МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

С.М. Платунова,
И.В. Елисеев,
Е.Ю. Авксентьева

EHTERNET SWITCH L2&L3. ПРОЕКТИРОВАНИЕ, НАСТРОЙКА, ДИАГНОСТИКА СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Учебное пособие

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО

по направлениям подготовки (специальности) 09.04.01 в качестве учебного пособия для реализации основных образовательных программ магистратуры

УНИВЕРСИТЕТ ИТМО

Санкт – Петербург

2018

Платунова С.М, Елисеев И.В., Авксентьева Е.Ю. Ethernet switches L2&L3. Проектирование, настройка, диагностика сетей передачи данных. Учебное пособие по дисциплинам: Теория проектирования вычислительных систем, Компьютерные сети и телекоммуникации, Архитектура и аппаратные средства вычислительных сетей. – СПб: НИУ ИТМО, 2018. – 87 с.

В учебном пособии описаны основы сетей передачи данных, их проектирование, настройка сетевого оборудования – коммутаторов второго и третьего уровней, применяемых в сетях передачи данных.

Учебное пособие предназначено для подготовки магистров по направлению 09.04.01.

Рецензент:

Бессмертный И.А., доктор технических наук, доцент, профессор факультета программной инженерии и компьютерной техники

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно – образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Оглавление

Введение

Данное пособие содержит основные сведения о коммутаторах второго и третьего уровней, настройку функций в сетях операторов связи и компьютерных сетях.

Глава 1. Назначение Metro Ethernet – коммутаторов

Рассмотрим пример корпоративной сети (рис. 1), на примере трехуровневой иерархической модели: Доступ – Агрегация – Ядро.

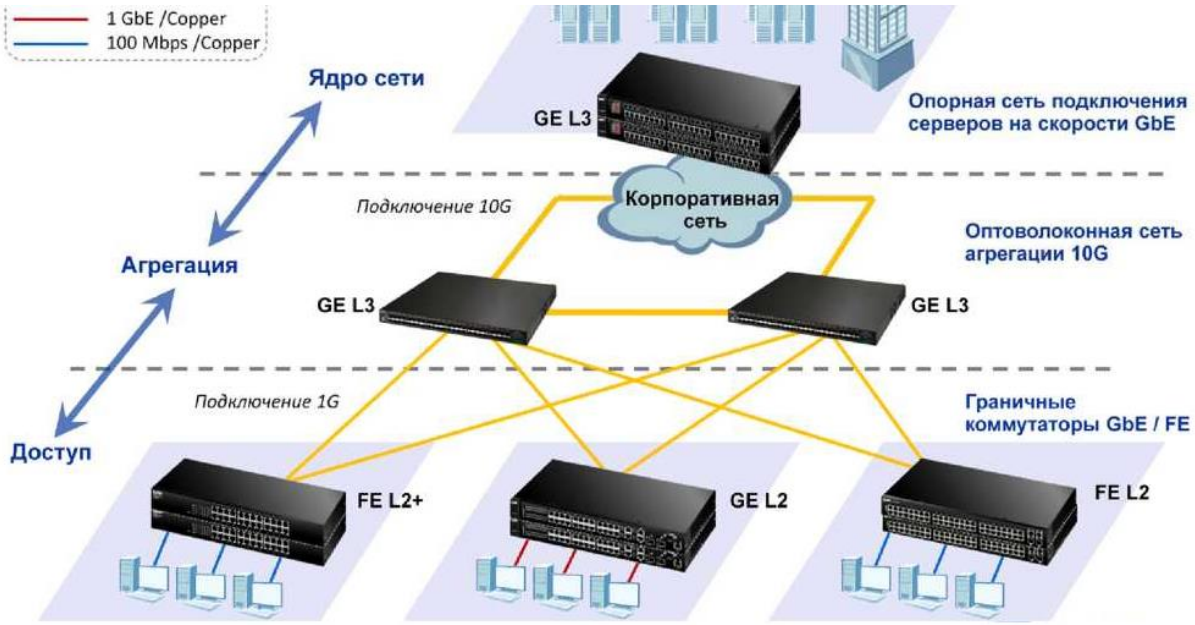

Рис. 1. Трехуровневая иерархическая модель сети

Распределение сетевых устройств по уровням происходит в соответствии с их функциями и производительностью, независимо от других устройств. Т.е. деление сети на уровни происходит больше по логическим принципам, чем по физическим.

На уровне доступа (access) располагаются граничные коммутаторы сети, к которым подключаются пользователи и оконечное оборудование.

Как правило, это управляемые L2/L2+ коммутаторы с медными 100 или 1000 Мбит/с портами для клиентов, и оптическими портами 1 GbE (реже 10 GbE) для подключения к корпоративной/операторской сети (uplink порты). Основной функционал – разделение, изоляция и приоритезация абонентского трафика на основе VLAN.

На уровне агрегации (распределения, distribution) происходит фильтрация абонентского трафика на основе ACL, маршрутизация между VLAN, управление multicast – рассылками.

На уровне агрегации используются протоколы покрывающего дерева для построения кольцевой/полносвязной топологии, иногда используется статическая и динамическая маршрутизация.

Как правило, используются оптические линии связи 1 – 10 GbE. Для сети агрегации выбирают L2+/L3 коммутаторы.
На уровне ядра (опорная сеть) происходит скоростная пересылка больших объемов пользовательского трафика.
Поэтому основное требования к коммутаторам опорной сети – высокая производительность, наряду с организацией резервирования оборудования.
Коммутаторы уровня ядра маршрутизируют или коммутируют трафик между узлами агрегации и/или между соседними сетями, к которым они подключены.
На практике это означает, что трафик от большого числа пользователей сначала агрегируется на едином узле распределения, а затем маршрутизируется или коммутируется на вышестоящее ядро или непосредственно на соседний узел агрегации, или непосредственно между подключенными абонентами.
Иерархическая и структурированная модель сети обеспечивает предсказуемую масштабируемость сети, позволяет гибко управлять потоками данных и поведением сети в случае сбоев.

Службы в сети

В связи с постоянным увеличением объемов используемых служб и приложений, простое объединение хостов между собой не может обеспечить требуемых параметров качества обслуживания (наличия обязательной пропускной способности, приоритезации трафика, безопасности и управления).
В коммутаторах часто реализованы гибкие функции по коммутации и маршрутизации трафика, безопасности, изоляции и приоритезации пользовательского трафика.
Использование современных сетевых устройств позволяет реализовать поддержку и управление такими функциями, как IPTV и VoIP, с гарантированным качеством сервиса.
Поддержка технологии PoE позволит питать Wi – FI точки доступа, IP – камеры и VoIP телефоны прямо по Ethernet кабелю.
Для повышения надежности сети используется защита от петель с помощью протоколов покрывающего дерева STP/RSTP/MSTP.
Протоколы динамической маршрутизации RIP и OSPF обеспечивают согласованность действий маршрутизаторов в сети, повышая производительность всей сети в целом.
Ведётся учет действий операторов, и поведения пользователей в сети. В коммутаторах реализован обширный набор функций для обработки трафика на втором и третьем уровне (L2, L3), разработанный как для нужд сегмента SMB (Small Medium Business), так и для операторов связи.
Для управления большим числом сетевых устройств предусмотрены возможности использования традиционных SNMP – менеджеров, так и фирменных технологий: управлением несколькими устройствами по одному IP – адресу или с использованием Element Management System (EMS).

Уникальной функцией некоторых коммутаторов является способность получать питание по технологии PoE на медном гигабитном порту (№9) по кабелю Ethernet от вышестоящего адаптера или коммутатора PoE 802.3af.
В таком сценарии не нужно подключать к коммутатору штатный адаптер питания и тем самым можно его разместить в тех местах, где отсутствует возможность провести силовой кабель питания 220 В.

Основные отличия управляемых коммутаторов

Основные отличия кроются в позиционировании коммутаторов (рис. 1):

- от рынка SMB (Small Medium Business) до операторов связи и поставщиков услуг Интернет.
- от уровня доступа до агрегации/ядра сети по медным и оптическим каналам связи.

Коммутаторы второго уровня L2 включают управляемые коммутаторы, предназначенные для операторов связи, и интеллектуальные коммутаторы (smart, или web – управляемые) предназначенные для рынка SMB (Small – Medium Business).
Высокопроизводительные коммутаторы уровня L3 рассчитаны для установки на уровне агрегации или ядра распределенной сети.
Данный класс устройств поддерживает коммутацию уровня L2+ для IPv4 и IPv6 протоколов, расширенную поддержку многоадресных рассылок IGMP IPv4 и MLD IPv6, классы обслуживания (DiffServ), многоуровневое резервирование, поддержку протоколов маршрутизации RIP, OSPF, VRRP, а также списки управления доступом ACL уровней L2/L3/L4.

Metro Ethernet

Metro Ethernet – это использование технологии Ethernet в MAN (Metropolitan Area Network) Отличие коммутаторов Metro Ethernet (рис. 2) от обычных Ethernet коммутаторов:

1. расширенный диапазон рабочих температур
2. дополнительные возможности по электропитанию
3. дополнительные возможности по контролю над устройством
4. дополнительные «операторские» функции (QinQ, L2PT)

Основные отличия коммутаторов Metro Ethernet от обычных Ethernet коммутаторов:

1. Расширенный диапазон рабочих температур
2. Гибкий выбор напряжения питания (220 вольт AC, 48 или 12 вольт DC)
3. Съемный фильтр для защиты от пыли
4. Размещение портов, выключателей и контактных групп на передней панели
5. Встроенный блок сигнализации

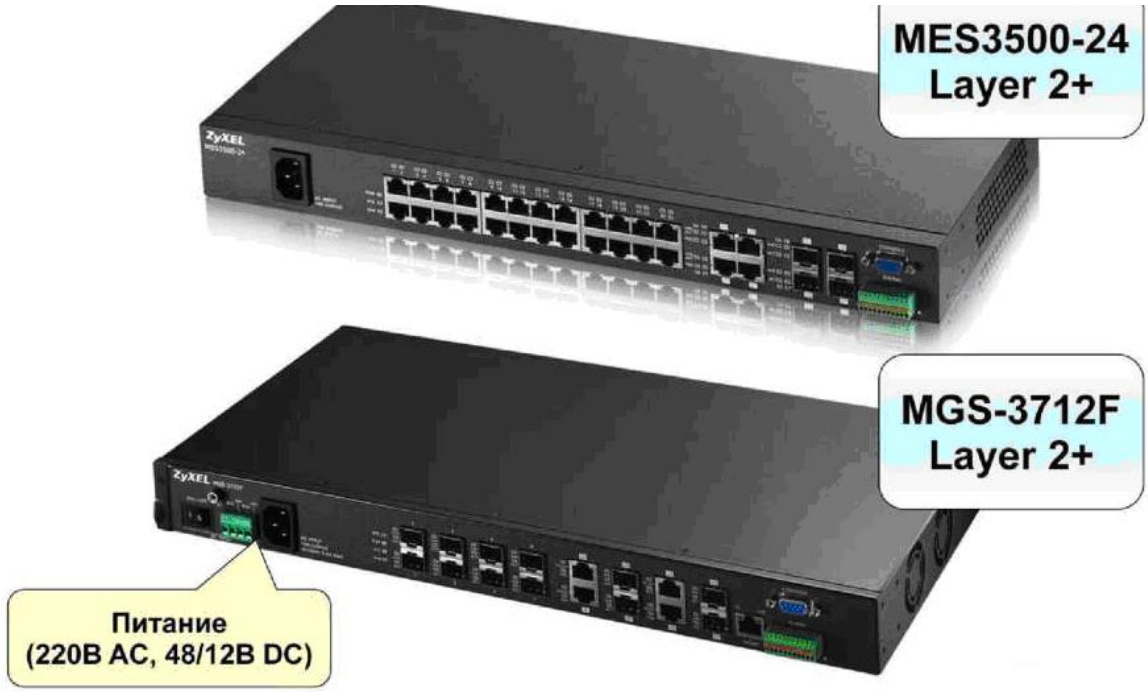

Рис. 2. Коммутаторы Metro Ethernet

Управляемые Metro Ethernet коммутаторы, например, компании zyxel, MGS-3712 и MGS-3712F – разработаны для применения на уровне агрегации распределенных сетей операторов связи и Интернет провайдеров, в частности:

1. Для объединения групп серверов в центрах обработки данных
2. Для агрегации и коммутации трафика на локальных и распределенных магистралях
3. Для агрегации трафика в операторских сетях на расстояниях до 80 км

Управляемый коммутатор Metro Ethernet модели MES3500-24 предназначен для:

1. Для установки на уровне доступа в широкополосных операторских сетях любых масштабов для предоставления абонентам услуг доступа в Интернет, IPTV и пакетной телефонии VoIP.
2. Для подключения операторских распределенных сегментов сети доступа с неблагоприятными условиями окружающей среды и необходимостью оповещения о несанкционированном доступе в коммутационный шкаф.
3. В городских проектах подключения наружных видеокамер, датчиков слежения и измерительных приборов электросети.

Разъем Alarm

Система сигнализации Metro Ethernet коммутаторов работает на базе двух типов датчиков (рис. 3):

1. Внутренние датчики – температура, напряжение, скорость вращения вентиляторов.
2. Внешние датчики – любые внешние датчики, например датчик дыма, датчик открытия дверцы коммутационного шкафа и т.д.

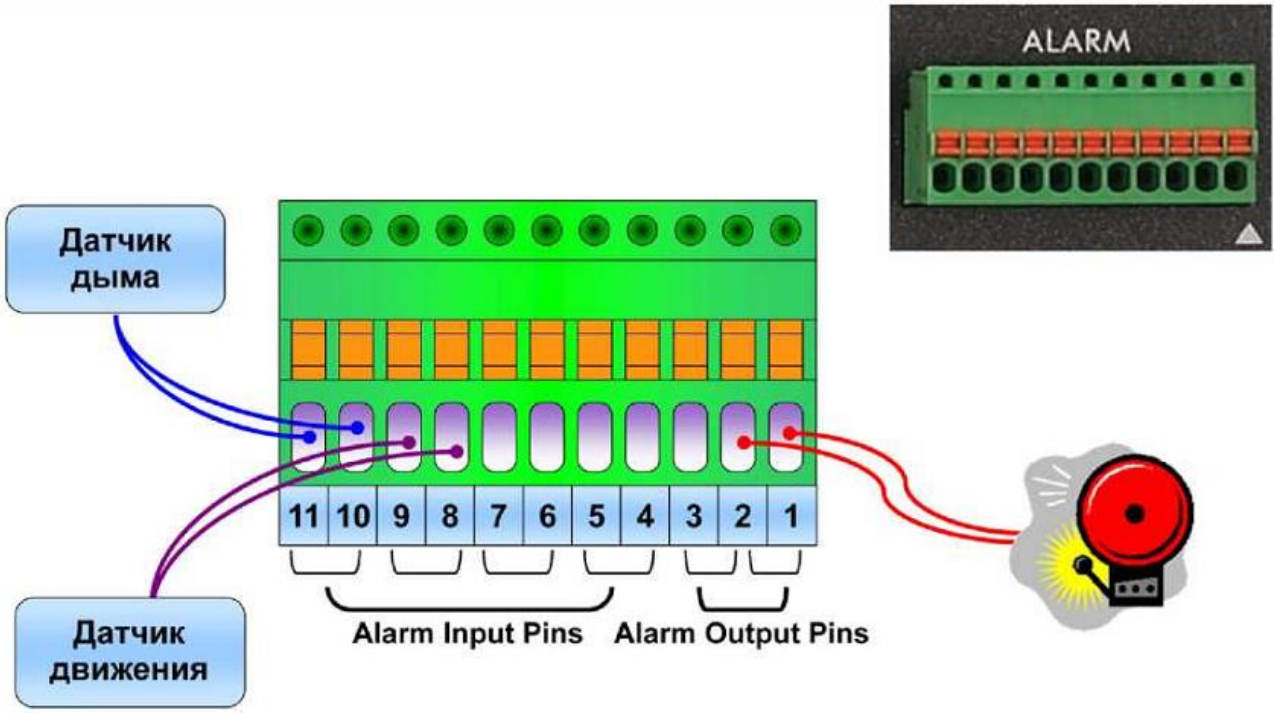

Рис. 3. Датчики коммутаторов Metro Ethernet

В случае срабатывания внутреннего датчика или внешнего датчика возможна настройка следующих сигнализаций:

1. Светодиод ALM на передней панели устройства.
2. Сигнализация, подключенная к разъему Alarm.
3. Запись в системный журнал.
4. Отправка сообщения SNMP Trap.

Можно подключить Ethernet – коммутаторы серии MES/MGS (с поддержкой функции внешней сигнализации) в последовательную цепь для ретрансляции аварийного сигнала.

При подключении внешней сигнализации к разъему Alarm, используются контакты (ALARM Output pins): контакт 1 – нормально замкнутый, контакт 2 – общий, контакт 3 – нормально разомкнутый.

При последовательном подключении Ethernet – коммутаторов используются контакты ALARM Output 3 и 2 (3 – нормально разомкнутый контакт и 2 – общий).

Учетные записи и привилегии

По умолчанию в коммутаторе создана одна учетная запись. Можно добавить до 4 дополнительных учетных записей, при этом для каждой записи определяется уровень привилегий.

При добавлении учетной записи через web – интерфейс уровень привилегий задать невозможно. Для этого необходимо использовать режим командной строки CLI.

В коммутаторах имеется возможность настроить 4 дополнительные учетные записи. Каждой учетной записи назначается свой уровень привилегий
Команды управления учетными записями:

Создание учетной записи:

(config)#logins username <name> password <passwd>

Назначение привилегий:

(config)#logins username <name> privilege <0 – 14>

Удаление:

(config)#no logins username <name>

Вывод таблицы учетных записей:

#show logins

Web – интерфейс

При входе в устройство по протоколу HTTP необходимо ввести имя пользователя и пароль.
Основное окно отображает текущую статистику по каждому порту (активен ли порт, LACP, количество переданных/ принятых пакетов, количество ошибок приема/передачи, текущая скорость передачи/приема в KB/s, время работы порта).
В левом окне располагается основное меню, состоящее из основных разделов:
Basic Settings — системная информация и основные настройки, такие как: режим работы VLAN, распределение приоритетов 802.1p по очередям и т.д.
Advanced Application — дополнительный функции, такие как: VLAN, Link Aggregation.
IP Application — настройка протоколов маршрутизации (для коммутаторов L3), статических маршрутов, DHCP Server/Relay и т.д.
Management — обновление микропрограммы, сохранение/восстановление конфигурации, просмотр таблиц MAC/ARP и т.д.
Чтобы сбросить статистику для отдельного порта, вводят номер соответствующего порта. Чтобы сбросить статистику для всех портов – выбирают Any и также нажимают кнопку Clear Counter.

Настройка IP – адреса

По умолчанию во всех коммутаторах интерфейс для внутреннего управления (*inband*) имеет IP – адрес 192.168.1.1/24 и для внешнего управления (*outband*) IP – адрес192.168.0.1/24.
Для управления устройством можно настроить другие IP – адреса из отличных от умолчания подсетей.
Назначая IP – адрес для управления коммутатором, также указывается VID (VLAN ID), которой должен принадлежать этот IP – адрес управления (данный VLAN должен быть отдельно создан в разделе Static VLAN).
При установке переключателя «Manageable» разрешается управлять коммутатором через порты, принадлежащие указанному VLAN через

назначенный IP – адрес. Не рекомендуется устанавливать переключатель «Manageable» для пользовательских VLAN.

Команды в CLI:

ip name – server <ip>
default – management <in – band|out – of – band>
Настройка In – band интерфейса:
vlan <1 – 4094> ip address inband – default <ip – address> <mask>
vlan <1 – 4094> ip address inband – default dhcp – bootp <cr>
vlan <1 – 4094> ip address inband – default dhcp – bootp release
vlan <1 – 4094> ip address inband – default dhcp – bootp renew
Настройка дополнительных IP – адресов для управления:
vlan <1 – 4094> ip address <ip – address> <mask> manageable
vlan <1 – 4094> ip address <ip – address> <mask> <cr>
vlan <1 – 4094> ip address default – gateway <ip – address>
Настройка Out – of – band интерфейса (Management интерфейс):
ip address <ip> <mask> ip address default – gateway <ip>

Функция iStacking

Функция iStacking применяется в том случае, когда используется один коммутатор для одновременного управления несколькими коммутаторами (до 24х) в одном широковещательном домене и в одной группе VLAN.

Рис. 4. Функция iStacking

Функция iStacking (рис. 4) позволяет использовать один коммутатор для управления множеством устройств. Все управляемые устройства должны быть в одном broadcast домене (т.е. быть подключены напрямую, и находиться в одной группе VLAN).

Выделяется головное устройство – Cluster Manager. Оно должно быть единственным в сети. Управляемых устройств Cluster Member может быть до 24.
Управляющим устройством может служить как коммутатор второго уровня, так и третьего.
Настройка сети iStacking осуществляется в меню Management > Cluster Management > Clustering Management Configuration

Команды в CLI:

cluster <vlan – id>
cluster name <cluster name>
cluster member <mac – address> password <password – str> cluster rcommand <mac – address>

Протокол SNMP

SNMP – протокол прикладного уровня, использующийся для управления и мониторинга устройств на основе TCP/IP.
Протокол SNMP используется для обмена управляющей информацией между системой сетевого управления и сетевым элементом.
Станция управления может управлять и осуществлять мониторинг коммутатора по сети (на коммутаторе должен быть настроен TCP/IP), с помощью протокола SNMP версии 1, 2c, 3.
Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют, какую информацию о коммутаторе необходимо получить (например, состояние порта и т.п.).

Рис.5. Настройка протокола SNMP

База управляющей информации (MIB) состоит из совокупности управляемых объектов, которыми агент и менеджер обмениваются по протоколы SNMP. Коммутаторы поддерживают общие базы MIB, и частные базы MIB, которые идут в архиве с микропрограммой устройства.
Используя любой SNMP менеджер с базами MIB, можно удаленно управлять и производить мониторинг большого числа коммутаторов в распределенной сети.
Настраивая параметры работы SNMP (рис. 5) в коммутаторе, выбирается версия SNMP (она должна совпадать с версией протокола на менеджере); Get/Set/Trap Community; IP – адреса и порты менеджеров (можно задать до четырех), которым будут отправляться сообщения Trap. Для SNMP v3 настраиваются параметры аутентификации – Username (который должен совпадать с учетной записью оператора, настроенной на коммутаторе).
В разделе Trap Group указывается, о каких типах событий коммутатор должен извещать определенных SNMP менеджеров, отправляя им Trap сообщения.

Syslog

С помощью протокола Syslog коммутаторы могут генерировать и пересылать по IP – сети извещения о событиях серверам Syslog, собирающим информацию о событиях. Протокол Syslog определен в стандарте RFC 3164. RFC определяет формат пакета, содержание и относящуюся к системному журналу информацию в сообщениях Syslog. Каждое сообщение Syslog содержит определение категории (facility) и уровни серьезности (level).
В меню SysLog можно настроить параметры внешних SysLog – серверов (до четырех), а также задать соответствие между видами сообщений (System, Interface, Switch, AAA, IP).
Команды CLI:
syslog <cr>
syslog type <type> <cr>
syslog type <type> facility <0 – 7>
syslog server <ip – address> level <level>
syslog server <ip – address> inactive
Общие настройки коммутатора
В меню Общие настройки задают System Name, Location – имя – описание и местонахождение коммутатора.
В этом же меню задаются временные настройки коммутатора: вручную или с помощью сервера времени (Daytime RFC – 867, Time RFC – 868, или NTP RFC – 1305).
Daylight Saving – функция автоматического перехода на зимнее/летнее время с указанием дня и часа перехода на летнее время и обратно.
Команды CLI:
time daylight – saving – time
time daylight – saving – time help
– week: first | second | third | fourth | last
– day: sunday | monday | tuesday | Wednesday | thursday | friday | saturday

– Month: january | february | march | april | may | june | july | august | september | october | november | december
– o'clock: 0 – 23
time daylight – saving – time start – date <week> <day> <month> <o'clock>
time daylight – saving – time end – date <week> <day> <month> <o'clock>

Функция Configure Clone

Функция Configure Clone позволяет быстро настраивать порт копированием настроек с другого порта того же коммутатора.
Source port: порт, настройки которого будут копироваться.
Destination: порты, в которые будут скопированы настройки Source port.

802.3ah OAM (Operations, Administration and Maintenance)

Функции 802.3 ah Ethernet OAM (эксплуатация, администрирование и обслуживание) уровня канала передачи данных, описанные в IEEE 802.3ah, представляют собой протокол мониторинга состояния канала.
В этом протоколе для передачи информации о состоянии канала между подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU).
Оба оконечных устройства должны поддерживать стандарт IEEE 802.3ah.
Так как функции Ethernet OAM уровня канала передачи данных работают на втором уровне модели OSI, для мониторинга или устранения неполадок с сетевыми соединениями не требуются ни протокол IP, ни протокол SNMP.
Управляемые Ethernet – коммутаторы часто поддерживают следующие функции IEEE 802.3ah:

1. Обнаружение (Discovery) – функция позволяет идентифицировать устройства на каждой из сторон канала Ethernet, атакже OAM – настройки этих устройств.
2. Удаленная обратная петля (Remote Loopback) – тест удаленной обратной петли на устройствах Ethernet. При работе кольцевого тестирования каждый кадр, попавший в порт, копируется и отправляется обратно, таким образом, оно позволяет проверить надежность и качество соединения.

Команды CLI:

ethernet oam <cr>
interface port – channel <port – list> ethernet oam <cr> interface port – channel <port – list> ethernet oam mode <active|passive> interface port – channel <port – list> ethernet oam remote – loopback supported ethernet oam remote – loopback test <port> [<number of packets> [<packetsize>]]

Контрольные вопросы по главе 1

1. Каково назначение Metro Ethernet – коммутаторов?
2. Что такое управляемый коммутатор и в чем отличие от неуправляемого?
3. Для чего служат учетные записи?
4. Каково назначение функции iStadking?

5. Каково назначение SMTP протокола?
6. Каково назначение функции 802.3 ah Ethernet OAM?

1. Глава 2 Функции 2 уровня

VLAN (Virtual Local Area Network) – виртуальные локальные сети

VLAN предназначены для:

1. разделения физической сети на несколько логических подсетей
2. изолирования каждого порта для увеличения безопасности
3. изолирования широковещательного трафика

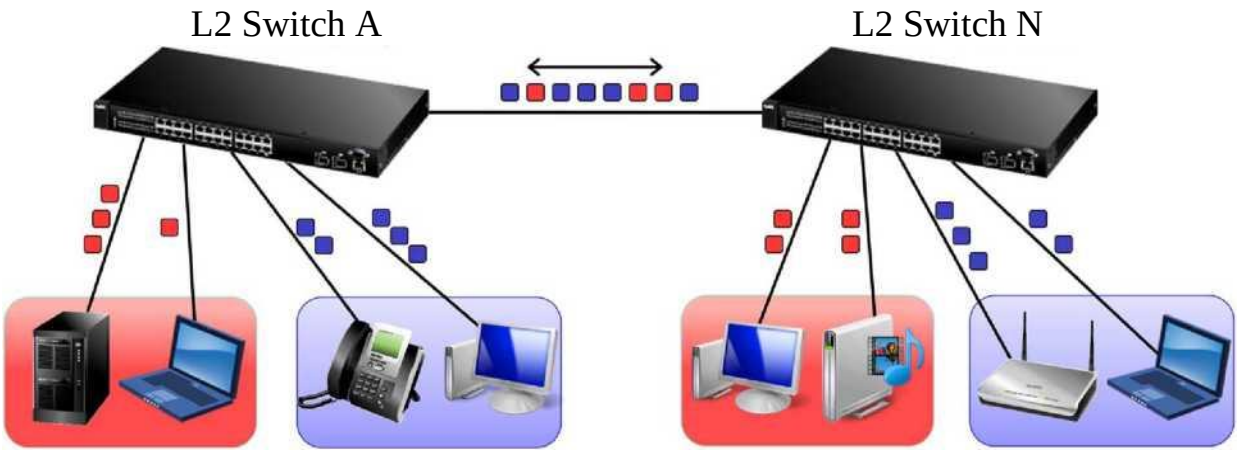

Рис. 6. Схема работы VLAN

Виртуальная локальная сеть (VLAN) (рис. 6) представляет собой общий широковещательный домен, который может охватывать множество физических локальных сетевых сегментов и узлов.

