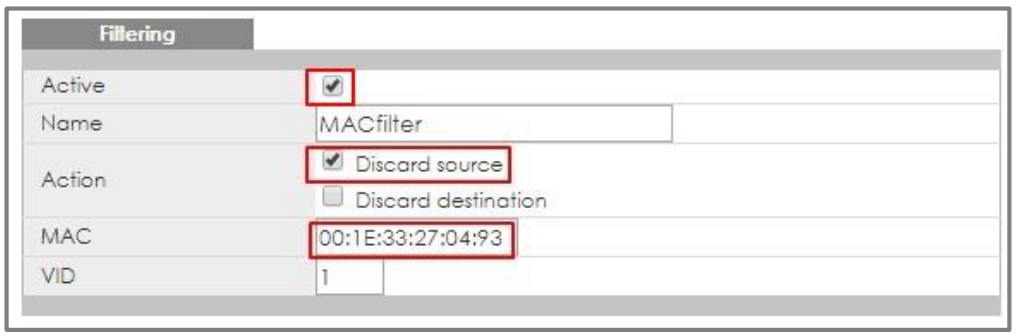


Иллюстрация 20 Настройка фильтра MAC-адресов для блокировки нежелательного трафика

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

5.2.1 Настройка конфигурации коммутатора Switch-1

1 Откройте Web-интерфейс и перейдите в **Menu > Advanced Application > Filtering**. Поставьте галочку в поле “Active” и задайте имя фильтра Name. Выберите в поле Action “**Discard source**”. Введите MAC-адрес, который нужно заблокировать и VID. Щелкните “Add”.



Примечание:

Используйте **Discard source** чтобы блокировать трафик **от** устройства с заданным MAC-адресом.

Используйте **Discard destination** чтобы блокировать трафик, который идет **к** устройству с заданным MAC-адресом.

5.2.2 Проверка результатов

1 Ping от PC-1 (его MAC-адрес 00:1E:33:27:04:93) не доходят до сервера Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.
Reply from 192.168.1.100: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

2 От PC-2 ping доходят до сервера Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

5.2.3 Почему это не работает

1 Заданный на Switch-1 MAC-адрес для блокировки трафика должен быть такой же, как MAC-адрес у PC-1.

5.3 Как настроить коммутатор для блокировки сканирования IP-адресов

В этом примере с помощью **Anti-ARP Scan** блокируются попытки сканировать IP-адреса устройств в локальной сети. ARP Scanning – это механизм сканирования, при котором за короткое время направляется много запросов ARP request для переполнения всего домена broadcast domain.

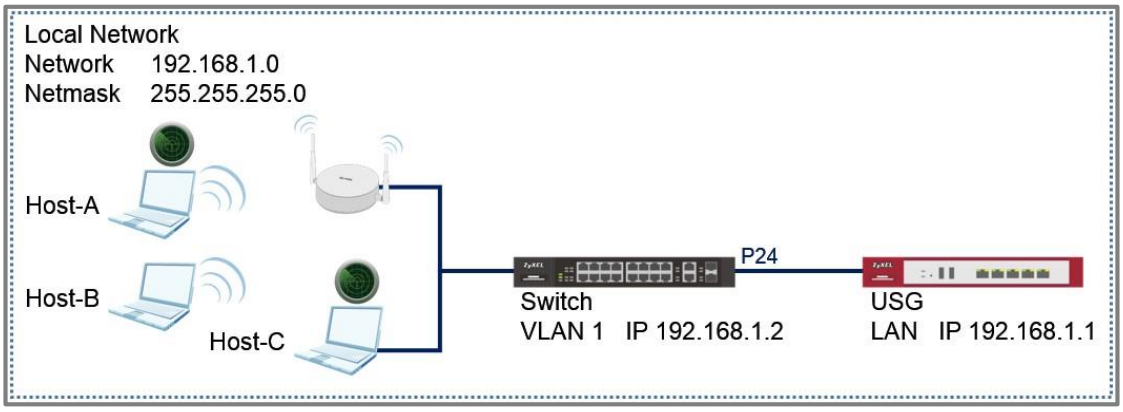


Иллюстрация 21 IP Scanning from Wired and Wireless Devices

Примечание:

Все сетевые IP-адреса и маски подсети относятся только к этому примеру.

В этом примере точка доступа Access Point использует значения по умолчанию Radio и SSID Profile.

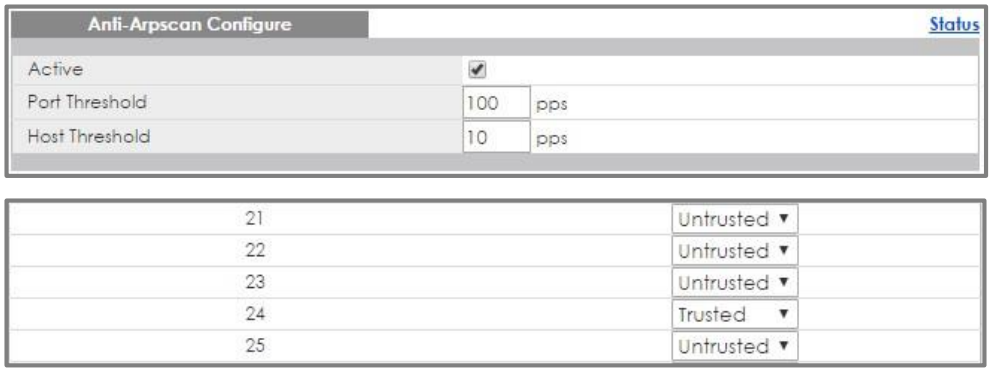
“Zenmap” – это утилита для сканирования IP-адресов.

Интерфейс пользователя (UI) в этом примере относится к коммутатору серии XGS4600.

5.3.1 Настройка конфигурации коммутатора

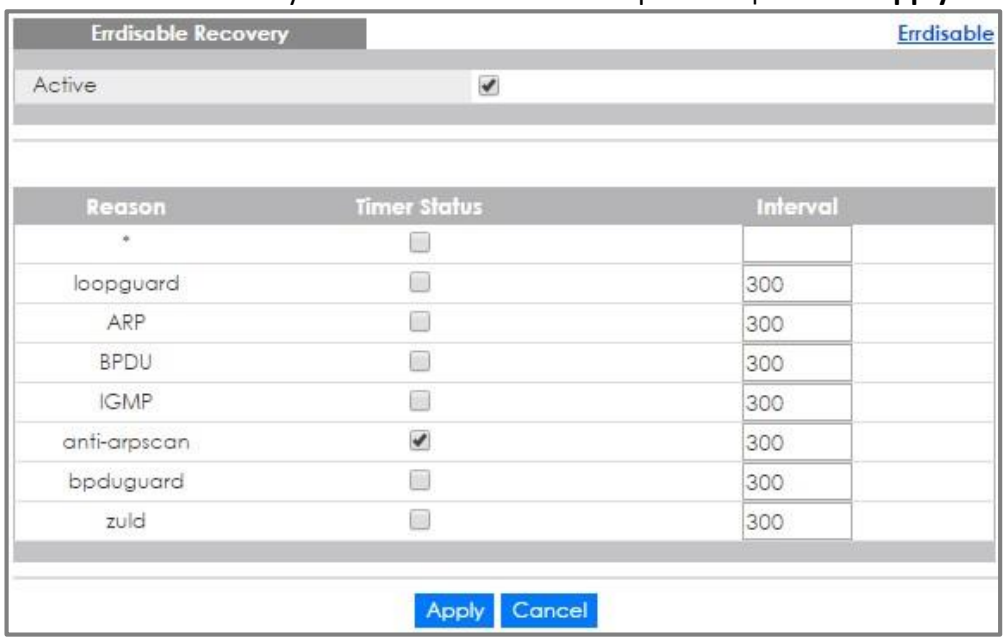
1 Откройте Web-интерфейс коммутатора.

2 Перейдите в **Advance Application > Anti-Arpscan > Configure**. Поставьте галочку в ACTIVE и задайте для порта uplink port (port 24) состояние “Trusted”. Щелкните **Apply**.



-Optional (опция)-

3 Перейдите в **Advance Application > Errdisable > Errdisable Recovery**. Поставьте галочку в ACTIVE и в поле anti-arpscan. Щелкните **Apply**.

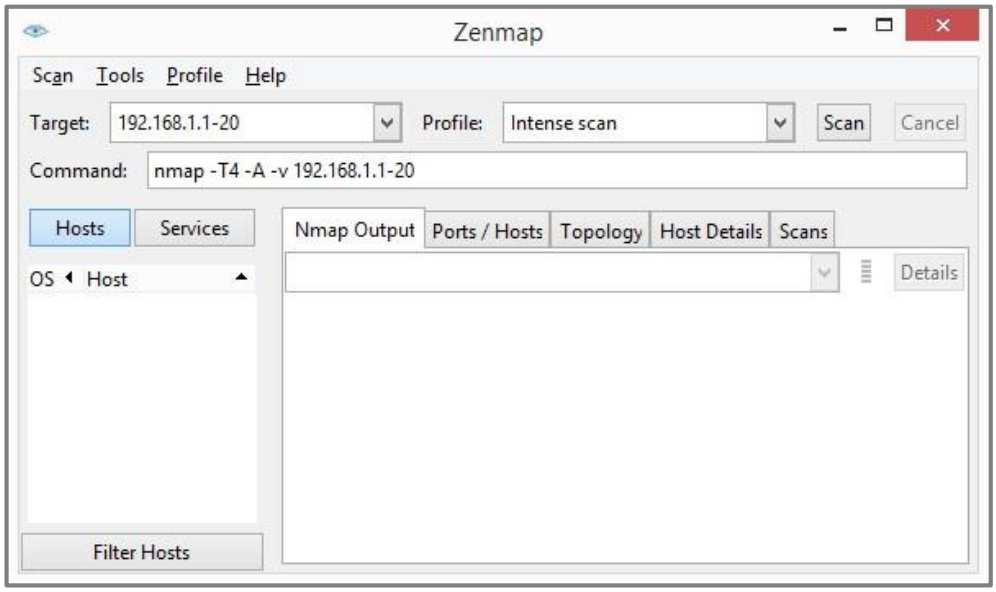


5.3.2 Проверка результатов

1 Загрузите и инсталлируйте пакет IP Scanning на Host-A и Host-C.

2 Соедините Host-A и Host-B через беспроводную точку доступа.

3 Запустите на Host-A сканирование IP-адресов от 192.168.1.1 до 192.168.1.20.



4 У Host-A теперь не будет доступа к USG.

```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.1.30: Destination host unreachable.
Reply from 192.168.1.30: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

5 Откройте Web-интерфейс коммутатора. Перейдите в **Advance Application > Anti-Arpscan > Host Status**. Для Host-A состояние должно быть “Err-Disable”.

Filtered host

Index	Host IP	MAC	VLAN	Port	State
1	192.168.1.30	74:d4:35:f4:6b:4e	1	1	Err-Disable

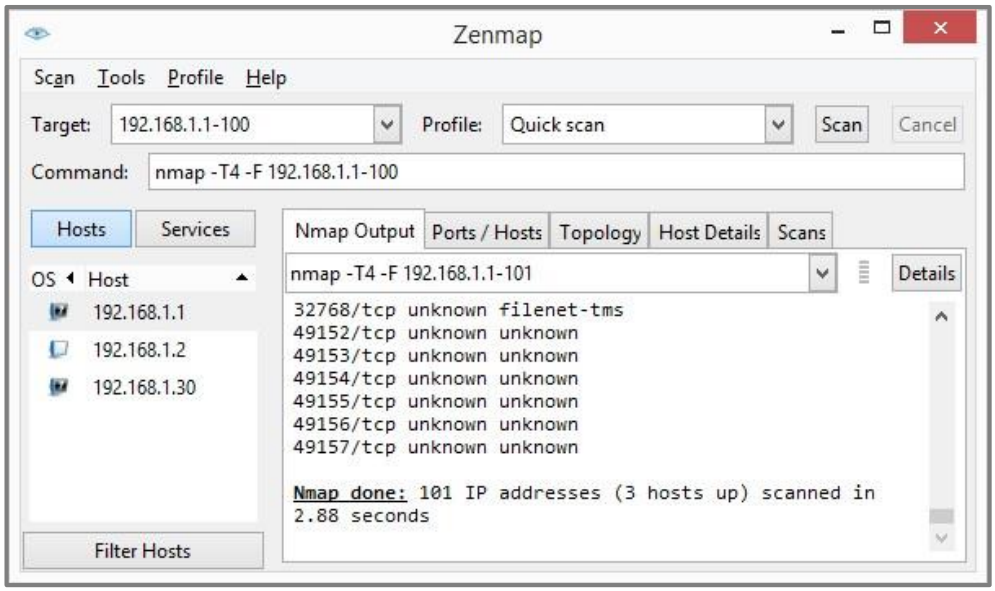
Примечание:

Если сконфигурировано Errdisable Recovery, то запись о Host-A снова появится по истечению интервала Errdisable Recovery Interval, после чего у Host-A снова будет доступ к USG.

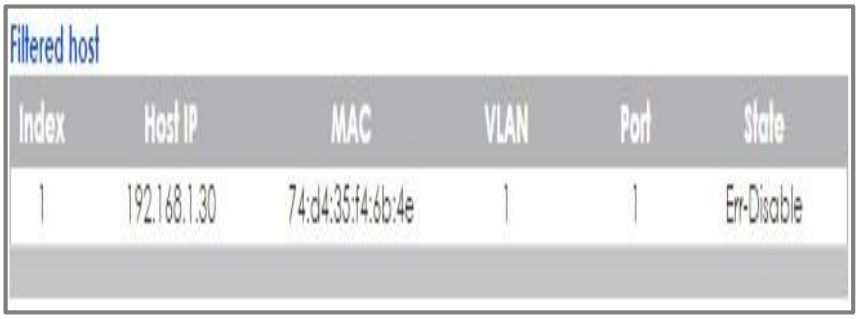
6 У Host-B по-прежнему должен быть доступ к USG.

7 Подсоедините Host-C к коммутатору.

8 Host-C должен быстро просканировать IP-адреса от 192.168.1.1 до 192.168.1.100.



9 У Host-C теперь нет доступа к USG.



10 Откройте Web-интерфейс коммутатора. Перейдите в **Advance Application > Anti-Arpscan**. Теперь у порта Port должно быть состояние Err-disabled.

Anti-Arpscan Status — Host Status | Trust Host | Configure

Anti-Arpscan is enabled

Port	Trusted	State
1	No	Forwarding
2	No	Err-disable
3	No	Forwarding
4	No	Forwarding
5	No	Forwarding

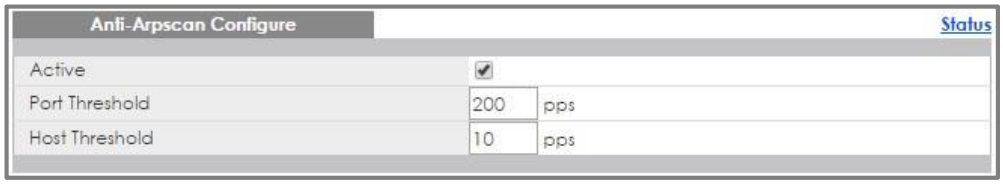
Примечание:
Если сконфигурировано Errdisable Recovery, то состояние порта Port 2 изменится на forwarding по истечению интервала Errdisable Recovery Interval, после чего у Host-C снова будет доступ к USG.

5.3.3 Почему это не работает?

1 Если после включения Anti-Arpscan нет доступа к серверам или локальному шлюзу, убедитесь, что “untrusted” стоит только для портов, который напрямую подключены к хостам или точке доступа. Порты, подключенные к серверам и локальному шлюзу, должны быть “trusted”.

2 Если у хостов, подключенных к точек доступа, нет доступа к локальному шлюзу, то нужно убедиться, что состояние порта точки доступа изменено на err-disable в **Advance Application > Anti-Arpscan**.

Если этот порт в err-disable, то попробуйте увеличить значение в **Port Threshold** in **Advance Application > AntiArpscan > Configure**.



5.4 Как настроить коммутатор и сервер RADIUS для доступа к сети с помощью аутентификации 802.1x Port Authentication

В этом примере показано, как настроить коммутатор на предоставление доступа машинам с действующими user credentials. С помощью аутентификации 802.1x Port обеспечивается доступам к сетевым ресурсам организации только для авторизованных пользователей.

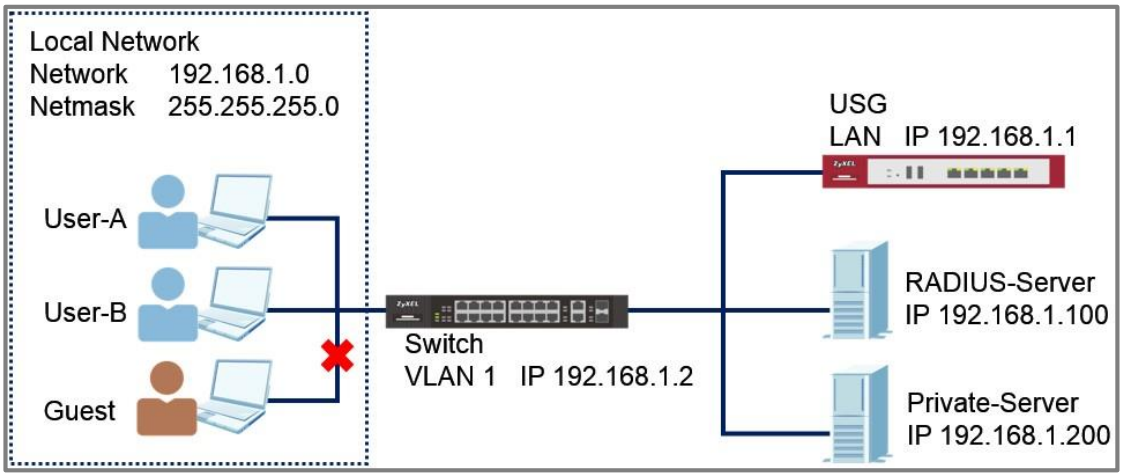


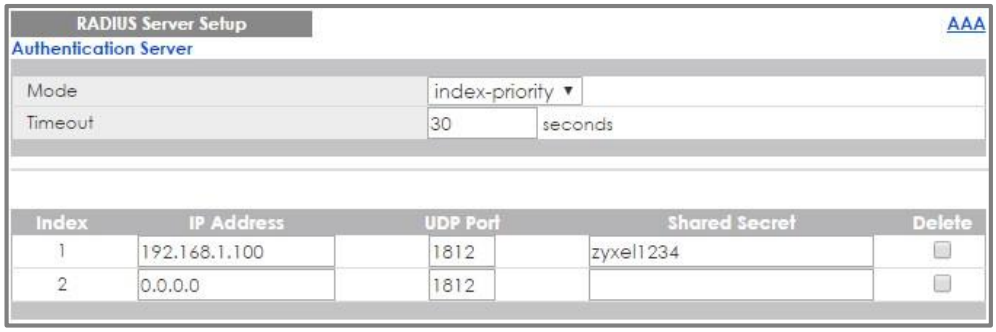
Иллюстрация 22 Аутентификация 802.1x Port Authentication обеспечивает доступ для авторизованных пользователей

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. Для аутентификации в этом примере используется сервер FreeRADIUS, работающий под управлением Ubuntu.
Интерфейс пользователя (UI) в этом примере относится к коммутатору серии XGS4600.

5.4.1 Настройка конфигурации коммутатора

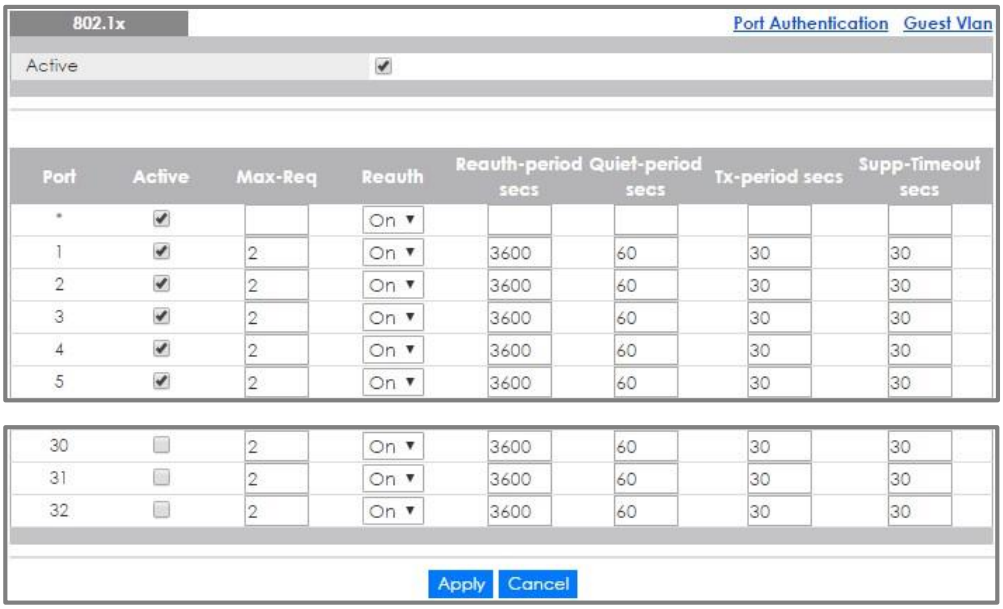
1 Откройте Web-интерфейс коммутатора.

2 Перейдите в **Advance Application > AAA > RADIUS Server Setup**. Настройте IP-адрес сервера RADIUS и shared secret. Щелкните **Apply**.



Примечание:
shared secret должен соответствовать секрету вашему профилю клиента must сервера RADIUS.

3 Перейдите в **Advance Application > Port Authentication > 802.1x**. Поставьте галочку в поле 802.1x Active и для всех портов, к которым подключены устройства. Не ставьте галочку для портов, к которым подключены **USG**, **RADIUS-Server** или **Private-Server**.



5.4.2 Настройка конфигурации сервера RADIUS

1 Отредактируйте профиль клиента в **/etc/freeradius/clients.conf**, сохраните файл и выйдите.

