Адрес: Россия, 124460, Москва, Зеленоград, Южная промзона, проезд 4806, д.4, стр.3, ЗАО "Ангстрем-Телеком"
Тел./Факс: (499) 731-14-16, (499) 731-37-64, (499) 731-09-76
E-mail: AKT@angtel.ru
http://www.angtel.ru

Коммутаторы доступа серии «Топаз»

Руководство пользователя
ЯКГШ.465615.003Д3.1-10

Редакция 1.2, 10.02.2016

Содержание

1 Введение

Настоящее руководство по конфигурированию распространяется на коммутаторы уровня доступа Ethernet L2+ серии «Топаз».

Руководство подробно разъясняет на примерах необходимые настройки для работы устройства в тех или иных сервисных моделях, обеспечения безопасности, управления и мониторинга. В целом, CLI ПО коммутатора является CISCO-like интерфейсом, что позволяет быстро освоить работу с ним большому количеству специалистов в области построения и эксплуатации сетей.

2 Модели обслуживания

В настоящее время на сетях различных провайдеров используются две основные сервисные модели для предоставления услуг абоненту: VLAN на пользователя и VLAN на сервис. Сервисы включают в себя Интернет, IPTV и IP-телефонию.

В каждой из модели используются один или два служебных VLAN: VLAN для управления и VLAN для динамического назначения IP-адресов STB-приставкам.

Модель VLAN на пользователя предполагает, что все сервисы, за исключением IPTV, предоставляются в каждом пользовательском VLAN изолированно друг от друга.

В модели VLAN на сервис для каждой из трех услуг резервируется отдельный VLAN, а все пользователи получают сервисы из этих VLAN. Изоляция абонентов между собой обеспечивается в этом случае технологией Protected Port или Private VLAN.

Помимо этого, сети доступа строятся по одной из двух основных топологий: кольцо или звезда. В кольце, как и в звезде, для дополнительного резервирования и увеличения пропускной способности может применяться технология агрегирования каналов.

Поддерживаемые коммутатором функции позволяют интегрировать устройства в обе из этих моделей.

2.1 VLAN на абонента

Конфигурация коммутатора для модели VLAN per User для 3-х абонентов:

```
bridge multicast filtering
vlan database
vlan 2-25,30,40
exit
ip igmp snooping vlan 30 multicast-tv 0.0.0.0
ip igmp snooping
ip igmp snooping vlan 2
ip igmp snooping vlan 3
ip igmp snooping vlan 4
ip igmp snooping vlan 30
!
interface vlan 2
name VLAN_USER_P1
!
interface vlan 3
name VLAN_USER_P2
!
interface vlan 4
name VLAN_USER_P3
!
interface vlan 40
name Management
ip address 192.168.1.12 255.255.255.0
ipv6 address 2001::12/64
!
interface fastethernet1/1/1
bridge multicast unregistered filtering
```

```
switchport access vlan 2
switchport access multicast-tv vlan 30
!
interface fastethernet1/1/2
bridge multicast unregistered filtering
switchport access vlan 3
switchport access multicast-tv vlan 30
!
interface fastethernet1/1/3
bridge multicast unregistered filtering
switchport access vlan 4
switchport access multicast-tv vlan 30
!
interface gigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 2-25,30,40
```

2.2 VLAN на сервис

В этой модели, представленной на рисунке 2.2.1, IPTV-трафик с помощью технологии MVR помещается в Multicast TV VLAN 200; Internet (PPPoE)-трафик с помощью функции Protocol Based VLAN в VLAN 3099; трафик STB (кроме IGMP) с помощью функции MAC Based VLAN – в VLAN 601; трафик IP-телефонии с помощью функции Subnet Based VLAN – в VLAN 4044. Весь оставшийся трафик помещается в VLAN 1000.

