D-Link®

DAS-3248

IP DSLAM
Руководство пользователя

Rev. 1.05 (Jan. 2007)

RECYCLABLE

Содержание:

Предисловие

Данное руководство является описанием технологий, использованных в коммутаторах ADSL (IP DSLAM) компании D-link и примеров их использования в повседневной настройке. Данное руководство не претендует на полноту перечисленных команд, а имеется своей целью показать структуру систем управления DSLAM (в том числе структуру командного режима CLI), их назначение и типовые приемы работы с ними.

Примечание 1: Несмотря на то, что данное руководство посвящено DSLAM DAS-3248, данный документ может быть использован также для настройки модели DSLAM DAS-3224 (имеющего 24 порта ADSL/ADSL2+)
Везде, где для DAS-3248 сказано о 48 портах (интерфейсах), для DAS-3224 следует читать 24 порта (интерфейса).

Примечание 2: Данное руководство справедливо **только** для внутреннего программного обеспечения версии **3.xx** устройств **DAS-3224,DAS-3224/BE,DAS-3248,DAS-3248F HW Rev. A1**
Для более ранних прошивок (версий 1.xx и 2.xx) смотрите предыдущие версии документа
Команды могут отличаться по синтаксису.

История версий документа.

Номер версии	Описание изменений
1.00	Исходная версия.
1.01	Изменена глава 3.Настройка DSL линий (раздел 3.1) • Добавлено описание тестирования и оценки линии ADSL (раздел 3.6) Изменена глава 10. Настройки QoS на DAS-3248: • Добавлено описание алгоритмов Rate Limiting (раздел 10.1.3) • Добавлено описание функции Flow Based Rate Limiting (раздел10.2.3) • Добавлено описание функции IRL (раздел 10.2.4) • Добавлено описание функции ORL (раздел 10.2.5) • Добавлено описание Traffic Class Profile (раздел 10.2.6)
1.02	Добавлено описание параметров профиля DSL линии, влияющих на помехоустойчивость (раздел 3.6.4) Изменена глава 7.Способы передачи пакетов • Добавлено описание функции Port Security (раздел 7.2.1) • Добавлено описание настройки типов коммутации (раздел 7.2.2) • Добавлено описание функции Virtual MAC (раздел 7.2.3) Изменена глава 9.Настройка пакетных фильтров: • Добавлены действия правил в раздел 9.1.1 • Добавлено описание обработки логических выражений (раздел 9.1.5) • Добавлено описание обработки пакетов в Control Plane (раздел 9.1.6) • Добавлено описание Generic List и Named List (раздел 9.1.7)
1.03	Добавлено описание функций: • VC Aggregation (раздел 4.6) • Q-in-Q (раздел 7.4) Добавлено описание POST теста устройства (Приложение B)
1.04	Добавлено описание функций: • Redundancy Aggregation (раздел 6.4) Раздел 6.4 версии 1.03 документа перемещен в раздел 6.5 настоящего документа.
1.04a	Добавлено описание настройки некоторых функций DAS-3248 посредством SNMP запросов (Приложение D)
1.05	Добавлены изменения, касающиеся релиза 3.xx программного обеспечения: • В Разделе 3.4 удалены описания параметров профиля линии AtucGsStandard, AtucGsAnnexType, AtucGsAdvertisedCapabilities, LineDmtConfMode.Вместо них изменено описание команды modify adsl line intf ifname dsl-x LineTransAtucConfig <val set> описания профиля ADSL порта • В Раздел 7.5 добавлено описание новых параметров IGMP Igmpversionmask, maxgrpallowed, startupqrycount, lastmemberqrycount, а также пример фильтрации группового трафика по 7.5.3.7 Добавлено описание некоторых команд управления таблицей коммутации в раздел 7.1. Добавлено описание команд включения/отключения SNMP Traps в Раздел 1.6.2. Исправлены примеры реализации функции Q-in-Q (Раздел 7.4.8) Расширено приложение D. Добавлены описания управления параметрами профиля линии DSL, параметрами модуляции ADSL посредством SNMP запроса. Расширено приложение C. Добавлены примеры конфигурирования generic filter.

Функциональные возможности DAS-3248

1. Основные преимущества системы
• 24/48 портовый ADSL/ADSL2/ADSL2+ абонентский интерфейс
• 2x10/100/1000BaseT или 1x10/100/1000BaseT и 1x1000Base Lx Uplink интерфейсы (в зависимости от выбранной модели устройства)
• Встроенные POTS сплитеры на всех портах ADSL
• Возможность каскадирования до 8 коммутаторов.
•50 контактный коннектор для ADSL+POTS IN или POTS OUT
•Входящая скорость передачи данных (Downstream) от 32 Кбит/с до 25 Мбит/с;
•Исходящая скорость передачи данных (Upstream) от 32 Кбит/с до3 Мбит/с (при использовании ADSL2+ Annex M)
• Возможность замены блока питания с 220 В переменного тока на 48 В постоянного тока

2. Безопасное и удобное управление
• Локальное RS-232 CLI и Ethernet SNMP/TELNET управление
• Удаленное встроенное SNMP/TELNET управление
• 2-уровня привилегии пользователя для управления
• SNMP версий: v1, v2c, v3
• Загрузка прошивки через TFTP
• Автоконфигурирование через TFTP

3.Спецификация ADSL части устройства:
•Соответствие стандартам :
ITU G.992.1 (G.DMT);G.DMT.bis;ITU G.992.2 (G.Lite);
ANSI T1.413 issue 2; ITU G.994.1 (G handshake) для ADSL,
G.992.3 для ADSL2 и G.992.5 для ADSL2+
• Поддержка расширений стандартов ADSL (Annex A,C,L,M), Annex B (**только для DAS-3224B/E**)
• Максимальная протяженность линии до 7 км (с использованием READSL2)
• Поддержка ATM OAM- I.610 (F5) Loopback test
• Расширенные возможности управления мощностью

4. Расширенные функции:
Функции физических интерфейсов
• Поддержка до 8 VC, 128 MAC адресов для каждого ADSL порта
• Поддержка 2K широковещательных MAC адресов на коммутатор DAS-3248
• Настраиваемый размер пакетов (от 64 до 1536)
• Поддержка функции Virtual Mac
• Поддержка DSL Bonding (ANSI T1.PP.427.01-2004)
Функции виртуальных сетей (VLAN)
• Поддержка Port-based VLAN и 802.1q VLAN (до 512 VLANs)
• Поддержка GVRP,GARP
• Поддержка стекирования VLAN (технология Q-in-Q)
• Поддержка Global VLAN (3-его уровня стекирования VLAN) в «прозрачном» режиме
Функции ATM инкапсуляций
• Поддержка RFC1483/2684 Bridged (EoA)
• Поддержка IPoA to IPoE Tunneling

• Поддержка PPPoA to PPPoE Internetworking
• Поддержка автоопределения (Autosensing) инкапсуляции ATM (PPPoA/EoA/IPoA)
• Поддержка автоопределения режима мультиплексирования ATM (LLC/VC mux)
• Поддержка VC Aggregation

Функции отказоустойчивости:

• Поддержка протокола Spanning Tree (802.1d)
• Поддержка Uplink Link Aggregation (Static и LACP (802.3ad))
• Поддержка Redundancy Aggregation (отказоустойчивого «избыточного» агрегирования)
• Поддержка StandBy режима для функции Redundancy Aggregation

Функции групповых сообщений:

• Поддержка IGMP v.1,v.2,v3

Функции безопасности:

• Поддержка фильтрации Ethernet, PPP, PPPoE, IP, TCP, UDP, IGMP, ICMP заголовков
• Поддержка списков управления доступом (ACL) по MAC (Per Port and Global) и IP адресам
• Поддержка управления качеством обслуживания Traffic prioritization (802.1 p)
• Поддержка ограничения скорости на ATM и Ethernet портах (IRL,ORL)
• Поддержка ограничения скорости по потокам (Flow Based Rate Limiting)

Прочие функции:

• Поддержка SNMP proxy

1.Начальная настройка DAS-3248

В данном разделе описывается подключение DAS-3248 и способы его конфигурирования.

Перед первым включением DAS-3248 убедитесь, что Вы выполнили все требования техники безопасности по установке устройства.

1.1.Обзор и внешний вид устройства

Базируясь на новейшей технологии ADSL2/2+, использование DAS-3248 поставщиками телекоммуникационных услуг позволяет получить эффективное по стоимости решение для быстрого развертывания различных коммуникационных сервисов в частных сетях и сетях общего пользования.
DAS-3248 является устройством типа IP DSLAM, который может сосредоточивать и управлять до 48 линий ADSL/ADSL2/2+. Управление DAS-3248 может производиться локально через интерфейс RS-232 или же удаленно по Telnet/SNMP.

Внешний вид DSLAM DAS-3248 показан на рисунке 1-1

Рисунок 1-1

DAS-3248 производится в двух модификациях:
DAS-3248 - имеет 2 1000baseT интерфейса и 100baseT для подключения к LAN сети
DAS-3248F – имеет 100baseT интерфейс,1000baseT интерфейс и 1000baseLX интерфейс (рассчитанный на подключение оптического одномодового кабеля, расстояние до 10км, разъем SC).

Внешние панели LAN модулей DAS-3248 и DAS-3248F изображены на рис. 1-2

LAN панели моделей DAS-3248	
	1*100BaseT-MGNT + 2*1000BaseT **Панель DAS-3248**
	1*100BaseT-MGNT+1*1000BaseT+ 1*1000LX **Панель DAS-3248F**

Рисунок 1-2

Назначение светодиодных индикаторов и органов управления на передней и задней панели на примере DAS-3248F показано на рисунках 1-3 и 1-4

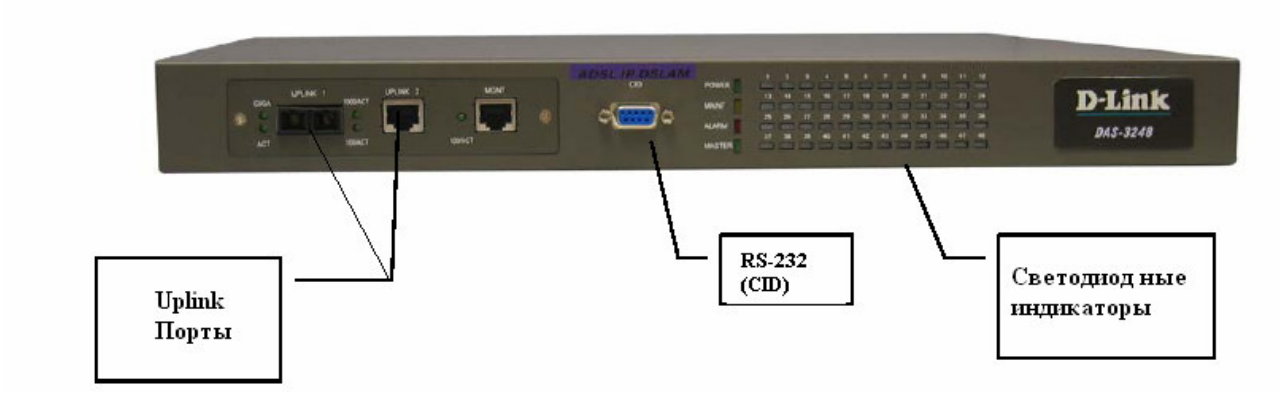


Рисунок 1-3

Рисунок 1-4

Как видно из рисунка 1-3 на передней панели имеются светодиодные индикаторы, показывающие текущее состояние системы и статус соединения, один модуль с тремя интерфейсами Ethernet 10/100 Мбит/с или 1 Гбит/с

Один из портов этого модуля выполняет назначение присоединения устройства к магистрали сети (Uplink), второй служит для стекирования с подобными себе устройствами (downlink) , третий служит для локального управления (MGNT).
Роль портов uplink и downlink могут быть изменены программно, поэтому для общности оба этих порта называют портами Uplink (Uplink1 и Uplink2).

Как видно из рисунка 1-4 на задней панели имеется разъем для подключения питания переменного тока 220 В.
Внимание: Данный блок питания может быть заменен на 48 В блок питания постоянного тока.
Замена блока питания производится только в условиях Сервис-Центра компании D-link.
Не пытайтесь самостоятельно заменить блок питания устройства. Обращайтесь в ближайшее региональное представительство компании D-Link по этому вопросу.

На задней панели имеются также одна (для DAS-3224) или две
пары(50-pin коннекторов Centronic для интерфейсов DSL и POTS (подключения телефонной сети)
Каждая пара интерфейсов предоставляет 24 порта с встроенным модулем сплиттера POTS ADSL/ADSL2/ADSL2+.
Цоколевка разъемов представлена в Приложении А настоящего руководства.

Обозначение состояний светодиодных индикаторов представлено на рисунке 1-5.

Рисунок 1-5

Индикатор	**Цвет**	**Цвет Описание**
POWER	Зеленый	Горит, когда питание включено
MAI NT	Желтый	Горит, когда заданы команды управления
ALARM	Красный	Горит в случае возникновения ошибки
MASTER	Красный	Горит, когда система работает, как мастер при объединении в стек (зарезервировано для будущих версий)
100/Act	Зеленый Мерцающий	Горит, когда подключен интерфейс Uplink Ethernet на скорости 100 Мбит/с Мерцает, когда производится передача через интерфейс
1000/Act	Зеленый Мерцающий	Горит, когда подключен интерфейс Uplink Ethernet на скорости 1000 Мбит/с Мерцает, когда производится передача через интерфейс
GIGA	Зеленый/Мерцающий	Мерцает, когда производится передача через интерфейс 1000LX
Act	Зеленый/Мерцающий	Горит, когда интерфейс

		1000LX активен
ADSL1 – ADSL48	Зеленый	Горит непрерывно, когда соединение ADSL активно
	Оранжевый	Горит в режиме установления соединения ADSL
	Красный	Горит, когда обнаружена потеря сигнала
	Серый (не горит)	Линия административно отключена

Примечание: Не отключайте питание, когда индикаторы "MAINT" и "ALARM" мигают одновременно.

1.2.Способы конфигурирования DAS-3248

Конфигурирование устройства можно производить двумя способами, через CLI или по протоколу SNMP.

- **CLI (Command Line Interface)** – интерфейс командной строки, базовый метод конфигурирования, использующий в своей основе набор текстовых команд.

Подключение к устройству необходимо производить через консольный порт RS-232 или через один из трех Ethernet портов. Для удаленного управления используется подключение по Telnet через сетевой канал связи.

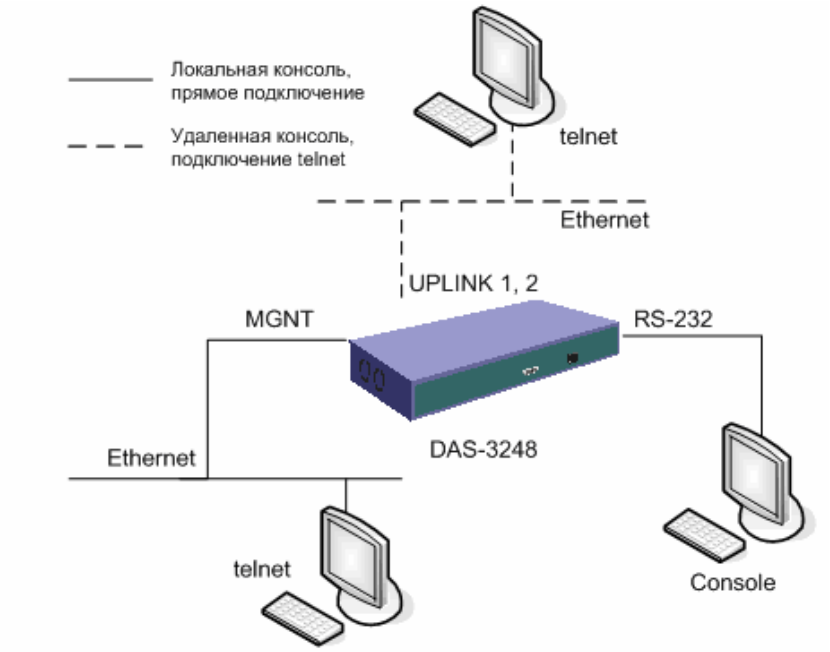


Рисунок 1-6

После первого включения устройства, по умолчанию, доступно три варианта подключения к CLI:

- консольный порт RS-232
- Gigabit Ethernet интерфейс UPLINK1 (eth-0)
- выделенный конфигурационный Fast Ethernet порт MGNT (eth-2)

<u>Важно:</u> При подключении через RS-232 используйте только тот кабель, который поставляется вместе с устройством.

После успешной загрузки устройства Вы увидите приглашение командной строки к вводу логина/пароля и версию программного обеспечения:

```
**********
Welcome to IP DSLAM
**********

Software Release: D.2.12.i1000.ADSL2+.A (COL2.10.2.0.051206) Date: Aug 24 2006
<CO-00179ADEBC9D>

login:
```

Настройки COM порта компьютера при подключении по RS-232 должны быть следующими:

Speed	9600 бит/с
Data bits	8
Parity	none
Stop bits	1
Flow control	none

Примечание: по умолчанию login: **Admin;** password**: Admin**

Для конфигурирования по Ethernet, необходимо подключить устройство в сеть через интерфейс UPLINK1 или MGNT кабелем, поставляемым в комплекте с устройством.

Структура CLI команды в общем виде:

<действие><группа><подгруппа><подгруппа второго уровня> <управляющее значение1>… <управляющееN значение N>

Пример: create bridge port intf portid 385 ifname eth-0 status enable

<действие>: указывает операцию, которая будет выполнена.
(“create”)
<группа>: указывает группу команд CLI, над которыми производится действие
(“bridge”)
<подгруппа>
(“port”)
<подгруппа второго уровня>
(“intf”)
<управляющее1 значение1>
(“portid 385”)
<управляющее2 значение2>
(“ifname eth-0”)
<управляющее3 значение3>
(“status enable”)

Примечание: Команда создает bridge port с номером интерфейса 385, именем eth-0 и устанавливает его в активное состояние.
Внимание: начиная с релиза 2.10 програмного обеспечения, в командном интерфейсе работает автодобавление комманд (по клавише Tab) .

1.3.Настройка параметров IP-интерфейса

В DAS-3248 используются три Ethernet интерфейса:

10/100/1000 BaseT/LX Uplink/Downlink interface	UPLINK1	eth-0
10/100/1000 BaseT Uplink/Downlink interface	UPLINK2	eth-1
1 x 100BaseT	MGNT	eth-2

1 x 100BaseT MGNT+
2 x 10/100/1000 BaseT/LX
Uplink/Downlink interface

Рисунок 1-7

- UPLINK1, UPLINK2 - рабочие интерфейсы, могут быть настроены как Uplink для подключения к сети, так и Downlink для стекирования.
- MGNT - конфигурационный порт для выделенного (out of band управления устройством).

Важно: По умолчанию сконфигурированы интерфейсы UPLINK1 (eth-0 ip 10.90.90.90, mask 255.255.255.0) и MGNT (eth-2 ip 10.90.91.91 mask 255.255.255.0). Для подключения убедитесь, что устройство и Ваш компьютер находятся в одной IP подсети.
Eth-1 сконфигурирован по умолчанию как downlink.
Примечание: Воспользуйтесь командой ping 10.xxx.xxx.xxx, чтобы проверить доступность устройства в сети Ethernet.

1.3.1.Настройка IP-адреса и маски подсети

Изменение IP адресов и маски подсети, производиться конфигурированием Ethernet интерфейсов DAS-3248. Ethernet интерфейсы являются частью взаимосвязанной логической структуры интерфейсов устройства.

Команды системы:

create ethernet intf

Описание: Создает ethernet интерфейс с заданными параметрами.

Синтаксис команды: create ethernet intf ifname interface-name [ip ip-address][mask net-mask][usedhcp true|false] [speed{auto|100BT|1000BT}] [type uplink|downlink][enable | disable][pkttype Mcast|Bcast|UnknownUcast|All|None] [orldecvalue][duplex half| full|auto][mgmtvlanid mgmtvlanid] [priority priority]

modify ethernet intf

Описание: Изменяет параметры заданного ethernet интерфейса.

Синтаксис команды: modify ethernet intf ifname interface-name [enable | disable][pkttype Mcast|Bcast|UnknownUcast|All|None] [ip ip-address][mask net-mask] [usedhcp true|false] [speed{auto|100BT|1000BT}] [orl decvalue] [duplex half|full|auto] [mgmtvlanid mgmtvlanid] [priority priority]

get ethernet intf

Описание: Получает информацию о заданном или о всех ethernet интерфейсах.

Синтаксис команды: get ethernet intf [ifname interface-name]

delete ethernet intf

Описание: Удаляет ethernet интерфейс с заданным именем.

Синтаксис команды: delete ethernet intf ifname interface-name

Таблица параметров:

ifname interface-name	Имя интерфейса для идентификации и обращения к нему. **Использование:** Create – Обязательно Delete – Обязательно Get – Опционально Modify – Обязательно **Принимает значения:** eth-0 ..2
ip ip-address	IP адрес взаимосвязан с маской сети, формируемой для интерфейса. Соединение с определенным IP адресом будет установлено, только если IP адрес определен или получен автоматически. Изменение маски сети для ethernet интерфейса поддерживается, только если IP адрес определен на данном интерфейсе или включена опция 'UseDhcp'. Использование UseDhcp и параметра ip-address одновременно недопустимо. **Использование:** Create - Опционально. Modify - Опционально **Принимает значения:** Любой IP адрес из принятых классов сетей A/B/C

	По умолчанию: для eth-0: 10.90.90.90; для eth-2 (MGNT): 10.90.91.91
mask net-mask	Сетевая маска ethernet интерфейса. Соединение с определенным IP адресом будет установлено, только если IP адрес определен или получен автоматически. Изменение маски сети для ethernet интерфейса поддерживается, только если IP адрес определен на данном интерфейсе или включена опция 'UseDhcp'. Использование UseDhcp и параметра ip-address одновременно недопустимо. **Использование:** Данный параметр не может быть установлен, если IP адрес интерфейса 0.0.0.0. Во всех других случаях данный параметр обязателен. **Принимает значения:** 255.0.0.0 - 255.255.255.255 **По умолчанию:** для eth-0: 255.255.255.0; для eth-2 (MGNT): 255.255.255.0
usedhcp true | false	Используется для получения IP адреса по протоколу DHCP для данного интерфейса. Одновременно использовать “usedhcp” и определенный вручную IP адрес невозможно. **Использование:** Опционально **Принимает значения:** true or false **По умолчанию:** false
speed {auto |100 BT| 1000BT}+	Параметр определяет скорость порта сетевого интерфейса. В “auto” скорость и режим соединения определяются автоматически по технологии автосогласования. **Использование:** Опционально. **Принимает значения:** auto, 100BT, 1000BT. **По умолчанию:** auto
type uplink|downink	Параметр определяет тип ethernet интерфейса. Физические интерфейсы Uplink типа используются для подключения к ethernet сети (максимально 2), а downlink интерфейсы к стекируемому устройству. Для Uplink интерфейсов, ip адрес не может быть не установлен, если usedhcp отключен. **Использование:** Опционально. **Принимает значения:** uplink, downlink. **По умолчанию:** uplink
enable|disable	Административный статус Ethernet интерфейса. **Использование:** Modify - Обязательно **Принимает значения:** enable or disable **По умолчанию:** enable
Duplex auto|half|full	Определяет режим работы порта. В “auto” определяется автоматически (дуплекс / полудуплекс). **Использование:** Опционально **Принимает значения:** auto, half, full **По умолчанию:** auto
Pkttype Mcast|Bcast|UnknownUcast | All|None	Определяет тип сетевых пакетов поддерживаемых интерфейсом. Параметр PktType поддерживается и может быть сконфигурирован для каждого из ethernet интерфейсов. По умолчанию, все сетевые пакеты буду

	переданы. Сконфигурированный интерфейс не будет передавать типы пакетов, не указанные в Pkttype. **Использование:** Create - Опционально Modify - Опционально **Принимает значения:** Mcast, Ucast, UnknownUcast, All **По умолчанию:** All
Orl decvalue	Данный параметр определяет output rate limiting. Значение определяется в Мбит/с. **Использование:** Create - Опционально Modify – Опционально **Принимает значения: любое** **По умолчанию:** 300
mgmtvlanid mgmtvlanid	VLAN для управляющего трафика на данном интерфейсе. Данный параметр может принимать ненулевое значение только, если на интерфейсе сконфигурирован ip адрес или включен клиент DHCP. Если управляющий Vlanid не определен (в «create» операции) или его значение установлено в ноль, система будет использовать значение 'portvlanid' ассоциированное с «bridge port» созданным для данного интерфейса. **Использование:** Create - Опционально Modify - Опционально **Принимает значения: любое из диапазона 1-4095**
priority priority	Задает значение 802.1p приоритета, который будет назначен всем пакетам, посылаемым через Mgmt VLAN на данном интерфейсе. Данный параметр доступен только в случае задания ip адреса на интерфейсе или включения опции UseDHCP. **Использование:** Create - Опционально Modify - Опционально **Принимает значения:** 0 -7

Изменение настроек UPLINK1 (eth-0):

	Команда	**Действие**
Шаг 1	$modify ethernet intf ifname eth-0 ip 192.168.0.50 mask 255.255.255.0	Изменить ethernet интерфейс на порту Uplink 1 (eth-0) с необходимым IP
Шаг 2	$get ethernet intf	Проверить настройки интерфейсов

Создание ethernet интерфейса UPLINK2 (eth-1):
Примечание: данный интерфейс создан в системе по умолчанию как downlink.

Внимание: в системе может быть создан только ОДИН интерфейс как uplink (второй обязательно должен быть downlink). Поэтому, чтобы создать eth-1 в системе как uplink, надо сначала удалить настройки обоих инетерфейсов и создать eth-0 как downlink (см.пример).
Примечание: Оба Uplink интерфейса могут быть использованы одновремено как Uplink только в случае агрегированного интерфейса.Читайте об использовании этой возможности в разделах 6.3 и 6.4

Пример переназначения функций Uplink интерфейсов.

	Команда	**Действие**
Шаг 1	$delete bridge port intf portid 385 $delete filter rule map ifname eth-0 stageid 1 ruleid 1 $delete ethernet intf ifname eth-0	Удалить интерфейс Eth-0
Шаг 2	$delete bridge port intf portid 386 $delete ethernet intf ifname eth-1	Удалить интерфейс Eth-1
Шаг 3	$create ethernet intf ifname eth-0 type downlink	Создать Ethernet интерфейс eth-1 как downlink
Шаг 4	$create bridge port intf portid 385 ifname eth-0 status enable	Создать bridge port 385 на интерфейсе eth-0
Шаг 5	$create ethernet intf ifname eth-1 ip 192.168.1.50 mask 255.255.255.0 enable	Создать второй ethernet интерфейс на порту Uplink 2 (eth-1)
Шаг 6	$create bridge port intf portid 386 ifname eth-1 learning disable status enable	Создать bridge port 386 на интерфейсе eth-1
Шаг 7	$get ethernet intf	Проверить настройки интерфейсов

Примечание: рекомендуем ознакомиться с описанием логической структуры интерфейсов DAS-3248 в приведенно в главе 2

1.3.2.Настройка управляющего VLAN (Management VLAN)

Управляющий VLAN используется для ограничения доступа к интерфейсу управления DAS-3248. После того, как будет задан идентификатор управляющего VLAN (VLANID), DAS-3248 будет принимать только те пакеты для управления, которые содержат 802.1q тег с тем же значением VLANID.

Значение идентификатора управляющего VLAN задается для Uplink интерфейса или, если используется Link Aggregation, для aggr интерфейса.

Команда	**Действие**
$ modify ethernet intf ifname eth-0 mgmtvlanid 1	Задать VLAN с идентификатором 1 в качестве управляющего для uplink интерфейса eth-0.
$ modify aggr intf ifname aggr-0 mgmtvlanid 1	Задать VLAN с идентификатором 1 в качестве управляющего для интерфейса агрегирования линков aggr-0.

1.3.3.Настройка выделенного MGNT порта

MGNT (Management Port) – выделенный конфигурационный порт, предназначенный для прямого подключения по Ethernet интерфейсу к терминалу управления системой.

Порт находится на передней панели DAS-3248, разъем типа RJ-45, подписан MGNT. Системное имя (ifname) данного интерфейса eth-2, по умолчанию интерфейс создан в системе и имеет IP адрес 10.90.91.91 с маской подсети 255.255.255.0.

Обычно, для дальнейшего конфигурирования системы необходимо изменить настройки данного порта в соответствии с адресным пространством Вашей сети. Для этого необходимо воспользоваться следующим набором команд:

Изменение настроек MGNT порта (eth-2):

	Команда	**Действие**
Шаг 1	$modify ethernet intf ifname eth-2 ip 10.91.92.91 mask 255.255.255.0	Изменить ip адрес ethernet интерфейса на порту MGNT (eth-2)
Шаг 2	$get ethernet intf ifname eth-2	Проверить настройки интерфейса

<u>Важно:</u> IP адрес MGNT порта, eth-2 интерфейса, должен быть из другой подсети, отличной от установленных на UPLINK1 (eth-0) и UPLINK2 (eth-1) портах.

<u>Экранный вывод:</u>

```
Set Done

Interface                : eth-2
Type                     : Uplink        UseDhcp     : False
IP Address               : 10.91.92.91    Mask       : 255.255.255.0
Pkt Type                 : ALL
Orl(mbps)                : 300
Configured Duplex        : Auto          Duplex      : None
Configured Speed         : Auto
ProfileName              : SPPROFILE
Mgmt VLAN Index          : -
Tagged Mgmt PDU Prio     : 0
trfclassprofileid        : 2
Ctl Pkts Instance Id     : 0
Speed                    : -
Operational Status       : Down          Admin Status : Up
```

1.4.Настройка синхронизации времени

SNTP (Simple Network Time Protocol, RFC-2030) – упрощенный протокол сетевого времени, широко используется для синхронизации часов в глобальной сети Интернет. Является упрощенной интерпретацией и модификацией протокола NTP (Network Time Protocol, RFC-1305).

SNTP может работать в юникастном (точка-точка), мультикастном (один передатчик - много приемников) или эникаст (несколько передатчиков - один приемник). Юникаст клиент посылает запросы специально выделенному серверу по его юникаст адресу и ожидает отклика, из которого он может определить время, а также сдвижку временной шкалы местных часов по отношению к шкале сервера. Мультикастный сервер периодически посылает сообщения по локальному мультикаст-адресу (IPv4 или IPv6). Мультикаст клиент воспринимает получаемые данные и не посылает никаких запросов. Эникастный клиент посылает запрос по локальному специально выделенному мультикастному (IPv4 или IPv6) адресу, при этом один или более эникастных серверов отправляют клиенту отклик. Клиент использует первый полученный отклик и устанавливает с соответствующим сервером связь в юникастном режиме. Последующие отклики от данного или других серверов игнорируются. Запросы номинально посылаются с интервалом от 64 до 1024 секунд, в зависимости от стабильности частоты клиента и от требуемой точности.

Мультикастные серверы должны реагировать на юникастные запросы клиентов, а также самостоятельно посылать мультикастные сообщения. Мультикастные клиенты могут посылать юникастные запросы, чтобы определить задержку распространения пакетов в сети между сервером и клиентом с тем, чтобы в дальнейшем продолжить работу в мультикастном режиме.

Юникастные клиенты должны быть снабжены именем сервера или его адресом. Если используется имя сервера, то необходим один или несколько адресов ближайших DNS-серверов. Мультикастные серверы и эникастные клиенты должны снабжаться значением TTL, а также местным широковещательным или групповым мультикастным адресом. Эникастные серверы и мультикастные клиенты могут конфигурироваться с привлечением списков пар адрес-маска. Это обеспечивает контроль доступа, так что операции будут производиться только с известными клиентами или серверами. Эти серверы и клиенты должны поддерживать протокол IGMP, а также знать местный широковещательный или групповой мультикастный адрес.

Команды системы:

modify sntp cfg

Описание: Изменить режим работы SNTP: (включить/выключить)
Синтаксис команды: modify sntp cfg [enable | disable]

get sntp stats

Описание: Получает информацию о текущих значениях счетчиков и параметров работы sntp

Синтаксис команды: get sntp stats

get sntp cfg

Описание: Получить информацию о режиме работы sntp
Синтаксис команды: get sntp cfg

Поля вывода команды:

Имя поля	Описание
Requests count	Число запросов посланных на SNTP сервер.
Responses count	Число подтвержденных запросов / ответов от SNTP сервера.
Invalid Responses count	Число ошибочных подтвержденных запросов / ответов от SNTP сервера.
Lost Responses count	Число запросов, на которые не было получено подтверждение за определенный лимит времени.
Last Time Stamp [MM/DD/ YYYY:HH:MM:SS]	Последнее установленное значение времени. Формат вывода: месяц/день/год: час, минута, секунда

reset sntp stats

Описание: Сбросить все счетчики параметров работы sntp.
Синтаксис команды: get sntp stats

create sntp servaddr

Описание: Получает информацию о текущих значениях работы sntp
Синтаксис команды: create sntp servaddr

get sntp servaddr

Описание: Получает информацию о текущих значениях работы sntp
Синтаксис команды: get sntp servaddr

Поля вывода команды:

Имя поля	Описание
Server Addr	IP адрес SNTP сервера
Status	Статус сервера: “Active”-используется / или в режиме «Standby» -не используется.

Настройка SNTP на заданный сервер:

	Команда	Действие
Шаг 1	$create sntp servaddr 172.23.3.45	Создать sntp подключение к серверу с заданным IP адресом.
Шаг 2	$modify sntp cfg enable	Включить использование SNTP
Шаг 3	$get sntp cfg	Проверить режим использования SNTP

<u>Важно:</u> Чтобы изменить IP адрес SNTP сервера, необходимо предварительно перевести настройку конфигурации SNTP в состояние "выключено" (Шаг 2 с параметром disable), после этого станет доступно создание нового IP адреса SNTP сервера. Для включения SNTP необходимо снова выполнить Шаг 2 с параметром enable.

Для проверки настроек работспособности SNTP:

	Команда	**Действие**
Шаг 1	$ get sntp stats	Получить информацию о работе SNTP

Установленное время и не нулевой показатель счетчика **Response count**, свидетельствуют о правильной работе SNTP.

<u>Экранный вывод:</u>

```
Requests count        : 162        Response count      : 4
Invalid Response count : 0         Lost Response count : 156
Last Time Stamp [MM/DD/YYYY::HH:MM:SS] : Thu Aug 18 11:51:02 2005
```

<u>Примечание:</u> В большинстве мест Интернет протокол гарантирует синхронизацию с точностью 1-50 мс, в зависимости от свойств источника синхронизации и сетевых задержек.

1.5.Настройка таблицы маршрутизации

Таблица маршрутизации в DAS-3248, представляет собой базу данных, в которой хранятся вся информация об ip маршрутах системы. Правильная настройка маршрутов в системе позволит организовать стабильную работу и исключить ошибки при передаче сетевых пакетов.
<u>Внимание:</u> Поскольку DAS-3248 является устройством второго уровня (ADSL коммутатором), маршрутизация не используется напрямую при пересылке пакетов от клиентских портов, а лишь для указания маршрутов к заданной подсети через Uplink порты, маршрута по умолчанию и для функции IPoA to IPoE Tunneling (эта функция рассматривает в главе 4 данного руководства).

<u>Команды системы:</u>

get ip route

Описание: Получить информацию о ip маршруте.
Синтаксис команды: get ip route [rid rid] [ip ip] [mask mask]

create ip route

Описание: Создать ip маршрут с заданными параметрами.
Синтаксис команды: create ip route [rid rid] ip ip mask mask gwyip gwyip [ifname ifname] [proxyarpstatus enable | disable]

delete ip route

Описание: Удалить ip маршрут.
Синтаксис команды: delete ip route [rid rid] ip ip mask mask

modify ip route

Описание: Изменить параметры заданного ip маршрута.
Синтаксис команды: modify ip route rid rid ip ip mask mask [ifname ifname] [proxyarpstatus enable | disable]

Таблица описания параметров команд:

Параметр	**Описание**
rid rid	Параметр RID задает идентификатор базы данных маршрутной информации (Routing Information Database). В данной базе содержится информация обо всех маршрутах в системе. Каждая RID идентифицирует поток данных и определяет для этого потока маршрутную информацию, базируясь на VLAN ID. Данная база данных может быть двух типов, IRD (Independent Routing Database) – независимая база данных маршрутной информации. В этом случае в системе присутствует более одной RID и каждая RID определяет различные маршруты. Если в системе созданы VLANID <X> и RID <X>, и база данных маршрутной информации сконфигурирована для IRD, то маршруты, содержащиеся в RID <X>, будут определять поток пакетов, следующий в VLAN <X>. Другой режим для данной базы данных называется SRD (Shared Routing Database) – разделяемая база данных. В этом случае в системе существует только одна RID, и все потоки описаны в ней. **Использование:** Create -- Опционально, Delete -- Обязательно Modify -- Обязательно Get -- Опционально
ip ip	IP адрес получателя, для данного маршрута. **Использование:** Create -- Обязательно Delete -- Обязательно Modify -- Обязательно Get -- Опционально **Принимает значения:** 0.0.0.0 - 223.255.255.0
mask mask	Устанавливает маску сети, логически используемую с адресом назначения, до сравнения её со значением поля ipRouteDest . Только абсолютные (от устройства в сеть)

	маршруты могут быть добавлены в нисходящем (downstream) направлении для IPOE интерфейсов. Маска для всех таких маршрутов должна быть 255.255.255.255. Маршрут по умолчанию в восходящее (upstream) направление, может иметь маску, только 0.0.0.0. **Использование:** Create -- Mandatory Delete -- Mandatory Modify -- Mandatory Get -- Optional **Принимает значения:** 0.0.0.0 - 255.255.255.0
gwyip gwyip	IP адрес следующего перехода для данного маршрута. Только абсолютные (от хоста в сеть) маршруты могут быть добавлены в нисходящем (downstream) направлении для IPOE интерфейсов. В таких случаях next hop должен быть IP адресом назначения. **Использование:** Create -- Mandatory **Принимает значения:** 0.0.0.0 - 223.255.255.0
ifname ifname	Индексное значение, которое однозначно идентифицирует локальный интерфейс, через который может быть достигнут следующий переход для данного маршрута. **Использование:** Create -- Optional Modify -- Optional
proxyarpstatus enable | disable	Указывает, должно ли выполняться Proxy ARP для данной записи таблицы маршрутизации. **Использование:** Create -- Optional Modify -- Optional **По умолчанию:** выключен

Создать маршрут по умолчанию:

	Команда	**Действие**
Шаг 1	$ create ip route ip 0.0.0.0 mask 0.0.0.0 gwyip 10.90.90.100	Создать маршрут по умолчанию, через шлюз с ip адресом 10.90.90.100
Шаг 2	$ get ip route	Проверить настройки таблицы маршрутизации

Экранный вывод:

Destination	Net Mask	Gateway	If-name	Route Type	Route Orig	Age(sec)
0.0.0.0	**0.0.0.0**	**10.90.90.100**	**eth-0**	**IND**	**LCL**	**0**
10.90.91.0	255.255.255.0	10.90.91.91	eth-2	DIR	DYI	0
10.90.91.91	255.255.255.255	127.0.0.1	lo-0	DIR	DYI	0
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	DIR	DYI	0

10.90.90.0	255.255.255.0	10.90.90.90	eth-0	DIR	DYI	0
10.90.90.90	255.255.255.255	127.0.0.1	lo-0	DIR	DYI	0

Примечание: созданный маршрут направляет все пакеты, для которых не найден маршрут, через шлюз 10.90.90.100, остальные маршруты для активных интерфейсов созданы системой динамически.

Создать маршрут к подсети:

	Команда	**Действие**
Шаг 1	$ create ip route ip 10.90.80.0 mask 255.255.255.0 gwyip 10.90.91.100	Создать маршрут к подсети 10.90.80.0, через шлюз с ip адресом 10.90.91.100
Шаг 2	$ get ip route	Проверить настройки таблицы маршрутизации

Экранный вывод:

	Destination	Net Mask	Gateway	If-name	Route Type	Route Orig	Age(sec)
→	**10.90.80.0**	**255.255.255.0**	**10.90.91.100**	**eth-2**	**IND**	**LCL**	**0**
	0.0.0.0	0.0.0.0	10.90.90.100	eth-0	IND	LCL	0
	10.90.91.0	255.255.255.0	10.90.91.91	eth-2	DIR	DYI	0
	10.90.91.91	255.255.255.255	127.0.0.1	lo-0	DIR	DYI	0
	127.0.0.0	255.0.0.0	127.0.0.1	lo-0	DIR	DYI	0
	10.90.90.0	255.255.255.0	10.90.90.90	eth-0	DIR	DYI	0
	10.90.90.90	255.255.255.255	127.0.0.1	lo-0	DIR	DYI	0

Примечание: созданный маршрут направляет все пакеты, адресованные в сеть 10.90.80.0/24 через шлюз 10.90.91.100

1.6.SNMP управление

Это раздел описывает протокол Simple Network Management Protocol (SNMP), SNMP MIB и его настройку на DSLAM

1.6.1.Обзор протокола SNMP

Понятие SNMP

SNMP (Simple Network Management Protocol, простой протокол сетевого управления) – это протокол уровня приложений, который упрощает обмен управляющей информацией между сетевыми устройствами. Протокол SNMP принадлежит стеку протоколов TCP/IP и используется для мониторинга и управления устройствами в сети.

В структуру SNMP входит три основных компонента:
• SNMP-менеджер
• SNMP-агент
• База управляющей информации MIB

SNMP-менеджер – это система, используемая для управления и наблюдения за устройствами с помощью протокола SNMP. В ней сосредоточена основная часть ресурсов обработки и хранения информации, требуемых для управления сетью

SNMP-агент – это программный модуль для управления сетью, который находится на управляемом устройстве. Агент обрабатывает данные устройства и отправляет локальную управляющую информацию в форме совместимой с SNMP управляющей системе.

База управляющей информации MIB (Management Information Base) – это виртуальное информационное хранилище сетевой управляющей информации. Доступ к базам MIB осуществляется посредством протокола управления сетью. Базы MIB состоят из управляемых объектов, обращение к которым происходит с помощью идентификаторов. Управляемый объект (иногда его называют MIB-модулем или просто MIB) – одна из нескольких характеристик управляемого устройства. Управляемые объекты состоят из одного или нескольких элементов, которые по существу являются переменными.

Протокол SNMP является простым протоколом типа «запрос - ответ». SNMP-менеджер выдает запросы, а SNMP-агент управляемого устройства отвечает на них. SNMP-менеджер может получать значения от агента или присваивать новые значения управляемому объекту агента используя операции Get или Set.

Рисунок ниже показывает процесс обмена информацией между SNMP-менеджером и клиентом. Менеджер может отправлять агенту запросы на получение или присвоение новых значений MIB. Агент может отвечать на эти запросы. Независимо от этих операций, агент может отправлять менеджеру сообщения для асинхронного оповещения его о каком-либо важном сетевом событии (операция Trap).

Рисунок 1-8. Процесс обмена информацией между SNMP-менеджером и клиентом

Оповещения SNMP

Одной из важных характеристик SNMP является возможность генерирования SNMP-агентом оповещений. Эти оповещения не требуют наличия запроса от менеджера SNMP. Асинхронные оповещения могут генерироваться как запросы *traps* или *inform*. Trap – это сообщение, предупреждающее SNMP-менеджера о важном сетевом событии. Inform – это оповещающее сообщение (trap), требующее от SNMP-менеджера подтверждения прочтения. Оповещения могут уведомлять о неправильной аутентификации пользователя, перезагрузке, потере соединения, потере соединения с соседним DSLAM или о других важных событиях.

Trap менее надежны, чем сообщения Inform, т.к. не требуют подтверждения их получения. Отправитель не сможет определить, был ли получен его Trap. SNMP-менеджер, который получает сообщение Inform, отправляет подтверждение в виде SNMP-ответа. Если отправитель не получил этот ответ, он повторно выполняет операцию Inform. Таким образом, сообщение Inform с большей вероятностью достигнет его предполагаемого получателя. Однако Trap более предпочтительны, чем Inform, т.к. используют меньше ресурсов DSLAM и сети.

Версии SNMP

Операционная система D-Link DSLAM поддерживает следующие версии SNMP:

- SNMPv1— Simple Network Management Protocol: первая реализация протокола, описанная в RFC 1157. Безопасность основана на community string.
- SNMPv2c—Административная структура для SNMPv2 на основе community string. SNMPv2c (“c” - обозначает «community») – экспериментальный протокол Интернет, определенный в RFC 1901, RFC 1905, и RFC 1906. SNMPv2c содержит дополнение к протоколу и типам данных, определенным ранее в SNMPv2p (SNMPv2 Classic), и использует модель безопасности на основе community string из первой версии SNMPv1.
- SNMPv3—3 версия протокола SNMP. SNMPv3 определен в RFC с 2273 по 2275. SNMPv3 обеспечивает безопасный доступ к устройствам, объединяя аутентификацию и шифрование, передаваемых через сеть пакетов.

Протокол SNMPv3 предоставляет следующие функции безопасности:

- Целостность сообщений (Message integrity)— для гарантии, что пакеты, не были испорчены в процессе передачи.
- Аутентификация (Authentication)—для определения, что сообщение получено из надежного источника.
- Шифрование (Encryption)—скремблирование содержимого пакета для предотвращения его изучения неавторизованным источником.

Оба протокола SNMPv1 и SNMPv2c используют безопасность на основе community (сообщества). Сообщество пользователей, которое может получить доступ к агенту MIB, определяется с помощью списков IP-адресов и по паролю.

В протокол SNMPv2c добавлена поддержка механизма получения больших блоков данных (bulk retrieval mechanism) и более подробных отчетов об ошибках, отправляемых управляющим станциям. Механизм получения больших блоков данных поддерживает передачу больших таблиц и информации большого объема за один запрос, уменьшая количество требуемых SNMP-запросов и ответов. В протоколе SNMPv2c улучшена обработка ошибок благодаря поддержке расширенных кодов, которые характеризуют различные виды условий возникновения ошибок. В SNMPv1 используется единственный код ошибки. Ошибка возвращает коды, которые сообщают о типе ошибки. Также сообщается о трех видах исключений: no such object (такой объект не существует), no such instance (такого экземпляра не существует) и end of MIB view (конец просмотра MIB).

Протокол SNMPv3 обеспечивает модели безопасности (security model) и уровни безопасности (security level). Модель безопасности – это стратегия аутентификации, которая устанавливается для пользователя и группы, в которой он находится. Уровень безопасности – это позволенный уровень безопасности внутри модели безопасности. Комбинация модели и уровня безопасности будет определять, какой механизм безопасности будет использоваться при обработке пакетов SNMP.

Сейчас доступны три модели безопасности: SNMPv1, SNMPv2c, и SNMPv3. В таблице, приведенной ниже, представлены комбинации моделей и уровней безопасности.

MIB библиотека функций SNMP доступна на сайте компании D-Link: ftp.dlink.ru

Настройка некоторых функций DSLAMa посредством SNMP запроса приведены в Приложении D настоящего руководства.

Таблица 1-1. Модели и уровни безопасности SNMP

Модель	Уровень	Аутентификация	Шифрование	Описание
v1	noAuthNoPriv	Community String	Нет	Для аутентификации используется совпадение Community String
v2c	noAuthNoPriv	Community String	Нет	Для аутентификации используется совпадение Community String
v3	noAuthNoPriv	Username	Нет	Для аутентификации используется совпадение имени пользователя
v3	authNoPriv	MD5 или SHA	Нет	Обеспечивает аутентификацию на основе протоколов HMAC-MD5 или HMAC-SHA
v3	authPriv	MD5 или SHA	DES	Обеспечивает аутентификацию на основе протоколов HMAC-MD5 или HMAC-SHA. Обеспечивает шифрование 56-бит DES дополнительно к аутентификации на основе

				стандарта CBC-DES (DES-56)

1.6.2.Настройка SNMP

- Создание, изменение, удаление community string
- Создание, изменение, удаление snmp host
- Создание, изменение, удаление snmp trap host
- Настройка snmp proxy
- Команды включения/отключения SNMP Traps

Создание, изменение, удаление community string

SNMP community string служит для определения отношений между SNMP-менеджером и агентом. Community string действует как пароль для управления доступом к SNMP-агенту DSLAM.

Команда **create snmp comm**

Описание: эта команда используется для создания community string.

Синтаксис команды
create snmp comm community community [access ro | rw]

Команда **get snmp comm**

Описание: эта команда используется для получения значения community string.

Синтаксис команды
get snmp comm [community community]

Команда **delete snmp comm.**

Описание: эта команда используется для удаления community string.

Синтаксис команды
delete snmp comm community community

Параметры:

Имя	Описание
community community	Определяет имя Community. **Тип:** Create -- обязательно Delete -- обязательно Get -- опционально
access ro | rw	Определяет права доступа, предоставляемые пользователям с этим именем community. ro – подразумевает права Read Only (только

	чтение), rw –подразумевает права Read-Write (чтение-запись). **Тип:** Create -- опционально **Значение по умолчанию:** ro

Пример**:** *$ create snmp comm community public*

Вывод
Verbose Mode On

Entry Created

Access community

---

ro public

Verbose Mode Off:

Entry Created

Описание полей вывода:

Имя	Описание
community community	Определяет имя Community.
Access	Определяет права доступа, предоставленные пользователям с этим именем community. ro – подразумевает права Read Only (только чтение), rw –подразумевает права Read-Write (чтение-запись).

Создание, изменение, удаление snmp host

Эта команда определяет управляющую станцию.

Команда **create snmp host**

Описание: эта команда используется для создания управляющего сетевого узла.

Синтаксис команды
create snmp host ip ip community community

Команда **get snmp host**

Описание: эта команда используется для получения информации об управляющем сетевом узле.

Синтаксис команды
get snmp host [ip ip] [community community]

Команда **delete snmp host**

Описание: эта команда используется для удаления управляющего сетевого узла.

Синтаксис команды
delete snmp host ip ip community community

Параметры:

Имя	Описание
ip ip	Определяет IP-адрес компьютера пользователя, который имеет права доступа. **Тип:** Create -- обязательно Delete -- обязательно Get – опционально
community community	Определяет имя Community. Эта Community должна существовать в таблице snmp community. **Тип:** Create -- обязательно Delete -- обязательно Get – опционально

Пример *$ create snmp host ip 172.25.34.34 community public*

Вывод
Verbose Mode On

Entry Created

Ip Address Community

172.25.34.34 public

Verbose Mode Off:

Entry Created

Описание полей вывода

Имя	Описание
ip ip	Определяет IP-адрес компьютера пользователя, который имеет права доступа.
community community	Определяет имя Community. Это имя должна существовать в таблице snmp community.

Создание, изменение, удаление snmp trap host
Эта команда определяет станцию-получателя оповещений trap.

Команда **create snmp traphost**

Описание: эта команда используется для создания станции-получателя оповещений trap.

Синтаксис команды
create snmp traphost ip ip community community [port port][version v1 | v2c]

Команда **get snmp traphost**

Описание: эта команда используется для получения данных о станции-получателе оповещений trap.

Синтаксис команды
get snmp traphost [ip ip] [port port]

Команда **delete snmp traphost**

Описание: эта команда используется для удаления станции-получателя оповещений trap.

Синтаксис команды
delete snmp traphost ip ip [port port]

Команда **modify snmp traphost**

Описание: эта команда используется для изменения станции-получателя оповещений trap.

Синтаксис команды
modify snmp traphost ip ip [port port] [version v1 | v2c]

Параметры

Имя	Описание
port port	Определяет порт, на который будут отправляться trap. **Тип:** Create – опционально Get – опционально Modify - опционально Delete – опционально **Значение по умолчанию**: 162
version v1 | v2c	Определяет версию trap, которая будет отправлена менеджеру. **Тип:** Create – опционально Get – опционально Modify - опционально **Значение по умолчанию**: v2c

Пример *$ create snmp traphost ip 172.25.34.34 community public*
Вывод
Verbose Mode On

Entry Created

Ip Address : 172.25.34.34

Community : public

Port : 162 Version : v2c

Verbose Mode Off:

Entry Created

Описание полей вывода

Имя	Описание
Ip Address	Определяет IP-адрес менеджера, на который отправляются trap.
Community	Определяет имя Community, используемое в trap.
Port	Определяет порт, на который отправляются trap.
Version	Определяет версию trap, которая отправляется менеджеру.

Настройка snmp proxy

Snmp прокси используется для получения сообщений протокола SNMP от агентов (обычно CPE устройств) и проксирования их на управляющую EMS станцию.

Команда **get snmp proxy host**

Описание: эта команда используется для получения данных о прокси-агенте.

Синтаксис команды
get snmp proxy host [ip ip *] [netcomm* netcomm *]*

Команда **create snmp proxy host**

Описание: эта команда используется для создания прокси-агента.

Синтаксис команды
create snmp proxy host ip ip *netcomm* netcomm *[hostport* hostport *]*

Команда **delete snmp proxy host**

Описание: эта команда используется для удаления прокси-агента.

Синтаксис команды
delete snmp proxy host ip ip *netcomm* netcomm

Команда **modify snmp proxy host**

Описание: эта команда используется для изменения прокси-агента.

Синтаксис команды
modify snmp proxy host ip ip *netcomm* netcomm *[hostport* hostport *]*

Параметры

Имя	Описание
ip ip	Определяет IP-адрес пользователя, который имеет права доступа для CPE для Community, определенной 'NetCommunity'. **Тип:** Create – обязательно Modify - обязательно Delete – обязательно Get – опционально

netcomm netcomm	Определяет Community со стороны сети « NET side ». Community настроенной для прокси-сервисов будет предоставлен наивысший уровень привилегий по сравнению с SNMP-агентом, т.е. если одна и та же community настроена в таблице SNMP Host и таблице Snmp Proxy, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться. **Тип:** Create – обязательно Modify - обязательно Delete – обязательно Get – опционально
hostport hostport	Определяет порт UDP менеджера, через который с помощью SNMP Proxy будут передаваться trap. Для запросов и ответов SNMP это поле не используется. **Тип:** Create – опционально Modify – опционально **Значение по умолчанию:** 162

Пример *$ create snmp proxy host ip* 172.25.2.100 *netcomm* Adsl1 *hostport* 1

Вывод
Verbose Mode On

Entry Created

Ip Address : 172.25.2.100

NET Community : Adsl1

Host Port : 1

Verbose Mode Off:

Entry Created

Описание полей вывода

Имя	Описание
ip Address	Определяет IP-адрес пользователя, который имеет права доступа для CPE для Community, определенной 'NetCommunity'.
NET Community	Определяет Community со стороны сети « NET side ». Community настроенной для прокси-сервисов будет предоставлен наивысший уровень привилегий по сравнению с SNMP-агентом, т.е. если одна и та же community настроена в таблице SNMP Host и таблице Snmp Proxy, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться.
Host Port	Определяет порт UDP менеджера, через который с помощью SNMP Proxy передаются trap. Для запросов и ответов SNMP это поле не используется.

Команда **get snmp proxy comm**

Описание: эта команда используется для получения данных о прокси-агенте

Синтаксис команды
get snmp proxy comm [netcomm netcomm *]*

Команда **create snmp proxy comm.**

Описание: эта команда используется для создания community strring прокси-агента

Синтаксис команды
create snmp proxy comm netcomm netcomm *cpecomm* cpecomm *lowif* lowif

Команда **delete snmp proxy comm**

Description Описание: эта команда используется для удаления community strring прокси-агента

Синтаксис команды
delete snmp proxy comm netcomm netcomm

Команда **modify snmp proxy comm**

Описание: эта команда используется для изменения community strring прокси-агента

Синтаксис команды
modify snmp proxy comm netcomm netcomm *[cpecomm* cpecomm *]*
Параметры

Имя	Описание
netcomm netcomm	Определяет Community со стороны сети « NET side ». Community настроенной для прокси-сервисов будет предоставлен наивысший уровень привилегий по сравнению с SNMP-агентом, т.е. если одна и та же community настроена в таблице SNMP Host и таблице Snmp Proxy, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться. **Тип:** Create – обязательно Modify - обязательно Delete – обязательно Get – опционально
cpecomm cpecomm	Определяет Community со стороны CPE «CPE side». Если пакет SNMP принимается через порт UDP, предназначенный для любого CPE, подключенного через канал DSL, community встроенная в запрос должна быть заменена на community со стороны CPE. **Тип:** Create – обязательно Modify – опционально
lowif lowif	Определяет самое наименьшее имя интерфейса, через

	который пакет, полученный с community 'NetCommunity' будет передан на сторону CPE. . **Тип:** Create – обязательно **Используемые значения:** 1 - IAD_MAX_INTERFACES

Пример *$ create snmp proxy comm netcomm* Adsl1 *cpecomm* Adsl *lowif* aal5-0

Вывод
Verbose Mode On

Entry Created

NET Community : Adsl1

CPE Community : Adsl

LowIfName : aal5-0

Verbose Mode Off:

Entry Created

Описание полей вывода

Имя	Описание
NET Community	Определяет Community со стороны сети « NET side ». Community настроенной для прокси-сервисов будет предоставлен наивысший уровень привилегий по сравнению с SNMP-агентом, т.е. если одна и та же community настроена в таблице SNMP Host и таблице Snmp Proxy, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться.
CPE Community	Определяет Community со стороны CPE «CPE side». Если пакет SNMP принимается через порт UDP, предназначенный для любого CPE, подключенного через канал DSL, community встроенная в запрос должна быть заменена на community со стороны CPE.
LowIfName	Определяет самое наименьшее имя интерфейса, через который пакет, полученный с community 'NetCommunity' будет передан на сторону CPE. .

Команда **get snmp proxy cfg**

Описание: эта команда используется для получения данных о состоянии функции SNMP Proxy

Синтаксис команды
get snmp proxy cfg

Команда **modify snmp proxy cfg**

Описание: эта команда используется для изменения состояния функции SNMP Proxy .