```
client 192.168.1.2 {
        secret = zyxel1234
        shortname = Switch
        nastype = other
}
```

Примечание:
IP-адрес клиента и его secret должны соответствовать management IP и shared secret коммутатора.

2 Добавьте следующие профили пользователей в **/etc/freeradius/users**, сохраните файл и выйдите.

```
User-A  Cleartext-Password := "zyxeluserA"
        Service-Type = Administrative-User

User-B  Cleartext-Password := "zyxeluserB"
        Service-Type = Administrative-User
```

3 Перезапустите сервис FreeRADIUS

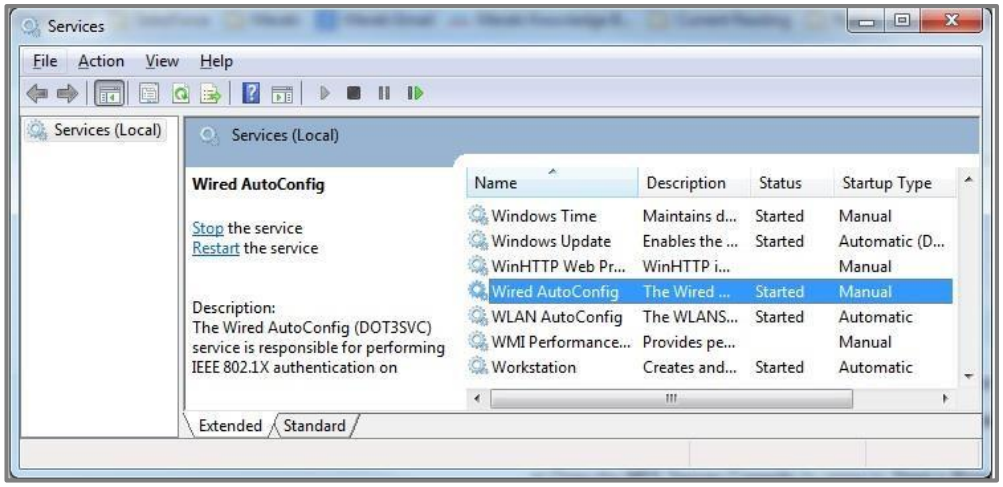
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
root@dhcppc68:/etc/freeradius#
```

5.4.3 Проверка результатов

1 Проверьте доступ для **User-A**, **User-B** и устройства **Guest**.

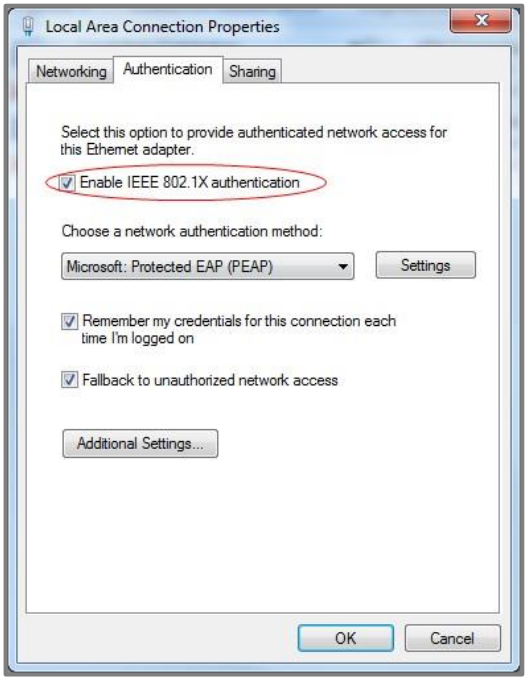
2 Если вы используете Windows, щелкните кнопку **Start button** и в окне поиска введите **services.msc**.

3 В окне Services найдите сервис **Wired AutoConfig**. Его статус должен быть “**Started”**.

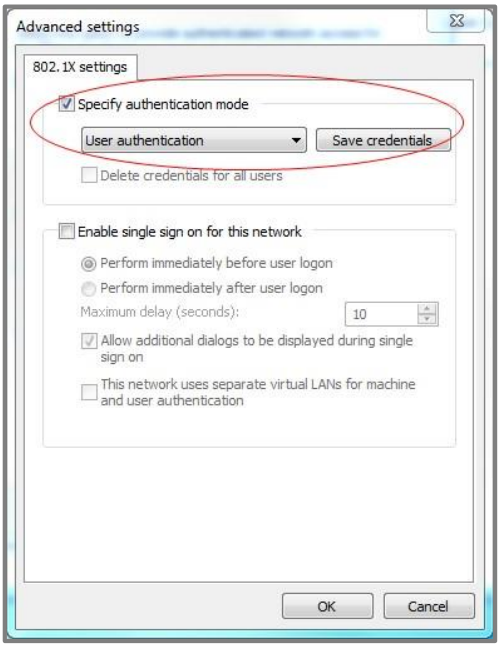


4 Щелкните правой кнопкой по сетевому адаптеру и выберите **Properties**.

5 Щелкните вкладку Authentication и поставьте галочку напротив “**Enable IEEE 802.1X authentication**”. В поле network authentication method должно стоять **Microsoft: Protected EAP (PEAP)**



6 Щелкните **Additional Settings**, выберите **Specify authentication mode** и задайте **User authentication**.



7 Подключите устройство User-A к коммутатору. Для User-A появится всплывающее сообщение “**Additional information is needed to connect to this network.**”

8 Введите имя пользователя username (**User-A**) и пароль password (**zyxeluserA**), соответствующие настройкам профиля пользователя на RADIUS-Server.

9 Устройства, использующие User-A и User-B, могут обмениваться данными с **USG** и **Private-Server**.

10 Подсоедините устройство User-A к коммутатору. Для User-A появится всплывающее сообщение “**Additional information is needed to connect to this network.**”

11 Введите username (**Guest**) и случайным образом подобранный пароль.

12 Устройства, использующие Guest credentials, не смогут обмениваться данными с **USG** и **Private-Server**.

5.4.4 Почему это не работает?

1 Если коммутатор не предоставляет доступ пользователям с корректными credentials, то это может быть вызвано следующими проблемами:

a. В имени пользователя и пароле учитывается регистр букв. Убедитесь, что вы набираете их в правильном регистре.

b. Сервер RADIUS ненадежный. Ping должны все время проходить от коммутатора к серверу RADIUS. Проверьте настройки сетевого соединения между коммутатором и сервером RADIUS.

c. У коммутатора и сервера RADIUS разный shared secret.

5.5 Как настроить коммутатор чтобы неавторизованные пользователи подключались к гостевой VLAN

В этом примере показано, как настроить коммутатор чтобы направлять в гостевую VKAN пользователей, которые не прошли аутентификацию 802.1x port либо у них истек срок действия credential. На практике это означает, что гости через USG могут выйти в Интернет, но у них нет доступа к серверу Private-Server, а пользователи с действующими credential могут получить доступ только к Private-Server.

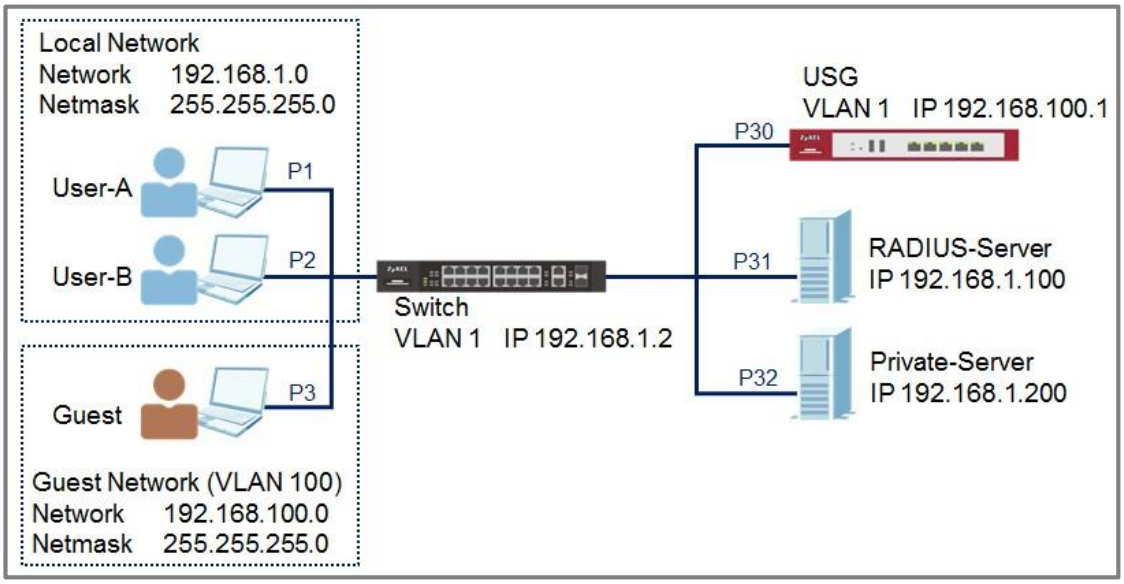


Иллюстрация 23 Настройка конфигурации коммутатора для того, чтобы неавторизованные пользователи подключались к гостевой VLAN

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

5.5.1 Настройка аутентификации 802.1x Port Authentication на коммутаторе

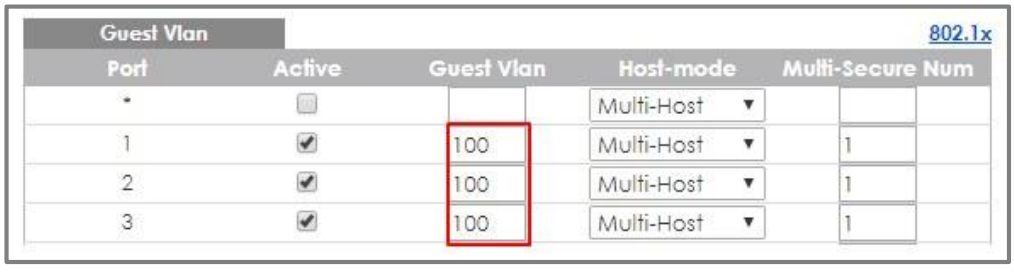
1 Настройте 802.1x для всех пользователей. Не включайте Port Authentication на портах, к которым подключены USG, RADIUS-Serve, и PrivateServer. О настройке Port Authentication см. **5.4 Как настроить коммутатор и сервер RADIUS для доступа к сети с помощью аутентификации 802.1x Port Authentication.**

5.5.2 Настройка VLAN for для VLAN

1 Настройте на коммутаторе VLAN для Guest VLAN (**VLAN 100**). **VLAN 100**: Задайте fixed port: 1, 2, 3, 30; untagged port: 1, 2, 3, 30; forbidden port: 31, 32; port 30: pvid=100. **VLAN 1**: Задайте forbidden port: 30. О изоляции VLAN 1 и 100 см. **2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN**.

5.5.3 Настройка Guest VLAN для Failed Authentication (ошибки аутентификации)

1 Перейдите в **Menu > Advanced Application > Port Authentication > 802.1x > Guest Vlan**. Активируйте Guest Vlan на port 1-3 и введите для guest Vlan значение **100**. Нажмите “Apply”.



5.5.4 Настройка RadiusServer

1 Отредактируйте профиль клиента в **/etc/freeradius/clients.conf**. Выйдите с сохранением файла.

```
client 192.168.1.1 {
        secret = thisisasecret
        shortname = Switch
        nastype = other
}
```

Примечание:
IP-адрес клиента и его secret должны соответствовать management IP и shared secret коммутатора.

2 Добавьте следующие профили клиентов в **/etc/freeradius/users**.

Выйдите с сохранением файла.

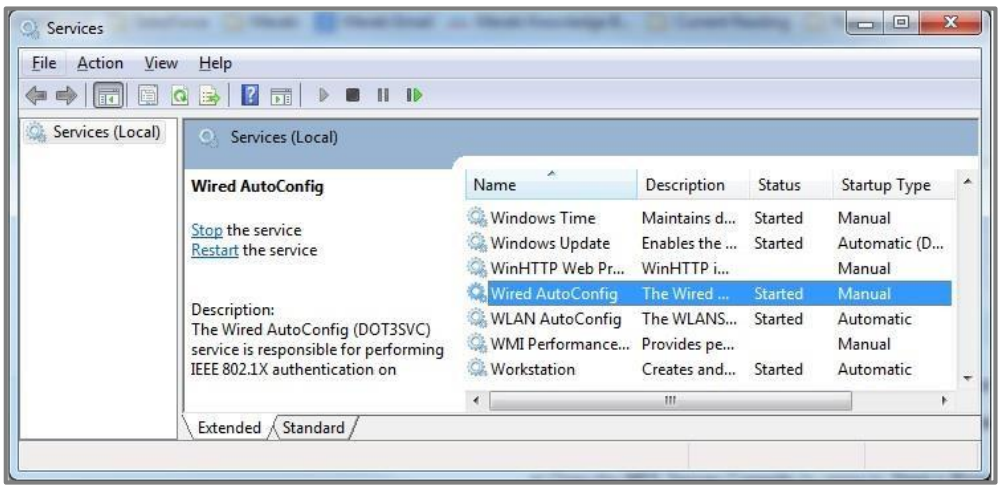
```
user  Cleartest-Password :="user1234"
      Service-Type = Administrative-User
```

3 Перезапустите сервис FreeRADIUS.

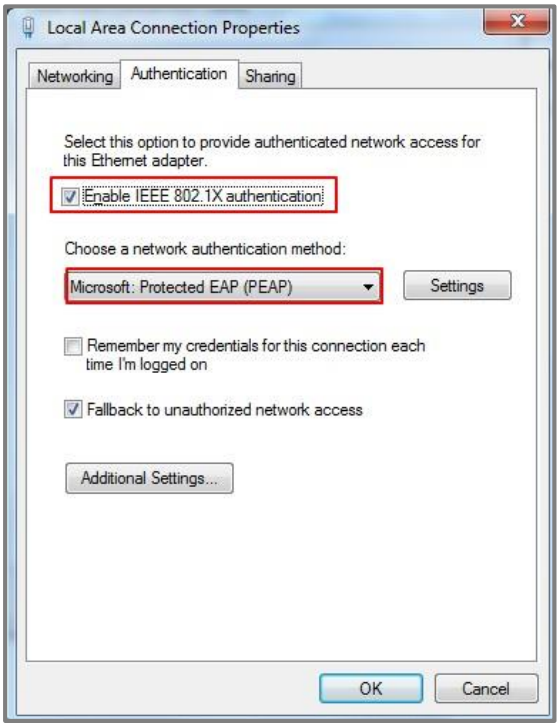
```
root@dhcppc68:/etc/freeradius# stop freeradius
stop: Unknown instance:
root@dhcppc68:/etc/freeradius# start freeradius
freeradius start/running, process 8800
```

5.5.5 Настройка параметров User-A, User-B и Guest

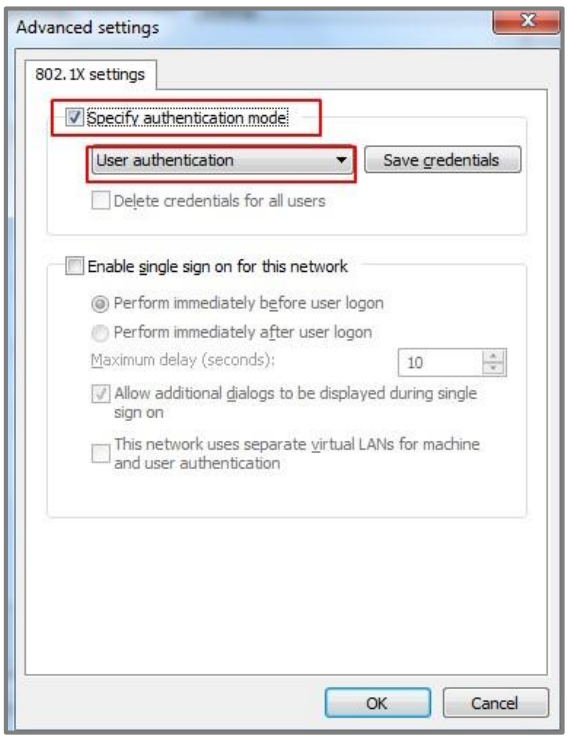
1 Найдите в окне **Services** сервис **Wired AutoConfig**. Его статус должен быть “Started”.



2 Щелкните правой кнопкой по сетевому адаптеру и выберите **Properties**. Щелкните вкладаку Authentication tab и поставьте галочку в “**Enable IEEE 802.1X authentication**”. В network authentication method должно стоять “**Microsoft: Protected EAP (PEAP)**”.



3 Щелкните **Additional Settings**, выберите **Specify authentication mode** и задайте **User authentication**.



5.5.6 Проверка результатов

1 Отсоедините и снова подсоедините PC к коммутатору. На PC появится всплывающее сообщение “**Additional information is needed to connect to this network**.”

2 Введите имя пользователя username (**User-A**) и пароль password (**zyxeluserA**), соответствующие настройкам профиля пользователя RADIUS-Server.

3 У устройств, использующих credential пользователей User-A и User-B, есть доступ к Private-Server.

4 Подключите устройство User-A к коммутатору. На User-A появится всплывающее сообщение “**Additional information is needed to connect to this network.**”

5 Введите имя пользователя username (Guest) и случайным образом выбранный пароль.

6 У устройств, использующих Guest credentials, не будет доступа к Private-Server, но будет доступ к USG.

7 Проверьте таблицу MAC-адресов коммутатора. Устройства с неправильными credentials, будут назначены в VLAN 100. (**Menu > Management > MAC Table > Search**)

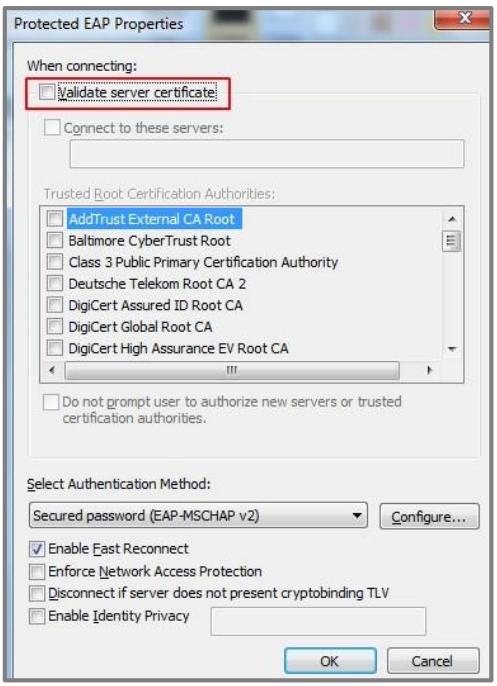
Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	100	3	Dynamic
2	20:6a:8a:39:fe:a9	1	12	Dynamic
3	3c:97:0e:30:0e:b8	1	12	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	100	CPU	Static
6	60:31:97:71:6d:15	1	12	Dynamic
7	60:31:97:71:6d:21	1	12	Dynamic
8	74:d4:35:f4:6b:4e	1	12	Dynamic
9	84:ef:18:95:08:e4	1	12	Dynamic
10	a0:8c:fd:1c:c0:b1	1	12	Dynamic
11	b8:ec:a3:0f:cf:9f	1	12	Dynamic
12	c8:6c:87:9f:51:f0	1	12	Dynamic
13	f0:de:f1:91:74:f8	100	1	Dynamic
14	fc:3f:db:39:66:80	1	12	Dynamic

5.5.7 Почему это не работает

1 Если на PC при подключении к коммутатору не выводится всплывающее сообщение аутентификации:

a. Посмотрите, проходит ли с коммутатора Switch ping на Radius-Server..

b. Щелкните правой кнопкой сетевой адаптер и выберите **Properties > Authentication > Additional settings**. Уберите галочку в “**Validate server certificate**”.