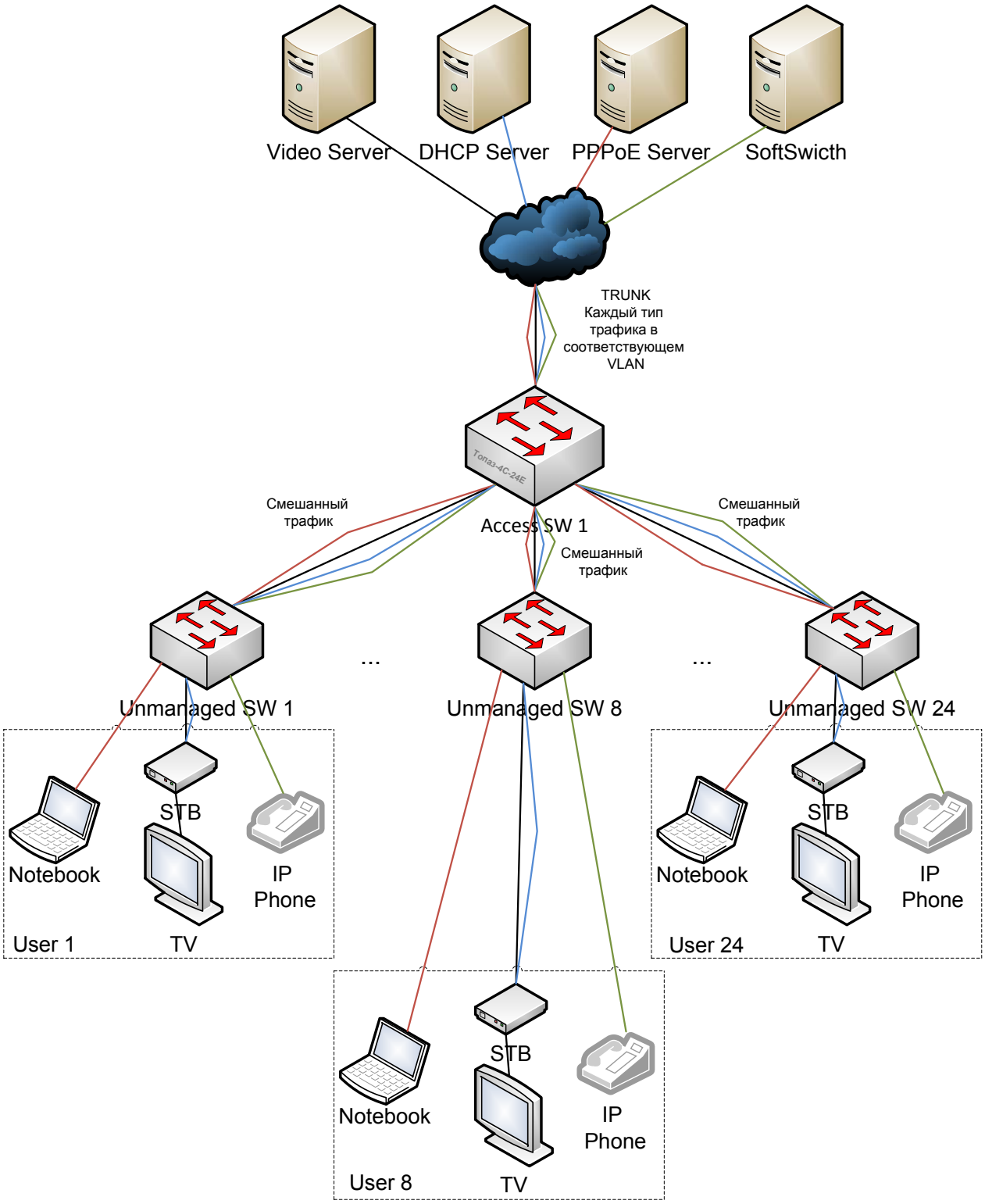

Рис. 2.2.1. Схема модели VLANна сервис

Ниже представлена конфигурация коммутатора для модели VLAN per Service для 3-х абонентов:

```
bridge multicast filtering
vlan database
vlan 40,200,601,1000,3099,4044
exit
vlan database
map protocol 8863 ethernet protocols-group 3
map protocol 8864 ethernet protocols-group 3
exit
```

```
vlan database
map mac 50:af:64:00:00:00 24 macs-group 1
map mac 50:af:65:00:00:00 24 macs-group 1
map mac 50:af:66:00:00:00 24 macs-group 1
map mac 50:af:67:00:00:00 24 macs-group 1
map mac 50:af:68:00:00:00 24 macs-group 1
map mac 50:af:69:00:00:00 24 macs-group 1
map mac 50:af:70:00:00:00 24 macs-group 1
map mac 50:af:71:00:00:00 24 macs-group 1
map mac 50:af:72:00:00:00 24 macs-group 1
map mac 50:af:73:00:00:00 24 macs-group 1
exit
vlan database
map subnet 192.170.1.0 24 subnets-group 2
exit
ip igmp snooping vlan 200 multicast-tv
ip igmp snooping
ip igmp snooping vlan 200
ip igmp snooping vlan 601
!
interface vlan 40
name Management
ip address 192.168.1.12 255.255.255.0
!
interface vlan 200
name VLAN_IPTV
!
interface vlan 601
name VLAN_DHCP
!
interface vlan 1000
name VLAN_Other
!
interface vlan 3099
name VLAN_PPPoE
!
interface vlan 4044
name VLAN_IPPhone
!
interface fastethernet1/1/1
bridge multicast unregistered filtering
switchport protected-port
switchport mode general
switchport general allowed vlan add 601,1000,3099,4044 untagged
switchport general multicast-tv vlan 200
switchport general map macs-group 1 vlan 601
switchport general map subnets-group 2 vlan 4044
switchport general map protocols-group 3 vlan 3099
switchport general pvid 1000
 !
interface fastethernet1/1/2
bridge multicast unregistered filtering
switchport protected-port
switchport mode general
switchport general allowed vlan add 601,1000,3099,4044 untagged
switchport general multicast-tv vlan 200
switchport general map macs-group 1 vlan 601
switchport general map subnets-group 2 vlan 4044
switchport general map protocols-group 3 vlan 3099
switchport general pvid 1000
 !
interface fastethernet1/1/3
bridge multicast unregistered filtering
switchport protected-port
switchport mode general
```

```
switchport general allowed vlan add 601,1000,3099,4044 untagged
switchport general multicast-tv vlan 200
switchport general map macs-group 1 vlan 601
switchport general map subnets-group 2 vlan 4044
switchport general map protocols-group 3 vlan 3099