За каждым портом коммутатора может быть закреплена определенная VLAN, которая может быть логически сегментирована в соответствии с ее функциями и задачами.

Порты одной VLAN имеют общий домен широковещательной (циркулярной) рассылки.

Порты, относящиеся к различным VLAN, не могут осуществлять рассылку между собой.

Другими словами, VLAN – это логическое сегментирование сети, применяемое для следующих целей:

1. Безопасности рабочей группы.
2. Повышения производительности сети, путем снижения нагрузки на неё.

Безопасность рабочей группы и сети.

Можно повысить уровень безопасности путем сегментирования сети на отдельные широковещательные домены.

Кроме того, можно регулировать размер и структуру домена путем регулирования размера и структуры VLAN.

Повышение производительности сети и контроль трафика.
VLAN позволяют группировать порты коммутатора таким образом, чтобы трафик ограничивался только членами той или иной группы.
Данная функция ограничивает одноадресную, многоадресную и широковещательную (лавинная адресация) рассылку только портами, включенными в конкретную VLAN.
VLAN делают возможным эффективное разделение трафика, обеспечивая более высокую пропускную способность сети.

Типы VLAN

Существует три типа VLAN:

1. VLAN на базе MAC (непопулярная реализация) позволяет объединять в сегмент MAC – адреса хост – машин.
2. VLAN на базе порта (port – based VLAN) позволяет создавать VLAN из различных портов одного коммутатора.
3. VLAN на базе признака (tag – based VLAN, 802.1Q) позволяет создавать VLAN на основе признака (тега).
   Признак, по которому можно идентифицировать VLAN, записывается в кадре Ethernet между MAC адресом источника и полем EtherType.

VLAN на базе признака (тега) 802.1 Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети.
В кадр Ethernet вставляется маркер (tag), в котором указывается идентификатор VLAN, принимающий значение от 1 до 4094 (номера 0 и 4095 зарезервированы для специальных целей).
Такой кадр называется маркированным (или тегированным, tagged).
Тег занимает 4 байта. Он состоит из TPID (Tag Protocol Identifier, 2 байта), 802.1p (поле приоритета – 3 бита, также называемое Priority Code Point (PCP)), CFI (1 бит) и VID (идентификатор VLAN – 12 бит).
Исходное поле EtherType сдвигается вправо.
На его место становится признак TPID, указывающий на новый тип кадра (802.1Q).
Поле CFI – однобитное поле, всегда равно 0 для Ethernet – коммутаторов, используется для совместимости Ethernet и Token Ring.
Добавление четырех байтов к максимальному размеру кадра Ethernet ведет к возникновению проблем в работе устаревших коммутаторов и сетевых адаптеров.
Это связано с тем, что максимальный размер маркированного кадра составляет не 1518 байт, а 1522.
Если невозможно заменить устаревшее оборудование, не поддерживающее увеличенные кадры, то можно на 4 байта уменьшить MTU в настройках сетевых устройств: с 1500 до 1496

Типы кадров, типы устройств

По наличию тега 802.1Q и по его заполненности все кадры можно поделить на три типа.

Untagged frame: Кадр, в котором не установлен тег 802.1Q.

Priority – tagged frame: Кадр, содержащий установленный признак VLAN, однако поле VID равно 0.

Такой кадр не принадлежит никакой VLAN, в нем имеет значение только поле приоритета 802.1p.

VLAN – tagged frame: Кадр с установленным тегом 802.1Q и VID не равным 0.

При внедрении в сеть стандарта 802.1Q устройства по отношению к данному стандарту поделятся на два типа.

VLAN – aware — это устройства, которые поддерживают признак VLAN 802.1Q имогут принимать пакеты с учетом этого поля.

VLAN – unaware — это устройства, которые не поддерживают 802.1Q. При передаче кадра на устройство VLAN – Unaware коммутатор должен удалить тег из кадра. При получении кадра без тега коммутатор должен установить тег по умолчанию.

Процесс 802.1Q (рис. 7)

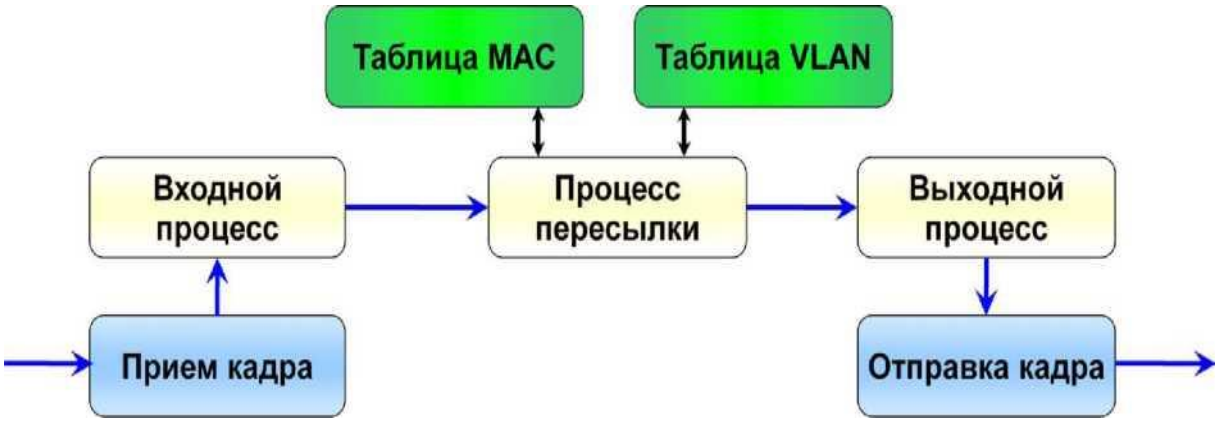

Рис. 7. Схема работы процесса 802.1Q

Входной процесс:

Если кадр пришел с тегом, то он без изменений направляется в процесс пересылки.

Если без тега, то на него ставится тег, согласно входному правилу.

Процесс пересылки:

Принимает решения о фильтрации или пересылке пакета в порт назначения, согласно таблицам VLAN и MAC.

Выходной процесс:

Определяет, оставлять ли тег VLAN в кадре.

Если известно, что к порту подключено устройство VLAN – unaware, то тег необходимо снять.

Входное правило (Port VLAN ID – PVID)

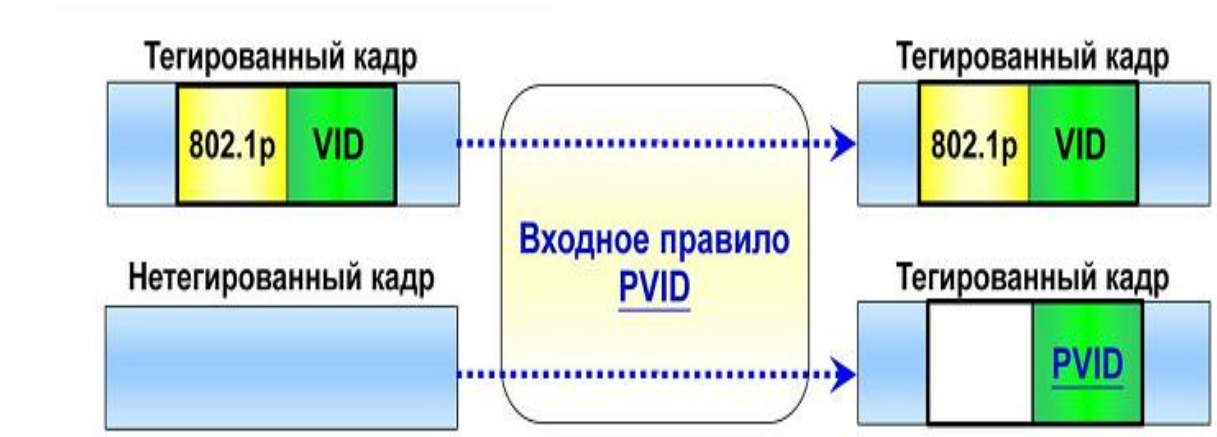

Рис. 8. Работа входного правила

Входное правило (Port VLAN ID или PVID), показанное на рисунке 8 работает следующим образом.

VLAN – aware устройства могут принимать как нетегированные, так и тегированные кадры.

Если поступивший кадр тегированный, то кадр передается без изменений в процесс пересылки

Если поступивший кадр нетегированный, то он или:

1. маркируется VID по умолчанию для данного порта (PVID)
2. маркируется 802.1 p по умолчанию для данного порта (802.1 p Priority)
3. передается в процесс пересылки PVID (Port VLAN Identifier)

VLAN ID по умолчанию, назначается на каждый физический порт.

Идентификатор VLAN для порта (PVID) используется для добавления тегов ко всем нетегированным кадрам, поступающим на этот порт.

После обработки поступившего кадра правилом PVID, кадр будет содержать тег с VLAN ID равным PVID.

На каждый порт коммутатора можно назначить свой PVID (но только один) в зависимости от подключенных устройств.

Входное правило PVID работает только с нетегированными кадрами, т.е. у пришедшего тегированного кадра замен не будет.

В настройках коммутаторов по умолчанию (при включении 802.1Q VLAN) на всех портах коммутатора установлен идентификатор PVID = 1.

Стоит отметить, что правило PVID устанавливает только поле VID в теге 802.1Q.

Значение же поля 802.1p (поле приоритета) в теге 802.1Q будет установлено в соответствии с настройками порта из раздела меню:

Basic Setup > Port Setup.

В настройках по умолчанию значение 802.1p = 0.

Входное правило на базе протокола

Входное правило на базе протокола, показанное на ри. 9 работает следующим образом.

Рис. 9. Работа входного правила на базе протокола

VLAN – aware устройства могут принимать как нетегированные, так и тегированные кадры.

Если поступивший кадр тегированный, то передается без изменений в процесс пересылки.

Если поступивший кадр нетегированный, то маркируется Protocol VID и передается в процесс пересылки.

Protocol VLAN Identifier – это идентификатор VLAN ID, зависящий от поля EtherType входного кадра.

Входное правило на базе протоколов IP, ARP и др. необязательно для использования, однако если оно используется, то срабатывать оно будет первым, до срабатывания правила PVID.

Функция Subnet – based VLAN

Рис.10. Схема работы функции на основе подсети источника

Функция Subnet – based VLAN позволяет маркировать кадры в зависимости от подсети источника, при этом используется стандарт 802.1Q.
То есть Subnet – based VLAN не является отдельным видом VLAN, а является дополнительным входным правилом для VLAN 802.1Q.
Рассмотрим схему работы (рис. 10). Три устройства подключены к неуправляемому коммутатору, который в свою очередь подключен к коммутатору с поддержкой VLAN, требуется разделить трафик от устройств по различным VLAN. (с помощью функции Protocol VID это сделать невозможно, так как все устройства передают пакеты IP с одним и тем же номером протокола.)
Функция Subnet – based VLAN срабатывает после того, как пришедшие немаркированные кадры были помечены PVID. Она меняет тег PVID на тег, описанный заранее настроенными правилами, зависящий от подсети источника

Функция DHCP Vlan Override

Применяется в случае одновременного использования DHCP VLAN и Subnet based VLAN, и позволяет передавать DHCP – запросы в DHCP VLAN, а не в Subnet based VLAN.
Настраивается эта функция в разделах:
Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN
Команды CLI функции Subnet – based VLAN:
subnet – based – vlan <cr>
subnet – based – vlan name <name> source – ip <ip> mask – bits <mask – bits> vlan <vid> priority <0 7> <cr>
subnet – based – vlan name <name> source – ip <ip> mask – bits <mask – bits> vlan <vid> priority <0 7> inactive

Функция DHCP VLAN

При включенной функции DHCP VLAN (рис. 11) коммутатор обнаруживает широковещательные кадры DHCP – запросов с адресом источника «0.0.0.0» (кадры от узлов, запрашивающих адрес у DHCP – сервера) помечает их специальным DHCP VLAN, в котором находится DHCP – сервер. Ответы от DHCP – сервера транслируются обратно в VLAN клиента. Таким образом, удается избежать получения DHCP запросов обычными клиентами, тем самым снижается нагрузка на сеть.
Для работы функции DHCP VLAN необходимо включить функцию DHCP – Snooping. Настройка DHCP VLAN происходит в разделе: Advanced Application > IP Source Guard > DHCP Snooping > Configure
Команды CLI функции DHCPVLAN:
dhcp dhcp – vlan <vlan – id>
subnet – based – vlan dhcp – vlan – override

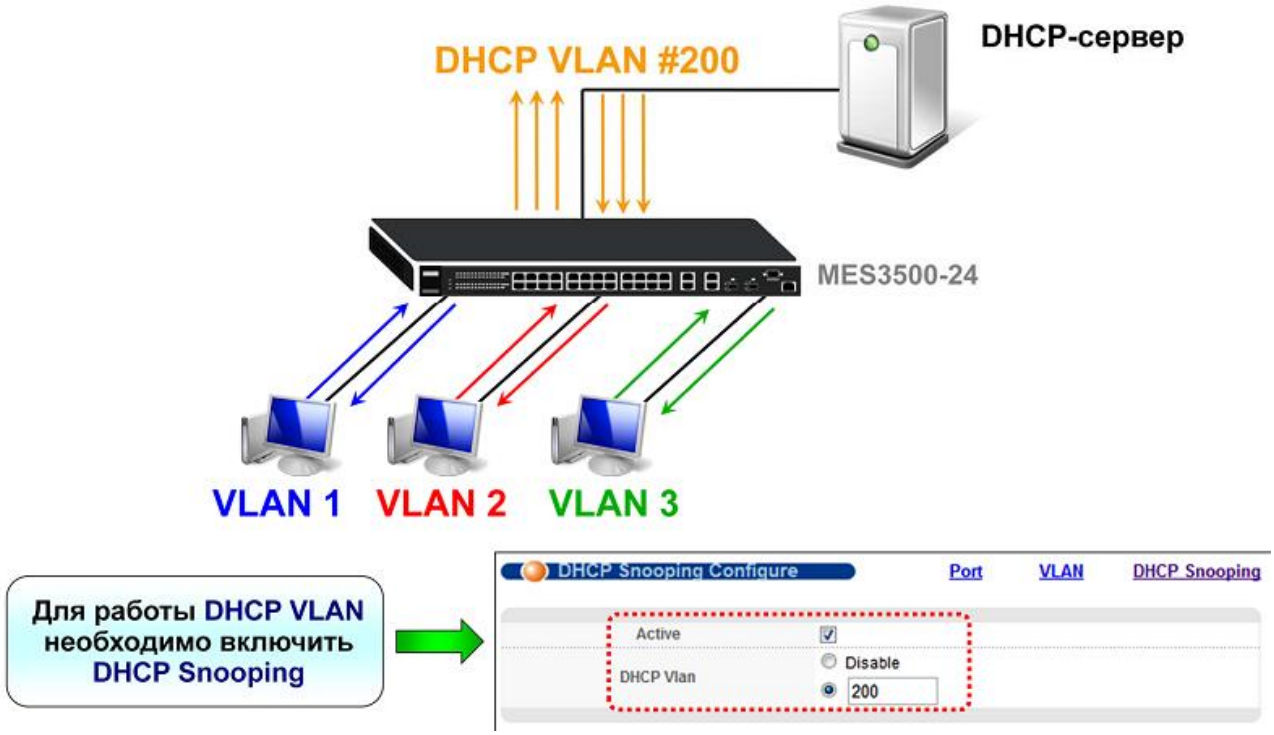

Рис. 11. Работа функции DHCP VLAN

Таблица Static VLAN

В меню VLAN отображается информация о текущих VLAN (статических и динамических).
Динамические VLAN регистрируются по протоколу GVRP, а статические вводятся вручную администратором.
Статические VLAN настраиваются в меню Static VLAN.
При настройке указывается имя,VID и состояния портов по отношению к данному VLAN:
Fixed – порт является выходным для указанной VLAN;
Forbidden – в порт запрещено передавать кадры, принадлежащие указанной VLAN;
Normal – в порт запрещено передавать кадры, принадлежащие VLAN, до тех пор, пока на этот порт не придет информация о данном VLAN по протоколу GVRP.
Состояние normal при отключенном GVRP эквивалентно состоянию forbidden.
В этом же меню настраивается Выходной процесс: установленный флаг Tx Tagging указывает, что маркер (тег) необходимо оставить при отправке кадра из порта.
С помощью статических таблиц VLAN регулируется только выдача маркированных кадров из коммутатора.
Например, если порт находится в состоянии forbidden по отношению к некоторому VLAN ID=200, то в порт запрещена выдача кадров с меткой 200. При этом получение на этот порт кадра с меткой 200 не запрещено. Проверку

входящих кадров можно включить отдельно, в меню VLAN Port Settings > Ingress Check.

Любой порт коммутатора одновременно может быть выходным для любого числа VLAN, вне зависимости от параметров выходного процесса (т.е. одновременно может производиться выдача кадров, как с тегами, так и без тегов).

Команды CLI:

vlan <1 – 4094> name <name – str>
vlan <1 – 4094> normal <port – list>
vlan <1 – 4094> fixed <port – list>
vlan <1 – 4094> forbidden <port – list>
vlan <1 – 4094> untagged <port – list>
vlan <1 – 4094> inactive
vlan <1 – 4094> help
vlan <1 – 4094> no fixed <port – list>
vlan <1 – 4094> no forbidden <port – list>
vlan <1 – 4094> no untagged <port – list>
vlan <1 – 4094> no inactive

GVRP (GARP VLAN Registration Protocol) – протокол динамической регистрации VLAN.

GVRP позволяет коммутаторам регистрировать (рис. 12) свои VLAN на соседних коммутаторах. Каждый коммутатор содержит таблицу Static VLAN, заполненную вручную, и пустую таблицу Dynamic VLAN.

После включения GVRP происходит обмен информацией о VLAN, и таблица Dynamic пополняется соответствующими записями.

Если нужно организовать передачу кадров VLAN 2 и 3, которые используются на коммутаторах A и D, то для того, что бы облегчить настройку остальных коммутаторов нашей сети и не создавать статические записи о этих VLAN на каждом коммутаторе, нужно включить поддержку протокола GVRP на всех коммутаторах сети через которые должны пройти кадры этих VLAN.

На коммутаторе B и C отсутствовали в статической таблице записи о 2 и 3 VLAN, то после обмена данными по GVRP порт 1 и 2 на коммутаторах B и C станет выходным для VLAN 2,3,4,5. Аналогично на порту 1 коммутаторов A и D появятся VLAN зарегистрированные на других коммутаторах.

GARP Timer – таймеры динамической регистрации VLAN. На каждом порту коммутатора есть три таймера: Join, Leave и Leave All.

В настройках коммутатора выставляются предельные значения для этих таймеров (таймауты), которые указываются в миллисекундах.

При достижении таймаута Join через порт осуществляется рассылка кадра с просьбой покинуть VLAN, порт устанавливается в состояние «Leaving» и по истечении таймера Leave происходит удаление записей, если за это время не получен кадр Join. Если какой – либо VLAN удаляется из таблицы (вручную

или автоматически), коммутатор посылает в сеть кадр Leave, чтобы другие коммутаторы тоже удалили VLAN из динамических таблиц.
Кроме того, каждый коммутатор рассылает кадры Leave All с периодичностью, указанной в поле Leave All.
При получении кадра Leave All все динамические записи переключаются в состояние «Leaving», а последующие кадры Join восстанавливают необходимую часть таблицы.
Такая процедура позволяет синхронизировать динамические VLAN

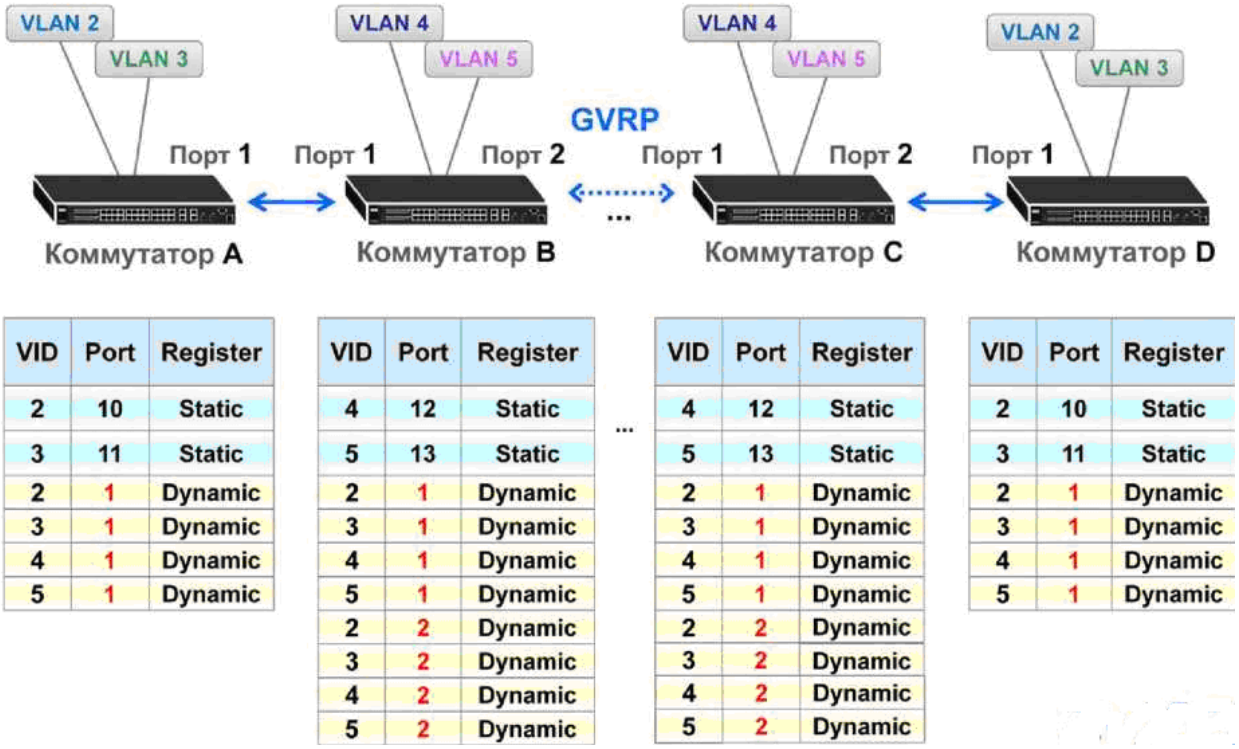

Рис. 12. Работа протокола динамической регистрации VLAN

VLAN на портах

Если включен Ingress check, то на порт принимаются только кадры с VLAN ID, для которого указанный порт является выходным.
PVID (Port VLAN Identifier) — идентификатор VLAN по умолчанию для порта – этим идентификатором будут помечаться приходящие нетегированные кадры.
GVRP — протокол передачи информации о VLAN по сети с одного коммутатора на другой.
Если требуется, его нужно включить как на всем коммутаторе, так и на отдельных портах.
Acceptable Frame Type — допустимые типы принимаемых кадров: любые, только с тегами, только без тегов.
VLAN Trunking — функция, позволяющая выпускать из порта кадры, принадлежащие неизвестным VLAN (VLAN называется неизвестным, если он отсутствует в таблице VLAN).

Isolation — порты, на которых включена данная опция, изолируются друг от друга, т.е. данные, пришедшие на такой порт, могут уйти только к CPU (управление) или к порту, на котором данная функция выключена.

Команды CLI:

interface port – channel <port – list> pvid <1 – 4094>
interface port – channel <port – list> ingress – check
interface port – channel <port – list> gvrp
interface port – channel <port – list> frame – type <all|tagged|untagged>
interface port – channel <port – list> vlan – trunking
interface port – channel <port – list> vlan1q port – isolation

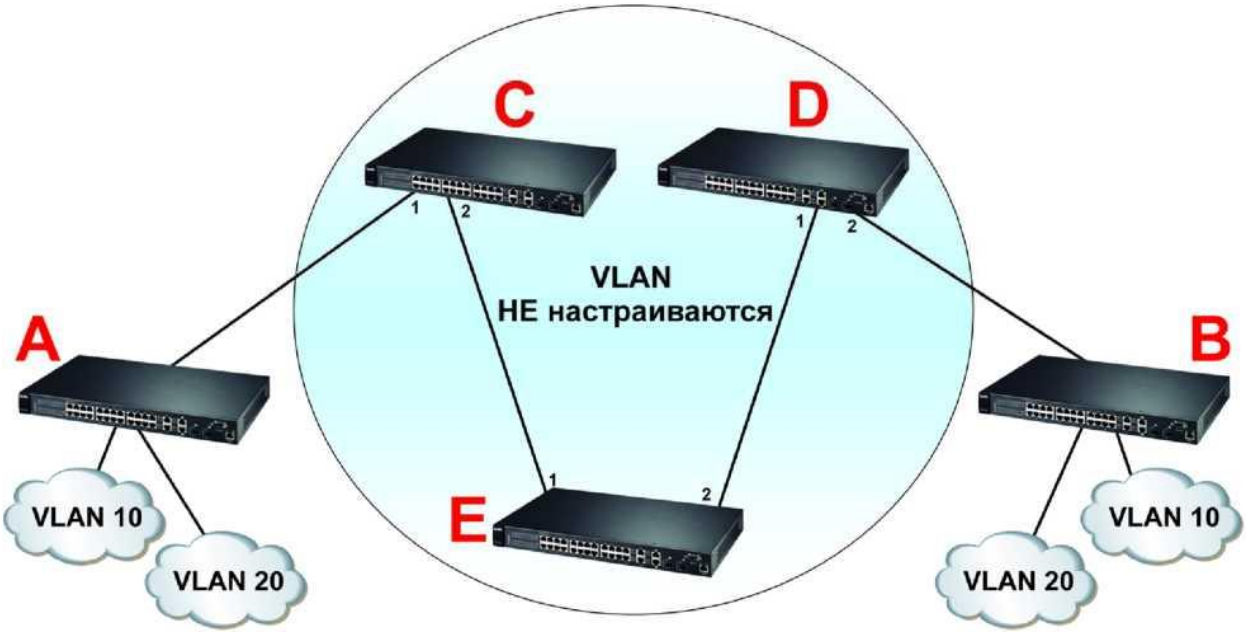

Рис. 13. Работа функции VLAN Trunking

Включение на порту функции (рис. 13) VLAN Trunking, разрешает выпускать из этого порта кадры, принадлежащие любым VLAN, за исключением тех, которые заведены статически или получены динамически по GVRP.

Другими словами в порт VLAN Trunk уходят только неизвестные VLAN, остальные же работают в соответствии с настройками, т.к. уже прописаны в таблицах VLAN и портов.