Синтаксис команды
modify snmp proxy cfg [status disable | enable *]*

Параметры

Имя	Описание
status disable	enable	Установка значения 'enable' для этого объекта активизирует функцию SNMP Proxy. **Тип:** Modify – опционально

Пример *$ get snmp proxy cfg*

Вывод
status : disable

Команды включения/отключения SNMP Traps
modify interface config ifname ifname **[trap** enable|disable**]**- предупреждения о изменении статуса интерфейсов (Up/Down). В роле ifname могут выступать интерфейсы : eth-*,atm-*,aal5-*, eoa-*, dsl-*, dslf-*, dsli-*, aggr-*.
modify snmp stats authentraps enable | disable **–** предупреждения о попытках неавторизованной идентификации по SNMP.

modify bridge tbg traps bindingstatus [enable | disable]- предупреждения связанные с подключение пользователя к другому порту, нежели к тому котрому он привязан (см. дальше режим Sticky). По умолчанию disabled.

modify bridge tbg traps dbtrapstatus [enable | disable **]-** предупреждения, посылаемые при изменении таблицы коммутации устройства (добавление, удаление или устаревание MAC адреса). По умолчанию disabled.

1.6.3. Remote Monitoring (RMON)

RMON (Remote Monitoring, удаленный мониторинг) является спецификацией стандартных средств мониторинга, которая определяет набор статистических характеристик и функций, обеспечивающих администраторов сети комплексной информацией по диагностике неисправностей, планированию и настройке производительности сети.

RMON, используемый совместно с SNMP-агентом на DSLAM позволяет
- просматривать трафик, проходящий через DSLAM
- просматривать трафик сегмента сети, не обязательно предназначенного для DSLAM

Комбинирование предупреждений и событий RMON с существующими MIB позволяет определить область мониторинга. RMON может требовать много процессорного времени, поэтому при его использовании необходимо убедиться, что производительность DSLAM не снизится.

RMON поставляет информацию в девять групп элементов мониторинга RMON, каждая из которых поддерживает отдельный набор данных, удовлетворяющих общим требованиям конфигурирования сети.

DSLAM DAS-3248 использует группу RMON Statistics.

Группа RMON Statistics: эта группа содержит статистические данные, измеренные датчиком на каждом интерфейсе устройства, для которого производится мониторинг.

Элементы группы: отброшенные пакеты, отправленные пакеты, отправленные байты (октеты), широковещательные пакеты, многоадресные пакеты, ошибки CRC, карликовые (runt) и гигантские (giants) пакеты, фрагменты, «мусор», коллизии и счетчики пакетов размером 64-128, 128-256, 256-512, 512-1024 и 1024-1518 байт.

Команды группы RMON Statistics

Команда **create srmon probe**

Описание: эта команда используется для создания зонда RMON (RMON probe).

Синтаксис команды
create srmon probe rindex rindex ifname interface-name owner owner-string

Команда **delete srmon probe**

Описание: эта команда используется для удаления зонда RMON.

Синтаксис команды
delete srmon probe rindex rindex

Команда **get srmon probe**

Описание: эта команда используется для получения информации и статистики.

Синтаксис команды
get srmon probe [rindex rindex]

Параметры

Имя	Описание
rindex rindex	Уникальный идентификатор зонда. **Тип**: Create – обязательно Delete – обязательно Get - опционально **Используемые значения**: *0-20*
Ifname interface-name	Указывает имя интерфейса. **Тип**: Create – обязательно **Используемые значения**: *eoa-0 - *, eth-0-**
Owner owner-string	Сущность, которая сконфигурировала этот зонд и поэтому использующая его ресурсы**.**

	Тип: Create – обязательно **Используемые значения**: Строка из максимум 64 ASCII символов.

Пример *$ get srmon probe rindex 1*
Вывод
Verbose Mode On

RMON Probe Index : 1

If-Name : eth-0 Stats Owner : GlobespanVirata

Total Octets : 800 Total Packets : 200

Total Broadcast Packets : 138 Total Multicast Packets : 200

Total 64 Octets : 100 Total 65-127 Octets : 200

Total 128-255 Octets : 200 Total 256-511 Octets : 300

Total 512-1023 Octets : 50 Total 1024-1518 Octets : 100

Описание полей вывода

Имя	Описание
RMON Probe Index	Уникальный идентификатор зонда.
Ifname	Указывает имя интерфейса. Оно может быть *eoa-0 - *, eth-0-**
Stats Owner	Сущность, которая сконфигурировала этот зонд и поэтому использующая его ресурсы**.**
Total Octets	Общее количество октетов данных (включая «плохие» пакеты), полученных сетью (за исключением битов синхронизации, но включая октеты FCS).
Total Packets	Общее количество полученных пакетов (включая «плохие», широковещательные и многоадресные пакеты).
Total Broadcast Packets	Общее количество полученных хороших широковещательных пакетов.
Total Multicast Packets	Общее количество полученных хороших многоадресных пакетов.
Total 64 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 64 октета (за исключением битов синхронизации, но включая октеты FCS).
Total 65-127 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 65-127 октетов (за исключением битов синхронизации, но включая октеты FCS).
Total 128-255 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 128-255 октетов (за исключением битов синхронизации, но включая октеты FCS).
Total 256-511 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 256-511 октетов (за исключением битов синхронизации, но включая октеты

	FCS).
Total 512-1023 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 512-1023 октетов (за исключением битов синхронизации, но включая октеты FCS).
Total 1024-1518 Octets	Общее количество полученных пакетов (включая «плохие» пакеты) размером 1024-1518 октетов (за исключением битов синхронизации, но включая октеты FCS).

1.7.Сохранение конфигурации

1.7.1.Виды конфигурационных файлов.

Как и любое активное сетевое устройство DAS-3248 имеет оперативную и энергонезависимую память (NVRAM).
Все изменения настроек интерфейсов и параметров системы произведенные с помощью консольных команд первоначально сохраняются только в оперативной памяти (и поэтому действительны только до следующей аппаратной или программной перезагрузки устройства).
Для постоянного применения необходимо сохранение изменений в энергонезависимой памяти устройства.

Такую функцию выполняет консольная команда **commit.**

Для увеличения отказоустойчивости и управляемости устройство хранит две конфигурации, и производит их замену путем ротации. Т.е. после первого применения команды commit устройство запоминает конфигурацию в бинарном файле **primcfg**. После второго применения commit устройство запоминает последнюю конфигурацию в файле primcfg , а файл primcfg переименовывает в **seccfg**.
При следующем сохранении конфигурации новые изменения перезаписываются в primcfg, а primcfg в seccfg, затирая таким образом наиболее старые изменения, хранившиеся в seccfg. Такая структура сохранения изменений дает возможность отката устройства к предыдущим изменениям или хранения двух разных конфигураций, между которыми возможно переключение консольными командами:
reboot config last – для загрузки primcfg
reboot config backup –для загрузки seccfg

1.7.2.Сохранение конфигурационных файлов на tftp сервере

Конфигурации устройства primcfg и secccfg могут быть выгружены на удаленный tftp сервер для резервного хранения.
Внимание: конфигурации хранятся в бинарном (двоичном) виде и выгружаются на tftp сервер в точно таком же виде.

Примечание:
Однако это не означает, что вы можете работать только с двоичными конфигурациями. В устройстве имеется возможность загрузки наряду с двоичными текстовых кофигураций. Процесс загрузки текстовых конфигураций, наряду с процессом обновления внутреннего программного обеспечения будет более подробно рассмотрен в главе 2.

Для сохранения конфигураций с устройства на tftp сервер используется консольная команда **upload**, для загрузки с конфигурации на tftp сервер используется команда **download**
(При этом tftp сервер должен быть запущен и доступен к моменту введения консольных команд).

Синтаксис команды для случая сохранения конфигураций на tftp:

Для последней конфигурации:
upload src /nvram/system/**primcfg dest** [имя файла кофигурации] **ip** [ip адрес tftp/tfp сервера] mode ftp/tftp

Для резервной конфигурации:
upload src /nvram/system/**seccfg dest** [имя файла конфигурации] **ip** [ip адрес tftp/tfp сервера] mode ftp/tftp

Пример:
upload src /nvram/system/primcfg dest myconfig.cfg ip 198.168.1.1

Синтаксис команды для случая загрузки конфигурации на tftp/ftp на устройство:

Для последней конфигурации:
download src <filename> dest /nvram/system/**primcfg ip** <ipaddress> [mode tftp]

Для резервной конфигурации:
download src <filename> dest /nvram/system/seccfg ip <ipaddress> [mode tftp]

Пример:
download src myconfig.cfg dest /nvram/system/primcfg ip 198.168.1.1

1.8.Вспомогательные команды CLI интерфейса.

help ? Вывод встроенной помощи (алфавитного списка команд). Также можно поступать и при выводе подкоманд (например, delete ?)

Commit
сохранение изменений конфигурации в энергонезависимой памяти

Verbose [on | off **]**
Включение или выключение режима вывода статуса объекта до и после ввода консольной команды (при отключенном режиме выводится только результат команды, то есть сообщение об успешном или неуспешном ее выполнении)

Ping <ip-address> [-s <decvalue>] [-w <decvalue>] [-t | -n <decvalue>] [-i <decvalue>]
Эхо-запрос (ICMP Echo) к заданному сетевому узлу,
где
-s размер пакетов;
-w время ожидания в секундах;
-tl n количество проб (-t бесконечное количество)
-i TTL (время жизни пакета)

traceroute {<ip-address> | dname <domain>} {ping | udp} [-m num-of-hops] [-w waittime]

[-p udp-port-number] [-q num-of-probes]

Сетевой маршрут к заданному сетевому узлу,
где ping **|** udp – типа запроса (по ICMP или UDP протоколу);
-m количество промежуточных пунктов;
-w время ожидания;
-p номер UDP порта, по которому производится запрос;
-q количество проб.

Пример: **$ traceroute 192.168.1.13 ping**
Tracing route to [192.168.1.13]
Over a maximum of 30 hops
1 0.000000 ms 0.000000 ms 0.000000 ms 192.168.1.13
Trace complete.

passwd [name]
Изменение пароля текущего пользователя

create user name user-name **passwd** password **[**root **|** user**]**
Создание нового пользователя в системе или изменение параметров существующего (например, смена пароля)
Имя и пароль пользователя могут быть длиной до 64 символов (допускаются буквы, цифры, и символ нижнего подчеркивания «_»)
Пользователь с правами root имеет полный доступ к командам системы, пользователь с правами user только на просмотр (get).

delete user
Удаление пользователя из системы

logout | quit | exit
Выхода из CLI режима

Promt prompt
Изменение системного приглашение командного режима на пользовательское приглашение

2.Логическая структура DAS-3248

2.1.Структура стека интерфейсов DAS-3248

Логические интерфейсы в DAS-3248 отражают стек преобразований, производимый над потоком данных. Подробнее сущность преобразований и команды операций с каждым из типов интерфейсов будут рассмотрены в последующих главах.

Схема организации логических интерфейсов DAS-3248 схематично представлена на рисунке 2-1:

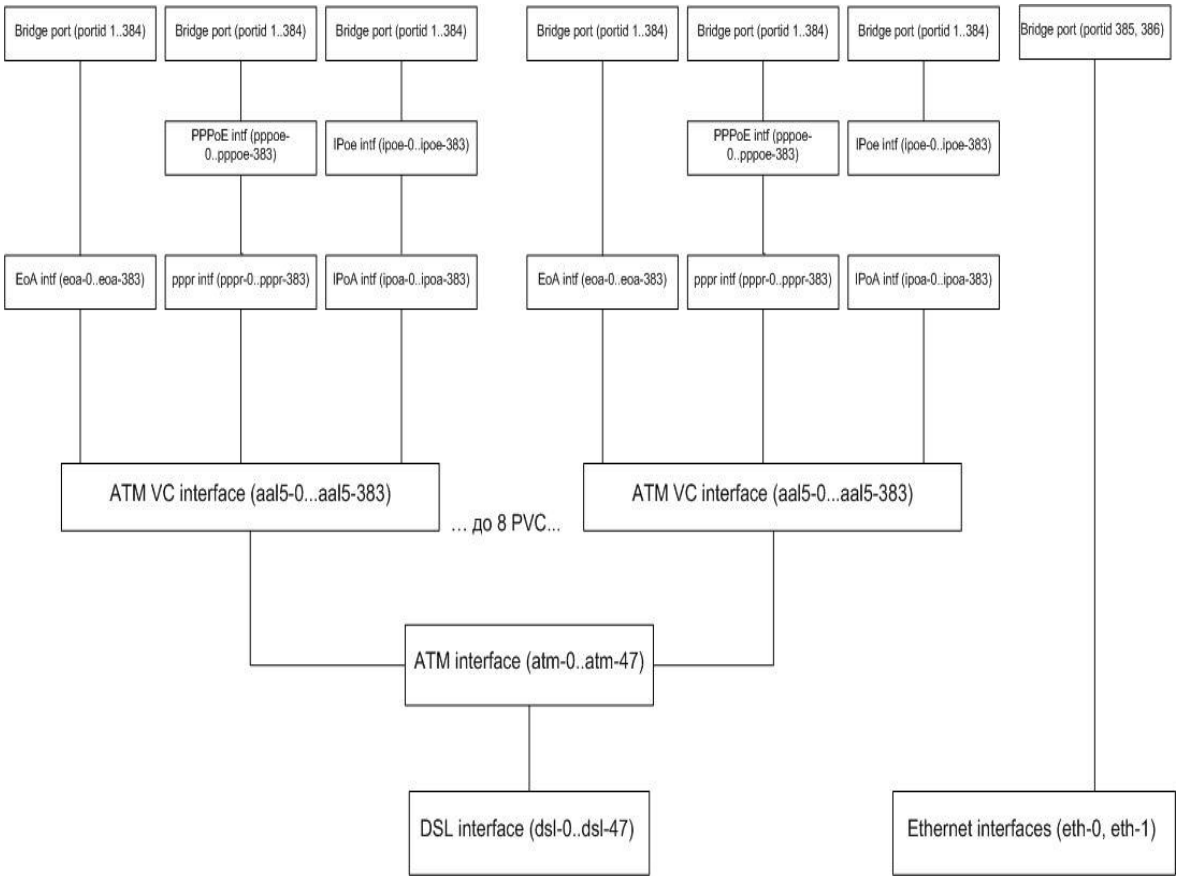


Рисунок 2-1.Логическая структура интерфейсов DAS-3248

Рассмотрим стек интерфейсов, созданный по умолчанию, для 1-го ADSL порта:

Bridge port	portid 1
EoA intf	eoa-0
ATM VC intf	aal5-0
ATM Port intf	atm-0
ADSL intf	dsl-0

Ниже будет дана краткая характеристика каждого типа интерфейсов данного стека.

Интерфейсы DSL

Служат для непосредственного управления соответствующими ADSL портами DAS-3248. Названия dsl интерфейсов лежат в диапазоне dsl-0...dsl-47. Интерфейс dsl-0 соответствует 1-ому ADSL порту, dsl-47 – сорок восьмому. DSL интерфейсы являются нижележащими интерфейсами для ATM портов. По умолчанию в DAS-3248 созданы все DSL интерфейсы.

Интерфейсы ATM (ATM порты)

Используются для управления ATM функционалом DAS-3248. Названия ATM интерфейсов лежат в диапазоне atm-0...atm-47. Интерфейс atm-0 соответствует 1-ому ADSL порту, atm-47 – сорок восьмому. ATM интерфейсы являются вышележащими над DSL интерфейсами и нижележащими для ATM VC интерфейсов.
На уровне ATM портов выполняются следующие действия:

1. Output rate limiting (ORL) – задание максимальной выходной полосы пропускания для данного ATM порта (в Кбит/с). Данное значение не должно превышать максимальную скорость соединения нижележащего ADSL порта.
2. OAM (ATM Loopback)
3. Настройка входящих очередей (через trfclass profile):
    a. Длина входной очереди.
    b. Размер очереди, при которой применяется IRL (Input rate limiting).
4. Настройка политик исходящих очередей (через sched profile)
    a. Дисциплина очередей.
    b. Параметры выбранной дисциплины.

По умолчанию в DAS-3248 созданы все ATM интерфейсы (порты).

Интерфейсы ATM VC

ATM VC интерфейсы предназначены для создания, настройки и удаления постоянных виртуальных соединений (PVC) ATM. DAS-3248 поддерживает до 8 ATM PVC на один ADSL порт, т.е. поверх одного ATM порта можно создать до 8 PVC. Названия ATM VC интерфейсов лежат в диапазоне aal5-0...aal5-383.
По умолчанию на DSLAM-е созданы 48 ATM VC интерфейсов (aal5-0...aal5-47) – на каждый ATM порт по одному VC. В случае если предполагается использовать несколько PVC на одном ADSL порту, пользователь должен сам создать необходимые ему VC интерфейсы. Ему доступны для использования любые имена из диапазона aal5-48...aal5-383. Дублирование имен интерфейсов DAS-3248 запрещено.
С помощью настройки ATM PVC интерфейсов возможно:

1. Задать идентификаторы постоянного виртуального соединения ATM (по умолчанию VPI 8 VCI 35).
2. Задать тип мультиплексирования (llc, vcmux, auto).
3. Применить Input Rate Limiting (IRL).
4. Указать тип канала (fast, interleave).

Интерфейсы EoA

EoA – логический интерфейс, лежащий поверх ATM PVC интерфейса и использующийся при инкапсуляции RFC 2684 (прежнее название RFC 1483) for Bridged Protocols. Имена EoA

интерфейсов лежат в диапазоне eoa-0..eoa-383. По умолчанию созданы 48 EoA интерфейсов с именами eoa-0...eoa-47 (поверх каждого ATM VC).
Для данного интерфейса можно задать тип поддерживаемого Ethernet трафика: Multicast, Broadcast, Unicast, Unknown unicast.

Интерфейсы PPPR и PPPoE

Данные интерфейсы служат для обеспечения прозрачной миграции с традиционных ATM-based DSLAM-ов на IP решения. Во время перехода с ATM на Ethernet/IP возможна следующая ситуация: часть сети будет оставаться ATM-based с используемым протоколом PPPoA, а часть – Ethernet/IP based и протоколом PPPoE. Технология PPPoA to PPPoE internetworking позволяет средствами DSLAM-а преобразовать PPPoA пакеты от CPE в пакеты PPPoE и послать их на BRAS. Подробнее о PPPoA to PPPoE internetworking читайте в рекомендации DSL Forum TR-101.
Имена PPPR (PPPoA relay) и PPPoE интерфейсов лежат в диапазонах pppr-0...pppr-383 и pppoe-0…pppoe-383 соответственно.

Интерфейсы IPoA и IPoE

Требуются для обеспечения функционала IPoA to IPoE internetworking. Обратитесь к рекомендации DSL Forum TR-101 за подробностями.
Имена IPoA и IPoE интерфейсов лежат в диапазонах ipoa-0…ipoa-383 и ipoe-0…ipoe-383 соответственно.

Bridge ports

Bridge port являются вершиной стека интерфейсов DAS-3248 и отвечают за Layer 2 forwarding. Bridge ports позволяют:

1. Создать соответствие ATM VC <-> VLAN. Причем в один VLAN можно включать несколько VC и один VC можно включать в несколько VLAN.
2. Включить блокировку и/или мониторинг клиентских MAC адресов.
3. Выставить 802.1p приоритет всем входящим пакетам.
4. Настроить соответствие между выходными очередями и значением приоритета.

Имена bridge портов (portid) лежат в интервале от 1 до 384 для eoa, pppoe и ipoe интерфейсов. Portid 385 и 386 соответствуют Gigabit Ethernet портам Uplink 1 (eth-0) и Uplink 2 (eth-1) соответственно.

2.2.Файловая структура ОС DAS-3248. Операции с ПО и конфигурациями.

2.2.1.Структура внутренней ОС DAS-3248.

Внутреннее функционирование DSLAM DAS-3248 построено на специальной внутренней операционной системе.

Внутренняя операционная система функционально состоит из:

- загрузчика (BootStrap)
- специального бинарного модуля проверки загрузки по TFTP/BootP (благодаря чему устройство доступно к удаленному автоконфигурированию из локальной сети)
- ядра системы (ControlPlane)
- уровня для связи с пользовательским интерфейсом (DataPlane)
- декомпрессора (поскольку часть системных файлов хранится в архивах формата GZIP для уменьшения занимаемого в памяти пространства).

Внутренняя операционная система имеет собственную древовидную файловую структуру, которая будет рассмотрена ниже. Кроме операций с системными файлами доступна загрузка пользовательских файлов в определенные каталоги по TFTP/FTP.

Все составные части ОС и пользовательские файлы хранятся постоянно на энергонезависимой памяти (NVRAM) и копируются в оперативную память (SDRAM) только при выполнении отдельных операций. Поэтому, файловый путь всех файлов начинается с \nvram.

Файлы во внутренней ОС DAS-3248 кроме обычных файловых атрибутов (имя, размер, дата и время создания, права доступа) имеют еще два атрибута:

- Состояние. Может быть или активным или неактивным.
  Применяется для системных файлов. На файл, помеченный как активный, передается управление при загрузке устройства, тогда как с файлом, помеченным как неактивный, при загрузке устройство ведет себя так, как будто данный файл не присутствуют в файловой системе.
  Такая схема позволяет обновлять системные файлы из локальной сети по протоколу tftp (текущий системный файл просто помечается как неактивный, и на его место загружается новый). Установка файлов из неактивного в активное состояние файлов осуществляется консольной командой **upgrade**.
- Версия.
  Цифровой индекс, служащий индикатором при обновлении файла. То есть, при обновлении файла с таким же именем вы должны сначала удалить старый файл предыдущей версии, а затем загрузить новый и произвести замену командой **upgrade** с индексом версии, увеличенным на единицу.

2.2.2.Порядок загрузки DSLAM. Расположение основных системных файлов.

Ознакомимся подробнее с назначением основных системных файлов, их расположением в памяти и порядком инициализации устройства. Диаграмма, показывающая порядок инициализации устройства представлена на рисунке 2-2.

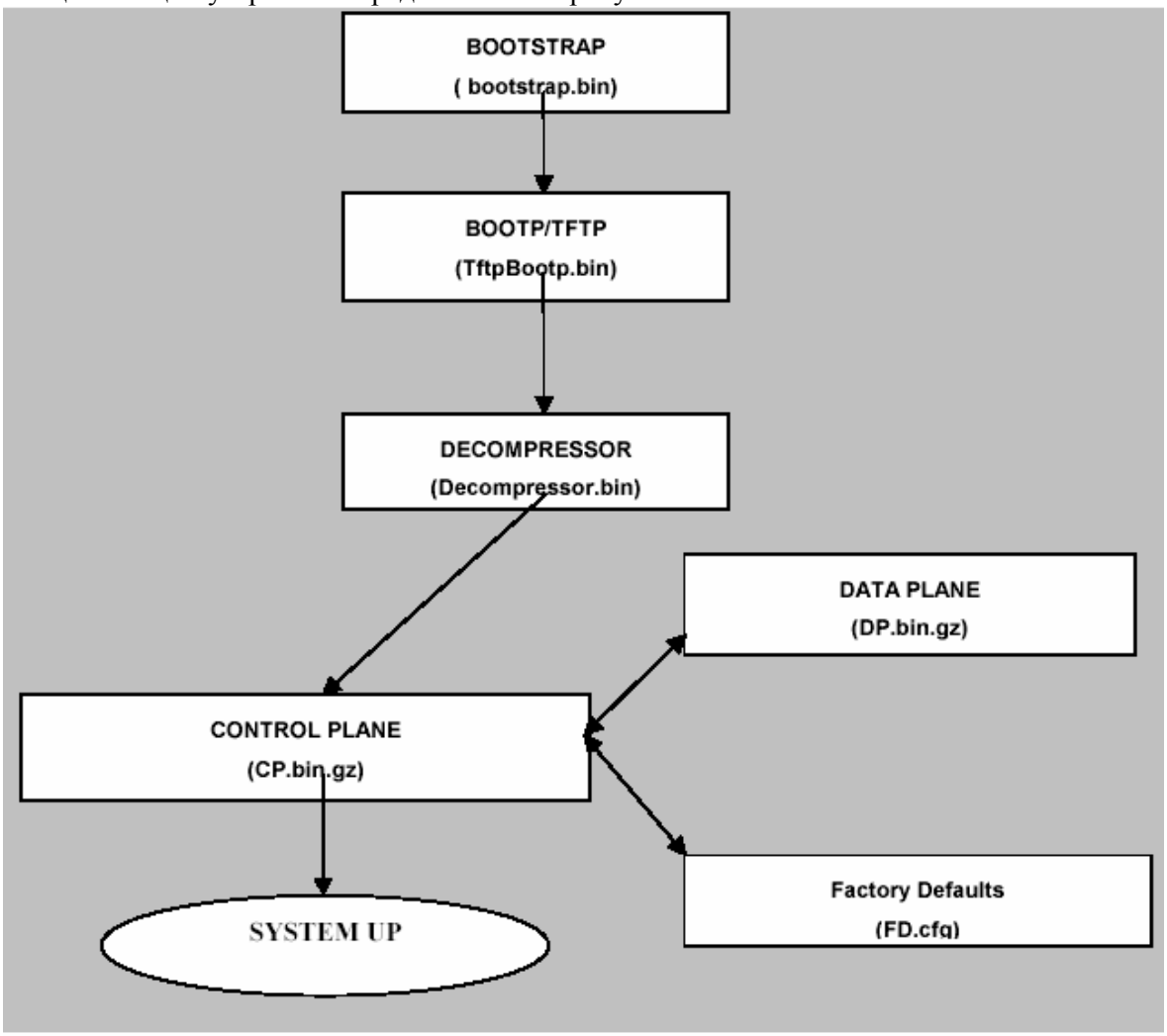


Рисунок 2-2.Порядок инициализации DAS-3248

BOOTSTRAP Загрузчик.
Исполняет роль, аналогичную BIOS . Этот бинарный файл ответствен за инициализацию памяти DAS-3248 и периферийных устройств. После инициализации, он читает двоичный BOOTP/TFTP файл из Flash памяти и передает управление на него. Располагается в первых 64K FLASH памяти.
Файл: Bootstrap.bin

BOOTP/TFTP Загрузчик внутренней ОС.
Проверяет Flash память на наличие активной копий составных частей внутренней ОС (ControlPlane и DataPlane), а также на наличие конфигурации по умолчанию (FD.cfg). Если активная копия хотя бы одного из этих файлов не обнаружена,

модуль пытается получить их посредством BOOTP/TFTP протокола с внешнего TFTP сервера.
Если активные копии всех файлов найдены, BOOTP/TFTP пропускает загрузку по сети и переходит к следующему действию. Он копирует двоичный файл декомпрессора из Flash в SDRAM и передает управление на него.
Файл: TftpBootp.bin
Расположение: /nvram/bin/bootptftp

Decompressor Декомпрессор.
Бинарный файл ControlPlane всегда хранится в архивированном виде (GZIP).Декомпрессор читает ControlPlane или из SDRAM или из Flash памяти (в зависимости от того, производилась ли загрузка по TFTP) , распаковывает его и передает управление на него.
Файл: Decompressor.bin
Расположение: /nvram/bin/decompressor

Control Plane Ядро внутренней ОС.
Control Plane –бинарный файл ответственный за инициализацию Dataplane и образование системы функционально. Кроме инициализации Hardware компонент, отвечает также за большинство функционала устройства (управление таблицей коммутации,фильтрацией пакетов, IGMP Snooping,Flow Based rate limiting, протоколы STP,GVRP,GARP,LACP,формирование IP стека).Также он применяет настройки по умолчанию (FD.cfg) к системе в момент ее загрузки.
Файл: CP.bin.gz
Расположение: /nvram/ bin/controlplane/CP.bin.gz

DataPlane Уровень связи с пользовальским интерфейсом.
DataPlane -Часть внутренней ОС, ответственная за связь с пользовательским интерфейсом. Кроме этого она отвечает за ATM подсистему устройства, Ethernet и Multicast bridging, фильтрацию пакетов.
Файл: DP.bin.gz
Расположение: /nvram/ bin/dataplane/DP.bin.gz

FD.cfg Файл заводских настроек (настроек по умолчанию) DSLAM.
Файл: FD.cfg
Расположение: /nvram/cfg/factorydef/FD.cfg

2.2.3. Каталоги внутренней файловой системы.

Этот раздел содержит файловые пути и описания всех основных каталогов файловой системы DAS-3248.

Каталог	Назначение
/nvram/bin/control/	Каталог содержит упакованный образ ControlPlane. Может содержать многочисленные версии образов.
/nvram/bin/dataplane/	Каталог содержит упакованный образ DataPlane. Может содержать многочисленные версии образов.
/nvram/bin/dslphy/	Каталог содержит двоичный образ драйвера DSL физического уровня. Может содержать только одну версию файла.
/nvram/cfg/factorydef/	Каталог содержит конфигурацию по умолчанию устройства (FD.cfg). Может содержать многочисленные версии файлов.
/nvram/cfg/manuf/	Каталог содержит специальную информацию изготовителя.
/nvram/user/	Каталог содержит файлы пользователя
/nvram/image/	Временный логический каталог, создающийся при операции загрузки внутреннего ПО. Доступен только в специальном режиме (Safe mode)
/nvram/bootloader/	Каталог, содержащий двоичный файл загрузчика Доступен только в специальном режиме (Safe mode)
/nvram/system/	Каталог, содержащий конфигурации основную и резервную системы **primcfg** и **seccfg.**

2.2.4. Команды работы с файлами.

list

Описание: Листинг внутренней файловой системы NVRAM
Синтаксис: list fname <name>, где
fname <name> - вывод информации об отдельном файле

Пример: **list**
Экранный вывод:

```
Flash size          : 4194304
Flash Block size    : 131072
Free Blocks in Flash : 0
/nvram/bin/control/
Name        : CP.bin.gz
```

```
Version    : 1          Size(bytes) : 2224273
Time       : Thu Aug 24 11:30:06 2006
Permission : RW         State       : active
Used Blocks : 17
/nvram/bin/dataplane/
Name       : DP.bin.gz
Version    : 1          Size(bytes) : 382977
Time       : Thu Aug 24 11:30:06 2006
Permission : RW         State       : active
Used Blocks : 3
/nvram/bin/dslphy/
Name       : dsl_10_330000003C00000D.bin.gz
Version    : 1          Size(bytes) : 255984
Time       : Thu Aug 24 11:30:06 2006
Permission : RW         State       : active
Used Blocks : 2
/nvram/cfg/factorydef/
Name       : FD.cfg
Version    : 1          Size(bytes) : 24004
Time       : Thu Aug 24 11:30:06 2006
Permission : RW         State       : active
Used Blocks : 1
/nvram/cfg/manuf/
/nvram/system/
Name       : CFG1
Version    : 1          Size(bytes) : 262032
Time       :
Permission : SYS        State       : active
Used Blocks : 2
Name       : CFG2
Version    : 1          Size(bytes) : 262032
Time       :
Permission : SYS        State       : active
Used Blocks : 2
```

Где:
Name- имя файла
Version – версия файла
Time- время создания
Syze – размер в байтах
Permission – права доступа к файлу. Файл может быть read-only, read-write или protected.
State – состояние. Файл может быть активным (Active) и неактивным (Inactive).
Used Blocks –количество использованных блоков памяти.

remove

Описание: Удалить файл
Синтаксис: **remove fname** file-name **[version** version**]**, где
fname file-name –имя файла,
version version - версия файла (необязательный параметр).

Данная команда работоспособная только в каталогах:
/nvram/bin/control/, /nvram/bin/control/, /nvram/bin/dataplane/,
/nvram/bin/dslphy, /nvram/cfg/factorydef/,/nvram/user/, /sdram/cfg, /sdram/user.

Пример:
$ remove fname /nvram/user/commands.cfg

Внимание: Будьте осторожнее при операциях удаления файлов.
Удаление хотя бы одного из системных файлов DP.bin.gz, CP.bin.gz или FD.cfg и последующая перезагрузка устройства приводят к неработоспособности устройства!!!

apply

Описание: Применить пользовательский конфигурационный текстовый файл (обычно он находится в формате .cfg)

Синтаксис: apply fname file-name **[version** version**] [besteffort** truelfalse**]** , где:
file-name –имя файла,
version- версия файла (необязательный параметр).
besteffort truelfalse – если данный флаг установлен в состояние true, исполнение файла немедленно прекращается после обнаружения первой же ошибки синтаксиса команд.

Команда применима только к каталогам /nvram/cfg/factorydef/, /nvram/user/, /sdram/cfg, /sdram/user.

upgrade

Описание: Обновить файл. Применяется для апгрейда (замены текущего файла обновленной версией). При применении данной команды файл, над которым производится операция, становится активным (а текущий активный становится в свою очередь неактивным), кроме того, индекс версии нового файла увеличивается на единицу. Для апгрейда файла в большинстве случаев необходимо удалить его старую копию, для того чтобы освободить пространство во flash памяти устройства.

Синтаксис: upgrade fname file-name **version** version , где:
fname file-name – имя файла
version version- версия

Команда применима только к каталогам /nvram/bin/control/,
/nvram/bin/dataplane/, /nvram/bin/decompressor,
/nvram/bin/dslphy, /nvram/cfg/factorydef/, /nvram/
user/

Пример:
1. Удалить старую версию файла
$remove fname /nvram/cfg/factorydef/FD.cfg version 1
2. Загрузить с TFTP сервера новую версию
$download src FD.cfg dest /nvram/cfg/factorydef/FD.cfg ip 192.168.100.66
3. Обновить файл.
$upgrade fname /nvram/cfg/factorydef/FD.cfg version 2

upload

Описание: Сохранение файла на ftp/tftp сервере.
Синтаксис:

upload src src-filename **dest** dest-filename **ip** ip-address **[mode** tftp | ftp**]** , где:
src src-filename – имя и путь к файлу-источнику
dest dest-filename – имя и путь к файлу-приемнику
ip ip-address – адрес tftp / ftp сервера
mode tftp | ftp – протокол передачи данных (ftp или tftp)

Пример:
$upload src /nvram/system/primcfg dest myconfig.cfg ip 198.168.1.1

download

Описание: Загрузка файла с удаленного ftp/tftp сервера.
Синтаксис:
download src src-filename **dest** dest-filename **ip** ip-address **[mode** tftp | ftp**]** , где:
src src-filename – имя и путь к файлу-источнику
dest dest-filename – имя и путь к файлу-приемнику
ip ip-address – адрес tftp / ftp сервера
mode tftp | ftp – протокол передачи данных (ftp или tftp)

Пример:
$download myconfig.cfg src dest /nvram/system/primcfg ip 198.168.1.1

2.2.5. Отображение информации о программном обеспечении. Команды управления загрузкой

get system info
Описание: Отображение информации о ПО
Синтаксис: get system info

Пример: $**get system info**

Экранный вывод:

```
Description      : 00000000000000000000000000000000000000000000000000
Name             :
Location         :
Contact          :
Vendor           :
LogThreshold  : 0
Object-id        : 1.3.6.1.4.1.171.10.65.1
Up Time(HH:MM:SS) : 0:32:17
HwVersion       : ADSL-1.0
CPLDVersion   : 1.9
CPSwVersion    : COL2.10.3.2.070221
CPSwVersion(Build): D.3.07.i1000.ADSL2+.A PRIMARY (GS_API_654/E.67.1.69)
DPSwVersion    : DP_B02_10_28_04_ip1000a
System Time      : Thu Jan 01 00:32:17 1970
Time Zone        : GMT
DST              : off
Services          : physical datalink internet end-to-end   applications
```

reboot

Описание: Команда управления загрузкой устройства. При ее выполнении будет произведен «горячий» рестарт системы и загрузка с определенными условиями.
Синтаксис:

reboot [control <nvram|network**>] [d<b>ataplane** <nvram|network**>] [config** <network |default | last | backup | clean | minimum | safe **>]**

где:

control <nvram|network**> -** Загрузка ControlPlane с NVRAM или из локальной сети по TFTP

dataplane <nvram|network> - Загрузка DataPlane с NVRAM или из локальной сети по TFTP

config <network |default | last | backup | clean | minimum | safe >- загрузка устройства в определенной конфигурации:

network – загрузка конфигурационного файла из локальной сети по TFTP.

default- загрузка настроек по умолчанию (FD.cfg)

last - загрузка последней сохраненной пользовательской конфигурации (primcfg).

backup - загрузка резервной пользовательской конфигурации (seccfg).
clean – загрузка устройства без конфигурации («чистая» конфигурация)
minimum- загрузка устройства с минимальной конфигурацией (сконфигурирован только eth-0 интерфейс)
safe – специальный режим для обновления системного ПО (применение его будет рассмотрено в следующих разделах).

Внимание: операции с ключами control и dataplane могут привести к выходу устройства из строя!!!
Данные операции являются инженерными и могут проводиться только в сервис-центрах компании D-link.

Примечание:
применение команды **reboot** без параметров и ключей приводит в загрузке с последней сохраненной конфигурацией.

2.2.6. Операции с конфигурациями. Типовые сценарии.

Как уже было сказано выше в Главе1, DAS-3248 имеет оперативные две конфигурации.
/nvram/system/primcfg - последняя сохраненная командой commit конфигурация,
/nvram/system/seccfg - предыдущая (резервная конфигурация).
Конфигурации являются бинарными (двоичными файлами) и могут быть выгружены и загружены посредством команд download и upload. Порядок действий при работе с файлами конфигурации приведен ниже.

2.2.6.1. Сохранение файла конфигурации на TFTP сервер

1. Выберите, какую конфигурацию (текущую или резервную) вы хотите сохранить
2. Запустите TFTP сервер, в качестве рабочей директории укажите ту, в которую вы хотите сохранить файл конфигурации
3. Скопируйте этот файл tftp из флеш DSLAM-а на TFTP сервер, в качестве ip указав ip адрес tftp сервера:
   $**upload src /nvram/system/primcfg dest Myconf.bin ip 192.168.7.3**
   (для сохранения текущей конфигурации)
   $upload src /nvram/system/seccfg dest Myconf.bin ip 192.168.7.3
   (для сохранения резервной конфигурации)

2.2.6.2.Загрузка файла конфигурации с TFTP сервера на NVRAM

1. Выберите, какую конфигурацию (текущую или резервную) вы хотите обновить.
2. Запустите TFTP сервер, в качестве рабочей директории укажите ту, в которой находится бинарный файл конфигурации
3. Скопируйте файл конфигурации по tftp во флеш DSLAM-а, в качестве ip указав ip адрес tftp сервера:

Например:
$download src myconf.bin dest /nvram/system/primcfg ip 192.168.7.3
(для текущей конфигурации)
$download src myconf.bin dest /nvram/system/seccfg ip 192.168.7.3
(для резервной конфигурации)

4. Введите команду:
$reboot config last -для загрузки устройства с текущей конфигурации
$reboot config backup- для загрузки устройства с резервной конфигурации

2.2.7. Создание, загрузка и применение скриптового файла команд.

Кроме загрузки конфигураций в двоичном виде в DAS-3248 доступна загрузка текстового скриптового файла по tftp протоколу.

Скриптовый файл – это обычный текстовый файл, содержащий набор команд CLI DAS-3248.

Внимание: скриптовый файл можно только загрузить на устройство.
Порядок действий по загрузке скриптового файла:

1. Запустите TFTP сервер, в качестве рабочей директории укажите ту, в которой находится скриптовый файл.
2. Скопируйте файл конфигурации по tftp в один из пользовательских каталог внутренней файловой системы DSLAM-а, в качестве ip указав ip адрес tftp сервера:
   Например:
   $download src mycfg.cfg dest /nvram/user/mycfg.cfg ip 192.168.7.3
   Внимание: При отсутствии (окончании) свободной Flash памяти для загрузки скриптового файла устройство выдает сообщение вида:
   Download Not Enough Resource error...
   Download Failed...
   В этом случае можно воспользоваться загрузкой скриптового файла в оперативную память:
   $download src dslam2.cfg dest /sdram/user/mycfg.cfg ip 192.168.7.3
3. Примените загруженный скриптовый файл командой
   $apply.
   Применения скриптового файла из оперативной памяти команда будет выглядеть так:
   $apply fname /sdram/user/mycfg.cfg

Внимание: Скриптовый файл при применении его командой apply будет анализироваться на правильность синтаксиса и применятся в покомандном режиме. При обнаружении ошибок синтаксиса неправильная команда будет пропущена и применение будет продолжено вплоть до последней команды. Если же вы хотите, чтобы применение файла прерывалось при обнаружении первой же ошибки используйте команду
$**apply /besteffort true**

2.2.8. Операции с программным обеспечением. Типовые сценарии.

2.2.8.1. Обновление ПО DAS-3248.Загрузка файла ПО с TFTP сервера в NVRAM.

Файл внутреннего ПО поставляется компанией D-link в виде единого сжатого файла с расширение .gz (т.е. без разбивки на ControlPlane и DataPlane).
Для операции смены внутреннего программного обеспечения он должен быть помещен в каталог **/nvram/image/** в специальном **safe** режиме, где он будет автоматически разархивирован и применен системой.

Для обновления программного обеспечения DSLAM-а DAS-3248 Вас понадобится файл прошивки с расширением bin.gz (в нашем примере он будет называться TEImage.bin.gz) и TFTP сервер.

Порядок обновления ПО:

4. Подключите консольный кабель к DAS-3248, запустите терминальную программу и включите питание DSLAM-а.
5. Дождитесь окончания загрузки, получите доступ к командной строке и введите команду:
   $**reboot config safe**
6. После перезагрузки устройства необходимо создать и настроить Ethernet интерфейс (DAS-3248 должен быть подключен к сети через порт UPLINK 1!!!)
   Например:
   $create ethernet intf ifname eth-0 ip 192.168.7.13 mask 255.255.255.0 enable

   Внимание: ip адрес созданного интерфейса должен находиться в одной подсети с tftp сервером.

   Примечание: Для DAS-3248F используется интерфейс UPLINK 2 и соответсвенно команда вида
   $create ethernet intf ifname eth-1 ip 192.168.7.13 mask 255.255.255.0 enable

7. Запустите TFTP сервер, в качестве рабочей директории укажите ту, в которой находится файл TEImage.bin.gz
8. Скопируйте этот файл по tftp во флеш DSLAM-а, в качестве ip указав ip адрес tftp сервера:
   $download src TEImage.bin.gz dest /nvram/image/TEImage.bin ip 192.168.7.3

   Внимание: для версий внутреннего ПО устройства ниже 1.70 (текущей пршивки) это команда выглядит следующим образом
   $download src TEImage.bin.gz dest /nvram/TEImage.bin ip 192.168.7.3

9. Дождитесь окончания загрузки файла и обновления flash.
   Внимание: Ни в коем случае не выключайте в этот время питание устройства!
10. После появления приглашения командной строки введите: reboot
11. После перезагрузки устройства введите команду reboot config default

На этом обновления внутреннего программного обеспечения закончено.

2.2.9. Автоконфигурирование DAS-3248.

DAS-3248 позволяет осуществить автоматическую удаленную загрузку конфигурационного файла из локальной сети по протоколу BootP/TFTP
командой **reboot config network.**

Данная команда изменяет состояние файла FD.cfg на неактивное и перегружает устройство, что позволяет загрузить на его место свой предварительно сформированный скриптовый файл. **IP адрес,** необходимый для загрузки, **DAS-3248 получает автоматически с внешнего DHCP сервера** находящего в той же сети, что и DSLAM, **а затем загружает скриптовый файл с внешнего TFTP сервера**. Новый файл FD.cfg замещает старый и после проверки синтаксиса всех команд переводится в активное состояние. Затем устройство автоматически перегружается в "нормальный" штатный режим.
Данная функция позволяет упростить обслуживание устройств и организовать удаленное централизованное конфигурирование (администратору сети необходимо лишь ввести CLI команду, выключить устройство, переправить его на объект, подключить к локальной сети один из портов Uplink и включить устройство).

Внимание:
1.Применение команды $reboot config network является необратимым. То есть, после ее применения, не существует способа вернуться в исходное состояние.
Вы должны обязательно загрузить файл FD.cfg с TFTP сервера.
2.Сформированный для данной операции скриптовый файл должен содержать команды создания всего стека протоколов «с нуля» (как на интерфейсах Ethernet , так и на портах ADSL)**.**

Пример:

```
verbose off
create user name admin passwd admin root
create dsl system

create ethernet intf ifname eth-0 ip 10.90.90.90 mask 255.255.255.0
create bridge port intf portid 385 ifname eth-0 status enable

create ethernet intf ifname eth-1 type downlink
create bridge port intf portid 386 ifname eth-1 status enable

create ethernet intf ifname eth-2 ip 10.90.91.91 mask 255.255.255.0
modify bridge mode enable

create atm port ifname atm-0 lowif dsl-0
create atm vc intf ifname aal5-0 lowif atm-0 vpi 8 vci 35
create eoa intf ifname eoa-0 lowif aal5-0
create bridge port intf ifname eoa-0  portid 1 learning enable status enable
modify adsl line profile ifname dsl-0    atucfrontenddesigntype el1508   atuchwpwrreduction
disable
……
create atm port ifname atm-47 lowif dsl-47
create atm vc intf ifname aal5-47 lowif atm-47 vpi 8 vci 35
```

```
create eoa intf ifname eoa-47 lowif aal5-47
create bridge port intf ifname eoa-47  portid 48 learning enable status enable
modify adsl line profile ifname dsl-47    atucfrontenddesigntype el1508   atuchwpwrreduction
disable

modify adsl line intf ifname dsl-0 enable
……
modify adsl line intf ifname dsl-47 enable

create filter rule entry ruleid 1 action sendtocontrol description IGMP
create filter subrule ip ruleid 1 subruleid 1 prototypefrom 2 prototypecmp eq
modify filter rule entry ruleid 1 status enable

create filter rule map ruleid 1 ifname eth-0 stageid 1
create filter rule map ruleid 1 ifname eoa-0 stageid 1
……..
create filter rule map ruleid 1 ifname eoa-47 stageid 1

modify igmpsnoop port info portid 385 status enable
modify igmpsnoop port info portid 1  status enable
……..
modify igmpsnoop port info portid 48  status enable

reate filter rule entry ruleid 2 action sendtocontrol status disable description EAPOL
create filter subrule ether ruleid 2 subruleid 1 dstmacaddrfrom 01:80:C2:00:00:03
dstmacaddrcmp eq
modify filter rule entry ruleid 2 status enable
create filter rule entry ruleid 3 action drop status enable description DATA_CLOSE
create filter rule entry ruleid 4 action drop status disable description DATA_OPEN

create d1x server srvrip 10.90.90.123 srvrsecret dlink1234 Usrname dlink pw
PASSWDpasswd0123456789

create d1x port portid 1 portctl force_auth
…
create d1x port portid 48 portctl force_auth

verbose on

end
```

Экранный вывод при автоконфигурировании:

```
$ reboot config network
Transfering Control to BootTftp binary

 Flash Present In System
 Flash size read in progress

 Flash Address 0x00: 89

 Flash Address 0x02: 16

 Flash size: 4M

 .......Flash size read successful...

 g_u32FlashSize     : 4194304

 g_u32FlashBlockSize: 131072
.............................
 FD is not active
 Columbia Package shall not be TFTPied

 Do you want to force its TFTP... Y/N? n
 Forced TFTP not requested

 Press 'F/f' to perform forced TFTP of a file
 'Enter' to skip ... 5 Seconds left

 Press 'D/d' to debug the Control Plane using GDB
 'Enter' to skip ... 5 Seconds left

 User did not request for debugging Control Plane......Continuing
 Primary Ethernet Interface for TFTP   :- eth-0
 Secondary Ethernet Interface for TFTP :- eth-1
 Could not TFTP on eth-0, reverting to eth-1
 TFTPing Factory Default...
#
 System coming up in normal mode...
```

3. После загрузки устройства в «нормальный» штатный режим необходимо сохранить настройки командой commit. В противном случае при следующей ппаратной перезагрузке устройства оно опять войдет в режим удаленного конфигурирования.

3.Настройка DSL-линий.

3.1.Теория и сущность технологии ADSL

ADSL — это технология, позволяющая сделать из медленной аналоговой телефонной линии скоростную цифровую линию. Главные достоинства - свободный телефон, высокие скорости передачи данных и высокое качество линии. При использовании ADSL можно одновременно работать в Интернете и разговаривать по телефону.

ADSL относится к классу широкополосных (broadband) технологий. Она обеспечивает скорость передачи данных в направлении к абоненту — до 7,5 Мбит/с, от абонента — до 1,5 Мбит. Один ADSL-канал может обеспечивать работу в Интернете целой группы пользователей. Оборудование, которое устанавливается на стороне заказчика, имеет интерфейс локальной сети Ethernet. Соответственно заказчик может легко подключить компьютер или локальную сеть.

Линии ADSL могут использоваться не только для подключения к Интернету, но и для создания распределенных корпоративных сетей по технологии VPN. Такой подход значительно упрощает топологию корпоративной сети, удешевляет ее строительство и эксплуатацию.

Благодаря тому, что в соединении не используется телефонная сеть общего пользования, которая имеет высокий уровень шумов и помех, возникает значительная разница в качестве ADSL и обычной телефонной линии. Вероятность ошибки на ADSL линии составляет 10E-8 — 10E-10 (так называемый уровень Bit Error Rate-BER). Для сравнения в обычной телефонной линии вероятность ошибки 10E-3 — 10E-5. По сравнению с системами спутникового и беспроводного доступа ADSL дает более высокое качество соединения, близкое к качеству волоконно-оптических линий.

Главное условие подключения к ADSL — на АТС абонента должно быть размещено соответствующее оборудование и линия должна быть переключена на него.

Дело в том, что «медный провод», приходящий к абоненту, подключен к телефонной станции, которая настроена на прием сигнала шириной 4 кГц, вполне достаточной для передачи голоса. Обычный модем просто подстраивается под возможности телефонной сети, а потому имеет скорость, ограниченную 56 Кбит/с. Однако, технические возможности самой «медной пары» гораздо выше, ее пропускная способность приближается к 1 МГц, и поэтому через нее можно передавать данные на высоких мегабитных скоростях.

Чтобы получить цифровую высокоскоростную линию, к окончаниям «медной пары» подключаются специальные цифровые устройства (сплиттеры или микрофильтры) — один на АТС, другой в квартире абонента — которые обеспечивают одновременную работу в линии телефона и Интернета. Один выход станционного сплиттера подключен с АТС, а другой к мультиплексору (DSLAM ,ATUC), объединяющему множество линий ADSL и связанному с Интернетом. Абонентский сплиттер устанавливается у входа в объект абонента, от него идут два провода — один к ADSL-модему (ATUR), а другой ко всем телефонным розеткам. Сплиттер иногда называют делителем, т.к. он отделяет аналоговый телефонный сигнал от цифровой полосы пропускания.

Более удобной для абонента является схема подключения с микрофильтрами, когда модем подключается к линии напрямую, а все телефоны, факсы и пр. аналоговые устройства подключаются к линии через микрофильтры.

Вся полоса пропускания «медной пары» с помощью сплиттера (микрофильтра) делится на два диапазона: низкочастотный для телефонной связи и высокочастотный для передачи данных.

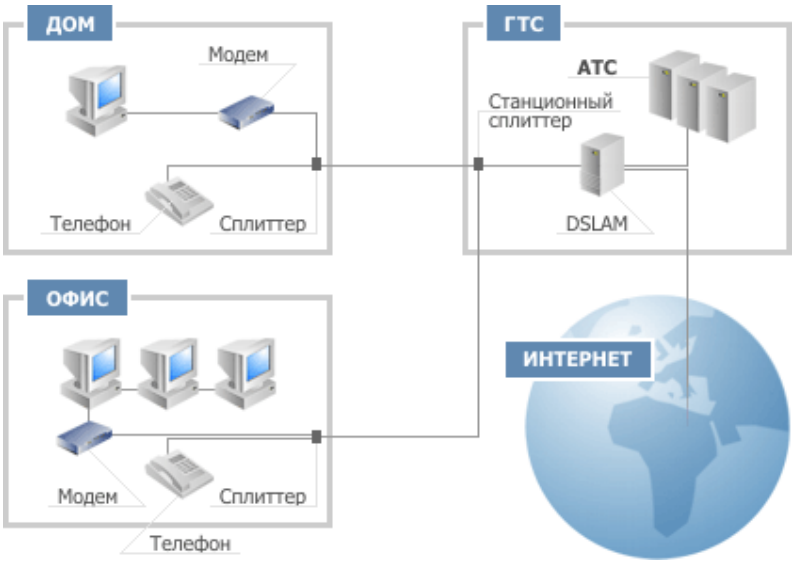


Рисунок 3-1

ADSL использует для кодирования сигналов линий дискретную многотональную технологию (DMT).

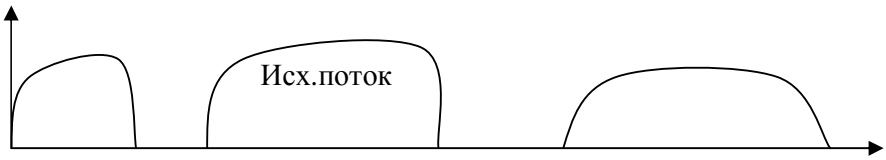
Смысл ее заключается в том, что вся полоса частот в 1.1 Мгц делится на 256 подканалов, называемых поднесущими. Каждый канал занимает по 4.3125Кгц. Некоторые из подканалов являются специализированными, другие не используются вообще. Нижние подканалы от 1 до 6 резервируются для полосы пропускания аналоговых телефонов в 4 Кгц., поэтому 25Кгц (4.3125*6) является точкой отсчета для диапазона служб ADSL. Между аналоговым телефоном и сигналами DTM имеется широкая защитная полоса частот (quardband).

Если отвлечься от технических деталей, то это можно представить себе так, как будто бы между абонентом и зданием АТС проложено 247 независимых телефонных линий. Часть из них служит для приема входящего потока (от Интернет-провайдера к абоненту), часть — для исходящего потока. Система управления построена так, что все-время идет мониторинг состояния каждого канала, и информация направляется в те из них, которые обладают наилучшими характеристиками.

Когда одна пара проводников работает в полнодуплексном режиме, нужно либо разделить диапазон частот для входящего и исходящего потоков (мультиплексирование с разделением по частотам – FDM), либо использовать эхоподавление.

Эхосигнал возникает из-за несогласования сопротивлений по пути следования сигнала, т.к. некоторая часть сигнала отражается обратно к передатчику. Когда один и тот же диапазон частот используется в обоих направлениях, отраженный сигнал можно перепутать с сигналом, генерируемым на удаленном конце цепи. Эхоподавление предполагает электронное «вычитание» посланного сигнала из принятого сигнала, что позволяет выявить сигналы, посланные с удаленного конца цепи.

При разделении частот (FDM) используются 32 канала исходящего потока (с 7-го) и только 218 каналов для входного потока, а при эхоподавлении используют ассиметричную полосу пропускания, 32 канала исходящего потока (с 7-го) и 250 каналов входящего потока. В результате в ADSL используются и FDM, и эхоподавление, т.к. полоса пропускания в ADSL асимметрична, но диапазоны частот для входящего и исходящего потоков частично перекрываются.



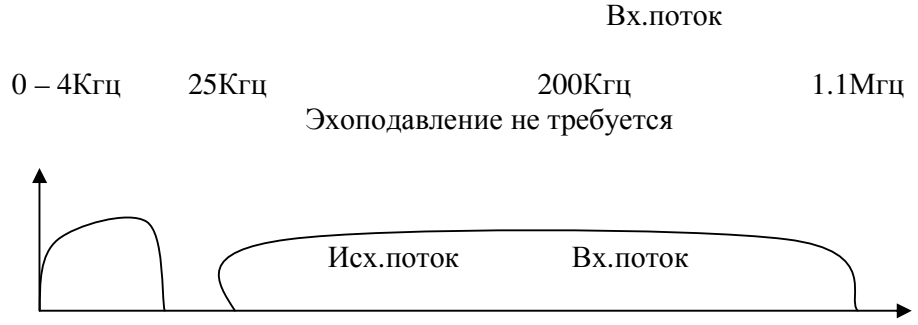


Рисунок 3-2

Каналы исходящего потока занимают нижнюю часть спектра из-за того, что затухание сигнала на этих частотах меньше, а клиентские передатчики обычно имеют меньшую мощность, чем передатчики местной станции.

Каждый из каналов использует собственный метод кодирования на основе QAM.

В идеале в левой части диапазона частот существует максимум для количества битов в секунду на подканал (поднесущую), которое сможет получать и принимать данное устройство. На больших частотах влияет расстояние, а на меньших – импульсные шумы и перекрестные помехи. В результате сигнал медленно затухает при увеличении частоты. Устройство DMT может измерить усиление (затухание) на каждой поднесущей и подстроить для канала скорость передачи таким образом, чтобы отразить реальное состояние канала.

Как будет представлен пакет IP битами ADSL? Все протоколы, включая ADSL, имеют многоуровневую структуру. На самом нижнем уровне описываются биты, представляющие коды DMT. Биты объединяются в кадры, из которых в ADSL формируется суперкадр. Т.о. кадр ETHERNET может содержаться внутри суперкадра ADSL. Суперкадр состоит из 68 обычных кадров и передается каждые 17 мс, некоторые кадры имеют спецназначение: CRC, индикаторные биты, кадр синхронизации и т.д.

Интерфейсы ADSL способны поддерживать не только единственный битовый поток от/к клиенту. Битовый поток внутри кадров может быть одновременно разбит не более чем на 7 несущих каналов. Из них до 4-х каналов – полностью независимые, для входного потока, и до 3-х каналов – двунаправленные, для входного и выходного потоков. Несущие каналы являются только логическими, а биты из всех каналов передаются по ADSL одновременно и не используют выделенных полос пропускания.