switchport general pvid 1000
!
interface gigabitethernet1/1/1
description TRUNK
switchport mode trunk
switchport trunk allowed vlan add 40,200,601,1000,3099,4044
bridge multicast unregistered filtering
switchport access vlan 3
switchport access multicast-tv vlan 30
!
```

3 Управление и мониторинг

3.1 Управление через SNMPv1/2c/3

Коммутатор поддерживает управление и мониторинг по протоколу SNMPv1/v2c/v3. Для этого на коммутаторе необходимо задать SNMP Community для v2c или группу, пользователя и область доступа к OID для SNMPv3.Также необходимо указать адрес Сервера, на который будут отправляться SNMP Trap.

```
!
snmp-server community comm_ro ro
snmp-server community comm_rw rw
snmp-server host 192.168.1.240 traps version 2c comm_trap
snmp-server host 2001::240 traps version 2c comm_trap
!
snmp-server engineID local default
snmp-server view Port ifAdminStatus.20 included
snmp-server group Admin v3 auth read Default write Port
snmp-server user Den Admin v3 auth md5 password priv password1
!
```

3.2 Отправка Syslog-сообщений

По умолчанию, происходит регистрация и запись событий в энергонезависимую память и вывод сообщений в окно терминала. Для задания сервера, на который будут отправляться Syslog-сообщения, необходимо ввести следующую команду:

```
!
logginhost 192.168.1.240
!
```

3.3 Синхронизация с NTP-сервером

Коммутатор поддерживает работу протокола SNTPv4 согласно RFC 2030.

Он включён как подпротокол в NTPv4, т.е. это не новый протокол, а способ использования NTP-пакетов и NTP-серверов в приложениях, где не требуется высокоточное время, либо оно недостижимо. SNTP реализован для синхронизации времени конечным клиентом, поскольку все преимущества протокола NTP проявляются именно в сети серверов, а для получения показаний конечным пользователем NTP излишне сложен. В этом случае клиент использует только часть информации UDP-пакета NTP-сервера. SNTP-клиент может работать с любыми версиями NTP-серверов.

Для получения времени от NTP-сервера (в примере – 192.168.1.240) необходимо задать следующую конфигурацию:

```
clock source sntp
clock timezone MSK +4
sntp unicast client enable
sntp client poll timer 60
sntp unicast client enable
sntp unicast client poll
sntp server 192.168.1.240 poll
```

4 Безопасность

4.1 Port Security

Для ограничения максимального количества MAC-адресов, изученных коммутатором на порту, можно использовать один из режимов работы функции Port Security.