Назначение этой функции следующее – если коммутатор стоит между двумя устройствами, формирующими VLAN (например, могут регистрироваться динамические VLAN, которые нужно "проводить" прозрачно в другие участки сети), то достаточно на двух портах включить VLAN Trunking и коммутатор эти VLAN пропустит.

Иначе пришлось бы в явном виде вводить все возможные VLAN в таблицу.

Пусть на коммутаторах A и B настроены VLAN 10 и VLAN 20.

Коммутатор A и B соединены через коммутаторы C, D и E.

Для корректной передачи трафика от коммутатора A к коммутатору B достаточно включить на портах коммутаторов C, D и E функцию VLAN Trunking, при этом создавать VLAN вручную или же при помощи протокола GVRP необходимости нет.

Команды CLI:
interface port – channel <port – list> vlan – trunking

Guest VLAN

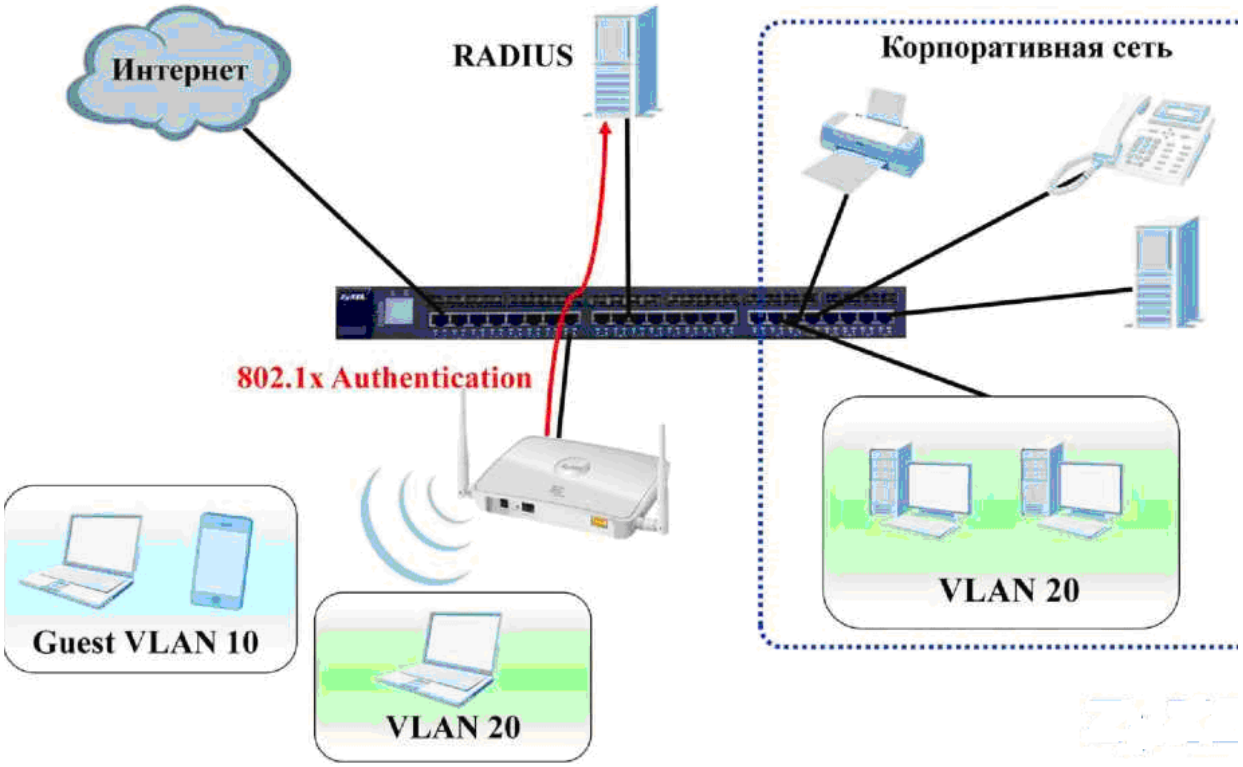

Рис. 14. Схема сети с функцией Guest VLAN

Guest VLAN (рис. 14) представляет собой сочетание аутентификации 802.1x и VLAN.
Перед получением доступа в сеть пользователь обязан пройти аутентификацию на RADIUS сервере.
При успешно пройденной аутентификации, пользователь автоматически включается в настроенный на коммутаторе статический VLAN (либо в VLAN, полученный в ответе от RADIUS сервера), членам которого разрешается доступ в корпоративную сеть.
В случае неудачного прохождения аутентификации, пользователь включается в неавторизованный VLAN, именуемый Guest VLAN (обычный VLAN).
Такой VLAN отдельно создается на коммутаторе, и членам данной VLAN разрешается только доступ в Интернет.
Guest VLAN работает в двух режимах: 1) Multi – Host; 2) Multi – Secure.
В режиме Multi Host аутетифицируется порт, т. е. фактически только первый абонент, подключившийся к порту.
В режиме Multi – Secure аутентифицируются все абоненты, подключенные к данному порту.
Последовательность настройки следующая:

1. Включить аутентификацию 802.1x на абонентском порту.
2. Настроить статический VLAN 10 на абонентском порту.

3. Настроить Guest VLAN 10 на абонентском порту.
4. Настроить статический VLAN 20 на абонентском порту.
5. Настроить PVID 20 на абоненском порту.

При успешной аутентификации абонент будет включён во VLAN 20, при неудачной — в Guest.

Функция Private VLAN

Private VLAN (рис. 15) предназначена для изоляции абонентов, подключенных к разным портам, но принадлежащих одному VLAN.
Promiscuous порт может взаимодействовать с любым портом, включённым в одну группу Private VLAN, т.е. такой порт является uplink портом.
Этот механизм является более гибким, чем Port Isolation

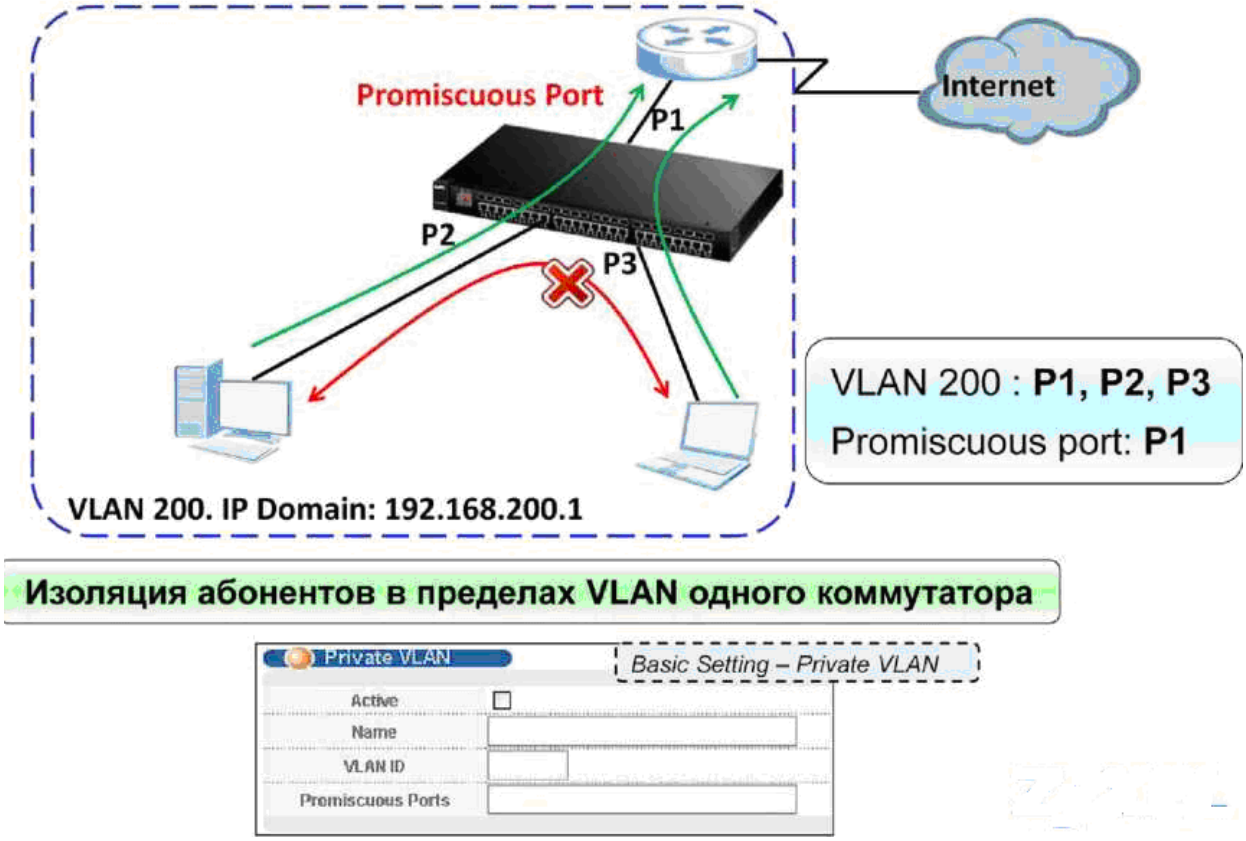

Рис.15. Схема сети с функцией Private VLAN

Функция Smart Isolation

Основной задачей Smart Isolation является изоляция трафика между абонентами, подключенными к разным коммутаторам, в рамках некоторого сегмента сети.
Поскольку Port Isolation и Private VLAN изолируют трафик только между абонентами одного коммутатора и не могут передать сведения об изоляции соседним коммутаторам, то при организации колец RSTP/MSTP абоненты, подключенные к соседним коммутаторам, могут обмениваться данными без участия вышестоящего шлюза.

Поскольку в последнее время для всех поставщиков услуг доступа к сети является обязательным требование — прохождение всего трафика абонентов через шлюз провайдера, требуется настроить запрет коммутаторам передавать абонентский трафик во все порты, кроме up – link.
Smart Isolation работает при одновременном включении Port Isolation или Private VLAN и RSTP или MSTP
При таких настройках трафик от абонентов передаётся только в порт Root. Трафик же пришедший на Root порт может быть передан на Designated порт. Требуется включение Port Isolation или Private VLAN с RSTP или MSTP

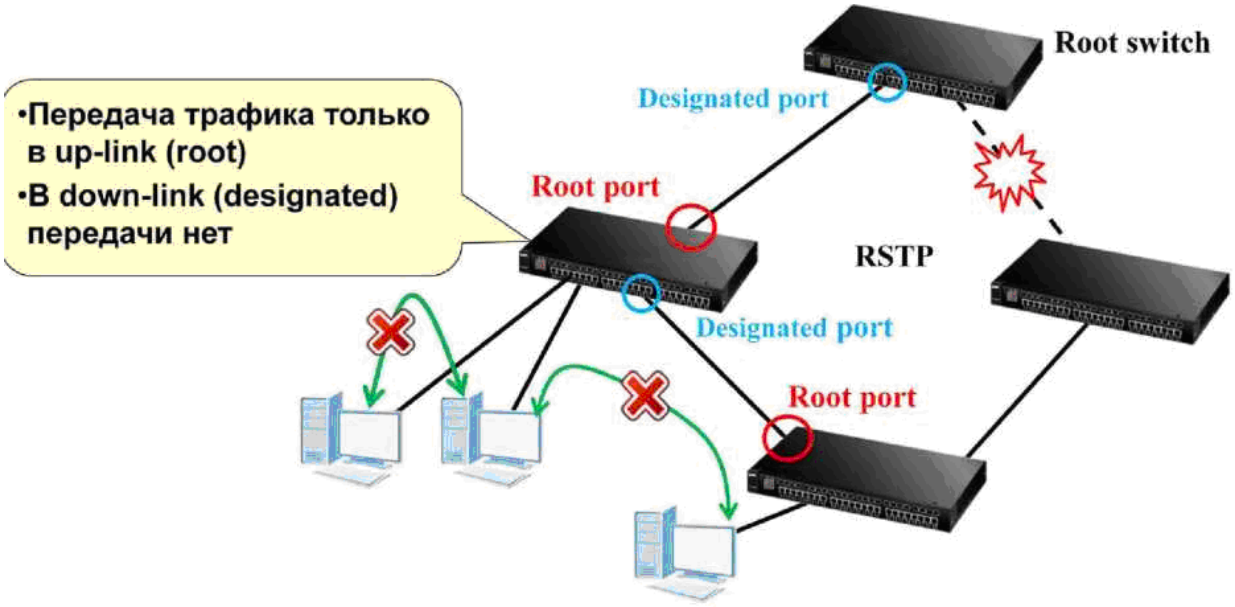

Рис.16. Схема задачи Smart Isolation

Для включения функции Smart Isolation (рис. 16) достаточно поставить одноименный флаг.
Но, к этому моменту уже должны быть настроены Port Isolation или Private VLAN и RSTP или MSTP.

QinQ

QinQ – технология, позволяющая назначать два VLAN – тега Ethernet – фрейму (рис. 17).
QinQ – технология активно используется провайдерами для увеличения количества доступных VLAN или прозрачного пропускания клиентских тегированных VLAN.
QinQ – это двухуровневое вложение меток VLAN в кадр, а также трансляция значений меток на лету.
Поддерживается не всеми устройствами с поддержкой VLAN.
Данная технология известна как Q – туннелирование и описана в стандарте IEEE802.1 ad.

QinQ не позволяет полноценно разделить домены сетей пользователей и провайдера, а позволяет преодолеть ограничение на количество идентификаторов VLAN в сети.

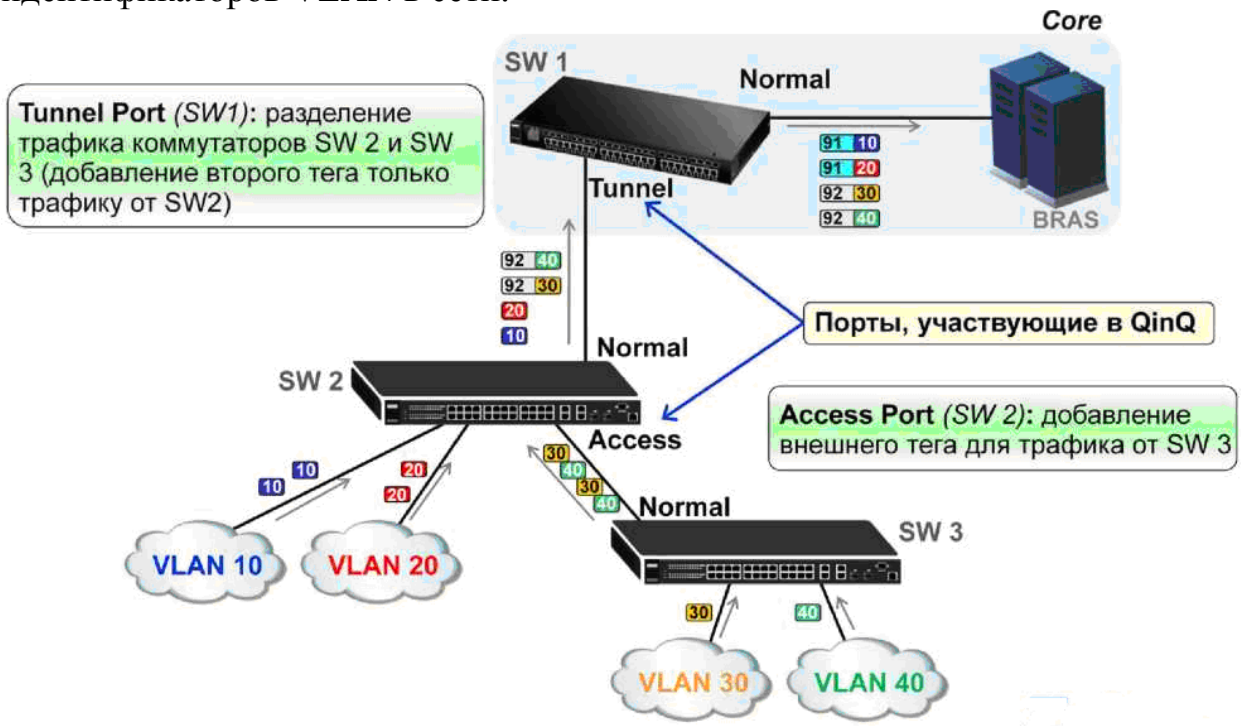

Рис.17. Работа QinQ – технологии

Входной процесс QinQ – Access Port

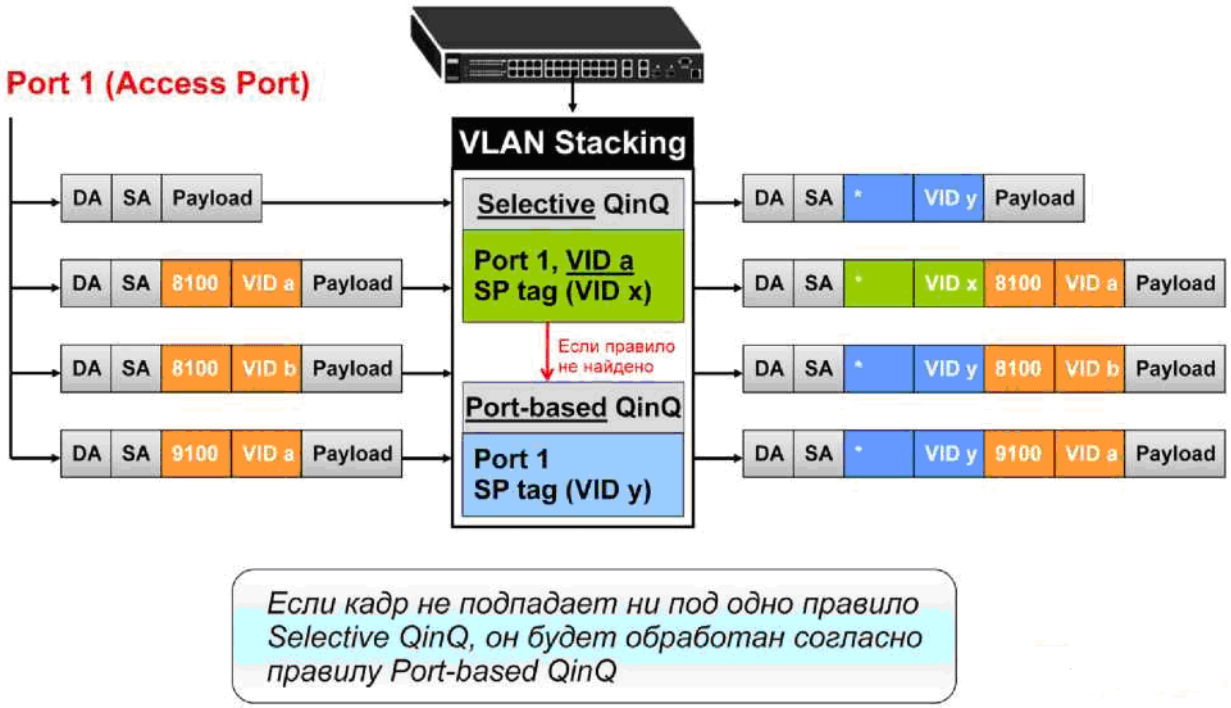

Рис.18. QinQ Access Port (Входной процесс обработки кадров QinQ)

При получении кадра на Access Port (рис. 18) (Входной процесс обработки кадров):

1. Если кадр без тега, на него ставиться тег с VID из настроек Port – based QinQ
2. Если кадр с тегом, у которого TPID равен 8100 и VID_a, попадающий под правило Selective QinQ, то добавляется новый тег с VID_x
3. Если кадр с тегом, у которого TPID равен 8100, но VID не попадает под правило Selective QinQ, то добавляется новый тег в соответствии с настройками Port – based QinQ

Если кадр пришел с тегом, у которого TPID отличается от 8100 (например, 9100, 88a8 и др.), коммутатор считает такой кадр нетегированным, и ставит тег с VID из настроек Port – based QinQ.

Правила Selective QinQ не применяются к Tunnel port.

Т.е., кадр, поступивший на коммутатор с Tunnel port, будет обрабатываться согласно правилам Port – based QinQ.

Входной процесс в этом случае таков: коммутатор добавляет новый тег только к тем кадрам, у которых поле TPID (у уже имеющегося) тега отличатся от настроенного на порту коммутатора Tunnel Port TPID.

Если же на поступившем кадре поле TPID уже имеющегося тега совпадает с настроенным Tunnel Port TPID на порту коммутатора, то тег добавляться не будет.

Входной процесс QinQ – Tunnel Port

Правила Selective QinQ не применяются к Tunnel port(рис. 19).

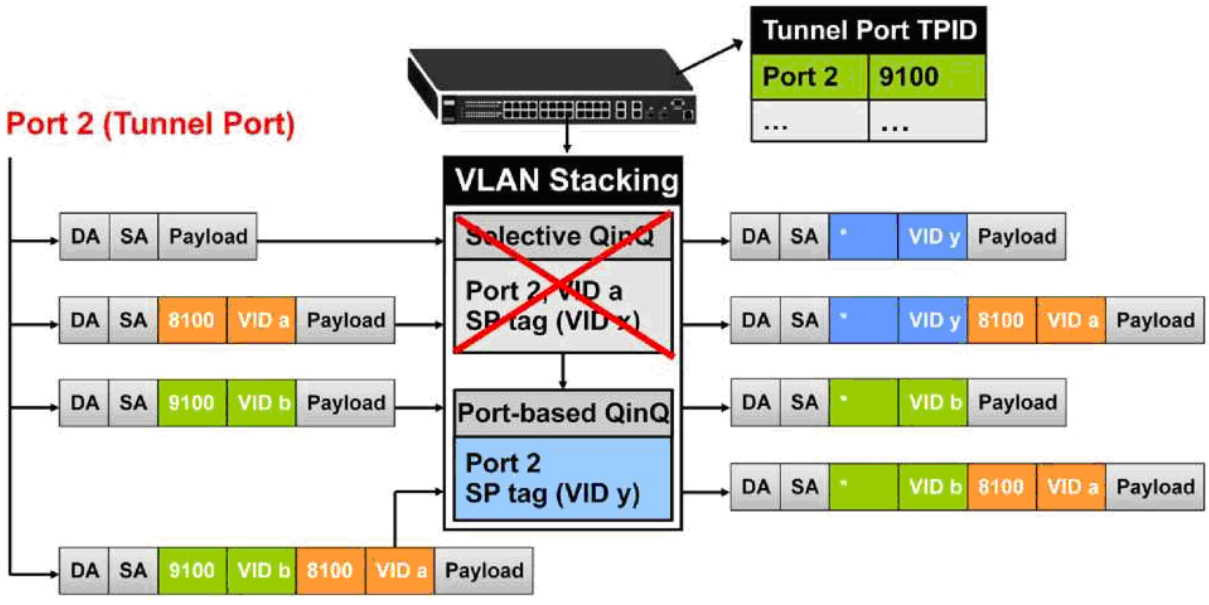

Рис.19. QinQ Tunnel Port (Входной процесс обработки кадров Q – in – Q)

Т.е., кадр, поступивший на коммутатор с Tunnel port, будет обрабатываться согласно правилам Port – based QinQ. Входной процесс для этого случая показан ниже.

Коммутатор добавляет новый тег только к тем кадрам, у которых поле TPID (у уже имеющегося) тега отличатся от настроенного на порту коммутатора Tunnel

Port TPID.
Если же на поступившем кадре поле TPID уже имеющегося тега совпадает с настроенным Tunnel Port TPID на порту коммутатора, то тег добавляться не будет.

Выходной процесс QinQ(рис. 20):

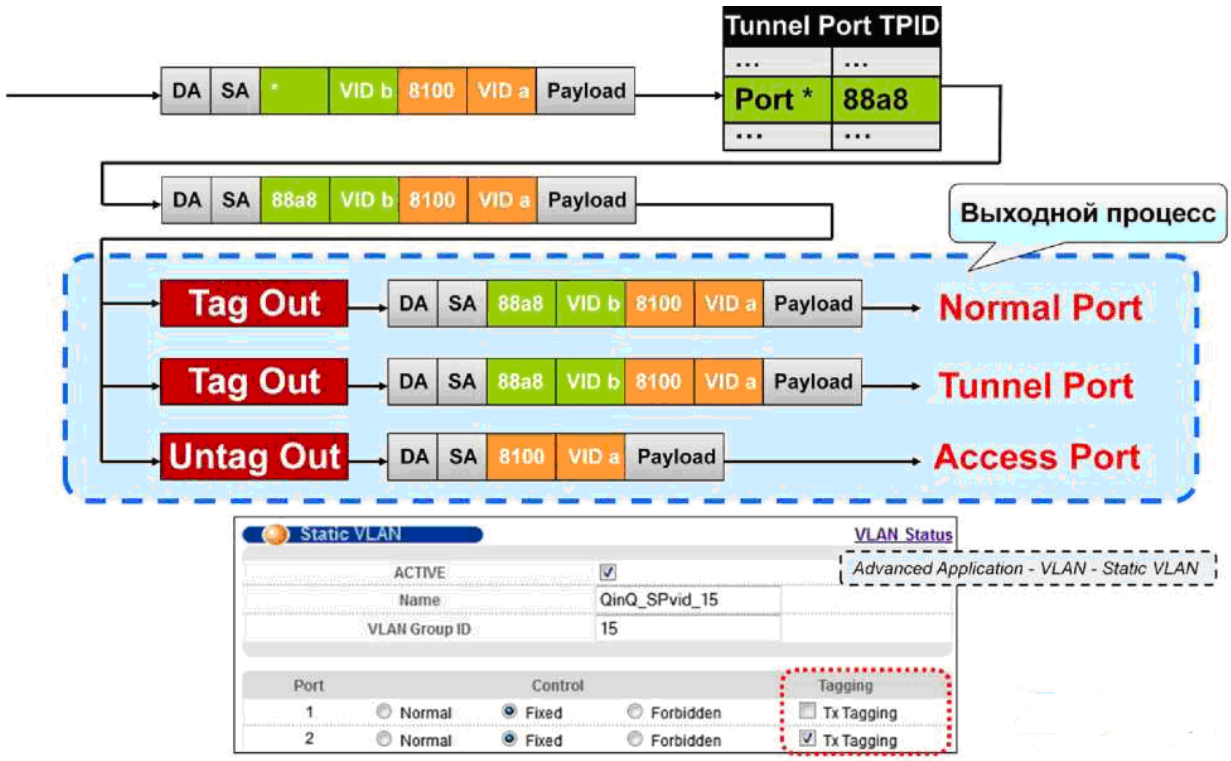

Рис. 20. Выходной процесс QinQ

Выходной процесс представлен ниже.

1. Заполнить поле TPID в соответствии с настройками порта
2. Для Tunnel port кадр должен выходить из порта с дополнительным тегом: в настройках Static VLAN – оставить галку Tx Tagging
3. Для Access port кадр должен выходить из порта без дополнительного тега: в настройках Static VLAN – убрать галку Tx Tagging
4. Для порта в роли «Normal port» (роль для процесса QinQ): если порт который подключен к сети провайдера – обязательно оставить галку Tx Tagging, ведь кадры, идущие в сеть провайдера должны уходить с тегами.

VLAN Mapping

Если у провайдера транспортных услуг (Service Provider, SP) уже имеется сеть с настроенными выходными VLAN, и внесение изменений нежелательно, как и использование VLAN Trunking,
то возможно использовать функцию VLAN Mapping для проброса трафика клиентов через сеть SP (рис. 21).

VLAN Mapping позволяет перемаркировать клиентский трафик из VLAN A в VLAN B, уже настроенный в сети SP.
Таким образом, клиентский трафик (VLAN A) будет проходить по сети Service Provider в VLAN B, и переводиться обратно в VLAN A при выдаче клиенту.