2 Если настройки shared secret коммутатора и PC **НЕ** совпадают, то аутентификация завершится ошибкой.

3 Если аутентификация успешно выполнена, но с PC не проходят ping на сервер, то нужно проверить конфигурацию 801.1X Port Authentication. **НЕ** включайте аутентификацию для порта uplink (port 2, 3 и 12).

4 Если у устройств в Guest VLAN нет доступа к USG, то убедитесь, что в коммутаторе создана и настроена Guest VLAN в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**.

5.6 Как настроить коммутатор и сервер RADIUS для предоставления доступа к сети по MAC-адресу устройства

В этом примере показано, как настроить конфигурацию коммутатора так, чтобы доступ был только у машин с определенными MAC-адресами. С помощью MAC Authentication можно разрешить доступ к внутренним ресурсам компании только для принадлежащих ей устройств.

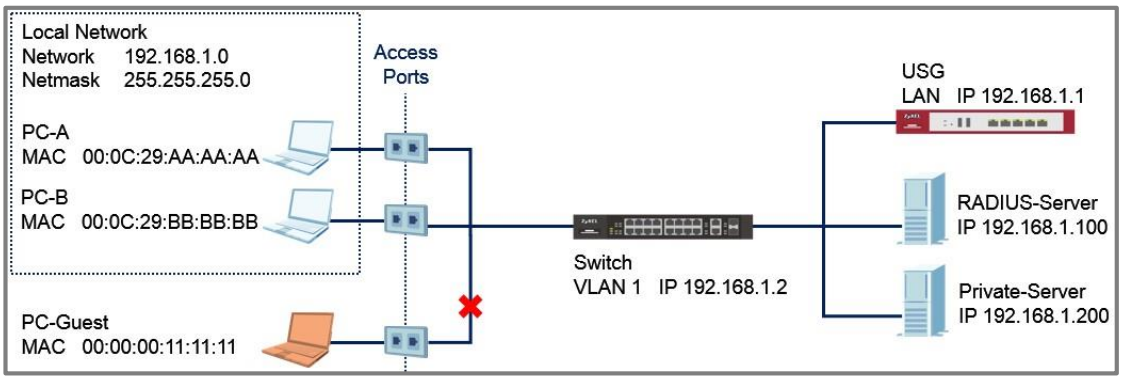


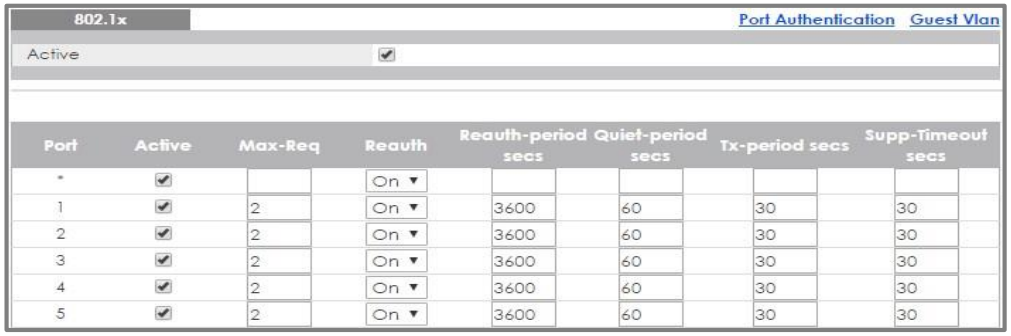
Иллюстрация 24 802.1x Port Authentication обеспечивает доступ для авторизованных устройств

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере для аутентификации используется сервер FreeRADIUS, установленным на сервере Ubuntu.
Интерфейс пользователя (UI) в этом примере относится к коммутатору серии XGS4600.

5.6.1 Настройка конфигурации коммутатора

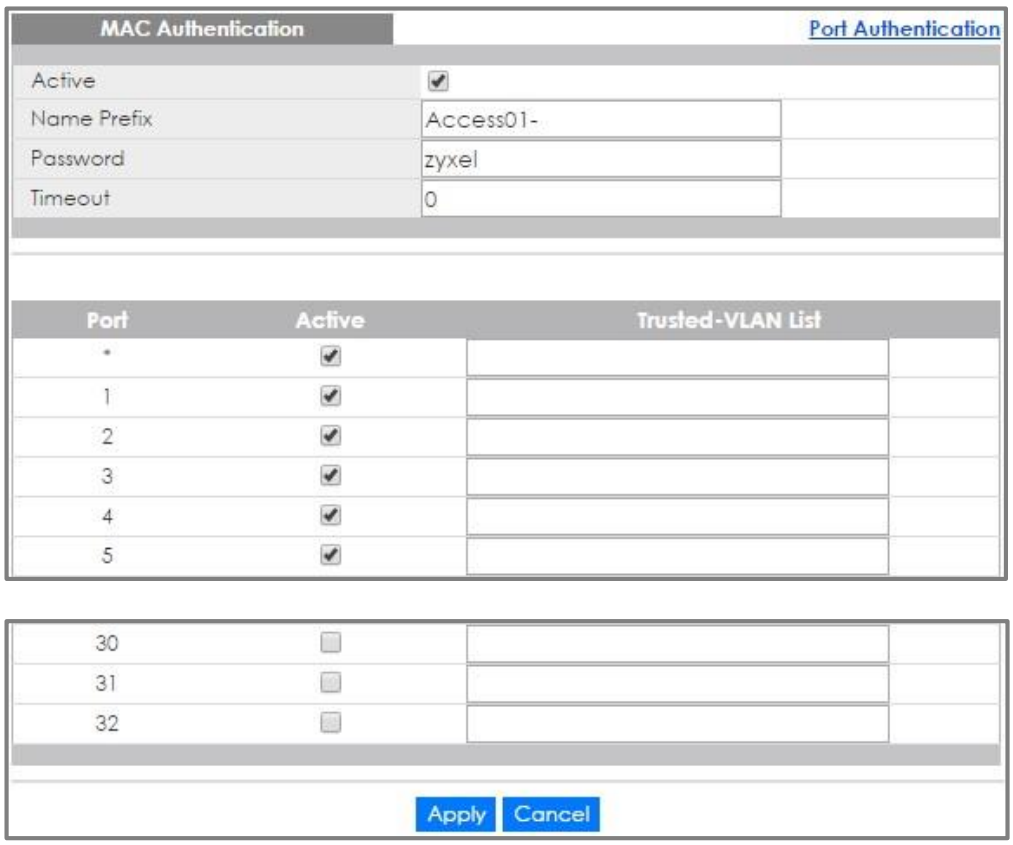
1 Откройте Web-интерфейс коммутатора.

2 Перейдите в **Advance Application > AAA > RADIUS Server Setup**. Настройте IP-адрес сервера RADIUS и задайте shared secret. Щелкните **Apply**.



Примечание:
shared secret должен соответствовать secret профиля клиента на сервере RADIUS.

3 Перейдите в **Advance Application > Port Authentication > MAC Authentication**. Поставьте галочку в поле MAC Authentication Active, а также для портов, используемых для доступа. Уберите галочку в ACTIVE для портов, которые подключены к **USG**, **RADIUS-Server** или **Private-Server**.



5.6.2 Настройка RADIUS-Server

1 Отредактируйте профиль клиента в **/etc/freeradius/clients.conf**. Выйдите с сохранением файла.

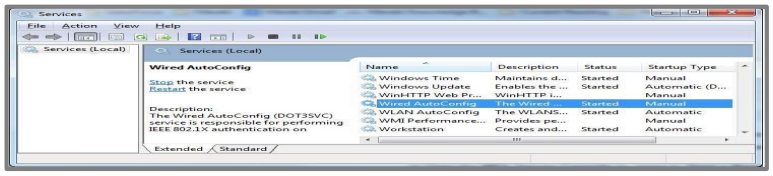
```
client 192.168.1.2 {
        secret = zyxel1234
        shortname = Switch
        nastype = other
}
```

Примечание:
У клиента IP-адрес и секрет должны соответствовать management IP и shared secret коммутатора.

2 Добавьте следующие профили пользователей в **/etc/freeradius/users**. Имя пользователя Username нужно ввести в формате **<Name Prefix><MAC Address of your device>**. Выйдите с сохранением файла.

```
Access01-00-0C-29-AA-AA-AA      Cleartext-Password := "zyxel"

Access01-00-0C-29-BB-BB-BB      Cleartext-Password := "zyxel"
```

3 Перезапустите сервис FreeRADIUS.



5.6.3 Проверка результатов

1 Подключите к коммутатору **PC-A**, **PC-B** и **PC-Guest**.

2 У PC-A и PC-B должен быть доступ к USG и Private-Server.

3 У PC-Guest должен отсутствовать доступ к USG и Private-Server.

5.6.4 Почему это не работает?

1. Если коммутатор не предоставляет доступ авторизованным устройствам:
    a. В профиле пользователя на RADIUS-Server нужно использовать MAC-адрес устройства в 16-ричном формате с заглавными буквами, разделенными тире (-) вместо двоеточий (:).
    b. У некоторых компьютеров, например, ноутбуков, может быть два MAC-адреса (LAN и Wireless). Убедитесь, что в профиле пользователя RADIUS Server используется правильный MAC-адрес.

2. Если коммутатор не предоставляет доступ авторизованным устройствам после исправления его конфигурации или конфигурации RADIUS-Server, то подождите несколько минут и снова попытайтесь получить доступ (по умолчанию таймаут повторной аутентификации устройства по MAC-адресу **300 секунд)**.

5.7 Как настроить коммутатор для предотвращения ARP spoofing

В этом примере объясняется, как настроить коммутатор для защиты от сетевых атак ARP Spoofing, в которых злоумышленник использует IP-адрес одного из основных компонентов сети (например, сервера или шлюза). ARP Spoofing приводит к отказу в обслуживании или перехвату передаваемой по сети информации. Функция ARP Inspection из IP Source Guard заставляет всех клиентов, подключенных к портам коммутатора, использовать IP-адреса, полученные от назначенного сервера DHCP.

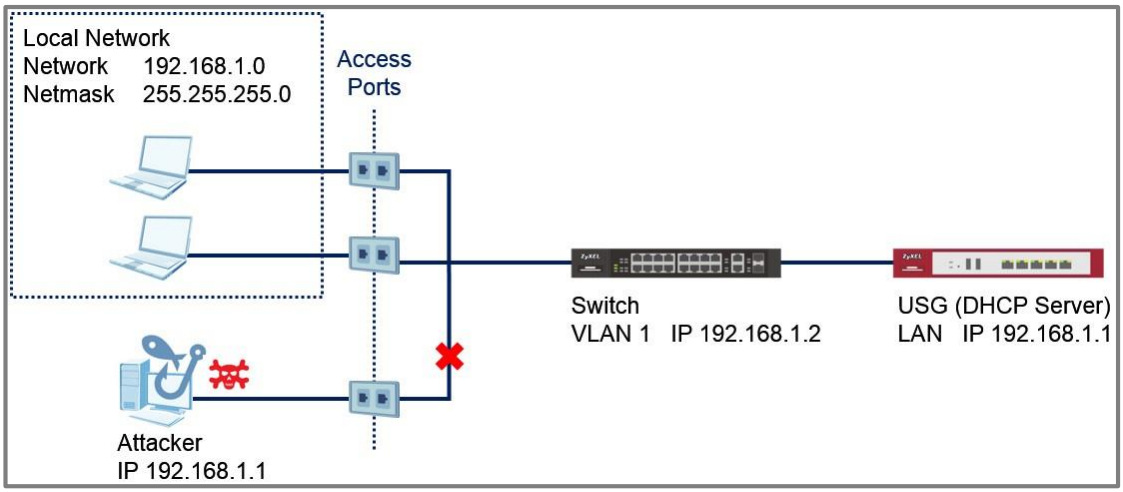


Иллюстрация 25 Злоумышленник использует для атаки IP-адрес USG

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. Интерфейсы пользователя относятся к коммутатору XGS4600.

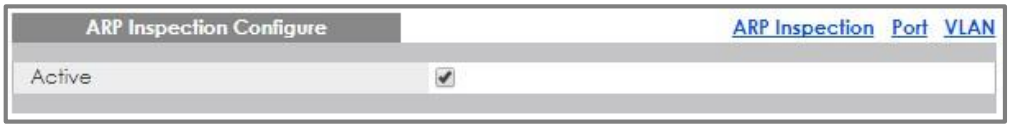
5.7.1 Настройка конфигурации коммутатора

1 Откройте Web-интерфейс коммутатора.

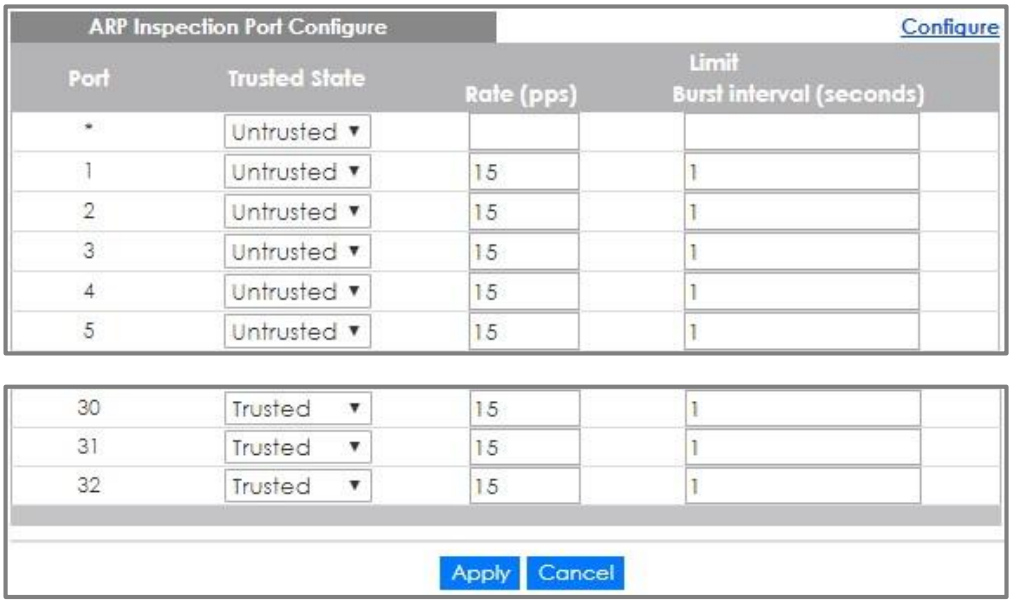
2 Настройте **DHCP Snooping** (см. **5.6.1**).

> Примечание:
> Нужно включить DHCP Snooping до настройки ARP Inspection.

3 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure**. Поставьте галочку в ACTIVE чтобы глобально включиить ARP Inspection.



4 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > Port**. Задайте все порты, используемые для доступа, как untrusted, а порты, к которым подключен USG или другие компоненты сети, как trusted. Щелкните **Apply**.



5 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > ARP Inspection > Configure > VLAN**. Введите Start VID и End VID. В этом диапазон PVID должны попасть порты, используемые для доступа. Щелкните **Apply**.

6 После ввода диапазона VID ниже должен быть выведен список VID. Выберите **Yes** для VLAN портов, используемые для доступа. Щелкните **Apply**.

5.7.2 Проверка результатов

1 Подключите устройство, которому динамически назначается IP-адрес, к порту коммутатора, используемого для доступа. У этого устройства должен быть доступ к USG.

2 Когда устройство получит IP-адрес откройте web-интерфейс коммутатора. Перейдите в **Advance Application > IP Source Guard > IPv4 Source**. В таблице IP Source Guard Table должна появиться запись об устройстве.

IP Source Guard | IPSG | Static Binding | DHCP Snooping | ARP Inspection

Index	MAC Address	IP Address	Lease	Type	VID	Port
1	20:6a:8a:39:fe:a9	192.168.1.30	2d23h59m40s	dhcp-snooping	1	1

3 Подключите другое устройство, у которого статический IP-адрес, к одному из портов коммутатора, используемых для доступа. В этом примере устройство пытается использовать IP-адрес USG “192.168.1.1”. Коммутатор не дает этому устройству доступ к другим устройствам.

5.7.3 Почему это не работает?

1 Если у устройств в локальной сети нет доступа к USG, т сначала можно проверить настройки DHCP Snooping на коммутаторе.

2 Если DHCP Snooping правильно настроен, но у устройств в локальной сети по-прежнему нет доступа к USG, то надо подождать несколько минут и снова проверить доступ к USG. ARP Inspection посылает MAC-адрес устройства в таблицу filter table. Время ожидание повторного подключения определяется значением в колонке “Expiry (sec)” column.

3 Некоторые устройства не могут получить доступ к USG по следующим причинам:

a. Порт, который подключен к USG, не является trusted.

b. Некоторые клиенты в сети не обновили свои настройки DHCP после перезагрузки коммутатора.

c. Исчерпан пул IP-адресов сервера DHCP.

5.8 Как настроить коммутатор для защиты от поддельных серверов DHCP

В этом примере показано, как надо настроить коммутатор для защиты от сетевых атак, при которых злоумышленники посылают клиентам поддельная конфигурация IP. DHCP Snooping блокирует настройки DHCP, которые приходят от порта untrusted. Обычно порты untrusted – это порты, к которым подключены офисные ПК или общедоступные розетки Ethernet.

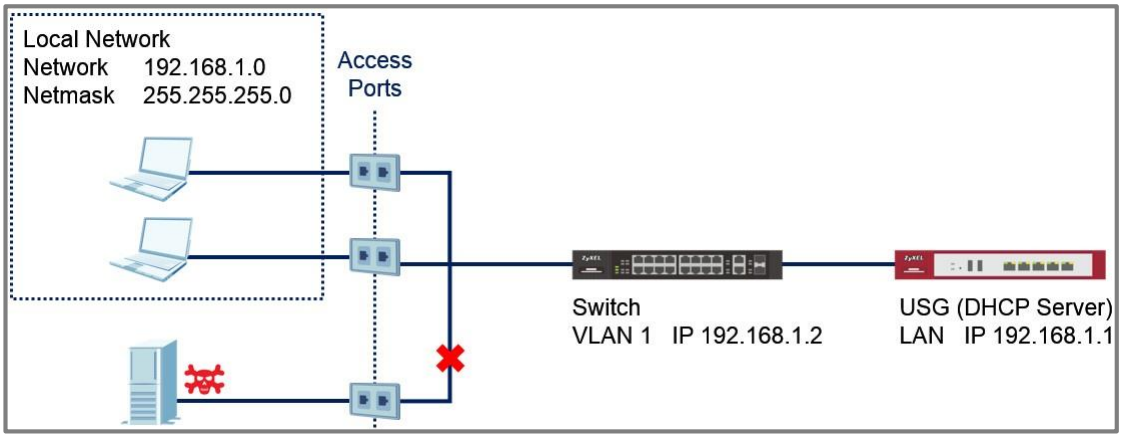


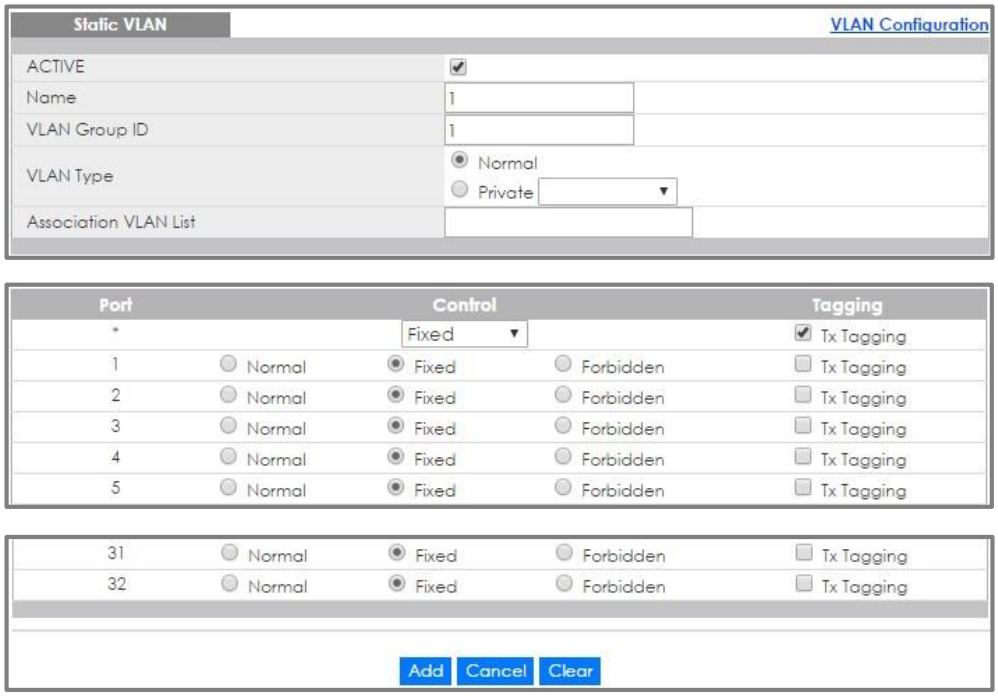
Иллюстрация 26 Поддельный сервер DHCP, подключенный через незащищенные порты, используемые для доступа

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети.
Все интерфейсы пользователя (UI) в этом примере относятся к коммутатору серии XGS4600.