Для установки ограничения в 5 MAC-адресов на порту необходимо задать следующую конфигурацию:

```
!
interface fastethernet1/1/1
no port security
port security mode max-addresses
port security max 5
port security
port security discard
!
```

4.2 Storm Control

Для защиты сети от возможного возникновения «штормов» трафика, рассылаемого широковещательно, можно установить ограничение на такой тип трафика (Broadcast/Multicast/UnknownUnicast):

```
!
interface fastethernet1/1/1
storm-control broadcast enable
storm-control broadcast level kbps 64
storm-control include-multicast unknown-unicast
!
```

4.3 IGMP Profile

Для разрешения пользователям подписываться только на определенные группы mulicast-рассылки необходимо создавать IGMP-профили. Система позволяет создать 24 профиля, в каждом из которых может быть 10 диапазонов. Разные профили можно применять к одному интерфейсу. Помимо этого, можно задавать ограничение на максимальное количество групп, на которое пользователь может подписываться.

Ниже приведена конфигурация, в которой создаются два пакета разрешенных каналов и закрепляются за пользователем, подключенным к первому порту. Также ему разрешено использовать три устройства для приема multicast-трафика.

```
!
bridge multicast filtering
vlan database
vlan 200
exit
ip igmp snooping
ip igmp snooping vlan 200
ip igmp snooping vlan 200 mrouter interface gi1/1/1
!
interface fastethernet1/1/1
 bridge multicast unregistered filtering
 switchport access vlan 200
 ip igmp profile allowed add 1
 ip igmp profile allowed add 2
 ip igmp max groups 3
!
```

```
interface gigabitethernet1/1/1
 switchport mode trunk
 switchport trunk allowed vlan add 200
!
exit
ip igmp profile 1 add 233.3.2.0 233.3.2.3
ip igmp profile 1 add 233.3.2.50 233.3.2.70
ip igmp profile 2 add 233.3.3.20 233.3.3.40
ip igmp profile 2 add 233.3.3.70 233.3.2.120
!
```

4.4 DHCP option 82

Опция 82 позволяет идентифицировать пользователя и сообщить DHCP-серверу с какого порта и какого устройства пришел запрос на получение адреса. Опция 82 работает в связке другой полезной функцией – DHCP Snooping.

DHCP Snooping позволяет защитить сеть от присутствия несанкционированного DHCP-сервера, пересылая запросы только на доверенный порт.

Ниже приведена конфигурация коммутатора, необходимая при использовании данной функции. Задаваться формат вставляемой информации может как глобально с использованием дескрипторов, так и конкретно на каждом интерфейсе. В случае использования обоих методов задания, формат на интерфейсе имеет больший приоритет и перекрывает глобальные настройки на этом интерфейсе:

```
!
vlan database
vlan 1000
exit
!
hostname –Topaz-test123-
ip dhcp snooping
ip dhcp snooping vlan 1000
ip dhcp option82
ip dhcp option82 format circuit-id ascii p%p
ip dhcp option82 format remote-id ascii %m|%h
!
interface vlan 1000
name USER_VLAN1000
!
interface fastethernet1/1/1
 switchport access vlan 1000
 description Moscow,ul.Uchebnaya,d.33
 ip dhcp option82
 ip dhcp option82 vlan 1000
!
interface fastethernet1/1/2
 switchport access vlan 1000
 ip dhcp option82
 ip dhcp option82 vlan 1000
 ip dhcp option82 format circuit-id ascii p02
!
interface gigabitethernet1/1/1
 switchport mode trunk
 switchport trunk allowed vlan add 1000
 ip dhcp snooping trust
!
```

4.5 PPPoE Intermediate Agent

Для того, чтобы оборудование BRAS, на котором терминируются сессии PPPoE, могло однозначно сопоставить сетевой трафик с абонентской линией, необходимо использовать функцию PPPoE Intermediate Agent (PPPoE+).

Во многом функции PPPoE+ соответствуют функциям DHCP Option 82 для идентификации абонента. PPPoE Intermediate Agent перехватывает идущие от пользователя пакеты PPPoE discovery и добавляет в них идентифицирующую информацию. Пакеты при этом отправляются только на доверенный порт (как правило, это UPLINK-порт).