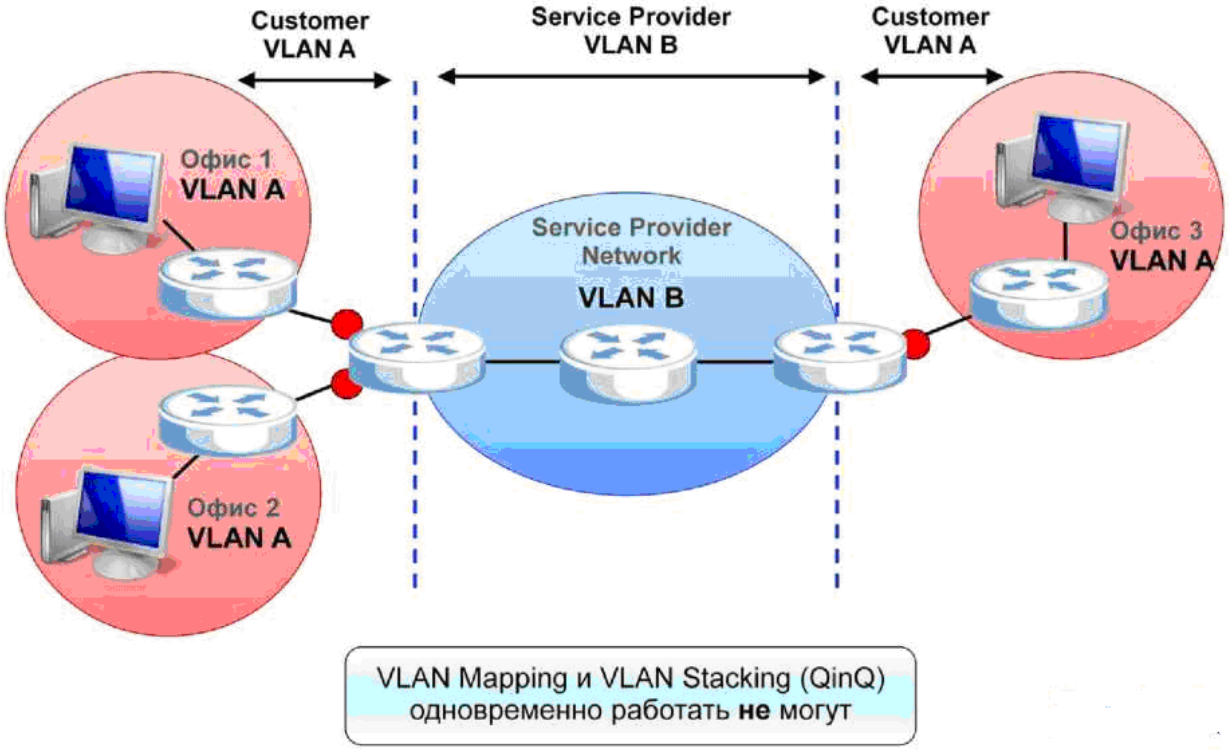

Рис.21. Работа проброса трафика клиентов через сеть

Функция Port Security

Функция Port Security позволяет ограничить количество узлов, подключенных к порту.
Можно включить эту функцию и запретить динамическое изучение MAC – адресов (разрешить только статические MAC – записи). Если же динамическое изучение разрешено, то количество адресов будет ограничено полем Limited Number of Learned MAC Address.
Функция Port Security используется для защиты от атак, направленных на переполнение таблицы коммутации, и от атак типа MAC – spoofing (подмены MAC – адреса на сетевом интерфейса ПК злоумышленника с целью обойти списки контроля доступа L2, получить доступ к серверам, маршрутизаторам, или скрыть компьютер, или заставить коммутатор отправлять злоумышленнику пакеты, предназначавшиеся другому устройству).
В этом же разделе включается функция MAC Freeze на определенных портах. Она предназначена для обеспечения безопасности на портах при динамическом заполнении таблицы MAC – адресов. После включения MAC Freeze на порту, коммутатор добавляет динамически изученные MAC – адреса в таблицу статических MAC – адресов, и прекращает дальнейшее запоминание MAC – адресов. Любое устройство с MAC – адресом, неизвестным коммутатору, будет заблокировано.

Например: администратор сети проверяет таблицу MAC – адресов на коммутаторе и видит, что она заполнена правильно, и все необходимые хосты присутствуют в таблице. Тогда администратор может остановить (заморозить – freeze) изучение MAC на этом порту, то есть запретить устройствам с другими MAC – адресами подключаться к этому порту.

Функция Link Aggregation

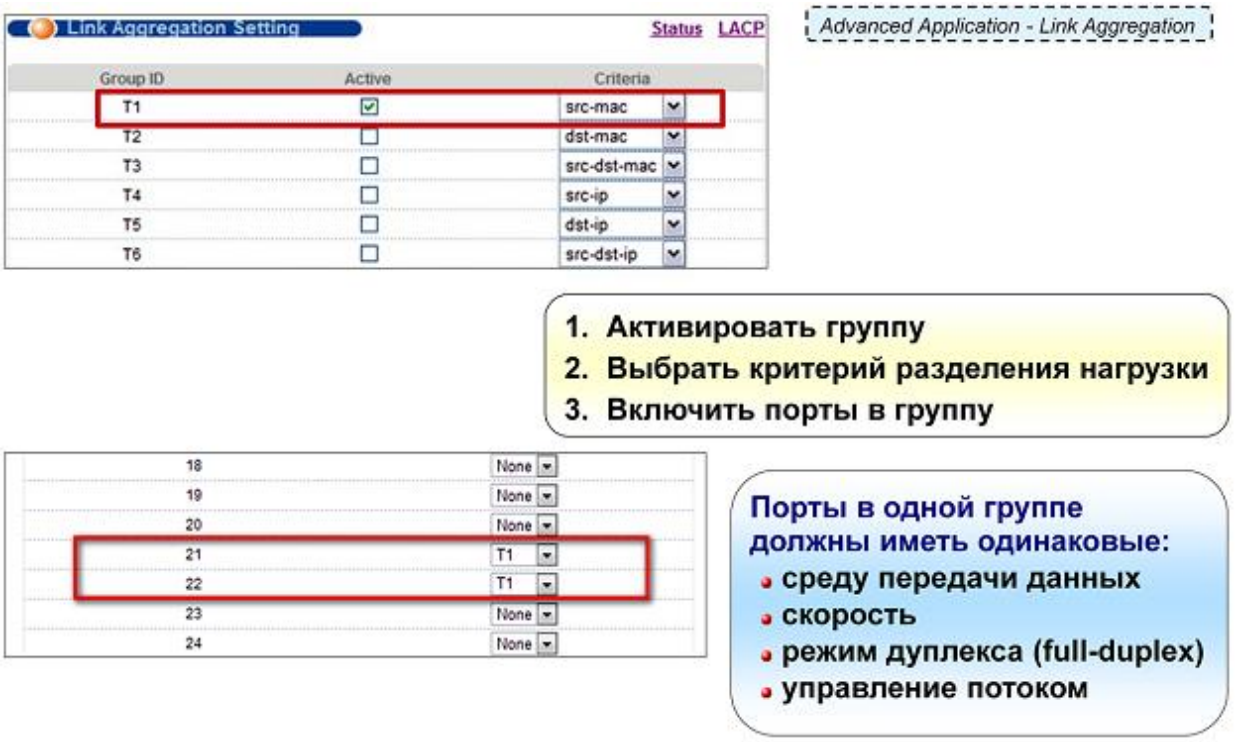

Рис. 22. Настройка агрегирования

Агрегирование (Trunk **или** Link Aggregation) – это объединение нескольких физических портов в один логический для увеличения пропускной способности и для обеспечения повышенной отказоустойчивости. Объединение нескольких физических линий в одну логическую: до 32 групп, до 24 портов в группе Также при агрегировании осуществляется поддержка протокола LACP
Стандарт Link Aggregation отвечает за **разделение** нагрузки, но не за **балансировку** нагрузки (Load Sharing vs. Load Balancing). Load Sharing равномерно распределяет таблицу MAC – адресов между всеми портами, входящими в агрегированный канал.

Таким образом, кадры с одним и тем же MAC – адресом назначения пойдут только по одному физическому каналу без увеличения скорости.

Принцип Load Sharing дает увеличение скорости передачи только в том случае, когда по агрегированному каналу передаются кадры с разными MAC – адресами назначения.

Количество групп агрегирования и максимальное число портов в этой группе, зависит от модели коммутатора.
В таблице (рис. 22) приведены данные для модельных линеек коммутаторов.

Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) — протокол управления агрегациями, описан в спецификации IEEE 802.3ad, в которой определена возможность объединения нескольких физических линий в один логический канал. Использование протокола LACP не обязательно, и не в каждой ситуации он необходим, рассмотрим две схемы:

Схема #1:

Агрегация настраивается между двумя коммутаторами, которые соединены напрямую друг с другом. Если один из физических каналов будет разорван, то оба коммутатора сами обнаруживают потерю физического соединения и перестают передавать данные по данному физическому соединению. Таким образом, использовать протокол LACP смысла не имеет.

Схема #2:

Пусть агрегация настраивается между двумя коммутаторами, при этом коммутаторы соединены через два медиаконвертера. Если разорвалось физическое соединение между медиаконвертерами, физический линк на коммутаторе может и не погаснуть (зависит от медиаконвертора). Следовательно, коммутаторы будут передавать данные по логически нерабочему соединению. В этой ситуации необходимо использование протокола LACP, который будет проверять работоспособность каждого физического соединения.

При настройке Link Aggregation обратим внимание на то, что порты, которые включаются в одну агрегацию, должны иметь одну и ту же среду передачи данных, скорость, режим дуплекса и настройки управления потоком (Flow Control).

Функция Link Aggregation имеет дополнительную возможность в настройке — шесть критериев разделения нагрузки между портами в одной группе агрегации:

1. Src – mac — базируется на основе MAC источника
2. Dst – mac — базируется на основе MAC назначения
3. Src – dst – mac (значение по умолчанию) — базируется одновременно на основе MAC источника и MAC назначения
4. Src – ip — базируется на основе IP источника
5. Dst – ip — базируется на основе IP назначения
6. Src – dst – ip — базируется одновременно на основе IP источника и IP назначения

Если входящие пакеты не имеют информации об IP при выборе критерия, например, Src – ip, тогда разделение нагрузки между портами в одной группе агрегации будет основываться на критерии Src – mac. Аналогично при выборе других критериев основанных на базе IP:

Команды CLI:

trunk <T1|T2|T3|T4|T5|T6>

trunk <T1|T2|T3|T4|T5|T6> lacp

trunk <T1|T2|T3|T4|T5|T6> interface <port – list>
trunk <T1|T2|T3|T4|T5|T6> criteria <src – mac|dst – mac|src – dst – mac|src – ip|dst – ip|src – dst – ip> no trunk <T1|T2|T3|T4|T5|T6> criteria <cr>
При настройке функции заполняют следующие поля:
System Proirity — приоритет, при помощи которого выбирается Master коммутатор. Чем меньше значение, тем больше шансов стать Master коммутатором.
LACP Timeout — интервал времени, через который будет проверятся работоспособность каждого физического соединения. Если порт не ответит после трех попыток, его состояние будет считаться “down”, и он удаляется из группы. После проверки соединений Master коммутатор будет отправлять Slave коммутатору текущую конфигурацию, то есть информацию о том, по каким физическим каналам можно передавать данные.
При настройке функции Link Aggregation, на портах коммутатора должны быть выключены следующие 4 функции, конфликтующие с Link Aggregation:

1. Filter.
2. Port Mirror.
3. Bandwidth Control.
4. Port Security.

Команды CLI:
lacp <cr>
lacp system – priority <1 – 65535>

Функция Port Mirroring (зеркалирование портов)

Функция Port Mirroring (зеркалирование портов) – позволяет дублировать трафик на порт мониторинга (рис. 23).

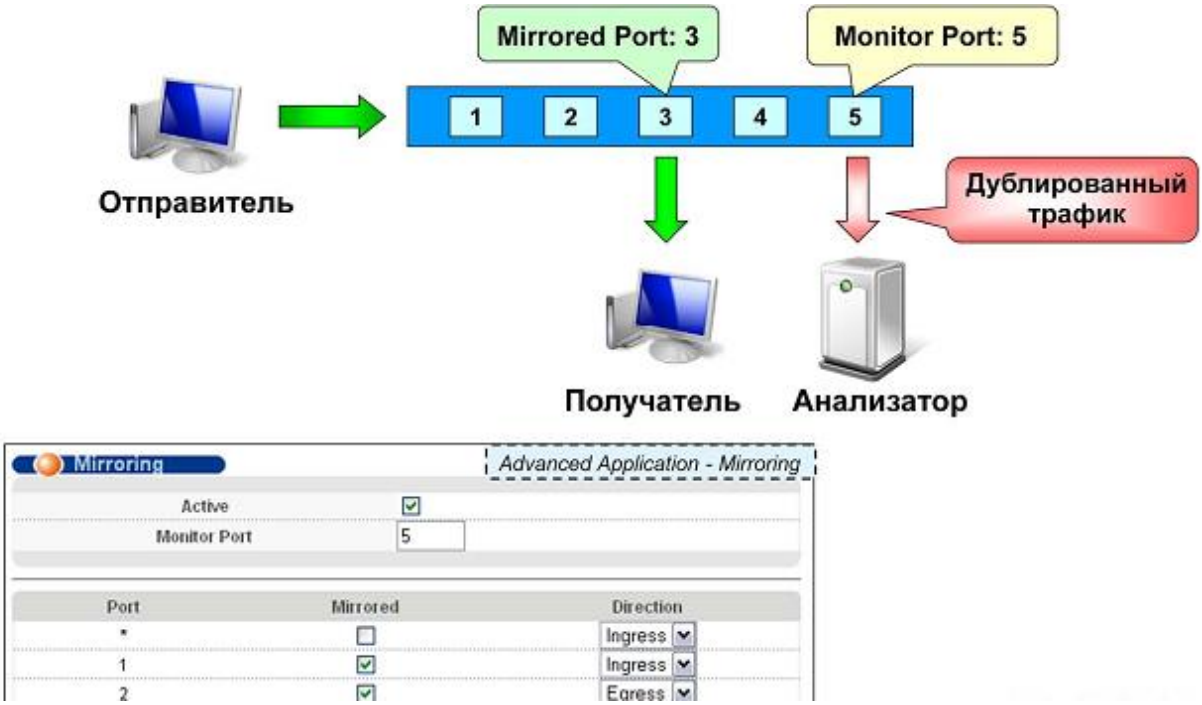

Рис.23. Схема работы и настойка зеркалирования

Возможно копирование как одного из потоков (входящего/исходящего), так и обоих потоков, с одного или нескольких портов.
При настройке необходимо включить функцию зеркалирования в соответствующем меню, выбрать порт, на который будут дублироваться кадры (Monitor Port), и выбрать направления.

Далее необходимо выбрать порты Mirrored, данные с которых будут дублироваться на порт Monitor. Порт, который выбран как Monitor Port, нельзя указать как Mirrored. Monitor порт может быть только один.

Зеркалирование удобнее выполнять с помощью классификатора и политики, так как в этом случае можно анализировать не весь подряд трафик, а только пакеты определенного типа.

Команды CLI:

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

Многоадресная рассылка Multycast

Групповая рассылка (multicast) работает по принципу «один источник – группа получателей». Рассмотрим следующий пример.

В сети существует три получателя сообщений с одного сервера. Сервер посылает только одно сообщение, которое «размножится» сетевыми устройствами и поступит группе подписчиков. Для этого необходимо организовать группу, и каждый получатель должен сообщить сетевым устройствам о присоединении к группе, либо на устройствах будет статическая запись о принадлежности того или иного физического порта к конкретной группе.
Для многоадресной рассылки зарезервирован диапазон ip адресов: с 224.0.0.0 по 239.255.255.255. Часть адресов в начале этого диапазона используется различными протоколами (OSPF, RIP – 2M, DVMRP и т д.) а так же для обращения к специальным группам, например:

- 224.0.0.1 : Все узлы данной подсети.
- 224.0.0.2 : Все маршрутизаторы данной подсети.
- 224.0.0.9 : маршрутизаторы RIP – 2.

Multycast MAC

Коммутаторы L2 для передачи кадров используют MAC – адреса. Механизм перевода multicast IP адреса в multicast MAC адрес привелен ниже.
Первые 3 октета multicast MAC адреса определены стандартом и равны 01:00:5e, а также определен первый бит четвертого октета и он равен 0. Остальные 23 бита копируются из multicast IP адреса.

При этом происходит потеря 1 бита информации (старшего бита из последних трех октетов), то есть, возможна ситуация, что различные multicast IP адреса будут преобразованы в одинаковые multicast MAC адреса, а именно:
224.1.1.1, 224.129.1.1
225.1.1.1, 225.129.1.1
…
238.1.1.1, 238.129.1.1
239.1.1.1, 239.129.1.1
все эти адреса будут преобразованы в один и тот же multicast MAC адрес – 01:00:5e:01:01:01

Static multucast forvarding

Самый простой вариант использования многоадресной рассылки – это создание статических записей, то есть ручная привязка физического порта к какой – либо multicast группе

Команды CLI:

multicast – forward name <name> mac <mac – addr> vlan <vlan – id> interface port – channel <port – list>
multicast – forward name <name> mac <mac – addr> vlan <vlan – id> inactive

IGMP

IGMP (Internet Group Management Protocol) – межсетевой протокол управления группами, используется для контроля и управления multicast – трафиком через локальную сеть в автоматическом режиме. IGMP работает только между маршрутизатором и клиентским хостом. Согласно модели OSI, IGMP – протокол сетевого уровня, но, несмотря на это, передается он поверх протокола IP.

Принцип работы протокола IGMPv1

Для присоединения к группе необходимо отправить IGMP – report на групповой адрес (на схеме – 224.1.1.1), чтобы стать членом группы. IGMP – Server отправляет General IGMP – query по адресу 224.0.0.1. Этот запрос используется для определения наличия хотя бы одного члена группы в подсети.
Когда хост получает IGMP – query, он запускает таймер обратного отсчета для каждой группы multicast, в которую он входит. Когда счетчик обнулится, хост отправит сообщение IGMP – report в группу, которая ассоциирована с таймером, чтобы сообщить, что он все еще является членом группы. Если узел хочет покинуть группу, он просто перестает отправлять какие – либо сообщения по протоколу IGMP.
В **IGMPv2** для присоединения к группе необходимо отправить сообщение IGMP – report на адрес группы. Если в сети существует несколько маршрутизаторов, то маршрутизатор с наименьшим IP – адресом выбирается в

качестве источника запросов. Другие маршрутизаторы не будут отправлять IGMP – query пакеты клиентам.
Алгоритм работы члена группы в подсети такой же, как и для IGMPv1, за исключением того, что значение таймера зависит от величины maximum response time. Если узел хочет покинуть группу, он отправляет сообщение IGMP – leave на адрес 224.0.0.2 (все маршрутизаторы подсети).
Когда маршрутизатор получает сообщение IGMP – leave, он отправляет запрос Group Specific IGMP – query для обнаружения хотя бы одного участника группы. Запрос отправляется на адрес группы. По сравнению с General IGMP – query, такой запрос не перегружает сеть ответами членов всех групп.

Принцип работы протокола IGMPv3

В IGMP v 3 была добавлена поддержка фильтрации адресов (source filtering). С помощью этого механизма узел может сообщить, с каких адресов он хочет получать пакеты, а с каких – нет.
При использовании протокола IGMPv3 получатели сообщают о принадлежности к группе многоадресной рассылки, используя приведенные ниже режимы.
Режим INCLUDE. В этом режиме получатель сообщает о членстве в группе узлов и приводит список адресов источников (список INCLUDE), от которых желательно получение данных.
Режим EXCLUDE. В этом режиме получатель сообщает о членстве в группе многоадресной рассылки и предоставляет список адресов источников (список EXCLUDE), от которых получение потоков данных нежелательно. При этом узел будет получать потоки данных только от тех источников, IP – адреса которых не перечислены в списке EXCLUDE. Для получения данных от всех источников узлы используют режим принадлежности к группе с пустым списком EXCLUDE.

IGMP Snooping

IGMP работает между клиентом и маршрутизатором на 3 – м и 4 – м уровне. По умолчанию коммутатор 2 – го уровня перенаправляет пакеты IGMP на все порты, т.к. MAC адрес назначения отсутствует в его таблице фильтрации. Таким образом, на втором уровне multicast теряет смысл групповой рассылки и приравнивается к broadcast.
Для решения этой проблемы на уровне L2+ используется технология IGMP Snooping. Коммутатор/мост просматривает полученные multicast кадры (Query и Report) для составления IGMP – таблицы. Эта таблица содержит записи multicast IP – адресов и портов. Теперь трафик multicast перенаправляется только в порты, входящие в группу.
Если группа multicast в коммутаторе не зарегистрирована, то выполняется действие unknown flooding или unknown discard в зависимости от настроек^
Unknown flooding: кадры неизвестных групп будут отправлены на все порты (flooding).

Unknown discard: кадры неизвестных групп передаваться не будут.
Таким образом, принципиальная разница между IGMP Server и IGMP Snooping заключается в том, что IGMP Server умеет создавать IGMP – пакеты, а IGMP Snooping умеет только просматривать проходящие IGMP – пакеты.

Настройка IGMP

Для включения отслеживания multicast трафика IGMP необходимо установить переключатель Active.
Querier – включает на коммутаторе режим IGMP Snooping Querier Proxy.
Host Timeout – время в секундах, по истечении которого коммутатор удаляет запись об участии в группе IGMP при отсутствии сообщений IGMP Report от порта.
802.1p Priority – указывается приоритет от 0 до 7, который, устанавливается коммутатором для исходящих управляющих пакетов IGMP. Выбор No – **Change** – оставляет приоритет 802.1p без изменений.
IGMP Filtering – активирует режим фильтрации IGMP с помощью заранее созданных фильтров групп, определяющих к каким multicast – рассылкам может подключаться абонент на порту.
Unknown Multicast Frame – действие коммутатора при получении неизвестного multicast – кадра (Drop – отбрасывание; Flooding – пересылка кадра на все порты)
Reserved Multicast Group – действие коммутатора при получении multicast кадра из зарезервированного диапазона 224.0.0.0~224.0.0.255, который используются для служебных нужд LAN подсети и некоторыми сетевыми протоколами (Например, RIPv2 и OSPF).
Команды CLI:
igmp – snooping <cr>
igmp – snooping 8021p – priority <0 – 7>
igmp – snooping host – timeout <1 – 16711450>
igmp – snooping leave – timeout <1 – 16711450>
igmp – snooping reserved – multicast – group <drop|flooding>
igmp – snooping unknown – multicast – frame <drop|flooding>
interface port – channel <port – list> igmp – immediate – leave
interface port – channel <port – list> igmp – group – limited <cr>
interface port – channel <port – list> igmp – group – limited number <number>
interface port – channel <port – list> igmp – filtering profile <name>
interface port – channel <port – list> igmp – querier – mode <auto|fixed|edge>

IGMP filtering

Профиль фильтрации IGMP определяет диапазон групп multicast, к которым могут подключаться пользователи, подключенные к коммутатору. Профили назначаются конкретным портам коммутатора. Каждому порту может быть назначен только один профиль, однако по одному профилю могут работать сразу несколько портов.

Фильтры IGMP позволяют определить список групп, к которым может подключиться клиент с определенного порта. В каждом фильтре можно настроить несколько диапазонов разрешенных IGMP адресов. Максимальное число диапазонов на коммутатор равно 256.

Immed. Leave – функция позволяет отключать порт от multicast – рассылки сразу же при получении Leave – сообщения (IGMP – v2).

Group Limited – опция включает ограничение числа multicast – групп, к которым может одновременно присоединяться порт.

Max Group Num – максимальное количество multicast – групп, к которым разрешено присоединяться данному порту одновременно. После регистрации порта в указанном количестве multicast – групп, все последующие IGMP Join сообщения будут отбрасываться.

IGMP Querier Mode – позволяет коммутатору определять порт, ведущий к IGMP серверу. Через этот порт будут пересылаться сообщения пользователей IGMP Join и Leave для подключения и отсоединения от multicast – рассылок:

• **Auto** – порт будет считаться подключенным к IGMP – серверу, если на него будет получено IGMP Query сообщение. На данный порт будут пересылаться пользовательские IGMP Join и Leave сообщения.

• **Fixed** – назначается порту, к которому подключен IGMP сервер. Данный порт всегда будет использоваться для пересылки пользовательских сообщений IGMP Join и Leave.

• **Edge** – порт, к которому не может быть подключен IGMP – сервер (например, пользовательский порт). Данный порт не будет доступен для пересылки пользовательских сообщений IGMP Join и Leave, а также коммутатор не будет хранить информацию, полученную от IGMP – сервера, подключенного к данному порту.

Команды CLI

igmp – filtering <cr>
igmp – filtering profile <name> start – address <ip> end – address <ip>
interface port – channel <port – list> igmp – immediate – leave
interface port – channel <port – list> igmp – filtering profile <name>
interface port – channel <port – list> igmp – group – limited <cr>
interface port – channel <port – list> igmp – group – limited number <number>
interface port – channel <port – list> igmp – querier – mode <auto|fixed|edge>

Настройки IGMP Filtering могут иметь дополнительные возможности:

Querier — функция, которая позволяет коммутатору рассылать General IGMP – query пакеты (IGMP Snooping Querier Proxy).

Immed. Leave – функция, которая позволяет исключать порт из дерева multicast – рассылки, если на порт приходит Leave – пакет (IGMP – v2).

Normal Leave, Fast Leave — это значение определяет в миллисекундах (от 200 до 6,348,800), сколько коммутатор будет ждать IGMP – report пакет, не удаляя порт из дерева multicast – рассылки, если на этот порт был получен IGMP – leave пакет.

В режиме **Normal Leave** коммутатор перенаправляет сначала IGMP – leave в uplink порт, IGMP – сервер, получив пакет leave, отправляет в ответ Group Specific IGMP – query, для того чтобы, можно было определить наличие в группе хостов желающих получать рассылку.
В режиме **Fast Leave** после получения коммутатором на порт пакета leave, он отправляет Group Specific IGMP – query членам группы сразу и перенаправляет leave в uplink порт коммутатора.
Group Limited – опция включает ограничение числа multicast – групп, к которым может присоединяться порт.
Max Group Num – максимальное количество multicast – групп, к которым разрешено присоединяться данному порту.
Throttling — если число multicast – групп достигает предела ограничения на порту (Group Limited), то возможны следующие действия:
• **Deny** — пакет IGMP – repport на добавление к новой группе multicast – рассылки будут удаляться (по умолчанию).
• **Replace** — пакет IGMP – repport не будет удален. Порт будет добавлен в дерево новой multicast – рассылки за счет исключения порта из одной, уже действующей на этот момент, рассылки.

Multicast + VLAN

Одновременное использование multicast рассылки и VLAN в некоторых случаях может привести к нежелательному дублированию трафика.
Например:

1. Два пользователя хотят подписаться на одну и ту же рассылку, но пользователи находятся в разных VLAN (VLAN 10 и VLAN 20), для этого они отправляют IGMP – report пакеты.
2. Коммутатор доступа перенаправит на IGMP – Server два IGMP – report пакета, один пакет в VLAN 10 и один пакет в VLAN 20.
3. IGMP – Server добавит в свою таблицу 2 записи, и, следовательно, в Порт 1 отправит multicast поток дважды: в VLAN 10 и в VLAN 20. Таким образом, все преимущества multicast потерялись, так как происходит дублирование трафика.