ADSL2

Технология ADSL2 логическим развитием технологии ADSL.
ADSL2 специально разрабатывался для улучшения скорости и дальности ADSL, в основном для достижения лучшей производительности на длинных линиях с помехами. ADSL2 может достигать скоростей приема и передачи до 12 Мбит/с и 1 Мбит/с соответственно, в зависимости от дальности и прочих факторов. Это стало возможным благодаря использованию более эффективных методов модуляции, уменьшению количества служебной информации, увеличению эффективности кодирования, и применению расширенных алгоритмов обработки сигнала. Системы ADSL2 используют меньшее количество служебной информации благодаря кадру с программируемым количеством служебных битов. Поэтому, в отличие от ADSL первого поколения, где служебные биты в кадре были фиксированы и потребляли 32 кбит/с от полезной информации, количество служебных бит в кадре может меняться от 4 до 32 кбит/с. В системах ADSL первого поколения на длинных линиях, где скорость передачи информации и так невысока

(например, 128 кбит/с), под служебную информацию фиксировано отведено 32 кбит/с (или более 25% общей скорости). В системах ADSL2, это значение может быть снижено до 4 кбит/с, что добавит к пропускной способности дополнительные полезные 28 кбит/с.
На длинных линиях, где, как правило, скорости передачи низки, ADSL2 позволяет достичь большей эффективности кодирования кода Рида-Соломона, исправляющего ошибки передачи данных в потоке. Это возможно благодаря улучшениям в кадрах, повышающим гибкость и программируемость при создании кодовых слов.
Вдобавок, механизм инициализации содержит множество улучшений, поднимающих скорость передачи в системах ADSL2:
— снижение мощности с двух сторон, позволяющее снизить перекрестные наводки;
— обнаружение размещения контрольного сигнала приемником, устраняющее помехи от АМ радио;
— обнаружение несущих, используемое приемником для инициализационных сообщений для устранения помех от АМ радио и других неприятностей;
— улучшения в области идентификации канала для настройки приемника и передатчика;
— отключение сигнала во время инициализации для включения схем подавления радиочастотных помех.
На рисунке 3-3 показаны скорость и дальность ADSL2 в сравнении с ADSL первого поколения. На длинных линиях ADSL2 даст прирост скорости на 50 кбит/с для входящего и исходящего потоков. Это увеличение скорости достигается на увеличенных на 180 метров линиях.

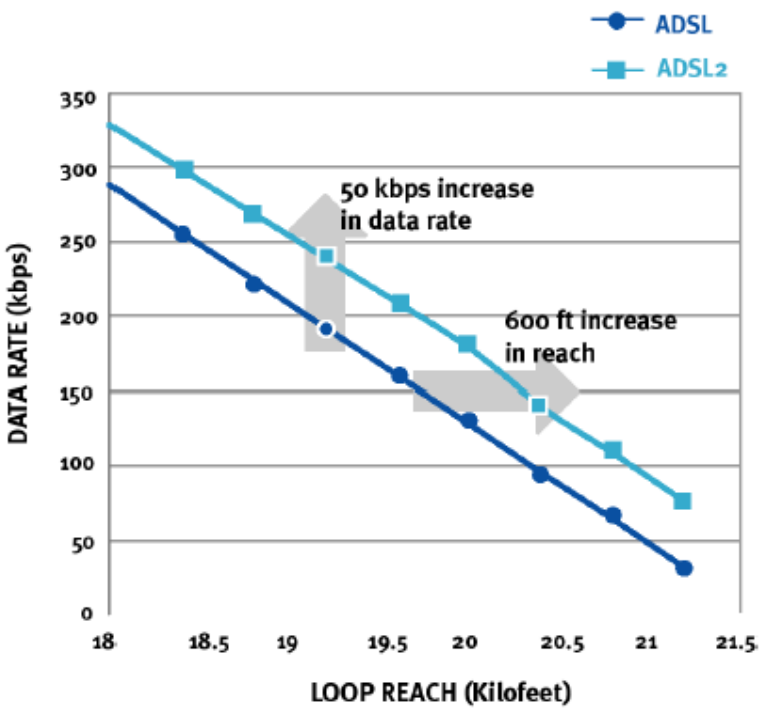


Рисунок 3-3

ADSL2plus

ADSL2plus разработан в ITU в январе 2003 и включен в стандарты ADSL в качестве G.992.5. Рекомендация ADSL2plus удваивает скорость входящего потока на линиях длиной менее 1500 метров.
В то время как первые два члена семейства стандартов ADSL2 устанавливают полосы частот входящего канала до 1.1 МГц и 552 кГц соответственно, ADSL2plus устанавливает полосу частот

для входящего канала до 2.2 МГц (рис.4). В результате достигается значительное увеличение скорости входящего канала на более коротких линиях (см. рис.3-5). Скорость исходящего канала ADSL2plus зависит от качества связи и находится в районе 1 Мбит/с.

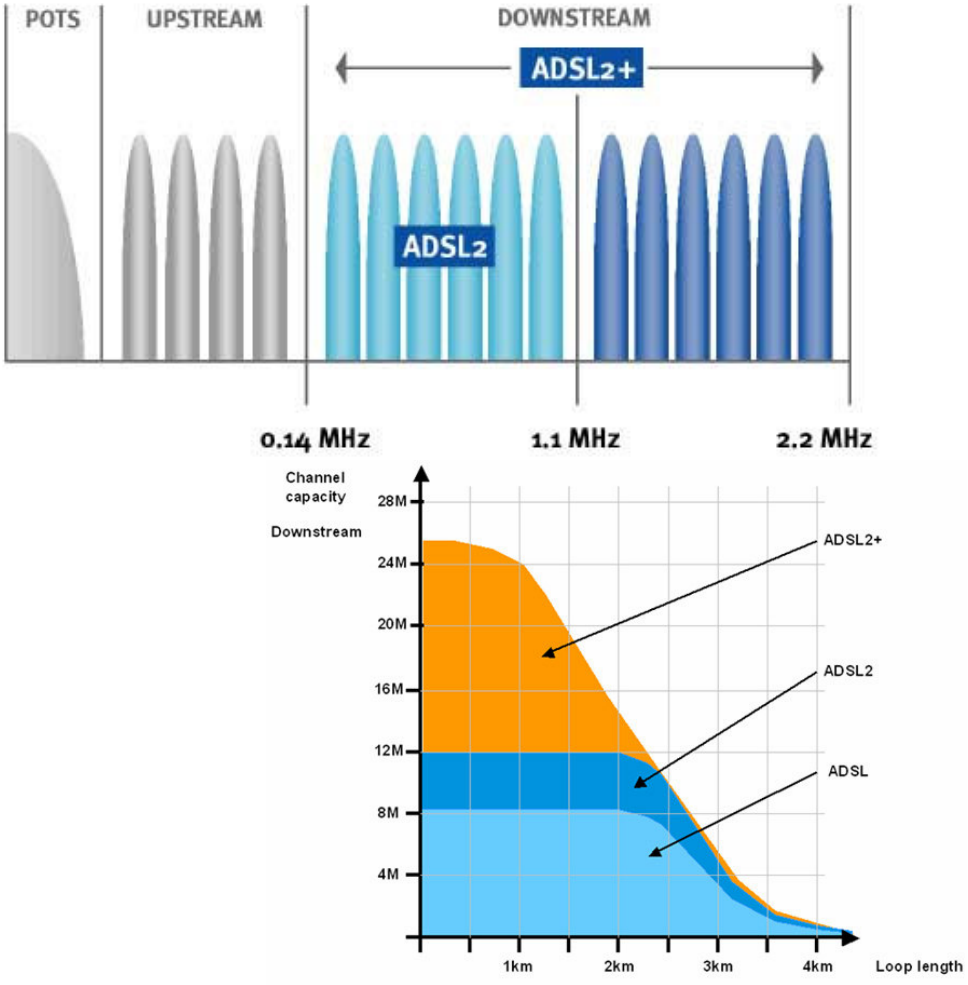


Рисунок 3-5

ADSL2plus может также использоваться для снижения перекрестных наводок. Для этого он может использовать тоны между 1.1 МГц и 2.2 МГц, маскируя частоты входящего канала в районе 1.1 МГц. Это может оказаться полезным, когда терминалы ADSL подключаются к центральному пункту через один и тот же кабель в том же порядке, в котором осуществлена подводка к домам клиентов (рис. 3-6). Перекрестные наводки от линий удаленных терминалов на линии от центрального пункта могут существенно снизить скорости передачи данных на линии от центрального пункта.

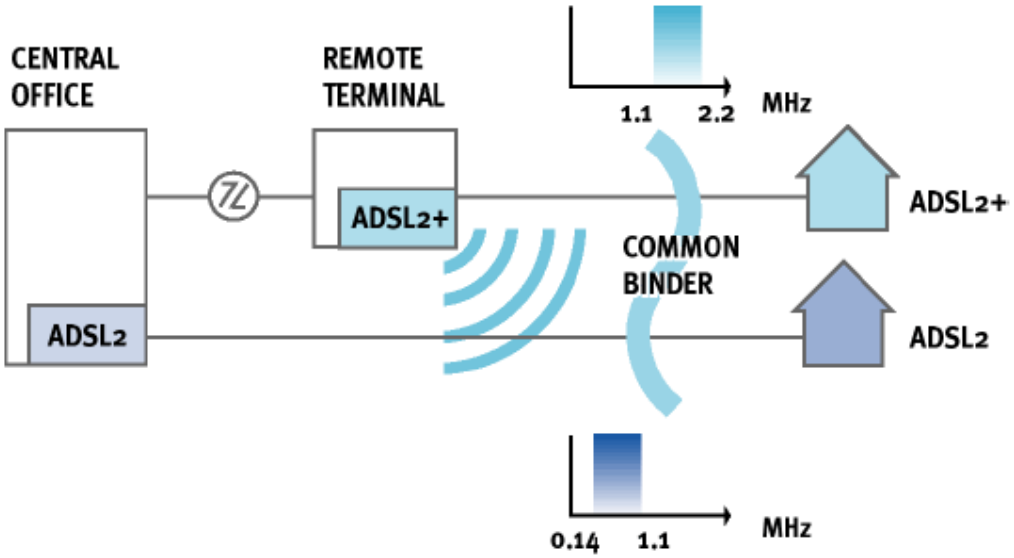


Рисунок 3-6

ADSL2plus может решить эту проблему путем использования частот ниже 1.1 МГц от центрального пункта к удаленному терминалу и частот между 1.1 МГц и 2.2 МГц от удаленного терминала до дома пользователя. Это уничтожит большинство перекрестных наводок между службами и защитит скорость передачи данных на линии от центрального офиса.

Увеличение помехоустойчивости. Перемеживание.
Перемеживание (Interleaving) – это процесс перестановки пользовательский данных в определенной последовательности. Он используется для того, что бы избежать последовательных ошибок.
Обычно в стандарте ADSL для исправления ошибок (Forward Error Correction- FEC) используется помехоустойчивый код Рида-Соломона, который предполагает добавление служебных байтов к каждому ADSL кадру (FEC Bytes).
Но если в линии передачи на медном проводе возникает шумовой выброс, он может воздействовать на несколько последовательно расположенных битов данных. Если в передатчике данные перемеживаются, то при устранении перемеживания данных на приемном конце не только восстанавливается исходная последовательность битов, но и происходит разнесение ошибочных данных по времени (ошибочные биты проявляются в разных байтах), что позволяется более эффективно исправлять ошибки передачи данных.
Включение процесса перемеживания ведет к дополнительной задержке или запаздыванию по времени, за которое данные передаются и по времени, за которое они становятся доступны получателю.
Поэтому в оборудовании DSL применяется два типа передачи данных – с перемеживанием (Interleave) и без него (Fast).
Режим с перемеживанием применяется для типов данных, не чувствительным к задержкам (например, передача данных), режим Fast для типов данных малочувствительным к ошибкам (например, голосовая телефония).

Приложения стандартов (Annex).
Внутри стандартов ADSL существуют приложения, расширяющие их дополнительными возможностями, например, путем переноса частотного диапазона спектра ADSL сигналов. Они обозначаются буквенными индексами (например, Annex B).

Внимание: Для использования Annex типов требуется поддержка его оборудованием на обоих концах линии (то есть и DSLAM, так и модемом).
В DAS-3248 используется 3 типа таких приложений.
Annex A – обозначает стандарт без переноса частотного диапазона (например, ADSL Annex A, ADSL 2+ Annex A).

Annex M - Приложение к стандартам ADSL2/2+ позволяющее достичь скорости до 3 Мбит/с за счет расширения спектра частот, занимаемых Upstream потоком данных.
Таким образом, DAS-3248 с применением всех расширений технологии (ADSL2+ Annex M) позволяет достичь теоретическойскорости Downstream потока до 24 Мбит/с , и Upstream до 3 Мбит/с.
Устройство позволяет программно переключаться с **Annex A** на **Annex M** и обратно.

Annex L (Reach-Extended ADSL2, ReADSL2)- Обозначает приложение к стандарту ADSL2, позволяющее увеличить максимально достижимую дальность ADSL с 18000 до 21000 футов (приблизительно с 6.1 км до 6.5 км). Высокие частотные спектры ADSL2 не могут быть использованы на предельных расстояниях в связи с сильным затуханием. По сравнению с классическим ADSL2 ReADSL2 позволяет увеличить расстояние покрытия при малых скоростях или увеличить скорость передачи на предельных расстояниях ADSL2.
Внимание: На DAS-3248 ReADSL2 включается автоматически при установке в качестве стандарта ADSL2, что обеспечивает автоматическую адаптацию к длине линии. На клиентском устройстве может потребоваться выбрать в качестве модуляции ReADSL2.

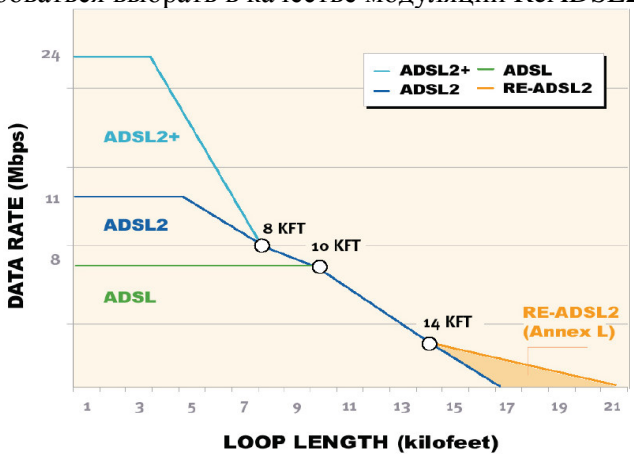


Рисунок 3-7

Annex B – обозначает перенос спектра для совместимости с оборудованием ISDN. В настоящее время это расширение также используется для совместимости технологии ADSL с квартирными охранными системами у абонентов. Частотный спектр Annex B показан на рисунке 3-8.
Внимание: Annex B поддерживается только в устройствах с аппаратной ревизией B (HW Rev. B), и только специальным ПО (прошивкой) устройства. Annex B несовместим с другими Annex. Обращайтесь в представительства компании D-link за более подробной информацией.

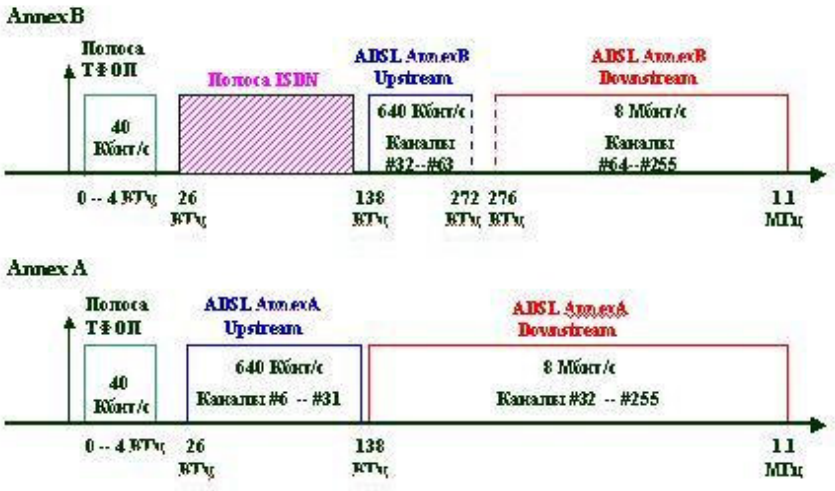


Рисунок 3-8

3.2.Включение/выключение ADSL- порта

Интерфейсы DSL служат для непосредственного управления соответствующими ADSL портами DAS-3248. Названия dsl интерфейсов лежат в диапазоне dsl-0...dsl-47. Интерфейс dsl-0 соответствует 1-ому ADSL порту, dsl-47 – сорок восьмому. DSL интерфейсы являются нижележащими интерфейсами для ATM портов. По умолчанию в DAS-3248 созданы все DSL интерфейсы

Для управления интерфейсами DSL используется команда.

modify adsl line intf

Описание**:** изменить параметры ADSL порта.
Синтаксис команды:
modify adsl line intf ifname ifname enable | disable ,
где ifname- имя порта ADSL

Примеры:
Административно выключить 1 порт ADSL
$modify adsl line intf ifname dsl-0 disable
Административно включить 1 порт ADSL
$modify adsl line intf ifname dsl-1 enable

3.3.Изменение информации профиля порта. Просмотр статуса порта

Для изменения парамеров порта DSL используется команда.

modify adsl line intf

Описание**:** изменение парамтеров ADSL порта.

Синтаксис команды:

modify adsl line intf ifname *ifname* [**linetransatucconfig** ansit1413 | etsi | q9921PotsNonOverlapped | q9921PotsOverlapped | q9921IsdnNonOverlapped | q9921isdnOverlapped | q9921tcmIsdnNonOverlapped | q9921tcmIsdnOverlapped | q9922potsNonOverlapeed | q9922potsOverlapped | q9922tcmIsdnNonOverlapped | q9922tcmIsdnOverlapped | q9921tcmIsdnSymmetric | adslPlusPotsNonOverlapped | q9921GspanPlusPotsNonOverlapped | q9921GspanPlusPotsOverlapped | q9923Adsl2PotsOverlapped | q9923Adsl2PotsNonOverlapped | q9925Adsl2PlusPotsOverlapped | q9925Adsl2PlusPotsNonOverlapped | q9923Readsl2PotsOverlapped | q9923Readsl2PotsNonOverlapped | adslPlusPotsOverlapped | q9921GspanPlusPlusPotsNonOverlapped | q9921GspanPlusPlusPotsOverlapped | q9923IsdnNonOverlapped | q9923IsdnOverlapped | q9925IsdnNonOverlapped | q9925IsdnOverlapped | q9923AnnexMPotsExtUsNonOverlapped | q9923AnnexMPotsExtUsOverlapped | q9925AnnexMPotsExtUsNonOverlapped | q9925AnnexMPotsExtUsOverlapped] [**dsbinsnrupdate** Disable | Enable] [**enable | disable**]

Одним из важнейших параметров порта является **LineTransAtucConfig,** позволяющий настраивать набор типов модуляций ADSL, поддерживаемых каждым из dsl портов.

Примечание 1: Через параметр **LineTransAtucConfig** могут выбраны один или более типов модуляции ADSL. Подключения всех не выбраных типов модуляций на данном порту будут игнорироваться.

Примечание 2: перед изменением параметров интерфейс необходимо административно выключить.

Примечание 3: Названия значения параметра с фрагментами в названиях «Overlapped» «NonOverlapped» и являются вариантами с эхоподавлением и без эхоподавления одного и того же типа модуляции (описание сущности эхоподавления в технологии ADSL читайте выше в разделе 3.1)

Значение параметра LineTransAtucConfig	**Описание типа модуляции**
ansit1413	ADSL ANSI T1.1413 (Скорость Downstream- до 8мбит/с, скорость Upstream-до 1 мбит/с)
etsi	Не используется в данном устройстве
q9921PotsNonOverlapped q9921PotsOverlapped	ADSL G.Dmt (Скорость Downstream- до 8мбит/с, скорость Upstream-до 1 мбит/с)
q9921IsdnNonOverlapped q9921isdnOverlapped	ADSL Annex B **только для DAS-3224/BE**
q9921tcmIsdnNonOverlapped q9921tcmIsdnOverlapped	Не используются в данном типе устройств

q9922potsNonOverlapeed q9922potsOverlapped	G.Lite (Скорость Downstream- до 1.5 мбит/с, скорость Upstream-до 0.5 мбит/с)
q9922tcmIsdnNonOverlapped q9922tcmIsdnOverlapped q9921tcmIsdnSymmetric q9921GspanPlusPotsNonOverlapped q9921GspanPlusPotsOverlapped	Не используются в данном типе устройств
q9923Adsl2PotsOverlapped q9923Adsl2PotsNonOverlapped	ADSL 2 (Скорость Downstream- до 12 мбит/с, скорость Upstream-до 1 мбит/с)
q9925Adsl2PlusPotsOverlapped q9925Adsl2PlusPotsNonOverlapped	ADSL 2+ (Скорость Downstream- до 24 мбит/с, скорость Upstream-до 1 мбит/с)
q9923Readsl2PotsOverlapped q9923Readsl2PotsNonOverlapped	READSL 2 Расстояние до 7 км.
adslPlusPotsOverlapped adslPlusPotsNonOverlapped	Не используются в данном типе устройств
q9921GspanPlusPlusPotsNonOverlapped q9921GspanPlusPlusPotsOverlapped	Не используются в данном типе устройств
q9923IsdnNonOverlapped q9923IsdnOverlapped	ADSL2 Annex B **только для DAS-3224/BE**
q9925IsdnNonOverlapped q9925IsdnOverlapped	ADSL2+ Annex B **только для DAS-3224/BE**
q9923AnnexMPotsExtUsNonOverlapped q9923AnnexMPotsExtUsOverlapped	ADSL2 Annex M (Скорость Downstream- до 12 мбит/с, скорость Upstream-до 3 мбит/с)
q9925AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped	ADSL2+ Annex M (Скорость Downstream- до 24 мбит/с, скорость Upstream-до 3 мбит/с)

Примеры:
Настроить **только** ADSL 2+ модуляцию на 1 порту ADSL :
$modify adsl line intf ifname dsl-0 disable
$ modify adsl line intf ifname dsl-0 LineTransAtucConfig q9925Adsl2PlusPotsNonOverlapped q9925Adsl2PlusPotsOverlapped
$modify adsl line intf ifname dsl-0 enable

Для просмотра статуса порта DSL используется команда.
get adsl line intf

Описание**:** просмотр статуса ADSL порта.
Синтаксис команды:
get adsl line intf ifname *ifname* , где ifname- имя порта ADSL

Примеры:
Административно выключить 1 порт ADSL
$get adsl line intf ifname dsl-0

В случае отсутствия параметра ifname выводится статус для всех портов устройства.

Экранный вывод:

```
IfName                      : dsl-0
Line Type                   : interleavedOnly    Coding Type           : dmt
GsUtopia  L2TxAddr          : 0                  GsUtopia L2RxAddr     : 0
GsUtopia L2RxAddr2nd        : 0                  GsUtopia  L2TxAddr2nd : 0
Gs Clock Type               : oscillator         Gs Action             : startup
Trans Atuc Cap              : ansit1413 q9921PotsNonOverlapped q9921PotsOverlapped q9922potsNonOverlapeed q9923Reads12PotsNonOverla
pped q9925Adsl2PlusPotsNonOverlapped q9925Adsl2PlusPotsOverlapped q9923Adsl2PotsNonOverlapped q9923AnnexMPotsExtUsNonOverlapped q992
5AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
Trans Atuc Actual           : -
Trans Atuc Config           : ansit1413 q9921PotsNonOverlapped q9923Reads12PotsNonOverlapped q9925Adsl2PlusPotsOverlapped q9923Adsl
2PotsNonOverlapped q9923AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
GsDmtTrellis                : trellisOn
Trans Atur Cap              : ansit1413 q9921PotsOverlapped q9921tcmIsdnOverlapped adslPlusPotsOverlapped q9923Reads12PotsNonOverla
pped q9925Adsl2PlusPotsNonOverlapped q9925Adsl2PlusPotsOverlapped q9923Adsl2PotsNonOverlapped q9921GspanPlusPotsOverlapped q9923Anne
xMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
PM Conf PMSF                : L3ToL0StateForce
Line DELT Conf LDSF         : inhibit
Curr Output Pwr(dBm/10)     : 0                  DS Bin SNR Update     : Enable
Bin Number    SNR Margin/bin
-----------------------------
[0 ]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[16]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[32]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[48]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
Oper Status                 : Down               Admin Status          : Up
```

3.4.Использование DSL-профайлов

Профайлы DSL используются для тонкой настройки параметров ADSL для каждого порта устройства (использование перемеживания, настройки минимальной и максимальная скорость в каждом из режимов и другие).

По умолчанию профайлы настроены на использование режима перемеживания (Interleave). Скорость по умолчанию не ограничена.

3.4.1.Изменение профайла

Профайл по умолчанию может быть изменен командой:

modify adsl line profile

Описание**:** изменить параметры ADSL порта.
Синтаксис команды:
modify adsl line profile ifname *ifname*
[atucrateadaptation fixed | adaptAtStartup| adaptAtRuntime **][atuctargetsnr** atuctargetsnr **]**
[atucmaxsnrmargin atucmaxsnrmargin **][atucgsrsintcorrectionup** atucgsrsintcorrectionup **]**
[atucfastmintxrate atucfastmintxrate **] [atucintlmintxrate** atucintlmintxrate **]**
[atucfastmaxtxrate atucfastmaxtxrate **] [atucintlmaxtxrate** atucintlmaxtxrate **]**
[atucmaxintldelay atucmaxintldelay **] [type** noChannel | fastOnly | interleavedOnly
| fastOrInterleaved | fastAndInterleaved **[atucgsdrstby** Disable |Enable**][atucgstxpoweratten**
atucgstxpoweratten**] [aturtargetsnrmargin** aturtargetsnrmargin **] [aturfastmintxrate**
aturfastmintxrate **] [aturintlmintxrate** aturintlmintxrate **] [aturfastmaxtxrate** aturfastmaxtxrat**e] [**
aturintlmaxtxrate aturintlmaxtxrate **] [atucmaxintldelay** atucmaxintldelay **] [atucmaxintldelay**
atucmaxintldelay **] [atucgsrsfastovrhdup** atucgsrsfastovrhdup]**[atucgsrsfastovrhddn**
atucgsrsfastovrhddn**][atucgsrsintcorrectionup** atucgsrsintcorrectionup]

[atucgsrsintcorrectiondn atucgsrsintcorrectiondn**][atucgsmaxdco** atucgsmaxdco]

Таблица описания параметров команд:

ifname *ifname*	Имя DSL интерфейса, лежит в диапазоне dsl-0..dsl-47. **Обязательный параметр.**
atucrateadaptation fixed | adaptAtStartup| adaptAtRuntime	Определяет форму адаптации скорости передачи. Fixed- фиксированная скорость.Не может изменяться AdapAtStartup, AdaptAtRuntime - скорость определяется динамически из выбранного диапазона скоростей. Ссылка: ADSL Forum TR- 005 для получения большей информации. **Необязательный параметр**
atuctargetsnr atuctargetsnr	Настройка отношения сигнал/шум. Это значение шума BER (Bit Error Rate-интенсивность появления ошибочных битов) в пределах от 10 в степени -7, или выше, которое модем должен достичь, для успешной инициализации. **Необязательный параметр** **Допустимые значения:** 0 - 310
atucmaxsnrmargin atucmaxsnrmargin	Настройка максимально допустимого отношения сигнал/шум (ОСШ). Если значение шума выше, то модем должен оптимизировать мощность излучения до приемлемого уровня. **Необязательный параметр** **Допустимые значения:** 0 - 310
Atucgsrsintcorrectionup *125us* | *250us* | *500us* | *1ms* | *2ms* | *4ms* |	Устанавливает время коррекции для буфера входящего потока. **Необязательный параметр**
atucfastmintxrate atucfastmintxrate	Настройка минимальной скорости передачи Downstream потока данных (от DSLAM к абоненту) для «Fast» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2) **Необязательный параметр**
atucintlmintxrate atucintlmintxrate	Настройка минимальной скорости передачи Downstream потока данных для «Interleave» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2)

	Необязательный параметр
atucfastmaxtxrate atucfastmaxtxrate	Настройка максимальной скорости передачи Downstream потока данных для «Fast» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2) **Необязательный параметр**
atucintlmaxtxrate atucintlmaxtxrate	Настройка максимальной скорости передачи Downstream потока данных для «Interleave» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2) **Необязательный параметр**
type noChannel | fastOnly | interleavedOnly | fastOrInterleaved | fastAndInterleaved	Параметр используется для настройки режима физической ADSL линии. (только Fast, только Inreleave или их комбинация. В случае комбинации режимов (fastAndInterleaved), режим будет выбираться на вышестоящих интерфейсах ATM PVC. **Необязательный параметр**
Atucgstxpoweratten 0|.1 |.2 | .3 |.4 | .5 |.6 |.7| .8|.9| 1|2| 3| 4|5 |6| 7| 8|9 |10|11|12	Значение затухания мощности в дБ Сигнала передатчика. По умолчанию 0. **Необязательный параметр**
atucgsdrstby Disable | Enable	Параметр предоставляет возможность отключать питание линии. **Необязательный параметр**
aturtargetsnrmargin aturtargetsnrmargin	Настройка предельного ОСШ. Это предельное значение мощности шума (10 в -7 степени), который модем должен превысить, чтобы успешно завершить инициализацию **Необязательный параметр**
aturfastmintxrate aturfastmintxrate	Настройка минимальной скорости передачи Upstream потока данных (от абонента к DSLAM) для «Fast» режима. Скорость указывается в бит/с в шестнадцатиричном виде. (См. примечание 2) **Необязательный параметр**
aturintlmintxrate aturintlmintxrate	Настройка минимальной скорости передачи Upstream потока данных для «Interleave» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2)

	Необязательный параметр
aturfastmaxtxrate aturfastmaxtxrate	Настройка максимальной скорости передачи Upstream потока данных для «Fast» режима. Скорость указывается в бит/с в шестнадцатиричном виде. (См. примечание 2) **Необязательный параметр**
aturintlmaxtxrate aturintlmaxtxrate	Настройка минимальной скорости передачи Upstream потока данных для «Interleave» режима. Скорость указывается в бит/с в шестнадцатеричном виде. (См. примечание 2) **Необязательный параметр**
aturmaxintldelay aturmaxintldelay	Конфигурируемое максимальное значение задержки интерливинга для interleave канала в upstream направлении. Данная задержка применяется только к данным interleave канала и определяет разницу во времени между байтами на входе интерливера и их эквивалентами на его выходе. Большие значения данной задержки ведут к лучшему разделению последовательных входных байт в выходном потоке, позволяя повысить устойчивость системы к импульсным шумам. **Принимает значения:** 0 - 255 **По умолчанию:** 16 **Необязательный параметр**
atucmaxintldelay atucmaxintldelay	Конфигурируемое максимальное значение задержки интерливинга для interleave канала в downstream направлении. Данная задержка применяется только к данным interleave канала и определяет разницу во времени между байтами на входе интерливера и их эквивалентами на его выходе. Большие значения данной задержки ведут к лучшему разделению последовательных входных байт в выходном потоке, позволяя повысить устойчивость системы к импульсным шумам. **Принимает значения:** 0 - 255 **По умолчанию:** 63 **Необязательный параметр**
atucgsrsfastovrhdup	Percent Overhead для Upstream Fast

Disable|3|6|12|25|50	буфера **Необязательный параметр**
atucgsrsfastovrhddn Disable|3|6|12|25|50	Percent Overhead для Downstream Fast буфера **Необязательный параметр**
atucgsrsintcorrectionup atucgsrsintcorrectionup	Interlieving correction time для Upstream буфера **Необязательный параметр**
atucgsrsintcorrectiondn atucgsrsintcorrectiondn	Interlieving correction time для Downstream буфера **Необязательный параметр**
atucgsmaxdco 64|128|256	Interleaving Maximum Depth. **Необязательный параметр**

Примечание 1: Перед изменением любых параметров существующего DSL интерфейс необходимо его выключить

$modify adsl line intf ifname dsl-22 disable

А после внесения всех необходимых изменений в конфигурацию необходимо включить его в работу
$modify adsl line intf ifname dsl-22 enable

Примечание 2: Изменение скорости на портах DSLAM
Скорость на DSL портах DSLAMa задается в шестнадцатеричном формате в **битах в секунду**. Таким образом, необходимую скорость в Мбит/с нужно два раза умножить на 1024 и полученное число перевести в шестнадцатеричный формат.
Наиболее используемые значения скоростей даны в таблице:

Скорость	**Значение в HEX**
128 Кбит/с	0x20000
256 Кбит/с	0x40000
512 Кбит/с	0x7d000
1 Мбит/с	0x100000
1.5 Мбит/с	0x180000
2 Мбит/с	0x200000
4 Мбит/с	0x400000
8 Мбит/с	0x800000
12 Мбит/с	0xc00000
16 Мбит/с	0x1000000

Пример1:

Interleaved режим:

$modify adsl line intf ifname dsl-22 disable

$modify adsl line profile ifname dsl-22 type InterleavedOnly atucintlmaxtxrate 0x177000 aturintlmaxtxrate 0x7d000
$modify adsl line intf ifname dsl-22 enable

Пример 2:
Fast режим:

$modify adsl line profile ifname dsl-22 type fastonly atucfastmaxtxrate 0x177000 aturfastmaxtxrate 0x7d000
$modify adsl line intf ifname dsl-22 enable

Внимание*:* Во время изменения максимальной скорости ADSL соединения Вы можете получить следующее диагностическое сообщение: *Error: ATUC transmission rate and orl rate conflict.* В этом случае нужно изменить значение ORL (output rate limiting) в настройках ATM порта, соответствующего выбранному ADSL порту, т.е. в случае ADSL порта dsl-22, значение ORL нужно изменять для ATM порта atm-22. ORL не должно превосходить максимальную скорость ADSL соединения.
Например:
$ modify atm port ifname atm-22 ORL 1536
Значение ORL указывается в десятичном формате и задается в **килобитах в секунду.**
$modify adsl line intf ifname dsl-22 disable

3.4.2.Просмотр ADSL профайла

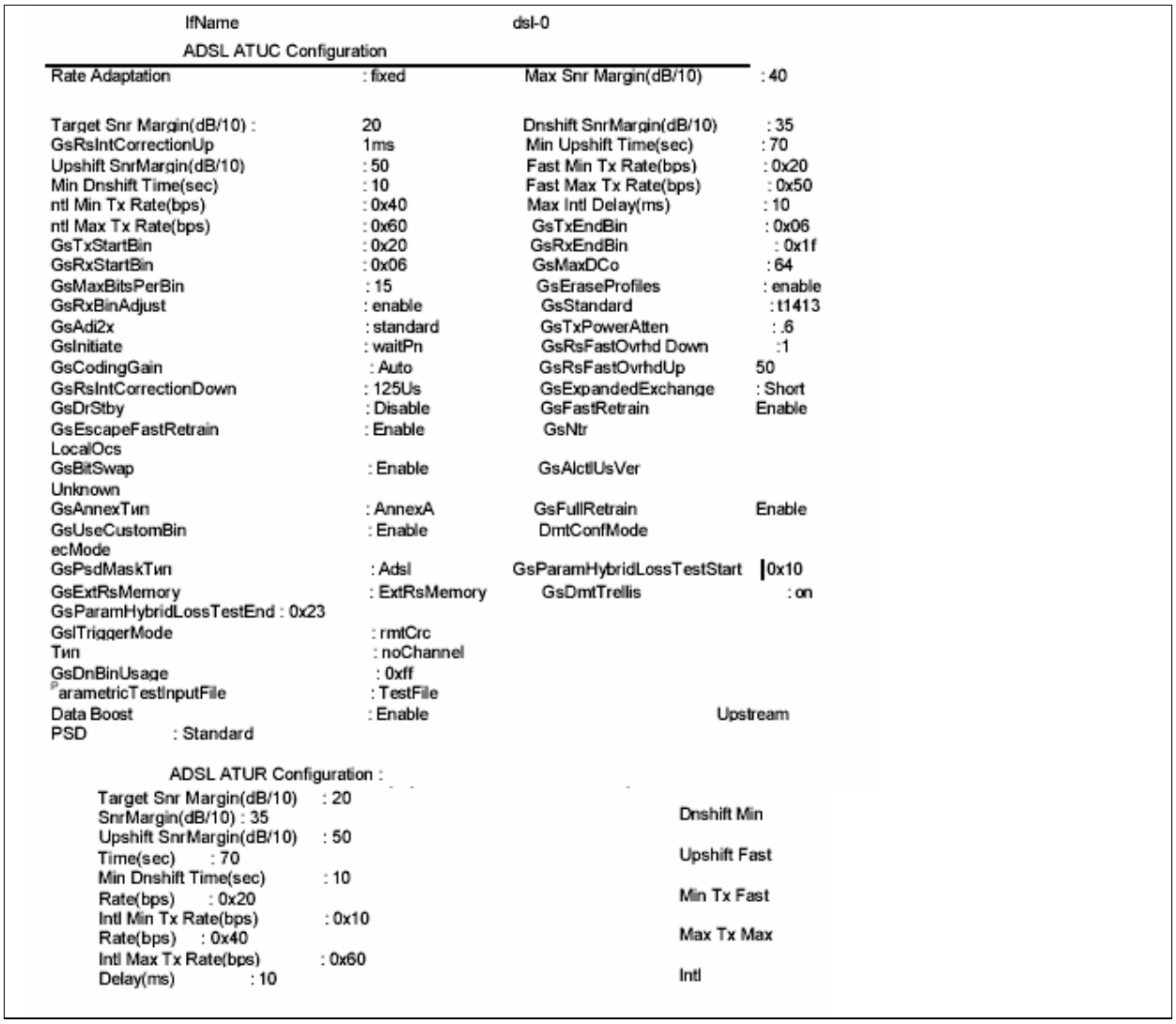
get adsl line profile

Описание**:** просмотр параметра ADSL порта.
Синтаксис команды:
get adsl profile ifname *ifname*, где ifname- имя порта ADSL .
В случае отсутствия параметра ifname выводятся профайлы ADSL для всех портов устройства

Пример:

$ get adsl line profile ifname dsl-0

Экранный вывод:



3.5.Включение ATM local loopback

ATM служит основной транспортной технологией переноса потока данных в сетях ADSL. Она как бы находится между ADSL -физическим уровнем и вышестоящими протоколами. Кроме того, эта технология позволяет переносить внутри одной физической медной пары более одного потока данных, оперируя виртуальными путями (PVC – к ним привязаны AAL5 интерфейсы DAS-3248). Подробнее о технологии ATM и ATM PVC вы можете прочитать в следующей главе.

Но ATM играет также существенную роль и для диагностики ADSL.

Применяя так называемую ATM local loopback, (Single End Loop Test (SELT) или Double End Loop Test (DELT)), можно судить производится ли перенос потока данных по физической паре или нет. Этот процесс можно назвать условно ATM ping (по аналогии с процессом эхо-запросов протокола ICMP для стека TCP/IP).

Внимание: ATM local loopback тест может производится, только если нижележащий интерфейс DSL находится в состоянии Up (как административно, так и операционно).

Для выполнения ATM local loopback служат команды:

modify oam lpbk

Описание**:** запрос выполнения теста ATM local loopback.

Синтаксис команды:

modify oam lpbk vc ifname *ifname* [e2e | seg **] [lbid** *lbid* **]**

Параметры команды:

ifname *ifname*	Имя AAL-5 интерфейса, лежит в диапазоне aal5-1..aal5-384. **Обязательный параметр**
e2e | seg	Вариант проверки. **Необязательный параметр**
lbid *lbid*	Идентификатор пункта ATM, в который производится ATM local loopback. В настоящее время не используется. **Необязательный параметр**

get oam lpbk

Описание**:** вывести результаты теста ATM local loopback.

Синтаксис команды:

get oam lpbk vc [ifname *ifname* **]**

В случае, если интерфейс не указан в команде, производится вывод результатов для всех имеющихся интерфейсов.

Пример:

Произвести тест ATM local loopback на 1 порту устройства

$ modify oam lpbk vc ifname aal5-0

$ get oam lpbk vc ifname aal5-0

Экранный вывод:

```
IfName          : aal5-0     VPI : 1          VCI : 1
LB Type         : e2e
OAM Location Id : 0xffffffffffffffffffffffffffffffff
OAM LB Result   : E2e Succeeded
```

Комментарий к экранному выводу:

Тест можно считать успешным, если поле OAM LB Result приняло значение E2e Succeeded или Seg Succeeded (в зависимости от выполняемого теста).

Другие возможные варианты окончания теста:

Result Unavailable- результат недоступен;

Seg Failed, E2e Failed - неуспешное прохождение теста;

Test Aborted- тест прерван во время исполнения (например, по причине разрыва физической линии);

Test In Progress- процесс теста не окончен (требуется подождать и повторить команды, описанные выше).

3.6.Просмотр параметров линии DSL.Оценка параметров линии.

Для просмотра параметров ADSL линии используются следующие команды:

3.6.1.Команды просмотра физических параметров линии

Позволяют узнать параметры физические параметры линии (кодирование, битовый массив состояний и т.д).

get adsl atuc physical

Описание**:** Просмотр параметров потока ADSL для данного порта в Downstream направлении

Синтаксис команды: **get adsl atuc physical [ifname** ifname **],** где ifname- наименование интерфейса dsl

get adsl atur physical

Описание**:** Просмотр параметров потока ADSL для данного порта в Upstrema направлении

Синтаксис команды: **get adsl atur physical [ifname** ifname **],** где ifname- наименование интерфейса dsl

Пример: **get adsl atur physical ifname dsl-0**

Экранный вывод:

```
Ifname                                  : dsl-0
Serial Number                           : CO123456
Vendor ID                               : Vendor123
Version Number                          : VerNo98114
Curr Status                             : LossOfFraming
Curr Snr Margin(dB/10)                  : 10          Curr Atn(dB/10)          : 10
CurrAttainable Rate(bps)                : 10          Curr Output Pwr(dB/10)   : 10
AturGsConfig                            : 0x0121020203
Chan Perf CD                            : 5           Chan Perf CU             : 5
Chan Perf BE                            : 5           Delt HLINSCds            : 2
Delt HLOGMTds                           : 8           Delt QLNMTds             : 5
DELT Last Tx State                      : dmtaturg9941
Overhead Channel                        : 4000        Delt SnrmtDs             : 100
Signal Atn(dB/10)                       : 40          System Vendor ID         : 12345678
ATU-R Self Test Result                  : 0x10        ATUR G9941 Vendor ID     : 12345678
Atur ACTPSDds (dB/10)                   : 90
Bin Number    Number of bits/bin
[0 ]          68  109 116 0   0   0   0   0   0   255 0   0   15  0   0   0
[16]          7   0   0   0   15  0   0   0   0   0   0   0   0   128 0   0
[32]          0   0   0   0   0   128 0   0   0   128 0   0   0   0   0   0
[48]          0   0   0   0   2   0   0   0   0   0   0   0   0   32  0   0
[64]          0   0   0   0   17  0   0   0   0   0   0   0   2   0   0   0
[80]          0   0   0   0   0   0   0   0   2   0   0   0   64  0   0   0
[96]          1   0   0   0   60  0   0   0   0   0   0   0   120 0   0   0
[112]         0   0   0   0   0   0   0   0   0   125 0   0   0   125 0   0
[128]         0   112 23  0   0   112 23  0   16  0   0   0   0   128 0   0
[144]         0   0   0   0   2   3   48  48  48  48  48  48  48  48  53  50
[160]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[176]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[192]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[208]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[224]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   255 255
[240]         255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
[256]         255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
[272]         255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
[288]         255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 0   0
[304]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0

[320]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[336]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[352]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[368]         0   0   0   0   0   0   0   0   0   0   0   0   0   48  48  48  48
[384]         48  48  48  48  53  50  0   0   0   0   0   0   0   0   0   0   0
[400]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[416]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[432]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[448]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[464]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[480]         0   0   0   0   48  48  48  48  48  48  48  48  53  50  0   0   0
[496]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[512]          0   0   0   0   0   0   0   0   2   0   0   0   12  32  0   0   0
[528]          12  32  0   0   172 84  143 2   0   0   0   0   0   0   0   0   0
[544]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[560]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[576]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[592]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[608]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[624]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[640]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[656]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[672]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[688]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
[704]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
```

```
 [720]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [736]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [752]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [768]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [784]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [800]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [816]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [832]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [848]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [864]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [880]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [896]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [912]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [928]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [944]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [960]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [976]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [992]          0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
 [1008]         0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
Delt HLINpsds
-------------
[0 ]           0
Delt HLOGpsds
-------------
[0 ]           0
Delt QLNpsds
------------
[0 ]           0
Delt DMT Bin SNR
----------------
[0 ]           0
DownStream Gains per bin
----------------------------
[0 ] 0   0    0    0
[4 ] 0   0    0    0
[12] 0   0    0    0
[16] 0   0    0    0
..
..
[508] 0  0    0    0
Transmit Spectrum Shaping info
----------------------------------
[ 0]     0    0    0    0    0    0    0    0
[ 8]     0    0    0    0    0    0    0    0
[ 16]    0    0    0    0    0    0    0    0
[ 24]    0    0    0    0    0    0    0    0
..
```

Описание параметров вывода:

ifname	Имя физического интерфейса
Serial Number	Строка определения производителя, которая идентифицирует производителя оборудования.
Vendor ID	Идентификационный код производителя.
Version Number	Определение номера версии производителя, который передается ATU сообщениями при инициализации.

Curr Status	Отображает текущий статус линии. Это битовый массив возможных состояний.
Curr Snr Margin(dB/10)	Ткущее отношение сигнал/шум
Curr Atn(dB/10)	Измеренная разница между общей переданной мощность ATU и общей полученной мощностью ATU интерфейсом (текущее затухание)
CurrAttainable Rate(bps)	Отображает максимальную достижимую текущую скорость передачи данных ATU интерфейса. Это значение будет равно, или больше текущего значения линейной скорости.
Curr Output Pwr(dB/10)	Измеренная общая мощность, преданная интерфейсом ATU. Это измерения, которые производились во время последней активации.
GsActualStandard	Действующий стандарт, использующийся для соединения, основанный на согласовании параметров с удаленным модемом.
Gs TxA tmCellCounter	Предоставляют Tx ATM ячейки счетчика.
GsRxA tmCellCounter	Предоставляют Rx ATM ячейки счетчика.
GsBertError	Предоставляет число битовых ошибок.
GsIdleBertError	Предоставляет число битовых ошибок.
GsIdleBertCell	Число пустых ячеек.
GsBertSync	Отображает состояние сигналов синхронизации: включен или выключен.
GsParametricTestResult	Отображает результат поведения параметрического теста петли для физической линии
GsSeltInfoValid	Отображает разрешенную информацию ATM Loopback
GsSeltLoopLen (in Feet)	Длина линии в футах, измеренная по данным ATM Loopback (SELT или DELT)
GsSeltLoopEnd	Показывает, доступна ли функция ATM Loopback в данный момент.
GsSeltLoopGauge	Показывает информацию по толщине проводов по данным петли ATM Loopback.
GsSeltUpShannonCap (in bps)	Показывает пропускную способность по методу Шеннона для исходящего

	потока в битах в секунду
GsSeltDownShannonCap (in bps)	Показывает пропускную способность по методу Шеннона для входящего потока в битах в секунду
Data Boost Status	Параметр, который показывает Статус DataBoost для соединения.
Parametric Info	Параметр, который показывает параметрический массив теста.

3.6.2.Команды просмотра параметров буфера канала

Позволяют просмотреть текущие (мгновенные) параметры передачи потока данных.
Для команд просмотра буфера канала были введены специальные типы подинтерфейсов dsl: dsli (для режима с перемеживанием) и dslf (для Fast режима).

get adsl atur channel

Описание**:** Просмотр качества канала ADSL для данного порта в Downstream направлении
Синтаксис команды:
get adsl atur channel [ifname ifname**]], где** где ifname- наименование подинтерфейса dsl (dsli или dslf)

get adsl atuc channel

Описание**:** Просмотр буфера канала ADSL для данного порта в Upstream направлении
Синтаксис команды:
get adsl atuc channel [ifname ifname**], где** где ifname- наименование подинтерфейса dsl (dsli или dslf)

Пример1: Параметры буфера Downsream потока (режим Interleave)

```
$ get adsl atuc channel ifname dsli-23

Ifname                : dsli-23
Interleave Delay(ms) : 5                    Curr Tx Rate(bps)          : 23017900
Prev Tx Rate(bps)    : 23126900             Crc Block Length(byte)     : 47430
Gs Curr Atm Status   : OK                   GsSymbolsPerRsWord         : 34
GsRsDepth            : 64                   GsRedundantBytesPerRsCode : 6
AtucChanPerfAtmCD    : 792738873            AtucChanPerfAtmCU          : 0
AtucChanGsINPdn      : 26                   AtucChanGsLOdn             : 5905
AtucChanGsMOdn       : 1                    AtucChanGsTOdn             : 2
AtucChanGsBOdn       : 248
$
```

Пример 2: Параметры буфера Downsream потока (режим Interleave)

```
$ get adsl atur channel ifname dsli-23

Ifname                : dsli-23
Interleave Delay(ms) : 14                   Curr Tx Rate(bps)          : 1022400
Prev Tx Rate(bps)    : 1008000              Crc Block Length(byte)     : 2511
Gs Curr Atm Status   : OK                   GsSymbolsPerRsWord         : 701
GsRsDepth            : 8                    GsRedundantBytesPerRsCode : 16
AturChanPerfAtmCD    : 670933895            AturChanPerfAtmCU          : 5342873
AturChanGsINPup      : 180                  AturChanGsLOup             : 283
AturChanGsMOup       : 8                    AturChanGsTOup             : 1
AturChanGsBOup       : 28
$
```

3.6.3.Команды просмотра качества канала

Позволяют узнать количество ошибок на линии.

get adsl atuc perf [ifname ifname**]**

Описание**:** Просмотр качества канала ADSL для данного порта в Upstream направлении

Синтаксис команды: **get adsl atuc perf [ifname** ifname**],** где ifname- наименование интерфейса dsl

get adsl atur perf [ifname ifname**]**

Описание**:** Просмотр качества канала ADSL для данного порта в Downstream направлении

Синтаксис команды: **get adsl atur perf [ifname** ifname**],** где ifname- наименование интерфейса dsl

Пример: **get adsl atur perf ifname dsl-0**

```
Ifname                 : dsl-0
Perf Valid Intervals   : 20
Perf Invalid Intervals : 30
AturPerfStatLossL      : 14
                              PerfData   Curr15Min    Curr1Day    Prev1Day
Time Elapsed/Monitored(sec)               10           20          30
LOFS (sec)                    40          45           35          50
LOSS (sec)                    30          65           75          20
LPRS (sec)                    10          95           30          80
ES (sec)                      90          85           32          90
Perf Stat SESL                41          48           67          65
Perf Stat UASL                37          49           90          50
Perf Stat FecsL               11          13           19          21
```

Параметры вывода:

ifname	Имя интерфейса
Perf Valid Intervals	Количество правильных интервалов (для режима с перемеживанием)
Perf Invalid Intervals	Количество неправильных интервалов (для режима с перемеживанием)
AturPerfStatLossL	Усредненное значение потерь синхронизации
LOFS (sec)	Количество секунд за определенный период, в которых были определены потери ADSL фреймов
LOSS (sec)	Количество секунд, за определенный период, в которых были определены потери синхронизации
LPRS (sec)	Количество секунд за определенный период, в которых были определены потери мощности сигнала
ES (sec)	Количество секунд за определенный период, в которых были определены CRC ошибки
Perf Stat SESL	Количество секунд с ошибками CRC за интервал превыщающий 10 секунд
Perf Stat UASL	Количество секунд зв период, которых синхронизация отсутствовала

3.6.4.Оценка параметров линии по результатам выполненных команд

- **Текущий ADSL стандарт**
  Определяется параметром **Trans Atuc Actual** по результатам команды
  $get adsl line intf ifname dsl-xx

- **Текущая (мгновенная) скорость передачи потока данных**
  Определяется параметром **Curr TX Rate** по результатам команд
  $get adsl atuc channel ifname dsli-xx (dslf-xx)
  $get adsl atur channel ifname dsli-xx (dslf-xx)

- **Отношение сигнал/шум (для Downstream и Upstream направлений)**
  Определяется параметром **Curr Snr Margin** по результатам команд
  $get adsl atuc physical ifname dsl-xx showview concise
  (для Downstream направления)
  $**get adsl atur physical ifname dsl-xx showview concise**
  (для Upstream направления)

  Чем данные значения больше, тем лучше качество физической линии.
  Для российских линий данные значения должны быть порядка 15-20 db (соответствует значению параметра 150-200)

- **Затухание в физической линии**

  Определяется параметром **Curr Atn** по результатам команд
  $get adsl atuc physical ifname dsl-xx showview concise
  (для Downstream направления)
  $**get adsl atur physical ifname dsl-xx showview concise**
  (для Upstream направления)
  Чем данные значения меньше, тем лучше качество линии (в идеале значение параметра должно быть 0).Предельное затухание 60db (соотвествуют значению параметра 600).

- **Время последнего изменения состояния интерфейса (в отсчете от последней перезагрузки устройства)**
  Определяется параметром **Last Change** по результатам команды
  $get interface stats ifname dsl-xx
  Эта команда показывает когда (на какой секунде от старта устройства) произошло последнее изменение состояния интерфейса. Эта величина меняется только при изменении состояния интерфейса.

- **Ошибки ADSL на интерфейсе по результатам команд**

  $get adsl atuc perf ifname dsl-xx
  (для Downstream направления)
  $get adsl atur perf ifname dsl-xx
  (для Upstream направления)

  Выводы:

1. Если количество ошибок велико, а ES мало, то на линии присутсвует импульсная помеха. Необходимо увеличить время перемеживания (Interleave Delay).

Это достигается параметрами **atucmaxintldelay и aturmaxintldelay** профиля ADSL интерфейса. Параметры действительны только для Interleave режима.
В случае сильной импульсной помехи на Fast режиме выход – только переход на Interleaving.

2. Если же количество ошибок примерно равно ES, то на линии присутствует постоянная помеха. В этом случае, необходимо увеличить количество FEC RS информации содержащейся в ADSL суперфреймах. Делается это по-разному для Fast и Interleave режимов.

   В случае Fast режима доступен только один параметр, влияющий на количество RS информации :
   Percent Overhead (параметры **atucgsrsfastovrhdup и atucgsrsfastovrhddn** профиля ADSL интерфейса). Данный параметр измеряется в процентах и показывает, отношение количества избыточных RS байт к общему размеру буфера данных.
   Percent Overhead принимает значения -Disable,1,3,6,12,25,50.
   Например, для размера фрейма 65 и количества избыточных байтов 16, получаем Percent Overhead равное 25%.

   В случае Interleave режима доступно три параметра, влияющих на количество RS информации : Interleave Delay (параметры **atucmaxintldelay и aturmaxintldelay),** Correction Time (параметры **atucgsrsintcorrectionup и atucgsrsintcorrectiondn)** и Maximum Interleave Depth (параметр **atucgsmaxdco).**
   Maximum Interleave Depth принимает значения равные - 64,128,256.

   Исходя из этих параметров, количество RS байт подсчитывается автоматически.
   Например, для Depth= 64, Delay =16мс,Correction Time= 1ms и размера буфера 65, получаем количество избыточных байтов 16.
   Общее правило: чем больше Correction Time, и чем больше Interleaving Delay при неизменной Maximum Interleave Depth ,тем больше избыточность информации (количество RS байт).

4. Настройка инкапсуляции ATM/AAL5

Основные понятия ATM .

Asynchronous **T**ransfer **M**ode (ATM)- это метод передачи информации между устройствами в сети маленькими пакетами, называемыми ячейками (cells). ATM служит основной транспортной технологией в сетях ADSL.

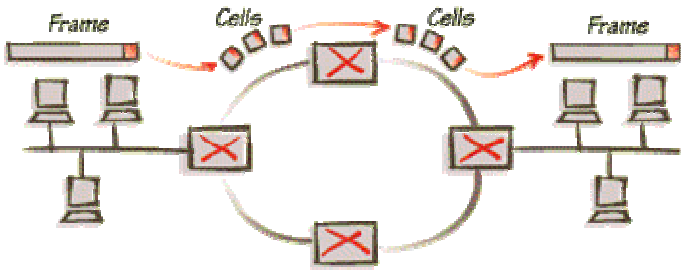


Рисунок 4-1

Все ячейки в ATM фиксированной длины - 53 байта. Ячейка состоит из двух частей: заголовка (cell header) размером 5 байт и поля данных (cell payload) размером 48 байт. Заголовок содержит информацию для маршрутизации ячейки в сети. Поле данных несет в себе полезную информацию, которую собственно и нужно передать через сеть.

Технология ATM способна передавать в поле данных ячеек абсолютно любую информацию. Для этого в ATM разработана концепция виртуальных соединений (virtual connection) вместо выделенных физических связей между конечными точками в сети.

Понятия виртуального канала и виртуального пути (VPI и VCI).

Коммутация пакетов в ATM происходит на основе идентификатора виртуального канала (Virtual Channel Identifier, VCI), который назначается соединению при его установлении и уничтожается при разрыве соединения. Адрес конечного узла ATM, на основе которого прокладывается виртуальный канал, имеет иерархическую структуру, подобную номеру в телефонной сети, и использует префиксы, соответствующие кодам стран, городов, сетям поставщиков услуг и т. п., что упрощает маршрутизацию запросов установления соединения.

Для ускорений коммутации в больших сетях используется понятие виртуального пути - Virtual Path, который объединяет виртуальные каналы, имеющие в сети ATM общий маршрут между исходным и конечным узлами или общую часть маршрута между некоторыми двумя коммутаторами сети. Виртуальный путь напоминает канал, содержащий множество кабелей, по каждому из которых может быть организовано виртуальное соединение. Идентификатор виртуального пути (Virtual Path Identifier, VPI) является старшей частью локального адреса и представляет собой общий префикс для некоторого количества различных виртуальных каналов. Таким образом, идея агрегирования адресов в технологии ATM применена на двух уровнях - на уровне адресов конечных узлов (работает на стадии установления виртуального канала) и на уровне номеров виртуальных каналов (работает при передаче данных по имеющемуся виртуальному каналу).

Поскольку виртуальные устройства подобны реальным, они также могут быть "выделенными" или "коммутируемыми". В сетях ATM "выделенные" соединения называются постоянными виртуальными соединениями (Permanent Virtual Circuit- PVC), создаваемыми по соглашению между пользователем и оператором (подобно выделенной телефонной линии). В сетях, построенных на основе технологии ADSL используются именно постоянные виртуальные соединения (PVC).

Стек протоколов ATM. Понятие AAL уровня.

ATM имеет трехуровневую модель, состоящую из следующих уровней:

- физического;
- уровня ATM;
- уровня адаптации ATM.