5.8.1 Настройка конфигурации коммутатора

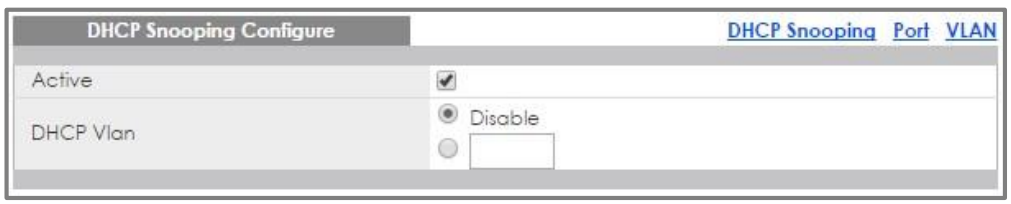
1 Откройте Web-интерфейс коммутатора.

2 Перейдите в **Advance Application > VLAN > VLAN Configuration > Static VLAN Setup**. В этом примере весь трафик, который идет через порты, используемые для доступа, пересылается в VLAN 1. VLAN 1 должна быть fixed и untagged для всех используемых для доступа портов. Щелкните **Add**.

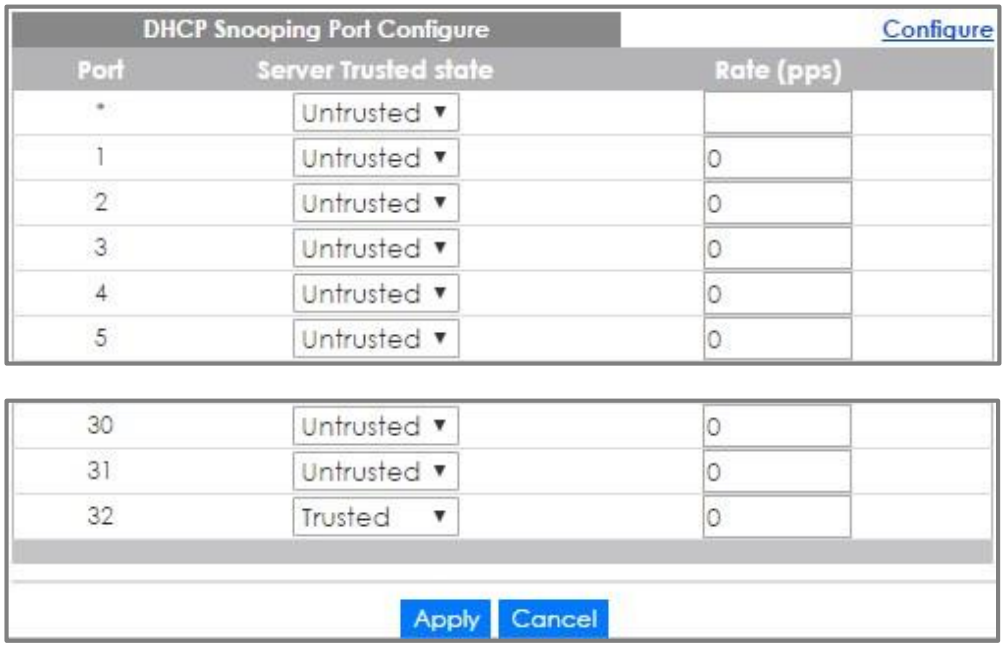


3 Перейдите в **Advance Application > VLAN > VLAN Configuration > VLAN Port Setup**. Настройте все используемые для доступа порта на PVID 1. Щелкните **Apply**.

4 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure**. Поставьте галочку в ACTIVE под DHCP Snooping Configure. Щелкните **Apply**.

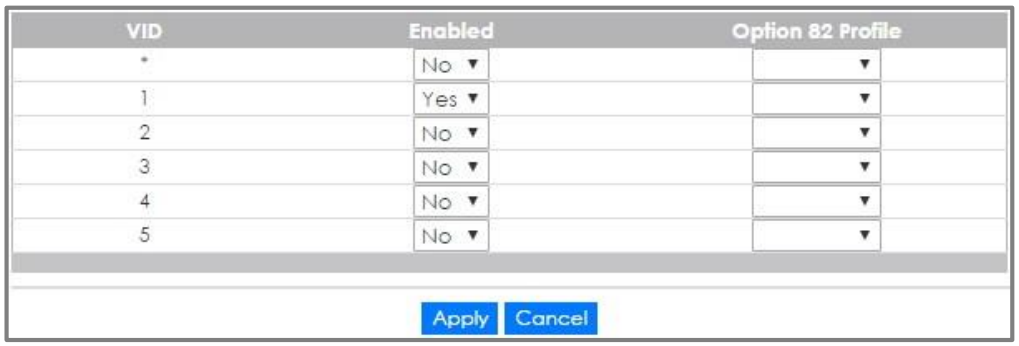


5 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**. Настройте все порты, используемые для доступа, как untrusted, а порты, к котором подключен USG или другие компоненты сети, должны быть trusted. Щелкните **Apply**.



6 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN**. Введите Start VID и End VID. В этот диапазон должны попадать PVID портов, используемых для доступа. Щелкните **Apply**.

7 После ввода диапазона VID ниже будет выведен список VID. выберите **Yes** для VLAN портов, используемых для доступа. Щелкните **Apply**.



5.8.2 Проверка результатов

1 Подключите поддельный Rogue-DHCP к одному из используемых для доступа портов.

В LAN interface создайте следующий пул DHCP Pool:

Starting IP Address : 172.16.1.10

End IP Address : 172.16.1.20

2 Подключите клиенты DHCP к другим портам, используемым для доступа. Клиенты должны получать только те IP-адреса, которые предоставляет USG.

5.8.3 Почему это не работает?

1. Если клиенты DHCP, подключенные к незащищенным портам для доступа, используют IP-адреса от Rogue-DHCP:
   a. Убедитесь, что все эти порты настроены как untrusted в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.
   b. Проверьте PVID порта, к которому подключен клиент DHCP. Убедитесь, что DHCP snooping включен для этой VLAN в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > VLAN**.

2. Если клиенты DHCP, подключенные к незащищенным портам для доступа, не могут получить IP-адреса от настоящего сервера DHCP:
   a. Убедитесь, что порт, к которому подключен настоящий сервер DHCP, определен как trusted в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.
   b. Если используется топология Ring, то оба резервированных порта должны быть определены как trusted в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > DHCP Snooping > Configure > Port**.

5.9 Как настроить IPSG static binding для доверенных (trusted) сетевых устройств

В этом примере показано, как настроить коммутатор чтобы разрешить устройству, которое использует администратор, использовать статический IP-адрес на порте доступа даже при включенной ARP Inspection. Это нужно для расширения возможностей устройства, используемого администратором, в том числе преимуществе настроенных для сети политик, ориентированных на IP-адреса. При этом другие устройства будут использовать только IP-адреса, предоставляемые настоящим сервером DHCP.

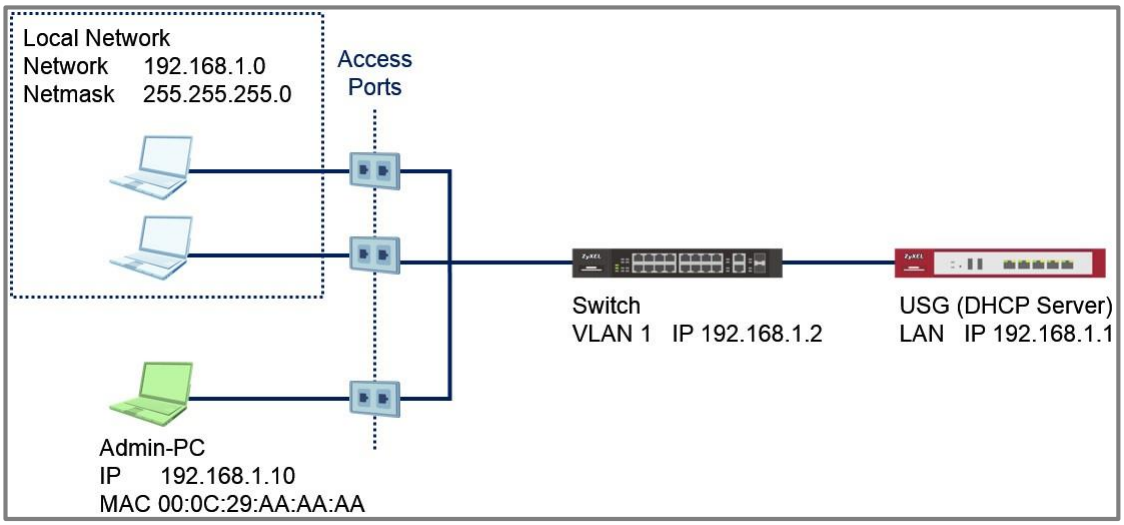


Иллюстрация 27 У устройства, используемого администратором и подключенного к порту доступа, статичный IP-адрес

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. Все интерфейсы пользователя (UI) в этом примере относятся к коммутатору серии XGS4600.

5.9.1 Настройка конфигурации коммутатора

1 Откройте Web-интерфейс коммутатора.

2 Настройте **ARP Inspection** (см. раздел **5.7.1**).

> Примечание:
> Для использования Static Binding нужно включить DHCP Snooping и ARP Inspection.

3 Перейдите в **Advance Application > IP Source Guard > IPv4 Source Guard Setup > Static Binding**. Создайте запись Static Binding с MAC- и IP-адресом вашего устройства. Введите VLAN и номер порта для устройства, которому разрешен доступ без ограничений. Щелкните **Add**.

5.9.2 Проверка результатов

1 Перейдите в **Advance Application > IP Source Guard**. Запись с MAC- и IP-адресом вашего устройства должна быть в таблице IP Source Guard Table Address со значениями “Static” в Type и “Infinity” в Lease.

2 Настройте ваш Admin-PC со статическим IP-адресом. В этом примере мы используем IP-адрес “192.168.1.10”. Подключите Admin-PC к любому используемому для доступа порту. У этого PC должен быть доступ к USG.

3 Настройте другой ПК с этим статическим IP-адресом “192.168.1.10”. У другого ПК не должно быть доступа к USG из-за несовпадения MAC-адреса.

5.10 Как настроить ACL на блокировку нежелательного трафика

В этом примере показано, как настроить ACL на блокировку нежелательного трафика. Можно задавать разные критерии блокировки. В данном примере ACL блокирует доступ к серверу для одного хоста в VLAN 10.

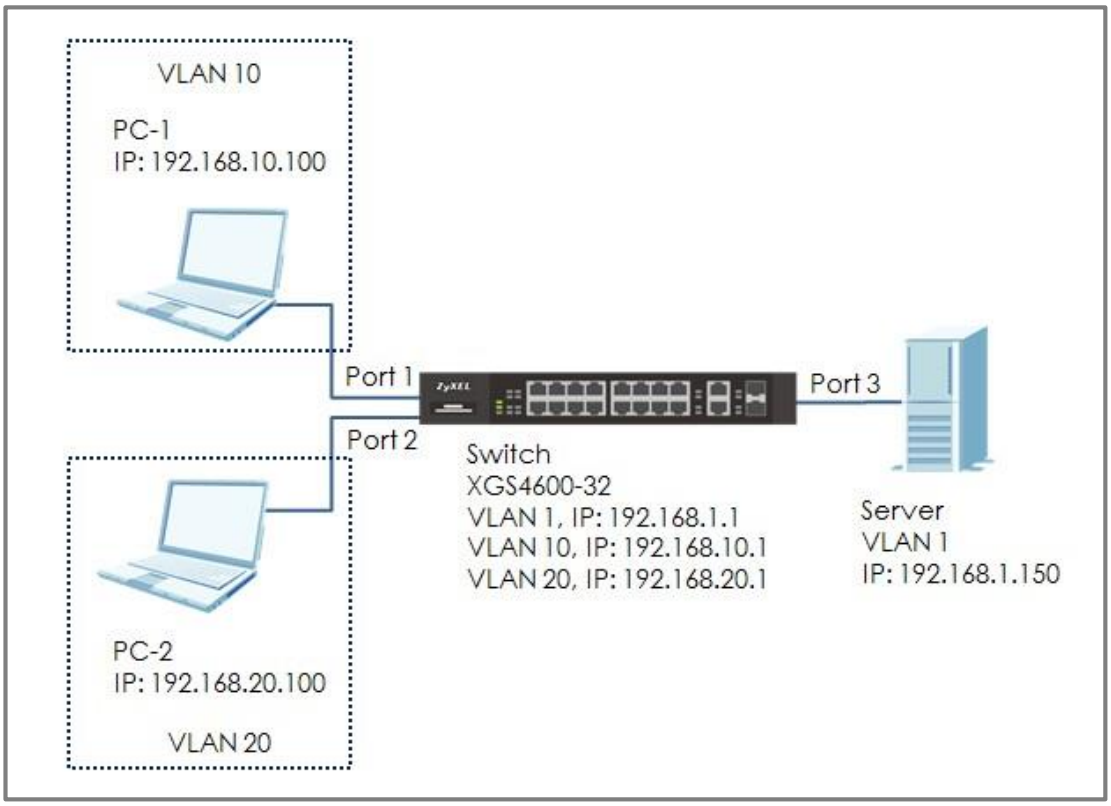


Иллюстрация 21 Настройка ACL на блокировку нежелательного трафика

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

5.10.1 Настройка VLAN и Route Traffic

1 Настройте параметры VLAN (VLAN 10 и VLAN 20) на коммутаторе (см. раздел: **2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN**).

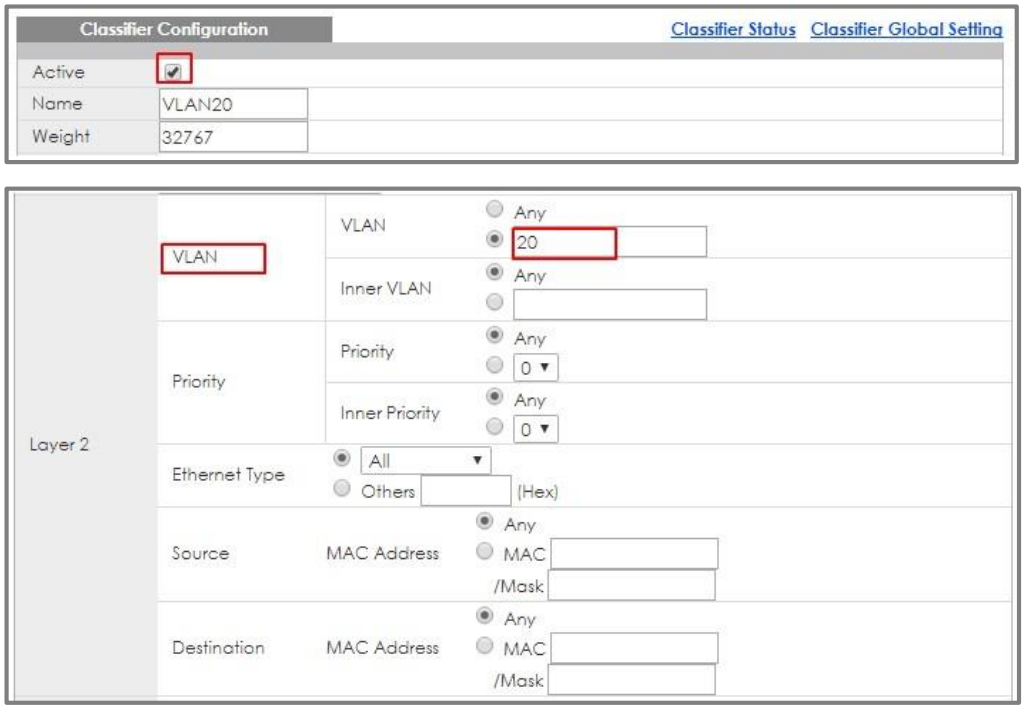
2 Настройте на коммутаторе интерфейсы VLAN IP (см. раздел: **2.2 Как настроить коммутатора для маршрутизации трафика между двумя VLAN**)

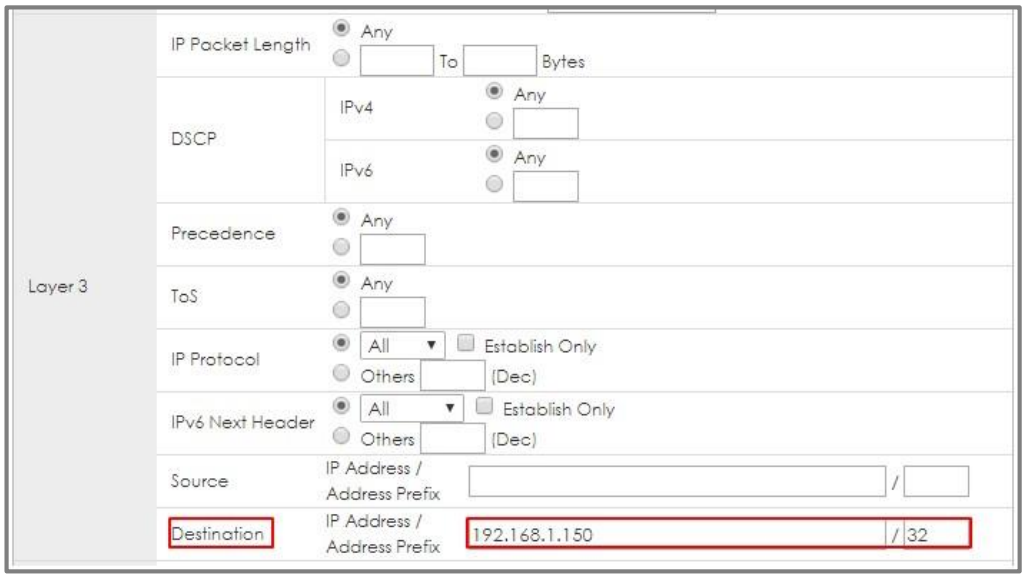
5.10.2 Настройка Classifier

1 Настройка Classifier: Перейдите в **Menu > Advanced Application > Classifier > Classifier Configuration**. Настройте Classifier для VLAN 20.

Примечание:
Подробнее о ACL см. **3.5 Как настроить ACL для ограничения скорости трафика IP**.