MVR (Multicast VLAN Registration)

MVR (Multicast VLAN Registration) — функция, которая позволяет передавать multicast трафик в одном VLAN.
Рассмотрим пример:

1. Два пользователя хотят подписаться на одну и ту же рассылку, для этого они отправляют IGMP – report пакеты, однако эти пользователи находятся в разных VLAN (VLAN 10 и VLAN 20).
2. Коммутатор доступа с включенной функцией MVR распознает, что это IGMP пакеты, и помещает их в специальный VLAN (например, VLAN 200) и отправляет IGMP – трафик на IGMP – server через этот VLAN.

3. IGMP – Server получает весь IGMP – трафик в одном VLAN, следовательно, и multicast рассылку он будет отправлять тоже в одном VLAN.

При настройке функции MVR необходимо выбрать роль для каждого порта. Возможно использование одной из трех ролей:

1. **Source Port** — это порт – источник, то есть узел, находящийся за этим портом, может как получать, так и отправлять multicast трафик, то есть это порт, ведущий к IGMP – серверу.
2. **Receiver Port** — это порт – получатель, то есть узел, находящийся за этим портом может только получать multicast трафик, но не может отправлять, то есть это порт, ведущий к клиенту.
3. **None** — порт, на котором многоадресная рассылка MVR не будет ни приниматься, ни отправляться.

Наличие флага в столбце Tagging означает, что многоадресная рассылка, уходящая с этого порта, будет отправляться тегированной.

Режимы работы MVR следующие:

1. **Dynamic** – коммутатор пересылает сообщения IGMP Join и Leave от абонентов в Source порты, в настроенной multicast VLAN. Работа в данном режиме позволяет другим IGMP – устройствам в сети (коммутаторам и источникам вещания) автоматически обновлять их таблицы пересылки multicast трафика, и регулировать пересылку multicast – трафика в их Receiver – порты (включать и отключать при необходимости).
2. **Compatible** – коммутатор не пересылает пользовательские IGMP сообщения в Source порт. Работа в данном режиме требует установки параметров пересылки multicast – трафика на всех других IGMP – устройствах в сети – вручную.

Команды в CLI:

mvr <vlan – id>
mvr <vlan – id> source – port <port – list>
mvr <vlan – id> receiver – port <port – list>
mvr <vlan – id> inactive
mvr <vlan – id> mode <dynamic|compatible>
mvr <vlan – id> name <name – str>
mvr <vlan – id> tagged <port – list>
mvr <vlan – id> 8021p – priority <0 – 7>
mvr <vlan – id> no source – port <port – list>
mvr <vlan – id> no receiver – port <port – list>
mvr <vlan – id> no tagged <port – list>
mvr <vlan – id> no inactive
mvr <vlan – id> no group <cr>
mvr <vlan – id> no group

Multicast IPv6

Multicast Listener Discovery, MLDP – один из протоколов стека протоколов IPv6. MLDP используется для определения получателей multicast – рассылок. В стеке протоколов IPv4 вместо него служил протокол IGMP.
Существует три типа MLD сообщений.

1) Multicast Listener Query, называемый также Query, двух типов:
   – General Query отправляется каждые 125 мс, чтобы узнать какие multicast – адреса имеют подписчики.
   – Multicast – Address – Specific Query для выяснения имеются ли подписчики у конкретной multicast – группы.
2) Multicast Listener Report – аналогично сообщению join в IGMP для IPv4.
3) Multicast Listener Done – аналогично сообщению leave в IGMP для IPv4

MLD Snooping

MLD Snooping — это функция, позволяющая коммутаторами второго уровня перенаправлять multicast траффик на порты, с которых пришли запросы.
При использовании MLD Snooping уменьшается количество управляющих сообщений.

MLD Snooping – proxy

Функция позволяет рассылать трафик получателям и НЕ рассылать не получателям.

Контрольные вопросы по главе 2

1. Назначение и фунции VLAN?
2. Типы VLAN?
3. Назначение и фунции 802.1Q?
4. Процесс 802.1Q?
5. Назначение Входного правила (Port VLAN ID – PVID)?
6. Назначение фунции Subnet – based VLAN?
7. Назначение фунции DHCP VLAN?
8. Назначение статических VLAN?
9. Назначение и фунции протокола GVRP?
10. Назначение и фунции Guest VLAN?
11. Назначение фунции Private VLAN?
12. Назначение фунции Smart Isolation?
13. Назначение и фунции QinQ – технологии?
14. Назначение и фунции VLAN Mapping?
15. Назначение фунции Port Security?
16. Назначение и фунции Link Aggregation?
17. Назначение фунции Port Mirroring?
18. Назначение и фунции Групповой рассылки?

Глава 3. Функции 2+ уровня

Функция Broadcast Storm Control

Если в сети, по какой – либо причине возникает широковещательный шторм, то данные не будут проходить через коммутатор из–за переполнения буферов ненужными пакетами.
Функция Broadcast Storm Control позволяет ограничить количество широковещательных (broadcast), многоадресных (multicast) пакетов, а также пакетов DLF (destination lookup failure).
Пакеты DLF генерируются коммутатором, когда происходит обращение по MAC – адресу, присутствующему в таблице фильтрации MAC, при отключенном порту назначения. Ограничение устанавливается на каждый порт отдельно на количество принятых пакетов в секунду.
Если пакеты указанного типа превышают ограничение, они отбрасываются.
Команды CLI:
storm – control <cr>
interface port – channel <port – list> broadcast – limit <cr>
interface port – channel <port – list> broadcast – limit <pkt/s>
interface port – channel <port – list> multicast – limit <cr>
interface port – channel <port – list> multicast – limit <pkt/s>
interface port – channel <port – list> dlf – limit <cr>
interface port – channel <port – list> dlf – limit <pkt/s>

Функция Loop Guard

Loop Guard – функция, которая позволяет предотвращать распространение широковещательных штормов.
Алгоритм работы функции следующий:

1. Коммутатор B, на котором включена функция Loop Guard на порту 2, с некоторой периодичностью отправляет в этот порт специальный probe – пакет, имеющий multicast – адрес назначения.
2. В случае, если на коммутаторе A нет шторма, полученный probe – пакет будет отправлен на все порты, за исключением порта, на который пакет был получен.
3. Если коммутатор A находится в состоянии шторма, пакет будет отправлен в т.ч., и на порт, с которого он был получен.

Таким образом, если коммутатор B получил probe – пакет, им же отправленный, значит коммутатор A находится в состоянии шторма и порт 2 выключается, атакже отправляется trap – пакет SNMP и добавляется запись в журнал событий.
После устранения причины шторма порт необходимо будет включить вручную, автоматически этого не произойдет.
Для автоматического включения порта, используется функция Error Disable,

рассматриваемая далее.

Защита от петель: Loop Guard & Spanning Tree

Схема работы защиты от петель показана на рис. 24.

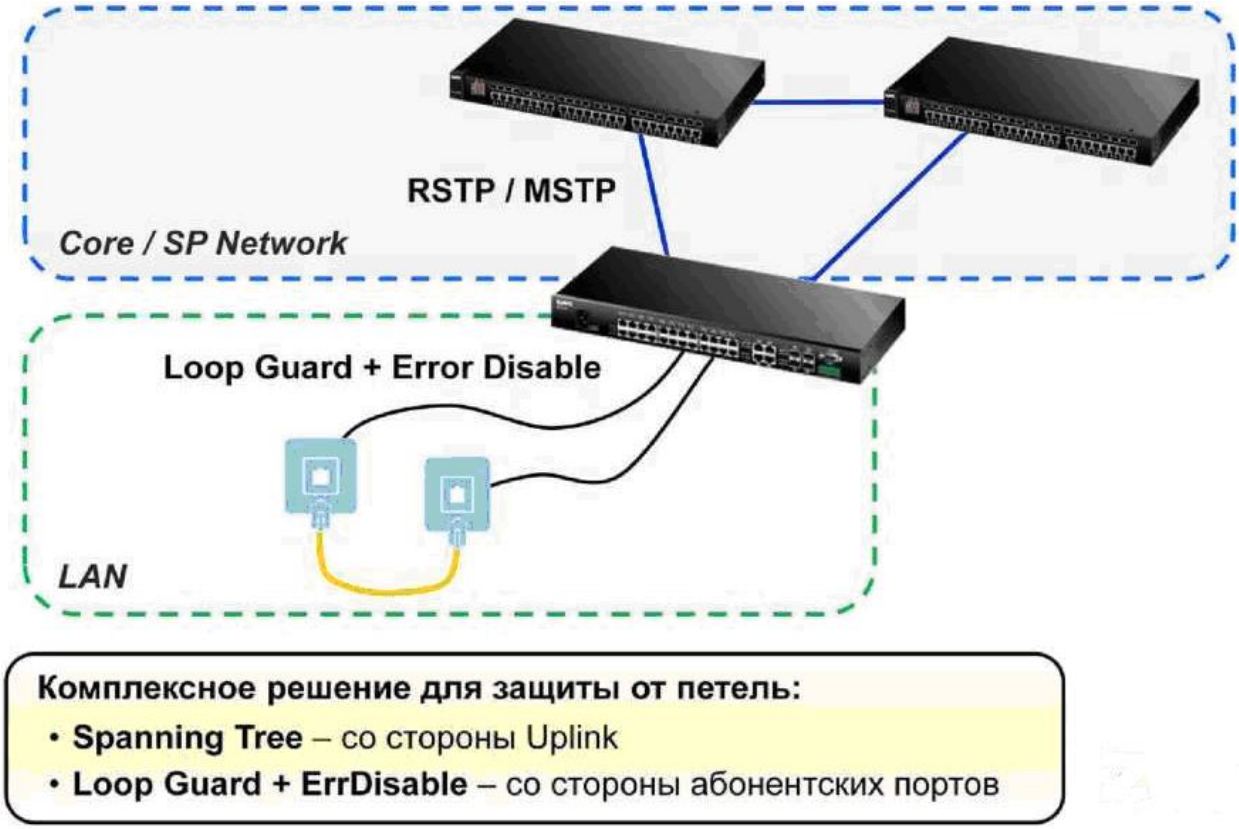

Рис. 24. Схема работы функции защиты от петель

Функция CPU Protection

Излишне большое число специальных пакетов, таких как ARP, BPDU, IGMP, которые проходят через коммутатор, оказывают большую нагрузку на центральный процессор.
Это могут быть как пакеты сети, так и искусственно создаваемые пакеты для осуществления DoS атаки. Это может вызвать перегрузку.
Для недопущения перегрузки процессора, функция CPU Protection позволяет ограничить входную скорость данных пакетов на порты коммутатора.
При превышении входной скорости порт можно отключить или отбрасывать пакеты, превысившие входную скорость.
Скорость входящих пакетов варьируется от 0 до 256

Функция Error disable

Причины срабатывания Error disable (рис. 25) – являются Loop Guard и CPU Protection

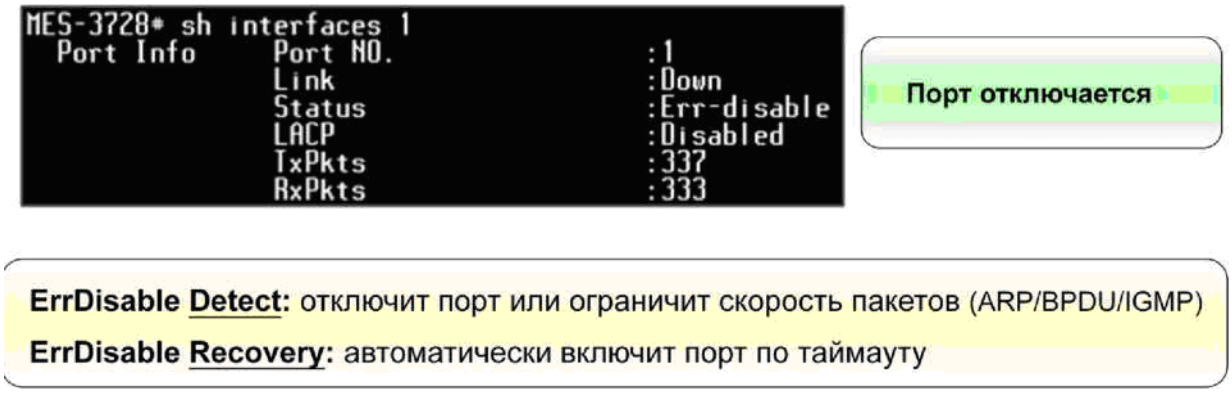

Рис. 25. Работа функции Error disable

Такие функции, как Loop Guard и CPU Protection могут отключить порт коммутатора или отбросить отдельные виды пакетов, если обнаружат аномалию. Например, петлю или превышение скорости BPDU пакетов.

Функция Error Disable and Recovery

В случае превышения пороговой скорости для принимаемых пакетов ARP, BPDU, IGMP возможно одно из трёх действий для функции Error Disable Detect:

1. **Inactive – port** – коммутатор отключает порт, на который поступали пакеты, которые поступили на его порт с превышением допустимой скорости;
2. **Inactive – reason** – коммутатор не обрабатывает центральным процессором ARP и IGMP пакеты, а также отбрасывает BPDU пакеты, которые поступили на его порт с превышением допустимой скорости;
3. **Rate – limitation** – коммутатор отбрасывает излишние пакеты ARP, IGMP, BPDU, поддерживая скорость входящих пакетов такой, чтобы обрабатывать их без излишней нагрузки на центральный процессор.

Если порт был отключен функцией ErrDisable Detect, не придется включать его вручную: функция Error Disable Recovery позволяет включить порт автоматически через определенный тайм – аут.

Для этого задаются тайм – ауты (Interval) в секундах для каждой из четырех возможных причин, по которой порт был отключен (Loop Guard, или превышение скорости пакетов ARP, BPDU, IGMP).

Если после автоматического включения порта, ErrDisable Detect снова обнаружит аномалию – порт снова отключится на указанный интервал времени, и так далее, пока проблема на подключенном оборудовании не будет устранена

QoS (Quality of service)

Качество обслуживания – это способность сетевых средств и устройств обеспечить требуемый сервис для некоторых классов трафика.

В коммутаторах качество обслуживания обеспечивается за счет изменения

порядка следования пакетов при передаче их из порта.

Предпочтение отдается пакетам с большим приоритетом, а приоритет определяется весом очереди, в которую пакет попадет.

Вес очереди – число, закрепленное за каждой из восьми очередей на каждом порту коммутатора. Веса очередей обрабатываются в соответствии с выбранным алгоритмом: SPQ, WRR или WFQ.

Выбор очереди зависит от значения поля 802.1p в заголовке VLAN. Отображение 802.1p на номер очереди, как и веса очередей, указывается в настройках коммутатора.

Классификаторы, политики и другие дополнительные средства управления позволяют в случае необходимости установить требуемое значение в поле 802.1p, чтобы пакет при выходе из порта попал в заданную очередь и получил должный приоритет.

Ethernet – коммутаторы, поддерживающие работу с классификаторами и правилами политики, имеют ограничения в 128 записей при создании классификаторов (Classifier) и правил политики (Policy Rule):

Классификатор

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

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

На третьем уровне коммутатор проверяет поля заголовка IP – пакета: поле DSCP, идентификатор протокола четвертого уровня (IP Protocol), IP – адреса источника и назначения, причем можно указать диапазон адресов с помощью маски, например, 192.168.1.0/24.

Кроме того, в случае протоколов TCP и UDP коммутатор может проверять порты источника и назначения (Socket Number), а также бит SYN протокола TCP (флаг Establish only).

Команды CLI:

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

Политики

Для настройки политики нужно выбрать классификатор из списка и затем указать действия Actions, применяемые к выбранному классификатору.

Если действие имеет параметр, то этот параметр должен быть установлен в соответствующем поле раздела Parameters.

В качестве действий (Actions) над выбранным типом трафика можно:

- разрешать/запрещать пересылку пакетов
- изменять приоритеты 802.1p и DSCP исходящих пакетов
- зеркалировать определенный тип трафика (указав порт коммутатора для отправки зеркалированного трафика)
- пересылать трафик на определенный порт коммутатора (явно указав выходной порт)
- изменять VLAN ID у исходящих кадров
- ограничивать пропускную способность отдельных типов трафика

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

- фильтрация по MAC – и IP – адресам;
- привязка MAC – и IP – адреса к определенному порту;
- фильтрация протоколов по идентификатору в заголовке пакета;
- фильтрация служб по номеру сокета (порта TCP/UDP);
- гибкое управление качеством обслуживания на базе 802.1p, TOS и DSCP;
- зеркалирование и перенаправление определенных типов пакетов на конкретный порт;
- изменение идентификатора VLAN,

Набор доступных действий в Политиках, на младших моделях коммутаторов будет немного сокращен.

Команды в CLI:

policy <name> policy help

Выходной порт. Обработка приоритетов 802.1 p

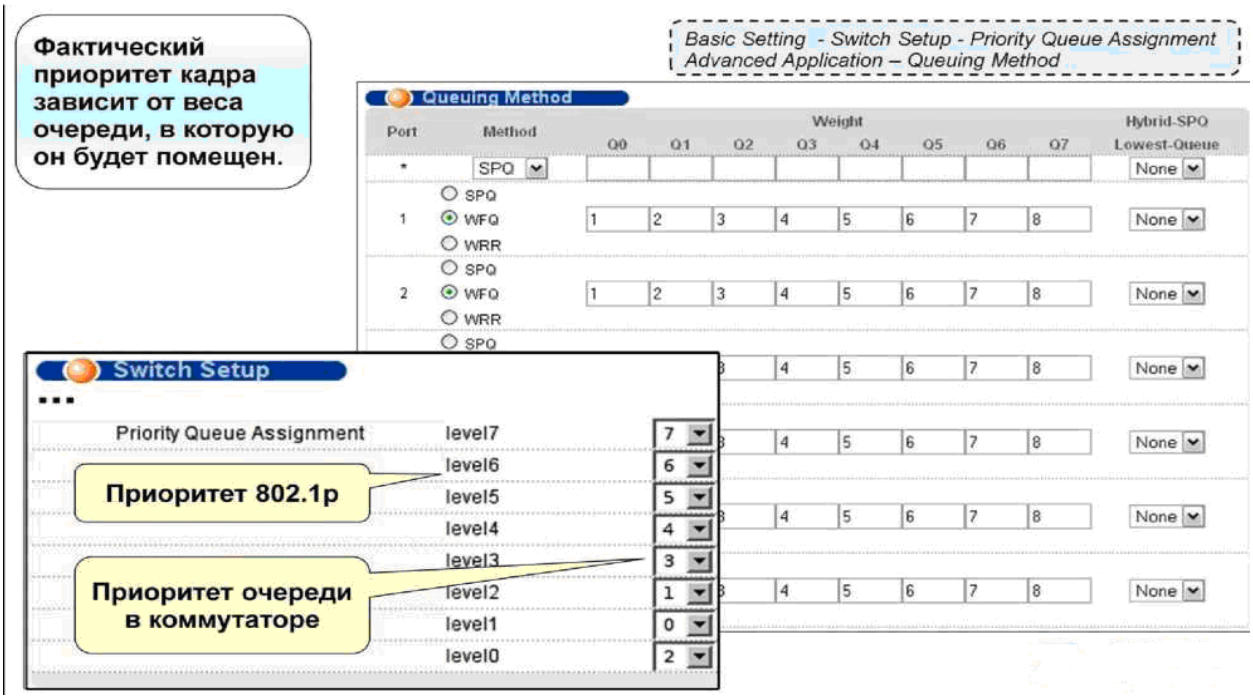

Рис. 26. Обработка приоритетов 802.1 p

Обработка приоритетов 802.1 p на выходном порту показана на рис. 26.

Стандарт IEEE 802.1p различает 8 отдельных типов трафика, путем

добавления в Ethernet – кадр метки, указывающего на класс обслуживания.
В коммутаторе имеется восемь (реже четыре) физических очередей выходного порта.
Выходные очереди порта ставятся в соответствие с приоритетами 802.1p. Трафик, попадающий в очередь с большим номером, проходит через коммутатор быстрее.
Трафик в очередях с меньшим номером может быть отброшен при перегрузке сети.
Другими словами, перед тем как кадр будет отправлен в канал, он помещается в одну из восьми выходных очередей порта.
Выбор очереди основывается на поле приоритета 802.1p, имеющем длину 3 бита (т.е. приоритет принимает значения от 0 до 7).
Фактический приоритет кадра зависит от веса очереди, в которую он будет помещен.
Правило размещения кадра в той или иной очереди в зависимости от поля 802.1p настраивается в меню Basic Settings > Switch Setup > Priority Queue Assignment.
Также выбирается механизм (алгоритм, Method) обработки очередей на каждом порту коммутатора.

Команды CLI:

interface port – channel <port – list> spq
interface port – channel <port – list> wrr
interface port – channel <port – list> wfq
interface port – channel <port – list> wrr <wt1> <wt2> ... <wt8>
interface port – channel <port – list> weight <wt1> <wt2> ... <wt8>

Алгоритмы обработки очередей

Три алгоритма обработки приоритетов показаны на рисунке 27.

SPQ (Strict Priority Queueing)

Алгоритм SPQ состоит в следующем. Пока кадры не будут полностью выбраны из очереди с высшим приоритетом, очереди с низшим приоритетом простаивают.
Если очереди высших приоритетов никогда не опустошаются, то велика вероятность того, что из наименее приоритетных очередей кадры не будут оправлены.

WRR (Weighted Round Robin)

Алгоритм WRR состоит в следующем. Каждой очереди присваивается определенный вес (рис. 27) в диапазоне от 1 до 15.
Время работы поделено на равные циклы, и в течение каждого цикла количество выбранных кадров соответствует весу очереди.

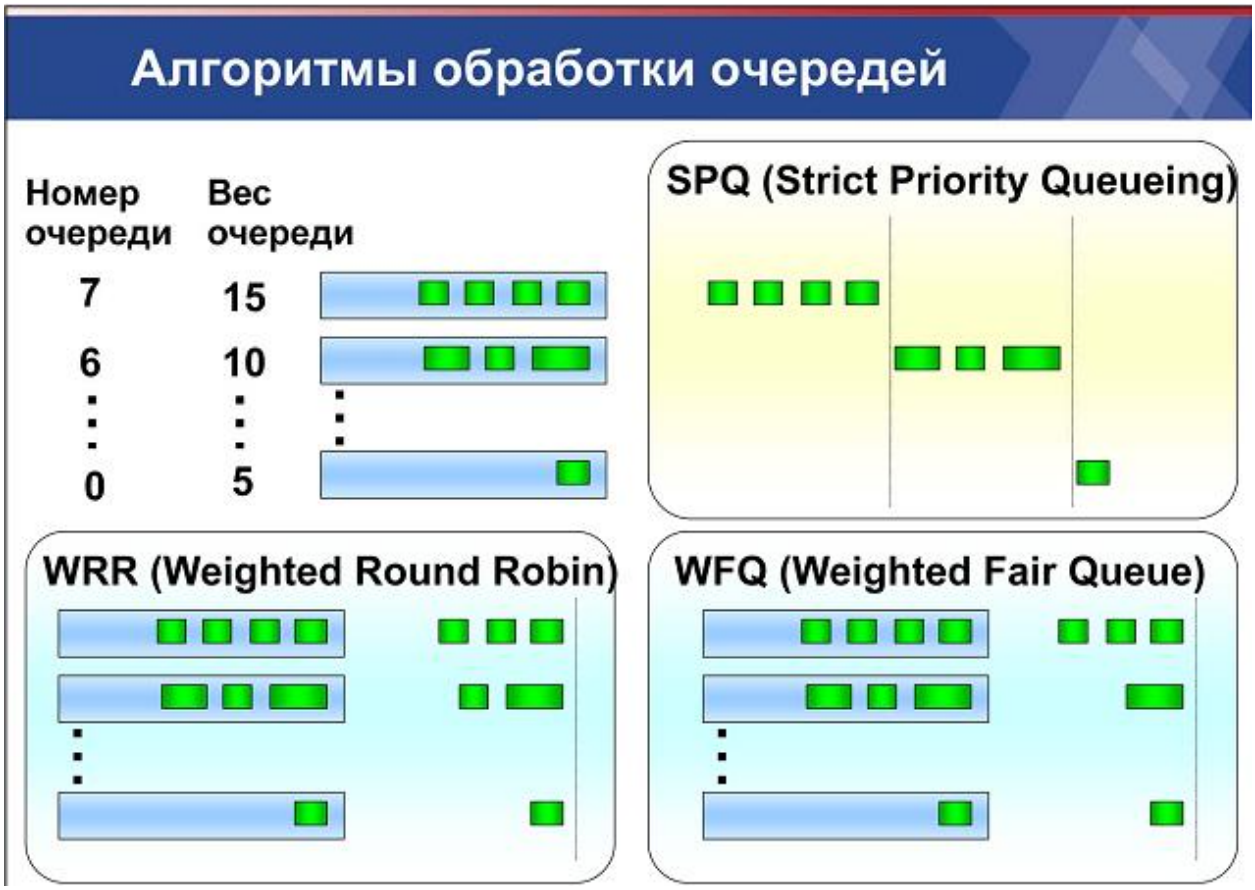

Рис. 27. Алгоритмы обработки очередей

WFQ (Weighted Fair Queue)

Алгоритм WFQ учитывает длины кадров и делит пропускную способность между потоками данных из различных очередей пропорционально весам очередей. Для каждой очереди выделяется гарантированная пропускная способность, которая определяется следующим выражением:
(вес текущей очереди)/(сумма весов всех очередей)* (скорость порта)
Таким образом, алгоритм WRR учитывает количество кадров, а алгоритм WFQ – реально передаваемый объем данных.
Обращаем внимание, что наличие реализации алгоритма WFQ зависит от модели коммутатора (на некоторых коммутаторах этот алгоритм не реализован), также на некоторых коммутаторах алгоритм обработки очередей настраивается не на каждом порту вотдельности, то есть на всех портах в один момент времени может работать только один из алгоритмов.
На старших моделях коммутаторов также можно установить гибридный метод обработки очередей на каждом порту (Hybrid – SPQ): выделив приоритетные очереди для обработки методом SPQ, а остальные по алгоритму WRR или WFQ.
Например, указав в качестве Lowest – Queue очередь Q5, коммутатор будет обрабатывать очереди Q5, Q6, Q7 алгоритмом SPQ, а остальные очереди (Q0 – Q4) с помощью выбранного метода: WRR или WFQ.

Контрольные вопросы по главе 3

1. Назначение фунции Broadcast Storm Control?
2. Назначение фунции Loop Guard?
3. Назначение фунции CPU Protection?
4. Назначение фунции Error disable?
5. Назначение фунции Error Disable Recovery?
6. Назначение фунции Классификатора?
7. Назначение фунции Политики?
8. Назначение алгоритма SPQ?
9. Назначение алгоритма WRR?
10. Назначение алгоритма WFQ?

Глава 4. Функции 2+ уровня. Дополнительные возможности

С помощью классификаторов и политик в коммутаторах возможно не только реализация QoS для пользовательского трафика, но и создание всевозможных списков ACL (Access Control List) и управления пропускной способностью.

Например, необходимо реализовать политику ограничения пропускной способности следущим образом.

Для ограничения пропускной способности надо установить переключатель Metering и ввести значение пропускной способности Bandwidth. Трафик, поступающий со скоростью свыше Bandwidth, считается внепрофильным (Out – of – Profile).

Далее необходимо выбрать действие для внепрофильного трафика (поступающего со скоростью свыше установленной), Out – of – ProfileAction.