Функции каждого уровня стека протоколов ATM показаны на рисунке 4-2:

<table>
<tr><td colspan="3">Верхние уровни сети</td></tr>
<tr><td rowspan="2">Уровни адаптации ATM (ALL1-5)</td><td rowspan="2">Подуровень конвергенции (CS)</td><td>Общая часть подуровня конвенгенции</td></tr>
<tr><td>Специфическая для сервиса часть</td></tr>
<tr><td colspan="2">Подуровень сегментации и реассемблирования(SAR)</td></tr>
<tr><td colspan="3">Уровень ATM (маршрутизация пакетов, мультиплексирование, управление потоком, обработка приоритетов)</td></tr>
<tr><td rowspan="2">Физический уровень</td><td colspan="2">Подуровень согласования передачи</td></tr>
<tr><td colspan="2">Подуровень, зависящий от физической среды</td></tr>
</table>

Рисунок 4-2

Наиболее важным является уровень адаптации (ATM Adaptation Layer, AAL). Он представляет собой набор протоколов AAL1-AAL5, которые преобразуют сообщения протоколов верхних уровней сети ATM в ячейки ATM нужного формата. Протоколы AAL при передаче пользовательского трафика работают только в конечных узлах сети (см. рис 3), как и транспортные протоколы большинства технологий.

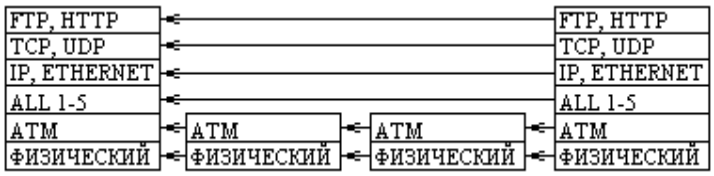


Рисунок 4-3

Уровень адаптации состоит из нескольких подуровней (см. рис.2). Нижний подуровень AAL называется подуровнем сегментации и реассемблирования (Segmentation And Reassembly, SAR). Эта часть не зависит от типа протокола AAL и занимается разбиением (сегментацией) сообщения, принимаемого AAL от протокола верхнего уровня, на ячейки ATM, снабжением их соответствующим заголовком и передачей уровню ATM для отправки в сеть. Верхний подуровень AAL называется подуровнем конвергенции - Convergence Sublayer, CS. Этот

подуровень зависит от класса передаваемого трафика. Протокол подуровня конвергенции решает такие задачи, как, например, обеспечение временной синхронизации между передающим и принимающим узлами (для трафика, требующего такой синхронизации), контроль и возможное восстановление битовых ошибок, контроль целостности передаваемого пакета.

Протоколы AAL для выполнения своей работы используют служебную информацию, размещаемую в заголовках уровня AAL. После приема ячеек, пришедших по виртуальному каналу, подуровень SAR протокола AAL собирает посланное по сети исходное сообщение с помощью заголовков AAL. После сборки исходного сообщения протокол AAL проверяет служебные поля заголовка и конца кадра AAL и на их основании принимает решение о корректности, полученной информации.

Ни один из протоколов AAL при передаче пользовательских данных конечных узлов не занимается восстановлением потерянных или искаженных данных. Максимум, что делает протокол AAL, - это уведомляет конечный узел о таком событии. Так сделано для ускорения работы сети ATM в расчете на то, что случаи потерь или искажения данных будут редкими. Восстановление потерянных данных (или игнорирование этого события) отводится протоколам верхних уровней, не входящим в стек протоколов технологии ATM.

Каждый протокол уровня AAL обрабатывает пользовательский трафик определенного класса.

Протокол AAL5 может поддерживать различные параметры качества обслуживания, кроме тех, которые связаны с синхронизацией передающей и принимающей сторон. Поэтому он обычно используется для всех классов трафика, относящегося к передаче компьютерных данных, т.е. трафик сетей, в которых конечные узлы работают по протоколам с установлением соединений (frame relay, X.25, LLC2, TCP) или без установления соединений (IP, Ethernet, DNS, SNMP).

Методы инкапсуляции данных в ATM.

Несмотря на всю сложность и разнообразность используемых решений в сетях доступа на основе ADSL, общая задача абонентских устройств доступа сводится к инкапсуляции трафика третьего (а иногда и второго) уровня в ячейки ATM для его последующей передачи по ADSL-соединению.

На противоположном конце соединения мультиплексор доступа (DSLAM) принимает потоки ячеек от отдельных абонентских устройств и агрегирует (мультиплексирует) их и декапсулирует (в случае IPDSLAM) поток данных для дальнейшей транспортировки в "восходящем" направлении - как правило, по магистральным каналам.

Выбор конкретного механизма инкапсуляции трафика канального и более высоких уровней модели OSI в ячейки ATM (точнее в кадры уровня AAL5 ATM) оказывает существенное влияние на стоимость, производительность, масштабируемость и простоту эксплуатации сети в целом. Наибольшее распространение получили следующие методы инкапсуляции:

(Более подробно они будут рассмотрены в соответствующих разделах, посвященных их настройке).

Легенда рисунков: Голубым цветом отмечены "родные" протоколы ATM, желтым – "вспомогательные" протоколы, обеспечивающие совместимость с программным

обеспечением, те или иные сервисы, оранжевым – этапы инкапсуляции этих протоколов в ATM:

- **EoA (Ethernet over ATM).** Регламентируется документом RFC1483 (RFC2684) в части, посвященной передачи по сети ATM коммутируемых (Bridged) протоколов.

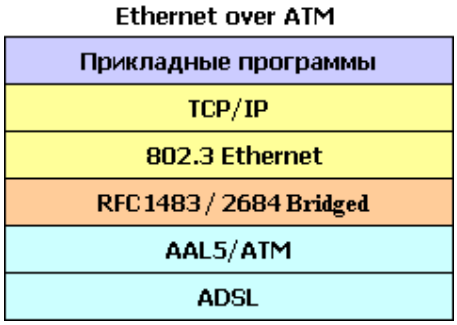


Рисунок 4-4

- **PPPoE over ATM.** Регламентируется документом RFC2516.

Рисунок 4-5

- **IPoA (IP over ATM).** Различаются два варианта реализации**:**

  a) Classical IPoA .Основной стандарт передачи IP поверх ATM. Регламентируется документом RFC 1577**.**

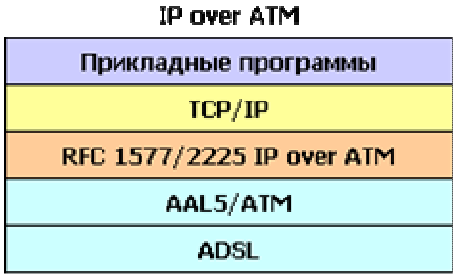


Рисунок 4-6

б) Routed IPoA (RFC1483 Routed). Регламентируется документом RFC1483 (RFC2684) в части, посвященной передаче по сети ATM маршрутизируемых (Routed) протоколов.

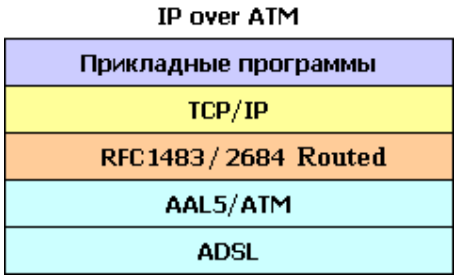


Рисунок 4-7

PPPoA (PPP over ATM). Регламентируется документом RFC 2364**.**

Рисунок 4-8

Понятие типа мультиплексирования.

К сожалению, AAL5 не обеспечивает мультиплексирование сессий (т.е. одновременную передачу данных нескольких протоколов сетевого уровня) внутри виртуального соединения ATM.

Поэтому для мультиплексирования данных используются дополнительные механизмы. Для каждого из методов инкапсуляции трафика в ячейки ATM существует **два** подхода к мультиплексированию данных по каналам ATM.

Первый метод заключается в мультиплексировании множества протоколов поверх **одного** виртуального канала ATM. Этот метод назван "**LLC Encapsulation**" (Logical Link Control).Общий механизм формирования и передачи пакетов протоколов сетевого уровня через виртуальное соединение при LLC инкапсуляции показан на рисунке 4-9

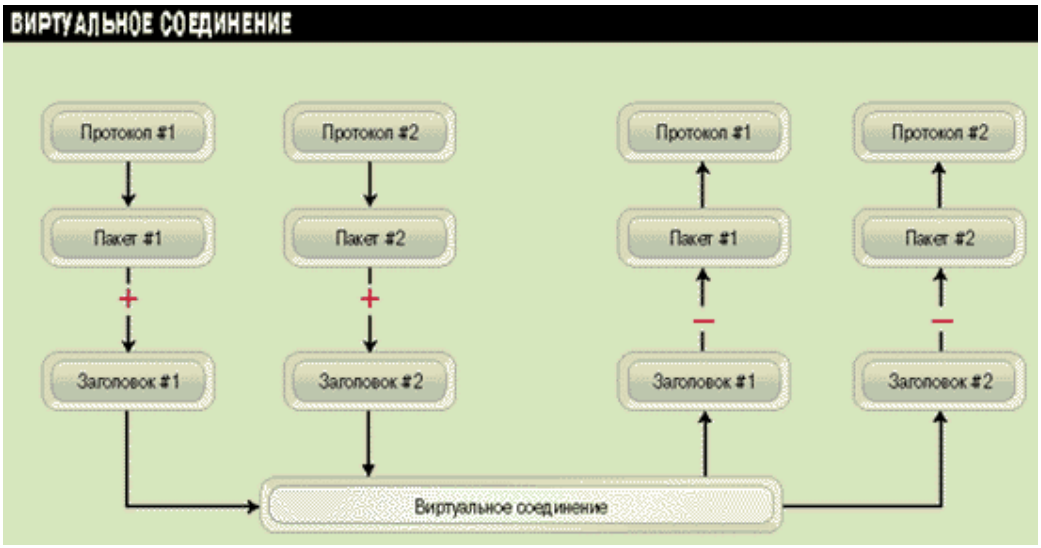


Рисунок 4-9

Этот метод используется наиболее часто в сетях на технологии ADSL и сконфигурирован в DAS-3248 по умолчанию.

Вторым методом является неявное мультиплексирование высокоуровневых протоколов виртуальными каналами ATM. Он называется мультиплексированием виртуальных соединений **multiplexing VC** (используется также аббревиатура **VC-Mux** (Virtual Channel based Multiplexing))или нулевой инкапсуляцией (Null encapsulation). Такой метод требует установления **множества** виртуальных соединений.

При таком методе через каждое виртуальное соединение передаются данные только одного протокола сетевого уровня, а тип протокола указывается при установлении соединения. В результате мультиплексирования и идентификации протокола не требуется. Такой метод может использоваться, например, когда приложения взаимодействуют напрямую, в обход протоколов нижних уровней.

Выбор конкретного метода инкапсуляции и режима мультиплексирования среди представленных выше, зависит от ADSL-провайдера, и с теоретической точки зрения является компромиссом между сложностью настройки и эффективностью работы с одной стороны и поддержкой имеющегося аппаратного и программного обеспечения – с другой.

4.1.Интерфейсы ATM.

Используются для управления ATM функционалом DAS-3248. Названия ATM интерфейсов лежат в диапазоне atm-0...atm-47. Интерфейс atm-0 соответствует 1-ому ADSL порту, atm-47 – сорок восьмому. ATM интерфейсы являются вышележащими над DSL интерфейсами и нижележащими для ATM VC интерфейсов.

create atm port
Описание: Используется для создания ATM порта.
Синтаксис команды: create atm port ifname interface-name **lowif** dsl-portinterface-name [enable | disable] [**Maxvpibits** maxvpibits][**Maxvcibits** maxvcibits] [**Orl** Orl]

modify atm port
Описание: используется для включения/выключения ATM порта.
Синтаксис команды: modify atm port ifname interface-name [enable | disable] [**maxvcs** maxvcs] [**Maxvpibits** maxvpibits] [**Maxvcibits** maxvcibits][**Orl** Orl]

delete atm port
Описание: используется для удаления ATM порта.
Синтаксис команды: delete atm port ifname interface-name

get atm port
Описание: используется для получения информации по одному *определенному ATM порту либо по всем ATM портам.*
Синтаксис команды: **get atm port [ifname** interface-name]

Таблица описания параметров команд:

ifname *ifname*	Имя DSL интерфейса, лежит в диапазоне dsl-0..dsl-47. **Обязательный параметр.**
lowif *dsl-port-interfacename*	Идентификатор DSL интерфейса, для которого настраивается ATM **Необязательный параметр.**
enable|disable	Статус ATM порта управления. **Необязательный параметр.**
Orl *orl*	Параметр определяет значение максимальной выходной скорости (в Кбит/с) для данного интерфейса. **Необязательный параметр.**
maxvcibits *max-vci-bits*	Максимальный номер идентификатора виртуального пути настроенного для ATM интерфейса.

	Значения параметров: от 1 до 8. **Необязательный параметр.**
maxvc *max-num-vccs*	Максимальный номер идентификатора виртуального пути (канала), поддерживаемого ATM интерфейсом. **Необязательный параметр.**
Maxvpibits *max-vpi-bits*	Максимальный номер идентификатора виртуального канала настроенного для ATM интерфейса. **Значения параметров:** от 1 до 16**.** **Значения по умолчанию:** 16.

Пример: $ get atm port ifname atm-0
Экранный вывод:

```
IfName: atm-0: gold 3                          LowIfName :
dsl-0
MaxVccs: 4                                     Class0thrshld :
MaxVpiBits : 9
RowStatus
Class1thrshld
Class0thrshld :UnknownVCI : 3
MaxVciBits : 10
Class0thrshld :Class1thrshld
Class0thrshld :
OAMSrc : 0xffffffffffffffffffffffffffffffff
ORL (kbps) : 64 02
Class2thrshld : 2
Active UnknownVPI : 2
ProfileName
Class3thrshld :
Oper Status : Up Up
Admin Status
```

4.2. Интерфейсы AAL5

AAL5 интерфейсы DAS-3224/3224/3248 предназначены для создания, настройки и удаления постоянных виртуальных соединений (PVC) ATM.

По умолчанию на DSLAM-е созданы 48 ATM VC интерфейсов (aal5-0...aal5-47) – на каждый ATM порт по одному VC. Имена данных PVC интерфейсов лежат в интервале: aal5-0 -aal5-47, где aal5-0 соответствует первому adsl порту, а aal5-47 – сорок восьмому.

DSLAM DAS-3248 поддерживает до 8 постоянных ATM соединений на один физический ADSL порт. В случае если предполагается использовать несколько PVC на одном ADSL порту, пользователь должен сам создать необходимые ему VC интерфейсы. Ему доступны для использования любые имена из диапазона aal5-48...aal5-383. Дублирование имен интерфейсов DAS-3248 запрещено.

С помощью настройки ATM PVC интерфейсов возможно также:

1. Задать идентификаторы постоянного виртуального соединения ATM
   Внимание: По умолчанию значения VPI -8,VCI-35. Убедитесь, что DSL модем клиента использует такие же параметры виртуального ATM соединения или измените их на используемые в вашей сети **идентично** на обоих устройствах.

2. Задать тип мультиплексирования (**llc, vcmux, auto**) .

3. Применить Input Rate Limiting (IRL).

4. Указать тип ADSL канала (**fast, interleave**). Для каждого VC интерфейса можно задать тип ADSL канала, по которому будут передаваться/приниматься ячейки данного PVC.
   Interleave - вносит задержку в передачу данных, но является более устойчивым к помехам (за счет применения помехоустойчивого кодирования).
   Fast - не вносит задержки в передачу данных, менее помехоустойчив.

4.2.1. Создание, настройка и удаление интерфейса AAL5

Для настройки AAL5 интерфейсов используются следующие команды CLI:

create atm vc intf

Описание**:** создает новый ATM VC.

Синтаксис команды:

create atm vc intf ifname *if-name* **vpi** *vpi* **vci** *vci* **lowif** *atm-port-interfacename*
[**enable | disable**] [**aal5**] [**a5txsize** *aal5-cpcs-tx-sdu-size*] [**a5rxsize** *aal5-cpcs-rx-sdu-size*] [**vcmux | llcmux | auto**] [**pvc**] [**channel** fast|interleaved]
[**mgmtmode** data|mgmt|DataAndMgmt| raw] **[maxnumproto** *maxnumproto*]
[**autostatus** Enable|Disable] [**autosupportedprot** none|{pppoa | eoa | ipoa}+]
[**autovcmuxforcedprot** None | pppoa | eoa | ipoa]
[**autosensetriggertype** dynamic |opstatechange]

Обратите внимание, что параметры, заключенные в квадратные скобки необязательны для заполнения.

Таблица описания параметров команд:

ifname *ifname*	имя ATM VC интерфейса, лежит в диапазоне aal5-0..aal5-383. **Обязательный параметр.**
vpi *vpi*	Virtual Path Identifier, Для того, чтобы изменить этот параметр, необходимо предварительно отключить данный VC интерфейс. Невозможно в одной команде одновременно изменить VPI и статус VC интерфейса. **Обязательный параметр.**
vci *vci*	Virtual Circuit Identifier, Для того, чтобы изменить этот параметр, необходимо предварительно отключить данный VC интерфейс. Невозможно в одной команде одновременно изменить VCI и статус VC интерфейса. **Обязательный параметр.**
lowif *atm-port-interfacename*	Имя ATM интерфейса, на котором будет создан данный VC интерфейс. **Обязательный параметр.**
enable | disable	Административный статус VC интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**
aal5	Тип AAL, используемый в VC. Поддерживается только AAL5. **Опциональный параметр. Значение по умолчанию** aal5**.**
a5txsize *aal5-cpcs-tx-sdu-size*	Максимальный размер передаваемого CPCS SDU. **Опциональный параметр. Значение по умолчанию** 1536**.**
a5rxsize *aal5-cpcs-rx-sdu-size*	Максимальный размер принимаемого CPCS SDU. **Опциональный параметр. Значение по умолчанию** 1536**.**
vcmux | llcmux | auto	Метод мультиплексирования. **Опциональный параметр. Значение по умолчанию** llcmux**.**
pvc	Тип PVC. Поддерживается только PVC. **Опциональный параметр. Значение по умолчанию** pvc**.**
channel fast|interleaved	Тип канала, по которому будут передаваться/приниматься ячейки данного PVC. **Опциональный параметр. Значение по умолчанию** interleaved**.**
mgmtmode data|mgmt|DataAndMgmt| raw	Определяет Management Mode данного ATM PVC. 1. **Data** - через данное PVC будет передаваться только data пакеты. 2. **Mgmt** – через данное PVC можно управлять CPE устройством. В случае Mgmt PVC поверх него не может быть создан EOA интерфейс. 3. **DataAndMgmt** – по одному ATM PVC

	может осуществляться как передача данных, так и управление удаленным CPE устройством. В этом режиме может использоваться только LLC мультиплексирование. **Опциональный параметр. Значение по умолчанию** Data.
maxnumproto *maxnumproto*	Максимальное число протоколов, одновременно поддерживаемых для данного PVC. **Опциональный параметр. Значение по умолчанию** 1**.**
Autostatus Enable|Disable	Режим автоконфигурирования стека протоколов верхнего уровня. **Опциональный параметр. Значение по умолчанию** Disable**.**
autosupportedprot none|{pppoa | eoa | ipoa}+	Список протоколов верхнего уровня доступных для автоконфигурирования. Данный параметр используется, если включен **Autostatus. Опциональный параметр. Значение по умолчанию.** pppoa eoa ipoa**.**
autovcmuxforcedprot None | pppoa | eoa | ipoa	Список протоколов верхнего уровня для PVC с VC-mux мультиплексированием доступных для автоконфигурирования. Данный параметр используется, если включен **Autostatus. Опциональный параметр. Значение по умолчанию** None**.**

Пример:
Команда для создания нового ATM VC LLC based поверх порта atm-23 (24 порт ADSL) с параметрами VPI 8, VCI 35:
create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-23

modify atm vc intf

Описание: изменяет параметры существующего ATM VC интерфейса.

Синтаксис команды:

modify atm vc intf ifname *ifname* **vpi** *vpi* **vci** [**enable | disable**]
[**a5txsize** *aal5-cpcs-tx-sdu-size*] [**a5rxsize** *aal5-cpcs-rx-sdu-size*] [**vcmux | llcmux | auto**]
[**mgmtmode** data|mgmt|DataAndMgmt| raw] [**autosupportedprot** none|{pppoa | eoa | ipoa}+]
[**autovcmuxforcedprot** None | pppoa | eoa | ipoa] [**autosensetriggertype** dynamic |opstatechange]

Внимание: Перед изменением любых параметров существующего ATM VC интерфейса необходимо его выключить

modify atm vc intf ifname aal5-51 disable

А после внесения всех необходимых изменений в конфигурацию VC необходимо включить его в работу
modify atm vc intf ifname aal5-51 enable

Пример**:**
Последовательность команд для изменения VPI и VCI ATM параметров интерфейса aal5-51- на новые значения (VPI 1, VCI 50):
modify atm vc intf ifname aal5-51 disable
modify atm vc intf ifname aal5-51 vpi 1 vci 50
modify atm vc intf ifname aal5-51 enable

delete atm vc intf

Описание**:** удаляет ATM VC интерфейс
Синтаксис команды:
delete atm vc intf ifname *ifname*

Пример**:**
команда удаления ATM VC интерфейса aal5-51
delete atm vc intf ifname aal5-51

get atm vc intf

Описание: просмотр статуса одного или всех ATM VC DAS-3248.
Синтаксис команды:
get atm vc intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** VC интерфейсов устройства**.**

Пример**:** Просмотр статуса интерфейса aal5-51
get atm vc intf ifname aal5-51

Экранный вывод:

VC IfName	:	aal5-51	Low IfName	:	atm-23
VPI	:	8	VCI	:	35
Admin Status	:	Up	Oper Status	:	Up
Aal5 Tx Size	:	1536	Aal5 Rx Size	:	1536
AAL Type	:	AAL5	AAL5 Encap	:	llcmux
Channel	:	Interleaved	Last Change (sec)	:	0
MgmtMode	:	Data	Row Status	:	Active
VC Type	:	PVC	VC Topology	:	Point to Point
Max simultaneous protocol			: 1		
Auto Status			: Disable		
Auto Supported Protocol			: pppoa eoa ipoa		
Auto VC Mux Forced Protocol			: None		
Auto Sense Trigger Type			: dynamic		
Auto Curr Sensed Encaps Type			: none		

4.3. RFC1483 Bridged. (Ethernet over ATM)

RFC1483 Bridged является одним из распространенных в ADSL-сетях методов инкапсуляции. Частным случаем RFC1483 Bridged является так называемая «мостовая схема». При ней модем играет роль интерфейса между ПК и линией ADSL. Он выполняет инкапсуляцию кадров Ethernet в ячейки ATM, а также осуществляет кодирование потоков данных перед их отправкой в линию (см. рис 4-10,4-11).
Стек протоколов Ethernet over ATM был изображен на рис.4-10.

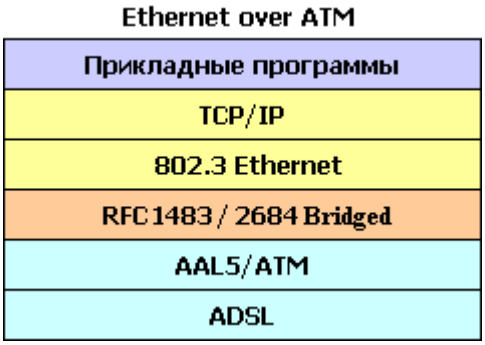


Рисунок 4-10

При передаче трафика по такой схеме используются функции моста, заголовки же третьего уровня не анализируются. Благодаря этому, модем может применяться для удаленного подключения сетей на базе Ethernet, в которых на третьем уровне задействуются протоколы, отличные от IP (в частности, IPX фирмы Novell).
Кроме того этот режим может быть использован для построения сети доступа на базе проткола PPPoE для прозрачной передачи пакетов от клиентских устройств к серверу авторизации PPPoE (BRAS- Broadband Remote Access Server).

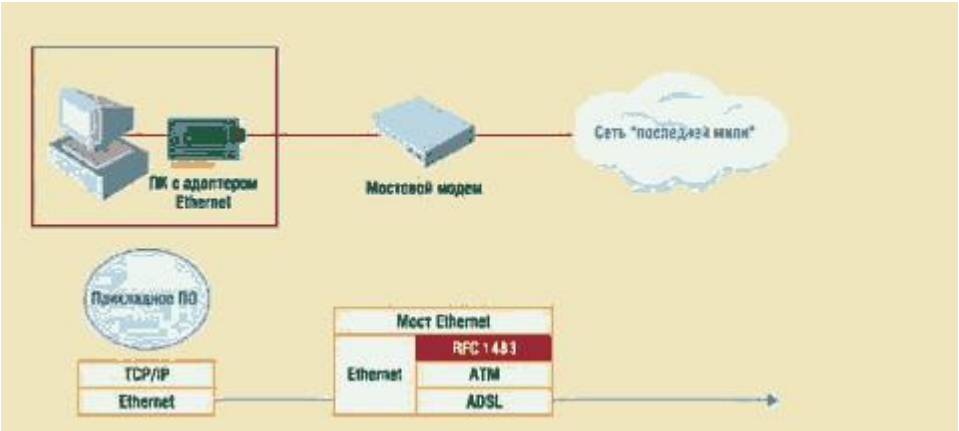


Рисунок 4-11

В соответствии со стеком EoA ,изображенным на рисунке 4-10, строится стек интерфейсов на DAS-3248, изображенный на рис.4-12.

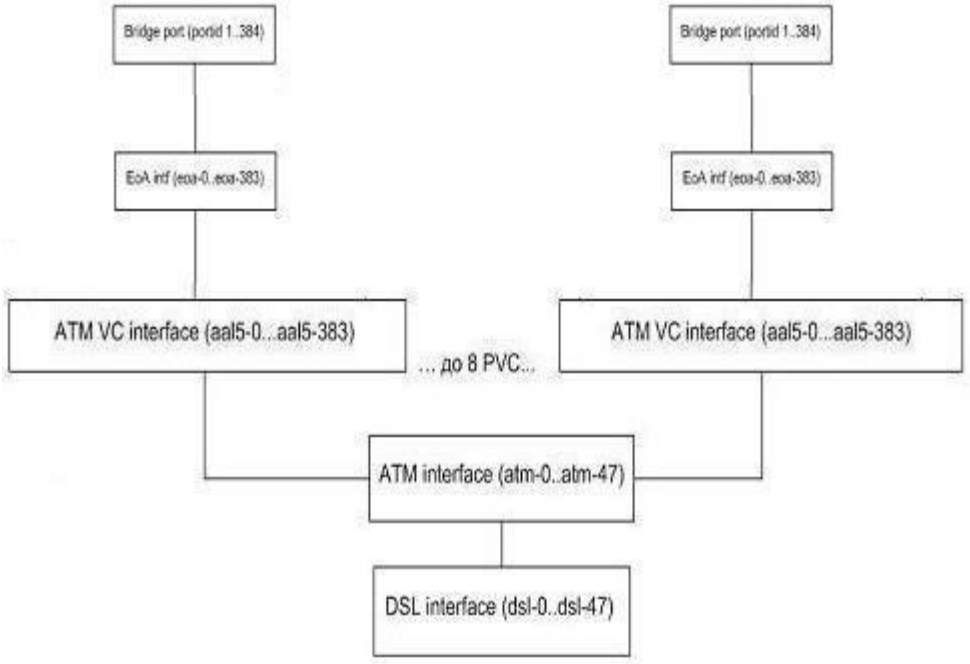


Рисунок 4-12

Внимание:
По умолчанию в сиситме уже созданы 48 EoA интерфейсов с именами eoa-0...eoa-47 (поверх каждого ATM VC).
Кроме того, поверх каждого из интерфейсов EoA создан Bridge интерфейс.
Таким образом, RFC1483 Bridged уже настроен по умолчанию на DAS-3248 и изменять конфигурацию нет необходимости.

Если же необходимо поднять второе логическое соединение поверх ADSL (используя второй VC AAL5 интерфейс), то необходимо создать стек интерфейсов, согласно рис.12, начиная с ATM VC интерфейса.
То есть:

1) Создать ATM VC интерфейс;
2) Создать EoA интерфейс;
3) Создать Bridge интерфейс.

Пример:
create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-23
create eoa intf ifname eoa-51 lowif aal5-51
create bridge port intf ifname eoa-51 portid 52 learning enable status enable

4.3.1. Создание, настройка и удаление интерфейса EoA

EoA – логический интерфейс, лежащий поверх ATM PVC интерфейса и использующийся при инкапсуляции RFC 2684 (прежнее название RFC 1483) for Bridged Protocols. Имена EoA интерфейсов лежат в диапазоне eoa-0..eoa-383. По умолчанию созданы 48 EoA интерфейсов с именами eoa-0...eoa-47 (поверх каждого ATM VC).
Для данного интерфейса можно задать тип поддерживаемого Ethernet трафика: Multicast, Broadcast, Unicast, Unknown unicast.

Для настройки EoA интерфейсов используются следующие команды CLI:

create eoa intf

Описание: создает новый EoA интерфейс.

Синтаксис команды:

create eoa intf ifname *ifname* **lowif** *lowif* **[pkttype {**multicast |broadcast |unknown-unicast**}+ |** all**]** **[fcs** false | true**][**enable|disable**]** **[inactivitytmrintrvl** *inactivitytmrintrvl*]**[configstatus** normal | config**]**

Таблица описания параметров команд:

ifname *ifname*	имя EoA интерфейса, лежит в диапазоне eoa-0..eoa-383. **Обязательный параметр.**
lowif *lowif*	Имя AAL5 интерфейса, на котором будет создан данный EoA интерфейс. **Обязательный параметр.**
[pkttype {multicast |broadcast |unknown-unicast**}+ | all | none**	Определяет тип трафика, разрешенный к передаче через данный интерфейс. 1.**Multicast**- только групповой. 2.**Broadcast**- только широковещательный. 3.**Unknown-unicast**- только неизвестный юникаст трафик. 4.**None**-только юникаст трафик от известных адресов. 5 .**All**-любой (включает все предыдущие типы).

	Опциональный параметр. Значение по умолчанию All.
fcs false| true	Определяет, будет, проверятся поле FCS (Frame Check Sequence) контрольная сумма кадра Ethernet. **Поддерживается только** false**.** **Опциональный параметр.**
enable | disable	Административный статус EoA интерфейса. **Опциональный параметр.** **Значение по умолчанию** enable**.**
inactivitytmrintrvl *inactivitytmrintrvl*	Определяет тайм-аут (в секундах), по истечению которого если через интерфейс не проходят данные, он помечается как неактивный. Значение 0 означает, что таймер выключен. Связан с настройкой **configstatus** EoA интерфейса и имеет смысл только в случае **configstatus Config.** **Опциональный параметр.** **Значение по умолчанию 0.**
configstatus Normal | Config	Определяет**,** является ли EoA интерфейс активным по требованию. **Normal**- интерфейс активен всегда. **Config**- интерфейс находится в неактивном состоянии после включения и активизируется олько после приема первого IPoA пакета от CPE. **Опциональный параметр.** **Поддерживается только значение** Normal. **Значение по умолчанию** Normal.

Пример:
Команда для создания eoa интерфейса поверх интерфейса aal-51.
create eoa intf ifname eoa-51 lowif aal5-51 enable

modify eoa intf

Описание**:** изменяет параметры существующего EoA интерфейса.

Синтаксис команды :

modify eoa intf ifname *ifname* **[pkttype {**multicast |broadcast |unknownunicast**}+|** all| none**]** **[fcs** false | true**][**enable|disable**] [inactivitytmrintrvl** *inactivitytmrintrvl***]**

Пример:
Команда для изменения параметра **pkttype** интерфейса eoa-51 на новые значения (pkttype bcast):
modify eoa intf ifname eoa-51 pkttype bcast

delete atm eoa intf

Описание: удаляет EoA интерфейс
Синтаксис команды**:**
delete eoa intf ifname *ifname*

Пример:
команда удаления EoA интерфейса eoa-51
delete eoa intf ifname eoa-51

get eoa intf

Описание: просмотр статуса одного или всех EoA интерфейсов DAS-3248.
Синтаксис команды:
get eoa intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** EoA интерфейсов устройства**.**

Пример: Просмотр статуса интерфейса eoa-51
get eoa intf ifname eoa-51

Экранный вывод:

```
IfName          :eoa-51        LowIfName       :aal5-51

FCS             :False

Pkt Type    : ALL
```

4.3.2. Создание, настройка и удаление bridge порта

Bridge port являются вершиной стека интерфейсов DAS-3248 и отвечают за Layer 2 forwarding. Bridge ports позволяют:

5. Создать соответствие ATM VC <-> VLAN. Причем в один VLAN можно включать несколько VC и один VC можно включать в несколько VLAN.

6. Включить блокировку и/или мониторинг клиентских MAC адресов.
7. Выставить 802.1p приоритет всем входящим пакетам.
8. Настроить соответствие между выходными очередями и значением приоритета.

Имена bridge портов (portid) лежат в интервале от 1 до 384 для eoa, pppoe и ipoe интерфейсов.

Для настройки Bridge интерфейсов используются следующие команды CLI:

create bridge port intf

Описание: создает новый Bridge интерфейс.

Синтаксис команды:

create bridge port intf portid *portid* **ifname** *ifname* **[maxucast** *maxucast-addresses* **]** [**learning** enable|disable][**status** enable|disable] [**stickystatus** enable | disable] [**fdbmodify** enable | disable][**aclGlbDenyApply** enable | disable] [**aclGlbTrackApply** enable |disable]

Таблица описания параметров команд:

portid *portid*	Идентификатор Bridge port, лежит в диапазоне1–384. **Обязательный параметр.**
ifname *ifname*	Имя интерфейса, на котором будет создан данный Bridge интерфейс. **Обязательный параметр.**
maxucast *maxucast-addresses*	Определяет максимальное количество MAC адресов, которому может быть обучен данный Bridge порт. **Опциональный параметр. Значение по умолчанию** 16.
learning enable|disable	Включает и выключает режим обучения MAC адресам. **Опциональный параметр. Значение по умолчанию** enable**.**
status enable|disable	Административный статус Bridge интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**
stickystatus enable | disable	Включает режим постоянной привязки MAC адресов к bridge порту. В состояние **enable** запись о MAC адресе не устаревает, поэтому однажды обученный определенному MAC

	адресу, порт сохраняет запись и не дает «обучится» данному MAC другой порт. Запись о MAC может быть стерта административным выключением интерфейса или переводом данной настройки в состояние **disable**(по истечению таймаута) В состоянии **disable** запись о MAC устаревает через некоторое время, поэтому другой bridge port может «обучится» MAC через определенное время (по таймауту) **Внимание** : При использовании режима sticky необходимо выключить floodsupport (для запрещения ходжения пакетов от неизвестных источников) глобально командой **$modify bridge tbg info floodsupport disable** Или на отдельном VLAN : **$modify vlan static vlanid xx floodSupport disable.** **Опциональный параметр. Значение по умолчанию** disable**.**
fdbmodify enable | disable	Определяет, может ли порт самостоятельно изменять базу данных MAC адресов (fdb) **Опциональный параметр. Значение по умолчанию** enable**.**
aclGlbDenyApply enable | disable	Определяет, может ли «черный» глобальный список запрещенных MAC адресов, созданных командой CLI **create global acl macentry deny** быть применен к данному bridge порту или нет. **Enable**- глобальный список применим к порту. **Disable**- не применим. **Опциональный параметр. Значение по умолчанию** enable**.**
aclGlbTrackApply Enable | Disable	Определяет, может ли глобальный список MAC адресов, за которыми включено «слежение» (протоколирование перехода MAC с порта на порт), созданных командой CLI **create global acl macentry track,** быть применен к данному bridge порту или нет.

	Enable- глобальный список применим к порту. **Disable**- не применим. **Опциональный параметр. Значение по умолчанию** enable**.**

Пример:
Команда для создания bridge интерфейса с portid 52 поверх интерфейса eoa-51.
create bridge port intf ifname eoa-51 portid 52 learning enable status enable

modify bridge port intf

Описание: изменяет параметры существующего Bridge интерфейса.
Синтаксис команды:

modify bridge port intf portid *portid* **[maxucast** *max-ucast-addresses* **] [learning** enable|disable][**status** enable|disable**] [stickystatus** enable | disable**][fdbmodify** enable | disable**][aclGlbDenyApply** enable | disable **][aclGlbTrackApply** enable | disable **]**

Пример:
Команда для изменения параметра learning bridge интерфейса с portid 52 на новые значения (leaning enable):
modify bridge port intf portid 52 learning disable

delete bridge port intf

Описание: удаляет bridge интерфейс
Синтаксис команды:

delete eoa intf portid *portid*

Пример:
команда удаления Bridge интерфейса с portid 52
delete bridge port intf portid 52

get bridge port intf

Описание: просмотр статуса одного или всех Bridge интерфейсов DAS-3248.
Синтаксис команды:

get bridge port intf [portid *portid***]**

Внимание: В случае если **portid** явно не указан в команде, выводится состояние **всех** EoA интерфейсов устройства**.**

Пример: Просмотр статуса bridge интерфейса с portid 52
get bridge port intf portid 52

Экранный вывод:

Port Id : 52	IfName : eoa-51
Max Unicast Addresses : 16	Learning Status : Enable
Port Oper Status : Disable	Port Admin Status: Enable
Sticky Status : Disable	FDB Modify : Enable
Acl Global Deny Apply : Enable	
Acl Global Track Apply: Enable	
Sensed IfIndex : -	

4.4. Point-to-Point over ATM (PPPoA)

Для авторизации пользователей провайдерами традиционно используется протокол PPP (протокол точка-точка) и его расширение для Ethernet (PPPoE), Он представляет широкие возможности и удобные механизмы авторизации, алгоритмы динамического присвоения IP-адресов, назначения DNS и других параметров стека TCP/IP и так далее.
Поэтому появились соответствующие виды инкапсуляции (PPPoA и PPPoE over ATM), описанные в документах RFC2364 и RFC2516 соответственно.
Стеки для данных видов инкапсуляции изображены на рис.13 и 14.

Рисунок 13

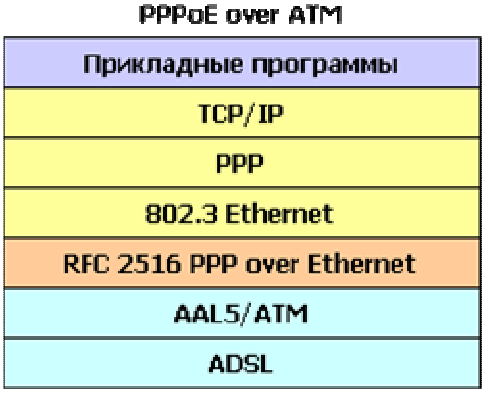


Рисунок 14

В DAS-3248 инкапсуляция PPPoA напрямую не используется, поскольку DSLAM не является конечным участником PPPoE туннеля (PPPoE клиентом или PPPoE сервером), а призван лишь обеспечить прохождение Ethernet пакетов.

PPPoE тоннель поднимает между клиентом (DSL-модемом) и BRAS (Broadband Remote Access Server). Пример схемы организации сети доступа на основе PPPoE показан на рис.4-15.

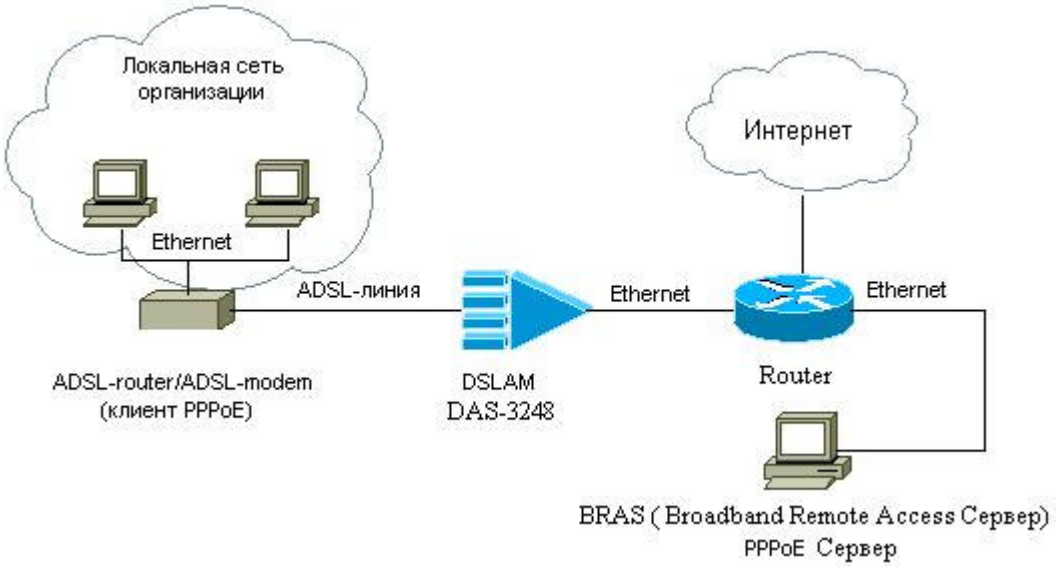


Рисунок 4-15

Однако PPPoA используется для настройки функции PPPoA to PPPoE internetworking, которая призвана обеспечить прозрачную миграцию с традиционных ATM-based DSLAM-ов на IP решения.

Во время перехода с ATM на Ethernet/IP возможна следующая ситуация: часть сети будет оставаться ATM-based с используемым протоколом PPPoA, а часть – Ethernet/IP based и протоколом PPPoE. Технология PPPoA to PPPoE internetworking позволяет средствами DSLAM-а преобразовать PPPoA пакеты от CPE в пакеты PPPoE и послать их на BRAS. Подробнее о PPPoA to PPPoE internetworking читайте в рекомендации DSL Forum TR-101.

4.4.1. Описание и особенности реализации PPPoA to PPPoE internetworking

Данная процедура позволяет IP DSLAM DAS-3248 принимать от ADSL CPE устройства PPPoA пакеты, преобразовывать их в пакеты PPPoE и передавать на внешний Broadband Remote Access Server (BRAS).

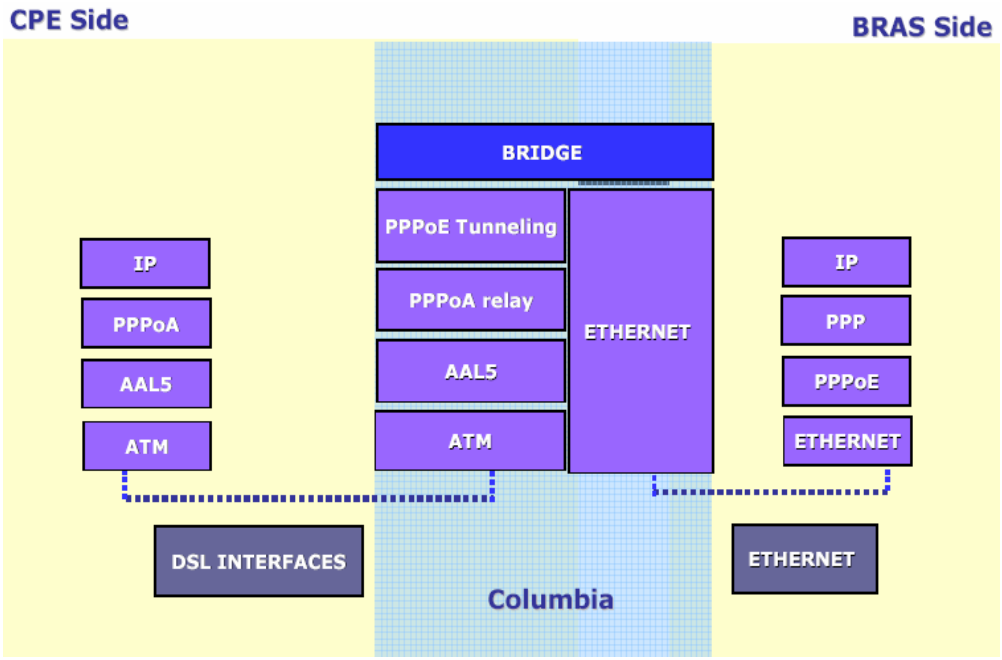


Рисунок 4-16: Стек протоколов для PPPoA to PPPoE Internetworking

Особенности реализации PPPoA to PPPoE internetworking на DAS-3248:

- Динамическое создание PPPoE сессии с BRAS для каждого PPPoA интерфейса.
- PPPoE сессия создается после получения первого PPPoA пакета от CPE, обычно это LCP пакет.
- Туннелирование всех PPPoA пакетов (Data и Control) поверх PPPoE сессии до BRAS.
- Настраиваемый MAC адрес, с которого DAS-3248 будет устанавливать PPPoE сессию к BRAS. Один MAC адрес может использоваться при терминировании нескольких PPPoA соединений. В этом случае для обратного преобразования PPPoE пакетов в PPPoA при отсылке их в сторону CPE используется идентификатор PPPoE сессии.
- В направлении Upstream к исходному PPPoA пакету при инкапсулировании его в кадр ethernet добавляется следующая информация:
  Source MAC address (конфигурируется для каждого PPPoA интерфейса)
  Destination MAC address (MAC адрес BRAS)
  VLAN tag (используется значение для bridge port ,ассоциированного с данным PPPoE интерфейсом)
  EtherType
  Session ID – идентификатор PPPoE сессии
- В направлении downstream обратное декапсулирование производится по Destination MAC address, VLAN ID, Source MAC address и Session ID
- Важно понимать, что комбинация 4-х параметров, перечисленных выше, должна быть уникальна.

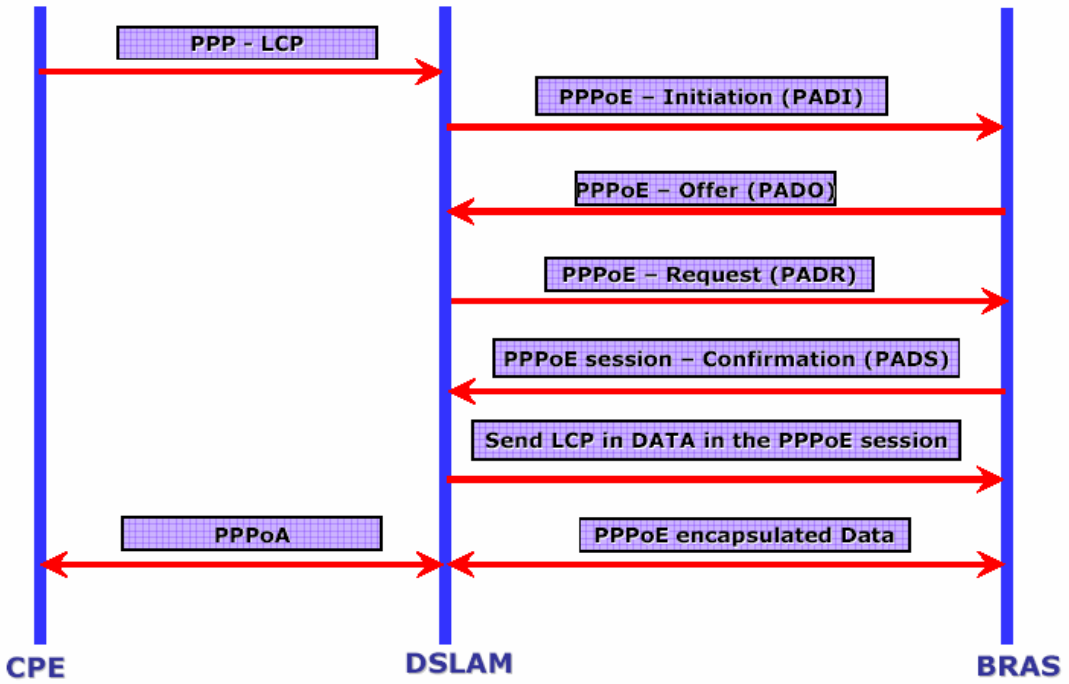


Рисунок 4-17: Инициирование PPPoA to PPPoE

Стек интерфейсов DAS-3248 PPPoA изображен на рис.4-18.

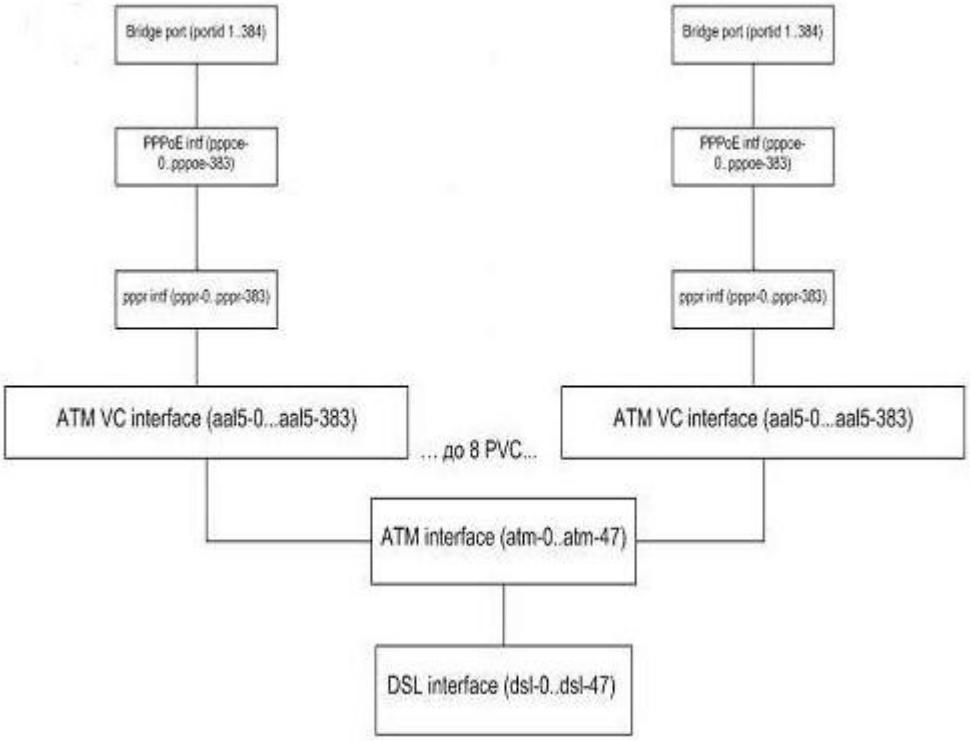


Рисунок 4-18

Логические интерфейсы, используемые для PPPoA to PPPoE internetworking:

- PPPoA relay interface – данный интерфейс настраивается над ATM PVC (AAL5) интерфейсом и отвечает за PPPoA функционал. В основном это передача ppp пакетов PPPoE интерфейсу и отслеживание статуса PPPoA сессии.
- PPPoE tunnel interface – данный интерфейс преобразует PPP пакеты, полученные от нижележащего интерфейса PPPoA, в пакеты PPPoE. Динамически устанавливает PPPoE сессию с BRAS и осуществляет наблюдение за статусом этой сессии.
- Bridge Port – настраивается над PPPoE интерфейсом, связывает PPPoA to PPPoE туннелирование с VLAN.

4.4.2.Создание, настройка и удаление интерфейса PPPoA Relay

Имена PPPR (PPPoA relay) интерфейсов лежат в диапазонах pppr-0...pppr-383.

create pppr intf

Описание: создает новый PPPR интерфейс.

Синтаксис команды:

create pppr intf ifname ifname **lowif** lowif

[maxpdu *maxpdu* **] [ppprackto** *ppprackto***]**
[lowiftoggletimerto *lowiftoggletimerto* **] [nature** dynamic | static **]**
[configstatus Normal | Config **] [**enable | disable**]**

Таблица описания параметров команд:

ifname *ifname*	имя PPPR интерфейса, лежит в диапазоне pppr-0..pppr-383. **Обязательный параметр.**
lowif *lowif*	Имя AAL5 интерфейса, на котором будет создан данный PPPR интерфейс. **Обязательный параметр.**
maxpdu *maxpdu*	Максимальный размер блока данных ATM PDU (Protocol Data Unit) **Опциональный параметр. Значение по умолчанию** 1492**.**
ppprackto *ppprackto*	Время в секундах, в течение которого интерфейс pppr ожидает прием подтверждения о завершении сессии передачи (LCP Terminate Ack).Пакет LCP типа Terminate-Ack используется сервером PPP для уведомления клиента о том, что его запрос на завершение сеанса PPP получен. Когда сервер PPP принимает пакет типа Terminate-Request, он должен ответить на него пакетом типа Terminate-Ack и инициировать завершение соединения. По истечению **ppprackto** посылается повторный перезапрос (Terminate-Request) о завершение сессии. **Опциональный параметр**.
lowiftoggletimerto *lowiftoggletimerto*	Время в секундах, в течение которого интерфейс не обрывает PPP сессию, если нижележащий интерфейс (AAL5) Переходит в состояние Down. По истечению этого интервала ppp сессия разрывается. **Опциональный параметр**.
nature dynamic | static	Определяет, является ли интерфейс статическим или динамическим .

	Dynamic-динамический Static-статический.
configstatus Normal | Config	Определяет**,** является ли EoA интерфейс активным по требованию. **Normal**- интерфейс активен всегда. **Config**- интерфейс находится в неактивном состоянии после включения и активизируется только после приема первого PPPoA пакета от CPE. **Опциональный параметр.** **Поддерживается только значение** Normal. **Значение по умолчанию** Normal.
enable | disable	Административный статус EoA интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**

Пример:
Команда для создания pppr интерфейса поверх интерфейса aal5-51.
create pppr intf ifname pppr-51 lowif aal5-51 enable

modify pppr intf

Описание: изменяет параметры существующего PPPR интерфейса.
Синтаксис команды:

modify pppr intf ifname ifname **[ppprackto** *ppprackto* **] [lowiftoggletimerto** *lowiftoggletimerto* **] [nature** dynamic | static **] [**enable | disable**]**

Внимание: Перед изменением любых параметров существующего PPPR интерфейса необходимо его выключить

modify pppr intf ifname pppr-51 disable

А после внесения всех необходимых изменений в конфигурацию PPPR необходимо включить его в работу
modify pppr intf ifname pppr-51 enable

Пример:

Последовательность команд для изменения параметра интерфейса **ppprackto** pppr-51 на новое значение:
modify pppr intf ifname pppr-51 disable
modify pppr intf ifname pppr-51 ppprackto 10

modify pppr intf ifname pppr-51 enable

delete atm eoa intf

Описание: удаляет PPPR интерфейс

Синтаксис команды:

delete pppr intf ifname *ifname*

Пример:

команда удаления PPPR интерфейса eoa-51

delete pppr intf ifname pppr-51

get pppr intf

Описание: просмотр статуса одного или всех PPPR интерфейсов DAS-3248.

Синтаксис команды**:**

get pppr intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** PPPR интерфейсов устройства**.**

Пример: Просмотр статуса интерфейса pppr-51

get pppr intf ifname pppr-51

4.4.3.Создание, настройка и удаление интерфейса PPPoE

Имена PPPoE интерфейсов лежат в диапазонах pppoe-0...pppoe-383.

create pppoe intf

Описание: создает новый PPPoE интерфейс.

Синтаксис команды:

create pppoe intf ifname ifname **lowif** lowif **[wanbridgeport** *wanbridgeport* **] [sessionid** *sessionid* **] [acmacaddr** *acmacaddr* **] macaddrprof** *macaddrprof* [**servicenameprof** *servicenameprof*] [**acnameprof** *acnameprof*] [**ethpkttype** type2 | 802_3] [**nature** dynamic | static] [enable | disable]

Таблица описания параметров команд:

ifname *if-name*	имя PPPoE интерфейса, лежит в диапазоне pppoe-0..ppoe-383. **Обязательный параметр.**
lowif *lowif*	Имя PPPR интерфейса, на котором будет создан данный PPPoE интерфейс. **Обязательный параметр.**
wanbridgeport *wanbridgeport*	Определяет WAN bridge порт, привязанный к инетерфейсу.0 означает, что доступен любой bridge порт. **Поддерживается только значение 0.** **Опциональный параметр.** **Значение по умолчанию** 0**.**
sessionid *sessionid*	Идентификатор сессии pppoe (session id).Данный параметр принимается только в случае статической сессии pppoe. **Опциональный параметр.** **Диапазон значений** 0-65535**.** **Значение по умолчанию** 0**.**
acmacaddr *acmacaddr*	AC (Access Concentrator) MAC- MAC адрес BRAS сервера, который будет использовать DAS-3248 для установления PPPoE сессии. **Опциональный параметр.**
macaddrprof *macaddrprof*	Profile id (идентификатор профиля), в котором указан MAC адрес интерфейса DAS-3248 для установления PPPoE сессии. **Обязательный параметр**
servicenameprof *servicenameprof*	Profile id (идентификатор профиля), в котором указано Service Name (имя сервиса) BRAS сервера, который будет использоваться DAS-3248. Значение *any* обозначает, что нет необходимости использовать AC Name. Значение *anyconfigured* означает, что любое значение AC будет принято. **Опциональный параметр.** **Значение по умолчанию** any
acnameprof *acnameprof*	Profile id (идентификатор профиля), в котором указано AC Name (Access Concentrator Name)- имя BRAS сервера, которое будет использоваться

	DAS-3248**.** Значение *any* обозначает, что нет необходимости использовать AC Name. Значение *anyconfigured* означает, что любое значение AC будет принято **Опциональный параметр.** **Значение по умолчанию** any
ethpkttype type2 ǀ 802_3	Определяет тип передаваемых пакетов Ethernet (**802.3** или **Type2**). **Опциональный параметр.**
nature dynamic ǀ static	Определяет, является ли интерфейс статическим или динамическим. Dynamic-динамический Static-статический. **Опциональный параметр.**
enable ǀ disable	Административный статус EoA интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**

Пример:

Последовательность команд для создания pppoe интерфейса поверх интерфейса pppr-51.

Задаем профиль, в котором указан MAC адрес, который будет использовать DAS-3248 для установления PPPoE сессии.

create pppoe global macprofile profileid 1 macaddr 00:0E:7F:61:C1:BE

Непосредственно создаем интерфейс.

create pppoe intf ifname pppoe-51 lowif pppr-51 macaddrprof 1 enable

modify pppoe intf

Описание: изменяет параметры существующего PPPoE интерфейса.