Ниже приведена конфигурация коммутатора при использовании данной функции. Задаваться формат вставляемой информации может как глобально с использованием дескрипторов, так и конкретно на каждом интерфейсе. В случае использования обоих методов задания, формат на интерфейсе имеет больший приоритет и перекрывает глобальные настройки на этом интерфейсе:

```
!
vlan database
vlan 1000
exit
!
hostname –Topaz-test123-
pppoe intermediate-agent
pppoe intermediate-agent format circuit-id ascii p%p
pppoe intermediate-agent format remote-id ascii %m:%h
!
interface vlan 1000
name USER_VLAN1000
!
interface fastethernet1/1/1
switchport access vlan 1000
description Moscow,ul.Uchebnaya,d.33
pppoe intermediate-agent
pppoe intermediate-agent vlan 1000
!
interface fastethernet1/1/2
switchport access vlan 1000
pppoe intermediate-agent
pppoe intermediate-agent vlan 1000
pppoe intermediate-agent format circuit-id ascii p02
!
interface gigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 1000
pppoe intermediate-agent
pppoe intermediate-agent vlan 1000
pppoe intermediate-agent strategy keep
pppoe intermediate-agent trust
!
```

4.6 AAA

Для процесса предоставления доступа и контроля над ним можно использовать как локальную базу пользователей, так и удаленный сервер. Во втором случае процессы аутентификации, авторизации и аккаунтинга могут осуществляться по протоколам RADIUS и TACACS+.

Далее приведен пример конфигурации коммутатора для работы по этим протоколам.

```
!
username angtel-admin privilege 15 password admin
radius-server host 192.168.1.10 key testkey
```

```
aaa authentication login RADIUS radius local
tacacs-server host 192.168.1.11 key testkey
aaa authentication login TACACS tacacs local
aaa accounting login start-stop group tacacs
ip ssh server
!
line telnet
login authentication TACACS
line ssh
login authentication RADIUS
!
```

В этом примере создаются два метода доступа:

1) Предоставление доступа осуществляется по протоколу RADIUS, в случае отсутствие связи с Сервером используется локальная база;
2) Предоставление доступа осуществляется по протоколу TACACS+, в случае отсутствие связи с Сервером используется локальная база;

Метод 1 применяется при попытке получить управление по протоколу Telnet, метод 2 применяется при попытке получить управление по протоколу SSH.

Кроме того, в примере включен аккаунтинг команд по протоколу TACACS+, который производится после успешных процессов аутентификации и авторизации пользователя по протоколу TACACS+ (в данном примере при попытке доступа через Telnet).

RADIUS Сервер при этом должен иметь настройки, описанные ниже. Файл /etc/mod-config/files/authorize (FreeRADIUS v3.0.3):

```
# Непривилегированный пользователь
operator Cleartext-Password := "operator"
         NAS-IP-Address = 192.168.1.230,
         Service-Type == 6,
         Cisco-AVpair = "shell:priv-lvl=1"

# Привилегированный пользователь
adminCleartext-Password := "admin"
NAS-IP-Address = 192.168.1.230,
         Service-Type == 6,
         Cisco-AVpair = "shell:priv-lvl=15"

# Пароль на enable
$enab15$ Cleartext-Password := "admin_angtel"
         NAS-IP-Address = 192.168.1.230,
         Service-Type == 6,
         Cisco-AVPair = "shell:priv-lvl=15"
```

Файл /etc/raddb/clients.conf (FreeRADIUS v3.0.3):

```
client 192.168.1.230 {
                      secret = testkey
                      shortname = Angtel
                     }
```

5 Построение кольцевой топологии

5.1 RSTP и Loopback Detection

Для построения кольцевой топологии, показанной на рисунке 5.1.1 , используют, как правило, протокол сходимости кольца RSTP. Протокол, работая на канальном уровне, позволяет делать топологию избыточной на физическом уровне, но при этом логически блокировать петли.