Для потока пакетов, превышающего заданный уровень Bandwidth, выполняются действия Out – of – profile (Наример, при перегрузке выходного канала):

1. отбросить пакет.
2. изменить поле DSCP.
3. отбросить в случае перегрузки выходного канала.
4. отменить решение об удалении, принятое в предыдущей политике.
5. изменить приоритет DSCP (Change the DSCP value).
6. отбрасывать трафик только в случае перегрузки сети (Set Out – Drop Precedence).
7. не отбрасывать кадр, ранее помеченный на отбрасывание (Do not drop the matching frame previously marked for droppin).

Пример перегрузки выходного канала.

Гибкий механизм управления перегрузками позволяет ограничивать пропускную способность, используемую каким – либо типом трафика, при этом ограничение вступает в силу лишь в случае необходимости.

Рассмотрим следующую схему:

Коммутатор получает трафик FTP от PC A и трафик HTTP от PC B.

На коммутаторе с помощью классификаторов и политик установлено ограничение пропускной способности для HTTP трафика 512 Kbps, а также указано, что трафик отбрасывать только в случае перегрузки выходного канала.

Пусть трафик HTTP превышает 512 Kpbs, однако пропускной способности второго порта хватает для отправки и FTP трафика и HTTP

В этом случае пропускная способность под HTTP уменьшаться не будет.

Если же трафик HTTP превышает 512 Kbps и пропускной способности *uplink* порта не хватает, то только в этом случае часть трафика будет отбрасываться.

Правила Access Control List (ACL). Приоритет обработки

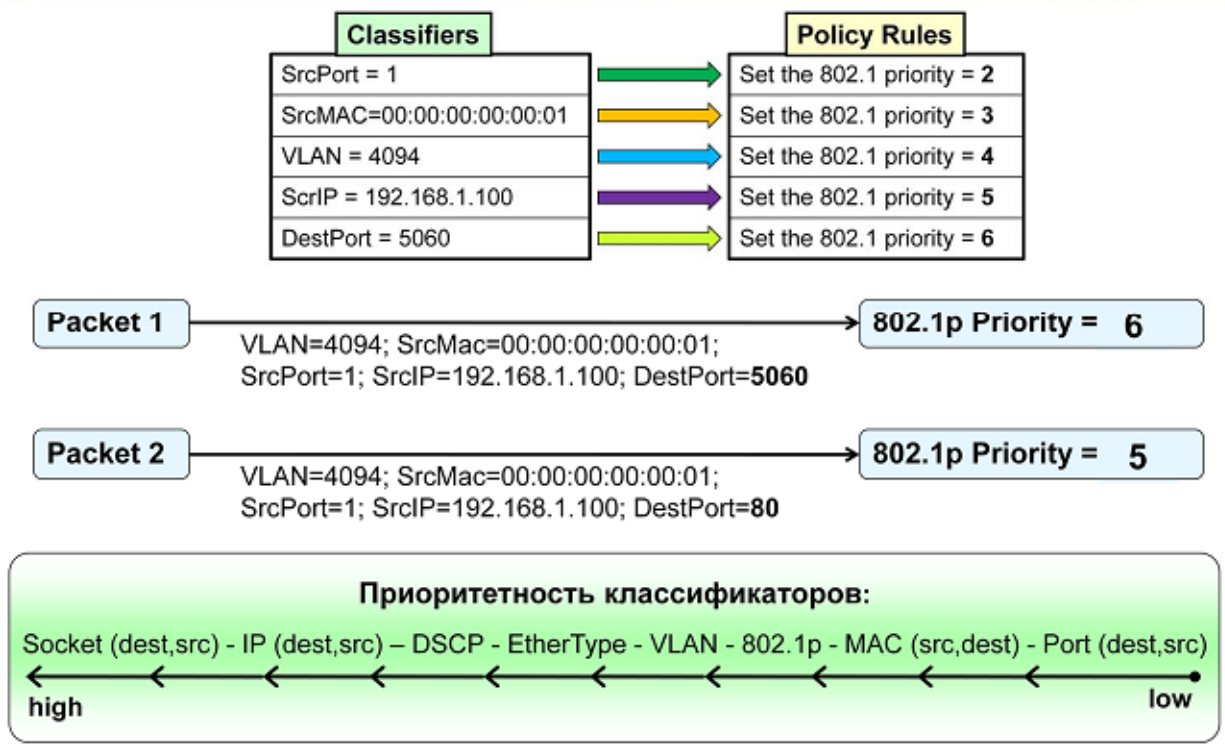

Рис. 28. Использование ACL

Если при использовании ACL (рис. 28) было создано несколько правил обработки трафика (на одном или на разных уровнях модели OSI), то нужно учитывать порядок их обработки в коммутаторе.

Порядок обработки классификаторов.

Главным критерием работы Политики – является Классификатор. Определенный тип трафика, выделенный с помощью классификатора, далее обрабатывается политикой.

Если трафик попадает под действие нескольких политик, то применяется только одна политика:

1. Если в коммутаторе создано несколько классификаторов, которые затем используются в разных политиках, причем классифицирование трафика происходит на одном уровне модели OSI, и трафик попадает под действие нескольких классификаторов, к такому трафику будет применена только одна политика. Выбор политики основан на имени использующегося в нем классификатора, сортировка имен классификаторов происходит по названию правил (name), чем старше первый (первые) символ(ы) – тем приоритетнее классификатор (например: классификатор с именем «zzz» более приоритетен, чем «aaa»).
2. Если в коммутаторе создано несколько классификаторов, которые затем используются в разных политиках, причем классифицирование трафика происходит на разных уровнях модели OSI, и трафик попадает под действие нескольких классификаторов, к такому трафику будет

применена только одна политика. Выбор политики основан на приоритете критерия в классификаторе.

Последовательность параметров классификатора от низшего приоритета к высшему приоритету:

Source – port > Destination – port > Packet – format > Destination – MAC > Source – MAC > Priority – VLAN ID > Ethernet – type > DSCP > IP – Protocol > Source – IP > Destination – IP > Source – Socket > Destination – Socket > Establish Only.

Т.е. если трафик одновременно попадет под действие двух и более классификаторов, которые далее используются в разных политиках, то отработает та политика, чей классификатор приоритетнее (например, если классификаторы были основаны на VLAN ID и Source IP пакета, то отработает политика с классификатором Source IP).

Блокировка Telnet – трафика

Рассмотрим пример: как запретить прохождение telnet – трафика через коммутатор, во всех VLAN и на всех портах, создав правило ACL.

С помощью классификатора (Classifier) выделить из всего потока пакетов telnet – трафик по номеру TCP порта службы telnet: 23.

Далее, с помощью правил политики (Policy Rule), создать новое правило. Выбрать классифицированный трафик – telnet, и действие (Action), выполняемое коммутатором над соответствующим классифицированным потоком трафика: Forwarding – Discard the packet – для отбрасывания пакетов.

Задача заблокировать доступ в Интернет.

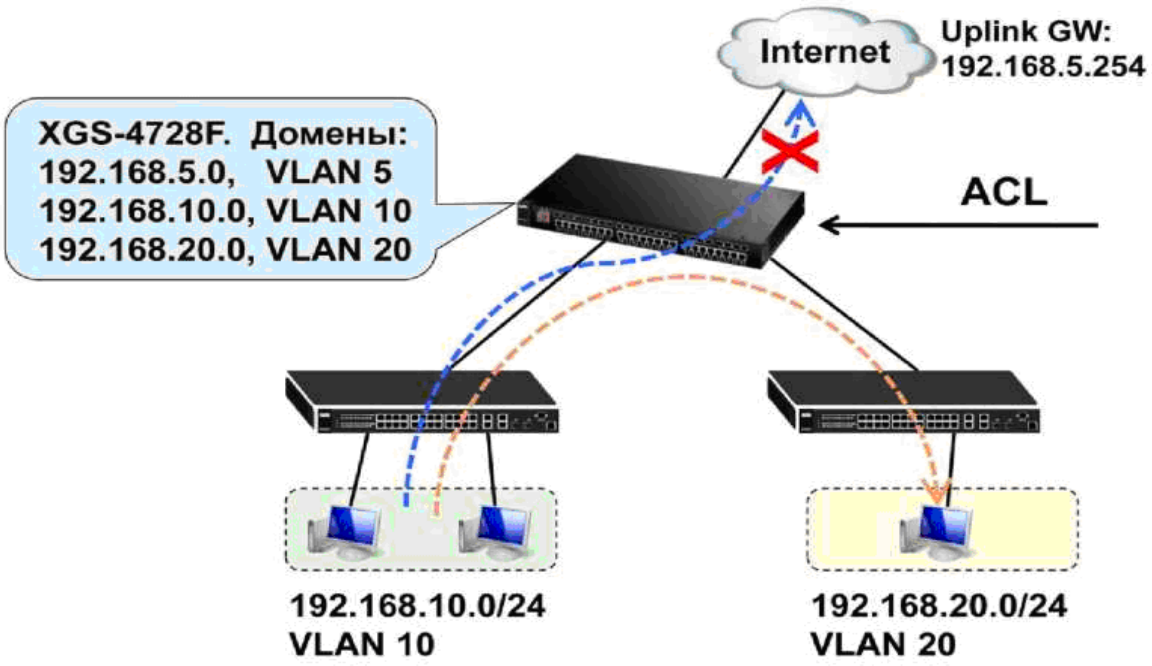

Рис. 29. Запрет доступ в Интернет некоторым пользователям

Рассмотрим следующую схему (рис. 29).
Требуется пользователям подсети 192.168.10.0 – запретить доступ в Интернет, но разрешить доступ к другой подсети 192.168.20.0 – создав соответствующее правило ACL в коммутаторе.
Для этого, на коммутаторе 3го уровня (на котором созданы IP – домены, и который подключен к Интернет) создают правила контроля доступа ACL.
На коммутаторе 3го уровня с помощью Классификатора выделяют весь исходящий трафик из подсети 192.168.10.0
Затем выделяют трафик из подсети 192.168.10.0 в подсеть 192.168.20.0
Далее, создают правило политики для блокирования всего трафика из подсети 192.168.10.0. указав действие Discard the packet для отбрасывания пакетов.
А затем создают еще одно правило политики, для разрешения трафика из подсети в подсеть 192.168.20.0: в разделе Forwarding установив значение Do not drop the matching frame previously marked for dropping для сохранения кадров, ранее помеченных на отбрасывание

Зеркалирование портов Port Mirroring

Для дублирования трафика на порт мониторинга можно использовать функцию Port Mirroring (зеркалирование портов).
К порту мониторинга коммутатора подключается ПК со специальной программой – сниффером для захвата и анализа сетевого трафика.
Однако, функция Port Mirroring зеркалирует сразу весь поток трафика на определенный порт коммутатора, что может повлечь замедление работы или даже зависание компьютера, на котором происходит захват пакетов в том случае, если через коммутатор передается большой объем трафика.
С помощью классификаторов и политик также можно производить зеркалирование трафика, однако более гибко, чем в функции Port Mirroring, отправляя на порт для мониторинга только пакеты определенного типа.
Например, настройки классификаторов и политик для мониторинга сигнального SIP – трафика.
Такая необходимость может возникнуть, например, при отладке или поиска причины возможных проблем при использовании технологии VoIP
Сначала с помощью классификаторов выделяют исходящие и входящие потоки SIP – трафика с Uplink – порта (например, порта 28) по UDP – порту 5060, который использует данный протокол.
Для этого необходимо создать два правила классификатора т.к. SIP сообщения отправляют как клиент, так и сервер.
С точки зрения коммутатора, сообщения от клиентов к серверу будут с Destination port=5060, а сообщения от сервера клиентам будут с Source port=5060.
Далее создается правило политики, в котором выбираются оба правила классификатора, выбирается действие – переслать кадры на мониторинг – порт (Send the packet to the mirror port).
Далее коммутатору необходимо назначить мониторинг – порт (mirror – port).

Это делается в разделе Advanced Applications > Mirroring: включают функцию port mirroring, и указыват monitor port (куда будет подключен анализатор пакетов), например порт 24.

Функция Bandwidth Control

Функция Bandwidth Control позволяет по каждому порту задать ограничение входящего и исходящего потока данных.
Для входящего потока (Ingress Rate) указывается два параметра: Commit Rate и Peak Rate.
Пакеты, превышающие порог Peak Rate, отбрасываются.
В выходной порт может поступать сразу несколько потоков данных из разных входных портов, однако пропускная способность порта ограничена – либо физическими возможностями выходного канала, либо принудительно – с помощью параметра Eggress Rate.
Если скорость выходного порта не позволяет обслужить все пакеты, то в первую очередь будут отброшены те, которые при входе в коммутатор превысили порог Commit Rate.
Управление пропускной способностью с помощью Bandwidth Control целесообразно выполнять на абонентских портах.
При этом сумма гарантированных скоростей всем пользователям, подключенным к коммутатору не должна превышать скорости всех Uplink портов коммутатора.
Bandwidth Control позволяет ограничивать как скорость скачивания данных пользователем (ingress rate), так и скорость закачки данных в сеть (egress rate).
Для входящего потока данных (к пользователю) можно указать максимальную, но негарантированную пиковую (Peak Rate) скорость, доступную пользователю при не полностью загруженном порту Uplinks коммутатора.
Команды CLI:
bandwidth – control <cr>
interface port – channel <port – list> bandwidth – limit cir <Kbps>
interface port – channel <port – list> bandwidth – limit cir <cr>
interface port – channel <port – list> bandwidth – limit pir <Kbps>
interface port – channel <port – list> bandwidth – limit pir <cr>
interface port – channel <port – list> bandwidth – limit egress <Kbps>
interface port – channel <port – list> bandwidth – limit egress <cr>

Функция IP Source Guard

Функция IP Source Guard в Ethernet – коммутаторах предназначена для обеспечения дополнительной защиты от несанкционированных действий пользователей.
Функция IP Source Guard включает в себя функции Static Binding, DHCP Snooping и ARP Inspection.
Функция защиты от подмены IP – адресов позволяет отфильтровывать

несанкционированные пакеты DHCP и ARP всети.

Для защиты от подмены IP – адресов применяется таблица привязок (Static Binding), позволяющая различать санкционированные и несанкционированные DHCP – и ARP – пакеты. При привязке используются следующие атрибуты:

1. MAC – адрес.
2. IP – адрес.
3. VLAN ID.
4. Номер порта.
5. Время аренды.

При получении коммутатором пакета DHCP или ARP производится поиск соответствующих MAC – адреса, идентификатора VLAN ID, IP – адреса и номера порта в таблице привязок.

При наличии привязки коммутатор пересылает пакет. Если привязки не найдено, пакет коммутатором отбрасывается.

IP Static Binding

*Binding – привязка

Рис. 30. Настройка статических записей адресов IP и MAC

IP Static Binding позволяет заносить статические записи в IP – MAC Binding Table (рис. 30). В случае Port Based VLAN вполе VID следует указывать 1.

Команды CLI:

ip source binding <mac – addr> vlan <vlan – id> <ip> <cr>

ip source binding <mac – addr> vlan <vlan – id> <ip> interface port – channel <interface – id>

Функция DHCP Snooping

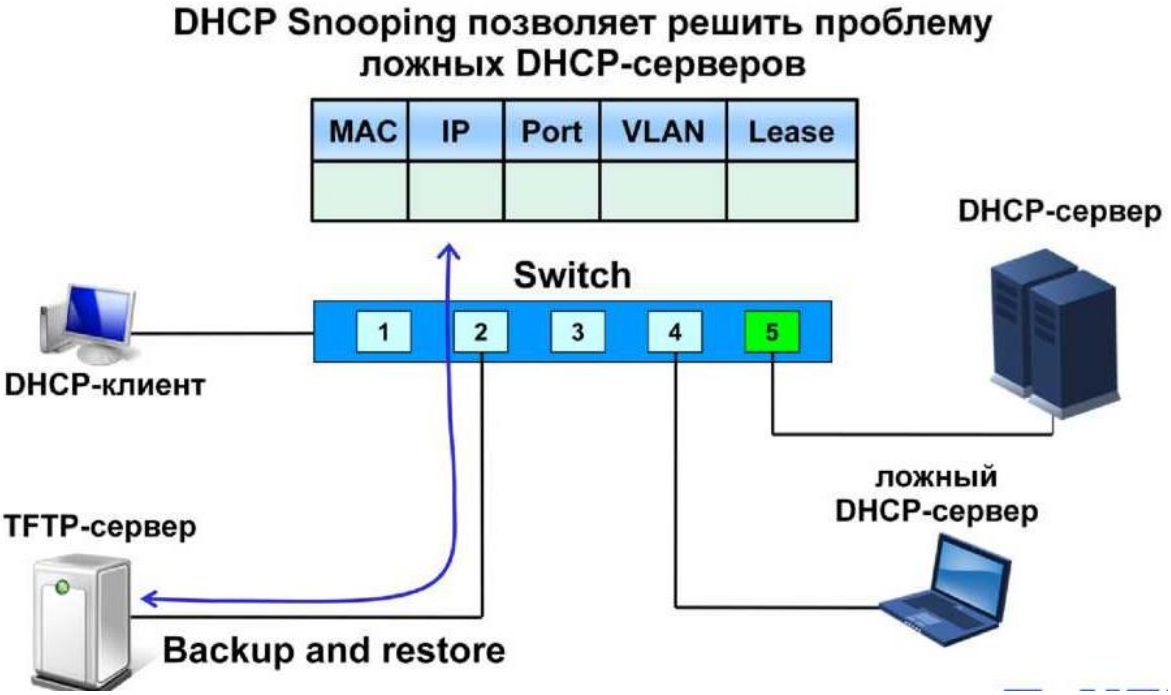

Рис. 31. Схема работы отслеживания DHCP

В любой сети есть вероятность того, что случайно, либо намеренно кто – то запустит на своём компьютере DHCP – сервер и будет наравне с легитимным DHCP – сервером выдавать адреса. Выдавая неправильные адреса, он может организовать атаку «отказ в обслуживании», а, выдавая правильные адреса, может указывать в качестве шлюза по умолчанию адрес своего компьютера и перехватывать сетевой трафик. (Snoopihg – Отслеживание).

При использовании функции DHCP Snooping (рис. 31) можно подключить DHCP – сервер к «**trusted**» порту, который задаётся вручную. В случае, если к данному коммутатору будет подключен ещё один DHCP – сервер, но уже к «**untrusted**» порту, все DHCP сообщения на этом порту будут отброшены, чтобы никто не смог получить IP – адрес от «ложного» DHCP – сервера.

Вторая задача, которую решает функция DHCP Snooping — заполнение динамической части таблицы IP MAC Binding Table адресами, которые DHCP – сервер выдает клиентам.

Также существует возможность резервного копирования и восстановления таблицы динамической части IP – MAC Binding Table про протоколу TFTP, так как при возможной перезагрузке коммутатора она будет стерта, а следовательно большая часть трафика будет отброшена функцией ARP Inspection.

Флаг Active включает функцию DHCP Snooping.

DHCPVlan — позволяет включить функцию DHCP Vlan и выбрать номер DHCP Vlan.

Agent URL — адрес, по которому коммутатор будет сохранять резервную копию динамической части IP MAC Binding Table.

Timeout Interval — время, в течение которого коммутатор будет пытаться произвести резервное копирование данных на узел, указанный в поле Agent URL

Write Delay Interval — интервал времени, через который коммутатор будет выполнять резервное копирование данных на узел, указанный в поле Agent URL

Renew DHCP Snooping URL — функция, которая позволяет принудительно обновить на коммутаторе динамическую часть таблицы IP MAC Binding Table с указанного адреса. При этом текущая динамическая часть таблицы IP MAC Binding Table остается. Если записи в таблице, взятой с указанного узла, противоречат записям в динамической части локальной таблицы IP MAC Binding Table, то приоритет имеют записи локальной таблицы.

Функция DHCP Snooping также позволяет ограничивать количество DHCP пакетов, поступающих на порт в единицу времени.

Поле Rate (pps) показывает максимальное число DHCP пакетов, получаемых на порт в секунду.

Поле Option82 позволяет добавлять в DHCP – запрос дополнительную информацию, такие как: номер слота и номер порта, на которые пришел DHCP – запрос, а так же номер VLAN, в котором пришел DHCP – запрос.

Поле Information позволяет добавлять в DHCP – запрос идентификатор устройства

Команды CLI:

dhcp snooping <cr>
dhcp snooping vlan <vlan – list>
dhcp snooping vlan <vlan – list> option
dhcp snooping vlan <vlan – list> information
dhcp snooping database <tftp://host/filename>
dhcp snooping database timeout <seconds>
dhcp snooping database write – delay <seconds>
interface port – channel <port – list> dhcp snooping trust
interface port – channel <port – list> dhcp snooping limit rate <pps>
show dhcp snooping <cr>
show dhcp snooping binding
show dhcp snooping database <cr>
show dhcp snooping database detail
renew dhcp snooping database <tftp://host/filename>
renew dhcp snooping database <cr>
clear dhcp snooping database statistics

Функция ARP inspection

Одна из наиболее часто используемых уязвимостей протокола ARP под названием ARP Spoofing выглядит следующим образом:

Злоумышленник (PC C) отправляет паре компьютеров с адресами MAC A и

MAC B (трафик между которыми он хочет прослушать) подложные ARP – ответы, в которых говорится, что IP – адреса этих компьютеров соответствуют MAC C.
Таким образом, когда PC Аили PC B будут отправлять IP – пакеты друг другу, они их будут упаковывать вкадры Ethernet с адресом назначения MAC C.
Далее, когда злоумышленник получит пакеты от PC A или PC B, он их перешлет реальным получателям, чтобы те не обнаружили фактов перехвата трафика.
Описанная выше ситуация предотвращается с помощью функции ARP Inspection (рис. 32), которая позволяет отбрасывать все ARP – пакеты, приходящие от недоверенных «**untrusted**» портов И корректные записи о которых не были найдены в таблице IP – MAC Binding Table.
Таким образом, все клиенты, которые имеют неправильные сочетания MAC/IP/Port/VLAN, не будут иметь доступ к сети.

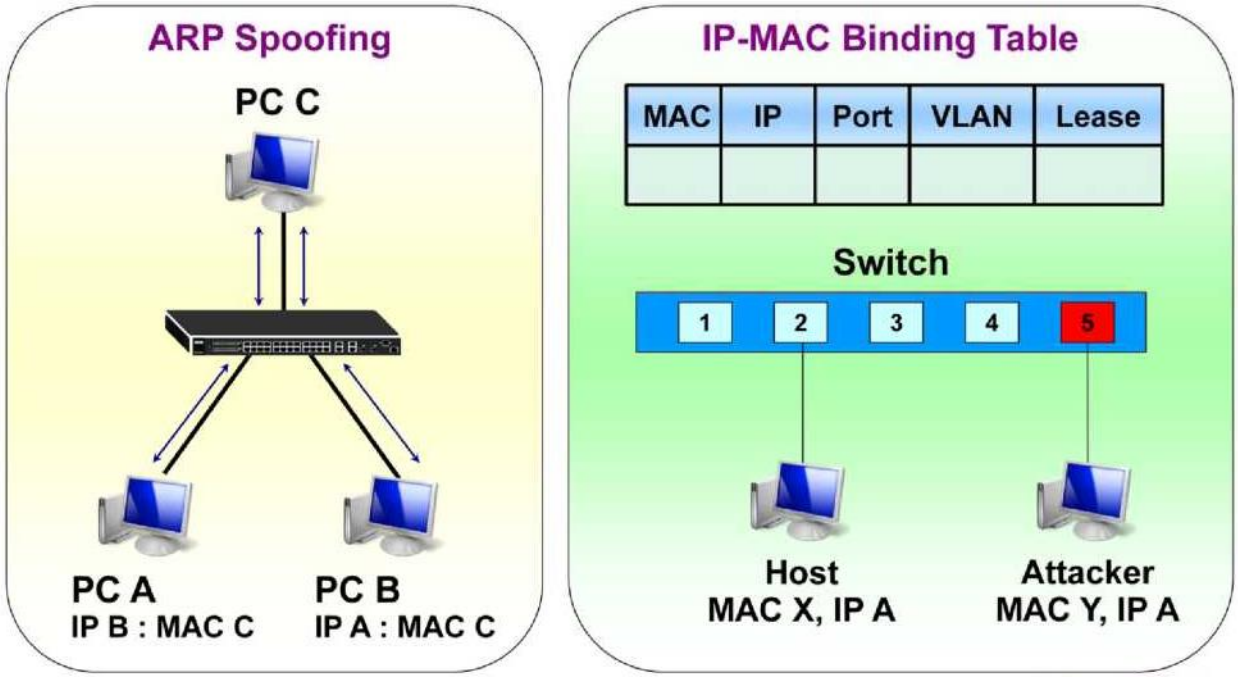

Рис. 32. Схема работы функции ARP и защита

При обнаружении коммутатором несанкционированного ARP – пакета им автоматически создается фильтр MAC – адресов, блокирующих трафик от MAC – адреса и сети VLAN, от которых поступил несанкционированный ARP – пакет. Время блокировки зависит от параметра Filter aging time (для бесконечной блокировки установите 0). Если какой то узел был заблокирован, то будет отображена причина блокировки (Reason), а поле Expiry показывает время в секундах, в течении которых будет действовать фильтр. Запись о блокировке можно удалить вручную (delete).
Вразделе Log profile указываются таймеры отправки syslog сообщений коммутатором, в случае если настроен сервер syslog.
Команды CLI:
arp inspection log – buffer entries <0 – 1024>

arp inspection log – buffer logs <0 – 1024> interval <0 – 86400>
arp inspection filter – aging – time <1 – 2147483647>
arp inspection <cr>
clear arp inspection filter
clear arp inspection log
clear arp inspection statistics <cr>
clear arp inspection statistics vlan <vlan – list>
no arp inspection filter <mac – addr> vlan <vlan – id>
Для функции ARP Inspection портам задаются роли:

1. Trusted port (доверенный) – приходящие ARP пакеты никогда не будут отброшены
2. Untrusted Port (недоверенный, ненадежный) – приходящие ARP пакеты будут отброшены в случае:
    2..1. Информация об отправителе не совпадает ни с одной из существующих привязок
    2..2. Скорость поступления ARP пакетов слишком высока. Можно указать максимальную скорость, с которой будут приниматься ARP – пакеты.

Для ограничения количества ARP запросов, поступающих на порт в единицу времени, задаются параметры:
Rate (pps) — максимальное число ARP пакетов, получаемых на порт в секунду.
Burst interval (seconds) — интервал времени для учета количества поступающих ARP запросов.
Например, если Rate=15 и Burst interval=1, то за интервал в 1 секунду, коммутатор примет максимум 15 ARP пакетов. Если Rate=15 и Burst interval=5, то за интервал, равный 5 секундам, коммутатор примет максимум 75 ARP кадров (т.е. за одну секунду, например, может поступить 71 ARP – пакет, а в остальные 4 секунды – по одному ARP пакету, и все они будут обработаны коммутатором).
Работу ARP Inspection можно настроить на определенном диапазоне VLAN, и указать должен ли коммутатор генерировать сообщения контрольного журнала (log) при получении ARP пакетов от каждой VLAN:

1. Deny – генерирование сообщения при отбрасывании ARP сообщений из данной VLAN;
2. Permit – генерирование сообщения при пересылке пакетов ARP от данной VLAN;
3. All – генерирование сообщения при каждом получении пакетов ARP от данной VLAN;
4. None – коммутатор не записывает информацию о получении сообщений ARP от данной VLAN.