Синтаксис команды:

modify pppoe intf ifname *ifname* **[wanbridgeport** *wanbridgeport* **] [sessionid** *sessionid* **] [acmacaddr** *acmacaddr* **] [macaddrprof** *macaddrprof* **]** [**servicenameprof** *servicenameprof*] [**acnameprof** *acnameprof*] [**ethpkttype** Type2ǀ 802_3] [**nature** dynamic ǀ static **] [enableǀdisable]**

Пример:

Команда для изменения параметра **nature** интерфейса pppoe-51 на новые значения (**nature static**):

modify pppoe intf ifname pppoe-51 nature static

delete atm eoa intf

Описание: удаляет PPPoE интерфейс
Синтаксис команды:

delete pppoe intf ifname *ifname*

Пример:
команда удаления EoA интерфейса pppoe-51
delete pppoe intf ifname pppoe-51

get pppoe intf

Описание: просмотр статуса одного или всех PPPoE интерфейсов DAS-3248.
Синтаксис команды:

get pppoe intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** PPPoE интерфейсов устройства**.**

Пример: Просмотр статуса интерфейса pppoe-51
get pppoe intf ifname pppoe-51

4.4.4.Создание, настройка и удаление bridge-порта

Bridge порт настраивается аналогично другим инкапсуляциям (см. выше раздел о RFC1483 Bridged), приведенным выше, только в качестве **ifname** интерфейса, на базе которого создается bridge порт, указывается pppoe интерфейс.
Пример:
create bridge port intf ifname pppoe-51 portid 52 learning enable status enable

4.3.5. Пример настройки PPPoA to PPPoE internetworking

	Команда	Действие
Шаг 1	$create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-23	Создать новый ATM VC интерфейс поверх 24 ADSL порта с параметрами VPI 8, VCI 35
Шаг 2	$create pppr intf ifname pppr-51 lowif aal5-51	Создать PPPoA Relay интерфейс непосредственно над AAL5 интерфейсом:
Шаг 3	$ create macprofile global profileid 1 macaddr 00:0E:7F:61:C1:BE	Указызать MAC адрес, который будет использовать DAS-3248 для установления PPPoE сессии:
Шаг 4	$create pppoe global serviceprofile profileid 1 servicename ISP1	Указать Service Name, который будет использоваться DAS-3248

		(необязательный параметр)
Шаг 5	$create pppoe intf ifname pppoe-51 lowif pppr-51 servicenameprof 1 macaddrprof 1	Создать PPPoE интерфейс
Шаг 6	$create filter rule entry ruleid 2 action sendtocontrol ruledir in applywhenreq enable description PPPR_CONTROL	Создать правило Generic фильтра так, чтобы все пакеты LCP передавались управляющему процессу. Это необходимо для обнаружения PPPoA сессии со стороны CPE.
Шаг 7	create filter subrule ppp ruleid 2 subruleid 1 prototypefrom 0xc021 prototypecmp eq	Создать подправило с указанием LCP протокола (тип протокола 0xC021)
Шаг 8	modify filter rule entry ruleid 2 status enable	Включить созданное правило
Шаг 9	create filter rule map ifname allpppoe stageid 1 ruleid 2	Привязать данное правило ко всем PPPoE интерфейсам
Шаг 10	create bridge port intf portid 52 ifname pppoe-51	Создать bridge port поверх ранее созданного PPPoE интерфейса
Шаг 11	$modify pppr intf ifname pppr-51 enable $modify pppoe intf ifname pppoe-51 enable $modify bridge port intf portid 52 status enable	Включить PPPoE, PPPR и bridge port в работу

4.5. IP over ATM

В настоящее время имеется два способа передачи IP трафика по сетям ATM: Classical IPoA (RFC1577) и Routed IPoA (RFC1483 Routed).

Технология Routed IPoA описана в документах RFC1483/RFC2684 в части, посвященной передачи трафика маршрутизируемых протоколов.

В данном случае кадры IP поверх ATM представляют из себя простую инкапсуляцию IP пакетов в AAL5 PDU, которые затем передаются по ATM PVC.

Стек протоколов для Routed IPoA изображен на рис.4-20

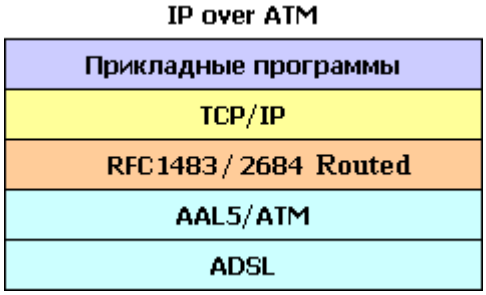


Рисунок 4-20

DAS-3248 сам непосредственно не проводит инкапсуляцию IPoA , поскольку является устройством второго уровня.
Однако IPoA используется в применении к IPoA to IPoE internetworking, которая призвана обеспечить совместимость с Routed IPoA интерфейсами на CPE устройствах Данная процедура позволяет IP DSLAM DAS-3248 принимать от ADSL CPE устройства IPoA пакеты, преобразовывать их в пакеты IPoE и передавать на внешний Broadband Remote Access Server (рис.4-21).

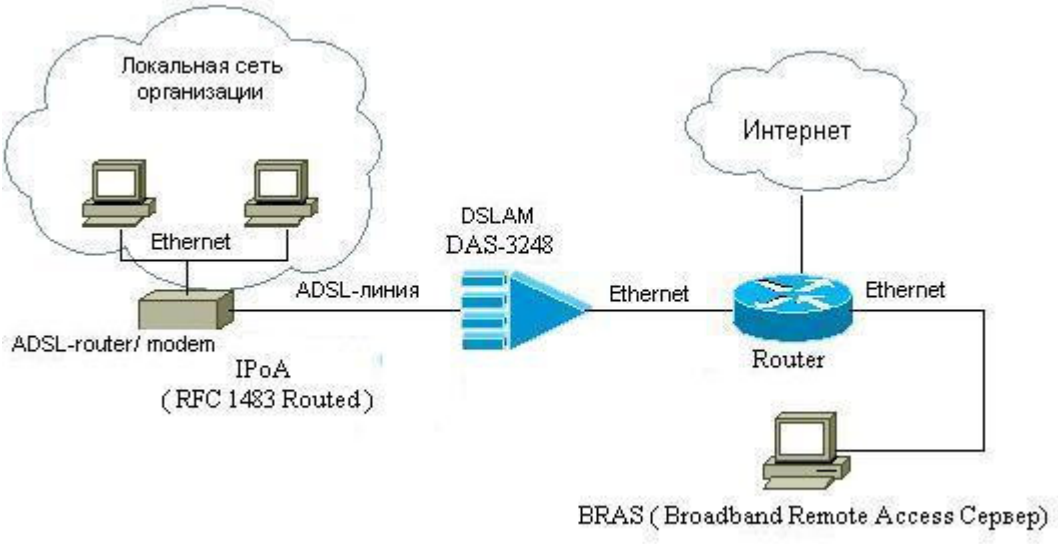


Рисунок 4-21

4.5.1. Описание IPoA to IPoE internetworking

Существующие в настоящее время на рынке абонентские устройства (CPE) часто имеют IPoA интерфейсы. Эти интерфейсы нуждаются в поддержке их сервисами Интернет-провайдеров. Кроме того, провайдеры в настоящее время имеют тенденцию перехода от ATM к IP решениям, поэтому поддержка таких интерфейсов становится особенно важна. Именно поэтому DAS-3248 поддерживает наряду с существующими RFC 2684 Bridged интерфейсами, также и IPoA (RFC2684Routed) интерфейсы.

Поскольку DAS-3248 по существу мост, прямая поддержка маршрутизируемых интерфейсов

здесь не применима. Технология IPoA to IPoE Tunneling обеспечивает терминирование IPoA трафика на ADSL интерфейсах устройства и туннелирование его к Ethernet интерфейсам DAS-3248 в восходящем (Upstream) направлении.

Для нисходящего трафика (Downstream) поддерживается два варианта перенаправления потока:
1) на основе IP адреса – IP address lookup, который используется для маршрутизации трафика на IPoE интерфейс (L3 Forwarding).
2) на основе MAC address / VLAN – MAC/ VLAN lookup (L2 Forwarding).

Upsteam трафик, протекающий от DSL к Ethernet интерфейсам DAS-3248, показан на рисунке 4-22 жирной стрелкой, начинающейся на CPE стороне DSLAM (DSL интерфейсы). Upstream поток использует L2 Forwarding (перенаправление, основанное на MAC адресе) и не требует привлечения для этой цели IP address lookup .

Downstream трафик, протекающий от Ethernet интерфейсов к DSL интерфейсам DAS-3248, показан на рисунке 4-22 жирной стрелкой, начинающейся на NET/WAN стороне DSLAM (Ethernet интерфейсы).

Для нормального EoA трафика достаточно лишь MAC адреса для принятия решения о перенаправлении трафика, и не требуется информации о его IP адресе.
L3 Forwarding (IP address lookup) используется лишь для передачи пакетов по направлению к IPoA интерфейсам.

4.5.2. Основные понятия IPoA to IPoE Tunneling.

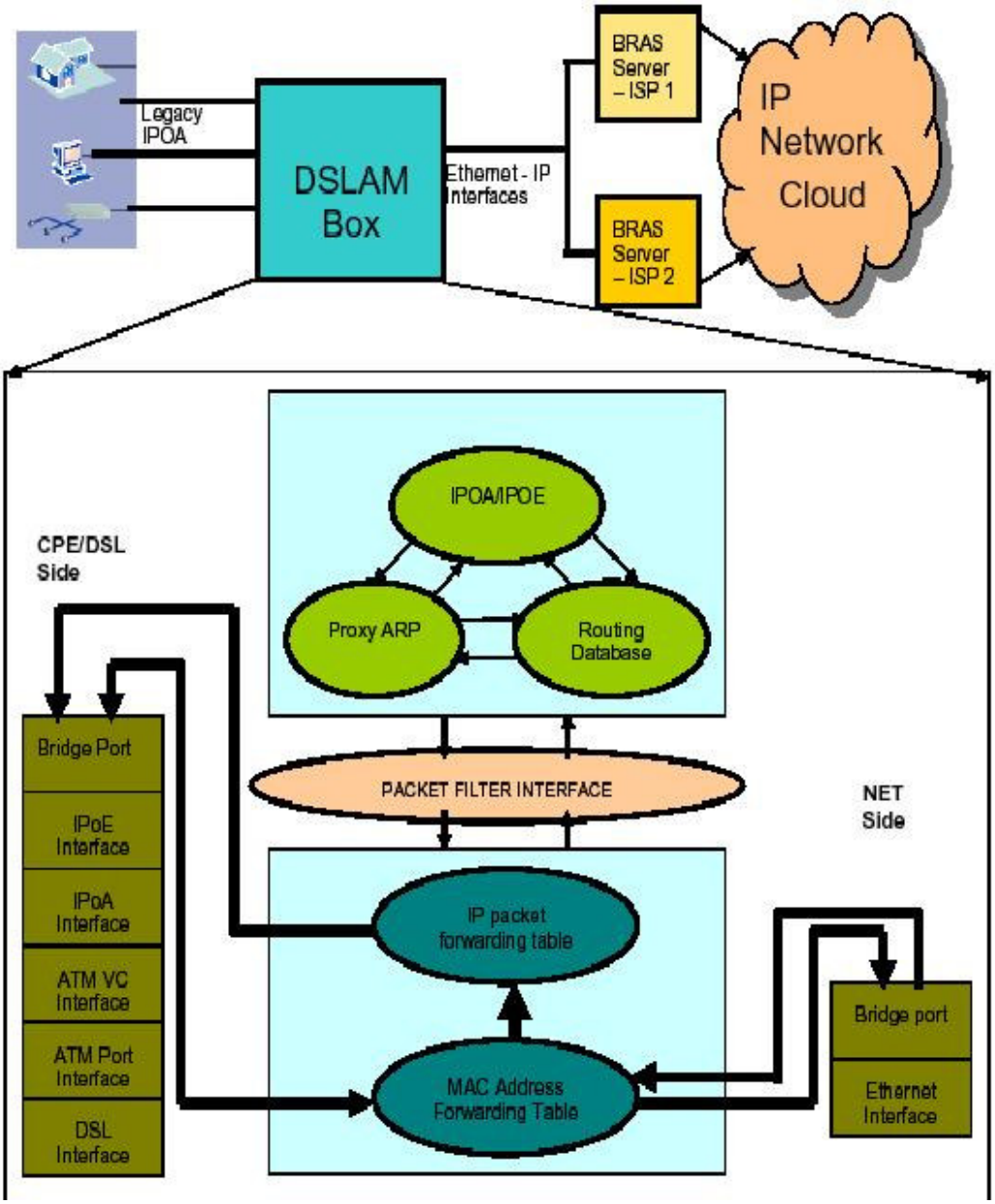


Рисунок 4-22.

Поясним понятия, изображенные на рис.4-22.

MAC Address Forwarding Table - таблица коммутации
Таблица коммутации - это таблица MAC адресов, используемая для перенаправления (L2 Forwarding) пакетов, основываясь на информации о MAC адресе назначения пакета, совместно с информацией о его VLAN теге.
Записи в MAC Address Forwarding Table могут создаваться как статически, так и динамически в результате обучения.

L2 Forwarding для IPoE трафика дает возможность перенаправлять трафик

к Ethernet интерфейсам DSLAM. Отсюда следует, что независимо от того, статические или динамические записи используется в MAC Address Forwarding таблице, обязательно должна существовать запись для WAN/NET стороны DSLAM. MAC адрес этой записи - это обычно MAC адрес BRAS сервера.

IP Address Lookup

IP address lookup по определению предполагает, что каждый принимаемый IP пакет проходит следующие шаги:

1) IP пакет достигает входного порта;
2) в таблице IP Address Lookup Table ищется IP маршрут с адресом назначения, соответствующим адресу назначения в прибывшем пакете;
3) если соответствие найдено, пакет перенаправляется на выходной порт.

Затем пакет перенаправляется через выходной порт на следующую точку IP маршрута (Next hop). Для пакетов нисходящего потока следующей точкой маршрута является IPoA интерфейс.

> Примечание: IP Address Lookup используется только для Downstream трафика. Для Upstream трафика используется L2 Forwarding.
>
> Для выбора типа перенаправления Downstream трафика используется параметр **routingstatus** IPoE интерфейса. Значение *enable* соответствует L3 Forwarding, а *disable*- L2 Forwarding.

Пакетный фильтр (Packet Filter Interface)- является модулем DAS-3248, позволяющим регистрировать пользовательские задания, решающие вопросы фильтрации определенных типов пакетов в общем информационном потоке. Пакетный фильтр используется любыми видами пользовательских модулей для получения и отправки пакетов (ATM ячеек, Ethernet пакетов, PPPoE фреймов). Для получения пакетов пользовательские задачи регистрируются в модуле пакетного фильтра.

Пользовательский модуль посылает пакеты, включающие атрибуты фильтра.

Атрибуты фильтра регистрируются модулем пакетного фильтра и включаются в обработку.

Поступающие пакеты фильтруются по атрибутам фильтра как на CPE стороне, так и на WAN интерфейсах DSLAM.

Поддержка модуля пакетного фильтра для IPoE интерфейсов включает в себя поддержку приема и передачи IPoE фреймов на IPoE интерфейс. Также пакетный фильтр занимается поддержкой приема и передачи ARP запросов и ответов, приходящих на WAN интерфейсы устройства.

Модуль ARP-прокси (Proxy ARP Module)

Основная задача прокси ARP модуля – поддержка ARP-таблицы. Данная задача выражается в следующем:

1) Управление ARP записями;
2) Генерация ARP запросов для разрешения соответствий IP-MAC. В случае IPoE это разрешение APR соответствий для BRAS серверов;
3) Обновление ARP кеша после обработки ARP ответов;
4) Осуществление непосредственно ARP-прокси функционала для набора IP адресов, обычно IPoE IP адресов.

IPoA/IPoE модуль - отвечает за конфигурирование IPoA и IPoE интерфейсов на DAS-3248.Его функции:

1) непосредственно создание, изменение, удаление IPoA и IPoE интерфейсов. IPoA интерфейсы обычно используется как высокоскоростные сервисы или Uplink к другому роутеру. Типичное их использование - предоставление IPoverATM схемы overDSL для подсоединения офиса или предприятия к Интернету;
2) конфигурирование Bridge порта над IPoE интерфейсом;
3) обработка триггеров от модулей ARP Proxy и Routing Database Module для включения/выключения IPoA to IPoE tunneling.
4) получение статистики для обоих типов интерфейсов: IPoA и IPoE.

Модуль таблицы маршрутизации (Routing Database Module)

Модуль таблицы маршрутизации является базой данных всей маршрутной информации в DAS-3248. Она ответственена за следующее:

1) управление маршрутами;
2) создание Upstream и Downstream маршрутизации для IPoE, основываясь на понятии RID.

Таблица маршрутизации содержит информацию обо всех IP маршрутах в системе.

Все маршруты и ARP записи в устройстве содержат в своем составе RID (Route Information Database) - идентификатор базы данных маршрутной информации. RID идентифицирует поток пакетов и определяет маршрутную информацию, связанную с этим потоком, базируясь на VLAN ID.

Максимальная величина RID равна системной переменной GS_CFG_MGMT_RID .

RID может быть создан, используя CLI ,следующим образом:

$create rid static rid <x>,

Где X может иметь значение от 1 до GS_CFG_MAX_RID.

Таблица маршрутизации может быть двух типов:

1) IRD (Independent Routing Database) - независимая таблица маршрутизации - когда в системе имеется более одного маршрута и каждый RID определяет только один маршрут. То есть, если созданы VLAN X и маршрут с RID X, это означает, что маршрут с RID X определяет поток пакетов, помеченных VLAN ID X.
2) SRD (Shared Routing Database) - общая таблица маршрутизации – когда в системе имеется только один RID и все потоки для всех зарегистрированных в системе VLAN ID направляются маршрутом, имеющим этот RID. В этом режиме невозможно создание более одного маршрута.

Для изменения режима работы таблицы маршрутизации служит команда:

$modify nbsize ridcap <X>,

где X может принимать значения *irdcapable* или *srdcapable*.

Чтобы эти изменения вступили в силу, нужно сохранить конфигурацию и перезагрузить систему.

4.5.3. Конфигурирование стека интерфейсов IPoA to IPoE Tunneling.

4.5.3.1. Клиентская сторона.

Рис.23 показывает, как должен выглядеть стек на клиентской стороне и какие команды CLI должны выполняться, чтобы создать каждый интерфейс в этой иерархии (подробно команды конфигурирования интерфейсов IPoA и IPoE описаны в разделах 4.4.4 - 4.4.6, а нижележащих интерфейсов в более ранних разделах).

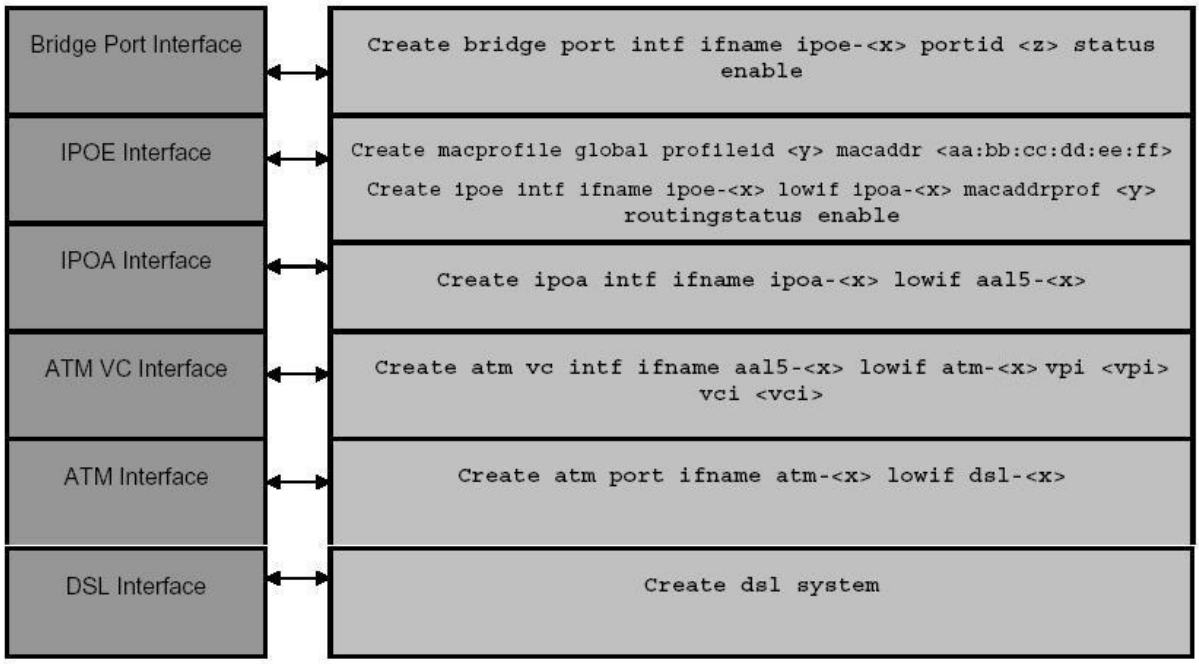


Рисунок 4-23

4.5.3.2 WAN/NET Сторона DAS-3248.

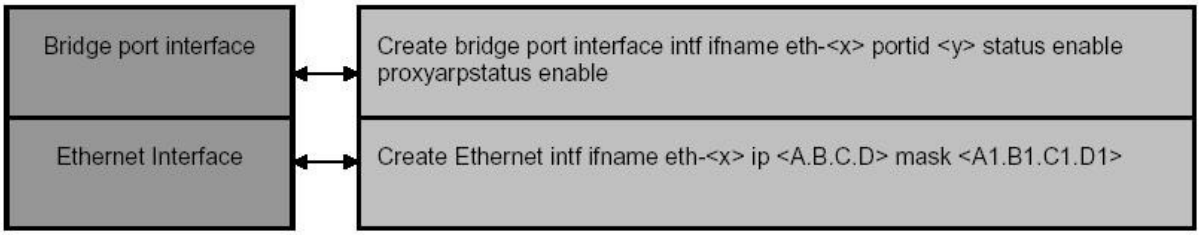


Рисунок 4-24

Рис. 24 объясняет, как должен выглядеть стек на WAN стороне DSLAM.

Сначала на WAN стороне создается Ethernet интерфейс, поверх которого должен быть создан Bridge порт.
На WAN стороне в основе стека может быть также агрегированный (aggregator) интерфейс.

4.5.4. Создание, настройка и удаление интерфейса IPoA

Для настройки IPoA интерфейсов используются следующие команды CLI:

create ipoa intf

Описание: создает новый IPoA интерфейс.

Синтаксис команды:

create ipoa intf ifname *ifname* **lowif** *lowif* **[configstatus** Normal | Config **]**
[enable|disable**]**

Таблица описания параметров команд:

ifname *ifname*	имя EoA интерфейса, лежит в диапазоне ipoa-0..ipoa-383. **Обязательный параметр.**
lowif *lowif*	Имя AAL5 интерфейса, на котором будет создан данный IPoA интерфейс. **Обязательный параметр.**
configstatus Normal | Config	Определяет**,** является ли IPoA интерфейс активным по требованию. **Normal**- интерфейс активен всегда. **Config**- интерфейс находится в неактивном состоянии после включения и активизируется только после приема первого IPoA пакета от CPE. **Опциональный параметр. Поддерживается только значение** Normal. **Значение по умолчанию** Normal.
enable | disable	Административный статус EoA интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**

Пример:
Команда для создания IPoA интерфейса поверх интерфейса aal5-51.
create ipoa intf ifname ipoa-51 lowif aal5-51 configstatus Normal enable

modify ipoa intf

Описание: изменяет параметры существующего IPoA интерфейса.

Синтаксис команды:

modify ipoa intf ifname *ifname* **[**enable|disable**]**

Пример:

Команды для включения и выключения интерфейса ipoa-51:

modify ipoa intf ifname ipoa-51 disable

modify ipoa intf ifname ipoa-51 enable

delete atm eoa intf

Описание: удаляет IPoA интерфейс

Синтаксис команды:

delete ipoa intf ifname *ifname*

Пример:

команда удаления IPoA интерфейса eoa-51

delete ipoa intf ifname eoa-51

get eoa intf

Описание: просмотр статуса одного или всех IPoA интерфейсов DAS-3248.

Синтаксис команды:

get ipoa intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** IPoA интерфейсов устройства**.**

Пример: Просмотр статуса интерфейса ipoa-51

get ipoa intf ifname ipoa-51

4.5.5. Создание, настройка и удаление интерфейса IPoE

Для настройки IPoE интерфейсов используются следующие команды CLI:

create ipoe intf

Описание: создает новый IPoE интерфейс.

Синтаксис команды:

create ipoe intf ifname *ifname* **lowif** *lowif* **macaddrprof** *macaddrprof*
[ethpkttype Type2 | 802_3 **] [inactivitytmrintrvl** *inactivitytmrintrvl* **]**
[routingstatus enable| disable **] [**enable | disable **]**

Таблица описания параметров команд:

ifname *ifname*	имя IPoE интерфейса, лежит в диапазоне eoa-0..eoa-383. **Обязательный параметр.**
lowif *lowif*	Имя IPoA интерфейса, на котором будет создан данный IPoE интерфейс. **Обязательный параметр.**
macaddrprof *macaddrprof*	Номер профиля (profile id),содержащего MAC адреса, привязанные к данному IPoE интерфейсу. Профиль MAC является общим путем для присвоения MAC адресов на интерфейсах. MAC адреса могут ассоциироваться с профилем, и этот профиль может присоединяться к интерфейсу. прежде чем создать IPoE интерфейс создается профиль MAC и связывается с интерфейсом. В настоящее время поддерживаются максимум 8 профилей в системе. **Обязательный параметр.** (для modify ipoe intf опциональный)
ethpkttype Type2	802_3	Ethpkttype - Тип пакета Ethernet, который может передаваться на этот IPoE интерфейс. Правильные величины Ethpkttype следующие: - Type 2 Ethernet Packet - 802.3 Ethernet **Опциональный параметр.** **Значение по умолчанию** Type2**.**
inactivitytmrintrvl *inactivitytmrintrvl*	Максимальное время в секундах для обнаружения любой деятельности на интерфейсе, по истечению которого если через интерфейс не

	проходят данные, он помечается как неактивный Обычно используется в случае динамического конфигурирования интерфейсов. Значение 0 означает, что таймер выключен. Связан с настройкой **configstatus** IPoA интерфейса, соответствующего данному IPoE интерфейсу, и имеет смысл только в случае **configstatus Config.** **Опциональный параметр.**
routingstatus enable| disable	Величина, определяющая потребность в IP Lookup в направлении Downstream . По умолчанию устанавливается в enable. Если параметр установлен в состояние disable, тогда комбинации уникальных Vlanid и MAC адреса, определенных пользователем будет достаточно, чтобы направить пакеты по назначению без поиска IP адреса. **Опциональный параметр.** **Значение по умолчанию** enable.
enable | disable	Административный статус IPoE интерфейса. **Опциональный параметр. Значение по умолчанию** enable**.**

Пример:

Команда для создания IPoE интерфейса поверх интерфейса ipoa-51.

create ipoe intf ifname ipoe-51 lowif ipoa-51 macaddrprof 1 enable,

где **macaddrprof** номер MAC профиля созданный заранее командой

create macprofile global profileid 1 macaddr XX:XX:XX:XX:XX:XX

modify ipoe intf

Описание: изменяет параметры существующего IPoE интерфейса.

Синтаксис команды:

modify ipoe intf ifname *ifname* **[macaddrprof** *macaddrprof* **][ethpkttype** Type2 | 802_3 **][inactivitytmrintrvl** *inactivitytmrintrvl* **]**
[routingstatus enable |disable **] [**enable | disable **]**

Внимание: Перед изменением любых параметров существующего IPoE интерфейса необходимо его выключить

modify ipoe intf ifname ipoe-51 disable

А после внесения всех необходимых изменений в конфигурацию IPoE необходимо включить его в работу
modify ipoe intf ifname ipoe-51 enable

Пример:
Последовательность команд для изменения параметра **ethpkttype** интерфейса ipoe-51 на новые значения (**ethpkttype 802_3**):
modify ipoe intf ifname ipoe-51 disable
modify ipoe intf ifname ipoe-51 ethpkttype 802_3
modify ipoe intf ifname ipoe-51 enable

delete atm eoa intf

Описание: удаляет IPoE интерфейс
Синтаксис команды:
delete ipoe intf ifname *ifname*

Пример:
команда удаления IPoE интерфейса eoa-51
delete ipoe intf ifname ipoe-51

get ipoe intf

Описание: просмотр статуса одного или всех IPoE интерфейсов DAS-3248.
Синтаксис команды:
get ipoe intf [ifname *ifname***]**

Внимание: В случае если интерфейс явно не указан в команде, выводится состояние **всех** IPoE интерфейсов устройства**.**

Пример**:** Просмотр статуса интерфейса ipoe-51
get ipoe intf ifname ipow-51

4.5.6. Создание, настройка и удаление bridge-порта на клиентской стороне.

Bridge порт настраивается аналогично другими инкапсуляциям (см. раздел о RFC1483 Bridged), приведенным выше, только в качестве **ifname** интерфейса, на базе которого создается bridge порт, указывается ipoe интерфейс.

Пример:
create bridge port intf ifname ipoe-51 portid 52 learning enable status enable

4.5.7. Создание, настройка и удаление bridge-порта на WAN стороне.

Bridge порт настраивается аналогично п.4.4.6, но в качестве **ifname** интерфейса, на базе которого создается bridge порт, указывается eth-0 или eth-1 интерфейс.
Крме того, контексте IPoA to IPoE Tunneling, вводятся дополнительный параметр для Bridge порта.

proxyarpstatus - необязательный параметр, который определяет, будут ли ARP запросы (для которых использовано Proxy ARP) приниматься и обрабатываться на этом интерфейсе. Параметр принимает два значения - enable и disable.

Пример:
create bridge port intf ifname eth-0 portid 53 status enable proxyarpstatus enable

4.5.8. Логика работы и конфигурирование Upstream потока в IPoA to IPoE Tunneling.

4.5.8.1. Конфигурирование ARP.

Текущая реализация IPoA to IPoE Tunneling подобна «половине маршрутизатора», у которого в Downstream направлении используется IP address lookup, а в Upstream направлении используется MAC address forwarding. Для Upstream потока должен быть сконфигурирован маршрут по умолчанию. Маршрут по умолчанию по существу означает, что весь трафик CPE должен пересылаться к WAN стороне.

$create ip route rid <x> ip 0.0.0.0 mask 0.0.0.0 gwyip <A.B.C.D> ifname ANYWAN

Шлюз (gwyip)- это обычно IP адрес BRAS сервера. Для всех тех IPoE интерфейсов, у которых vlan id bridge портов отображаются на данный RID, должен использоваться этот маршрут по умолчанию. Этот маршруту требуется для ARP записи BRAS (адрес IP A.B.C.D), который должен разрешаться таким образом, чтобы upstream MAC address forwarding мог произойти. ARP может конфигурироваться или статически или динамически. В зависимости от вышесказанного, или в MAC address forwarding таблице создается статическая запись или эта запись будет создана динамически.

Статическое конфигурирование ARP
$create arp rid <x> ip <A.B.C.D> macaddr <a:b:c:d:e:f>
$gvrp port info portid <IPOE-BrigePortId> portvlanid <x>

Как сказано выше маршрут по умолчанию добавлен для адреса IP A.B.C.D для rid <x>. ARP для этого адреса IP разрешается как результат создания статической ARP записи для IP адреса <A.B.C.D> и rid<x> как показано в первой команде.

Примечание:
В случае IRD, vlanid <x> отображается на RID <x> , в случае же SRD , Vlanid <x> должен отображаться на RID <y>, где <y> -некоторый RID созданный в SRD режиме. VlanId <x> и RID <x / y> должны быть уже созданы в системе ранее.

Vlanid в bridge port, созданного над IPoE интерфейсом определен как <x>, что значит что весь upstream трафик из CPE получает теги этого Vlan Id. Bridge порт WAN стороны должен быть членом этого VLAN. Вторая команда, показанная выше, иллюстрирует, как PVID может быть привязан к bridge порту.

Следующая команда CLI иллюстрирует как VLAN ID <m> может создаваться в системе с портами-членами <a> и <b>.

$create vlan static vlanid <m> vlanname <NAME> egressports <a> <b>

В случае IRD, IPoE интерфейс, у которого vlan id bridge порта равно <x> и отображается на RID <x> ,может использовать для форвардинга upstream трафика MAC адрес, сконфигурированный статически.

Но для протекания upstream трафика необходимо, чтобы существовала запись в MAC address forwarding таблице для этого MAC. Эта запись должна быть конфигурирована как путь для всего трафика с MAC адресом назначения a:b:c:d:e:f и vlanid <x> ,предназначенного WAN стороне. Например, в команде данной ниже, для создания статической записи в MAC address forwarding таблице, Bridge port id <Y> представляет собой bridge порт одного из интерфейсов на WAN стороне.

$create bridge static ucast vlanid <x> ucastaddr <a:b:c:d:e:f> portid <Y>

Динамическая конфигурование ARP
Как сказано выше, для IP адреса A.B.C.D был добавлен маршрут по умолчанию (с RID <x>).

$modify gvrp port info portid <IPOE-BridgePortId> portvlanid <x>

Vlanid Bridge порта, созданного над IPoE интерфейсом определен как <x>, поэтому весь Upstream трафик от CPE получает этот Vlan Id. WAN bridge порт должен также быть членом этого VLAN. Следующие CLI команды иллюстрируют, как VLAN ID <m> может создаваться в системе с его членами - bridge портами <a> и <b>.

$create vlan static vlanid <m> vlanname <NAME> egressports <a> <b>

Следовательно, в случае случай IRD, IPoE интерфейс, чей vlan id bridge порта (равный <x>) , отображается на RID <x>, является маршрутом по умолчанию для Upstream трафика, но без создания статической ARP записи.
В таком сценарии, ARP должен разрешатся динамически.

$create ip route rid <X> ip <E.F.G.H> mask 255.255.255.255 gwyip <E.F.G.H>
ifname ipoe-<N> proxyarpstatus enable

Upstream маршрут уже создан для RID <x>. Создание же вышеуказанного маршрута для Downstream трафика назначает IP адрес IPoE интерфейса. Также он определяет, что для IP маршрутизации, будет использоваться IP адрес <E.F.G.H> для RID <X> и он будет маршрутизироваться на ipoe-<N> интерфейс. Используя всю эту информацию, генерируется ARP запрос для IP адреса, определенном в маршруте по умолчанию как адрес шлюза . BRAS отвечает на этот ARP запрос. Получив ARP ответ от BRAS, ARP таблица корректируется для этого RID. Кроме того, на основании обучения MAC адресу источника, создается запись в MAC address forwarding таблице, которая является необходимым условием для протекания Upstream трафика.

4.5.8.2. Логика работы IPoA to IPoE Tunneling в Upstream направлении

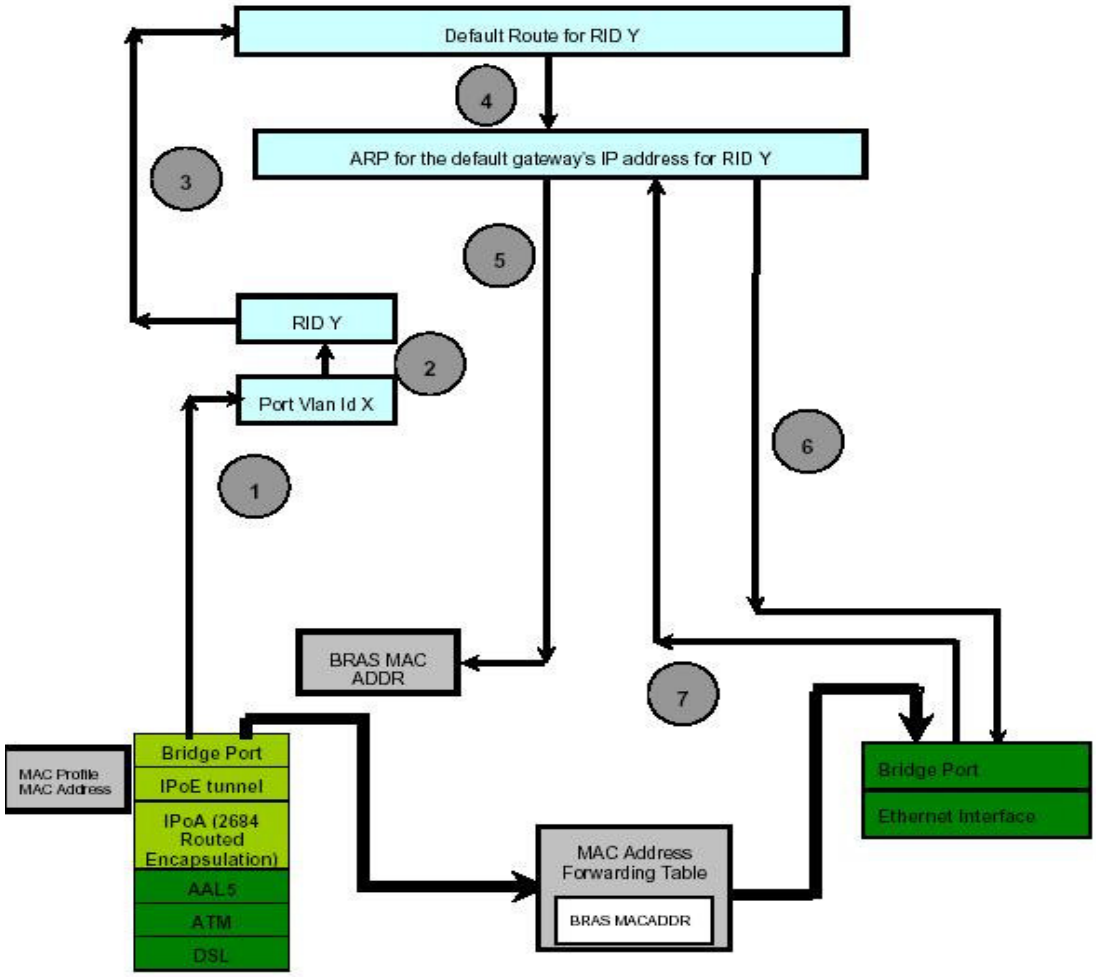


Рисунок 4-25. Алгоритм IPoA to IPoE в Upstream направлении

Шаг 1.Создается Bridge port на соответствующем IPoE интерфейсе. VLAN ID X данного порта используется для отображения его на соответствующий RID.

Шаг 2. В случае IRD режима таблицы маршрутизации VLAN ID X отображается один в один на соответствующий RID. В случае SRD режима VLAN ID X отображается на единственный маршрут, созданный устройством. Если VLAN с ID X не создан в системе, то ничего происходить не будет. Трафик будет протекать только в том случае, если соответствующий VLAN создан на обеих сторонах DSLAM (т.е. на Bridge интерфейсах поверх IPoE и Ethernet интерфейсов), а также оба эти интерфейса являются членами одного VLAN.

Шаг 3.Для того чтобы Upstream трафик мог протекать в системе, в системе должен быть создан маршрут по умолчанию с соответствующим RID .

Шаг 4.Если маршрут по умолчанию уже существует, проверяется, разрешен ли ARP-запрос для маршрута по умолчанию с тем же RID или с другим.

Шаг 5. Если ARP разрешается с тем же RID, тогда Destination MAC адрес во всех таких пакетах должен быть MAC адресом, обозначенным данной ARP записью. Обычно это MAC адрес BRAS сервера.

Шаг 6. Если ARP не решается, посылается ARP запрос к BRAS серверу для этого RID. ARP запрос должен быть тегированным пакетом с vlanid соответствующим данному RID.

Шаг 7: ARP ответ, полученный от BRAS, корректирует ARP-кеш DAS-3248 для этого RID. Обновляется также и MAC address forwarding таблица. Как только Arp запрос разрешен, Upstream трафик для данного RID может протекать. Destination MAC адрес во всех таких пакетах должен быть MAC адресом, указанным ARP записью (как было показано в шаге 5).

Если ARP разрешен, тогда IPoE интерфейс имеет информацию относительно своего собственного MAC адреса (из информации MAC профиля, полученным интерфейсом получил при его создании), MAC адреса BRAS (из ARP) и Vlanid, который должен использоваться для маркировки пакет (Vlan Id bridge порта). Таким образом, пакеты, приходящие со стороны CPE, могут туннелироватся в Ethernet фреймы, созданные используя вышеуказанную информацию WAN стороны. Поскольку, IP lookup не используется для Upstream трафика, в MAC address forwarding таблице
нужно иметь запись для MAC адреса BRAS для того, чтобы пакеты, предназначенные для WAN стороны, могли быть пересланы корректно. Эта запись может быть или создана динамически посредством обучения с использованием MAC адреса источника (когда ARP ответ принимается со стороны BRS) или может быть сконфигурирована статически.

4.5.9. Логика работы и конфигурирование Downstream потока в IPoA to IPoE Tunneling.

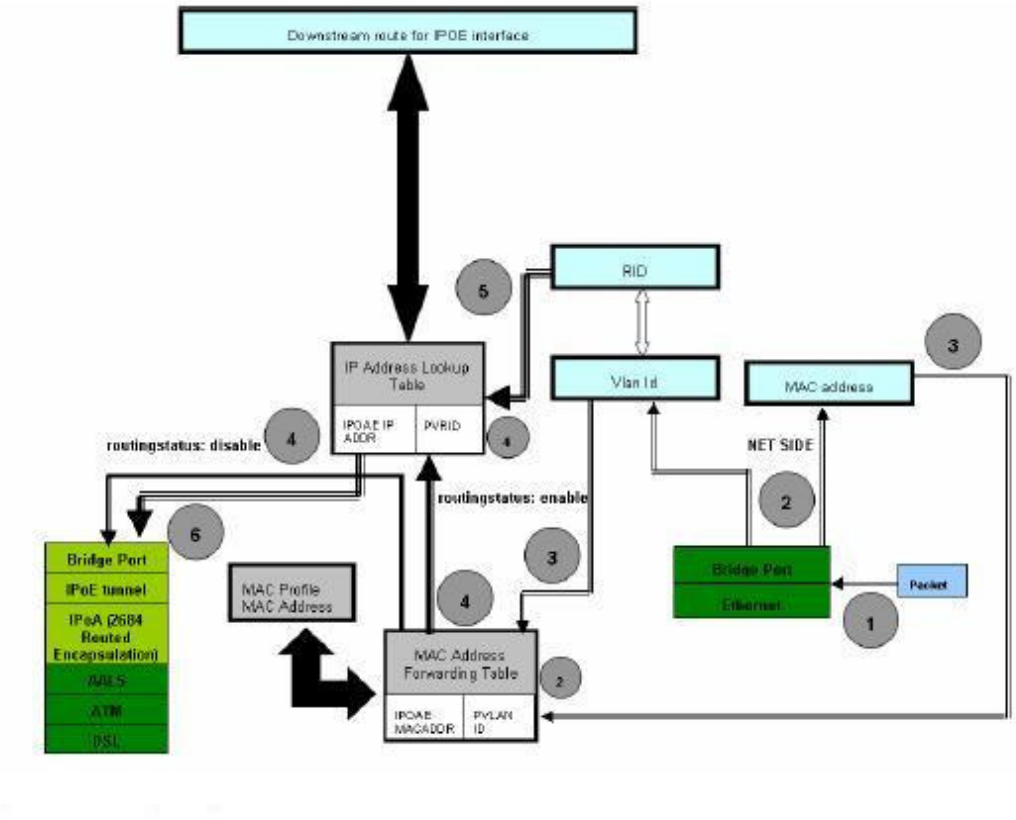


Рисунок 4-26. Алгоритм работы IPoA to IPoE в Downstream направлении

Рисунок 4-26 описывает последовательность действий, происходящих при работе с Downstream потоком. В зависимости от конфигурации параметра routingstatus на IPOE интерфейсе возможны один из двух следующих вариантов:

- IP lookup, базирующийся на IP адресе (изображен толстой стрелкой на рисунке 4-26).
- Прямая пересылка пакета на IPOE интерфейс без IP Lookup (изображен тонкой стрелкой на рисунке 4-26).

Шаг 1. Пакет, предназначенный для IPoE интерфейса, принимается WAN интерфейсом DSLAM. Если пакет untagged, он будет промаркирован Vlan Id Bridge порта WAN интерфейса.

Шаг 2. Используя MAC адрес назначения и Vlan Id пакета, производится L2 Forwarding. Запись в MAC address forwarding таблице создается, используя MAC адрес в MAC профиля, связанного с IPoE интерфейсом и VlanId bridge интерфейса, созданного над IPoE интерфейсом.

Шаг 3. Комбинация VlanId и MAC адреса используется для lookup, как было объяснено в шаге 2.

Если routingstatus установлен в enable тогда:

Шаг 4. IP lookup требуется для этого IPoE пакет. IP lookup производится, базируясь на RID и IP адресе назначения в пакете.Информацию о RID получаем, как производную от VlanId ,прочитанную из пакета (используя таблицу маршрутизации и маршрут, добавленный для этого RID).

Шаг 5. Информация о RID обследуется в контексте установления режима маршрутизации (IRD или SRD).

Шаг 6. Если IP lookup увенчался успехом, пакет инкапсулируется в Routed RFC 2684 LLC/VC формат и посылается CPE стороне DAS-3248 на интерфейс, установленный в ходе IP lookup поиска.

Если routingstatus устанавлен в disable тогда,

Шаг 4. Уникальная комбинация MAC адреса и VlanId используется, чтобы найти CPE интерфейс и перенаправить ему пакет.

Внимание:
Для протекания как Upstream, так и Downstream трафика, требуется, чтобы соответствующий VlanId и RID были созданы в системе. Соответствующие IPoE и WAN интерфейсы должны быть члена этого VLAN.
Bridge порт над IPoE интерфейсом должен быть создан и административно включен.

4.5.10. Логика работы и конфигурирование Proxy ARP в IPoA to IPoE Tunneling.

DAS-3248 поддерживает ARP-прокси для IP адресов, сконфигурированных на IPoE интерфейсах. Если ARP запрос приходит для такого IP адреса, DAS-3248 в ответ на ARP запрос посылает ARP ответ с аппаратным адресом соответствующим MAC адресу, содержащемуся в MAC профиле, связанному с IPoE интерфейсом. Алгоритм работы ARP-прокси показан на рис.4-27

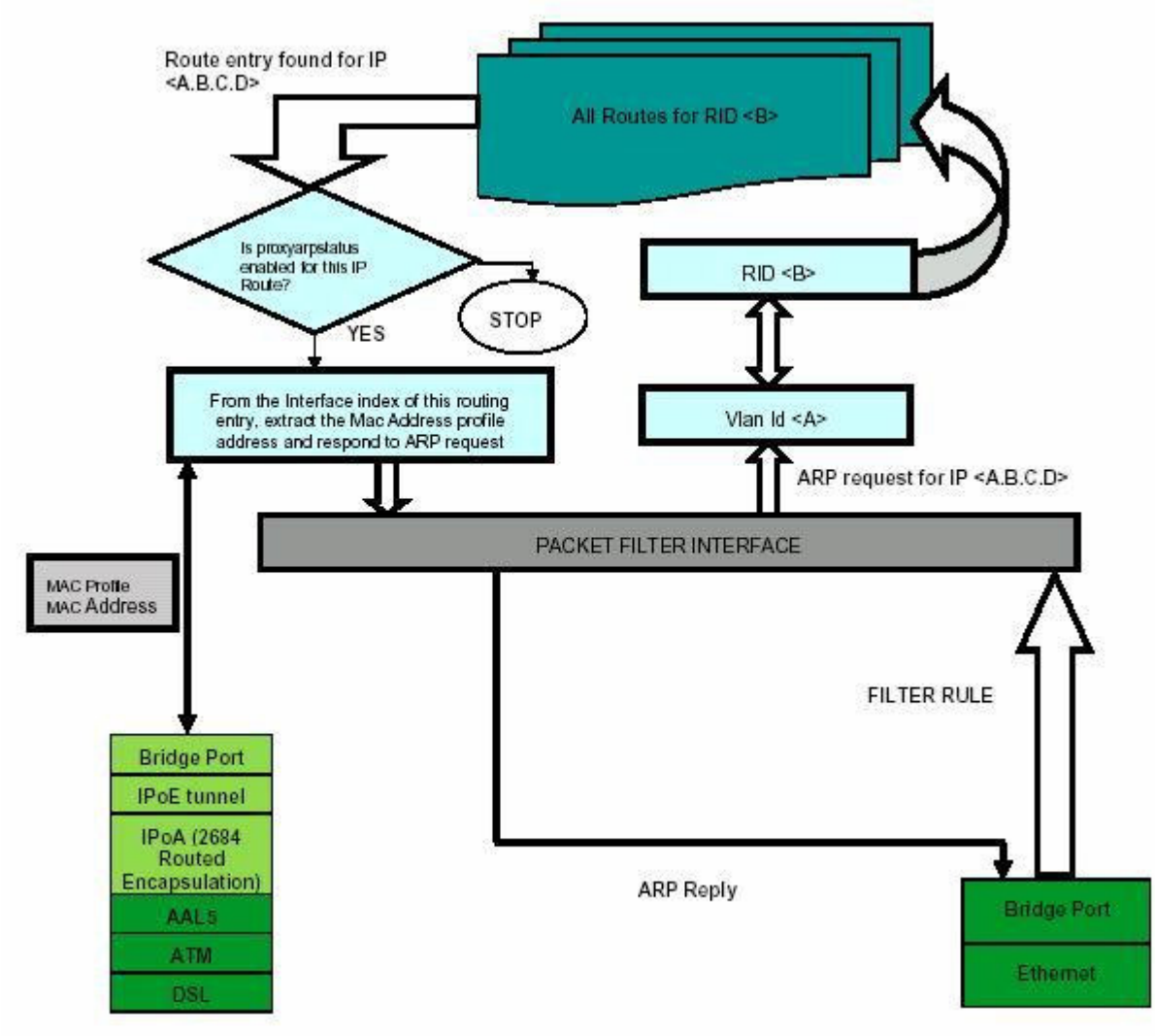


Рисунок 4-27.Алгоритм работы ARP-прокси

1.ARP запрос принимается с WAN стороны DAS-3248. VLAN Id, содержащийся этом в пакете, указывает на соответствующий RID.

2. Если существует Downstream маршрут для соответствующего RID и IP адрес на который пришел ARP запрос- это является достаточной информацией, чтобы ответить на ARP запрос.

3. Аппаратный адрес для ответа ARP получается из профиля адреса MAC, связанного с Downstream маршрутом IPoE интерфейса.

4. Для ARP-прокси параметр proxyarpstatus bridge порта на WAN стороне должен быть в состоянии enable. Этот параметр определяет, будет ARP-прокси функционал использоваться для ARP запросов на этом интерфейсе.

5. Запись в таблице маршрутизации для адреса IP, для которого пришел ARP запрос, должна иметь параметр proxyarpstatus в состоянии enabled.

6. Для того чтобы ARP-прокси модуль чтобы получить все ARP запросы от WAN стороны, должно быть создано правило для пакетного фильтра DAS-3248, которое посылает копию

всех ARP запросов в Management Plane.Поле description этого правила должно быть IPoE_CONTROL.

Следующее CLI команды показывают конфигурирование ARP-прокси:

1. $modify bridge port intf portid <X> proxyarpstatus enable
   Эта команда показывает, что ARP запросы, полученные с WAN интерфейса DSLAM, соответствующего этому порту моста будут разрешаться, используя ARP-прокси.

2. $modify ip route rid <Z> ip <A.B.C.D> mask <E.F.G.H> proxyarpstatus enable
   Эта команда показывает, что ARP-прокси будет использоваться для IP адреса определенного в этом маршруте и для этого RID.

3. $create filter rule entry ruleid <Y> action copytocontrol description IPOE_CONTROL applywhenreq enable
4. $create filter subrule ether ethertypefrom 0x806 ethertypecmp eq dstmacaddrfrom ff:ff:ff:ff:ff:ff dstmacaddrcmp eq ruleid <Y> subruleid 1
5. $create filter rule map ifname alleth stageid 1 ruleid <Y> ordered 1
6. $modify filter rule entry ruleid <Y> status enable

Первая команда в вышеуказанном наборе команд создает правило с действием copytocontrol. Это означает, что все пакеты, подпадающие под это правило должны копироваться в Control Plane и, следовательно, ARP-прокси модуль имеет возможность получить их.
Вторая команда создает подправило в пределах вышеуказанного правила, которое определяет, что пакеты с широковещательным MAC адресом в поле MAC адреса назначения и типом Ethernet 0x806(ARP), должны было обработаны этим фильтром. Другими словами, это означает, что все запросы ARP на всех VLAN должны быть обработаны.
Третья команда отображает созданное правило фильтра на все интерфейсы WAN .Это значит, что оно применяется для всех пакетов, принимаемых с WAN стороны.
Четвертая команда активирует (включает) правило.

4.5.11. Пример настройки IPoA to IPoE internetworking

В качестве WAN интерфейса используется eth-0 (поверх него по умолчанию создан bridge id 385 интерфейс).
В качестве CPE интерфейса используется 24 ADSL порт.
Используется IP Lookup.
Используется IRD режим работы таблицы маршрутизации.
Используется Proxy ARP.
BRAS сервер имеет IP 192.168.100.1 и MAC адрес 00:0E:7F:61:C1:BE

	Команда	Действие
Шаг 1	$vlan static vlanid 3 vlanname IPoE_1	Создать корреспондирующий VLAN
Шаг 2	$create rid static rid 3	Создать RID
Шаг 3	$create ip route rid 3 ip 0.0.0.0 mask 0.0.0.0 gwyip 192.168.100.1 ifname anywan	Создать default route для этого RID
Шаг 4	$create atm vc intf ifname aal5-51 vpi 1 vci 50 lowif atm-23	Создать новый ATM VC интерфейс поверх 24 ADSL порта с параметрами VPI 1, VCI 50
Шаг 5	$create ipoa intf ifname ipoa-51 lowif aal5-51	Создать IPoA интерфейс непосредственно над AAL5 интерфейсом.
Шаг 6	$create macprofile global profile id 1 macaddr 00:0E:7F:61:C1:BE	Указать MAC профиль, который будет использоваться IPoE интерфейсом
Шаг 7	$create ipoe intf ifname ipoe-51 lowif ipoa-51 macaddrprof 1 routingstatus enable	Создать IPoE интерфейс
Шаг 8	$create bridge port intf ifname ipoe-51 portid 52	Создать bridge интерфейс поверх IPoE интерфейса
Шаг 9	$modify vlan static vlanname IPoE_1 egressports 52 385	Сделать CPE bridge порт и WAN bridge порт членами корреспондирующего VLAN
Шаг 10	$modify gvrp port info portid 52 portvlanid 3	Включить CPE bridge порт в VLAN
Шаг 11	$create ip route rid 3 ip 192.168.100.200 mask 255.255.255.255 gwyip 192.168.100.200 ifname ipoe-51 ProxyArpStatus enable	Присвоить IPoE интерфейсу IP и создать маршрут с этим IP и соответвующим RID (Proxy ARP включен)
Шаг 12	$modify bridge port intf portid 385 proxyarpstatus enable	Включить Proxy ARP на WAN bridge интерфейсе
Шаг 13	$create filter rule entry ruleid 2 action	Создать правило с действием

	copytocontrol description IPOE_CONTROL applywhenreq enable	copytocontrol. Все пакеты, подпадающие под это правило должны копироваться в Control Plane и, следовательно, ARP-прокси модуль имеет возможность получать их.
Шаг 15	$create filter subrule ether ethertypefrom 0x806 ethertypecmp eq dstmacaddrfrom ff:ff:ff:ff:ff:ff dstmacaddrcmp eq ruleid 2 subruleid 1	Создать подправило в пределах вышеуказанного правила, которое определяет, что пакеты с широковещательным MAC адресом в поле MAC адреса назначения и типом Ethernet 0x806(ARP), должны было обработаны этим фильтром.
Шаг 16	$create filter rule map ifname alleth stageid 1 ruleid 2	Отобразить созданное правило фильтра на все интерфейсы WAN (Ethernet)
Шаг 17	$modify filter rule entry ruleid 2 status enable	Включить созданное правило
Шаг 18	$modify bridge port intf portid 52 status enable	Включить CPE bridge port в работу

4.6.Агрегирование AAL5 интерфейсов (VC Aggregation).

Что такое VC Aggregation?

Традиционно в сетях доступа поддерживается взаимнооднозначное соответствие между bridge интерфейсами, EoA/PPPoA/IPoA интерфейсами и ATM VC (AAL5) интерфейсами. Тем не менее, может сложиться ситуация, требующая поддержки посредством VC AAL5 многочисленных приоритезированных потоков. Такая задача требует от устройства поддержки многочисленных VC AAL5 для единственного Bridge интерфейса для переноса различных видов трафика, базируясь на приоритете.
Для решения этой задачи на DAS-3248 была создана функция VC aggregation.

СущностьVC aggregation заключается в том, что создается логический агрегирующий интерфейс (VC aggregator, VCaggr-x) над одним или более AAL5 интерфейсами, который агрегирует трафик VC, на базе которых он создан и передает трафик единственному EoA/PPPoA/IPoA интерфейсу. Величины приоритета в пакетах используются при демультиплексировании Downstream трафика.

Отметим также, что EoA/IPoA/PPPoA интерфейс, созданный на единственном AAL5 интерфейсе и EoA/IPoA/PPPoA интерфейс, созданный на многочисленных AAL5 интерфейсах могут сосуществовать в одном ATM интерфейсе.
Но при этом ATM AAL5 интерфейсы, участвующие в VC aggregation не могут принадлежать разным ATM интерфейсам.
Следующий рисунок (рис.4-28) изображает гибридную модель VC aggregation в приложении к Downstream потоку данных.