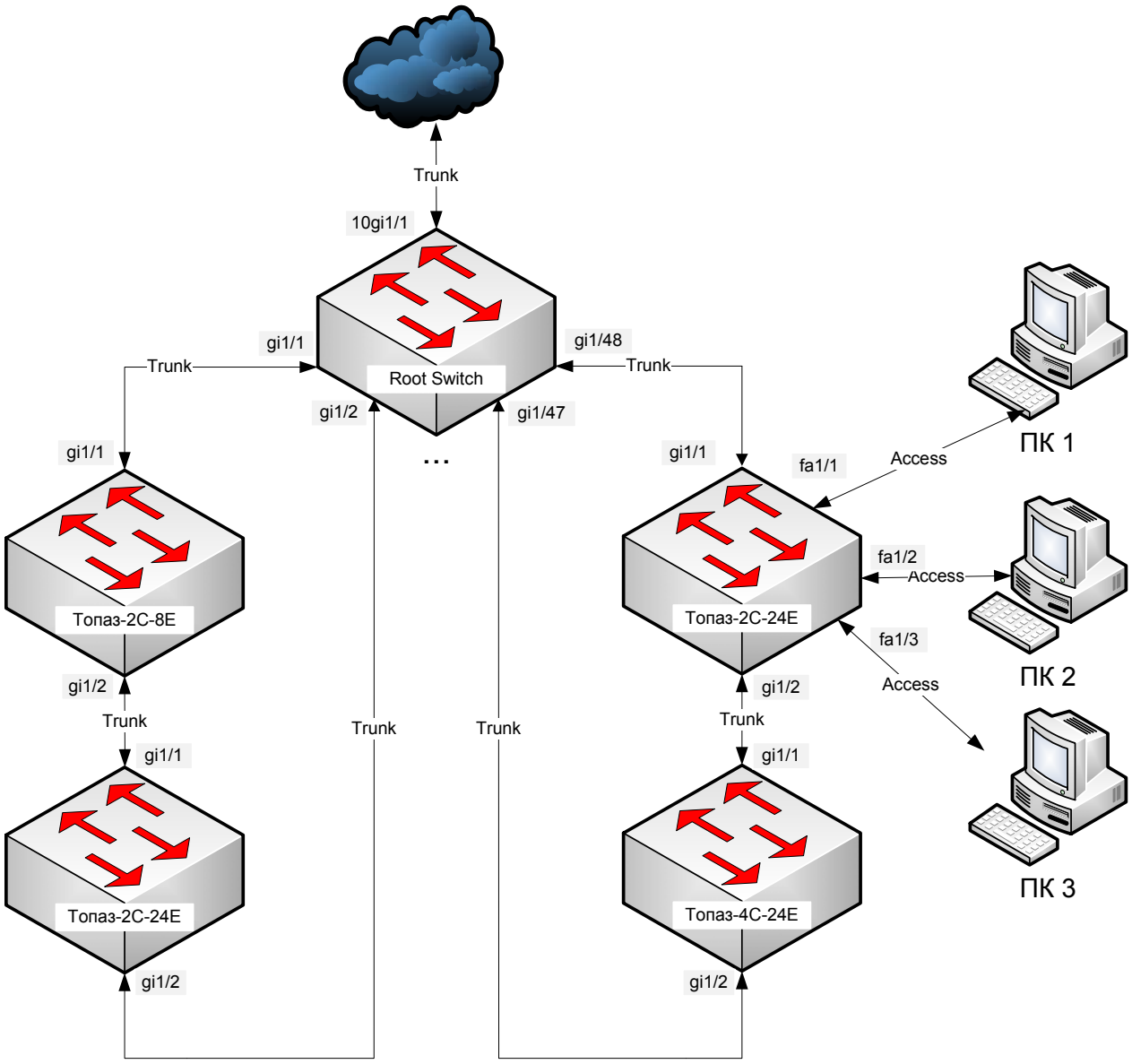

Рис. 5.1.1. Кольцевая топология в сетях доступа

Протокол включен по умолчанию на всех физических интерфейсах, поэтому рекомендуется отключать его на всех абонентских портах, которые не участвуют в построении кольца.

Кроме того, коммутатор поддерживает возможность фильтрации STP BPDU пакетов, которую также необходимо включать на абонентских портах.

Другой полезной функцией, которую также рекомендуется включать на абонентских портах, является Loopback Detection. Она позволяет защитить устройство и сеть от возможного возникновения петель. Далее приведен пример настроек для коммутатора доступа с 3-мя абонентами, участвующего в построении кольцевой топологии:

```
!
loopback-detection enable
```

```
loopback-detection mode base-mac-addr
errdisable recovery interval 30
errdisable recovery cause loopback-detection
!
interface fastethernet1/1/1
spanning-tree disable
spanning-tree bpdu filtering
loopback-detection enable
!
interface fastethernet1/1/2
loopback-detection enable
spanning-tree disable
spanning-tree bpdu filtering
!
interface fastethernet1/1/3
loopback-detection enable
spanning-tree disable
spanning-tree bpdu filtering
!
```

5.2 MSTP

Другим протоколом, который также используется в сетях с кольцевой топологией и описан в стандарте IEEE 802.1s, является MSTP. MSTP обеспечивает как быструю сходимость сети, так и возможность баланса нагрузки в сети с настроенными VLAN.

Протокол позволяет настраивать несколько независимых «деревьев» STP в разных VLAN. Каждое такое «дерево» может иметь свою независимую от других «деревьев» топологию.