Команды CLI:
interface port – channel <port – list> arp inspection trust
interface port – channel <port – list> arp inspection limit rate <pps> <cr>
interface port – channel <port – list> arp inspection limit rate <pps> burst interval

<seconds>
arp inspection vlan <vlan – list> <cr>
arp inspection vlan <vlan – list> logging [all|none|permit|deny]

Контрольные вопросы по главе 4

1. Назначение фунции ACL?
2. Назначение функции Port Mirroring?
3. Назначение фунции Bandwidth Control?
4. Назначение фунции IP Source Guard?
5. Назначение фунции IP Static Binding?
6. Назначение фунции DHCP Snooping?
7. Назначение фунции ARP inspection?

Глава 5. Функции 3 уровня

Домены маршрутизации

В коммутаторе третьего уровня настраиваются домены маршрутизации – подсети IP, в которых коммутатор выступает шлюзом по умолчанию.
Каждая подсеть привязана к определенной VLAN.
Внутри подсети осуществляется коммутация второго уровня.
Например, в коммутаторах XGS – 4000 – й серии можно настроить не более 128 подсетей.
Кроме того, в коммутаторе имеется специальный порт Management для управления.
Для работы с коммутатором через этот порт нужно установить Management IP Address, не входящий ни в одну из основных IP – подсетей.

Команды CLI:

ip address <ip> <mask> ip/mask of management port
ip address default – gateway <ip> gateway of management port
ip name – server <ip>
default – management <in – band|out – of – band>
vlan <1 – 4094> ip address <ip – address> <mask> <cr>
vlan <1 – 4094> ip address <ip – address> <mask> manageable
vlan <1 – 4094> ip address default – gateway <ip – address>

Функция DHCP Server

На IP – доменах можно включать различные службы, например DHCP Server. Функция DHCP Server позволяет автоматически выдавать IP – адреса клиентам сети. Для настройки необходимо указать:

1. VID – идентификатор VLAN, внутри которого работает DHCP – сервер
2. Client IP Pool Starting Address – начальный IP – адрес пула
3. Size of Client IP Pool – размер пула IP – адресов
4. IP Subnet Mask – маска подсети
5. Default Gateway – шлюз по умолчанию для клиентов DHCP
6. Primary/Secondary DNS Server – адреса первичного и вторичного DNS – сервера

Все коммутаторы L3 также поддерживают функцию DHCP Smart Relay и DHCP Relay per VLAN .

Команды CLI:

dhcp server <vlan – id> starting – address <ip – addr> <subnet – mask> size – of – client – ip – pool <1 – 253> <cr>
dhcp server <vlan – id> starting – address <ip – addr> <subnet – mask> size – of – client – ip – pool <1 – 253>[default – gateway <ip – addr>] [primary – dns <ip – addr>] [secondary – dns <ip – addr>]

Функция Сервер IGMP

В коммутаторах 3 – го уровня можно включить встроенный сервер IGMP, который будет регистрировать участников групп multicast и перенаправлять им потоки multicast.

Потоки multicast могут непосредственно приходить от генераторов потоков на один из портов коммутатора, либо могут быть запрошены у других коммутаторов 3 – го уровня по протоколу DVMRP.

Сервера IGMP включаются на IP – доменах. Функция IGMP – Snooping должна быть при этом выключена.

Сервер IGMP не работает одновременно с функцией IGMP snooping, поэтому IP – домен, на котором включен сервер IGMP, должен быть привязан к одному физическому порту. IP – домен, на который приходит поток multicast, тоже должен быть привязан к одному физическому порту.

Например, использован сервер IGMP и коммутатор L2 с функцией MVR. Между коммутаторами в канале trunk передаются кадры с маркером VLAN. На XGS – 4728F настроено 4 IP – домена:

IP: 172.17.0.0/16 VLAN 12 – подсеть генератора потока multicast

IP: 10.10.0.0/16 VLAN 100 – подсеть IGMP – сервера

IP: 192.168.8.0/24 VLAN 108 – подсеть клиента A

IP: 192.168.3.0/24 VLAN 103 – подсеть клиента B

Клиенты A и B находятся в разных VLAN. Эти VLAN маршрутизируются на XGS – 4728F, т. е. на уровне Ethernet клиенты друг от друга изолированы. Можно было бы включить два IGMP – сервера на VLAN 108 и 103, но тогда поток multicast в канале trunk передавался бы дважды, что недопустимо, особенно с ростом количества клиентских VLAN.

С помощью функции MVR запросы IGMP транслируются из клиентских VLAN в VLAN 100, и сервер IGMP запущен на VLAN 100.

Поток multicast передается в канале trunk в VLAN 100 и транслируется в клиентские VLAN на коммутаторе L2.

Команды в CLI:

interface route – domain <ip – address>/<mask> ip igmp <v1|v2|v3>

interface route – domain <ip – address>/<mask> ip igmp robustness – variable <2 – 255>

interface route – domain <ip – address>/<mask> ip igmp query – interval <1 – 65535>

interface route – domain <ip – address>/<mask> ip igmp query – max – response – time <1 – 25>

interface route – domain <ip – address>/<mask> ip igmp last – member – query – interval <1 – 25>13,76

Статические маршруты

Коммутатор обычно использует шлюз по умолчанию для маршрутизации исходящего трафика от компьютеров локальной сети в Интернет.

Чтобы обеспечить возможность отправки данных устройству недоступному

через шлюз по умолчанию необходимо использовать статические маршруты.

Протоколы RIP OSPF

RIP – протокол динамической маршрутизации

RIP (Routing Information Protocol) – достаточно простой протокол динамической маршрутизации, позволяющий L3 – коммутаторам обмениваться информацией о маршрутах друг с другом.

В качестве метрики RIP использует число переходов (хопов, hops, или – число промежуточных узлов).

Максимальное число хопов в RIP = 15 (метрика 16 означает бесконечность), что позволяет использовать протокол только в небольших сетях.

Однако протокол RIP прост в конфигурации.

Отправка и получение пакетов RIP контролируется полем Direction:

1. Both — коммутатор периодически осуществляет широковещательную рассылку своей таблицы маршрутизации и использует всю получаемую информацию RIP
2. Incoming — коммутатор не рассылает пакеты RIP Однако принимает все поступающие пакеты RIP
3. Outgoing — коммутатор рассылает пакеты RIP Но не принимает поступающие пакетов RIP
4. None — коммутатор не рассылает пакеты RIP и игнорирует все поступающие пакеты RIP

Формат и способ рассылки пакетов RIP коммутатором управляются полем Version (заметьте, что при приеме, маршрутизатор распознает оба формата).

Основное отличие протокола версии RIP – 2 и RIP – 1 заключается в возможности RIP – 2 рассылать не только адрес сети, но еще и маску подсети.

Как в случае выбора RIP – 2B, так и в случае выбора RIP – 2M рассылка информации о маршрутах осуществляется в формате RIP – 2, а различие заключается в том, что:

1. В RIP – 2B используется широковещательная рассылка (по адресу 255.255.255.255)
2. В RIP – 2M используется *multicast* рассылка (по зарезервированному адресу 224.0.0.9). RIPvl и RIPv2 используют UDP порт 520/

OSPF – протокол типа «состояния связей»

Протокол динамической маршрутизации OSPF использует Алгоритм Дейкстры для нахождения кратчайшего пути.

Алгоритм Дейкстры — алгоритм на графах, изобретенный Э. Дейкстрой, который находит кратчайшее расстояние от одной из вершин графа до всех остальных.

Протокол OSPF (протокол предпочтения кратчайшего пути) применяется для обмена маршрутной информацией внутри автономной системы (АС). АС – группа соединенных между собой локальных сетей, использующих единый протокол обмена информацией о маршрутах (рис. 33).
OSPF – протокол типа «состояния связей» (link state protocol).
OSPF имеет ряд преимуществ перед дистанционно – векторными протоколами, такими как RIP. OSPF обладает более быстрой сходимостью и может работать в сетях со сложной топологией.
В качестве метрик может использоваться стоимость связей, пропускная способность, количество переходов, производительность, время передачи данных туда и обратно и надежность.

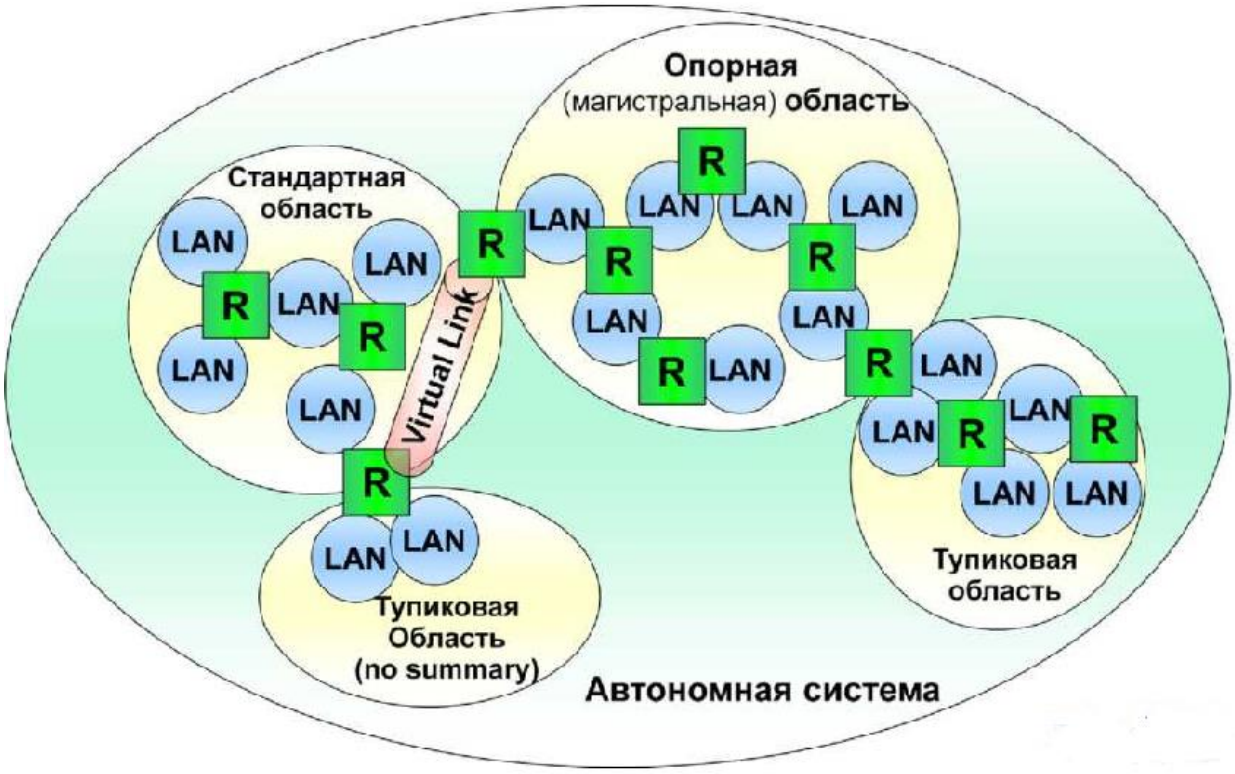

Рис. 33. Работа функции OSPF

Например, стоимость маршрута может складываться из суммарной стоимости связей, стоимость которых – произвольное целое число, назначаемое при настройке OSPF, которое может учитывать надежность и скорость соединения.
В OSPF предусмотрена возможность уведомления всех узлов сети об изменении топологии (например, о разрывах соединений) для быстрого пересчета кратчайших путей.
Обозначения на рис. 33 следующие: R – маршрутизатор; LAN – локальная сеть (отдельная IP – подсеть.
Автономная система OSPF может быть разделена на несколько логических областей (area).
Каждая область – это группа смежных локальных сетей.
Разделение на дополнительные зоны (области) позволяет:

1. снизить нагрузку на CPU маршрутизаторов за счет уменьшения

количества перерасчетов по алгоритму SPF (маршрутизаторы будут анализировать только граф отдельной области, а не всей автономной системы).
2. уменьшить размер таблиц маршрутизации.
3. уменьшить количество пакетов обновлений состояния канала.

Каждой области присваивается уникальный 32 – битный идентификатор зоны (area ID).

Типы областей автономной системы:

Магистральная (опорная, backbone area) область, формирует ядро сети OSPF, имеет идентификатор 0.0.0.0.

Все остальные зоны подключены к магистральной области напрямую или через виртуальный канал.

Опорная зона играет роль по распространению маршрутной информации и транзиту пакетов между всеми остальными областями.

Стандартная область, принимает обновления каналов и маршрутные данные.

Stub – область (тупиковая, нетранзитная) – область, имеющая только одно подключение к другой внутренней области, и не имеющая маршрутов во внешнюю сеть.

Если же маршрутизаторам из тупиковой зоны надо передать информацию за границу автономной системы, то они используют маршрут по – умолчанию.

Если Stub – область содержит только один маршрутизатор (по совместительству являющийся шлюзом к другой внутренней области), то такая область называется No Summary.

Внутри такой области не будет производиться рассылка маршрутной информации (LSA сообщений).

OSPF маршрутизаторы делятся на 4 типа:

1. Internal Router (IR) — внутренний маршрутизатор, расположенный внутри области.
2. Area Border Router (ABR) — граничный маршрутизатор, соединяющий две или несколько областей.
3. Backbone Router (BR) — маршрутизатор, имеющий интерфейс к магистральной области, или внутренний маршрутизатор магистральной области.
4. AS Boundary Router — граничный маршрутизатор автономной системы, соединяющий магистральную область с другими автономными системами.

Каждому OSPF маршрутизатору необходимо назначить произвольный уникальный 32 – битный идентификатор – Router ID.

Каждой области назначается произвольный уникальный 32 – битный идентификатор зоны – area ID. Магистральной области всегда назначается идентификатор 0.0.0.0.

Идентификаторы могут быть указаны в десятичном формате или в формате записи IP – адреса.

Идентификаторы зон и коммутаторов не являются IP – адресами, а только

имеют похожий формат записи, и могут совпадать в написании с любым назначенным IP – адресом.

Принцип работы OSPF следующий.

Все OSPF – маршрутизаторы обмениваются информацией о маршрутах, для построения синхронизированной базы данных состояний каналов в рамках одной автономной системы или одной области.

Для этого они обмениваются сообщениями *Hello*, чтобы подтвердить наличие соседних маршрутизаторов OSPF, затем устанавливают отношения соседства (смежности).

Далее пара маршрутизаторов в состоянии смежности обменивается сообщениями с описаниями базы данных (Database Description, DBD) друг с другом, позволяющими построить синхронизированную базу данных состояния каналов.

Маршрутизатор, получив информацию о базе данных соседа, сохраняет её у себя в памяти, и далее ретранслируют её всем остальным соседям (кроме отправившего маршрутизатора).

База данных состояний каналов непрерывно обновляется посредством множества сообщений LSA (Link State Advertisement – объявление о состоянии канала или маршрутизатора, определено 10 типов LSA).

База данных состояний каналов содержит записи, которые включают в себя идентификаторы маршрутизаторов, связанные с ним каналы и стоимости путей.

После того как все маршрутизаторы обменяются такими сообщениями,

Каждое из устройств использует базу данных состояний каналов и алгоритм Дейкстры для вычисления путей к пунктам назначения в сети с наименьшей стоимостью.

При изменении топологи (по сути – изменения состояния канала), маршрутизатор, обнаруживший это изменение, делает рассылку об изменении состоянии канала, и далее каждый маршрутизатор вновь пересчитывает пути, с помощью SFP алгоритма.

Для предотвращения множественной рассылки копий LSA сообщений между всеми маршрутизаторами, протокол OSPF предусматривает механизм автоматического выбора назначенного маршрутизатора (Designated Router, DR), который управляет процессом рассылки LSA в сети, а также резервного назначенного маршрутизатора (Backup Designated Router, BDR).

Для этого каждому маршрутизатору вручную указывается приоритет.

К выбору DR надо подходить внимательно: каждый маршрутизатор области должен установить отношения соседства (смежности) с DR.

Если какой – либо маршрутизатор обнаруживает изменения в сети, то он отправляет это изменение не всем маршрутизаторам сразу, а только DR, который затем уже разошлет эту информацию остальным маршрутизаторам сети.

Протокол OSPF предусматривает механизм резервирования DR в случае выхода его из строя, путем определения «запасного» маршрутизатора BDR.

Под интерфейсом в OSPF понимается канал между OSPF – маршрутизатором и

OSPF сетью.

С интерфейсом связывается информация о состоянии, адрес и маска подсети. При настройке OSPF, прежде всего для интерфейса включается передача трафика OSPF, а затем интерфейс добавляется к области.

Если некая область не может быть напрямую подключена к опорной области, то необходимо создать виртуальный канал (Virtual link).

Виртуальный канал должен быть настроен на маршрутизаторах немагистральной области и магистральной области.

Чтобы настроить на коммутаторе протокол OSPF, необходимо выполнить следующие задачи:

1. включить протокол OSPF.
2. создать области OSPF.
3. создать интерфейсы и связать их с областями.
4. при необходимости, создать виртуальные каналы для доступа к удаленным областям.

Команды CLI :

router ospf <router – id>
router ospf <router – id> exit
router ospf <router – id> area <area – id> <cr>
router ospf <router – id> area <area – id> name <name>
router ospf <router – id> area <area – id> authentication <cr>
router ospf <router – id> area <area – id> authentication message – digest
router ospf <router – id> area <area – id> stub <cr>
router ospf <router – id> area <area – id> stub no – summary
router ospf <router – id> area <area – id> default – cost <0 – 16777214>
router ospf <router – id> area <area – id> virtual – link <router – id> <cr>
router ospf <router – id> area <area – id> virtual – link <router – id> name <name>
router ospf <router – id> area <area – id> virtual – link <router – id> authentication – same – as – area
router ospf <router – id> area <area – id> virtual – link <router – id> authentication – key <key>
router ospf <router – id> area <area – id> virtual – link <router – id> message – digest – key <keyid> md5
<key>
router ospf <router – id> redistribute static <cr>
router ospf <router – id> redistribute static metric – type <1|2> metric <0 – 16777214>
router ospf <router – id> redistribute rip <cr>
router ospf <router – id> redistribute rip metric – type <1|2> metric <0 – 16777214>
router ospf <router – id> network <ip – addr/bits> area <area – id>
router ospf <router – id> passive – iface <ip – addr/bits>

По умолчанию, протокол OSPF отключен, и требует включения.

Также необходимо указать значения полей:

1. Router ID – уникальный идентификатор OSPF – маршрутизатора. По

форме записи похож на IP – адрес, но им не является.

2. Redistribute Route – механизм перераспределения маршрутов позволяет коммутатору импортировать и прозрачным образом транслировать в сеть OSPF маршруты, полученные с использованием других протоколов маршрутизации (RIP и статических маршрутов).
3. Type: 1 – для протоколов маршрутизации (таких как RIP), у которых внешние метрики напрямую сопоставимы с внутренней стоимостью OSPF. 2 – для протоколов маршрутизации, у которых внешние метрики несопоставимы со стоимостью OSPF.
4. Metric VHlue – стоимость маршрута (в диапазоне от 0 до 16777214).
5. Area ID – уникальный идентификатор области, для которого используется формат IP – адреса Authentication – для получения маршрутов только от доверенных маршрутизаторов, можно включить аутентификацию на всех маршрутизаторах, с указанием общего пароля из 8 или 16 символов (Simple/MD5).
6. STUB Network – необходимо включить, если область является тупиковой (через которую невозможен транзит трафика из других областей)
7. No Summary – установите переключатель, если маршрутизатор не должен отправлять/принимать объявления LSA (n/t/ если в области находится только один маршрутизатор).
8. Default route cost – стоимость для маршрута по – умолчанию в тупиковой области, нужная для маршрутизаторов, являющимися внешними по отношению к основному OSPF – домену (если не указать, то маршрут по – умолчанию не добавляется).
9. Итоговая таблица со всеми настроенными областями OSPF отображается в нижней части экрана OSPF Coniguration.

Далее осуществляется привязка интерфейса к созданной ранее области.

1. из раздела Network необходимо выбрать IP – интерфейс.
2. Area ID – выбор области, которую необходимо связать с данным интерфейсом.
3. Authentication – если будет использоваться аутентификация, то на всех маршрутизаторах одной области необходимо использовать одинаковый режим.
4. Key ID – в случае выбора MD5 в поле Authentication – указывается используемый номер аутентификации.
5. Key – в случае выбора типа аутентификации Simple – введите 8 символов пароля, и в случае MD5 – 16 символов.
6. Cost – стоимость интерфейса, используемая для вычисления таблицы маршрутизации. По умолчанию, стоимость интерфейса =15(допустимые значения 0 – 65535).
7. Priority – приоритет, назначенный интерфейсу, используемый при выборах назначенного маршрутизатора (DR) и резервного назначенного маршрутизатора (BDR). Допустимые значения 0 – 255, значение 0 исключает маршрутизатор из участия в выборах.

Virtual link

Для доступа в область, не подключенную к магистрали непосредственно, нужно настроить виртуальный канал (virtual link), проходящий через некоторую промежуточную область.
Поле Area ID – выбирается ID области, которую необходимо передавать через Virtual Link
Поле Peer Router ID – это уникальный идентификатор граничного (удаленного) маршрутизатора, подключенного к магистральной области, с которым устанавливается виртуальный канал.
Параметры аутентификации аналогичны настройкам обычной OSPF – области.

Протокол внешней маршрутизации BGP

BGP – Border Gateway Protocol имеет следующие свойства:

1. обеспечивает взаимосвязь между независимыми сетями.
2. использует рассылку только обновлений.
3. содержит ряд функций, повышающий безопасность (например, аутетинфикацию пользователя).
4. обеспечивает контроль правильности работы маршрутизаторов и сетевых соединений.
5. в качестве протокола транспортного уровня использует TCP.
6. обновления рассылаются каждые 4 с.

Особенности BGP:

1. использует принцип ближайшего соседа.
2. вместе с адресом отсылает его маску для идентификации узла.
3. позволяет осуществлять настройку политики маршрутизации (различать пользователей).
4. распространяет информацию о достижимости – о расположенных внутри автономной системы получателях.
5. относится одновременно к дистанционно – векторным протоколам и протоколам на основе состояния соединения.
6. контролирует взаимодействие одноранговых маршрутизаторов (спикеров BGP) для исключения рассылки противоречивой информации.

Основные типы сообщений BGP

1. Open – открыть – инициализация взаимодействия.
2. Update – обновить – обновляет маршрутную информацию.
3. Notification – известить – ответ на неверное сообщение.
4. Keepalive – проверить – проверка возможности соединения между двумя BGP – спикерами.

Сообщение BGP минимум 20 байт, максимум 4096 байт.
Сообщение BGP содержит поля:

- маркер,
- длина,
- тип,
- номер версии,

- номер автономной системы,
- время удержания соединения,
- идентификатор сообщения,
- длина поля параметров,

параметры (необязательное поле, имеет переменную длину, используется при настройке BGP).

Сообщение BGP всех типов имеют общий стандарт заголовка.

Заголовок сообщений BGP включает в себя поля – маркер, длина, тип.

Маркер – специальная комбинация, служащая для обозначения начала сообщения.

Назначается по взаимной договоренности маршрутизаторов, участвующих в обмене информацией.

1. размер маркера 16 байт.
2. длина – значение от 19 до 4096.
3. тип – один из 4х.

Каждый тип сообщения BGP имеет свой формат.

Контрольные вопросы по главе 5

1. Что такое домены таршрутизации?
2. Назначение функции сервера DHCP?
3. Назначение функции сервера IGMP?
4. Назначение функции статических маршрутов?
5. Назначение функции протокола RIP?
6. Назначение функции протокола OSPF?
7. Назначение функции Virtual Link?
8. Назначение функции протокола BGP?

Глава 6. Дополнительные функции L3 третьего уровня

Функция Load Sharing

Load Sharing использует методику маршрутизации ECMP (Equal Cost Multi – Path). Это позволяет осуществлять маршрутизацию пакетов, для которых есть несколько альтернативных маршрутов до сети назначения, и стоимости этих маршрутов равны, через разные маршрутизаторы. Выбор маршрутизатора основан на значении ключа, получаемого в результате работы hash функции над IP адресом источника и IP адресом назначения, или только над IP адресом источника.
Функция Load Sharing работает как со статическими маршрутами, так и при применении протоколов динамической маршрутизации (например, OSPF). Используя функцию ECMP, возможно улучшить производительность сети, балансируя нагрузку между несколькими маршрутизаторами.
Для настройки Load Sharing необходимо определить критерий (Source — Destination IP или Source IP) и временные интервалы жизни записи в таблице (Aging Time) и время повторного опроса не найденных MAC адресов соседних маршрутизаторов (Discover Time).

Протокол IPv6

IPv6 – протокол маршрутизации, отвечающий за адресацию, маршрутизацию и фрагментацию пакетов отправляющим узлом. Протокол IPv6 призван заменить своего предшественника IPv4.
Протокол IPv6 (рис. 34) вскоре станет ключевой составляющей технологии сетей следующего поколения. Он несет в себе огромные возможности. Чтобы удовлетворить растущий спрос на решения для IPv6 со стороны операторов связи, сегмента SMB идомашних пользователей, компания ускоряет выпуск готовых к использованию в сетях IPv6 продуктов, помогая клиентам осуществить плавный переход и развертывание и максимально использовать новые возможности IPv6.
Рассмотрим технические отличия и новшества протокола IPv6. По сравнению с IPv4, в IPv6 длина адресов увеличена в 4 раза, до 128 бит. Это позволило существенно расширить адресное пространство. Увеличение длины адресов повлекло и увеличение заголовка.
IPv6 адреса записывается в виде 16 – ти битных полей, в шестнадцатеричном виде (нечувствительно к регистру).
При этом начальные (и только начальные) нули в 16 – ти битных полях – необязательны и могут быть сокращены для удобства записи.
В IPv6 определены несколько типов адресов, которые будут рассмотрены далее. Каждый типа адреса имеет свой формат.