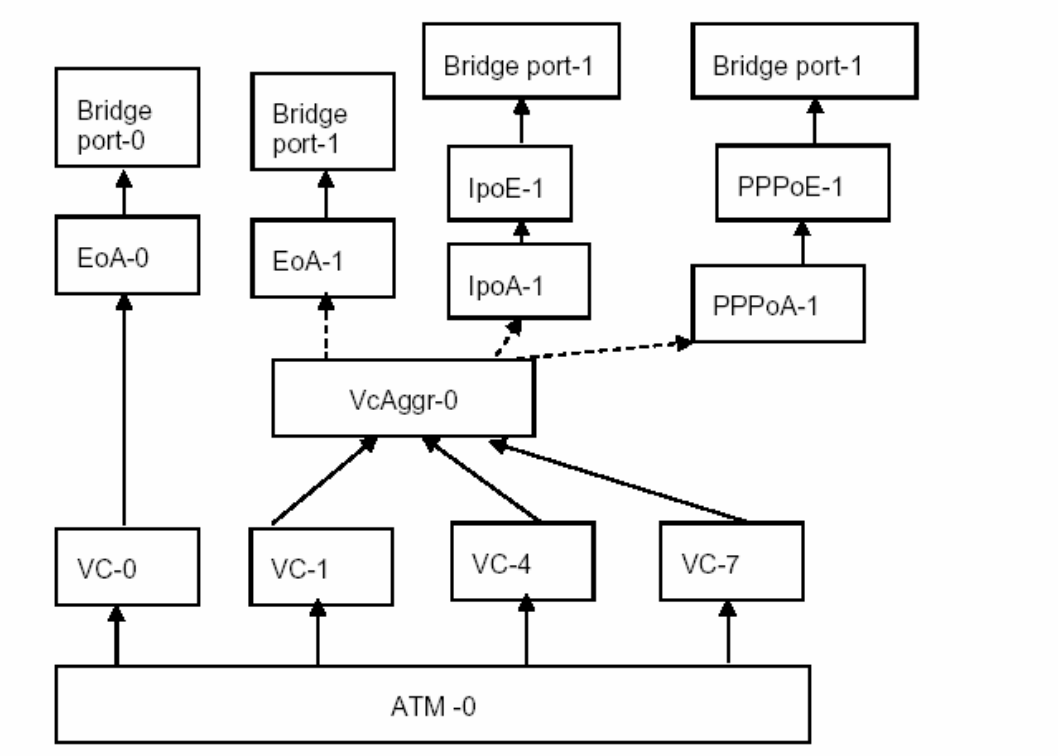


Рисунок 4-28

4.6.1.VC Aggregation.Основные понятия.

Downstream приоритет.

Поскольку многочисленные AAL5 VC интерфейсы могут существовать под EoA/PPPoA/IpoA интерфейсом, то для определения VC назначения, в который должен быть направлен пакет, поступивший с Uplink порта, должен использоваться какой-либо критерий. Таким критерием является приоритет базового VC AAL5. Приоритет, связанный с пакетом будет использован в качестве решающего показателя при выборе VC назначения.

Каждому AAL5 интерфейсу в VC aggregator интерфейсе присваивается свой Downstream приоритет. Возможные (правильные) варианты величин приоритетов - 0-7 или отсутствие приоритета. Один AAL5 интерфейс может иметь один или более приоритетов или не иметь его вообще (отсутствие приоритета). Приоритеты могут модифицироваться «на лету». Все приоритеты, которые не ассоциированы с каким-либо конкретным VC AAL5 интерфейсом, автоматически прикрепляются к AAL5 по умолчанию (определяется при создании VC aggregator интерфейса).

Upstream приоритет.
Регенерация приоритета необходима для дифференциации сервисов. В DAS-3248, регенерация приоритета поддерживается на уровне Bridge интерфейса для

дифференцирования сервисов на уровне клиента (или на уровне Bridge интерфейса). С применением VC aggregation трафик многих VC AAL5 мультиплексируется в VC Aggregator интерфейс, что требует дополнительной поддержки устройством маркировки пакетов приоритетами на основе базового VC AAL5. Существует два типа приоритетов для Upstream потока:

Приоритет Регенерации (upstrmregenprio): Для уже маркированных приоритетом пакетов, полученных от клиента.
Приоритет по умолчанию (upstrmdefprio): Для немаркированных приоритетом пакетов, полученных от клиента.

Наиболее вероятный сценарий с развертыванием VC aggregation - пересылка немаркированных пакетов между клиентом и провайдером. В Upstream направлении, клиентские устройства на своей стороне демультиплексируют общий поток данных в отдельные VC, базируясь на пользовательском приоритете. Провайдер на своей стороне вставляет в пакеты маркер приоритета и затем мультиплексирует трафик. Конфигурирование Upstream приоритета по умолчанию для каждого VC должно подчиняться именно этой логике.

В сценарии, когда пакеты между клиентом и провайдером являются уже маркированными приоритетом, осуществляется регенерация приоритетов, чтобы урегулировать различие приоритета установленного клиентским устройством и фактическим значением приоритета, устанавливаемым провайдером клиенту.

Другими словами, немаркированные до этого приоритетом пакеты маркируются приоритетом **upstrmdefprio**, а маркированные пакеты ремаркируются приоритетом **upstrmdefprio.**

4.6.2.Создание VC Aggregator интерфейса.

VC Aggregator создается в два этапа:
1.Создание VC Aggr Карты.
VC Aggr Карта представляет собой совокупность VC AAL5 интерфейсов и Upstream и Downstream приоритетов этих интерфейсов. Карта должна содержать по крайней мере один AAL5 VC интерфейс. Максимальное количество AAL5 VC, которые могут входить в карту - 8.

2. Прикрепление VC Aggr интерфейса к VC Aggr карте.
Также в этом пункте выбирается VC AAL5 интерфейс по умолчанию.
Внимание:
Число VC AAL5 интерфейсов не может изменяться на VC Aggr карте, после того как она связывается с VC Aggr Интерфейсом.

Пример конфигурирования VC Aggregation.

1.Создаем новые AAL5 VC интерфейсы:

$create atm vc intf ifname aal5-70 lowif atm-0 VPI 0 VCI 35 enable
$create atm vc intf ifname aal5-71 lowif atm-0 VPI 0 VCI 36 enable

2. Создаем VC Aggr карту:
$create atm vcaggr map mapid 1 vc aal5-70 dnstrmpriolist 0 1 upstrmdefprio 3 upstrmregenprio 6
$create atm vcaggr map mapid 1 vc aal5-71

3.После создания карты, связываем ее с vcaggr интерфейсом (AAL5 интерфейсом по умолчанию назначается AAL5-70):
$create atm vcaggr intf ifname vcaggr-0 mapid 1 defaultdnstrmvc aal5-70 enable

5. Агрегация DSL каналов

Агрегация DSL каналов используется для объединения нескольких DSL линий для переноса одного потока ATM. Данная технология может быть использована для предоставления требуемой полосы пропускания таким приложениям как, например, потоковое видео или для увеличения радиуса покрытия сети DSL при одинаковой или даже большей скорости.
Реализация агрегации DSL каналов DAS-3248 базируется на стандарте ANSI T1.PP.427.01-2004 (https://www.atis.org/atis/docstore/doc_display.asp?ID=3505). Передающая сторона добавляет к каждой ATM ячейке идентификатор очередности (sequence ID, SID). SID используется для восстановления исходного порядка ATM ячеек на принимающей стороне. Вместе с добавлением идентификатора очередности DAS-3248 использует управляющий протокол, основанный на обмене контрольными сообщениями ASM (autonomous status messages) в соответствии с данным ANSI стандартом.
ANSI T1.PP.427.01-2004 определяет группу агрегации как двунаправленный ATM поток, передаваемый по нескольким двунаправленным каналам через несколько физических сред передачи в обоих upstream и downstream направлениях. Управляющий канал также является двунаправленным ATM потоком, состоящим из ATM сообщений ASM. ASM – это сообщения уровня адаптации AAL5, занимающие одну ячейку. Данные сообщения передаются и принимаются по выделенному виртуальному соединению со значениями VPI = 0 и VCI = 20 (по умолчанию). Одна группа агрегации не может включать в себя несколько CPE или CO устройств. В соответствии со стандартом, если физическое соединение поддерживает несколько логических каналов, то эти каналы не могут быть агрегированы вместе в одну группу.
ATM стек при использовании агрегации DSL линков представлен на рис. 5-1.

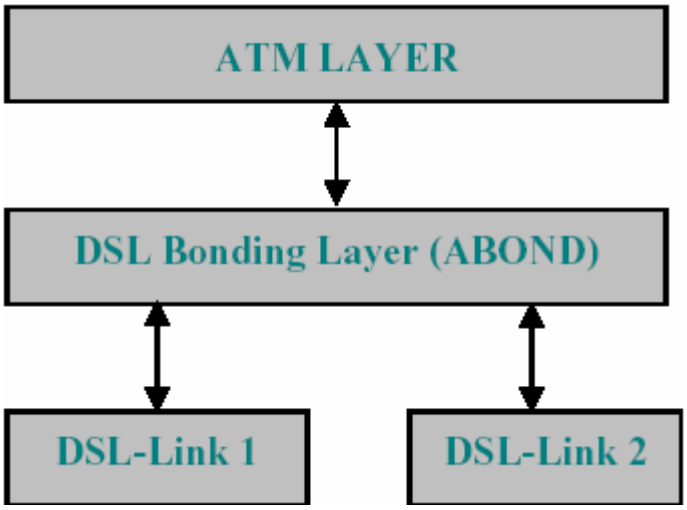


Рисунок 5-1: ATM стек.

Агрегация DSL каналов поддерживается DAS-3248, начиная с версии программного обеспечения 1.40. Рассматриваемая технология реализована в виде логического интерфейса, используемого как нижележащий интерфейс для ATM интерфейса.
Агрегация DSL имеет следующие ограничения и особенности:

- агрегирование минимум двух и максимум 8 соединений;

- агрегирование соединений с различной скоростью (допускается разница в скорости в 4 раза);
- динамическое добавление и удаление соединений из группы;
- независимое агрегирование в upstream и downstream направлениях (если требуется);
- агрегирование любых портов;
- поддержка до 32 групп агрегирования;
- поддержка 8-ми и 12-ти битного форматов SID;
- предоставление статистики для групп и отдельных соединений;
- поддержка MIB, определенных в стандарте;

5.1 Стек протоколов при использовании агрегации DSL

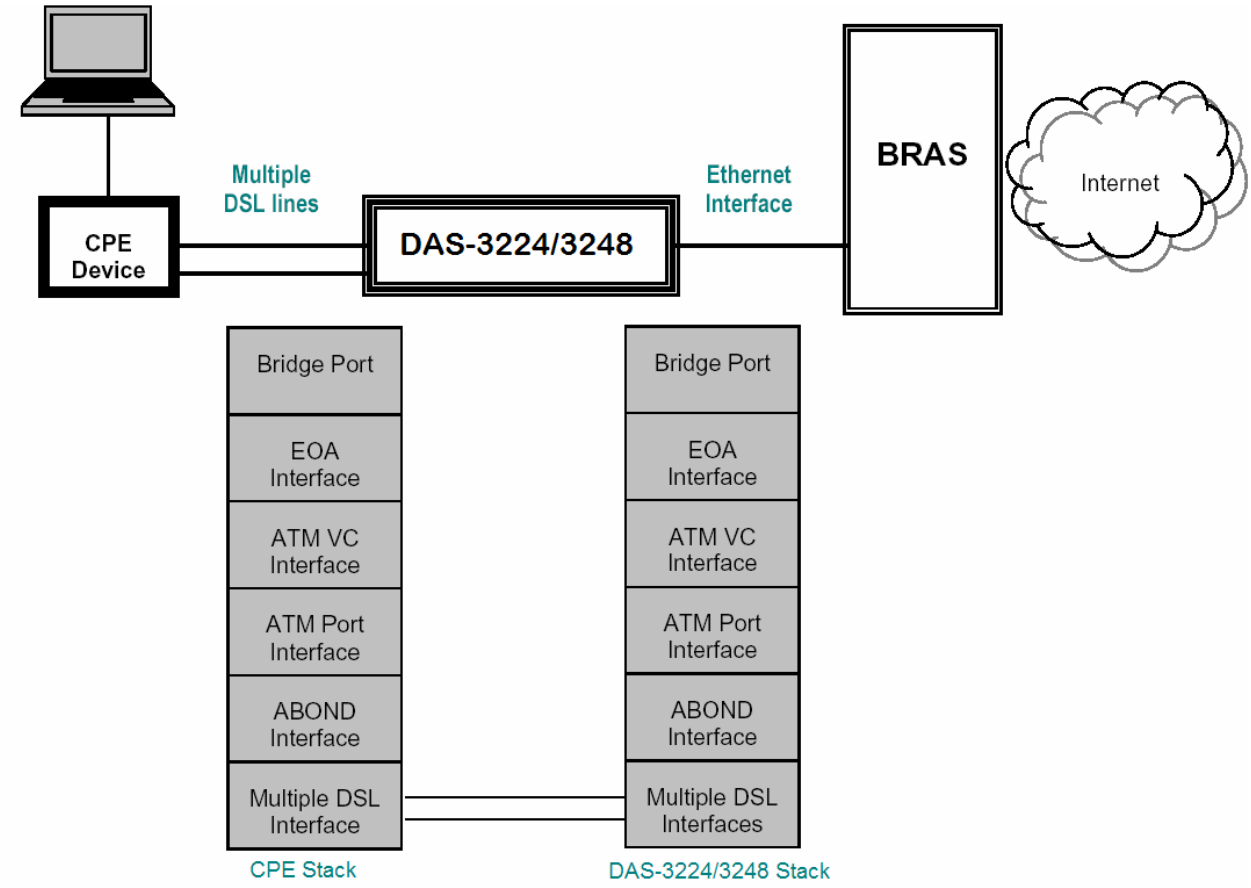


Рисунок 5-2: Стек протоколов при использовании агрегации DSL.

Для использования агрегации DSL необходимо создать нужные стеки протоколов на CO и CPE оборудовании. Рис. 5-2 отображает конфигурацию стеков CO и CPE для типичного сценария использования агрегации DSL соединений.
Если все необходимые интерфейсы созданы, DSLAM и ADSL модем начинают обмениваться данными, используя следующую процедуру:

1. DSLAM посылает CPE сообщения ASM для инициализации агрегирования.
2. CPE подтверждает инициализацию.

3. После успешной инициализации агрегирования DSLAM начинает вставлять SID во все ATM ячейки, следующие в направлении downstream.
4. CPE получает данные ячейки и восстанавливает исходный порядок их следования по SID.
5. Аналогично DSLAM, CPE также вставляет в посылаемые в upstream направлении ATM ячейки идентификаторы SID, которые используются DSLAM для восстановления правильного порядка следования ячеек.
6. DSLAM и CPE регулярно (не реже одного раза в секунду) обмениваются сообщениями ASM для поддержания текущего агрегирования и информирования напарника обо всех изменениях в конфигурации.

5.2 Построение стека протоколов на DAS-3248 для агрегации DSL соединений

Для того чтобы создать необходимый для функционирования агрегации DSL линков стек протоколов на DAS-3248 необходимо:

- создать интерфейс ABOND Group;
- добавить DSL интерфейсы в ABOND Group;
- настроить одинаковую задержку на данных интерфейсах;
- отключить DataBoost на выбранных ADSL интерфейсах;
- настроить формат SID с помощью конфигуратора глобальных системных параметров nbsize;
- настроить формат SID при настройке группы;
- настроить VPI, VCI управляющего VC;
- включить abond link;
- включить интерфейс Abond Group;
- создать ATM порт поверх интерфейса ABOND;
- создать один из трех возможных стеков протоколов.

Рассмотрим каждый шаг подробнее.

5.2.1 Создание, просмотр статуса, изменение и удаление ABOND group

Имена ABOND group интерфейса лежат в интервале **abond-0 .. abond-31**. Параметр Group ID должен быть уникальным для каждого ABOND интерфейса. Если скорость агрегированного соединения окажется ниже сконфигурированных значений, работа данной группы будет невозможна. По умолчанию протокол ASM включен. Его отключение повлечет за собой отключение функций передачи и обработки ASM сообщений. Значения по умолчанию для параметров **MinAggrRateUpstrm** и **MinAggrRateDnstrm** равны нулю. Это означает, что ABOND интерфейс не будет учитывать их при переходе из состояния down в состояние up. Параметры Diffdelaytoldnstrm и Diffdelaytolupstrm отображают максимально возможную дифференциальную задержку в downstream и upstream направлениях соответственно. На настоящий момент максимальное и значение по умолчанию параметра Diffdelaytolupstrm

составляют 4 мс. Для параметра Diffdelaytoldnstrm максимальное и значение по умолчанию составляют 24 мс и 4 мс соответственно. Пользователь должен настроить ADSL интерфейсы таким образом, чтобы разница их задержки на interleaving (дифференциальная задержка) не превосходила значения, сконфигурированные для ABOND интерфейса.
Параметр Linkhecthreshold указывает порог ошибок HEC в процентах от пропускной способности канала и отражает его качество.
Numoflinkupforgrpup определяет число каналов, которые должны находиться в состоянии up, перед тем как агрегированный интерфейс будет пытаться, используя протокол ASM, начать передачу по агрегированному каналу.
ASMIrlThreshold определяет число буферов, которые будут использоваться для полученных сообщений ASM. Максимальное и значение по умолчанию данного параметра равны 8.
Atmportusrate используется для вычисления размера буфера, необходимого для изменения порядка следования ATM ячеек по их SID.

Команды системы:

create abond group intf ifname

Описание: Создает abond group интерфейс с заданными параметрами.
Синтаксис команды: create abond group intf ifname ifname groupid groupid [minaggrrateupstrm minaggrrateupstrm] [minaggrratednstrm minaggrratednstrm] [diffdelaytolupstrm diffdelaytolupstrm] [diffdelaytoldnstrm diffdelaytoldnstrm] [asmprotocol Enable | Disable] [sidformat EightBitSid | TwelveBitSid] [maxrxbitrateratio maxrxbitrateratio] [linkhecthrshld linkhecthrshld] [numoflinksupforgrpup One | All] [asmirlthreshold asmirlthreshold] [maxatmportusrate maxatmportusrate]

get abond group intf

Описание: Отображает текущее состояние и параметры abond group интерфейса.
Синтаксис команды: get abond group intf [ifname ifname]

delete abond group intf ifname

Описание: Удаляет заданный abond group интерфейс.
Синтаксис команды: delete abond group intf ifname ifname

modify abond group intf

Описание: Изменяет состояние и/или параметры abond group интерфейса.

Синтаксис команды: modify abond group intf ifname ifname [groupid groupid] [minaggrrateupstrm minaggrrateupstrm] [minaggrratednstrm minaggrratednstrm] [diffdelaytolupstrm diffdelaytolupstrm] [diffdelaytoldnstrm diffdelaytoldnstrm] [asmprotocol Enable | Disable] [sidformat EightBitSid | TwelveBitSid] [maxrxbitrateratio maxrxbitrateratio] [linkhecthrshld linkhecthrshld] [numoflinksupforgrpup One | All] [asmirlthreshold asmirlthreshold] [maxatmportusrate maxatmportusrate] [enable | disable]

Таблица параметров:

ifname ifname	Имя ABOND интерфейса служит для идентификации и обращения к нему. Возможные значения abond-x. Изменение и удаление данного интерфейса невозможно, если он включен. **Использование:** Create – Обязательно. Delete – Обязательно. Get – Опционально. Modify – Обязательно. **Принимает значения:** abond-0.. abond-31
groupid groupid	Идентификатор группы. Данное поле конфигурируется статически во время создания группы и не должно изменяться. Этот параметр может быть использован для обнаружения ошибок в конфигурации или помощи в управлении агрегированным соединением. **Использование:** Create - Обязательно. Modify – Опционально.
minaggrrateupstrm minaggrrateupstrm	Минимальная агрегированная скорость (в бит/с) в направлении upstream. **Использование:** Create - Опционально. Modify – Опционально. **По умолчанию:** 0
minaggrratednstrm minaggrratednstrm	Минимальная агрегированная скорость (в бит/с) в направлении downstream. **Использование:** Create - Опционально. Modify – Опционально. **По умолчанию:** 0
diffdelaytolupstrm diffdelaytolupstrm	Максимальная дифференциальная задержка среди ADSL соединений, входящих в группу, в направлении Upstream. **Использование:** Create - Опционально. Modify - Опционально. **Принимает значения:** 0 – 4 мс. **По умолчанию:** 4 мс.
diffdelaytoldnstrm diffdelaytoldnstrm	Максимальная дифференциальная задержка среди ADSL соединений, входящих в группу, в направлении

	Downstream. **Использование:** Create - Опционально. Modify - Опционально. **Принимает значения:** 0 – 24 мс. **По умолчанию:** 4 мс.
asmprotocol Enable | Disable	Включение/выключение протокола ASM. При отключении данного протокола произойдет статическая привязка ADSL соединений в группу агрегирования. DAS-3248 будет считать, что CPE известны все параметры конфигурации (формат SID, число линков в группе и их идентификаторы). При включении данного протокола DSLAM будет автоматически информировать CPE о значении этих параметров путем рассылки ASM сообщений. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения:** enable or disable **По умолчанию:** enable
sidformat EightBitSid | TwelveBitSid	Формат SID: 8 или 12 бит. **Использование:** Create – Опционально. Modify – Опционально. **По умолчанию:** 12 бит
maxrxbitrateratio maxrxbitrateratio	Максимальная величина отношения значений пропускной способности ADSL соединений, входящих в группу агрегации, в направлении upstream. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения :** 1 - 4 **По умолчанию:** 4
linkhecthrshld linkhecthrshld	Значение отношения количества ошибок HEC к пропускной способности upstream (в процентах), которое будет использоваться как порог при принятии решения – может ли данный ADSL канал стать членом группы. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения:** 1 - 10 **По умолчанию:** 2
numoflinksupforgrpup One | All	Число ADSL линков, находящихся в состоянии up, необходимое для запуска ASM протокола. **Использование:** Create - Опционально. Modify – Опционально. **По умолчанию:** One
asmirlthreshold asmirlthreshold	Порог IRL (Input Rate Limiting) для ASM сообщений. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения:** 1 - 8 **По умолчанию:** 8

maxatmportusrate maxatmportusrate	Максимальная пропускная способность ATM порта. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения:** 0 - 8000 **По умолчанию:** 4000
enable | disable	Административное состояние интерфейса. **Использование:** Create – Опционально. Modify – Опционально. **Принимает значения:** enable, disable **По умолчанию:** enable

5.2.2 Управление DSL интерфейсами, входящими в группу агрегации

Команды системы:

create abond link entry ifname

Описание: Добавление ADSL интерфейса в группу агрегации.
Синтаксис команды: create abond link entry ifname ifname lowif lowif [txlinkadminstatus Enable | Disable] [rxlinkadminstatus Enable | Disable]

get abond link entry

Описание: Просмотр списка интерфейсов, входящих в группу агрегации.
Синтаксис команды: get abond link entry [ifname ifname] [lowif lowif]

delete abond link entry ifname

Описание: Удаление ADSL интерфейса из группы агрегации.
Синтаксис команды: delete abond link entry ifname ifname lowif lowif

modify abond link entry ifname

Описание: Изменение параметров ADSL интерфейса, входящего в группу агрегации.
Синтаксис команды: modify abond link entry ifname ifname lowif lowif [txlinkadminstatus Enable | Disable] [rxlinkadminstatus Enable | Disable]

Таблица параметров:

ifname ifname	Имя ABOND интерфейса служит для идентификации и обращения к нему. Возможные значения abond-x. Изменение и удаление данного интерфейса невозможно, если он включен. **Использование:** Create – Обязательно. Delete – Обязательно. Get – Опционально. Modify – Обязательно. **Принимает значения:** abond-0.. abond-31
lowif lowif	Идентификатор DSL интерфейса. **Использование:** Create - Обязательно. Modify – Обязательно. Delete – Обязательно. Get – Опционально. **Принимает значения:** dsl-X, dsli-X, dslf-X
txlinkadminstatus txlinkadminstatus	Указывает, будет ли производиться передача данных через данное соединение. **Использование:** Create - Опционально. Modify – Опционально. **По умолчанию:** Enable
rxlinkadminstatus rxlinkadminstatus	Указывает, будет ли производиться прием данных через данное соединение. **Использование:** Create - Опционально. Modify – Опционально. **По умолчанию:** Enable

5.2.3 Настройка дифференциальной задержки DSL соединений

На настоящий момент DAS-3248 поддерживает только нулевое значение дифференциальной задержки в upstream и downstream направлениях. Следовательно, пользователь должен обеспечить требуемое значение дифференциальной задержки путем соответствующей настройки DSL соединений.

Команды системы:

modify adsl line profile

Описание: Изменение параметров adsl профайла DSL порта.

Синтаксис команды: modify adsl line profile ifname <interface-name> atucmaxintldelay <value> aturmaxintldelay <value>

Таблица параметров:

ifname ifname	Имя ADSL интерфейса, которому принадлежит данный профайл. Возможные значения dsl-xx. Изменение профайла невозможно пока включен соответствующий ADSL интерфейс. **Использование:** Get – Опционально. Modify – Обязательно. **Принимает значения:** dsl-0.. dsl-23 (47)
atucmaxintldelay atucmaxintldelay	Конфигурируемое максимальное значение задержки интерливинга для interleave канала в downstream направлении. Данная задержка применяется только к данным interleave канала и определяет разницу во времени между байтами на входе интерливера и их эквивалентами на его выходе. Большие значения данной задержки ведут к лучшему разделению последовательных входных байт в выходном потоке, позволяя повысить устойчивость системы к импульсным шумам. **Использование:** Modify – Обязательно. **Принимает значения:** 0 – 255 **По умолчанию:** 63
aturmaxintldelay aturmaxintldelay	Конфигурируемое максимальное значение задержки интерливинга для interleave канала в upstream направлении. Данная задержка применяется только к данным interleave канала и определяет разницу во времени между байтами на входе интерливера и их эквивалентами на его выходе. Большие значения данной задержки ведут к лучшему разделению последовательных входных байт в выходном потоке, позволяя повысить устойчивость системы к импульсным шумам. **Использование:** Modify – Опционально. **Принимает значения:** 0 - 255 **По умолчанию:** 16

Примечание*:* более подробно настройка ADSL профайлов рассмотрена в Главе 3.

5.2.4 Отключение DataBoost на ADSL линиях

DAS-3248 не поддерживает агрегирование DSL соединений при включенном databoost, поэтому пользователь должен выключить databoost на всех линиях, входящих в группу агрегирования.

Следующая команда служит для отключения databoost:

Команды системы:

modify adsl line profile

Описание: Изменение параметров adsl профайла DSL порта.
Синтаксис команды: modify adsl line profile ifname <interface-name> databoost disable

Таблица параметров:

ifname ifname	Имя ADSL интерфейса, которому принадлежит данный профайл. Возможные значения dsl-xx. Изменение профайла невозможно пока включен соответствующий ADSL интерфейс. **Использование:** Get – Опционально. Modify – Обязательно. **Принимает значения:** dsl-0.. dsl-23 (47)
databoost Enable | Disable	Включение/Выключение опции DataBoost **Использование:** Modify – Опционально. **Принимает значения:** Enable, Disable **По умолчанию:** Enable

5.2.5 Глобальное изменение формата SID

Команды системы:

modify nbsize

Описание: Изменение параметров глобальной конфигурации DAS-3248.
Синтаксис команды: modify nbsize abondglbsidfmt <eightbitsid/twelvebitsid>

get nbsize

Описание: Просмотр параметров глобальной конфигурации DAS-3248.
Синтаксис команды: get nbsize

Замечание: Данная команда изменяет глобальный формат SID, который будет использоваться всеми группами агрегирования. Форматом SID по умолчанию является 12-ти битный формат. Изменения в nbsize вступят в силу только после команды commit и перезагрузки DAS-3248. Если при изменении параметров группы формат SID не изменялся, то для данной группы будет использоваться формат, заданный в nbsize. Иначе – явно указанный при изменении параметров группы.

Таблица параметров:

abondglbsidfmt EightBitSid | TwelveBitSid	Формат SID, который будет использоваться для всех интерфейсов AbondGroup, которые могут быть созданы в системе. Изменения данного параметра вступят в силу после перезагрузки DSLAM. **Использование:** Modify – Опционально. **Принимает значения:** EightBitSid, TwelveBitSid **По умолчанию:** TwelveBitSid

5.2.6 Глобальное изменение значений VPI/VCI управляющего канала

modify nbsize

Описание: Изменение параметров глобальной конфигурации DAS-3248.
Синтаксис команды: modify nbsize abondglbctrlvpi <vpi value> abondglbctrlvci <vci value>

Замечание: Данная команда изменяет глобальные значения VPI/VCI, используемые всеми группами агрегирования для управляющего канала. Значения по умолчанию VPI = 0, VCI = 20. Изменения в nbsize вступят в силу только после команды commit и перезагрузки DAS-3248. Изменение значений VPI/VCI управляющего канала доступно только через nbsize, т.е. все группы имеют одинаковую пару значений VPI, VCI.

5.2.7 Изменение TxLinkAdminStatus и RxLinkAdminSatus ADSL соединений, входящих в группу

Для того чтобы данные могли передаваться через какое-либо ADSL соединение, входящее в группу агрегирования, параметр TxLinkAdminStatus должен быть включен.
Соответственно, чтобы через adsl соединение данные могли приниматься, должен быть включен параметр RxLinkAdminSatus. Изменение значений данных параметров может происходить в любое время, при этом уведомление о каждом изменении будет передано CPE в виде ASM сообщения.

Команды системы:
modify abond link entry ifname <interface name> **lowif** <interface name> **[txlinkadminstatus** <enable | disable>] **[rxlinkadminstatus** <enable | disable**>]**

5.2.8 Включение ABOND group интерфейса

Для работы группы агрегирования необходимо административно включить ABOND group интерфейс:
Команды системы:

modify abond group interface ifname <interface name> **enable**

Замечание: ABOND group interface не может быть включен, если в него входит меньше двух ADSL соединений. Параметры данного интерфейса могут быть изменены только после его выключения.

5.2.9 Создание ATM порта поверх ABOND интерфейса

Команды системы:

create atm port ifname <interface name> **lowif** <bondig interface name>

Замечание: команда создания ATM интерфейса вернет ошибку, если суммарная скорость ADSL портов, входящих группу агрегирования, будет меньше значения ORL, указанного для данного ATM порта.

Далее поверх созданного ATM порта нужно создать один из трех возможных стеков интерфейсов. Более подробно стеки интерфейсов описаны в главе 2.

6. Настройка Uplink Интерфейсов

Uplink интерфейсы – интерфейсы, которые могут быть использованы для подключения к IP backbone (магистрали).
На корпусе DAS-3248 они обозначены соответственно Uplink 1 и Uplink 2.
Соответствие Uplink интерфейсов их обозначениям во CLI интерфейсе приведены в таблице 6-1.

10/100/1000 BaseT/FX Uplink interface	UPLINK1	eth-0
10/100/1000 BaseT/FX Uplink interface	UPLINK2	eth-1

Таблица 6-1

Рисунок 6-1 отображает сеть доступа с использованием Uplink интерфейсов.

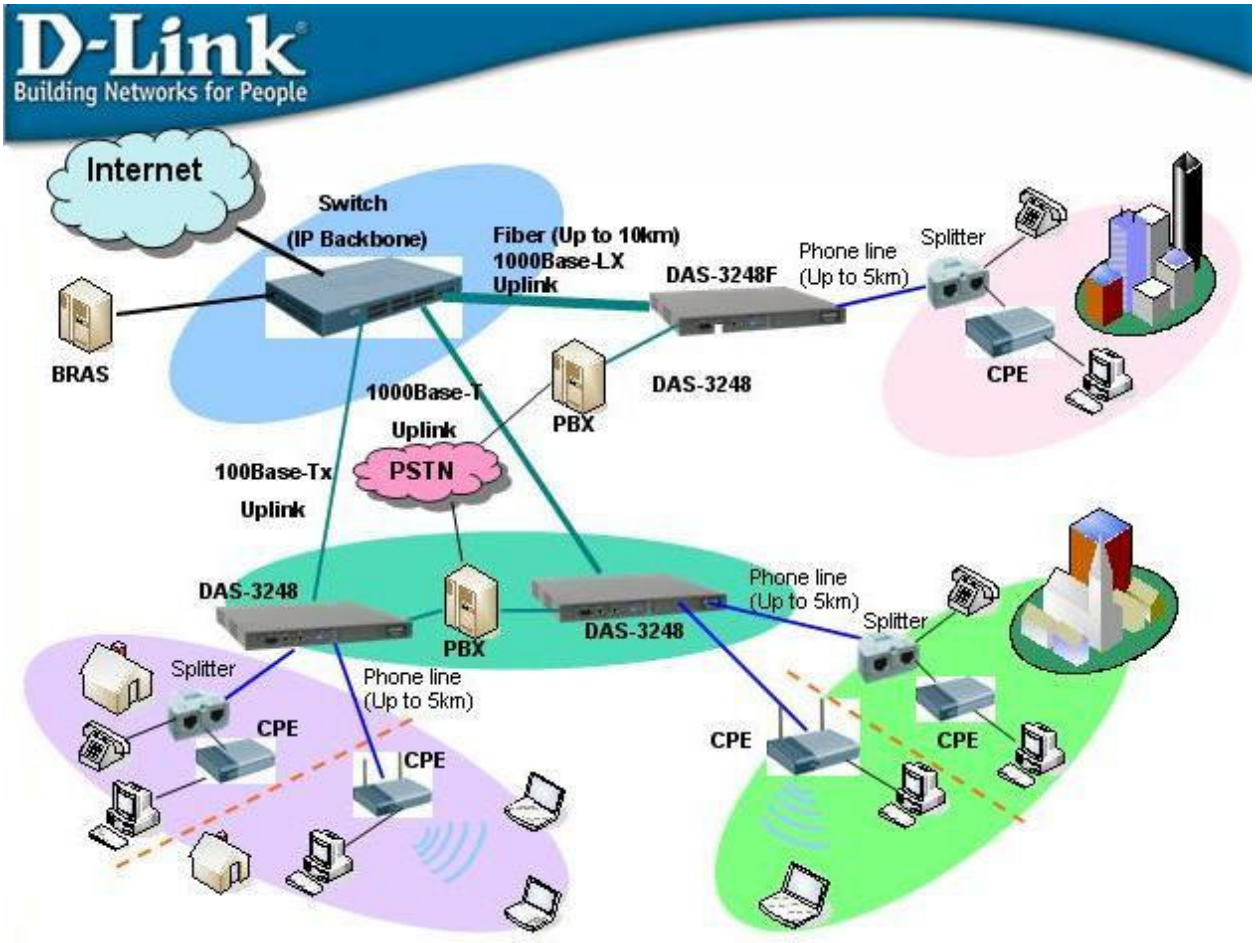


Рисунок 6-1.Пример сети доступа с использованием Uplink интерфейсов

6.1. Типы Uplink Интерфейсов.

Uplink интерфейсы могут применяться не только для подключения к IP Backbone, но и для стекирования.
DAS-3248 позволяет осуществлять стекирование до 8 устройств подобного себе типа (см. рис.2), увеличивая тем самым плотность портов и улучшая масштабируемость сети доступа. Таким образом, на одном узле доступа может быть сгруппировано до 384 портов.

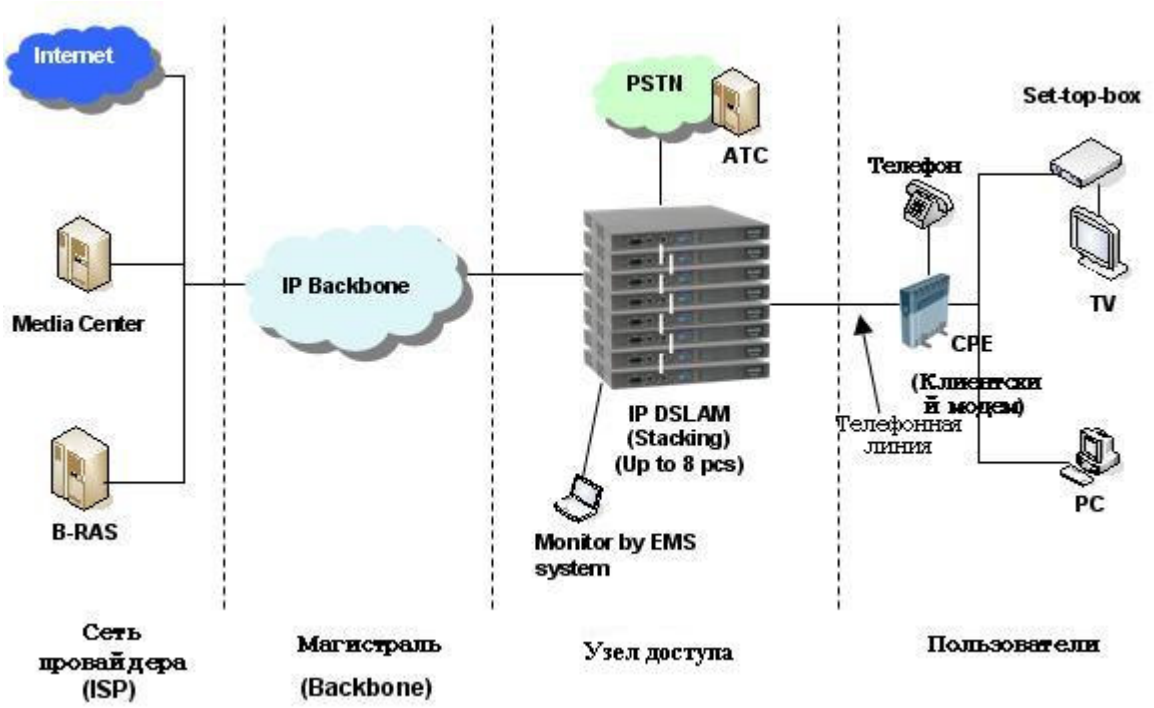


Рисунок 6-2.Пример сети доступа со стекирование DAS-3248

Поскольку для стекирования используются те же самые интерфейсы Uplink1(eth-0) и Uplink 2(eth-1), что и для подключения к IP backbone, для них вводится понятие типа интерфейса (Uplink- для подключения к магистрали, Downlink-для стекирования). Подробнее процесс настройки стекирования будет описан в разделе 6.4.

Тип интерфейса eth-0 (eth-1) задается параметром **type** при его создании командой **create ethernet intf**

Примечание: по умолчанию тип eth-0- uplink, eth-1- downlink

create ethernet intf
Описание: создать ethernet интерфейс
Синтаксис**:**

create ethernet intf *ifname* interface-name [ip *ip-address*] [mask *net-mask*] [type *uplink*|*downlink*][enable |disable]

(полный синтаксис команды смотрите в главе 1)

Пример 1:
Создать Uplink интерфейс eth-0 с IP 192.168.7.15:
$create ethernet intf ifname eth-0 **type uplink** ip 192.168.7.15 mask 255.255.255.0 enable

Экранный вывод:

```
Interface          : eth-0
Type               : Uplink        UseDhcp      : False
IP Address         : 192.168.7.15  Mask         : 255.255.255.0
Pkt Type           : ALL
Orl(mbps)          : 100
Configured Duplex  : Auto          Duplex       : Full
Configured Speed   : Auto
Class0thrshld      : 100           Class1thrshld: 100
Class2thrshld      : 100           Class3thrshld: 100
Class4thrshld      : 100           Class5thrshld: 100
Class6thrshld      : 100           Class7thrshld: 100
ProfileName        : SPPROFILE
Mgmt VLAN Index    : -
Tagged Mgmt PDU Prio: 0
Speed              : 100BT
Operational Status : Up            Admin Status : Up

Set Done
```

Пример 2:
Создать Downlink интерфейс eth-1:
$create ethernet intf ifname eth-1 **type downlink** enable

Экранный вывод:

```
Interface          : eth-1
Type               : Downlink      UseDhcp      : False
IP Address         : 0.0.0.0       Mask         : 0.0.0.0
Pkt Type           : ALL
Orl(mbps)          : 100
Configured Duplex  : Auto          Duplex       : None
Configured Speed   : Auto
Class0thrshld      : 100           Class1thrshld: 100
Class2thrshld      : 100           Class3thrshld: 100
Class4thrshld      : 100           Class5thrshld: 100
Class6thrshld      : 100           Class7thrshld: 100
ProfileName        : SPPROFILE
Mgmt VLAN Index    : -
Tagged Mgmt PDU Prio: -
Speed              : -
Operational Status : Down          Admin Status : Up
Set Done
```

Важно:

1.Тип интерфейса назначается **только** при его создании и **не может изменяться**. Для изменения типа eth интерфейса его необходимо удалить и вновь создать с другим типом.

2.Только один интерфейс из двух (eth-0 и eth-1) может быть Uplink, второй **обязательно** должен быть Downlink (исключение составляет случай, когда оба интерфейса используются внутри одного агрегированного линка (см. 6.3)).

3.Если типа интерфейса не указан явно CLI командой, он принимается как **uplink**.

6.2. Настройка скорости/дуплекса

Uplink интерфейсы позволяют настаивать их скорость (10Мбит/с, 100 Мбит/с, 1 Гбит/с или Авто) и дуплекс, то есть способность порта одновременно передавать и принимать ethernet пакеты (halfduplex, fullduplex или Авто).

Настройка скорости и дуплекса производится CLI командами

create ethernet intf

modify ethernet intf

create ethernet intf

Описание: создать ethernet интерфейс

Синтаксис:

create ethernet intf ifname *interface-name* [ip *ip-address*] [mask *net-mask*] [speed { *auto*|*10BT*|*100BT*|*1000BT* }] [enable |disable]
[duplex *half*|*full*|*auto*]

modify ethernet intf

Описание: изменить параметры ethernet интерфейса

Синтаксис:

modify ethernet intf ifname *interface-name* [ip *ip-address*] [mask *net-mask*] [speed {*auto*|*10BT*|*100BT*|*1000BT*}] [enable |disable]
[duplex *half*|*full*|*auto*]

(полный синтаксис команд смотрите в главе 1)

Пример:

$modify ethernet intf ifname eth-0 duplex half speed 100BT ip 192.168.7.15 mask 255.255.255.0 enable

Экранный вывод:

```
Interface       : eth-0
Type            : Uplink      UseDhcp     : False
IP Address      : 192.168.7.15  Mask      : 255.255.255.0
Pkt Type        : ALL
Orl(mbps)       : 100
```

```
Configured Duplex   : Half          Duplex      : Half
Configured Speed    : 100BT
Class0thrshld       : 100           Class1thrshld: 100
Class2thrshld       : 100           Class3thrshld: 100
Class4thrshld       : 100           Class5thrshld: 100
Class6thrshld       : 100           Class7thrshld: 100
ProfileName         : SPPROFILE
Mgmt VLAN Index     : -
Tagged Mgmt PDU Prio: 0
Speed               : 100BT
Operational Status  : Up            Admin Status : Up

Set Done
```

Важно: Параметры скорости и дуплекса связаны друг с другом, поэтому в CLI команде должны присутствовать оба этих параметра, даже если изменяется только один из них.

6.3. Агрегирование каналов. Функция Link Aggregation.

Агрегирование каналов (Link Aggregation) - технология, позволяющая объединять несколько однотипных сетевых физических соединений в одно логическое для увеличения пропускной способности.

Ограничения технологии агрегирования каналов для DAS-3248:

1) агрегироваться могут только Uplink Ethernet интерфейсы, обозначенные на устройстве как Uplink1 и Uplink2);
2) максимальное количество агрегированных интерфейсов для устройства - один;

Пример сети доступа с использованием Link Aggregation приведен на рис.3.

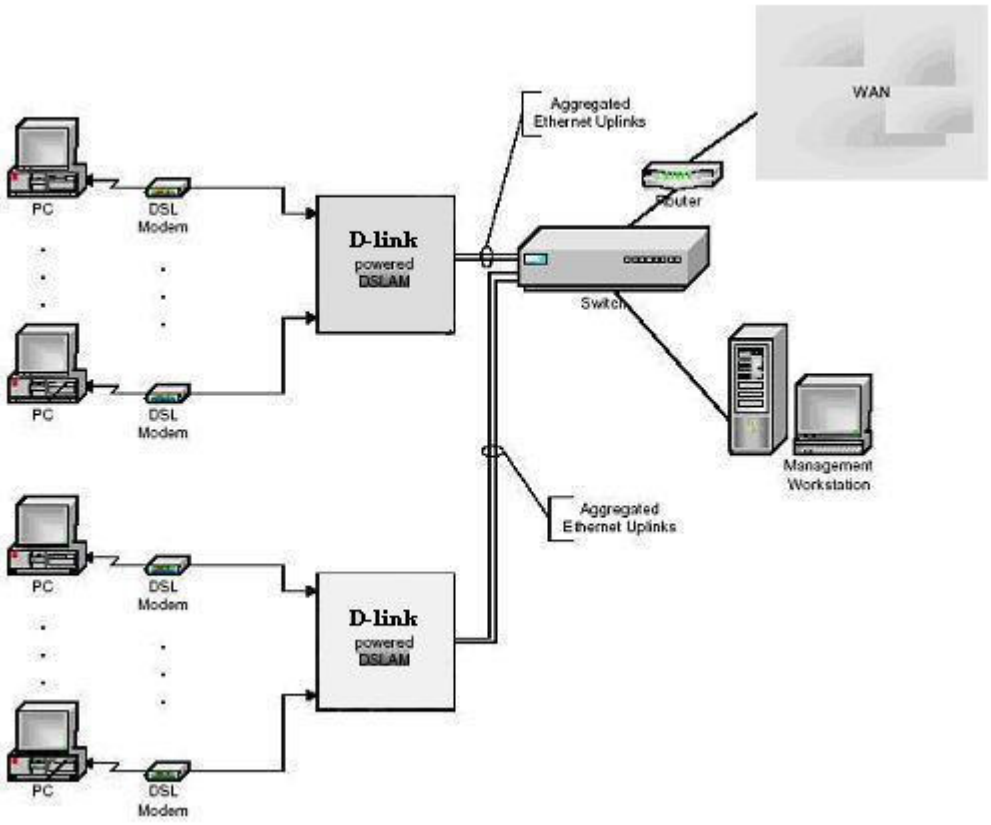


Рисунок 6-3: Использование Link Aggregation.

6.3.1. Виды Link Aggregation

Существует два вида агрегации линков:

а) статическая (Static Bounding)
б) динамическая (LACP)

Статическое агрегирование не стандартизировано, поэтому совместимость устройств различных производителей при использовании Static Bonding не гарантируется.

Протокол динамической агрегации каналов LACP определяется общепринятым стандартом IEEE 802.3ad.

Главное отличие LACP от Static Bounding состоит в том, что LACP позволяет динамически добавлять и удалять физические интерфейсы в Link Aggregation, для чего по агрегированному каналу передаются специальные кадры протокола LACP (LACPDU). Тогда как при Static Bounding группа конфигурируется вручную, и изменение ее состава требует вмешательства человека.
Однако, в обоих случаях при выходе из строя одного из физических интерфейсов, входящих в группу, происходит автоматическое перераспределение трафика между оставшимися интерфейсами.

6.3.2. Понятие, функции и структура агрегированного интерфейса (aggregator)

Для Link Aggregation в DAS-3248 специально введено понятие агрегированного интерфейса (aggregator).
Aggregator - это логический интерфейс, занимающий промежуточное положение между физическими Ethernet интерфейсами и Bridge интерфейсом.
Соответствующий стек интерфейсов DAS-3248 изображен на рис. 4.

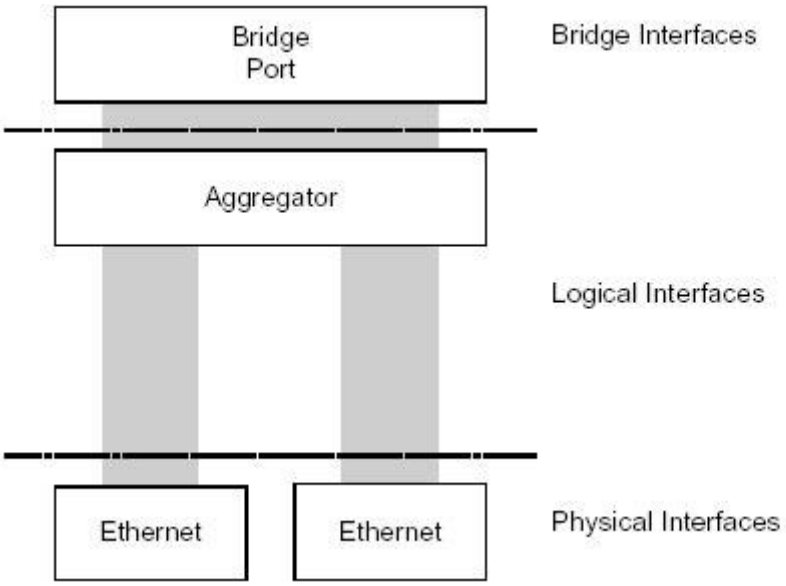


Рисунок 6-4: Стек интерфейсов DAS-3248 при использовании Link Aggregation.

Aggregator собирает трафик с нескольких физических интерфейсов и направляет его в виде одного потока вышележащему bridge порту. В обратном направлении данный интерфейс получает трафик от bridge порта и распределяет его между физическими интерфейсами, входящими в Link Aggregation .

Структура агрегированного интерфейса показана на рис.6-5:

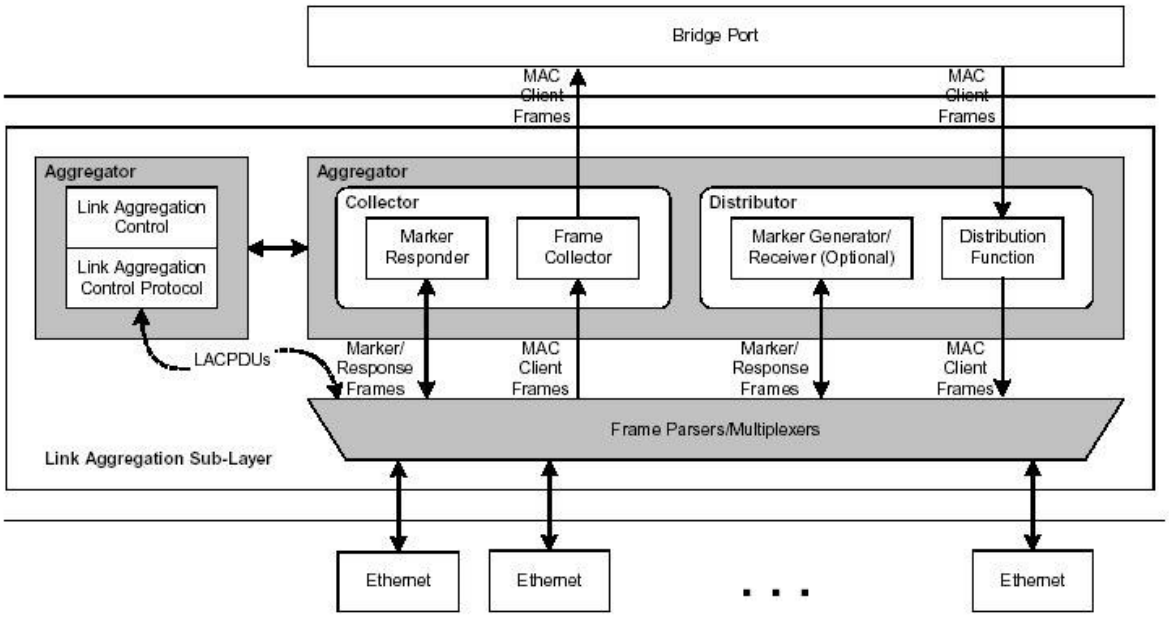


Рисунок 6-5: Архитектура агрегатора.

Функцию распределения трафика обеспечивает блок агрегированного интерфейса, названный Distributor.
Дистрибьютор на основе определенных критериев разделяет единый поток трафика, полученный от bridge port-а, на множество элементарных потоков и направляет каждый элементарный поток в соответствующий Ethernet интерфейс. Несколько элементарных потоков могут быть переданы через один и тот же линк, но один и тот же элементарный поток может быть передан только через один Ethernet интерфейс. Такое разделение на элементарные потоки и ассоциирование элементарного потока только с одним Ethernet интерфейсом очень важно для обеспечения доставки кадров данного потока в правильной последовательности. Т.к. каждый элементарный поток ассоциирован только с одним Ethernet интерфейсом, то во время использования агрегации линков очередность следования кадров каждого элементарного потока будет сохранена.

Критерии, используемые для классификации трафика в элементарные потоки, различны и зависят от конкретной реализации. Для этих целей DAS-3248 использует MAC адрес источника, содержащийся в заголовке каждого кадра.

В обратном направлении Frame Collector располагает кадры, полученные от различных Ethernet интерфейсов, в нужном порядке в общей очереди. Далее кадры из данной очереди передаются на bridge port. Порядок, в котором кадры были получены на индивидуальном Ethernet интерфейсе, будет сохранен также в общей очереди (это необходимо для обеспечения последовательной доставки). См. рис. 6-6.

Иногда бывает нужно передать элементарный поток с одного Ethernet интерфейса на другой. Этого можно достигнуть двумя способами:

- подождать некоторое время перед началом отправления кадров через новый интерфейс

- использовать некий протокол для синхронизации

Традиционный подход предполагает, что отправитель данных на некоторое время прекращает передачу через старый интерфейс и затем начинает передачу данных через вновь выбранный интерфейс, предполагая, что за время ожидания, получатель получит и доставит все кадры со старого интерфейса.

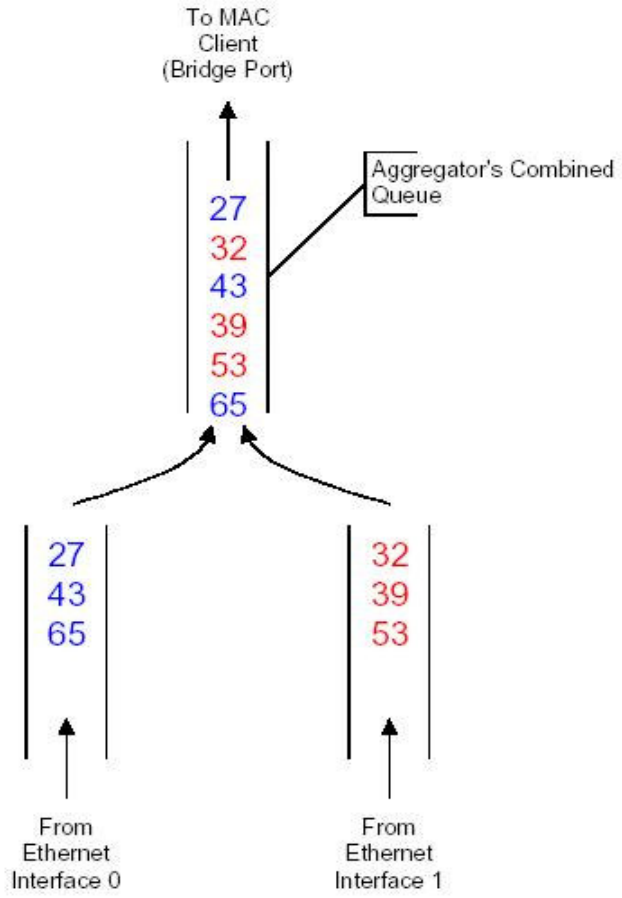


Рисунок 6-6: Сохранение исходной последовательности кадров.

Новый подход использует специальный маркерный протокол для синхронизации передачи. Отправитель посылает специальное маркерное сообщение через старый интерфейс, после этого передача каких бы то ни было данных через данный интерфейс прекращается.
После получения отправителем ответа на свое маркерное сообщение он знает, что все кадры, переданные ранее его маркерного сообщения, успешно получены на приемной стороне, и можно начинать передачу данных через вновь выбранный интерфейс

Генератор/Приемник маркеров отвечает за генерацию маркерных сообщений, а также за их прием и обработку. Ответчик маркеров (Marker Responder) служит для ответа на полученные маркерные сообщения путем отсылки сообщений marker response.

6.3.3. Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) предоставляет стандартное средство обмена информацией между двумя смежными устройствами для того, чтобы они могли динамически настраивать Link Aggregation. В отличие от Static Bonding, при использовании протокола LACP администратор только указывает потенциал агрегирования; реальное агрегирование осуществляется путем обмена пакетами LACPDU между оконечными системами.
Данный протокол работает путем обмена информацией о состояниях. Каждый партнер получает информацию о состоянии своего партнера от него самого. LACPDU, посылаемый каждым устройством, содержит информацию о его текущем состоянии (actor information) и его собственное представление о состоянии своего партнера (partner information). Если будет найдено несоответствие, то произойдет обмен LACPDU, который позволит исправить данную ситуацию. Формат LACPDU кадра представлен на рис. 6-7.

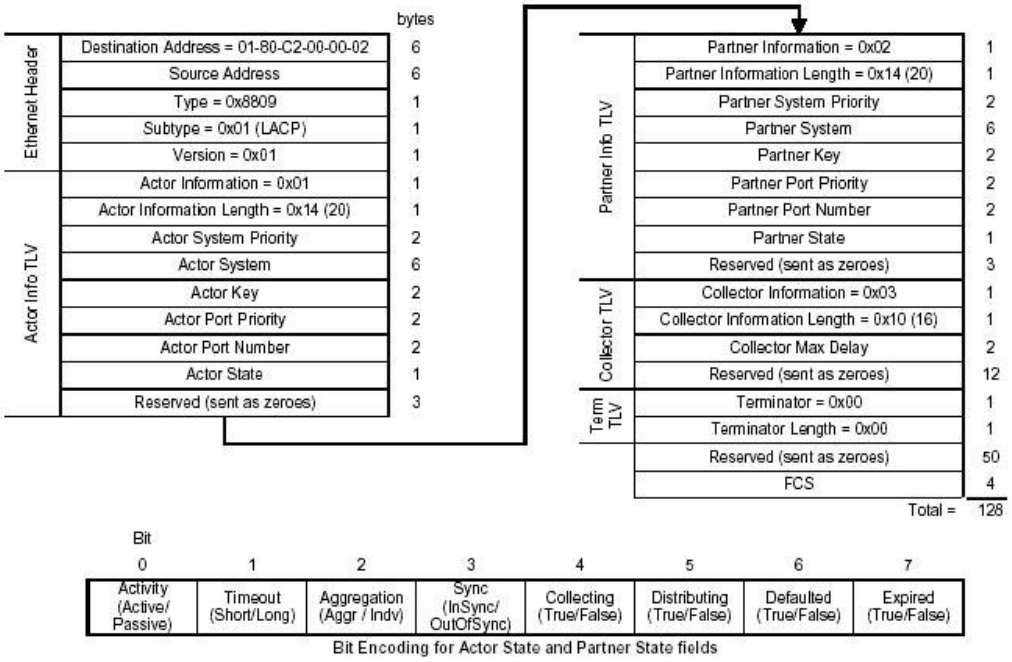


Рисунок 6-7: Формат LACP кадра.