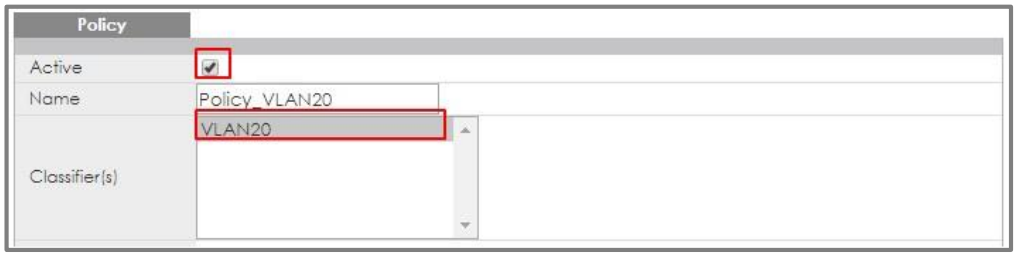
2 Classifier для VLAN 20: Поставьте галочку в поле “Active” и введите имя для Classifier. Настройте **Layer 2 > VLAN** как **20** и **Layer 3 > Destination** как **192.168.1.150/32**. Нажмите “Add”.




Layer 3
IP Packet Length
Any
To
Bytes
DSCP
IPv4
Any
IPv6
Any
Precedence
Any
ToS
Any
IP Protocol
All
Establish Only
Others
(Dec)
IPv6 Next Header
All
Establish Only
Others
(Dec)
Source
IP Address / Address Prefix
Destination
IP Address / Address Prefix
192.168.1.150
/ 32

5.10.3 Настройка правила политики Policy Rule

1 Настройте **Policy Rule**: Перейдите в **Menu > Advanced Application > Policy Rule**. Policy Rule для VLAN 20: поставьте галочку в “Active” и введите имя правила в Policy Rule Name. Выберите Classifier в VLAN 20 (VLAN20). Настройте действия при соответствии этому Classifier: **Action > Forwarding > Discard the packet**. Нажмите “Add”.



5.10.4 Проверка результатов

1 ping PC-1 доходят до сервера Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.
Reply from 192.168.1.200: Destination host unreachable.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