Например, создадим 4 независимых дерева в разных VLAN: Instance 1 – VLAN 10, Instance 2 – VLAN 283, Instance 3 – VLAN 282, Instance 4 – VLAN 599. Как показано на рисунке 5.2.1, у нас имеется два кольца, в каждом строится по два независимых дерева в разных VLAN.

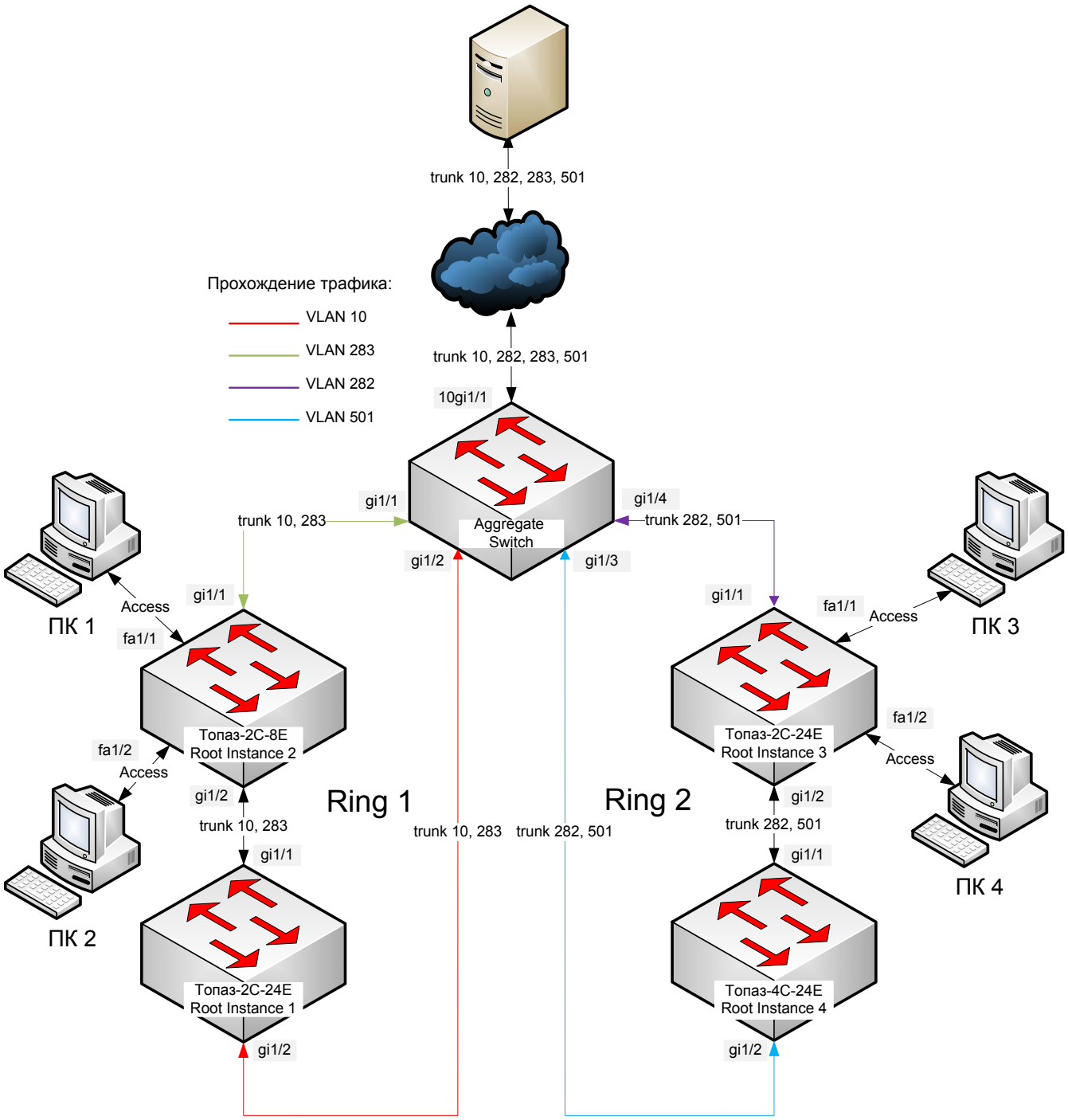

Рис. 5.2.1. Кольцевая топология сетей доступа с балансировкой нагрузки

Конфигурация для коммутаторов доступа в первом кольце, в этом случае, будет выглядеть следующим образом:

```
!
vlan database
vlan10,383
exit
!
spanning-tree mode mst
spanning-tree mst configuration
instance 1 vlan 10
instance 2 vlan 283
instance 3 vlan 282
instance 4 vlan 501
name Region
revision 1
```

```
!
interface fastethernet1/1/1
switchport access vlan 10
spanning-tree disable
spanning-tree bpdu filtering
!
interface fastethernet1/1/2
switchport access vlan 283
spanning-tree disable
spanning-tree bpdu filtering
!
interfacegigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 10,283
!
interfacegigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 10,283
!
```