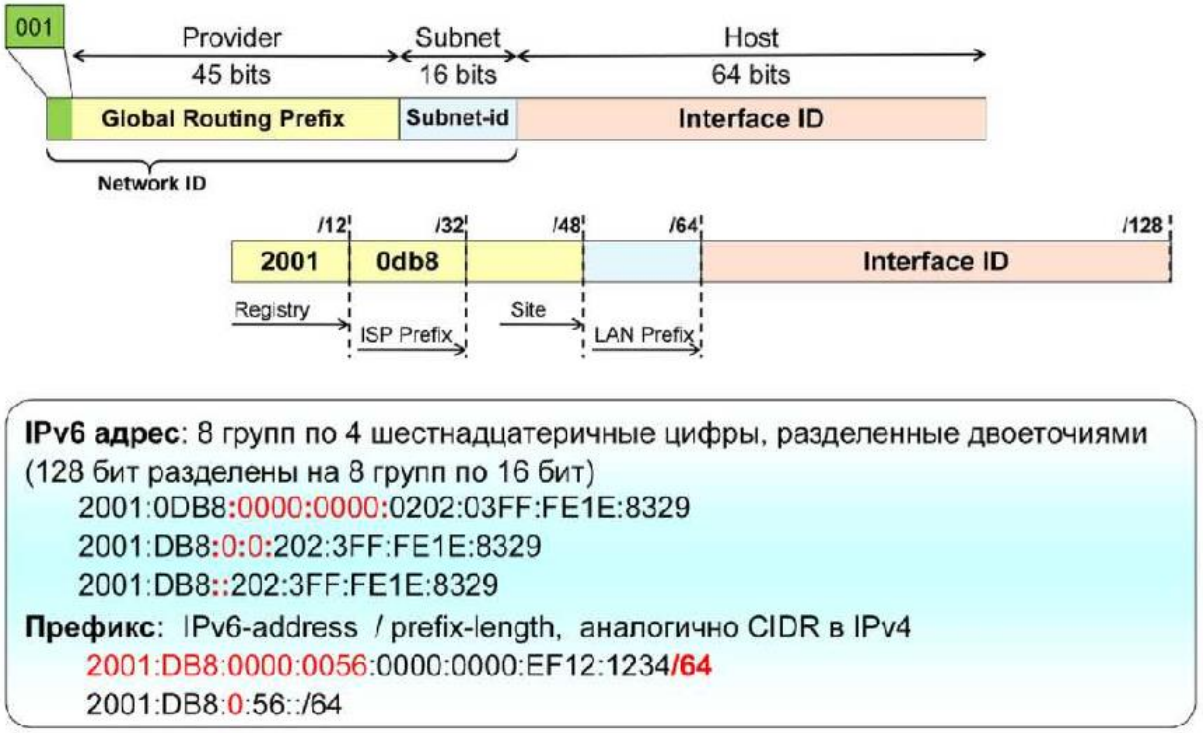

Рис. 34. Описание IPv6

Процесс выдачи Global IPv6 адресов контролирует IANA (Орган присвоения номеров Интернета). К настоящему моменту IANA выделила блок адресов 2000::/3 для начального использования IPv6 на глобальном уровне. Пять региональных регистрационных центров интернета (RiR) разделяют на меньшие блоки адресное пространство (/32). И наконец (через национальных и локальных интернет регистраторов), достающиеся Провайдерам интернета (ISP) блоки адресов подлежат расщеплению на более мелки части, предоставляя конечным пользователям не отдельные адреса, а целые подсети (/48). Префикс /64 означает, что у конечного клиента не будут использоваться подсети.

Для такого «деления», как и в IPv4 протоколе (CIDR), используются маски, называемые префиксами (prefix). Классовой адресации в IPv6 нет.

Поле Interface ID unicast адреса может быть назначено несколькими путями:

1. Автоматически сгенерировано по формату EUI – 64 (на основе MAC – адреса хоста).
2. Автоматически сгенерированное случайное число.
3. Назначено по DHCP.
4. Задано вручную.

Заголовок протокола IPv6 имеет фиксированную длину 40 октетов что в 2 раза больше заголовка Ipv4, однако заголовок IPv6 был упрощен. Длина адреса Ipv6 выросла в 4 раза, до 128 бит, что позволило существенно расширить адресное пространство IPV6.

Заголовок IPv6 содержит меньше полей, что ускоряет обработку пакетов.

Поля заголовка IPv6:

Version: аналогично IPv4. Содержит номер 6.

Traffic class: аналогично полю TOS в IPv4. Функции поля остались те же (как и в IPv4)
Flow label: Новое поле в IPv6. Служит для пометки потока данных, вцелях упрощения процедуры обработки однотипного.
Payload length: функции аналогичны полю "Total length“ в IPv4.
Next header: определяет тип информации, располагающейся сразу за основным заголовком IPv6 (например TCP, UDP). Однако это может быть и дополнительный заголовок. Данное поле аналогично полю "Protocol“ в IPv4.
Hop Limit: аналогично полю TTL в IPv4, поле определяет максимальное число переходов IP – пакета при передаче его по сети. Каждая пересылка пакета уменьшает значение поля на единицу.
Source address: поле длиной 16 октетов с адресом источника пакета.
Destination address: поле длиной 16 октетов с адресом получателя пакета.
Далее могут следовать дополнительные заголовки, число которых может варьироваться.
Существенным изменением стало упразднение заголовка контрольной суммы, что позволяет увеличить скорость обработки пакета маршрутизатором. Функции проверки корректности пакета возлагаются на канальные и транспортные протоколы.

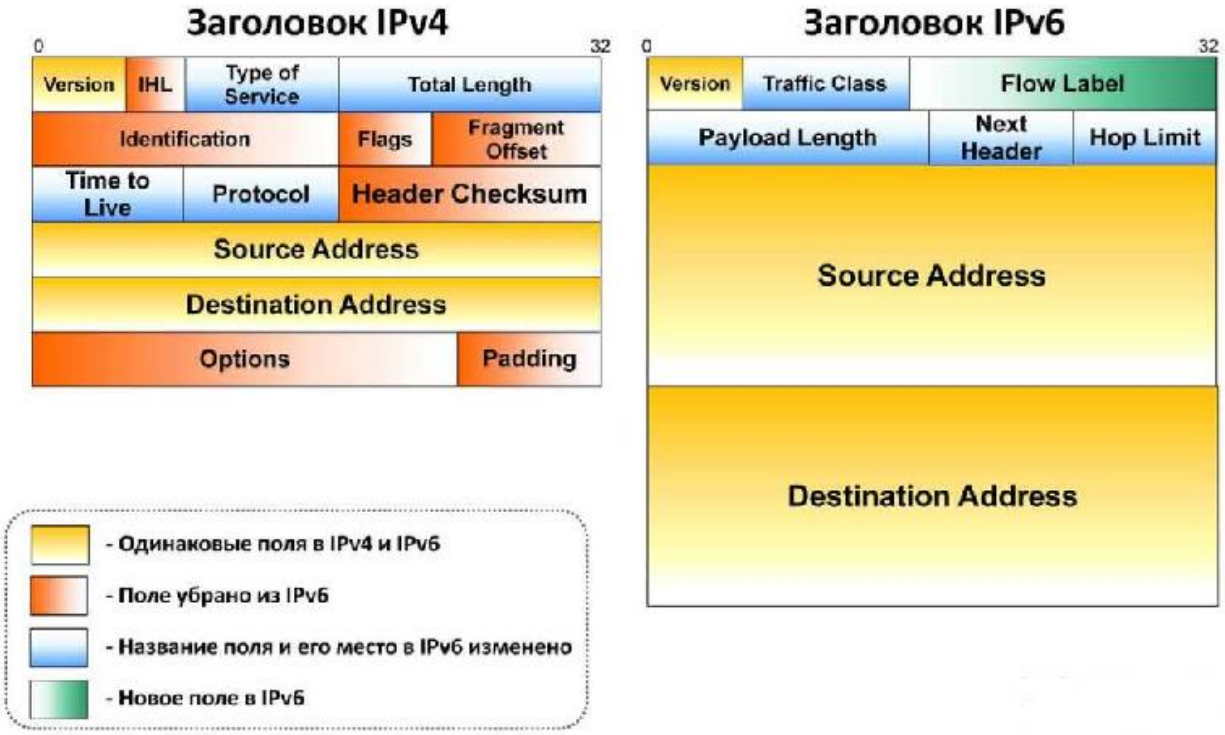

Рис. 35. Заголовки IPv6 и IPv4

IPv6 определяет (рис. 35) фиксированную длину заголовка: 40 октетов (320 бит). IPv6 пакет может быть дополнен дополнительным заголовком (Extension Header). Полезные данные пакета (PDU) содержат протокол более высокого транспортного уровня, или это могут быть сетевые данные (ICMPv6).
В IPv4 минимальный блок передаваемых данных MTU составлял 68 октетов (при рекомендованных минимальных 576 октетов). Т.е. любой пакет IPv4 имеет

длину минимум 64 октета. В IPv6 минимальный MTU равен 1280 октетам (при 1500 рекомендуемых).

В IPv6 реализован механизм Path MTU discovery, позволяющий автоматически найти минимальный MTU на пути следования пакетов между источниками, что предотвращает фрагментацию пакетов в IPv6 сетях (механизм Path MTU Discovery использует ICMPv6 сообщения).

Максимальный поддерживаемый размер IPv6 пакета – 64К октетов, однако максимальный размер фрейма многих протоколов гораздо меньше.

Для передачи больших блоков данных используется jumbo payload в расширенном заголовке Hop – by – hop option. Размер таких джамбограмм – до 4 гигабайт.

Типы адресов

Unicast адреса в IPv6 предназначены для идентификации конкретного интерфейса в сети. Существует несколько типов unicast адресов:

1. Global unicast.
2. Unique local unicast.
3. Link – local, которые будут рассмотрены далее.

В IPv6 отсутствует broadcast – адреса.

Вместо них широкое развитие получили **multicast** адреса, использующиеся, в том числе (помимо предоставления различных сервисов конечным пользователям), и для служебных нужд (например, широковещательные адреса IPv4 (обычно xxx.xxx.xxx.255) выражаются multicast адресом в IPv6.

Существует ряд зарезервированных multicast – адресов для обращения ко всем узлам сети, всем маршрутизаторам, DHCP – серверам сети и др.

Anycast – совершенно новый типа адресов, определенный в IPv6, определяющий группу устройств. Однако, в отличии от multicast, пакет, посланный на anycast адрес доставляется только одному интерфейсу – ближайшему. Синтаксически anycast адреса не отличаются от unicast адресов, т.к. anycast адреса назначаются группе интерфейсов из пространства адресов unicast.

Link – local адреса генерируются узлом автоматически, служат для взаимодействия узлов одной подсети, а также для автоматической настройки адреса, поиска маршрутизатора, обнаружения соседей.

Unique Local unicast адреса служат для сетей с приватным адресным пространством, на подобии Private IP – адресов в Ipv4. Изначально для этих целей использовался диапазон Site – local адресов, к настоящему моменту выведенный из употребления.

Global Unicast адреса – «белые», глобальные адреса IPv6 для работы в Интернет.

Диапазон Global Unicast адресов:

2000::/3 ~ 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, однако из выделенного диапазона для реального использования на сегодняшний момент выделены только несколько подсетей, в числе которых:

2001:db8::/32 – документирование и примеры (**Global IPv6**)

2001:7f8::/32 – для выдачи блоков точкам обмена интернет – трафиком
2001:0::/32 – для клиентов Teredo
2002::/16 – для технологии туннелирования 6to4
Тип IPv6 адреса определяется его лидирующими байтами. По этим байтам можно понять, к какому типу относится тот или иной адрес. Это упрощает маршрутизацию. Комбинация лидирующих байтов называется префиксом.
В таблице показаны протоколы и выполняемые ими функции.

Протокол	**Функция**
IPv6	Адресация, маршрутизация, фрагментация пакетов отправителем
I**CMPV6**	Диагностические функции и отчеты об ошибках Поиск соседей; определение MTU; сообщение сетевого префикса, адреса шлюза и др. **Замена протоколов ICMPv4, ARP, IGMP**
Neighbor Discovery	Использует ICMPv6 Для взаимодействия соседних узлов, поиска DNS – серверов и др. Заменяет протокол ARP, и сообщения ICMPv4 Router Discovery и ICMPv4 Redirect message
Multicast Listener Discovery	Использует сообщения ICMPv6 для определения получателей multicast запросов Замена протокола IGMP для IPv6 сетей
DHCPv6	Назначение адресу хосту, как *альтернатива* механизму автоконфигурации Сервер DHCPv4 выдает маску подсети для каждого адреса В IPv6 маска сети выдается с помощью ICMPv6 Router Advertisements ,а не сервером DHCPv6.

Протокол ICMPv6

Протокол ICMPv6 выполняет диагностические функции и сигнализирует об ошибках, связанных с неудачной доставкой Ipv6 пакетов.

Протокол Neighbor Discovery

Neighbor Discovery Protocol служит для взаимодействия соседних узлов, и включает в себя обмен сообщениями для разрешения адресов, автонастройку адреса конечных точек сети, выявления дублирующихся адресов, поиска доступных путей и DNS – серверов, обнаружения подсетей и поддержки доступности информации о путях другим активным соседним узлам. Neighbor Discovery заменил протокол Address Resolution Protocol (ARP), и сообщения ICMPv4 Router Discovery и ICMPv4 Redirect.
Neighbor Discovery Protocol, NDP (Протокол Обнаружения Соседей) —

протокол из набора Internet Protocol Suite, используемый совместно с IPv6. Протокол работает сетевом уровне, описан в (RFC 4861).
Этот протокол использует пять различных типов ICMPv6 сообщений.
Протокол ND повышает надежность доставки пакетов при наличии проблемных маршрутизаторов или подключений, или непостоянных

Протокол Multicast Listener Discovery

Протокол Multicast Listener Discovery (MLD) заменил IGMP, использовавшийся в IPv4 сетях.MLD – это набор сообщений ICMPv6, отвечающих за управление получателями многоадресных рассылок.
Multicast Listener Discovery, MLDP – один из протоколов стека протоколов IPv6. MLDP используется для определения получателей широковещательных запросов. В стеке протоколов IPv4 вместо него служил протокол IGMP/
Существует три типа MLD сообщений.

1. Multicast Listener Query, называемый также Query, двух типов:
   General Query отправляется каждые 125 мс чтобы узнать какие multicast – адреса имеют подписчики.
   Multicast – Address – Specific Query для выяснения имеются ли подписчики у конкретной multicast – группы.
2. Multicast Listener Report – аналогично сообщению join в IGMP для IPv4.
3. Multicast Listener Done – аналогично сообщению leave в IGMP для IPv4

MLD Snooping — это функция, позволяющая коммутаторами второго уровня перенаправлять multicast траффик на порты, с которых пришли запросы.
При использовании MLD Snooping уменьшается количество управляющих сообщений.

Функция DHCPv6

В IPv6 хост может самостоятельно сконфигурировать сетевой адрес, или использовать службу DHCPv6.
Однако, в IPv6 сетях назначение сетевого префикса (маски) осуществляется с помощью сообщения ICMPv6 Router Advertisements, а не DHCPv6 сервером.
Сервер DHCPv6 также не выдает адрес default gateway (шлюз сам должен объявить о себе с помощью Neighbor Discovery, ND). Адреса DNS серверов также объявляются с помощью ND.
ICMPv6 позволяет узлам в сети выполнять диагностику и сообщать о проблемах. Как и в IPv4, в ICMPv6 реализовано два типа сообщений: сообщения об ошибках, таких как "недоступность адресата", "пакет слишком большой", "превышение времени" и информационных сообщений, таких как "echo request" и "echo reply".
ICMPv6 состоит из заголовка и полезных данных протокола. Заголовок содержит только три поля: тип (8 бит), код (8 бит), и контрольная сумма (16 бит).

L3 коммутаторы (ex. XGS-4728F)	L2+ коммутаторы (ex. MES3500-24)
Статическая маршрутизация IPv6	–
IPv6 over Ethernet	
DHCPv6 Relay/Client	
ICMPv6	
IPv6 Path MTU discovery	
NDP (Neighbor Discovery Protocol)	
IPv6 stateless auto-configuration: host/router	
Фильтрация IPv6 адресов	
ACL на основе IPv6 адресов	
Dual stack - IPv4 и IPv6	
MLD Snooping / proxy	

Рис. 36. IPv6 функции коммутаторов

Тип определяет тип сообщения, значения в диапазоне от 0 до 127 указывают на ошибки, аот 128 до 255 на информационное сообщение.
Значение поля кода зависит от типа сообщения и обеспечивает дополнительный уровень детализации сообщений.
Поле контрольной суммы обеспечивает минимальный уровень безопасности для проверки ICMPv6 пакета.
ICMPv6 сообщения инкапсулированы в пакеты IPv6, сполем Next Header 58.
На рис. 36 представлены IPv6 функции коммутаторов, реализованные в микропрограмме версии 4.0
В коммутаторах часто на задней панели может имеется разъем для подключения резервного электропитания.

Блок питания BPS – 120

Блок питаня позволяет подать постоянное напряжение на коммутатор, если возникнет сбой в электропитании коммутатора от сети 220 В. К BPS – 120 можно подключить до шести устройств, но в случае сбоя питание будет подаваться только на одно из них.
Основное назначение BPS – 120 – обеспечить надежность функционирования сети в случае выхода из строя блока питания коммутатора

Energy Efficient Ethernet

В коммутаторах с поддержкой IEEE 802.3az (Energy Efficient Ethernet) реализованы функции энергосбережения для большей энергоэффективности оборудования.

Возможность динамически регулировать выходную мощность порта в зависимости от активности линка, наличия трафика в реальном времени и длины кабеля позволяют сократить потребление электроэнергии.
При этом сохраняется полная совместимость с существующим сетевым оборудованием.
Функция **Traffic detection** в составе Energy Efficient Ethernet (EEE) отслеживает активность сетевого трафика, и в периоды простоя или не незначительного трафика, динамически регулирует энергопотребление, которое в обычном режиме тратится на поддержание работы Ethernet Physical Layer даже в моменты простоя. Необходима поддержка EEE на обоих концах линка.
Функция **Inactive link detection** (также называемая Auto Power Down) позволяет обнаруживать неактивные порты коммутатора и снижать энергопотребление на таких портах: отключаются почти все функции физического уровня, а энергия тратится только на проверку поступающих импульсов от удаленной стороны, и при поступлении такого импульса порт автоматически переходит в нормальный режим работы.
В традиционных Ethernet – сетях мощность передатчика выбирается исходя из максимально возможной длины кабеля.
Функция **Cable length detection** (также называемая Short Reach) позволяет коммутатору автоматически измерять длину подключенных Ethernet – кабелей и в соответствии с ней снижать мощность каждого порта (т.е. чем короче кабель, тем меньше мощности потребляет порт).

Контрольные вопросы по главе 6

1. Назначение и фунции протокола IPv6?
2. Назначение и фунции протокола ICMPv6?
3. Назначение и фунции протокола Neighbor Discovery Protocol?
4. Назначение и фунции протокола Multicast Listener Discovery?
5. Назначение и фунции протокола DHCPv6?
6. Назначение и фунции Energy Efficient Ethernet?

Глоссарий

ARP (Address Resolution Protocol) – протокол определения MAC – адреса по известному IP – адресу.
BPDU (Bridge Protocol Data Unit) — кадр, используемый протоколом STP/RSTP при построении дерева.
CLI (Command Line Interface) — интерфейс командной строки.
DA (Destination Address) — адрес назначения.
DHCP (Dynamic Host Configuration Protocol) —протокол, позволяющий компьютерам автоматически получать IP – адрес и другие параметры, необходимые для работы в сети TCP/IP.
DSCP (DiffServ Code Point) — 6 – битовоеполевзаголовке IP – пакета, обычно используется для приоритезации.
DVMRP (Distance Vector Multicast Routing Protocol) — дистанционно –

векторный протокол маршрутизации групповых рассылок (RFC 1075).
EAP (Extensible Authentication Protocol) — расширяемый протокол аутентификации. Известные расширения этого протокола: EAP – MD5, EAP – TLS (со взаимной аутентификацией сторон с помощью сертификатов) и EAP – TTLS (с аутентификацией сервера на основе сертификата и аутентификацией клиента по логину и паролю).
EEE (Energy – Efficient Ethernet) – функции энергосбережения для большей энергоэффективности оборудования (802.3az).
FCS (Frame Check Sum) — контрольная сумма кадра.
GVRP (GARP VLAN Registration Protocol) – протокол динамической регистрации VLAN.
GUI (Graphical User Interface) — графический интерфейс пользователя, например web – браузер.
GVRP (GARP VLAN Registration Protocol) — протокол динамической регистрации VLAN, основанный на GARP.
HDAP (Host Discovery and Address assignment Protocol) — протокол для обнаружения узла и назначения адреса, используется устройствами для централизованного управления iStacking.
ICMP (Internet Control Message Protocol) – протокол управляющих сообщений и сервисных функций. Используется для передачи сообщений об ошибках и исключительных ситуациях, при передаче данных.
ICMPv6 – адаптированный протокол ICMP для IPv6 сетей. Выполняет диагностические функции и сигнализирует об ошибках, связанных с неудачной доставкой Ipv6 пакетов.
IGMP (Internet Group Management Protocol) — протокол управления группами многоадресных рассылок. (RFC 1112, RFC 2236, RFC 3376).
L/T (Length/Type) — поле Типа/Длины кадра Ethernet.
LACP (Link Aggregation Control Protocol) — протокол управления агрегированными каналами.
L2PT (Layer 2 Protocol Tunnel) —функция для передачи кадров протоколов CDP, STP, VTP, PAGP, LACP, UDLD через сеть провайдера второго уровня.
MAC (Media Access Control) — управление доступом к среде.
MAC – адрес — адрес устройства в локальной сети.
MLD (Multicast Listener Discovery) – протокол стека IPv6, использующий сообщения ICMPv6, аналогичный по функциям протоколу IGMP в IPv4.
MSTP (Multiple Spanning Tree Protocol) — алгоритм покрывающего дерева, работающий внутри VLAN. VLAN в сети может быть несколько, отсюда и название алгоритма (IEEE 802.1s).
MRSTP (Multiple RSTP) — реализация RSTP в некоторых коммутаторах , позволяющая включать один коммутатор в несколько деревьев RSTP. Для этого на коммутаторе указываются группы портов, относящихся к различным экземплярам RSTP
MTU (Maximum Transfer Unit) — максимальный размер пакета, допустимый к передаче в данном сегменте локальной сети.

Multicast (Групповая рассылка) – тип широковещания, работающий по принципу «один источник – группа получателей», используя при этом специальный диапазон ip – адресов.
MVR (Multicast VLAN Registration) — метод отправки групповых рассылок в отдельном VLAN .
NAT (Network Address Translation) — это механизм в сетях TCP/IP, позволяющий преобразовывать IP – адреса проходящих пакетов. (RFC 1631, RFC 3022)
NAPT (Network Address Port Translation) — частный случай механизма NAT, который помимо подмены IP – адресов проходящих пакетов обеспечивает подмену TCP/UDP портов проходящих пакетов. (RFC 3022)
Neighbor Discovery Protocol – протокол стека Ipv6, использующий сообщения **ICMPv6**, по функционалу заменил протокол Address Resolution Protocol (ARP), и сообщения ICMPv4 Router Discovery и Redirect в IPv4 сетях.
OSPF (Open Shortest Path First) — протокол маршрутизации на основе состояния связей (link – state) (RFC 2328).
PEAP (Protected Extensible Authentication Protocol) — защищенный расширяемый протокол аутентификации. Приблизительно то же самое, что EAP – TTLS, инициатива Microsoft и Cisco.
QoS (Quality of Service) — качество обслуживания.
QinQ (802.1Q in 802.1Q, VLAN Stacking) — расширение к стандарту IEEE 802.1Q, описывающее повторное тегирование уже тегированного трафика для увеличения числа VLAN в сети или дополнительной логической изоляции трафика и QoS на магистальных соединениях.
RADIUS (Remote Authentication Dial – In User Service) — служба, отвечающая за аутентификацию пользователей. На сервере RADIUS хранится информация о пользователях и паролях (RFC 2865, RFC 2866).
RIP (Routing Information Protocol) — дистанционно – векторный маршрутизирующий протокол. Из – за медленной сходимости применяется только в небольших сетях (RFC 1058, RFC 2453).
RFC (Request For Comment) — общее название документа – рекомендации комитета IETF (Internet Engineering Task Force).
RSTP (Rapid Spanning Tree Protocol) — улучшенная редакция протокола STP с быстрым восстановлением связности сети при разрывах в активной топологии (IEEE 802.1w).
SA (Source Address) — адрес источника.
SFP (Small Factor Pluggable) — универсальный модуль для подключения оптоволоконного канала к коммутатору.
SPQ (Strict Priority Queueing) — алгоритм обработки очередей на порту коммутатора.
STP (Spanning Tree Protocol) — протокол покрывающего дерева, служит для удаления циклов из сети(IEEE 802.1d).
TACACS+ (Terminal Access Controller Access Control System) – протокол управления доступом для сетевых устройств через централизованные сервера,

обеспечивая раздельные AAA – сервисы. TACACS+ потенциально медленнее RADIUS, но более безопасен.
TCI (Tag Control Information) — управляющая информация, содержащаяся в теге 802.1Q.
TOS (Type of Service) — флаговое поле в заголовке IP – пакета. Флаги отвечают за тип обслуживания – «наилучшее время», «наименьшая стоимость» ит.п.
TPID (Tag Protocol Identifier) — идентификатор протокола тега (маркера) 802.1Q.
VID (VLAN Identifier) — идентификатор VLAN.
VLAN (Virtual Local Area Network) — виртуальная локальная сеть.
VRRP (Virtual Router Redundancy Protocol) — протокол виртуального отказоустойчивого маршрутизатора (RFC 3768).
WDM (Wavelength Division Multiplexing) — метод полнодуплексной передачи данных по одному оптоволоконному кабелю, когда прямой и обратный сигналы передаются на различных длинах волн.
WFQ (Weighted Fair Queuing) — алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и объеме отправляемых данных.
WRR (Weighted Round Robin) — простой циклический алгоритм управления «взвешенными» очередями пакетов, основан на весах очередей и количестве отправляемых пакетов.

Литература

1. Основы локальных компьютерных сетей. [Электронный ресурс]: учеб. пособие / Сергеев А.Н. [и др.]. — Электрон. дан. — Санкт – Петербург: Лань, 2016. — 184 с. — Режим доступа: https://e.lanbook.com/book/87591. — Загл. с экрана.

2. Информационные системы и сети. [Электронный ресурс]: учеб. пособие / Гладких Т.В. [и др.]. — Электрон. дан. — Санкт – Петербург: Лань, 2016. — 86 с. — Режим доступа: https://e.lanbook.com/book/92230. — Загл. с экрана.

3. Локальные сети и интернет. [Электронный ресурс]: учеб. пособие / Заика А.А. [и др.]. — Электрон. дан. — Санкт – Петербург: Лань, 2016. — 323 с. — Режим доступа: https://e.lanbook.com/book/100727. — Загл. с экрана.

4. Сайт производителя сетевого оборудования Zyxel. [Электронный ресурс]. — Режим доступа: www.zyxel.ru

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

Факультет программной инженерии и компьютерной техники специализируется на подготовке специалистов по разработке компьютерных систем и новейших технологий программирования. Вектор развития факультета определяется прогнозом потребностей компьютерной и программной индустрии через 10-20 лет. Факультет ПИиКТ готовит специалистов грядущей постинформационной эпохи – эпохи виртуальной реальности, киберфизических систем и интернета вещей.
Центр образования при факультете ПИи КТ реализует следующие направления деятельности:

- подготовка магистров по направлению 09.04.01 «Информатика и вычислительная техника»;
- подготовка бакалавров (без отрыва от производства – очно – заочная форма обучения) по направлению 09.03.01 Информатика и вычислительная техника;
- переподготовка специалистов, имеющих высшее образование, с выдачей государственного диплома о дополнительном (к высшему) образовании с присвоением квалификации;
- переподготовка специалистов, имеющих высшее и среднее профессиональное образование с выдачей государственного диплома о переподготовке с правом работы по новой специальности;
- повышение квалификации с выдачей государственного свидетельства (удостоверения)/сертификата Университета ИТМО.

С сентября 2003 года в центре образования проводится обучение по программным продуктам фирмы 1С последних версий. С 2007 года на базе центра образования создан авторизованный Учебный центр фирмы ZyXEL, в котором проводится обучение теории и практике применения современного сетевого оборудования для построения LAN – WAN сетей с использованием оборудования и технологий ZyXEL. В 2012 году был создан Авторизованный Учебный центр фирмы QNAP для подготовки сертифицированных специалистов по системам IP – видеонаблюдения и сетевых хранилищ данных.

Светлана Михайловна Платунова

Игорь Владимирович Елисеев

Елена Юрьевна Авксентьева

Ehternet switch l2&l3. Проектирование, настройка, диагностика сетей передачи данных

Учебное пособие

В авторской редакции
Редакционно – издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно – издательский отдел
Университета ИТМО
197101, Санкт – Петербург, Кронверкский пр., 49