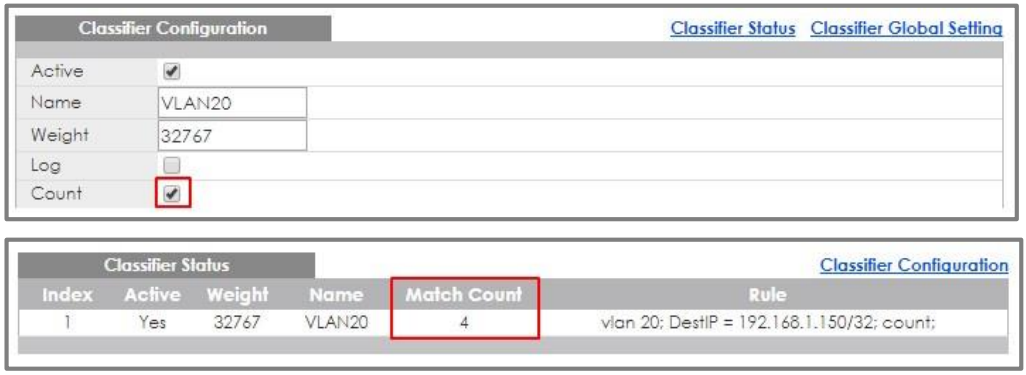
2 Из-за настроек ACL с PC-2 (VLAN 20) ping не доходят до сервера Server.

```
C:\Users\User>ping 192.168.1.150

Pinging 192.168.1.150 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.150:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

5.10.5 Почему это не работает

1 При настройке Classifier нужно правильно задать адреса отправителя и получателя трафика. Например, если создать policy rule только для source VLAN 20, но не для destination IP (Server IP: 192.168.1.150), то коммутатор будет блокировать весь трафик от VLAN 20 независимо от его получателя.

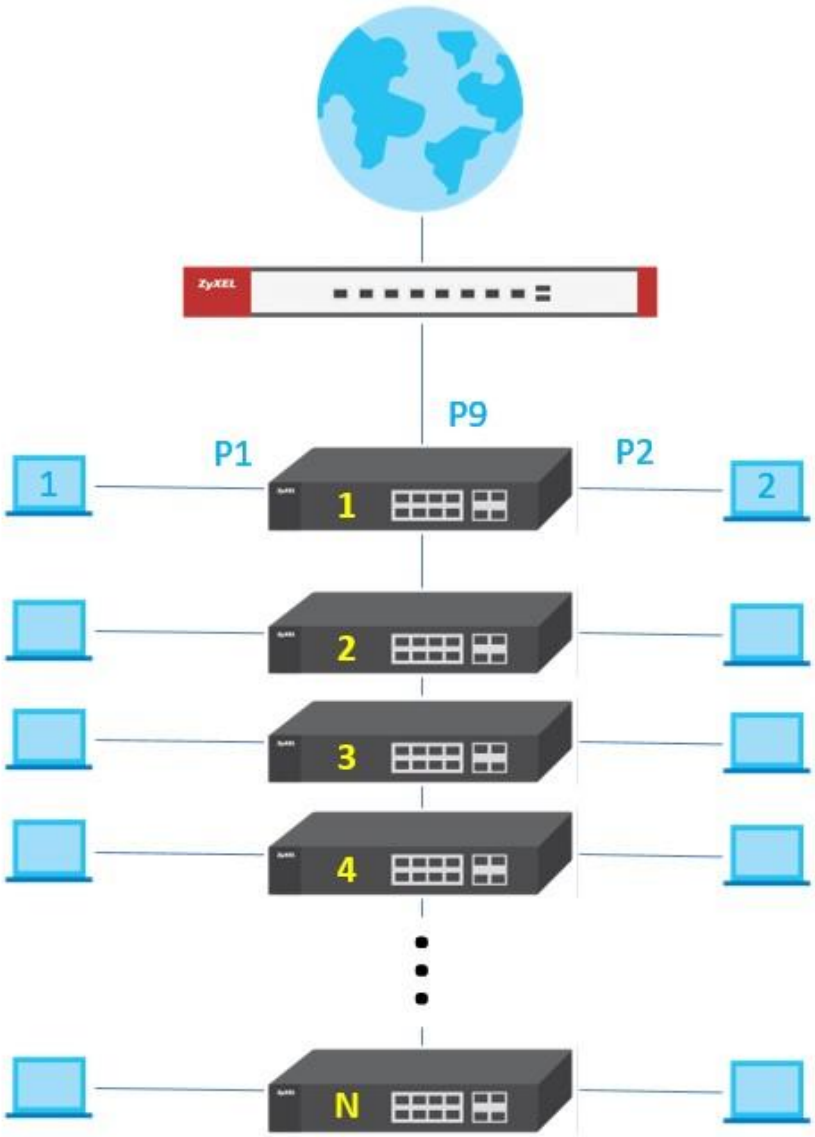
2 Перейдите в **Menu > Advanced Application > Classifier**. Поставьте галочку в “Count”. Если трафик соответствует classifier, то Match Count у этого classifier должен увеличиваться при каждом обновлении web-страницы.



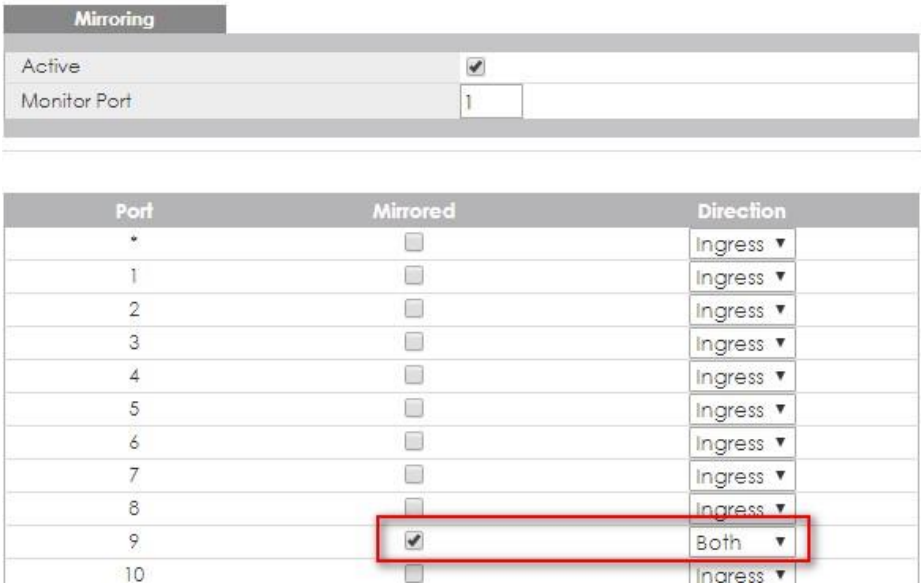
5.11 Как с помощью ACL зеркалировать трафик, соответствующий определенному критерию

Функция port mirroring дублирует трафик на порт мониторинга для его контроля без внесения дополнительной задержки. Она применяется для диагностики и для усиления контроля трафика.

В некоторых ситуация порт мониторинга может получать различный трафик если основной порт – это порт up/down link между устройствами, например, как в показанной на следующей иллюстрации ситуации:



В этом примере к коммутатору подключены другие коммутаторы и ПК.
PC 1 используется для мониторинга трафика между PC2 и Интернетом.
Обычно port 1 настраивается как порт мониторинга monitor port, а порт port 9 будет зеркалированным портом в обоих направлениях.



При таком подходе зеркалируется большой поток пакетов поскольку через порт port 9 коммутатора switch 1 идет агрегированный трафик в Интернет и поэтому зеркалированный трафик трудно классифицировать.

В описанной ниже процедуре настраивается фильтр зеркалированных пакетов с помощью ACL и в результате мониторинг выполняется только для трафика, соответствующего определенному критерию.

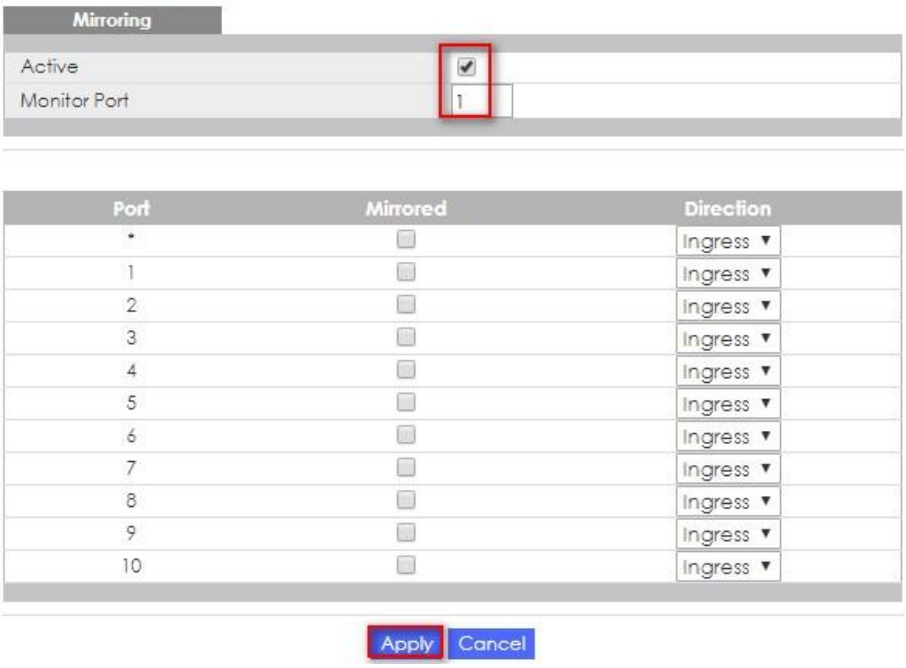
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети.

5.11.1 Настройка ACL

1 Откройте web-интерфейс коммутатора Switch-1.

2 Перейдите в **Advanced Application > Mirroring**.

Активируйте порт port 1 и назначьте его Monitor Port.



3 Перейдите в **Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting**.

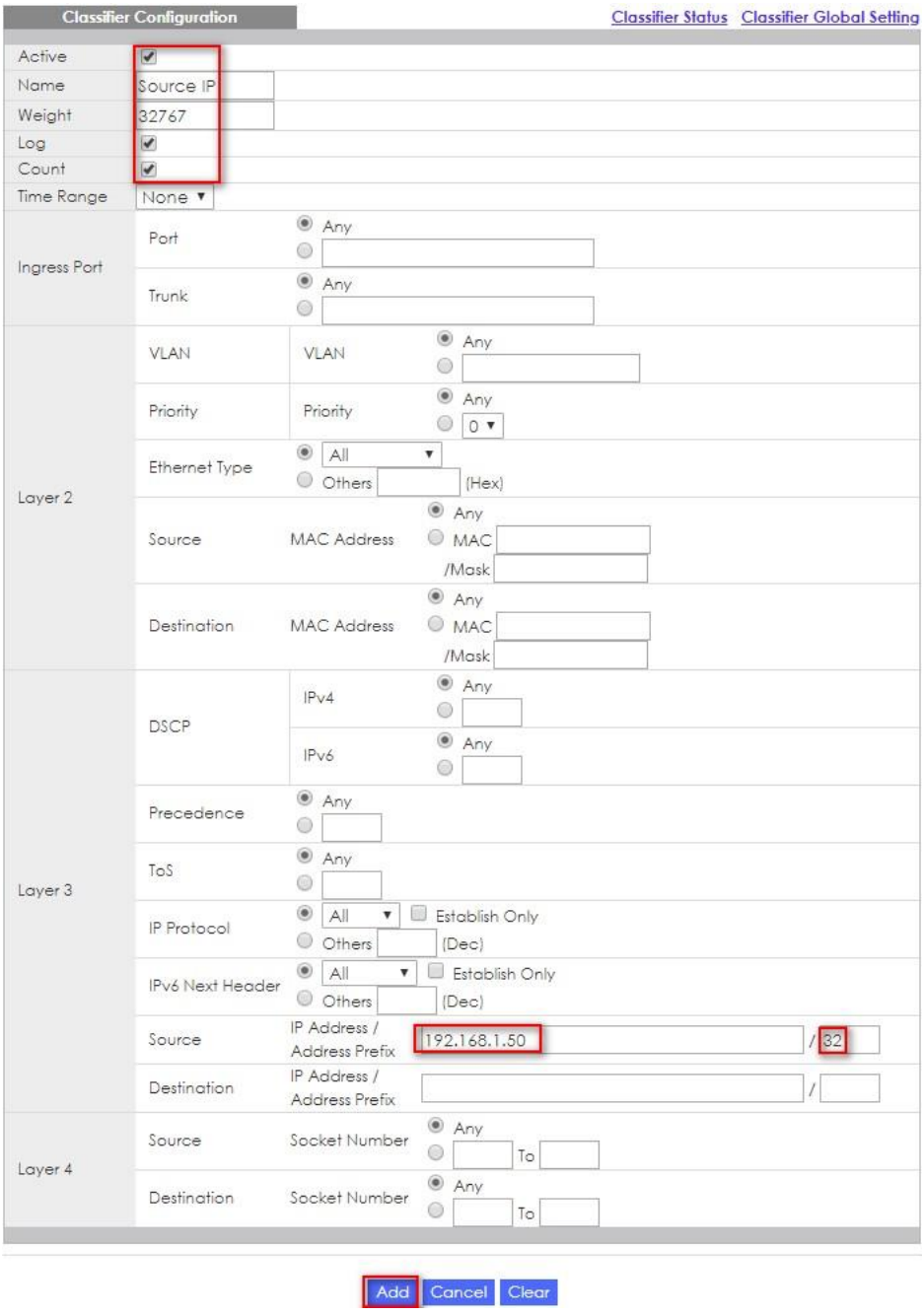
Настройте Match Order как “manual”, поставьте галочку в “Logging” и щелкните Apply.

4 **Advanced Application > Classifier > Classifier Configuration**.

Поставьте галочку в “Source IP” и задайте Weight 32767.

Поставьте галочку в “Log” и “Count”.

В Source IP введите IP-адрес PC 2 IP, задайте Address Prefix “32” и затем щелкните “Add” для создания.

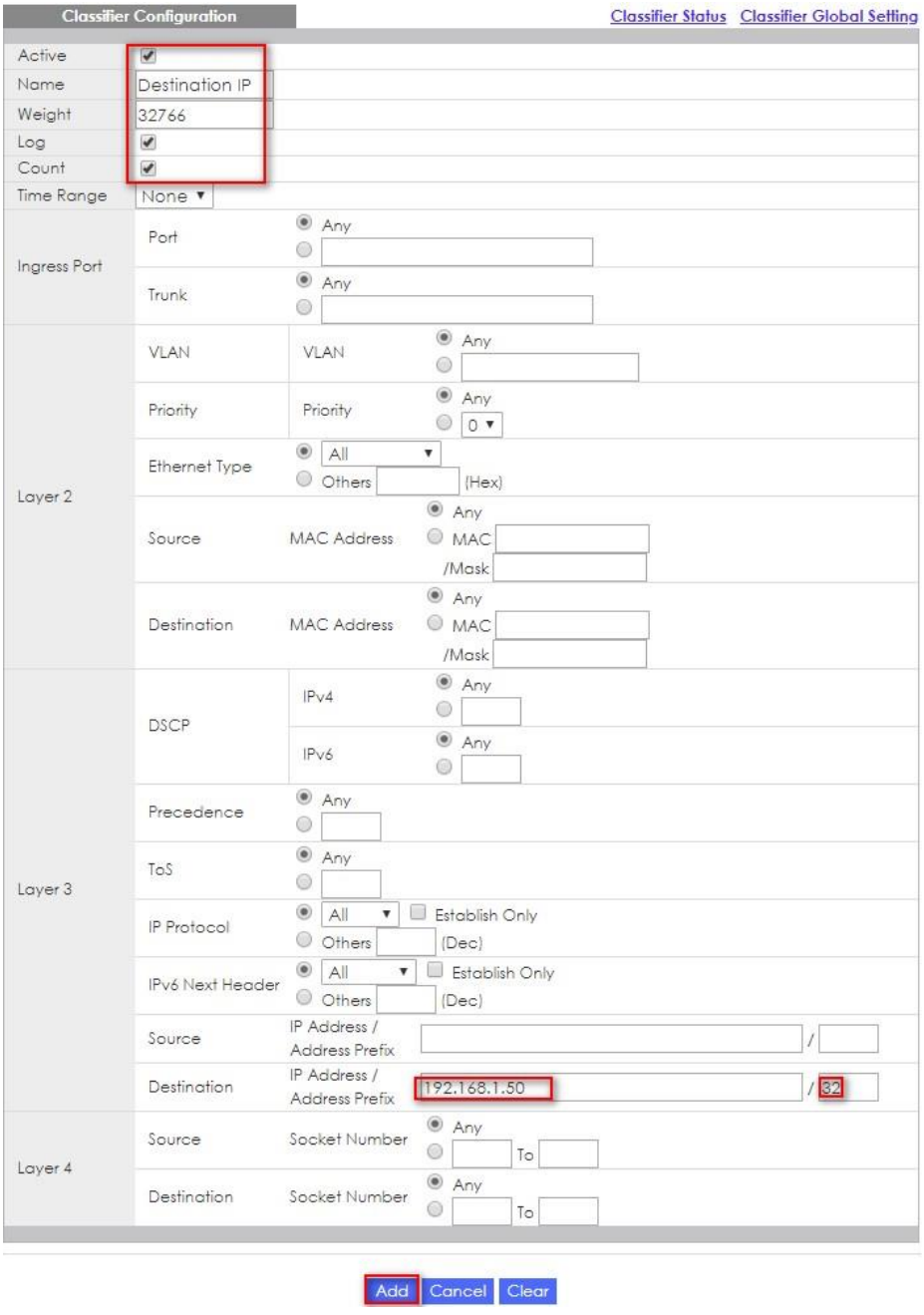

Classifier Configuration
Classifier Status
Classifier Global Setting
Active
Name
Source IP
Weight
32767
Log
Count
Time Range
None
Ingress Port
Port
Any
Trunk
Any
Layer 2
VLAN
VLAN
Any
Priority
Priority
Any
0
Ethernet Type
All
Others
(Hex)
Source
MAC Address
Any
MAC
/Mask
Destination
MAC Address
Any
MAC
/Mask
Layer 3
DSCP
IPv4
Any
IPv6
Any
Precedence
Any
ToS
Any
IP Protocol
All
Establish Only
Others
(Dec)
IPv6 Next Header
All
Establish Only
Others
(Dec)
Source
IP Address / Address Prefix
192.168.1.50
/ 32
Destination
IP Address / Address Prefix
/
Layer 4
Source
Socket Number
Any
To
Destination
Socket Number
Any
To
Add
Cancel
Clear

5 Advanced Application > Classifier > Classifier Configuration.

Поставьте галочку в Activate для Name “Destination IP” и Weight 32766.

Поставьте галочки в “Log” & “Count”.

В Destination IP address введите IP-адрес PC 2, задайте Address Prefix “32” и затем щелкните “Add” для создания.

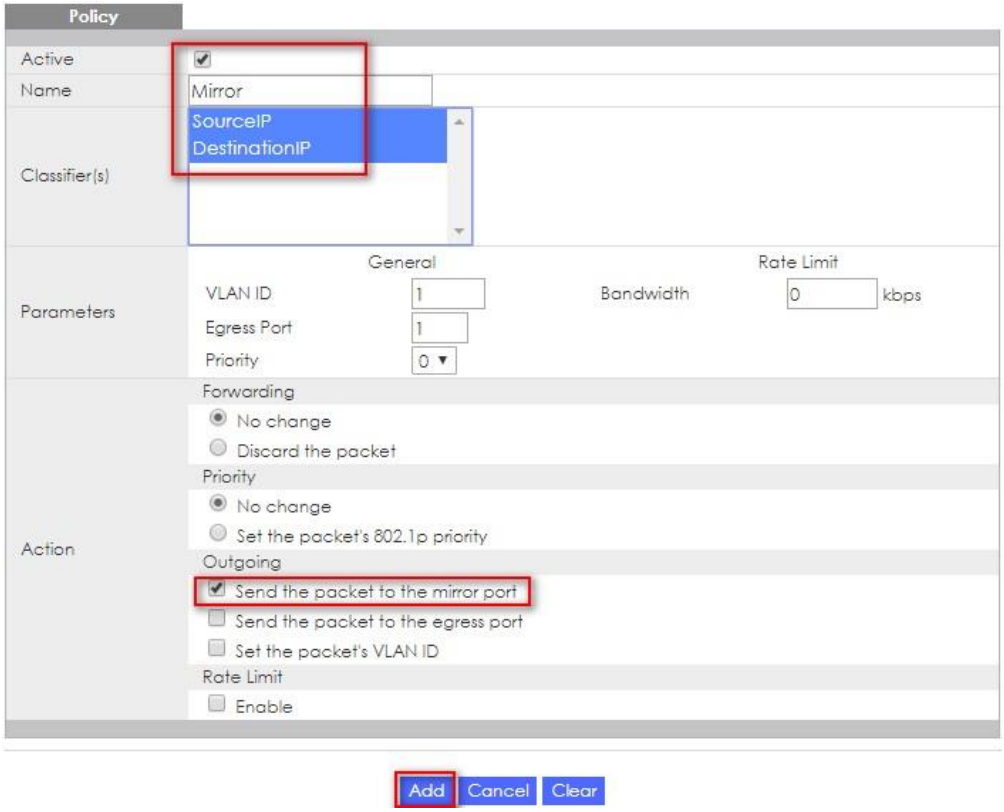


6 **Advanced Application > Policy Rule.**

Поставьте галочку в Activate для Name “Mirror”.

Выберите для classifiers как “Source IP”, так и “Destination IP”.

Поставьте галочку в “Send the packet to the mirror port” для Outgoing Action и щелкните “Add” для создания.



5.11.2 Проверка результатов

1 Перейдите в **Advanced Application > Classifier**.

Счетчик match count для обоих classifier должен увеличиваться пока PC 2 обменивается трафиком с Интернетом.

Go to

Classifier Status — Classifier Configuration

Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	Source IP	147	SrcIP = 192.168.1.50/32; count; log;
2	Yes	32766	Destination IP	104	DestIP = 192.168.1.50/32; count; log;

2 Использование Wireshark для перехвата пакетов к PC1.

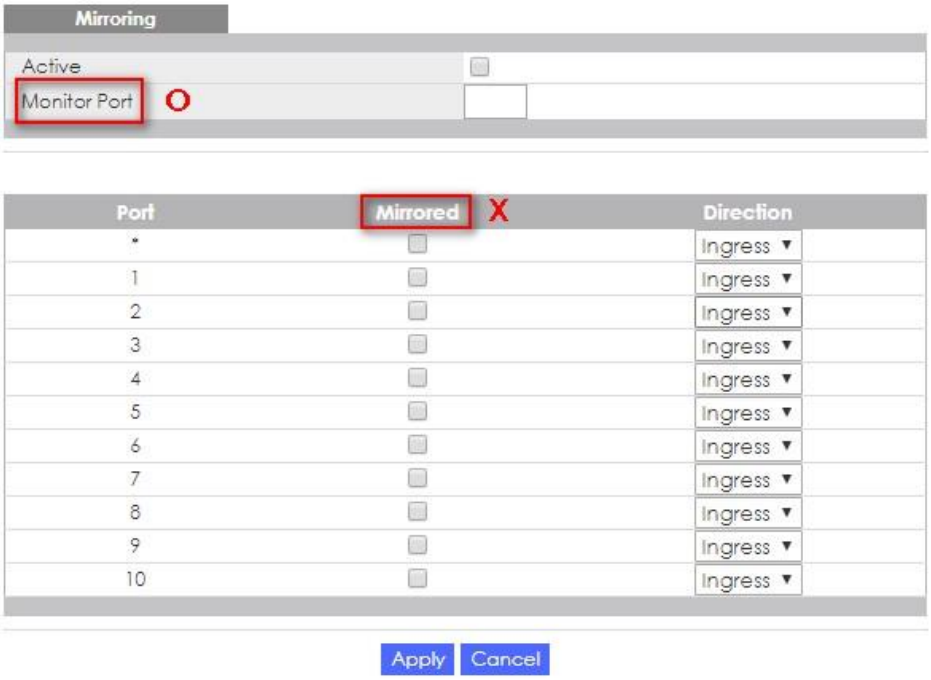
В таблицу будет зеркалированный трафик PC2.

Source	Destination	Protocol	Length	VID	Info
192.168.1.50	192.168.1.1	ICMP	74		Echo (ping) request
192.168.1.50	192.168.1.147	ICMP	74		Echo (ping) request
192.168.1.50	192.168.1.147	ICMP	74		Echo (ping) request
192.168.1.147	192.168.1.50	ICMP	74		Echo (ping) reply
192.168.1.147	192.168.1.50	ICMP	74		Echo (ping) reply

5.11.3 Почему это не работает

1 В **Advanced Application > Policy Rule**, в поле Outgoing Action стоит “Send the packet to the mirror port”.

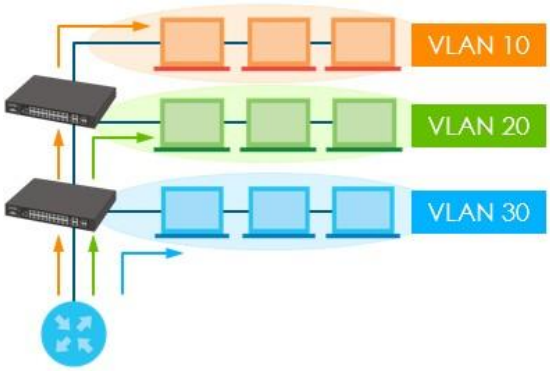
mirror port здесь означает [Monitor Port] но НЕ [Mirrored Port] в **Advanced Application > Mirroring**.



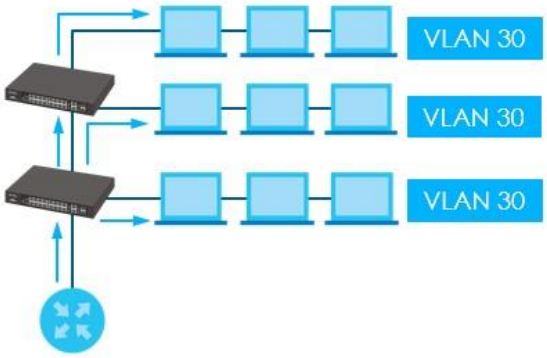
5.12 Как разделить трафик с помощью L2 Port Isolation

Часто требуется разделить в сети трафик разных клиентов и устройств.

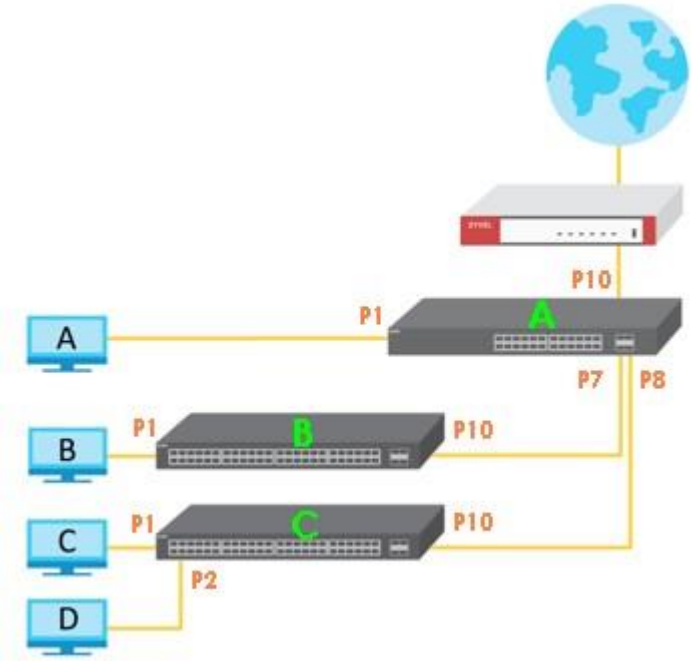
Самый простой способ изоляции трафика – это создание разных VLAN для разделения локальной сети LAN на разные домены broadcast.



Однако в некоторых ситуациях требуется изолировать трафик клиентов, которые относятся к одной подсети или VLAN, например, в сети отели гости могут использовать одну подсеть и VLAN для доступа к Интернету, но между собой они не могут обмениваться трафиком.



В коммутаторах Zyxel корпоративного класса используется функция “Port Isolation”, которая вызывается через **Advanced Application -> VLAN -> VLAN Configuration -> VLAN Port Setup** и разделяет трафик между портами, относящимися к одной VLAN.



Имя	Устройство	VLAN	IP-адрес	Маска подсети
Gateway	USG310	1	192.168.1.254	255.255.255.0
Switch A	GS2210-8	1	192.168.1.1	255.255.255.0
Switch B	GS2210-8	1	192.168.1.2	255.255.255.0
Switch C	GS2210-8	1	192.168.1.3	255.255.255.0
Client A	PC	1	192.168.1.101	255.255.255.0
Client B	PC	1	192.168.1.102	255.255.255.0
Client C	PC	1	192.168.1.103	255.255.255.0
Client D	PC	1	192.168.1.104	255.255.255.0

В этом сценарии, взятом из реального проекта, все клиентские ПК находятся в одной подсети и VLAN.