Обмен LACPDU происходит независимо для каждого линка и является линкозависимым. Данные PDU никогда не выйдут за пределы того линка, через который они были посланы.

Active / Passive

Каждая оконечная система может участвовать в агрегировании как Активный или Пассивный партнер. Активный партнер периодически посылает LACPDU независимо от состояния своего партнера. Пассивный партнер напротив, посылает LACPDU, только если его партнер является Активным.

> Примечание: Если оба партнера настроены пассивными, они никогда не смогут обменяться LACPDU друг с другом и агрегирование не будет реализовано. Таким образом, для успешного установления LACP агрегированного линка необходимо, чтобы один из партнеров был сконфигурирован как активный.

Slow / Fast Periodic Transmission

LACPDU периодически передаются обеими оконечными системами для обмена информацией об агрегировании. Посылка LACPDU происходит либо с низкой частотой (раз в 30 секунд), либо с высокой (раз в 1 секунду). Это зависит от того, использует партнер длинные тайм-ауты (90 секунд) или короткие (3 секунды).

System ID

Каждая оконечная система при агрегировании идентифицируется уникальным System ID. System ID - это обычно MAC адрес данной системы, предваряемый 2-байтным System Priority (рис.8).
Чтобы избежать синхронных изменений на обеих оконечных системах, которые могут помешать переходу линка в стабильное состояние, динамически изменять извещения о своих возможностях разрешено только конечной системе Link Aggregation имеющей наименьший System ID.

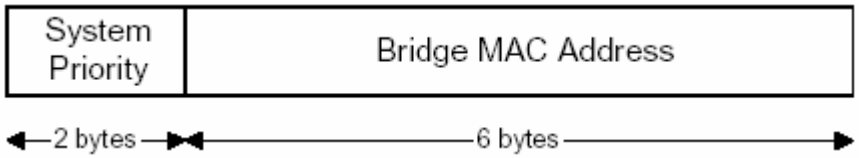


Рисунок 6-8: Структура System ID

Администратор может контролировать соответствующие числовые значения System ID путем соответствующей настройки System Priority.

Port ID

Подобно System ID, каждому способному к агрегации порту в оконечной системе присваивается Port ID (рис.6-9). Port ID – это пара значений номера порта (Port Number) и приоритета порта (Port Priority).

Примечание: Port Priority играет роль, аналогичную System Priority в System ID и никак не связан с QoS.

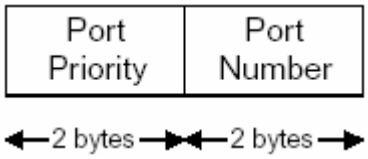


Рисунок 6-9: Структура Port ID

Ключ

Оконечная система при использовании System ID может обнаружить, что некое множество ее линков оканчиваются на смежной партнерской системе, однако данное обстоятельство не является достаточной причиной для того, чтобы агрегировать эти линки, поскольку партнер может быть не готов к такому взаимодействию.

Для сигнализации о готовности двух устройств создать агрегированный линк друг с другом служит одинаковая величина ключа (Key). Значение ключа является административно присваиваемым и базируется на нескольких параметрах таких, например, как характеристики линка (например, 10 Мбит/с линки не могут агрегироваться с Fast Ethernet линками), аппаратные ограничения, сетевые ограничения, и политики.

Каждому порту, способному к агрегированию, административно присвоено некое значение ключа. Каждый aggregator в системе также имеет административно присвоенный ключ.

Система может помечать какой-либо из линков как отдельный линк, даже если ему присвоен ключ. Такой линк никогда не будет использоваться во время агрегирования.

Административно назначенные и рабочие значения

Существует два вида значений ключа и состояния: рабочие и административно заданные. Первые отражают значение, используемые в данный момент. Вторые – значения, настроенные администратором.

Административно назначенный набор значений может быть также сконфигурирован и для соседнего устройства. Данный набор будет использован, если информация о партнере недоступна или устарела. Таким образом, данный сосед также будет иметь два набора значений – рабочий (текущие значения) и административный (значения, которые будут использованы, если информация о партнере недоступна).

Группа Link aggregation

Линки, оканчивающиеся на одной и той же смежной системе и имеющие один ключ для обеих систем, принадлежат одной Link Aggregation Group (LAG).
Каждая такая группа идентифицируется уникальным LAG ID, который формируется комбинацией следующих параметров каждой из смежных систем:

- system ID
- текущее значение ключа
- Если линк является одиночным - Port ID, в противном случае 0

Например, если System ID двух смежных систем - S и T . Значения ключей, назначенные данному линку S и T равны соответственно 100 и 200, то LAG ID будет [(S, 100, 0), (T, 200, 0)]. Пусть, данные системы имеют 6 общих линков, пронумерованных от 1 до 6. Значения ключей и выбор типа линка (член агрегированной группы/одиночный), заданные администратором, показаны в табл. 2. Последний столбец данной таблицы отображает результирующий LAG ID для каждого линка. Анализ данных LAG ID ведет к следующим выводам:

- линки 1, 2 и 5 имеют один и тот же LAG ID, следовательно, могут быть агрегированы вместе;
- хотя система S сконфигурировала линки 3 и 4 как агрегируемые, но, поскольку T назначила им другие ключи, они не могут быть агрегированы;

- хотя обе системы S и T назначили ключи 4 и 6 таким образом, чтобы допустить возможность агрегирования, тем не менее, т.к. линк 6 помечен как одиночный оконечной системой S, агрегирование невозможно.

Link/ Port	System S		System T		LAG Id
	Key	Aggr/ Indv	Key	Aggr/ Indv	
1	100	A	200	A	[(S, 100, 0), (T, 200, 0)]
2	100	A	200	A	[(S, 100, 0), (T, 200, 0)]
3	150	A	200	A	[(S, 150, 0), (T, 200, 0)]
4	150	A	300	A	[(S, 150, 0), (T, 300, 0)]
5	100	A	200	A	[(S, 100, 0), (T, 200, 0)]
6	150	I	300	A	[(S, 150, 6), (T, 300, 0)]

Таблица 6-2: Пример агрегированной группы.

Реализация агрегирования и изменение настроек

LACP агрегирование реализовано следующим образом:

1. **Порт определяет свой LAG ID.**

Порт идентифицирует свой LAG ID исходя из рабочих величин, полученных как из своих административно задаваемых параметров, так и с помощью LACPDU.

2. **Соглашение обоих партнеров о LAG ID.**

Каждая конечная система проверяет LAG ID своего партнера, и в случае обнаружения различия системы обмениваются LACPDU, пытаясь скорректировать ситуацию.

3. **Порт присоединяется к совместимому Aggregator-у.**

Совместимый Aggregator – тот, который имеет тот же действующий ключ, что и присоединяемый порт. Все линки, присоединенные к Aggregator-у, имеют одинаковый LAG ID.

4. **Порт сигнализирует о своей готовности передавать данные пользователя.**

Бит синхронизации (Sync) устанавливается в поле состояния системы (Actor State - см. рис.5), и происходит отправка LACPDU другой оконечной системе, чтобы просигнализировать о готовности порта к передаче информации.

5. **Порт включает функцию сбора и распределения пакетов.**

Порт включает свой коллектор и информирует об этом другую оконечную систему, посылая LACPDU с установленным битом Collecting в Actor State (см. рис.6-7). После приема LACPDU с установленным Collecting битом, пришедший от своего партнера, включается дистрибьютор.

Примечание: Статус Transmit/Receive агрегатора является
логическим ИЛИ Distributing/Collecting статусов портов, присоединенных к агрегируемому интерфейсу.

После установления агрегирования, каждый входящий в него порт подвергается постоянному наблюдению для управления его членством в LAG. При обнаружении изменения состояния одного из портов, входящих в данную группу, которое больше не позволяет ему оставаться членом этой LAG (например, произошло изменение значения ключа), данный линк переводится из текущей группы в новую.

Чтобы отсоединиться от агрегатора, порт проходит следующую последовательность шагов:
1. Порт перестает выполнять функции сбора и распределения пакетов.
2. Порт сообщает блоку Distributor агрегированного порта, что он не больше является частью агрегированной группы.
3. Порт информирует своего партнера об изменении своей конфигурации.
4. Порт сообщает блоку Collector агрегированного интерфейса, что он больше не является частью агрегированной группы.

Обработка LACP PDU фреймов в DAS-3248.

LACPDU фреймы в соответствии со стандартом IEEE 802.3 имеют мультикастовый MAC адрес назначения 01:80:c2:00:00:02.
Действие, которое должно выполняться при приеме мультикастовых фреймов с MAC адресом назначения 01:80:c2:00:00:xx, определяется в DAS-3248 настройкой MAC профиля (resvdmac profile) , который может быть ассоциирован как с отдельной VLAN, так и со всем устройством (глобальный профиль). Варианты действий с пакетами: переслать (forwarding), отбросить(drop) или участвовать (participate).
Чтобы LACP работал, необходимо, чтобы над фреймами выполнялось действие participate. Кроме того, поскольку LACP работает на уровне ниже VLAN bridging, конфигурирование мультикастового адреса LACP должно быть выполнено в глобальном профиле.
Конфигурирование группового адреса 01:80:c2:00:00:xx в глобальном профиле приводит аннулированию любой привязки того же MAC адреса в профилях, связанных с отдельными VLAN.
Таким образом, исходя из вышесказанного, для функционирования LACP необходимо в глобальном MAC профиле добавить запись с мультикастовым адресом 01:80:c2:00:00:02 и действием Particpate прежде, чем включить и настроить LACP.

Последовательности CLI команд DAS-3248 для этого действия:

$get bridge tbg info
$create resvdmac profile param Profileid x mcastaddr 01:80:c2:00:00:02 action participate
или
$create resvdmac profile info profileid x
$create resvdmac profile param Profileid x mcastaddr 01:80:c2:00:00:02 action participate
$modify bridge tbg info resvmacprofileid x

Где x – номер MAC профиля.

Важно: DAS-3248 необходимая запись в resvdmac профиль уже добавлена по умолчанию.

6.3.4. Marker Protocol.

Протокол маркера (Marker Protocol) используется, чтобы синхронизировать передачу элементарного потока с одного на другой физический интерфейс агрегированной связи. Протокол базируется на простой модели запрос-ответ. Сообщения Marker Protocol являются 128-байтными фреймами Ethernet. Формат фрейма Marker Protocol показан на рис 6-10.

		bytes
Ethernet Header	Destination Address = 01-80-C2-00-00-02	6
	Source Address	6
	Type = 0x8809	1
	Subtype = 0x02 (Marker Protocol)	1
	Version = 0x01	1
TLV Tuple	Marker Info = 0x01 / Response Info = 0x02	1
	Information Length = 0x10 (16)	1
	Requester Port	2
	Requester System	6
	Requester Transaction Id	4
	Pad = 0x0000	2
Term TLV	Terminator = 0x00	1
	Terminator Length = 0x00	1
	Reserved (sent as zeroes)	90
	FCS	4
	Total =	128

Рисунок 6-10: Структура фрейма Marker Protocol

Каждая сторона может послать специальное маркерное сообщение (Marker Message) чтобы изменить конечную точку одного или более элементарных потоков кадров. Другая сторона при получении маркерного сообщения отвечает Marker Response, содержащим те же параметры Port/System/Transaction, что и исходном сообщении.

6.3.5.Команды CLI Link Aggregation на DAS-3248

Команды работы с агрегированным интерфейсом:

create lacp aggr

Описание: создание агрегированного (Aggregator) интерфейса.

Синтаксис команды:

create lacp aggr aggrifname *aggrifname* **[actorsystemprio** *actorsystemprio* **]** **[actoradminkey** *actoradminkey* **] [collectormaxdelay** *collectormaxdelay* **] [aggrtype** static | lacp **]**

modify lacp aggr

Описание: Изменение параметров агрегированного (Aggregator) интерфейса.

Синтаксис команды:

modify lacp aggr aggrifname *aggrifname* **[actorsystemprio** *actorsystemprio* **]** **[actoradminkey** *actoradminkey* **] [collectormaxdelay** *collectormaxdelay* **] [**aggrtype static | lacp **]**

delete lacp aggr

Описание: Удаляет агрегированный интерфейс.

Синтаксис команды:

delete lacp aggr aggrifname *aggrifname*

get lacp aggr

Описание: просмотр статуса агрегированного интерфейса.

Синтаксис команды:

get lacp aggr [aggrifname *aggrifname***]**

Пример:
$ get lacp aggr aggrifname aggr-0

Экранный вывод:

Output Aggr IfName : aggr-0	
Mac Address : 23:45:67:89:00:01	Aggregate : true
Actor Sys Priority : 2	Partner Sys Priority : 2
Actor Sys ID : 23:45:67:89:00:01	Partner Sys ID : 23:45:67:89:00:01 Actor
Oper Key : 10	Partner Oper Key : 2
Actor Admin Key : 1000	
Aggregation Type : Static	

Таблица описания параметр команд:

Параметр	Описание
aggrifname *aggrifname*	Имя агрегированного интерфейса Доступные значения: aggr-0…255. Обязательный параметр.
actorsystemprio *actorsystemprio*	2 октетная величина административно назначаемого приоритета в System ID.

	Доступные значения: 0..255. **Опциональный параметр.**
actoradminkey *actoradminkey*	Текущая величина Administrative Value Key. Доступные значения:1..65535. **Опциональный параметр.**
collectormaxdelay *collectormaxdelay*	16-битная величина (в десятках микросекунд), определяющая максимальную задержку, которая может навязываться блоком Collector агрегированного интерфейса. При превышении этой величины кадр считается устаревшим и отбрасывается.
aggrtype static | lacp	Тип Link Aggregation : Static Bounding или LACP. **Опциональный параметр.**

Команды работы с отдельными портами, входящими в Link Aggregation группу:

modify lacp aggrport info

Описание: Изменение параметров порта.

Синтаксис команды**:**

modify lacp aggrport info ifname *ifname* **[actoradminkey** *actoradminkey***]** **[partadminkey** *partadminkey***] [actorportprio** *actorportprio***] [partadminportprio** *partadminportprio***] [actorsysprio** *actorsysprio***] [partadminsysprio** *partadminsysprio***]** **[partadminsysid** *partadminsysid***]** **[partadminport** *partadminport***][actoradminstate** activity | timeout | aggr **]** **[partadminstate** activity | timeout| aggr**] [aggrstatus** enable|disable**]** **[pktpriority** *pktpriority* **]**

get lacp aggrport info

Описание**:** просмотр статуса порта.

Синтаксис команды**:**

get lacp aggrport info [ifname *ifname***]**

Пример:

$ get lacp aggrport info ifname eth-0

Экранный вывод:

Output Interface : eth-0	Port Is Aggregate : true
Actor Oper Key : 10	Partner Oper Key : 2
Actor Admin Key : 1000	Partner Admin Key : 2
Actor Port Priority : 1	Partner Admin Port Priority : 1

Actor System Priority : 2	Partner Oper Port Priority : 1
Actor System ID : 23:45:67:89:00:01	Partner Admin Sys Priority : 2
Actor Port : 2 Partner	Oper Sys Priority : 2
Partner Admin Sys Id : 23:45:67:89:00:01	Partner Admin Port : 1
Partner Oper Sys Id : 23:45:67:89:00:01	Partner Oper Port : 1
Port Actor Admin State : distrib	
Port Partner Admin State : activity	
Port Actor Oper State : default	
Port Partner Oper State : default	
Attached Agg ID : aggr-0	Selected Agg ID : aggr-0
Aggregation Status : Enable LACP	PacketsPrio :2

get lacp aggrport list

Описание**:** просмотр списка интерфейсов, входящих в состав агрегированный линк.

Синтаксис команды:

get lacp aggrport list

Пример:

$ get lacp aggrport list

Экранный вывод:

```
Output Aggr IfName : aggr-0
 Port List : eth-0 eth-1
```

get lacp aggrport stats

Описание**:** просмотр LACP статистики порта.

Синтаксис команды:

get lacp aggrport stats [ifname *ifname* **]**

Пример:

$ get lacp aggrport stats eth-0

Экранный вывод:

Interface : eth-0	
LACPDUs Rx : 1	LACPDUs Tx : 1
MarkerPDUs Rx : 1	MarkerPDUs Tx : 1
Marker Response PDUs Rx : 1	Marker Response PDUs Tx : 1
Unknown Rx : 1 Illegal Rx : 1	

reset lacp aggrport stats

Описание**:** сброс LACP статистики порта.

Синтаксис команды:

reset lacp aggrport stats ifname *ifname*

Таблица описания параметров команд:

Параметр	Описание
ifname *ifname*	Имя Ethernet интерфейса. **Обязательный параметр.**
actoradminkey *actoradminkey*	Текущая величина Administrative Value Key. Доступные значения:1..65535. **Опциональный параметр.**
partadminkey *partadminkey*	Текущая величина Administrative Value Key партнера. Доступные значения:1..65535. **Опциональный параметр.**
actorportprio *actorportprio*	1 байтная величина административно назначаемого приоритета Port Priority. Доступные значения:0..255. **Опциональный параметр.**
partadminportprio *partadminportprio*	1 байтная величина административно назначаемого приоритета Port Priority партнера. Доступные значения:0..255. **Опциональный параметр.**
actorsysprio *actorsysprio*	2 октетная величина административно назначаемого приоритета в System ID (System Priority). Доступные значения:0..255. **Опциональный параметр.**
partadminsysprio *partadminsysprio*	2 октетная величина административно назначаемого приоритета System ID (System Priority) партнера. Доступные значения:0..255. **Опциональный параметр.**
partadminsysid *partadminsysid*	6 байтный MAC адрес партнера в Systsem ID (Bridge MAC Address партнера). Доступные значения:00:00:00:00:00:00-FF:FF:FF:FF:FF:FF. **Опциональный параметр.**
partadminport *partadminport*	Номер порта партнера (Partner Port Number) Доступные значения: 0..65535. **Опциональный параметр.**
actoradminstate activity | timeout | aggr	Административное состояние. **Опциональный параметр.**

partadminstate activity | timeout| aggr	Административное состояние партнера. **Опциональный параметр.**
aggrstatus enable|disable	Триггер включения возможности агрегирования порта. **Опциональный параметр.**

Пример создания агрегированной связи на DAS-3248

а) статический Link Aggregation (Static Bounding):

	Команда	Действие
Шаг 1	$delete bridge port intf portid 385 $delete bridge port intf portid 386 $delete filter rule map ifname eth-0 stageid 1 ruleid 1 $delete ethernet intf ifname eth-0 $delete ethernet intf ifname eth-1	Удалить настройки по умолчанию интерфейсов eth-0 (Uplink 1) eth-1 (Uplink2).
Шаг 2	$create ethernet intf ifname eth-0 $create ethernet intf ifname eth-1	Создать eth-0 и eth-1 интерфейсы без IP адреса (он будет создан на агрегированном интерфейсе)
Шаг 3	$create aggr intf ifname aggr-0 ip 192.168.7.198 mask 255.255.255.0	Создать агрегированный интерфейс aggr-0 с IP 192.168.7.198
Шаг 4	$create lacp aggr aggrifname aggr-0 aggrtype **static**	Указать тип агрегированного интерфейса (Static Bounding)
Шаг 5	$ modify lacp aggrport info ifname eth-0 aggrstatus enable *$* modify lacp aggrport info ifname eth-0 aggrstatus enable	Указать, что eth-0 и eth-1 входят в состав агрегируемого линка.
Шаг 6	$ create bridge port intf portid 385 ifname aggr-0 status enable	Создать Bridge интерфейс поверх агрегированного интерфейса aggr-0
Шаг 7	$ get lacp aggrport list aggrifname aggr-0 $ get lacp aggr aggrifname aggr-0	Проверить настройки интерфейса aggr-0
Шаг 8	$ commit	Сохранить настройки

б) динамический Link Aggregation (LACP):

	Команда	Действие
Шаг 1	$delete bridge port intf portid 385 $delete bridge port intf portid 386 $delete filter rule map ifname eth-0 stageid 1 ruleid 1	Удалить настройки по умолчанию интерфейсов eth-0 (Uplink 1) eth-1 (Uplink2).

	$delete ethernet intf ifname eth-0 $delete ethernet intf ifname eth-1	
Шаг 2	$create ethernet intf ifname eth-0 $create ethernet intf ifname eth-1	Создать eth-0 и eth-1 интерфейсы без IP адреса (он будет создан на агрегированном интерфейсе)
Шаг 3	$create aggr intf ifname aggr-0 ip 192.168.7.198 mask 255.255.255.0	Создать агрегированный интерфейс aggr-0 с IP 192.168.7.198
Шаг 4	$create lacp aggr aggrifname aggr-0 aggrtype **lacp**	Указать тип агрегированного интерфейса (LACP)
Шаг 5	$modify lacp aggrport info ifname eth-0 aggrstatus enable $modify lacp aggrport info ifname eth-1 aggrstatus enable	Указать, что eth-0 и eth-1 входят в состав агрегируемого линка.
Шаг 6	$create bridge port intf portid 385 ifname aggr-0 status enable	Создать Bridge интерфейс поверх агрегированного интерфейса aggr-0
Шаг 7	$get lacp aggrport list aggrifname aggr-0 $get lacp aggr aggrifname aggr-0	Проверить настройки интерфейса aggr-0
Шаг 8	$ commit	Сохранить настройки

6.4.«Избыточное» отказоустойчивое агрегирование Uplink интерфейсов (Redundancy aggregation).

Redundancy aggregation – функция, которая позволяет использовать два Ethernet интерфейса DAS-3248 в качестве одной Uplink связи (агрегированного интерфейса) с распределенной загрузкой (load-sharing).
Если один из Ethernet интерфейсов отказывает, в этом случае вторая связь остается в работе и автоматически берет всю нагрузку на себя.
Принцип использования агрегированного интерфейса подобен функции Link aggregation, описанной в предыдущем разделе. Однако, разница между отказоустойчивым «избыточным» агрегированием и Link Aggregation функцией состоит в том, что Link aggregation предназначено в первую очередь для увеличения пропуской способности, а Redundancy Aggregation ставит своей главной целью отказоустойчивость. Кроме того, при «избыточном» агрегировании Ethernet интерфейсы могут оканчиваться не только на одном устройстве (рис.6-11), но и на различных устройствах (рис.6-12).

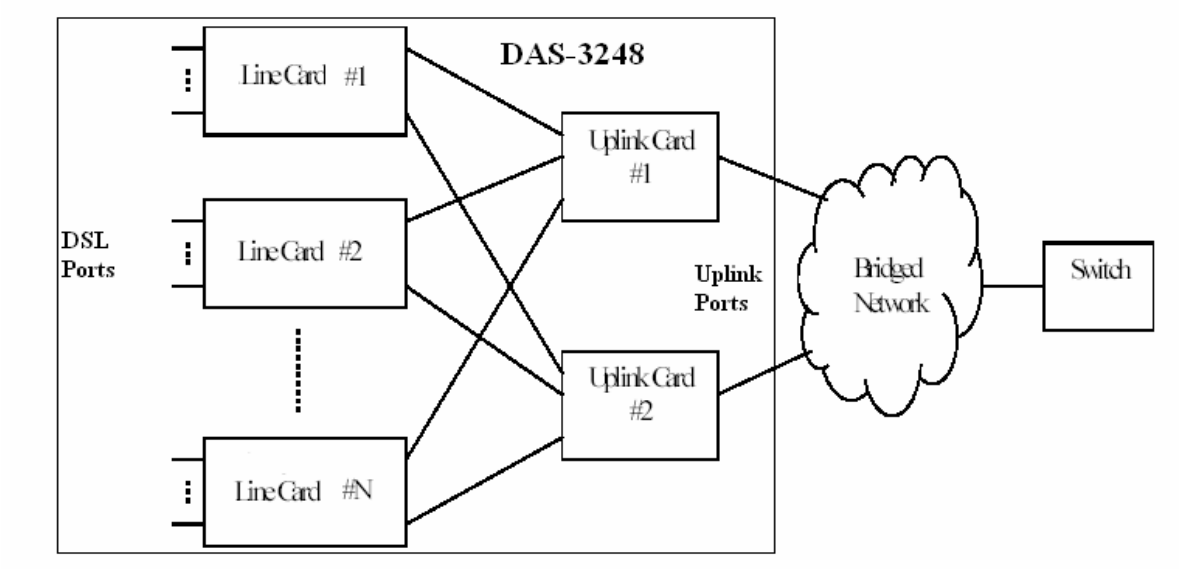


Рисунок 6-11.Схема сети доступа с использованием функции Redundancy Aggregation и коммутатора как точки конвергенции

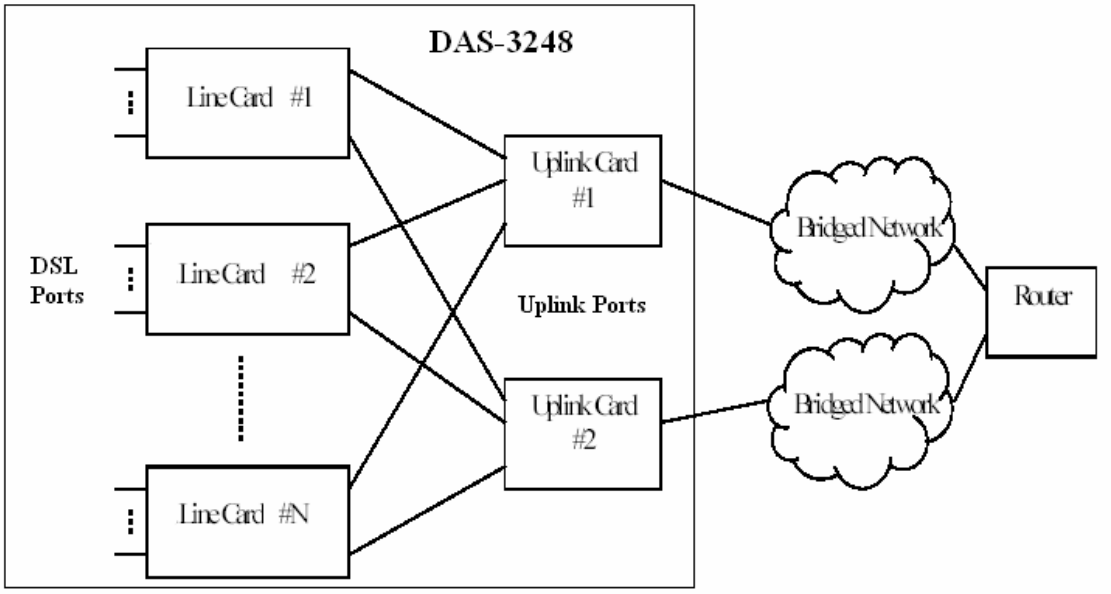


Рисунок 6-12.Схема сети доступа с использованием функции Redundancy Aggregation и маршрутизатора как точки конвергенции

6.4.1.Алгоритм работы функции.

1. Штатный режим:
   - Upstream трафик равномерно распределен по двум Uplink связям.
   - Оба порта Ethernet используются как один Bridge порт (т.е. логически для таблицы коммутации DAS-3248 как один интерфейс).
   - Ethernet связи могут завершаться на разных оконечных устройствах. В результате чего есть опасность получать один тот же широковещательный и групповой трафик от обеих связей. Следовательно, необходимо убедиться, что клиентские порты

устройства (порты DSL) будут получать только единственный экземпляр пакетов этого типа.

2. Случай, когда одна связей выходит из строя.
   - Система использует оставшуюся связь как единственную, и весь Upstream трафик пересылается через эту связь. В Downstream направлении, трафик также будет приходить только через оставшуюся в работе Uplink связь.
   - Когда отказавшая Uplink связь восстанавливает свою работоспособность, система возвращается в режим распределенной нагрузки.

6.4.2.Понятие Redundancy. Принцип распределения потока данных. Опции Redundancy aggregation.

DAS-3248 поддерживает понятие избыточности (redundancy).
Избыточность означает, что два интерфейса Ethernet будут обработаны из одной точки обучения таблицы коммутации DAS-3248 (то есть, таблица коммутации будет всегда иметь только одну запись для каждого MAC адреса, использующего один или более “избыточных” интерфейсов Ethernet).

Распределение потока данных.
Для коммутации Upstream потока при двух активных связях применяется распределение нагрузки, базирующееся на Source MAC (рисунки 6-13,6-14).
Когда одна из связей отказывается, весь трафик направляется по активной связи.

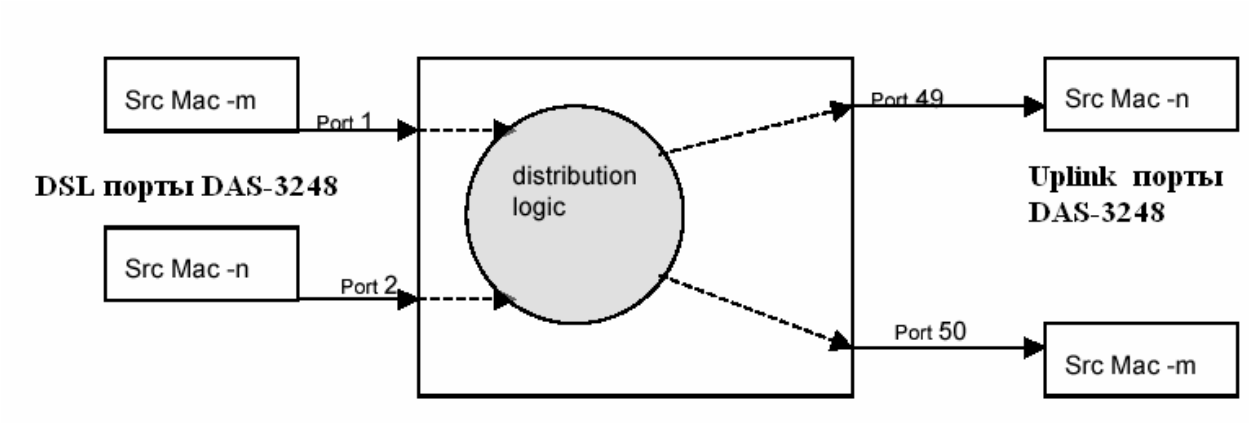


Рисунок 6-13.Логика Source MAC распределения для Upstream потока

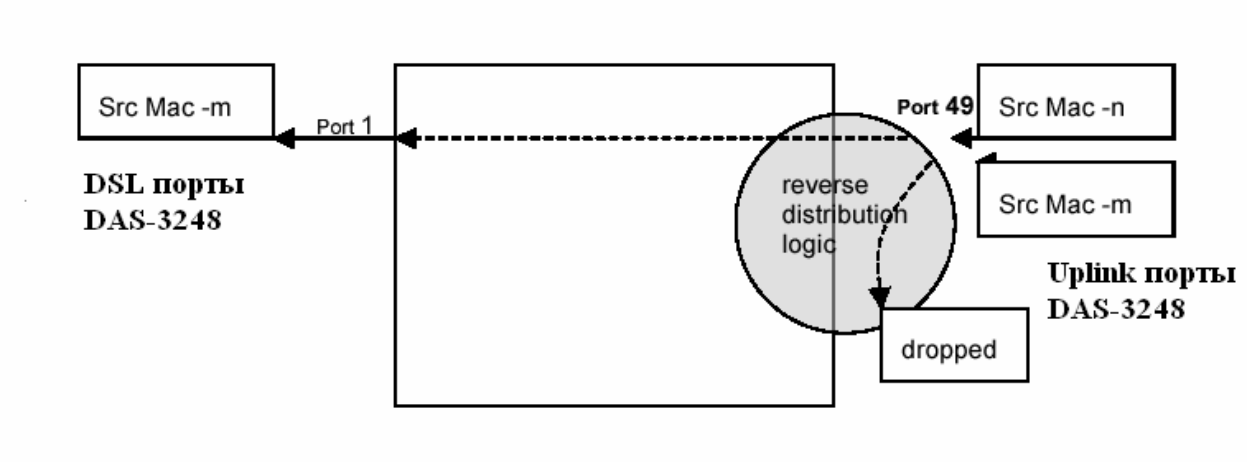


Рисунок 6-14.Логика обратного распределения (Reverse distribution).

Опции Redundancy aggregation
DAS-3248 также поддерживает несколько дополнительных настроек (опций) для функции Redundancy aggregation:

а) **Reverse distribution.**
Дополнительная опция, которая позволяет пользователю определять, должно ли осуществляется (или нет) обратное распределение (reverse distribution) для Dowstream трафика, когда обе связи являются активными. Если такая возможность включена, для Downstream потока, как для юникастового, так и для группового типа трафика используется распределение, базирующееся на MAC адресе назначения (Destination MAC address), использующее такой же алгоритм, который используется для Source MAC распределения Upstream трафика. Когда любая из избыточных (агрегированных) связей отказывает, весь трафик принимается с активной связи. Это позволяет избежать дублирования трафика на клиентском устройстве.

Для групповых протоколов (IGMP/GMRP) трафик, базируется на логике группового распределения посредством группового адреса.

В случае если Uplink устройство является маршрутизатором или коммутатором 3 уровня, эта функция не требуется и может быть отключена. По умолчанию, если параметр опции не указан явно в CLI команде, reverse distribution опция считается включенной.

б) **FallBack.**
Дополнительная опция, которая позволяет включить или выключить триггер отказоустойчивости для функции Redundancy aggregation.
Установка данной опции в disable, приводит к тому, что при отказе одной из Ethernet связей, трафик, передававшийся по ней, не будет автоматически переадресован оставшейся в работе связи, а будет дожидаться восстановления «своей» Ethernet связи. Данная опция может быть полезна при передаче группового трафика (мультикаст трафика), чтобы исключить повторную передачу пакетов.
При использовании распределения отказ одного из Ethernet связей приведет к тому, что мультикаст-маршрутизатор начинает посылать пакеты через оставшуюся в работе связь, используя тот же групповой адрес. При восстановлении связи, трафик начнет дублироваться.

По умолчанию, если параметр Fallback опции не указан явно в CLI команде, опция считается включенной.

в) **FDB overwrite control.**
Дополнительная опция, позволяющая выключить изменение таблицы коммутации для Redundancy агрегированной связи. Это позволяет прекратить затопление сети (flooding) широковещательными пакетами, возвращающими по «петле», образованной двумя Ethernet интерфейсами в случае, если в качестве Uplink устройства используется один коммутатор, на который подключены оба Ethernet интерфейса.
В случае выключения изменения таблицы коммутации, повторные (возвращенные по петле) пакеты будут отброшены (рисунок 6-15).
В случае, когда в качестве Uplink устройства выступают два разных коммутатора или маршрутизатор, опция не является необходимой.

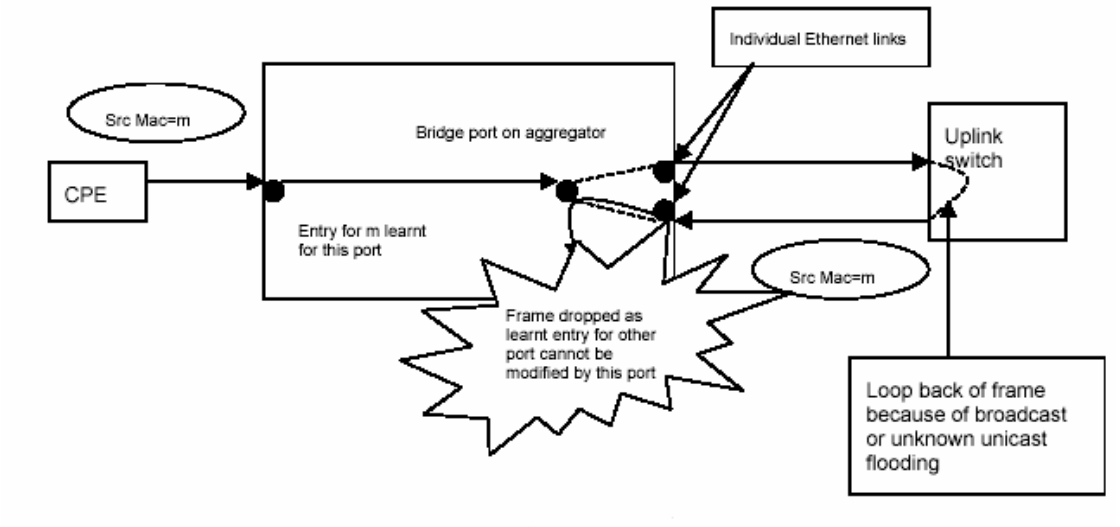


Рисунок 6-15. Принцип предотвращения «петли» (loopback) с использованием опции FDB overwrite control

6.4.3.Пример конфигурирования Redundancy Aggregation

	Команда	**Действие**
Шаг 1	$delete bridge port intf portid 385 $delete filter rule map ifname eth-0 stageid 1 ruleid 1 $delete ethernet intf ifname eth-0	Удалить интерфейс eth-0
Шаг 2		

	$delete bridge port intf portid 386 $delete ethernet intf ifname eth-1	Удалить интерфейс eth-1
Шаг 3	$create ethernet intf ifname eth-0 $create ethernet intf ifname eth-1	Создать Ethernet интерфейсы eth-0 и eth-1 без IP адреса
Шаг 4	$create aggr intf ifname aggr-0 ip 192.168.7.15 mask 255.255.255.0	Создать агрегированный интерфейс aggr-0 с IP адресом
Шаг 5	$create rdncy aggr info ifname aggr-0 [revdistrib Enable|Disable] [fallback Enable|Disable]	Установить тип агрегирования Redundancy. Установить состояние (включено или выключено) дополнительных опций Reverse distribution и Fallback. Если данные опции не указаны в команде явно, считается, что они включены.
Шаг 6	$create bridge port intf portid 385 ifname aggr-0 status enable [fdbmodify disable]	Создать bridge port 385 поверх агрегированного интерфейса В случае использования параметра **fdbmodify disable** включается функция FDB overwrite control.
Шаг 7	$get ethernet intf	Проверить настройки интерфейсов

6.4.4. Standby режим функции Redundancy aggregation.

Особняком при использовании «избыточного» агрегирования стоит режим StandBy, при котором два Ethernet интерфейса **не используются вместе** (в режиме распределенной загрузки), а **только попеременно**.

Один из интерфейсов помечается как активный (основной), второй standby (резервный).

Весь трафик от клиентских портов DSLAMa будет проходить **только** через активный интерфейс (рисунок 6-16).

Активным становится тот интерфейс, который первый устанавливается в рабочее состояние.

При отказе линии связи активного интерфейса, интерфейсы меняются ролями. То есть, активный становится StandBy, а StandBy- активным.

При восстановлении интерфейса, его роль сохраняется неизменной до тех пор, пока не откажет интерфейс, являющийся в данный момент основным.

Процесс ротации ролей интерфейсов при использовании Standby режима функции Redundancy aggregation показан в таблице 6-3.

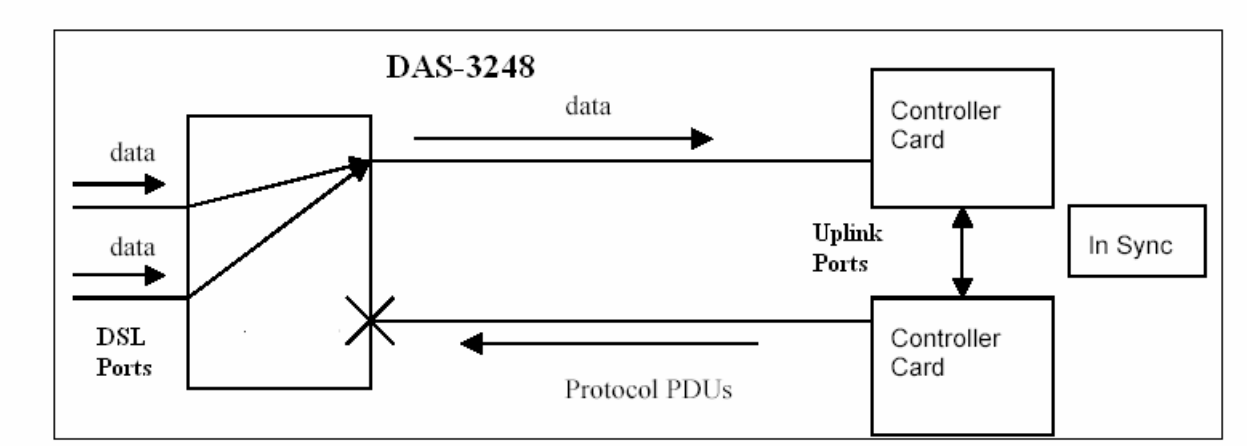


Рисунок 6-16. Standby режим функции Redundancy aggregation.

Интерфейсы	**Комментарий**	**Операционный статус Ethernet интерфейсов: 1- интерфейс в работе (Up) 0-Отказ (Down)**	**Действие функции StandBy**
Eth-0 **Eth-1**	Оба интерфейса в нерабочем состоянии	0 0	Нет действий
Eth-0 **Eth-1**	Eth-0 в рабочем состоянии	1 0	Eth-0 помечается как активный (весь трафик идет через Eth-0)
Eth-0 **Eth-1**	Eth-1 в рабочем состоянии	1 1	Eth-1 помечается как StandBy интерфейс, (весь трафик по-прежнему идет только через Eth-0)
Eth-0 **Eth-1**	Отказ Eth-0 линии связи	0 1	Eth-1 становится активным интерфейсом, (весь трафик идет через Eth-1)
Eth-0 **Eth-1**	Восстановление Eth-0 линии связи	1 1	Eth-0 становится StandBy интерфейсом, (весь трафик идет по-прежнему только через Eth-1)

Таблица 6-3. Принцип работы StandBy режима функции Redundancy aggregation.

Команды управления режимом StandBy.

Перед включением режима StandBy создайте агрегированный интерфейс aggr-0 с типом агрегирования redundancy, как было показано на примере выше (то есть, пройдите шаги 1-7, указанные в примере).

Включение режима StandBy для агрегированного интерфейса

$modify actstdby aggr info ifname aggr-0 status enable

Выключение режима StandBy для агрегированного интерфейса (обратный переход в режим load-sharing).

$modify actstdby aggr info ifname aggr-0 status disable

6.5.Стекирование DAS-3248.

В DAS-3248 используется стекирование методом каскадирования.
Таким способом можно объединить до 8 однотипных устройств.

Каскадирование – последовательное объединение между собой двух или более устройств с помощью однотипных, регулярных интерфейсов, при этом каждое из устройств является независимым с точки зрения управления. Используется обычно при необходимости получить большее количество портов с высокой плотностью. Достоинством такого подхода является простота реализации, а также отсутствие дополнительных расходов.

Согласно правилам каскадирования один из Uplink интерфейсов каждого DAS-3248 (по умолчанию eth-0) используется для присоединения к магистрали (для мастера стека) или к «вышестоящему» устройству стека и имеет типа uplink, а второй - для присоединения к «нижестоящему» устройству и имеет тип downlink (пример такого стекирования приведен на рисунке 6-17).
Кроме того, уникальный IP адрес для устройства указывается только на Uplink интерфейсах устройств. Downlink интерфейсы не имеют IP адреса.

По умолчанию тип eth-0- uplink, eth-1 - downlink. Кроме того, поверх каждого из eth интерфейсов уже создан bridge порт, что позволяет осуществлять L2 Forwarding между устройствами.

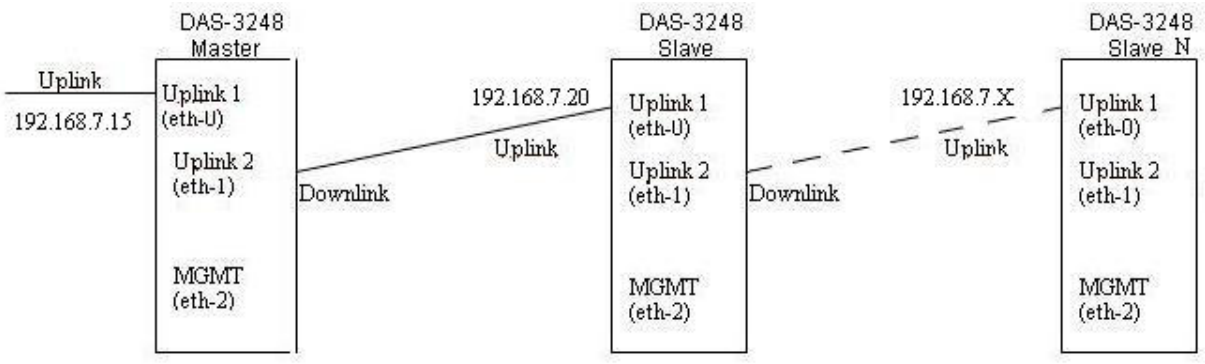


Рисунок 6-17

Таким образом, для выполнения стекирования по схеме, показанной на рисунке 6-17 необходимо:

1) Соединить устройства между собой ethernet кабелем таким образом, чтобы Uplink 2 Интерфейс каждого следующего устройства в стеке присоединялся к eth-1 предыдущего;

2) Присоединить Uplink 1 мастера стека к IP Backbone;

3) Настроить IP адреса, взятые из одной IP подсети, на каждом устройства в стеке командой **modify ethernet intf:**

modify ethernet intf ifname eth-0 192.168.7.15 mask 255.255.255.0
modify ethernet intf ifname eth-0 192.168.7.20 mask 255.255.255.0
……. …….
modify ethernet intf ifname eth-0 192.168.7.X mask 255.255.255.0

7.Способы передачи пакетов

7.1.Понятие передачи пакетов. Типы передачи

Информация в информационных сетях, как правило, передается отдельными порциями, кусками, называемыми пакетами (packets). Предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт).

Каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество служебной информации. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет (как на почтовом конверте – адреса получателя и отправителя).

Таким образом, процесс передачи пакетов представляет собой процесс транспортировки пакетов от адреса-источника к адресу назначения.
В общем случае число адресов назначения может быть больше одного.
Поэтому существует три типа адресов и, соответсвенно, три типа передачи пакетов:

unicast: Одиночная передача. Пакет, посланный по уникастному адресу, доставляется только тому адресу, который указан как адрес назначания в теле пакета. Настройка функций, свзязанных с Unicast передачей данных, описана в разделе 7.2.

broadcast: Широковещательная передача. Пакет, посланный по броадкастному адресу, доставляется всем адресам сегмента локальной сети. Данные рассылки абсолютно необходимы таким протоколам, как DHCP, BootP, но иногда являются помехой, излишне засоряющей каналы связи. Для сегментирования сети применяется технология VLAN, описанная в разделе 7.3.

multicast: Групповая передача. Пакет, посланный по мультикастному адресу, доставляется группе адресов («подписанным» в данную группу). Управление группами осуществляется протолоком IGMP . Более подробно групповые рассылки данных описаны в разделе 7.4.

7.2.Настройка функций, связанных с передачей данных.

7.2.1.Таблица коммутации. Port Security.

Для устройств 2 уровня (коммутаторов, в том числе и коммутаторов ADSL – DSLAM)) характерно наличие в устройствах таблицы коммутации (Forwarding Table), в которой содержатся MAC адреса сетевых устройств, находящихся за соответствующими физическими портами устройства. Поскольку количество и состав MAC адресов изменяться со временем могут на каждом порту, то ручное ведение таблицы было бы не рациональным. Поэтому было введено понятие обучения (Learning) портов.
В режиме обучения порт автоматически наполняет таблицу коммутации MAC адресами содержащимися в поле Source MAC address приходящих Ethernet пакетов и удаляются из нее через определенное время (таймаут) называемый временем жизни MAC адреса.
По умолчанию это значение равно 300с.
Просмотр таблицы коммутации устройства производится командой
$ get bridge forwarding

Изменение времени жизни MAC адресов в таблице коммутатции в DAS-3224/3248 производится командой **modify bridge tbg info aging.**
Пример: $ modify bridge tbg info aging 200

Для запрещения пересылки через таблицу коммутации отдельных типов пакетов используются команды:
$modify bridge tbg info floodsupport disable – запрещение пересылки пакетов Unicast от неизвестных источников
$ **modify bridge tbg info bcastsupport support disable -** запрещение пересылки широковещательных пакетов
$ **modify bridge tbg info mcastsupport support disable-** запрещение пересылки групповых пакетов

Чтобы предотвратить перегрузку DSLAM MAC адресами, а также улучшить безопасность сети, применяется функция Port Security, позволяющая порту обучится только заданному количеству MAC адресов и отвергающая все пакеты со всеми иными MAC.
Ограничение Port Security конфигурируется параметром **maxucast** команды **modify bridge port.** Значение по умолчанию 16.

Примечание: параметр **maxucast** изменяется только при выключенном интерфейсе. Таким образом, для изменения параметра интерфейс надо перевести в состояние disable, а по окончанию обратно в состояние enable.

Пример:
$ modify bridge port intf portid 1 status disable
$ modify bridge port intf portid 1 maxucast 5
$ modify bridge port intf portid 1 status enable

7.2.2.Настройка типа коммутации.

$modify nbsize bridgemode Restricted|Unrestricted|Residential
Определяет режим пересылки пакетов по умолчанию (глобально)

Restricted – определяется пункт назначения пакета, и если им является другой клиентский (ADSL порт) такой пакет отбрасывается. Таким образом, в этом режиме **запрещена** передача данных между клиентскими портами (только от клиентских портов на Uplink порты).

Unrestricted – Пакеты анализируется в любом случае.
Таким образом, в этом режиме **возможна** передача данных, как напрямую между клиентскими портами, так и на аплинк порт (решение принимается в зависимости от адреса назначения в соответствии с таблицей коммутации DSLAM). Другое название этого режима Full bridging.

Residential – пакеты данных от клиентских (ADSL портов) передаются на Uplink порты DSLAM сразу без анализа адреса назначения. Другое название этого режима Half bridging.

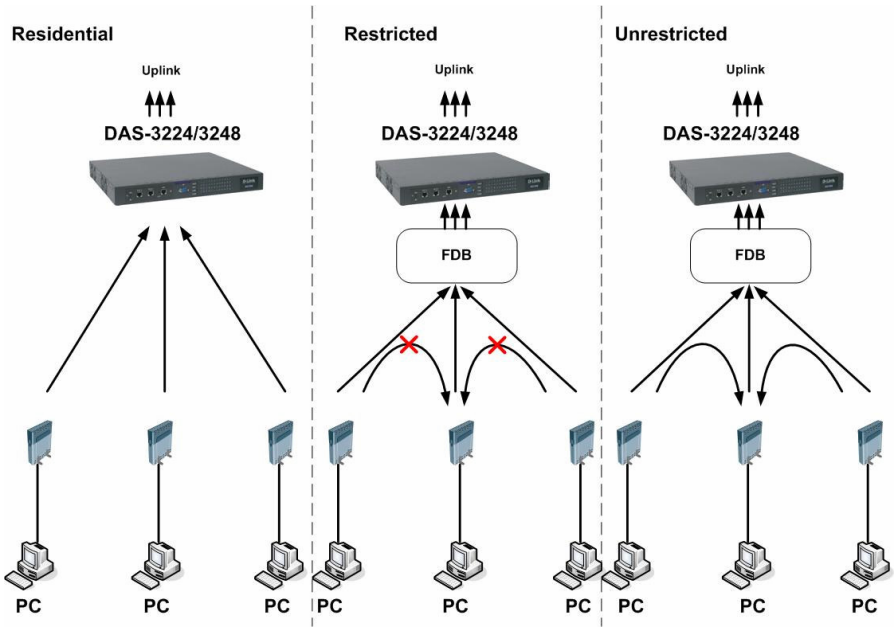


Рисунок 7-1

Также режим коммутации может определяться для каждого созданного в системе VLAN (т.е локально) через команду :
modify vlan static vlanname bridgingmode Restricted| Unrestricted| Residential

7.2.3.Функция Virtual MAC

Virtual MAC - функция ADSL коммутатора (DSLAM), которая позволяет подменять MAC адрес источника (Hardware MAC CPE адрес) в пакетах 2 уровня, на заранее заданные Virtual MAC.
Применяется на EoA интерфейсах устройства.

Причины применения Virtual MAC

1.Ограничение масштабируемости сети на устройствах 2 уровня.
Сети на устройствах 2 уровня используют таблицы адресов MAC (Forwarding таблицы, таблицы коммутации), адресное пространство которых является плоским и не обладает иерархией. Эти таблицы могут переполняться, когда несанкционированные пользователи входят в сеть и затопляют сеть (флудинг) большим количеством пакетов с различными MAC адресами и VLAN Id.

2.Проблемы идентификации порта.
В Ethernet DSLAM нет механизма, который позволяет однозначно сопоставить Ethernet пакеты с портом DSL, от которого эти пакеты были получены. Адрес MAC не может использоваться для идентификации, поскольку конечные пользователи могут легко изменить адреса MAC. Кроме того, в сети доступа могут появиться многочисленные устройства с идентичными адресами MAC или случайно (преднамеренно) измененными MAC адресами.

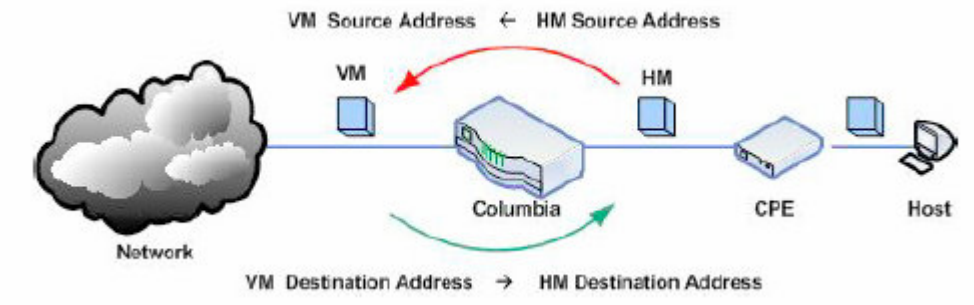


Рисунок 7-2.Сущность функции Virtual MAC.

Virtual MAC адреса чаще всего используются, чтобы однозначно идентифицировать DSLAM_ID + DSL_PortID + UserID в сети доступа и выбирается соответствующим образом, однако ничего не мешает выбирать произвольный адрес для Virtual MAC.

Структура модуля обработки Virtual MAC.

Модуль обработки функции Virtual MAC состоит из трех частей:

1.Базы Virtual MAC (Virtual MAC Database)
База данных содержит список записей сопоставления Virtual MAC– Hardware MAC .

2. Записей Virtual MAC Database статического типа.

В этом типе случае, записи таблицы трансляции VirtualMac в Hardware MAC создается и изменяется только вручную.

3. Записей Virtual MAC Database динамического типа.
В этом случае создается профиль, содержащий пул пустых VirtualMac адресов.
Virtual MAC динамически сопоставляются с Hardware Mac адресами из этого пула. Кроме того, динамические записи имеют преимущество, поскольку позволяет системе автоматически изменять сопоставление Virtual MAC- Hardware MAC.

Ограничения применения функции Virtual MAC:
1. Функция Virtual MAC не будет работать для тех адресов MAC, которых нет в таблице коммутации и изучение которых (Learning) выключено на соответствующем порту.
2. Невозможно ассоциировать два различных виртуальных MAC адреса с одним MAC адресом, источником которого являются два различных порта с различными VLAN.
3. С каждым Hardware MAC может быть сопоставлен только один Virtual MAC.

Конфигурирование функции Virtual MAC:
Примечание: Функция Virtual MAC конфигурируется только при выключенном eoa интерфейсе. Таким образом, для изменения параметра интерфейс надо перевести в состояние disable, а по окончанию обратно состояние enable.

1. Создать новую запись в базе данных функции VirtualMAC:
$ create vmac database m2vmacdbid 1

2. Создать статическую запись в базе Virtual MAC Database:
$ create vmac map static m2vmacdbid 1 hostmacaddr 0:6:6:6:6:6 vmacaddr 0:7:7:7:7:7

3. Создать динамическую запись в базе Virtual MAC Database
$ create vmac map static hostmacaddr dynamic vmacaddr 0:1:1:1:ff:ff m2vmacdbid 1 count 2

4. Приложить запись Virtual MAC к интерфейсу
$ modify eoa intf ifname eoa-0 disable
$ modify eoa intf ifname eoa-0 m2vmacdbid 1
$ modify eoa intf ifname eoa-0 enable

5. Включить Virtual MAC Traps (позволяет отслеживать статус Virtual MAC через SNMP)
$ modify bridge tbg traps vmactrapstatus enable

6. Проверить Virtual MAC Database
$ get vmac map curr

7.3. Виртуальные локальные сети в DAS-3248

В данном разделе рассказано о технологии сегментации трафика на физическом уровне, применяемой в устройствах DAS-3248.

7.3.1. Понятие VLAN

VLAN (Virtual Local-Area Network, IEEE 802.1q) - группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети.

Передача кадров между разными виртуальными сегментами на основании адреса канального уровня невозможна, независимо от типа адреса - уникального, группового или широковещательного. Внутри виртуальной сети (VLAN) кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра.

Используются три типа VLAN и широковещательных доменов:

- IEEE 802.1Q VLAN
- VLAN на базе портов
- VLAN на базе MAC-адресов

Все типы VLAN позволяют сегментировать сеть с целью уменьшения размеров широковещательных доменов. VLAN по стандарту IEEE 802.1Q поддерживают метки пакетов, которые позволяют распределять VLAN по всей локальной сети (при условии, что все устройства сети поддерживают стандарт IEEE 802.1Q).

Основные понятия стандарта IEEE 802.1q:

Egress - порты, которые передают информацию о маркере (VID).

Untagged - нетегированные порты. Порты, к которым подключено сетевое оборудование не поддерживающее VLAN и не распознающее маркеров 802.1q.
Для того чтобы оборудорвание не распознающее маркеров могло участвовать в обмене данными с применением VLAN на **Untagged** портах введено понятие PortVLAN ID (PVID), обозначающее каким маркером надо тегировать входящие на данный порт пакеты.