Для коммутаторов второго кольца:

```
!
vlan database
vlan 282,501
exit
!
spanning-tree mode mst
spanning-tree mst configuration
instance 1 vlan 10
instance 2 vlan 283
instance 3 vlan 282
instance 4 vlan 501
name Region
revision 1
!
interface fastethernet1/1/1
switchport access vlan 282
spanning-tree disable
spanning-tree bpdu filtering
!
interface fastethernet1/1/2
switchport access vlan 501
spanning-tree disable
spanning-tree bpdu filtering
!
interface gigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 282,501
!
interface gigabitethernet1/1/2
switchport mode trunk
switchport trunk allowed vlan add 282,501
!
```

Коммутатор агрегации:

```
!
vlan database
vlan 10,282,283,501
exit
!
```

```
spanning-tree mode mst
spanning-tree mst configuration
instance 1 vlan 10
instance 2 vlan 283
instance 3 vlan 282
instance 4 vlan 501
name Region
revision 1
!
interface gigabitethernet1/1/1
switchport mode trunk
switchport trunk allowed vlan add 10,283
!
interface gigabitethernet1/1/2
switchport mode trunk
switchport trunk allowed vlan add 10,283
!
interface gigabitethernet1/1/3
switchport mode trunk
switchport trunk allowed vlan add 282,501
!
interface gigabitethernet1/1/4
switchport mode trunk
switchport trunk allowed vlan add 282,501
!
```

Теперь, для того чтобы балансировать нагрузку трафика, необходимо в каждом из Instance задать корневой коммутатор, определив на нем низкий приоритет в нужном Instance. Например:

```
spanning-tree mst 1 priority 0
```

6 Качество обслуживания

6.1 QoS на основе меток

Обеспечение качества обслуживание в сетях в основном предполагает обработку высокоприоритетного трафика (IPTV, IP-Телефонии) без потерь. Трафик на основании CoS-меток или DSCP помещают на узлах в различные очереди: IPTV и IP-Телефонию – в высокоприоритетные очереди, оставшийся трафик – в менее приоритетную очередь. Высокоприоритетные очереди при этом обрабатываются по алгоритму строгой приоритезации, оставшиеся – на основании весовых коэффициентов.

Конфигурация в сетях, где для классификации используются CoS-метки (например, CoS 7 – IPTV, CoS 6 – IP-Телефония и CoS 2 – Internet), выглядит следующим образом:

```
!
priority-queue out num-of-queues 2
wrr-queue cos-map 1 2
wrr-queue cos-map 3 6
wrr-queue cos-map 4 7
!
```

Конфигурация в сетях, где для классификации используются CoS-метки (например, DSCP41 – IPTV, DSCP30 – IP-Телефония иDSCP8 – Internet), выглядит следующим образом:

```
!
qos trust dscp
priority-queue out num-of-queues 2
qos map dscp-queue 8 to 1
qos map dscp-queue 30 to 3
qos map dscp-queue 41 to 4
!
```

6.2 QoS на основе потока

В случаях, когда необходимо обеспечить высокий приоритет определенному потоку трафика не на основании полей DSCP или CoS, можно создать и применить политику с использованием списка доступа, определяющего любой возможный тип трафика. Например, ниже приведенная конфигурация позволяет определить трафик с MAC-адресом источника 50:af:73:45:12:ab в высокоприоритетную очередь:

```
!
qos advanced
mac access-list extended MAC_Source
permit 50:af:73:45:12:ab 00:00:00:00:00:00 any
permit any any
exit
mac access-list extended Permit_All
permit any any
exit
class-map CMAP_MAC_Source
match access-group MAC_Source
exit
class-map CMAP_Permit_All
match access-group Permit_All
exit
policy-map EXAMPLE
class CMAP_MAC_Source
set queue 4
exit
```

```
class CMAP_Permit_All
exit
exit
!
interface gigabitethernet1/1/1
service-policy input EXAMPLE
!
```