Изоляция L2 port isolation на коммутаторах позволяет:

1. Обеспечить доступ к Интернету для всех ПК.
2. Блокировку трафика между ПК.

Далее описана процедура внедрения изоляции портов L2 с помощью трех коммутаторов GS2210-8.

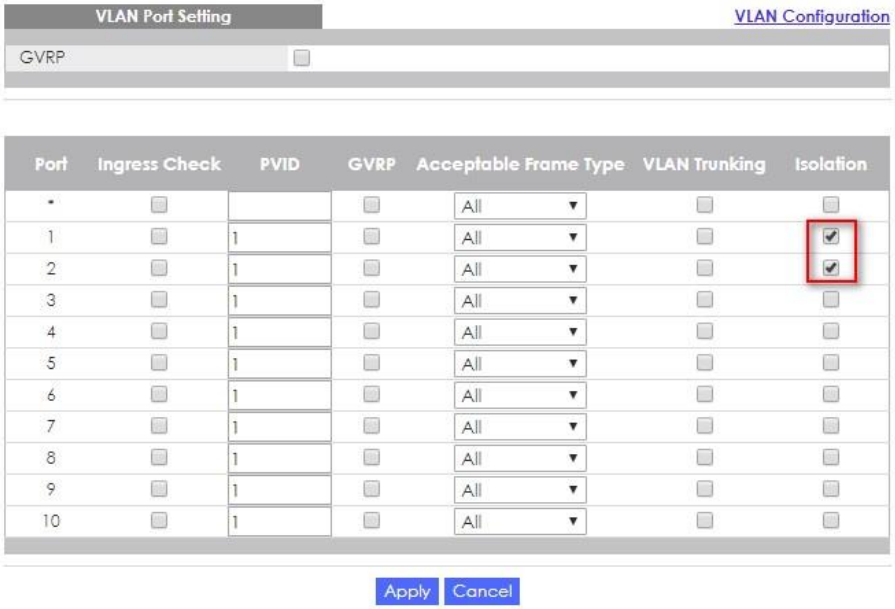
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети.

5.12.1 Настройка конфигурации коммутатора

1 Откройте web-интерфейс коммутатора Switch C.

2 Перейдите в Advance Application > VLAN > VLAN Configuration > VLAN Port Setup

Поставьте галочку напротив в Isolation для портов port 1 и 2.

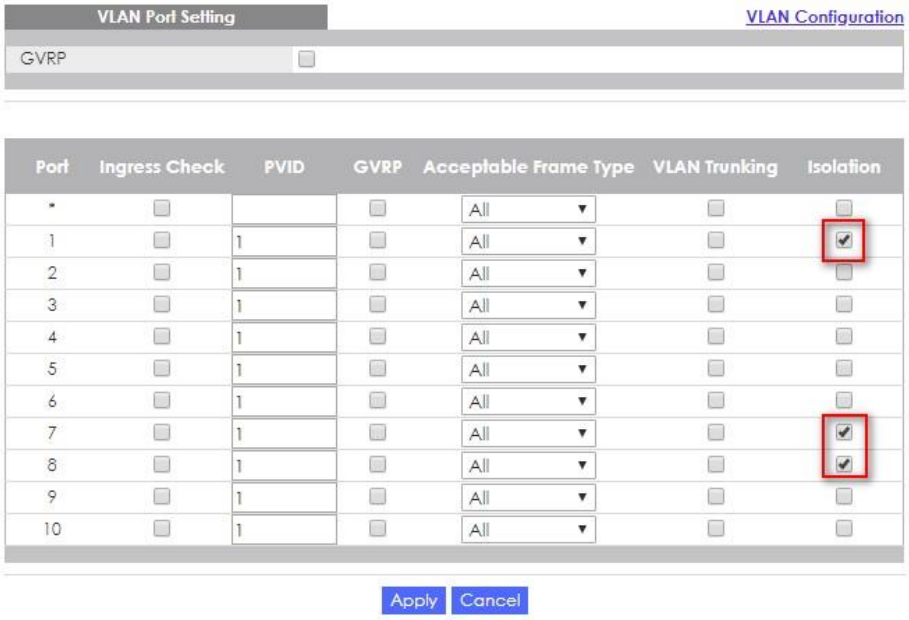


Примечание:
Если к коммутатору switch B подключено несколько клиентов, то его нужно настраивать точно также, как коммутатор Switch C. В данном случае к коммутатору switch B подключен только один клиент, поэтому такая настройка не нужна.

3 Откройте web-интерфейс коммутатора Switch A.

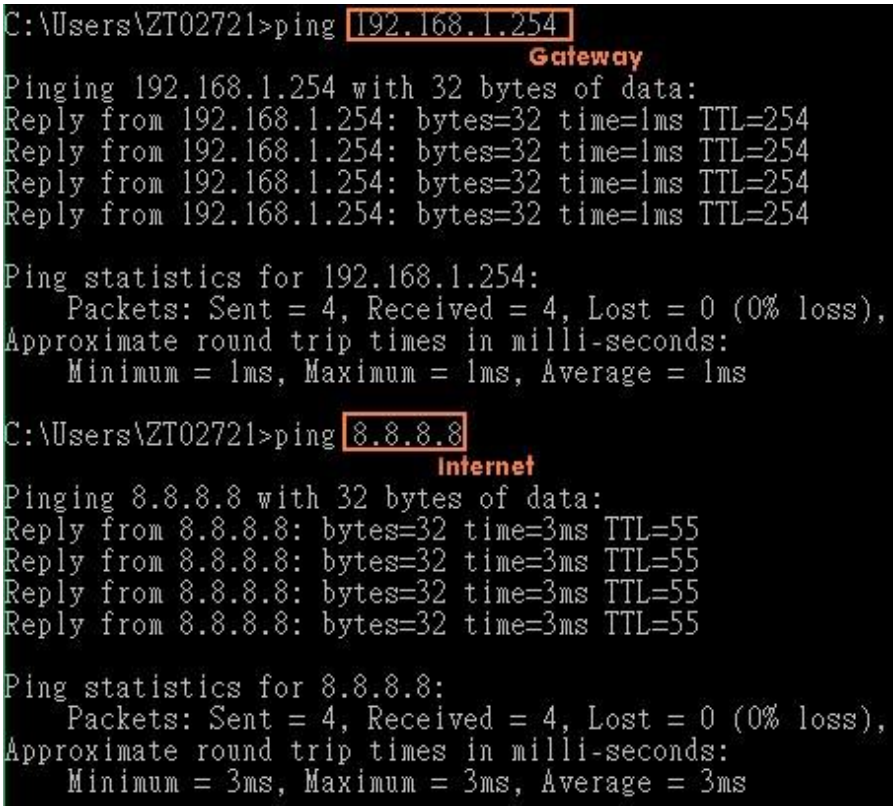
4 Перейдите в Advance Application > VLAN > VLAN Configuration > VLAN Port Setup

Поставьте галочку в port Isolation напротив портов 1, 7 и 8.

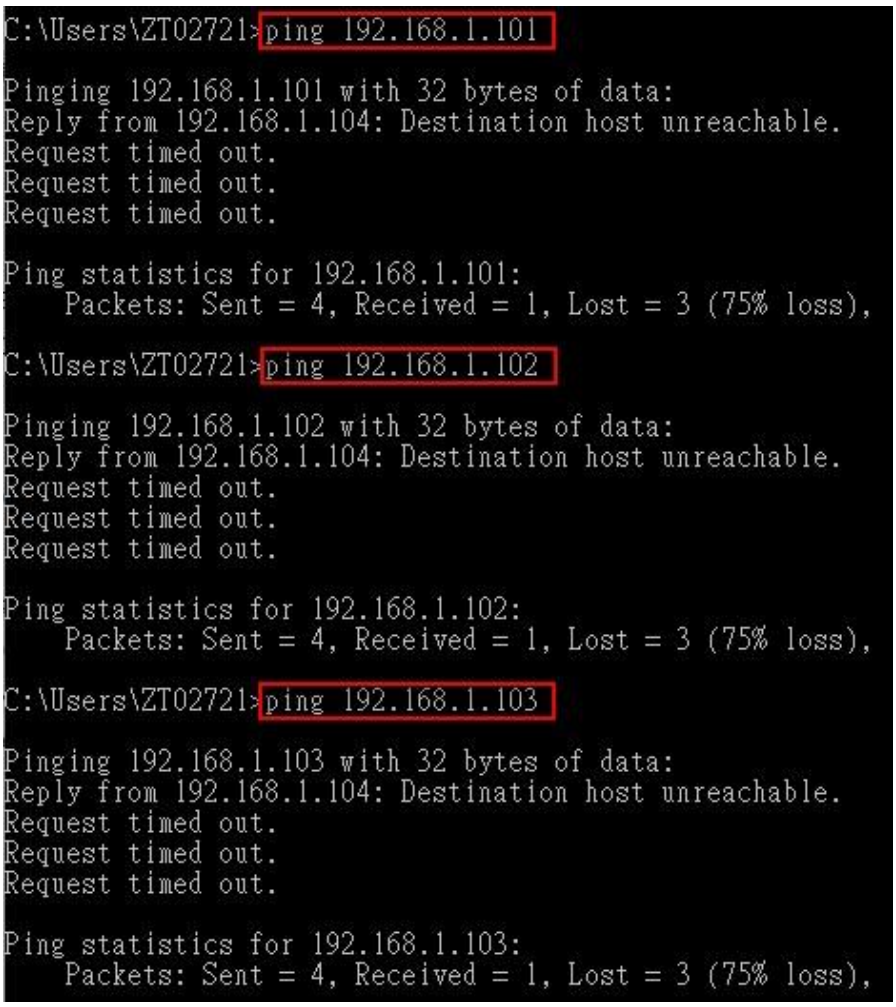


5.12.2 Проверка результатов

1 Client D может посылать ping на шлюз и у него есть доступ к Интернету.



2 У Client D нет доступа к клиентам Client A, B и C.



5.12.3 Почему это не работает

1 L2 port isolation работает для отдельных портов, но не для VLAN, поэтому если порты настроены как изолированные между собой, они не могут обмениваться трафиком даже если они в одной VLAN.

Внедрение VOIP

6.1 Как настроить VLAN для IP-телефона с помощью LLDP-MED

В этом примере показано, как с помощью LLDP-MED настроить VLAN ID для IP-телефонов. Любой IP-телефон, подключенный к коммутатору, будет назначен в определенную VLAN в зависимости от порта коммутатора. Далее мы расскажем о других способах пересылки трафика VOIP в определенную (голосовую) VLAN. С помощью VOIP администраторы могут присвоить повышенный приоритет голосовому трафику если сеть перегружена для гарантии высокого качества соединения для гарантии высокого качества телефонной связи по VOIP.

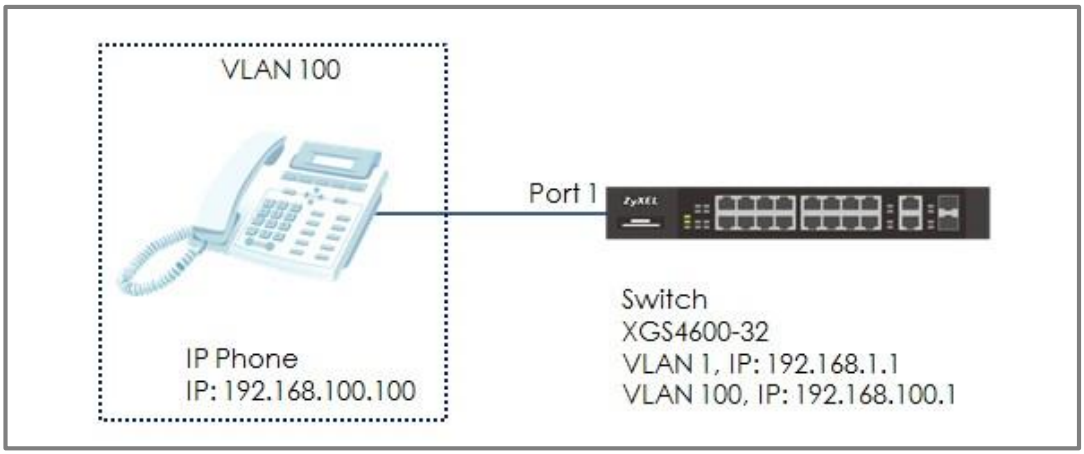


Иллюстрация 23 Использование LLDP-MED для настройки VLAN для IP-телефона

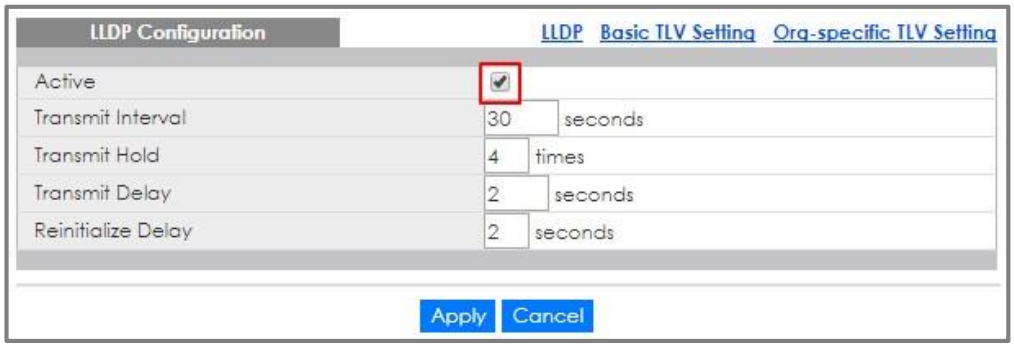
Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

6.1.1 Настройка VLAN для IP-телефона

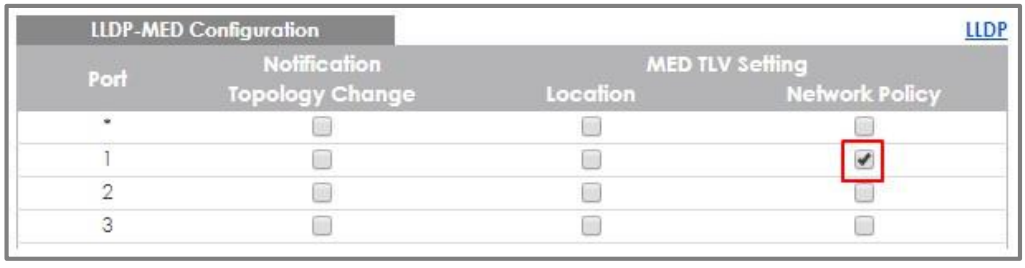
1 Настройте VLAN 100 на коммутаторе Switch (см. **2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN**). VLAN 100 создается для IP-телефона.

6.1.2 Настройка конфигурации коммутатора

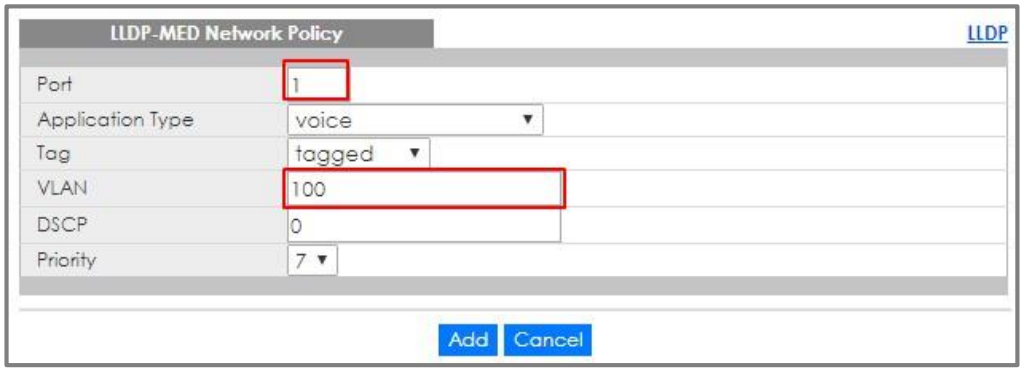
1 Откройте web-интерфейс и перейдите в **Menu > Advanced Application > LLDP > LLDP Configuration**. Для LLDP configuration в Active должна стоять галочка.



2 Откройте Web-интерфейс и перейдите в **Menu > Advanced Application > LLDP > LLDP-MED Configuration**. Поставьте галочку в “Network Policy” для port 1 (это порт, к которому подключен IP-телефон).

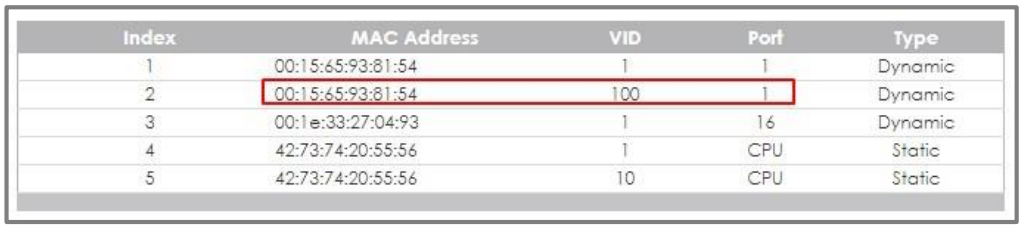


3 Откройте web-интерфейс и перейдите в **Menu > Advanced Application > LLDP > LLDP-MED Network Policy**. Введите номер порта 1 в поле port и введите номер VLAN, к которой будет подключен IP-телефон (VLAN 100), а в поле DSCP оставьте “0”. Затем назначьте приоритет Priority. Щелкните “Add”.



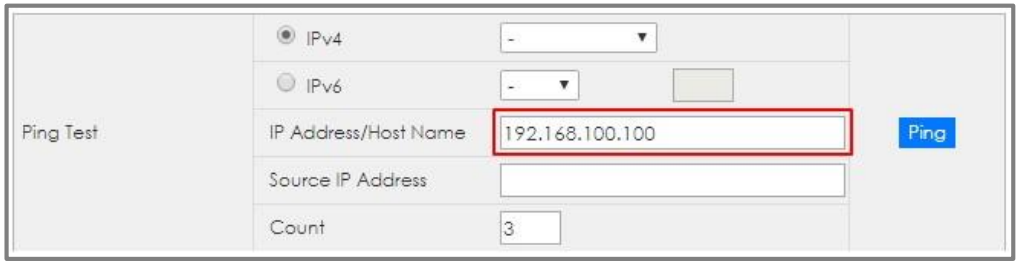
6.1.3 Проверка результатов the Result

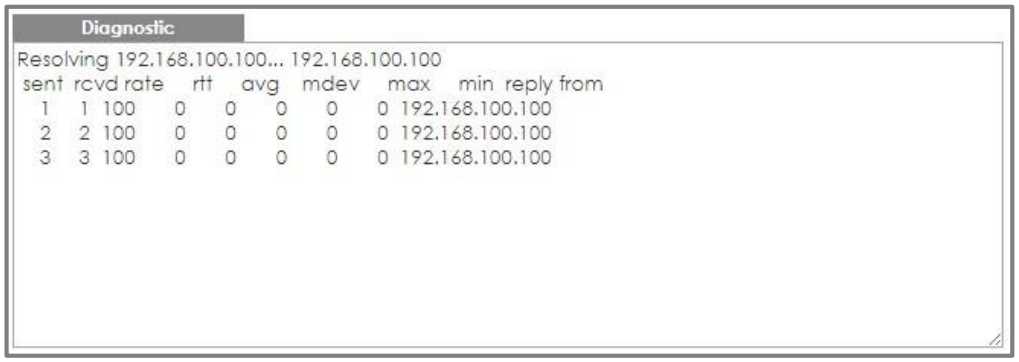
1 Перейдите в **Menu > Management > MAC Table > Search.** Посмотрите таблицу MAC-адресов. У IP-телефона MAC-адрес должен быть в VLAN 100.



Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	1	1	Dynamic
2	00:15:65:93:81:54	100	1	Dynamic
3	00:1e:33:27:04:93	1	16	Dynamic
4	42:73:74:20:55:56	1	CPU	Static
5	42:73:74:20:55:56	10	CPU	Static

2 Откройте web-интерфейс и перейдите в **Menu > Management > Diagnostic > Ping test**. Проверьте, что с коммутатора ping доходят до IP-телефона.





6.1.4 Почему это не работает

1 Если MAC-адрес IP-телефона не удалось назначить в VLAN 100, то проверьте, поддерживает ли IP-телефон LLDPMED. На коммутаторе должен быть включен LLDP-MED.

2 Поскольку IP-телефону назначен VLAN ID с помощью функции **Network Policy** в LLDP-MED, то голосовой трафик от коммутатора должен иметь тэг, соответствующий IP-телефону. Port 1 в VLAN 100 на коммутаторе должен быть **tagged out** (галочка в TX tagging) чтобы ping от коммутатора доходили до IP-телефона.

3 Поскольку IP-телефону назначен VLAN ID с помощью функции **Network Policy** в LLDP-MED, то нужно убедиться, что IP-телефон поддерживает LLDP-MED и у него включен LLDP-MED.

6.2 Как настроить коммутатор чтобы изолировать трафик VOIP от трафика данных

В этом примере показано, как с помощью Voice VLAN можно отделить трафик голосовой трафик untagged VOIP от трафика данных untagged data. В отличие от традиционных приложений VOIP функция Voice VLAN отделяет трафик VOIP и трафик данных как только трафик **доходит до коммутатора**., т.е. архитектура VLAN начинает работать на коммутаторе, а не на самом IP-телефоне.

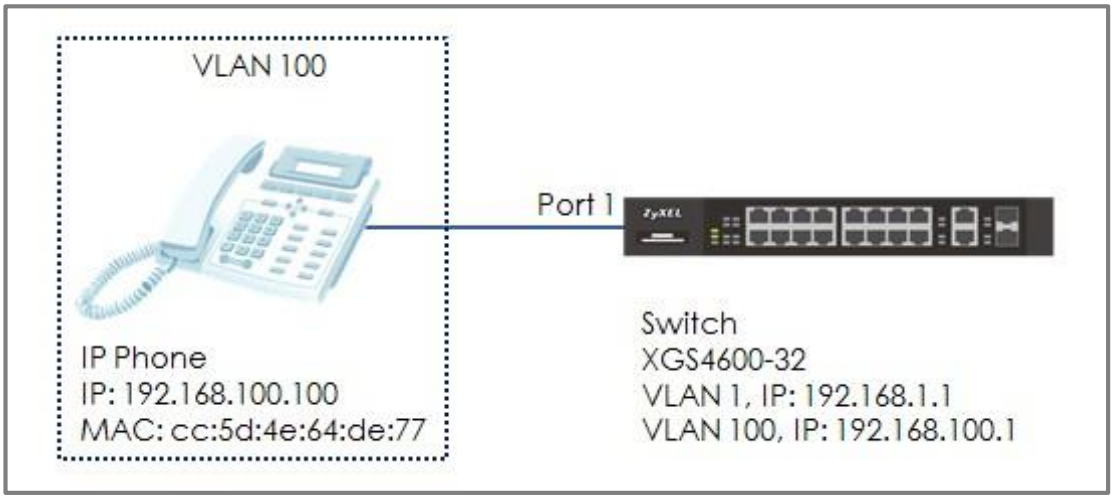


Иллюстрация 24 Настройка Voice VLAN для разделения трафика VOIP от трафика данных

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру, поэтому для вашей сети их нужно заменить на соответствующие реальные IP-адреса и маски подсети. В этом примере используется коммутатор XGS4600-32 (версия микропрограммы: V4.50).

6.2.1 Настройка VLAN 100 для IP-телефона

1 Настройте VLAN 100 на коммутаторе (см. **2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN**). VLAN 100 создана как Voice VLAN для IP-телефона.

6.2.2 Настройка Voice VLAN

1 Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Введите номер Voice VLAN (в данном примере это VLAN 100). Щелкните “Apply”.

2 Настройте OUI Setup: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Настройте адрес OUI. (можно ввести MAC-адрес.) В данном примере это cc:5d:4e:64:de:77. Настройте маску OUI как **ff:ff:ff**:00:00:00. Щелкните “Add”.

Примечание:
В результате этих настроек коммутатор будет направлять в Voice VLAN трафик от всех устройств, у которых MAC-адрес от cc:5d:4e:**00:00:00** и до cc:5d:4e:**ff:ff:ff**.

6.2.3 Проверка результатов

1 Перейдите в **Menu > Management > MAC Table > Search.** Убедитесь, в таблице MAC-адресов IP Phone назначен в VLAN 100.

Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	42:73:74:20:55:56	1	CPU	Static
3	42:73:74:20:55:56	100	CPU	Static
4	cc:5d:4e:64:de:77	100	1	Dynamic

2 Откройте Web-интерфейс и перейдите в **Menu > Management > Diagnostic > Ping test**. Убедитесь, что с коммутатора ping доходит до IP-телефона.

Diagnostic

```
Resolving 192.168.100.100... 192.168.100.100
 sent  rcvd rate    rtt    avg    mdev    max    min  reply from
    1     1  100      0      0       0      0      0  192.168.100.100
    2     2  100      0      0       0      0      0  192.168.100.100
    3     3  100      0      0       0      0      0  192.168.100.100
```

Diagnostic

```
Resolving 192.168.100.100... 192.168.100.100
 sent  rcvd rate    rtt    avg    mdev    max    min  reply from
    1     1  100      0      0       0      0      0  192.168.100.100
    2     2  100      0      0       0      0      0  192.168.100.100
    3     3  100      0      0       0      0      0  192.168.100.100
```

6.2.4 Почему это не работает

1 Если IP-телефона нет в voice VLAN, то проверьте его MAC-адрес. Обычно MAC-адрес указан на наклейке в основании IP-телефона. Этот MAC-адрес должен попадать в диапазон настроек Voice VLAN OUI.

2 Возможно, у IP-телефона неправильные настройки. Нужно проверить:

a. Если у IP-телефона VLAN **включена** и VLAN для него - это **Voice VLAN**: Коммутатор сохранит настройки Voice VLAN и присвоит повышенный приоритет IP-телефону. IP-телефон будет обрабатывать только тэгированный трафик. В данном случае порт port 1 в VLAN 100 на коммутаторе нужно настроить как **tagged out** (поставить галочку в поле TX tagging).

b. Если на IP Phone **включена** VLAN, но эта VLAN – не **Voice VLAN** коммутатора, то коммутатора **не будет** применять изменения трафика VOIP для IP-телефона.

Если на IP Phone **выключена** VLAN, то коммутатор назначит Voice VLAN и повышенный приоритет трафику VOIP IP-телефона и в результате IP-телефон будет посылать и получать только нетегированный трафик(**untagged)**. В данном случае порт port 1 в VLAN 100 на коммутаторе нужно настроить как **untagged out** (убрать галочку в поле TX tagging).

6.3 Как настроить конфигурацию коммутатора чтобы улучшить качество голосового трафика

В этом примере показано, как с помощью Voice VLAN можно улучшить качество голосового трафика. Как уже говорилось в 6.2, Voice VLAN не только группирует голосовой трафик в выделенную VLAN, но и назначает этому трафику повышенный приоритет. Приоритет Voice VLAN priority можно назначать как тегированному, так и нетегированному трафику.

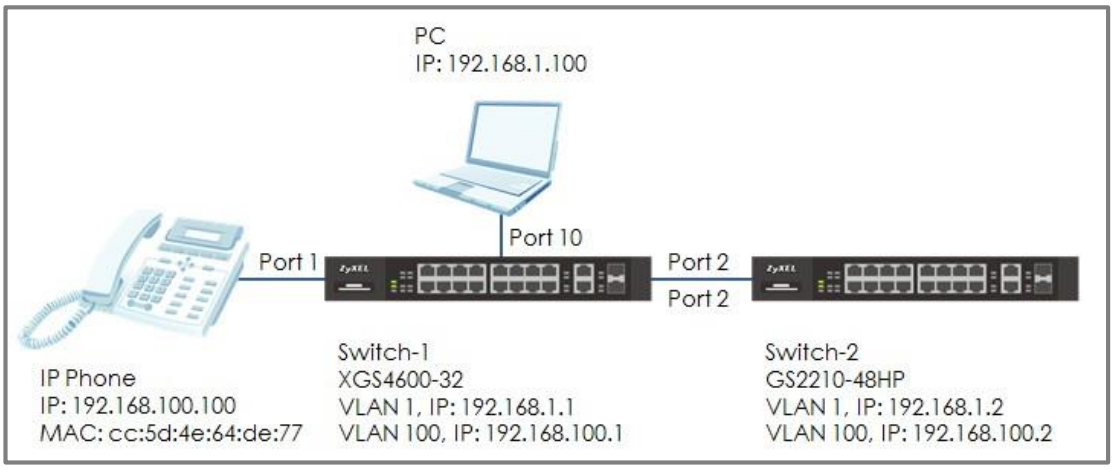


Иллюстрация 25 Настройка Voice VLAN для отделения трафика VOIP traffic от трафика данных

Примечание:
Все сетевые IP-адреса и маски подсети относятся только к этому примеру. Их нужно заменить на реальные IP-адреса и маски подсети вашей сети. В этом примере используется XGS4600-32 (Firmware Version: V4.50) и GS2210-48HP (Firmware Version: V4.30).

6.3.1 Настройка VLAN для голосового трафика

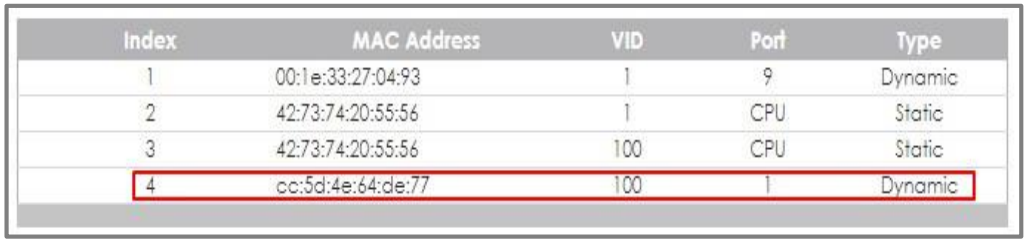
1 Настройте VLAN 100 на коммутаторах Switch-1 и Switch-2. (см. **2.1 Как настроить коммутатор чтобы изолировать трафик разных отделов с помощью VLAN**). VLAN 100 создана для Voice VLAN. Убедитесь, что

устройства в in VLAN 100 могут обмениваться данными через коммутаторы Switch-1 и Switch-2.

6.3.2 Настройка Voice VLAN

1 Откройте web-интерфейс и перейдите в: **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Введите номер в поле Voice VLAN. В данном примере это VLAN 100. Назначьте приоритет трафику, в данном случае priority=**6**. Щелкните “Add”.

2 Настройте OUI Setup: Откройте web-интерфейс и перейдите в **Menu > Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup**. Настройте адрес OUI. (можно ввести MAC-адрес, в данном примере cc:5d:4e:64:de:77). Введите в поле OUI **ff:ff:ff**:00:00:00. Щелкните “Add”.

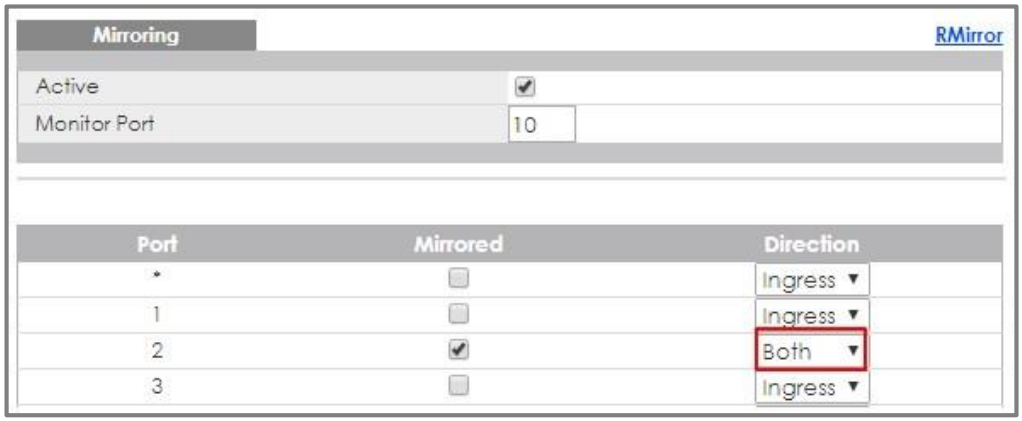


Index	MAC Address	VID	Port	Type
1	00:1e:33:27:04:93	1	9	Dynamic
2	42:73:74:20:55:56	1	CPU	Static
3	42:73:74:20:55:56	100	CPU	Static
4	cc:5d:4e:64:de:77	100	1	Dynamic

Примечание:
Коммутатор будет направлять весь трафик от устройств, у которых MAC-адрес в диапазоне cc:5d:4e:**00:00:00** - cc:5d:4e:**ff:ff:ff** , в Voice VLAN.

6.3.3 Настройка зеркалирования для проверки результатов

1 Для проверки результатов мы с помощью зеркалирования проверяем, получили ли пакеты тот приоритет, который назначен. Откройте web-интерфейс и перейдите в **Menu > Advanced Application > Mirroring**. Поставьте галочку в поле “Active”. Введите в поле Monitor port номер порта, используемого для мониторинга трафика. Поставьте галочку напротив порта, который нужно зеркалировать (в данном примере это порт port 2). В Direction выберите Both”. Щелкните “Apply”.

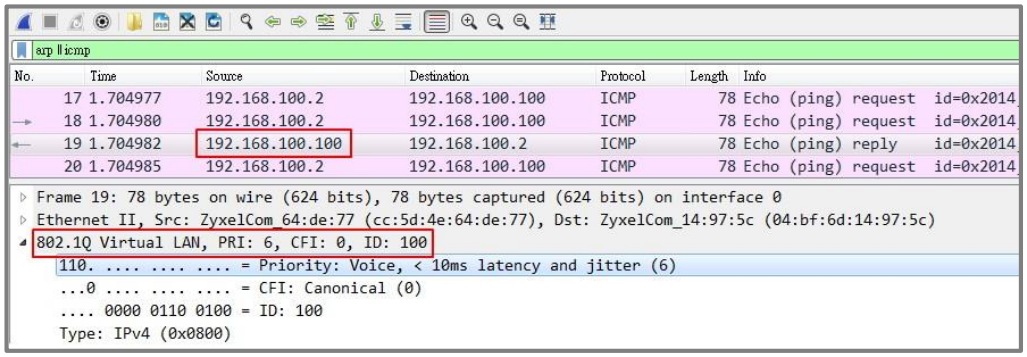


6.3.4 Проверка результатов

1 Подключите PC к коммутатору Switch-1. Запустите **Wireshark** для мониторинга пакетов. Настройте фильтр на “**arp || igmp**”.

2 Проверьте, доходят ли ping с коммутатора Switch-2 на IP-телефон: Откройте Web-интерфейс и перейдите в **Menu > Management > Diagnostic > Ping test**. ping с коммутатора Switch-2 успешно доходят до IP-телефона.

3 Проверьте пакеты с IP Phone (**192.168.100.100**) на Wireshark. В заголовке VLAN должно быть указана, что назначен приоритет Voice VLAN priority “6”.



6.3.5 Почему это не работает

1 Если приоритет не соответствует настойкам voice VLAN, то проверьте MAC-адрес IP-телефона. Обычно MAC-адрес указан на наклейке в основании IP-телефона. Этот MAC-адрес должен попадать в диапазон настроек Voice VLAN OUI.

3 Возможно, у IP-телефона неправильные настройки. Нужно проверить:

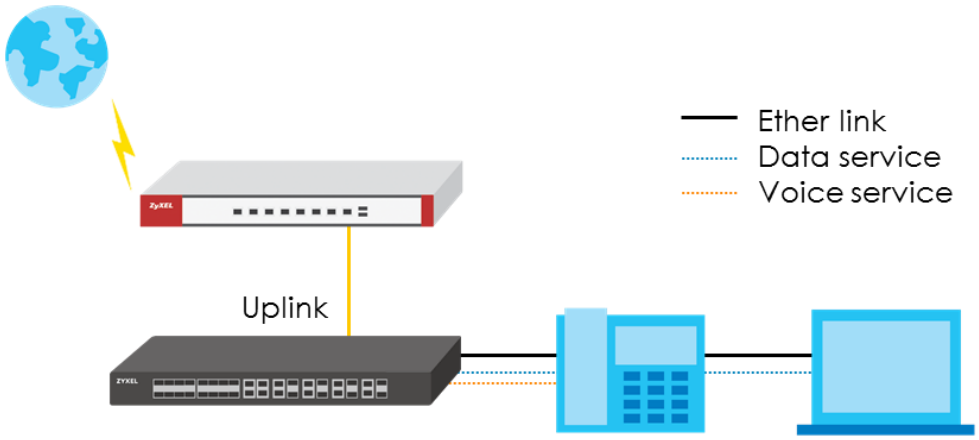
a. Если у IP-телефона VLAN **включена** и VLAN для него - это **Voice VLAN**: Коммутатор сохранит настройки Voice VLAN и присвоит повышенный приоритет IP-телефону. IP-телефон будет обрабатывать только тэгированный трафик. В данном случае порт port 1 в VLAN 100 на коммутаторе нужно настроить как **tagged out** (поставить галочку в поле TX tagging).

b. Если на IP Phone **включена** VLAN, но эта VLAN – не **Voice VLAN** коммутатора, то коммутатора **не будет** применять изменения трафика VOIP для IP-телефона.

3 Некоторые сетевые карты компьютеров NIC не поддерживают использование информации 802.1Q (VLAN). Если в Wireshark не выводится информация 802.1Q, то попробуйте использовать другую сетевую карту NIC, например, сетевой адаптер с интерфейсом USB.

6.4 Как настроить Voice VLAN на коммутаторе Zyxel

Voice VLAN использует для отделения пакетов голосового трафика от пакетов других сервисов. Для улучшения качества телефонной связи голосовым пакетам назначается повышенный приоритет.



IP-телефоны сегодня используются во многих офисах, поэтому при проектировании офисной сети важно обеспечить повышенный приоритет для голосового трафика.

Обычно IP-телефон подключается кабелем к коммутатору, а к другому порту коммутатора подключены настольные ПК или ноутбуки. Таким образом, коммутатор работает как мост между коммутатором и ПК, поэтому нужно с помощью Voice VLAN отделить пакеты голосового трафика от IP-телефона от пакетов с данными от ПК и присвоить им более высокий приоритет.

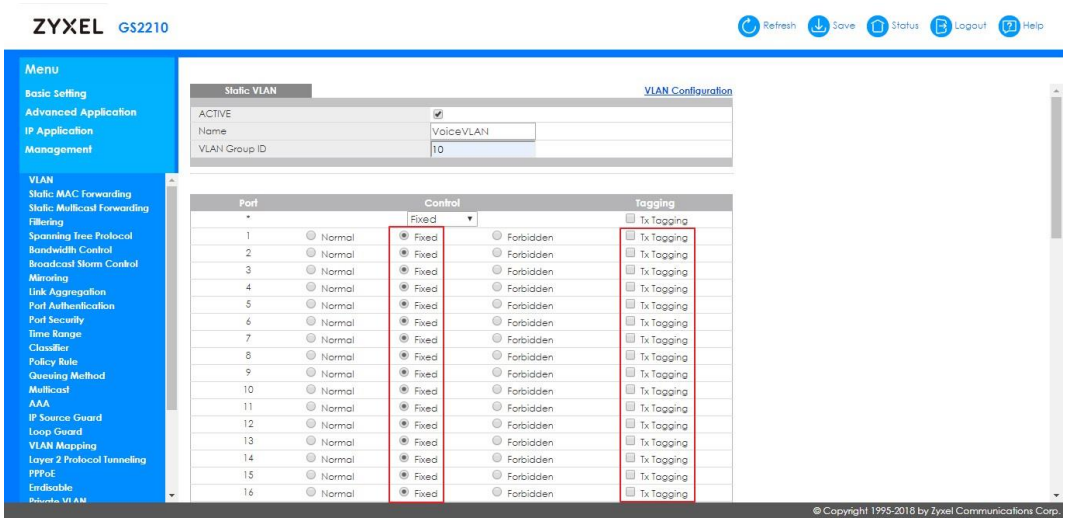
Ниже приведены инструкции по разделению трафика IP-телефона и PC без использования разных тегов VLAN для них. Коммутатор будет добавлять отдельные тэги VLAN для пакетов голосового трафика и пакетов данных при их получении и затем перенаправлять их в аплинк.

6.4.1 Настройка конфигурации

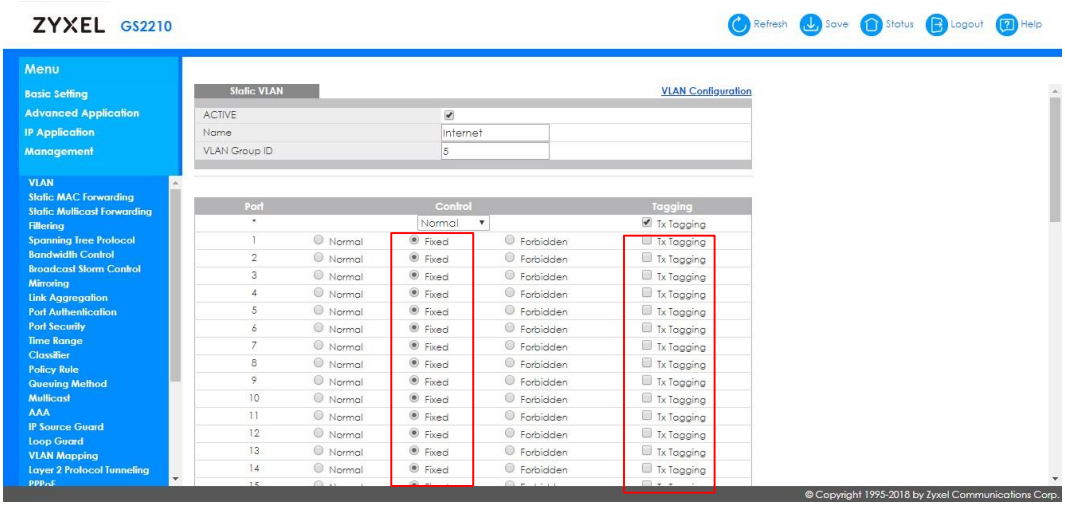
Следующую процедуру настройки конфигурации коммутатора можно применять к смарт-коммутаторам серии GS1920 и более мощным моделям коммутаторов Zyxel.

Создайте интерфейсы VLAN

Создайте VLAN для передачи пакетов голосового трафика, выберите порты, к которым подключены IP-телефоны, уберите галочки в поле Tx tagging чтобы не на нужно было настраивать VLAN на каждом IP-телефоне по отдельности.

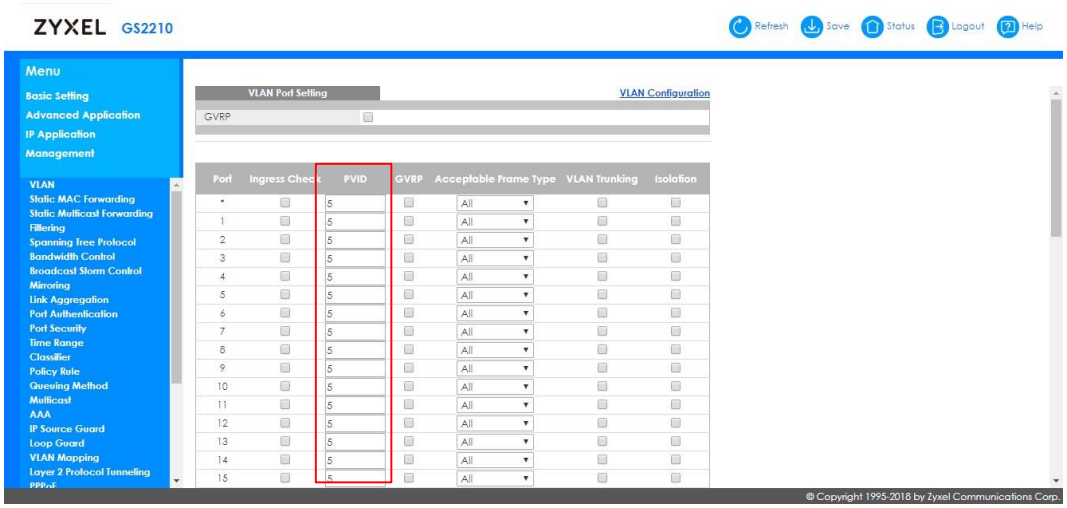


Создайте другую VLAN для передачи пакетов с данными, уберите галочки в Tx tagging.



Для порта uplink включите Tx Tagging для передачи пакетов с тегами VLAN.

Настройте PVID чтобы отделить пакеты с данными от пакетов с голосовым трафиком. Номер PVID должен совпадать с номером VLAN, созданной для передачи пакетов с данными.

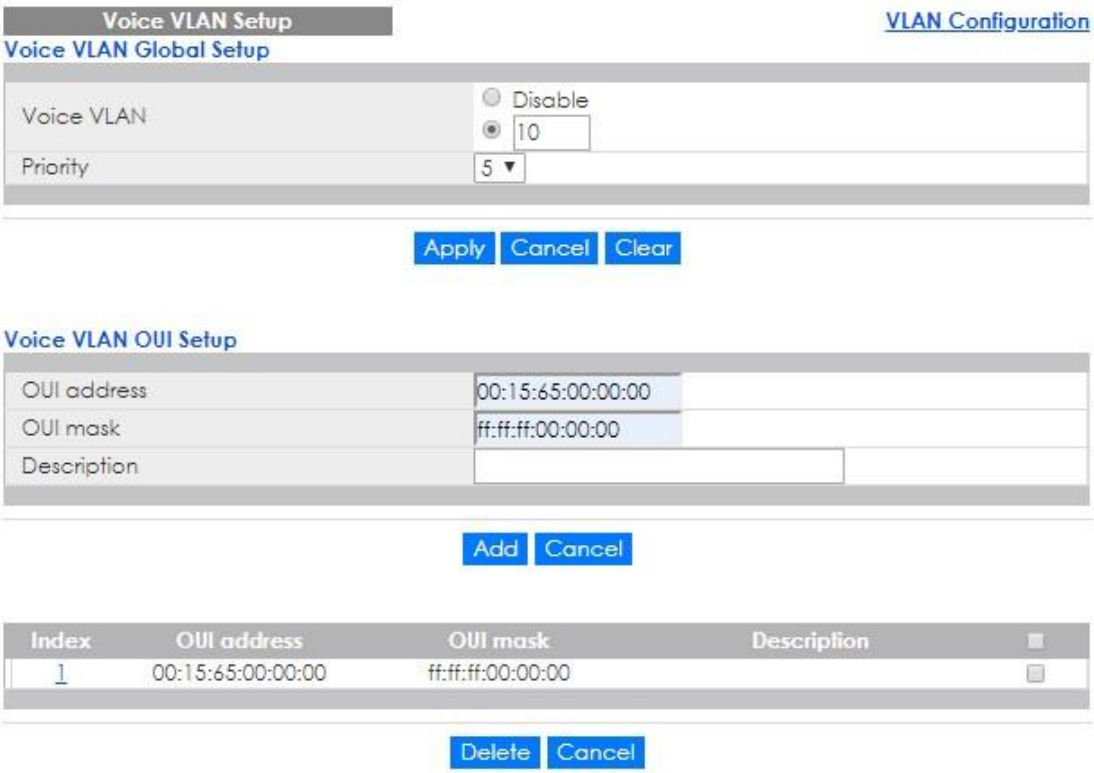


После настройки PVID для пакетов с данными нужно настроить в коммутаторе функцию “Voice VLAN” для идентификации пакетов с голосовым трафиком.

Настройка Voice VLAN

Настройте номер Voice VLAN и приоритет чтобы у пакетов голосового трафика был более высокий приоритет. Номер Voice VLAN должен совпадать с номером VLAN, которая раньше для передачи голосового трафика.

Задайте адрес OUI addresses. OUI – это относящиеся к вендору первые 3 байта а MAC-адреса. По определенному MAC-адресу IP-телефона коммутатор может правильно идентифицировать голосовой трафик. Коммутатор Zyxel поддерживает до шести вендоров OUI.



Примечание:

В этой инструкции описывается простое конфигурирование Voice VLAN на автономном коммутаторе серии GS1920 или более мощной. Такая настройка конфигурации коммутатора позволяет без какой-либо дополнительной настройки IP-телефонов построить отдельные VLAN и внедрить правила передачи данных и голоса, при которых голосовой трафик получает более высокий приоритет.

6.4.2 Проверка результатов

Перейдите в VLAN Configuration чтобы проверить статус VLAN. Для VLAN 10 статус должен быть Voice VLAN.

VLAN Status | VLAN Configuration

VLAN Search by VID | Search

The Number of VLAN: 3.

Index	VID	Elapsed Time	Status
1	1	48:16:52	Static
2	5	0:06:11	Static
3	10	0:06:29	Voice

Убедитесь, что в таблице mac-адресов mac-адресу IP-телефона соответствует VLAN 10, а mac-адресу PC соответствует VLAN 5.

```
GS2210# show mac a a
  Port        VLAN ID          MAC Address              Type
  13          10               00:15:65:93:81:54        Dynamic
  13          5                00:1e:33:28:0a:84        Dynamic
```

Index	MAC Address	VID	Port	Type
1	00:15:65:93:81:54	10	13	Dynamic
2	00:1e:33:28:0a:84	5	13	Dynamic
3	38:d5:47:8d:0b:91	1	24	Dynamic

6.4.3 Почему это не работает

Если IP-телефон не работает, то проверьте следующие настройки:

a. Если у IP-телефона VLAN **включена** и VLAN для него - это **Voice VLAN**: Коммутатор сохранит настройки Voice VLAN и присвоит повышенный приоритет IP-телефону. IP-телефон будет обрабатывать только тэгированный трафик. В данном случае порт port 1 в VLAN 100 на коммутаторе нужно настроить как **tagged out** (поставить галочку в поле TX tagging).
b. Если на IP Phone **включена** VLAN, но эта VLAN – не **Voice VLAN** коммутатора, то коммутатора **не будет** применять изменения трафика VOIP для IP-телефона.
c. Если у IP-телефона VLAN выключена: коммутатор присвоит Voice VLAN и настройки приоритет VOIP-трафику IP-телефона. В результате IP-телефон будет посылать и принимать только нетегированный трафик (untagged). В этом случае порт port 1 в VLAN 100 надо настроить как untagged out (убрать галочку в поле TX tagging).