Кроме этого, в параметрах каждого VLAN можно дополнительно указать возможность запрещать юникаст пакеты от неизвестных источников **floodsupport** (флуд-контроль) и/или широковещательные пакеты **bcastsupport** (броадкаст-контроль).

7.3.2.Создание, настройка и удаление Static VLAN

Команды системы:

create vlan static

Описание: Создает vlan с заданными параметрами.

Синтаксис команды: create vlan static vlanname vlanname vlanid vlanid [egressports egressports|none][forbidegressports forbidegressports|none] [untaggedports untaggedports|none][bridgingmode bridgingmode] [floodsupport enable|disable][bcastsupport enable|disable]

modify vlan static

Описание: Изменяет параметры заданного vlan

Синтаксис команды**:** modify vlan static (vlanname vlanname | vlanid vlanid)[egressports egressports|none] [forbidegressportsforbidegressports|none] [untaggedports untaggedports|none][bridgingmode bridgingmode] [floodsupport enable|disable][bcastsupport enable|disable]

delete vlan static

Описание: Удаляет заданный vlan.

Синтаксис команды: delete vlan static (vlanname vlanname | vlanid vlanid)

get vlan static

Описание: Получает информацию по vlan.

Синтаксис команды: get vlan static [vlanname vlanname | vlanid vlanid]

Таблица параметров:

Параметр	Описание
vlanname vlanname	Административно определяемая строка, которая может быть использована для идентификации VLAN. Это обязательный параметр для команды «create». С командами get/modify/delete - допустимо идентифицировать vlan по имени и по vlan id . **Использование:** Create – Обязательно Delete – Опционально Get – Опционально Modify – Опционально **Принимает значения:** любая строка размером до 64 символов .
vlanid vlanid	VLAN идентификатор. **Использование:** Create – Обязательно Delete – Опционально Get – Опционально Modify – Опционально Для **delete**, **get**, **modify** – может использоваться **vlanname** или **vlanid.** **Принимает значения:** *1 – 4095*
egressports egressports | none	Устанавливает порты, каждый из которых ассоциирован с типом “egress” (список egress портов) для данного управляющего VLAN. При задании более одного значения, они разделяются пробелами. **Использование:** Опционально **Принимает значения:** *1 – 386* **Значение по умолчанию:** none
forbidegressports forbidegressports | none	Устанавливает порты, которые запрещенные к управлению, будучи включенными, в список “egress” типа портов для данного VLAN. Они могут быть включены в “untagged” тип. **Использование:** Optional **Принимает значения:** *1 – 386* **По умолчанию:** none
untaggedports untaggedports | none	Устанавливает порты, которые могут передавать “egress” пакеты данного VLAN, как, “untagged” . При задании более одного значения, они разделяются пробелами. **Использование:** Optional **Принимает значения:** *1 – 386* **По умолчанию:** none
bridgingmode bridgingmode	Параметр полностью определяет режимы «моста» для данного VLAN. Данное значение может быть ассоциировано с тремя типами, базирующиеся на

	глобальном значении “fullBridgingStatus”. Данные значения могут быть “restricted bridging” (ограниченный), “unrestricted full bridging” (не ограниченный) и “residential bridging”. Если пользователь не выбрал специально режим “bridging mode” в момент создания VLAN, режим принимает глобально установленное значение “bridging mode”. Пользователь может изменить режим “bridging mode” для уже созданного VLAN. Если динамически полученное значение для VLAN было создано и установлено, пользователь может установить только глобальное значение “bridging mode” для данного VLAN. По умолчанию “residential VLAN”, может включать другой “residential VLAN”, разрешая только один сетевой “bridge port “, принадлежащий ему. Данный порт может быть автоматически добавлен в “VLAN по умолчанию”, если только это сетевой “bridge port” будучи добавленный в VLAN. Впоследствии, пользователь может добавить любой другой сетевой порт в “egressportlist” и “untaggedportslist” только после удаления ранее добавленных сетевых портов “bridge port”. Режим “Unrestricted bridging ” не может применяться для “bridge ports” созданных поверх PPPoE интерфейса, тем не менее,VLAN может быть “unrestricted”. **Использование:** Create -- Optional Modify -- Optional **Принимает значения:** Restricted, Unrestricted, Residential **По умолчанию:** residential
floodsupport enable|disable	Используется если необходимо запретить или разрешить unicast пакеты от неизвестных источников для данного VLAN По умолчанию значение параметра enable. Неизвестные unicast пакеты могут распространяться на все порты VLAN, если глобальное значение (представлено в Dot1dTpInfo) установлено в “enable” или “throtte” и значение на VLAN так же “enable” или “drop’. **Использование:** Create -- Optional Modify -- Optional **Принимает значения:** GS_STATE_ENABLE, GS_STATE_DISABLE
bcastsupport enable|disable	Параметр определяет распространение broadcast пакетов для данного VLAN. По умолчанию система получает значение enable, когда VLAN создан. Broadcast пакеты могут распространяться через все

	порты VLAN, если глобальное значение (представлено в Dot1dTpInfo) и значение первичного vlan установлены в “enable”. **Использование:** Create -- Optional Modify -- Optional **Принимает значения:** GS_STATE_ENABLE, GS_STATE_DISABLE **По умолчанию:** GS_CFG_DEF_VLAN_BCAST

Создать VLAN с заданными параметрами:

	Команда	**Действие**
Шаг 1	$create vlan static vlanname Dlink vlanid 100	Создать vlan с именем Dlink, с номером vlanid 100
Шаг 2	$modify vlan static vlanid 1 untaggedports none egressports none	Исключить все порты из дефолтового VLAN (VID 1)
Шаг 3	$modify vlan static vlanname Dlink egressports 1 2 23 385 untaggedports 1 2 23 floodSupport disable bcastsupport disable	Изменение параметров VLAN По этой команде порты 1 2 23 становятся нетегированными членами Vlan Dlink, порт 385 (Uplink1) тегированным членом VLAN (транком). Внимание: Тегированными являются только те порты порты, которые присутствует в списке egressports, но которых нет в списке untaggedports.
Шаг 4	$modify gvrp port info portid 1 portvlanid 100 acceptframetypes all ingressfiltering true $modify gvrp port info portid 2 portvlanid 100 acceptframetypes all ingressfiltering true $modify gvrp port info portid 23 portvlanid 100 acceptframetypes all ingressfiltering true	Команды, производящие присваиваивание PVID Bridge портам,(то есть ассоциирующие входящие в определенный порт кадры с определенным тегом VLAN). Данная команда будет описана подробно в разделе посвященному настройке протокола GVRP настоящего руководства.
Шаг 5	$get vlan static	Проверить настройки VLAN

Примечание: В случае операции с группой портов, порты перечисляются через пробел.

7.3.3.Протоколы GVRP, GARP.Настройка GVRP

Протокол GARP

Протокол GARP (Generic Attribute Registration Protocol – базовый протокол регистрации атрибутов) обеспечивает возможность рассылки атрибутов, служащую подписчикам в приложениях GARP для регистрации и исключения (de-register) значений атрибутов у других участников GARP в ЛВС на базе мостов (Bridged LAN). Участник (подписчик) GARP на базе моста или пользовательской станции содержит прикладную компоненту (application component) GARP и информационную декларацию GARP (GARP Information Declaration или GID), связанные с каждым портом моста. Распространение информации между участниками GARP для одного приложения на базе моста осуществляется за счет компоненты распространения информации GARP (GARP Information Propagation или GIP). Обмен протокольными данными между участниками GARP осуществляется на базе сервиса LLC типа 1, с использованием групповых адресов MAC и формата PDU, определенного для приложений GARP.

Протокол GVRP

Протокол GVRP (GARP VLAN Registration Protocol – протокол регистрации GARP VLAN) определяет приложения GARP, обеспечивающие сервис динамической регистрации VLAN. Этот протокол использует значения GID и GIP, обеспечивающие общее описание состояния машины и общие сведения о механизмах распространения, определенных для использования в приложениях на базе GARP.

Формат пакетов GVRP совпадает с форматом GARP, отличаясь лишь назначением поля типа атрибута. Это поле принимает значение 1 для группового атрибута VID (VID Group Attribute Type).

Протокола GVRP позволяется делать прозрачный перенос через промежуточные сетевые устройства информации определенных VLAN, не регистрируя порт статически на них, что избавляет администатора от необходимости прописывать статические VLAN на все устройствах, входящих в цепь передачи данных.

Команды DAS-3248 для настройки GVRP

modify gvrp info
Описание**:** Глобальное включение/выключение протокола GVRP.
Синтаксис команды:
modify gvrp info gvrpstatus enable/disable

modify gvrp port info

Описание**:** изменить параметры GVRP для определенного порта.

Синтаксис команды:
modify gvrp port info portid portid [**portvlanid** portvlanid] [**acceptframetypes** all | tagged] [**ingressfiltering** False | True] [**gvrpstatus** enable | disable] [**restrictedvlanreg** False | True] [**pktpriority** pktpriority] [**psvlanid** psvlanid] [**ppstatus** enable|disable] [**ctosprofileid** ctosprofileid | None]

Параметры команды:

portid *portid*	Имя Bridge интерфейса, на котором производится настройка парметров. **Обязательный параметр.**
portvlanid portvlanid	PortVlanID (PVID), ассоцированный с данным Bridge интерефейсом. Данный параметр обязательно необходим для настройки Static VLAN. **Необязательный параметр**
acceptframetypes all | tagged	Разрешить пропускать все входящие кадры (помечая их portvlanid) ,либо только тегированные, отбрасывая нетегированные. **Необязательный параметр** **Допустимые значения:** 0 - 310
ingressfiltering False | True	Фильтрация входящих пакетов. Если **ingressfiltering** True,то пакеты, принадлежащие к VLANам, не зарегистрированным на этом порту будут отброшены. **Необязательный параметр**
gvrpstatus enable | disable	Локальное включение протокола GVRP на отдельном порту **Необязательный параметр**
restrictedvlanreg False | True	Запрет регистации новых динамических VLAN GVRP **Необязательный параметр**
pktpriority pktpriority	Приоритет, используемый для постановки пакетов в определенную очередь пакетов
psvlanid psvlanid	Определяет PSVID, приявязанный к порту DSLAM (для функии Q-in-Q) **Необязательный параметр** **По умолчанию :None**
ppstatus enable|disable	Используется совместно с функцией Q-in-Q. Определяет, является ли данный порт портом поставщика услуг (enable) или оконечным портом (disable).

	Данный параметр изменятся **только** привыключенном bridge интерфейсе. **Необязательный параметр** **По умолчанию :None.**
ctosprofileid ctosprofileid | None	Содержит привязку CtoS профиля к порту (для функии Q-in-Q)

Пример:
$modify gvrp port info portid 1 portvlanid 100 acceptframetypes all ingressfiltering true

get gvrp port stats
Описание**:** Просмотр статистики протокла GVRP
Синтаксис команды:

get gvrp port stats [portid portid]

Данная команда служит для просмотра информации о количестве сообщений GVRP

Пример:
$get gvrp port stats portid 1

7.4.Стекирование VLAN. Технология Q-in-Q.

Что такое Q-in-Q?
Существующая технология Ethernet становится все более дешевым и более популярным решением для строительства сети с каждым годом. Сети Ethernet расширяются и растут в объемах. Это ведет к развертыванию на основе Ethernet сетей уже не локальных сетей (LAN), а сетей городского и более крупного масштаба – сетей MAN (Metro Area Network).

Существующая поддержка VLAN, основанная на IEEE 802.1Q, уже не способна масштабироваться в таких сетях из-за ограниченных возможностей 802.1q (стандарт поддерживает только 4094 VLAN) и, следовательно, требуется стекирование VLAN для работы в сетях MAN.

Метод стекирования VLAN, также известный как Q-in-Q , является механизмом, в котором один VLAN (Виртуальная Локальная Сеть) может инкапсулироваться внутри другого VLAN (рисунок 7-3). Это позволяет разделить сеть среди нескольких сервис-провайдеров или крупных клиентов одного провайдера, допуская, чтобы каждый из них мог использовать все адресное пространство VLAN, регламентированное 802.1q.
То есть, например, два провайдера, использующих сеть MAN, могут подключать клиента к одной и той же VLAN с VLANID 1 и клиенты не будут видеть трафик друг друга.

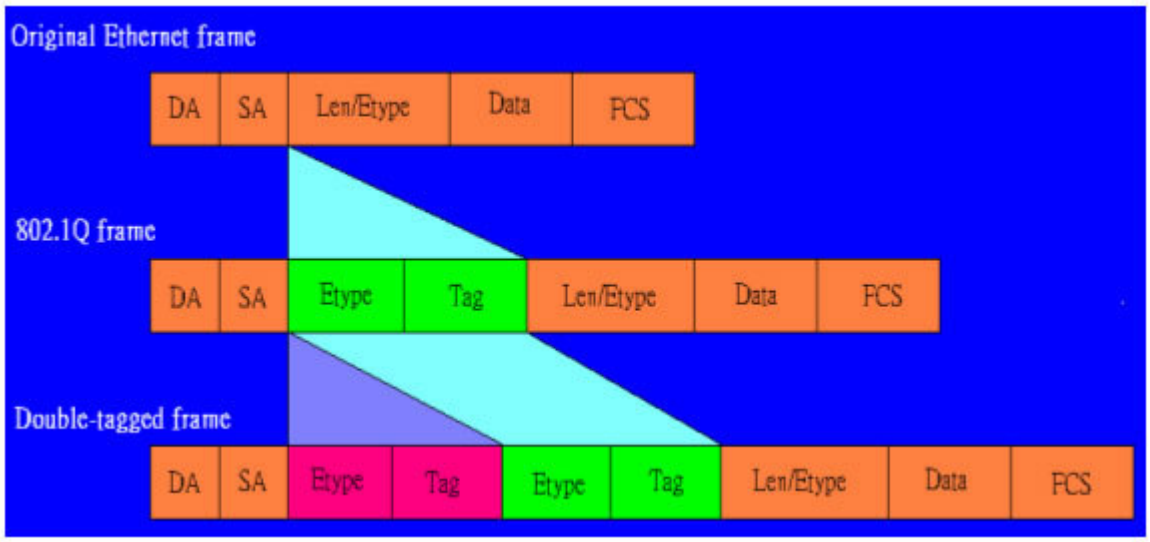


Рисунок 7-3.Структура Ethernet фрейма при использовании Q-in-Q.

Также сети MAN могут разделять трафик между клиентами в целях безопасности или дифференциации уровней услуг.
В типовом сетевом сценарии развертывания сети MAN DAS-3248 находится на краю сети поставщика (Ethernet Aggregation Network).Позиция DSLAM показана на Рисунке 7-4.

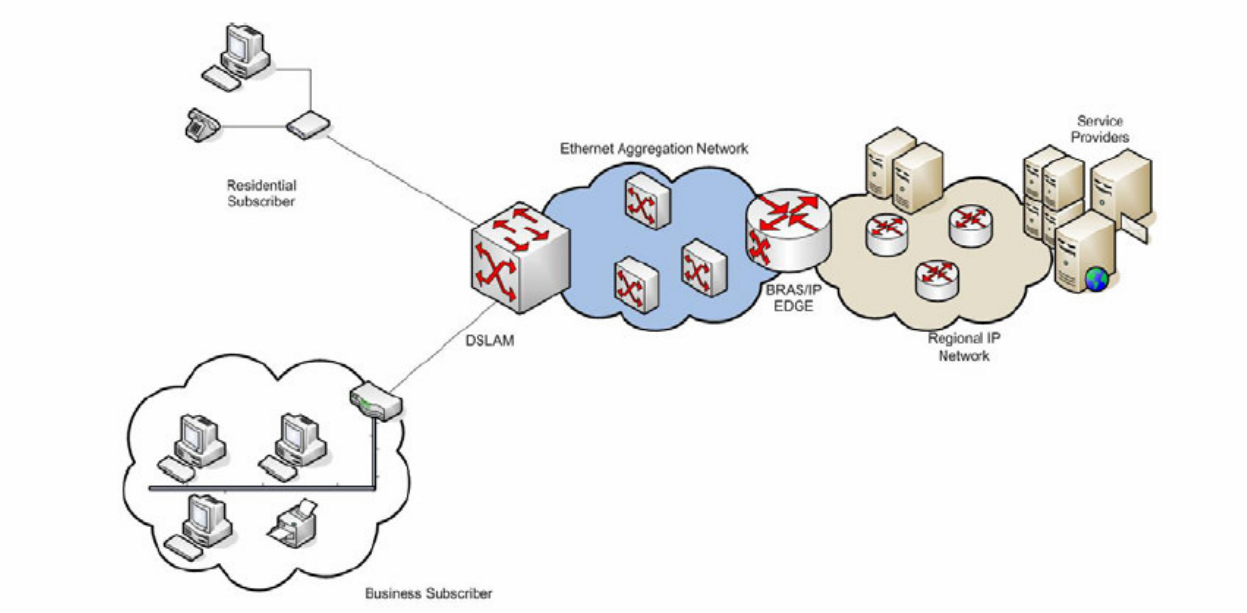


Рисунок 7-4.Схема сети MAN

7.4.1.Использование Q-in-Q. Типовые сценарии.

7.4.1.1. Резидентные клиенты или клиенты малого бизнеса
Для типичного резидентного клиента или SOHO клиента, первичный мотив установления соединения с провайдером - услуга доступа.
Для этого типа сети характерны следующие требования к провайдеру услуг:

1. Трафик между отдельными CPE (клиентскими устройствами) будет следовать модели клиент-сервер.
2. В зависимости от типа подписки, может быть необходимость предоставлять различные услуги различным абонентам. Абоненты могут делиться на группы в зависимости от типа предоставляемых услуг.
3. Кроме того, к самой сети доступа предъявляются следующие требования:
a) Сеть доступа должна обслуживать многочисленных поставщиков услуг (провайдеров).
b) Идентификация порта. Может достигаться использованием VLAN для идентификации порта.
в) Масштабирование. Адресация большого количества портов приводит к потребности в иерархической адресации. Эта схема может быть подобной использованию VPI и VCI в сетях ATM.

7.4.1.2. Клиенты среднего и крупного бизнеса.
В добавлении к требованиям резидентных клиентов клиенты среднего и крупного бизнеса имеют дополнительные требования к провайдерам услуг. Они могут быть следующие:

1. Услуга арендованного канала. Эта услуга должна в общем случае обеспечивать прозрачную связь между двумя (и более) корпоративными сетями со своей устоявшейся сетевой архитектурой (в том числе и VLAN).

Различается два вида услуги арендованного канала:

а) Услуга эмуляции выделенной линии (E-Line).
E-Line услуга - услуга арендованного канала или выделенный канал между двумя портами DSLAM на одном VLAN (VLAN Trunk). Задача услуги - получить тегированные или нетегированные фреймы Ethernet от клиента и пережать данные во второй порт, участвующий в услуге E-line. В этом случае данные должны направляться между только двумя участвующими в обмене портами. Данные просто перенаправляется между двумя портами, никакой дополнительной обработки их не проводится. Это оптимизирует время пересылки пакетов.

б) Услуга эмуляции локальной сети (E-LAN сервис).
E-LAN услуга имеет два или больше портов-участников и, следовательно, на DSLAM проводится обработка пакетов (поиск порта назначения по таблице коммутации). Для этой услуги характерно выделение специфического VLAN пространства, а сеть поставщика услуг просто пересылает трафик клиента от одного участника услуги E-LAN к другому.

2. Виртуальная частная сеть (VPN).VPN должна обеспечивать услугу прозрачной LAN сети между двумя точками присутствия провайдера через публичную сеть

3. QoS. Необходимо обеспечивать требования качества сервиса (QoS) согласно договору SLA (Service Licence Aggrement - договора о предоставлении услуг клиенту сервис-провайдером).

4. Развертывание вышеперечисленных бизнес услуг провайдером имеет следующие требования к сети доступа:
а) Изоляция трафика. Деловой трафик клиента должна быть выделятся из всего остального трафика в сети. Это требование может быть удовлетворено использованием выделенных VLAN для каждого бизнес-клиента.
б) Прозрачность трафика для VLAN сетей. Требуется, чтобы поступающие фреймы сами могли бы быть тегированными VLAN, и тег сохранялся без изменений при передаче трафика клиента через сеть провайдера.

7.4.2. Реализация Q-in-Q на DAS-3248.

7.4.2.1.Общая концепция.

DAS-3248 поддерживает технологию Q-in-Q, начиная с программной версии 2.10.
Существуют следующие режимы управления VLAN в DAS-3248:

1. Native VLAN (802.1q). Native VLAN – нормальная поддержка 802.1Q VLAN.
2. Q-in-Q. Режим поддержки стекирования VLAN.

Переключение режимов работы с VLAN производится командой:
nbsize vlanmode stackedmode|nativemode ,где:
nativemode- 802.1q VLAN режим.

stackedmode- Q-in-Q режим.

Внимание: после применения команды необходимо сохранить настройки командой $commit и перезагрузить устройство.

В Q-in-Q режиме вводятся следующие понятия:

а) C-VLAN (Customer VLAN)
C-VLAN – V-LAN , использующийся клиентом («внутренний» VLAN)
C-VLAN однозначно идентифицируется параметром C-VLANID.
C-VLAN создается командой:
create vlan static vlanname name **vlanid** vlanid

б) S-VLAN (Service VLAN)
VLAN пространство, использующееся сетью провайдера («внешний» VLAN)
S-VLAN однозначно идентифицируется параметром S-VLAN ID.
S-VLAN создается командой:
create vlan svlanid svlanid svlanid

в) Виртуальный VLAN (Virtual VLAN)
Если многочисленным поставщикам услуг необходимо использовать для различных целей один и тот же C-VLAN, адресное пространство VLAN будет определяться комбинацией S-VLAN и C-VLAN. С другой стороны, провайдеру может потребоваться одновременное использование в дополнении к этому еще и E-Line или E-LAN услуги, для чего будет необходима прозрачная пересылка C-VLAN через операторские сети, в которых направление пересылки определяться благодаря S-VLAN .
Виртуальный VLAN - абстракция, которая прячет привязку C-VLAN ID –S-VLAN ID за Virtual VLAN ID. Преимущество этой абстракции - то, что все типы клиентов могут поддерживаться одновременно и число Virtual VLAN в системе может быть ограничено только доступной памятью устройства.
В Q-in-Q режиме DAS-3248 выполняет операции входящей и исходящей VLAN фильтрации, обучения таблицы коммутации и поиск в таблице коммутации выполняются, опираясь на Virtual VLAN ID.
Virtual VLAN может быть создана (при существующих C-VLAN и S-VLAN) командой:
create vlan virmap svlanid svlanid **cvlanid** cvlanid **vvlanid** vvlanid

г) Global VLAN ID (Third VLANID)
Технология Q-in-Q иерархическая по своей сути, поэтому кратность вложенности VLAN может быть увеличена. Возможен сетевой сценарий, в котором необходимо будет подключать третий уровень вложенности VLAN (назовем его Q-in-Q-in-Q), чтобы однозначно идентифицировать абонента в пределах VLAN пространства. Это требование удовлетворяется использованием Global VLAN ID, который может включаться в пакет прежде, чем послать пакет и, который может быть удален только после получения пакета в порт поставщика услуги.

Global VLAN ID не интерпретируется DAS-3248, однако может прозрачно пропускаться через DAS-3248. Приоритет, использованный для Global VLAN ID должен быть таким же, как для S-VLAN.
Third VLAN ID задается командой CLI:
modify nbsize tvlanid tvlanid
Примечание: после применения команды необходимо сохранить настройки перезагрузить устройство.

7.4.2.2. Дифференциация портов по назначению

Каждый порт может быть классифицирован или как порт поставщика услуг (порт, подключенный к сети сервис-провайдера) или как оконечный порт (порт, подключенный к сети клиента). За портом поставщика фреймы данных должны передаваться и приниматься с использованием тега S-VLAN ID, за конечным портом фреймы данных должны передаваться и приниматься или как нетегированные фреймы или иметь тег C-VLAN ID. Global VLAN на порту поставщика услуг будет поддерживаться, только если он сконфигурировано глобально.
Режим использования порта DSLAM выбирает командой **modify gvrp port info portid** portid **ppstatus** enable|disable , при выключенном Bridge интерфейсе.
Параметр ppstatus это команды соответствует:
Enable –порту поставщика услуг
Disable- оконечному порту.

7.4.2.3. Типы Service VLAN (S-VLAN).

S-VLAN могут разделяться в сети поставщика по типам услуг, то есть одни S-VLAN переносят резидентный трафик, другие - деловой трафик. Следовательно, S-VLAN должны конфигурироваться так, чтобы однозначно идентифицировать тип трафика переносимого каждым S-VLAN. Таким образом, имеется два типа S-VLAN, базирующихся на природе их использования (Residential и Business).

7.4.2.4. Идентификация S-VLAN.

S-VLAN определяется в поступившем фрейме Ethernet одним из следующих способов:

- Из анализа S-VLAN тега в поступившем фрейме.
- Базируясь на привязке порта DSLAM к S-VLAN (PSVID).
  При подключении бизнес-клиента на порт DSLAM ему присваивается уникальный S-VLAN ID. В этом случае, сеть поставщика услуг получает тегированные фреймы бизнес клиента для прозрачной пересылки данных через «выделенную» бизнес-сеть. Следовательно, C-VLAN ID используется самим клиентом по его усмотрению, а S-VLAN ID идентифицирует бизнес-клиента. Вплоть до 4094 бизнес клиентов может быть подключено по такой схеме в одной сети агрегации Ethernet.
  PSVID может быть прикреплен к порту DSLAM командой CLI:
  $modify gvrp port info portid portid **psvlanid** psvid
- Базируясь на C-VLAN ID. Данный способ используется для резидентных клиентов, когда они посылают в сеть сервис-провайдера теговые фреймы. В этом случае, клиент посылает C-VLAN ID в своем пакете данных, и этот тег может быть заменен (или не заменен) PVID тегом (клиентским тегом, привязанным к порту DSLAM). Поскольку S-VLAN тег для поставщика услуги привязан к C-VLAN тегу, который добавляется к

принятому пакету прежде, чем послать его в сеть поставщика услуг, следовательно, в сети поставщика C-VLAN ID используется, чтобы идентифицировать клиента, и S-VLAN ID используется, чтобы идентифицировать поставщика услуги. После определения S-VLAN определения, C-VLAN уже не требуется.

- Базируясь на классификации потока. В этом случае S-VLAN тег определяется исходя из идентификации потока данных на клиентском порту и S-VLAN тег, который должен использоваться в сети поставщика однозначно идентифицирует определенный поток данных клиента. Различие с предыдущим случаем заключается в том, что S-VLAN тег определяется, исходя из типа потока или типа трафика.
- Базируясь на CtoS Profile .
  Основной составляющей CtoS профиля является таблица, которая содержит C-VLAN ID и S-VLAN ID пары (C, S). Когда на входной порт приходит фрейм с C-VLAN ID равным C', в этой таблице ищется и определяется пара (C', S'), S' определяет S-VLAN ID для этого фрейма. Кроме привязки C-VLAN тега к S-VLAN тегу, вы можете также создать в таблице пару для связывания нетегированных фреймов с определенным S-VLAN ID (Untagged, S''). В этом случае, нетегированные пакеты будут становиться тегированными S-VLAN ID тегом, равным S''.Если для C' не находится соответствия в таблице CtoS, то все фреймы, приходящие с C-VLAN ID равным C', будут отброшены.

  CtoS Profile является интерфейсом пользователя, который увязывает CtoS таблицу с определенными портами DSLAM. Вы можете создать профиль с любым количеством портов.
  На порту DSLAM может быть одновременно сконфигурирован как PSVID, так и CtoSProfile. В этом случае S-VLAN ID определяется на основании CtosProfile, а не PSVID.

  CtoS профиль создается следующими командами CLI:
  1.Создать профиль:
  create vlan mapprofile info profileid ctosprofileid **profiletype CtoS**
  2.Определение C-VLANID и S-VLAN ID:
  create vlan mapprofile param profileid ctosprofileid **vlan1** vlan1 **vlan2** vlan2,
  где vlan 1- C-VLAN ID, vlan2- S-VLAN ID.
  3.Привязка CtoS профиля к порту осуществляется командой:
  modify gvrp port info portid portid **ctosprofileid** ctosprofileid

7.4.2.5.Определение приоритета S-VLAN.

S-VLAN приоритет может определяться для входящего фрейма на основании одного из следующих путей:

- Базируясь на приоритете S-VLAN тега во входящем фрейме. Если фрейм тегирован SVLAN, то S-VLAN приоритет определяется применением этого приоритета в качестве входного аргумента для регенерации приоритета (изменения приоритета) S-VLAN, связанного с входным портом DSLAM.
- Базируясь на приоритете C-VLAN тега: Если фрейм тегирован только C-VLAN, то C-VLAN приоритет может быть использован для регенерации приоритета S-VLAN.
- Базируясь на потоке. То же что и для определения S-VLAN ID, базирующегося на потоке данных.
- Базируясь на приоритете по умолчанию для S-VLAN .

Если на DSLAM принят нетегированный входящий фрейм, то приоритет defSVprio входного порта может использоваться как S-VLAN приоритет (устанавливается CLI командой **modify bridge port prioinfo** portid **portid defsvprio** defsvprio).

7.4.2.6. Идентификация S-VLAN tag protocol ID

По умолчанию в качестве идентификатора Q-in-Q протокола в Ethernet фреймах используется значение 0x9100. В качестве идентификатора использования Third VLAN используется 0x9200 в Ethernet фреймах.

Если пользователь хочет изменить эти величины, он может это сделать посредством CLI команд:

modify nbsize svlanprotocolid 0xXXXX
modify nbsize tvlanprotocolid 0xXXXX

Примечание: После изменений в nbsize необходимо сохранить настройки и перезагрузить устройство.

7.4.2.7.Управление S-VLAN в DAS-3248. Параметры управления Q-in-Q.

Для управления S-VLAN в DAS-3248 (команда CLI **create vlan svlan** svlanid) существуют следующие параметры:

- **Тип S-VLAN (параметр svlantype).**
  Параметр принимает два значения. Business и Residental.
  В случае резидентных клиентов для фильтрации и пересылки пакетов используется стандартное Virtual VLAN распределение, то есть взаимооднозначная связь между C-VLAN и S-VLAN.
  В случае же бизнес-клиента, C-VLAN ID не может однозначно назначаться для Virtual VLAN распределения. Это свойство используется для разделения типов S-VLAN.
- **C-VLAN Preserve режим (параметр cvlanpreservemode).**
  Параметр принимает два значения: Preserve и NotPreserve.
  Этот параметр выбирает режим тегирования C-VLAN для S-VLAN.
  Preserve означает, что CVLAN тег подвергается преобразованиям только в соответствии с поведением dot1Q, то есть, базируясь только на Virtual VLAN распределении, но не будет перезаписан PVID, если полученный фрейм C-VLAN тегированный.
  При этом типе привязки, PVID будет использован при тегировании только нетегированных фреймов.
  NotPreserve означает, что C-VLAN тег при получении тегированных фреймов DAS-3248 будет определяться на основании PVID порта вхождения. C-VLAN тег входящего пакета в этом случае может быть использован только в случае применения C2S профиля или тегировании, базирующего на потоке данных.

- **C-VLAN QoS Preserve (параметр cvlanqospreservemode)**

Этот управляющий параметр определяет метод регенерации приоритета (изменения приоритета) для C-VLAN тега. Принимает два значения - Preserve или Regenerate.

Preserve означает, что приоритет для C-VLAN тега должен остаться неизменным. Regenerate означает, что приоритет для C-VLAN тега должно подвергнуться приоритетной обработке, базирующейся на таблице очередей и приоритетов, определенной согласно IEEE 802.1p.

7.4.3. Приоритезация трафика с Использованием Q-in-Q.

Приоритетная обработка 802.1p базируется на пакетах, принятых на оконечных портах DSLAM или портах поставщика услуг. Класс трафика всегда привязан к приоритету S-VLAN, который в свою очередь определяется на основании приоритета порта или через регенерацию приоритета или через внутренний приоритет, если используется фильтрация трафика и через приоритет на S-VLAN тега, полученного портом поставщика. Приоритет для бизнес и резидентных клиентов определяется следующим образом:

7.4.3.1. Бизнес Клиент

Приоритетные характеристики для бизнес клиентов следующие:

- C-VLAN приоритет присутствует во входящем пакете.
- S-VLAN приоритет будет таким же, как и C-VLAN приоритет.
- S-VLAN приоритет может изменяться на основании регенерации приоритета.
- Если пакет первоначально нетегированный, для C-VLAN и S-VLAN будет использоваться приоритет по умолчанию данного порта.
- Определение приоритета на основе потока (Flow based priority) перезаписывает текущий S-VLAN приоритет.

7.4.3.2. Резидентный Клиент

- Если принят нетегированный пакет, используется приоритет по умолчанию как для C-VLAN, так и S-VLAN.
- Если принят тегированный пакет, используется регенерация приоритета как для C-VLAN, так и S-VLAN.
- C-VLAN регенерация управляется флагом S-VLAN, которая идентифицирует, должен ли приоритет быть сохранен или перезаписан.
- В добавлении ко всему, определение приоритета на основе потока и отдельные приоритеты на основе других способов обработки могут сосуществовать одновременно.

7.4.4. Порядок обработки потока данных при использовании Q-in-Q.

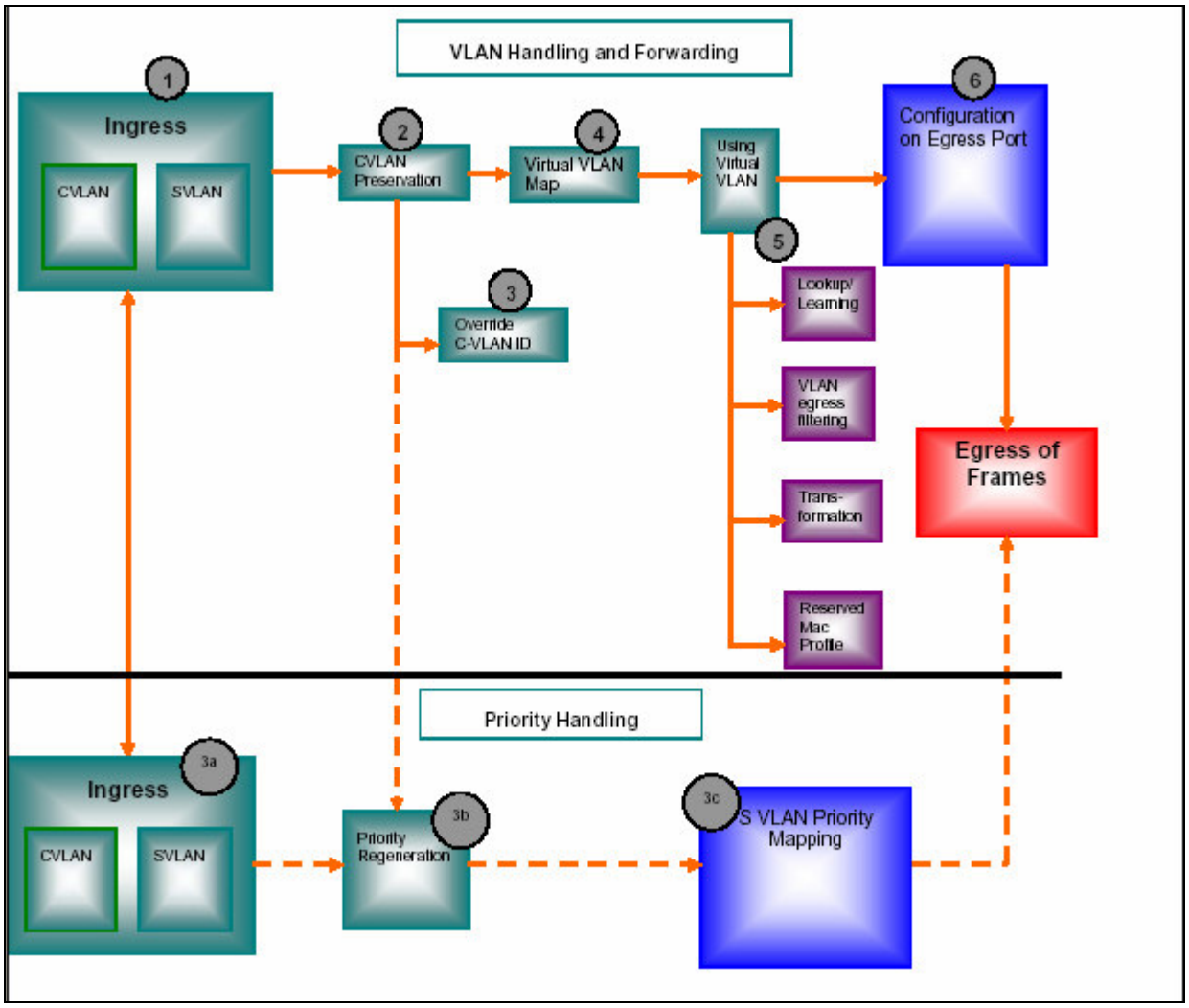


Рисунок 3.Порядок обработки VLAN тегов пакетов в DAS-3248 при использовании Q-in-Q

Порядок обработки пакетов при использовании Q-in-Q:

1. Пакет принимается на входящий интерфейс. Во входящем пакете определяются C-VLAN и S-VLAN теги, исходя из нижеследующего:

Определение C-VLAN тега.
C-VLAN определяется, используя:

- Тег C-VLAN фрейма, если таковой имеется.
- C-VLAN тег, содержащийся в пакете, используется, если C2S Profile связан и приложен на данный оконечный порт.

- Если пакет не содержит C-VLAN тег и профиль C2S не приложен к порту или пакет приходит не из доверенной сети, используется PVID.
- C-VLAN может также быть определен на основании классификации потока.

Определение S-VLAN тега.

S-VLAN может быть определен, используя:

- S-VLAN тег, содержащийся в пакете.
- Если пакет не содержит S-VLAN тег, используется PSVID.
- Если C-VLAN определен, S-VLAN может также может быть определен через CtoS профиль.
- S-VLAN может также быть определен, базируясь на классификации потока.

2 . Применяется режим сохранения (Preserve режим) для C-VLAN ID и приоритета C-VLAN, исходя из конфигурации S-VLAN.

3. Если согласно конфигурации S-VLAN C-VLAN должен быть перезаписан, то дальнейшем применяется PVID в качестве C-VLAN ID.

3a) Определяется C-VLAN и S-VLAN приоритет на входящем кадре:

- C-VLAN приоритет определяется, используя тег C-VLAN или приоритет по умолчанию defSrcPrio, или через классификацию потока.
- S-VLAN приоритет определяется, используя, тег C-VLAN, если фрейм не тегирован S-VLAN ID или через приоритет S-VLAN тега, или через приоритет по умолчанию defSrcPrio, или через классификацию потока.

3b) Применяется, если таковая сконфигурирована, регенерация приоритета на входном порту. Регенерация используется, если поступающие S-VLAN и C-VLAN ID содержат приоритетную информацию, которая должна изменяться на заранее известную заданную величину. В течение регенерации:

- S-VLAN приоритет изменяется, если он определен, базируясь на S-VLAN теге.
- C-VLAN приоритет изменяется, если он определен, базируясь на C-VLAN теге, и базируясь на конфигурации S-VLAN.

3c) S-VLAN приоритет отображается на класс трафика исходящей очереди, базируясь на таблице соответствия очередей и приоритетов, сконфигурированных в исходящем порте. Класс трафика используется для выходного фрейма.

4.Используя C-VLAN ID и S-VLAN ID, формируется Virtual VLAN.

5. Используя конфигурацию Virtual VLAN, выполняются следующие задачи:

- Поиск порта назначения в таблице коммутации;
- Изучение (Learning) фреймов Ethernet таблицей коммутации;
- VLAN выходная фильтрация;
- V-LAN трансформация для C-VLAN тега;
- Применение резервных MAC профилей (Reserved MAC Profile).

6. S-VLAN тег добавляется или удаляется из выходного фрейма, базируясь на конфигурации выходного порта:

- Для порта поставщика услуг - посылается фрейм, содержащий сформированный S-VLAN тег;
- Для оконечного порта – посылает фрейм без S-VLAN тега. CtoS профиль может быть использован, если профиль приложен на исходящий порт, чтобы перезаписать C-VLAN тег, если для C-VLAN определен режим NotPreserve.
- C-VLAN определение. C-VLAN тег определяется на основании S-VLAN тега, если это требуется.

7.4.5.VLAN транкинг (VLAN Trunk).Особенности и ограничения применения услуги E-line.

Услуга E-line сетей MAN- есть VLAN Trunk и, как следует из его названия, является прямым соединением двух портов DSLAM, являющихся участниками одного и того же VLAN. Тогда весь трафик из одного порта направляется на другой порт, то есть происходит эмуляция выделенного канала.

При такой функции увеличивается производительность передачи данных, поскольку не используется поиск порта назначения по таблице коммутации и обучение порта MAC адресам.

Если есть требование маршрутизировать трафик только между двумя портами на VLAN, VLAN Trunk позволяет это делать. Основное требование для трафика, участвующего в VLAN Trunk - VLAN идентификация, для того корректно перенаправлять трафик между двумя участвующими порты. Таким образом, мы получаем выделенную линию, где трафик туннелируется, используя VLAN.

Vlan Trunk указывается параметром **bridgingmode CrossConnect** команды create vlan static.

DAS-3248 имеет возможность применить VLAN Trunk к выбранным VLAN, тогда как другие VLAN могут управляться с помощью стандартного поиска по таблице коммутации (по VLAN и MAC адресу). Тем не менее, при использовании VLAN Trunk, неизвестные юникастные и незарегистрированные групповые адреса не изучаются таблицей коммутации.

Кроме того, применение VLAN Trunk имеет еще целый ряд особенностей и ограничений. Например, флуд-контроль для юникастных пакетов не производится при применении VLAN Trunk (так как не производится поиск по таблице коммутации). Тоже самое касается групповых и широковещательных пакетов.

В режима Q-in-Q, VLAN Trunk прилагается к Virtual VLAN. Пакеты с собственными MAC адресами не будут фильтроваться. Это происходит, поскольку VLAN Trunk эмулирует виртуальную трубу, в котором MAC адреса, переносимые в туннелированных пакетах могут быть MAC адресами с локальным значением и, следовательно, могут ненамеренно конфликтовать с собственными MAC адресами DAS-3248.

PPPoA to PPPoE Internetworking не поддерживается в VLAN Trunk .

Из-за отсутствия любого поиска, в VLAN Trunk режиме пакетные фильтры созданные, используя интерфейс пакетной фильтрации на базе VLAN, не будут работать. Тем не менее, фильтры, как и прежде, управляют любой классификация трафика и QoS .

IGMP при использовании VLAN Trunk может только передавать IGMP трафик из одного порта на другое, но никакие групповые данные не создаются. Для Upstream потока, IGMP Snooping функция может быть включена только на портах, не входящих в VLAN Trunk.

7.4.6.Совместимость Q-in-Q с другими технологиями, использованными в DAS-3248.

7.4.6.1 Управление Ethernet портами. Management VLAN при использовании Q-in-Q.
Как было описано выше, для управления VLAN существуют два режима: Native и Q-in-Q. Управление Ethernet портами при использовании Native режима было рассмотрено в Главе1. Для управления же интерфейсами Ethernet в режиме Q-in-Q, кроме C-VLAN поддерживаются также тегирование интерфейсов управляющими V-LAN S-VLAN и T-VLAN. В этом случае, соответствующие VLAN теги включается в пакеты Ethernet при передаче и проверяются при получении пакета. VLAN ID всех трех уровней могут быть модифицированы через команды CLI при создании интерфейса управления Ethernet или позднее.

Сконфигурированные VLAN ID будут частью VLAN тегов, вставляемых в кадры Ethernet при передаче пакета. При приеме пакета на управляющий интерфейс кадры будут проверяться на наличие в них соответствующих VLAN тегов, и в случае несовпадения, полученные пакеты будут отброшены.
Настройки по умолчанию: величина T-VLAN ID, S-VLAN ID и CVLAN ID – 0 (по умолчанию не определены). Приоритет C-VLAN также не задан.

Консольные команды для управления Management VLAN при использовании Q-in-Q:
Для создания интерфейса управления Ethernet с использованием C-VLAN ID, используйте команду:
create Ethernet intf ifname <name> ip <ddd.ddd.ddd.ddd> mask<ddd.ddd.ddd.ddd> mgmtvlanid <dec>
Для создания интерфейса управления Ethernet с использованием S-VLAN ID, используйте команду:
create Ethernet intf ifname <name> mask ip <ddd.ddd.ddd.ddd> mask <ddd.ddd.ddd.ddd> mgmtsvlanid <dec>
Для создания интерфейса управления Ethernet с TVLAN ID (Third VLAN Tag) как параметром, команду:
create Ethernet intf ifname <name> ip <ddd.ddd.ddd.ddd> mask <ddd.ddd.ddd.ddd> mgmttvlanid <dec>

Для модификации параметров используйте команды modify:
modify Ethernet intf ifname <name> mgmtvlanid <dec> priority <dec>
modify Ethernet intf ifname <name> mgmtsvlanid <dec>
modify Ethernet intf ifname <name> mgmttvlanid <dec>

7.4.6.2. Назначение и использование Reserved MAC Profile.
Домен поставщика услуг и домен клиента - две разных сети. Поэтому управляющие протоколы, использующие зарезервированные MAC адреса, работают в одной сети и не создаются помех протоколам, работающим в другой сети.
Такими протоколами являются, например, протоколы групп STP и GARP, а также LACP и некоторые другие. Эти протоколы используют область зарезервированных IEEE802.3 MAC адресов 01:80:c2:00:00:00 - 01:80:c2:00:00:ff.
Примечание: подробнее смотрите http://standards.ieee.org/regauth/groupmac/tutorial.html

DAS-3248 поддерживает управление протоколами, использующими MAC адреса диапазонов 01:80:c2:00:00:00-01:80:c2:00:00:0f и 01:80:c2:00:00:20-01:80:c2:00:00:2f через Reserved MAC Profile.

В случае резидентных клиентов DAS-3248 будет частью домена поставщика услуг, поэтому любые широковещательные пакеты, полученные из сети клиента, должны быть отброшены. В случае бизнес-клиента для E-Line и E-LAN услуг пакеты должны прозрачно тунеллироваться через домен поставщика услуг в другую часть E-Line или E-LAN сети.

К примеру, с помощью Reserved MAC Profile DAS-3248 может прозрачно участвовать в протоколе 802.1x для аутентификации клиентских устройств.

Reserved MAC Profile определяют поведение каждого MAC адреса из зарезервированного диапазона MAC. Reserved MAC Profile прилагаются на отдельные Virtual VLAN или глобально на все VirtualLAN, если не указана его привязка. Глобальный MAC профиль может быть только один.

С MAC адресами возможны следующие действия при использовании Reserved MAC Profile:

- Drop- отбрасывает пакеты для этого адреса MAC
- Participate –прозрачно пропускать пакеты для этого протокола
- Transformed broadcast- туннелировать пакеты в другой узел посредством S-VLAN.

Если MAC адрес из диапазона 01:80:c2:00:00:00-01:80:c2:00:00:ff не описан в Reserved MAC профилях, то по умолчанию для него принимается действие Drop.
Поскольку Reserved MAC Profile могут прикладываться к MAC адресу или глобально или с использованием определенных Virtual VLAN, то необходимо разграничить сферы влияния этих профилей.

Политика использования Reserved MAC Profile такова.
Действие, сконфигурированное для определенного MAC адреса в глобальном Reserved MAC профиле, прилагается на все Virtual VLAN, независимо от действия, определенного в профилях, связанных с конкретными Virtual VLAN. Для всех других MAC адресов, которые не представлены в профиле, действие может быть сконфигурировано пользователемс помощью локальных профилей (прилагаемых к Virtual VLAN). Для MAC адресов, которые не описаны ни в глобальных, ни в локальных профилях, действует действие по умолчанию.
Команды конфигурирования Reserved MAC Profile:

Глобально:
1.Создать профиль

create resvdmac profile info profileid id
2.Определить параметры профиля
create resvdmac profile param Profileid id **mcastaddr** XX:XX:XX:XX:XX:XX **action** <action>
3.Задать текущий глобальный MAC профиль (изменить привязку профиля по умолчанию на пользовательский глобальный профиль).
modify bridge tbg info resvmacprofileid id

Локально (в применении к определенным Virtual VLAN):
1.Создать профиль
create resvdmac profile info profileid id
2.Определить параметры профиля
create resvdmac profile param Profileid id **mcastaddr** XX:XX:XX:XX:XX:XX **action** < action>
3.Применить профиль к Virtual VLAN (создать локальный Reserved MAC Profile):
modify vlan static vlanname vlanname **resvmacprofileid** resvmacprofileid

7.4.6.3. Совместимость IPoA to IPoE Tunneling и Q-in-Q.

При использовании Q-in-Q IPoA функция используется в основном для резидентных клиентов. В Native режиме использования VLAN пользователь может сконфигурировать на Bridge интерфейсе (созданному поверх IPoE интерфейса) VLAN, базирующуюся на привязке к порту DSLAM (PortBased VLAN). В Q-in-Q режиме такая VLAN создается при помощи C-VLAN ID и PSVID, сконфигурированному на заданном порту.

Для Upstream трафика маршрут для Virtual VLAN определяться на основе C-VLAN ID и S-VLAN ID. RID определяется исходя из Virtual VLAN ID. Следовательно, специальная запись будет создана на Virtual VLAN ID, которая идентифицирует собственные MAC адреса для IPoA to IPoE Tunneling. IPoE Интерфейс требует определения параметров S-VLAN, C-VLAN, MAC адрес источника и MAC адреса назначения для инкапсулирования их в Upstream трафик.

Для Downstream маршрута, сначала определяется RID и затем производится поиск IP адреса IP исходя из RID, точно также как это делается в Native режиме. После такого конфигурирования, DAS-3248 сможет желать независимое от BRAS назначение IP адресов.

IPoA to IPoE Tunneling не применяется для бизнес-клиентов, хотя DAS-3248 не имеет встроенных ограничителей от использования этого механизма. Для бизнес-клиента, более правильным является метод, когда в сети развернут DHCP сервер, чтобы однозначно назначать IP адреса в пределах S-VLAN, в которых RID определяется, исходя из S-VLAN .

7.4.6.4. Совместимость PPPoA to PPPoE Internetworking с Q-in-Q.

При использовании Q-in-Q IPoA функция используется в основном для резидентных клиентов. В Native режиме использования VLAN пользователь может сконфигурировать на Bridge интерфейсе (созданному поверх PPPoA интерфейса) VLAN, базирующуюся на привязке к порту DSLAM (PortBased VLAN). В Q-in-Q режиме такая VLAN создается при помощи C-VLAN ID и PSVID, сконфигурированному на заданном порту.

Для Upstream трафика маршрут для Virtual VLAN определяться на основе C-VLAN ID и S-VLAN ID. Следовательно, специальная запись будет создана на Virtual VLAN ID, которая идентифицирует собственные MAC адреса для PPPoA to PPPoE Internetworking и требуется повторный поиск по таблице коммутации для Downstream маршрута.

Повторный поиск будет базироваться на Virtual VLAN ID, собственном MAC адресе, MAC адресе access concentrator (AC) и session id. Это позволяет делать независимое от BRAS назначение Session ID.

PPPoA to PPPoE Internetworking не применяется для бизнес типа клиентов, хотя DAS-3248 не имеет встроенного ограничителя от использования этого механизма. Для бизнес клиента более правильным является метод, когда другой конец VPN (E-LAN) – правильно сконфигурированный PPPoE сервер, который назначает уникальные Session ID в пределах S-VLAN, где Virtual VLAN ID определяется из S-VLAN.

7.4.7. Настройки Q-in-Q по умолчанию

Когда система переходит в режим Q-in-Q, по умолчанию используются следующие настройки:

1. Создается S-VLAN 1 с параметрами:
а) Тип -Residental.
б) C-VLAN preservation -802.1q.
в) Режим QoS C-VLAN- Regenerate.

2. Все порты создаются по умолчанию оконечные порты.

3. Создается Virtual VLAN 1, членами которого являются все порты как нетегированные члены VLAN.
Он связывает C-VLANID=1 , S-VLANID=1 в VirtualVlanID =1.

4. TVLAN (Third VLAN Tag) не определен по умолчанию.

5. Создается Reserved Mac Profile с Profileid 1 и действием для MAC адресов 01:80:c2:00:00:20 и 01:80:c2:00:00:21 – TransformedBcast (для протокола GVRP) и действием для MAC адреса 01:80:c2:00:00:02 - Participate (для протокола LACP). Этот профиль связывается со всеми VLAN по умолчанию.

7.4.8. Типовые сценарии Q-in-Q. Примеры использования.

В этом разделе приведены три наиболее распространенных примера использования технологии Q-in-Q:

- Пример подключения бизнес клиента
- Пример подключения бизнес клиента (услуга E-line)
- Пример подключения бизнес клиента (услуга E-LAN).

7.4.8.1. Пример подключения бизнес клиента.

Выполните следующие шаги:

1.Переведите DAS-3248 в режим Q-in-Q:
$nbsize vlanmode stackedmode
$commit
$reboot

2.Пометьте bridge port 385 (Uplink1) как провайдерский порт
(добавляющий теги второго уровня).
$modify bridge port intf portid 385 status disable
$ modify gvrp port info portid 385 ppstatus enable
$ modify bridge port intf portid 385 status enable

3. Создайте C-VLAN, указав C-VLANID и порты, которые будут входить в этот C-VLAN.
$ create vlan static vlanname v2 vlanid 2 egressports 20 385 untaggedports 20
$ modify gvrp port info portid 20 psvlanid 3 portvlanid 2

4. Создайте S-LAN, указав SVALID и S-VLAN тип residential
$ create vlan svlan svlanid 3 svlantype residential cvlanpreservemode preserve cvlanqospreservemode regenerate

5. Создайте Virtual VLAN, объединив S-VAN ID и C-LAN ID.
$ create vlan mapprofile info profileid 1 profiletype ctos
$ create vlan virmap svlanid 3 cvlanid 2 vvlanid 2

6.Сохранить конфигурацию
$ commit

7.4.8.2. Пример подключения бизнес-клиента (услуга E-Line).

Выполните следующие шаги:

1. Переведите DAS-3248 в режим Q-in-Q и перезагрузите устройство.
$**nbsize vlanmode stackedmode**
$commit

$reboot

2.Пометьте bridge port 385 (Uplink1) как провайдерский порт
(добавляющий теги второго уровня).
$modify bridge port intf portid 385 status disable
$ modify gvrp port info portid 385 ppstatus enable
$ modify bridge port intf portid 385 status enable

3.Создайте C-VLAN с режимом bridgemode CrossConnect. Этот параметр определяет прямое соединение портов DSLAM (без анализа пакетов).
$ create vlan static vlanname v2 vlanid 2 egressports 20 385 untaggedports 20 Bridgingmode crossconnect
$ modify gvrp port info portid 20 psvlanid 3 portvlanid 2

4. Создайте S-VLAN, указав SVALID и S-VLAN тип business
$ create vlan svlan svlanid 3 svlantype Business cvlanpreservemode preserve cvlanqospreservemode regenerate

5.Создайте Virtual VLAN, объединив S-VAN ID и C-LAN ID.
$ create vlan mapprofile info profileid 1 profiletype ctos
$ create vlan virmap svlanid 3 cvlanid 4097 vvlanid 2

6.Сохранить конфигурацию
$ commit

7.4.8.3. Пример подключения бизнес-клиента (услуга E-LAN).
Выполните следующие шаги:

1. Переведите DAS-3248 в режим Q-in-Q:
$**nbsize vlanmode stackedmode**
$commit
$reboot

2.Пометьте bridge port 385 (Uplink1) как провайдерский порт
(добавляющий теги второго уровня).
$modify bridge port intf portid 385 status disable
$ modify gvrp port info portid 385 ppstatus enable
$ modify bridge port intf portid 385 status enable

3. Создайте S-VLAN, указав SVALID и S-VLAN тип business:
$ create vlan svlan svlanid 3 svlantype Business cvlanpreservemode preserve cvlanqospreservemode regenerate

4. Создайте C-VLAN, указав C-VLANID и порты, которые будут входить в этот C-VLAN.
$ create vlan static vlanname v2 vlanid 2 egressports 20 385 untaggedports 20
$ modify gvrp port info portid 20 psvlanid 3 portvlanid 2

5.Создайте Virtual VLAN, объединив S-VAN ID и C-LAN ID.
$ create vlan mapprofile info profileid 1 profiletype ctos
$ create vlan virmap svlanid 3 cvlanid 4097 vvlanid 2

6.Сохранить конфигурацию
$ commit

7.5.Групповая рассылка (IGMP Snooping)

IP хосты используют протокол IGMP (Internet Group management Protocol) для уведомления всех непосредственно подключенных multicast маршрутизаторах о своем членстве в группе множественной рассылки. Протокол IGMP является неотъемлемой частью IP. Поддержка этого протокола должна быть реализована на всех хостах, получающих multicast трафик.
IGMP Snooping – это процесс перехвата и анализа IGMP сообщений между хостами и маршрутизаторами. Используется термин snooping (слежка – англ.), т.к. коммутатор второго уровня просматривает заголовки третьего уровня в поисках необходимой ему информации, но при этом не осуществляет реальной обработки пакетов на третьем уровне.
IGMP Snooping предоставляет информацию DAS-3248 о принадлежности его портов к группам множественной рассылки, позволяя соответствующим образом изменять таблицу multicast форвардинга, что обеспечивает коммутацию multicast трафик только на те порты, которые подключены к данной multicast группе, тем самым достигается существенная экономия полосы пропускания.
Рисунок 7-3 отображает принцип работы IGMP Snooping. Уведомления (reports) посылаются со стороны CPE multicast маршрутизатору (Net Side). Это могут быть уведомления о членстве в группе, о покидании multicast группы и уведомления в ответ на запросы (queries) multicast маршрутизатора. Queries передаются с Net Side DAS-3248 (один из Uplink портов) на сторону CPE.

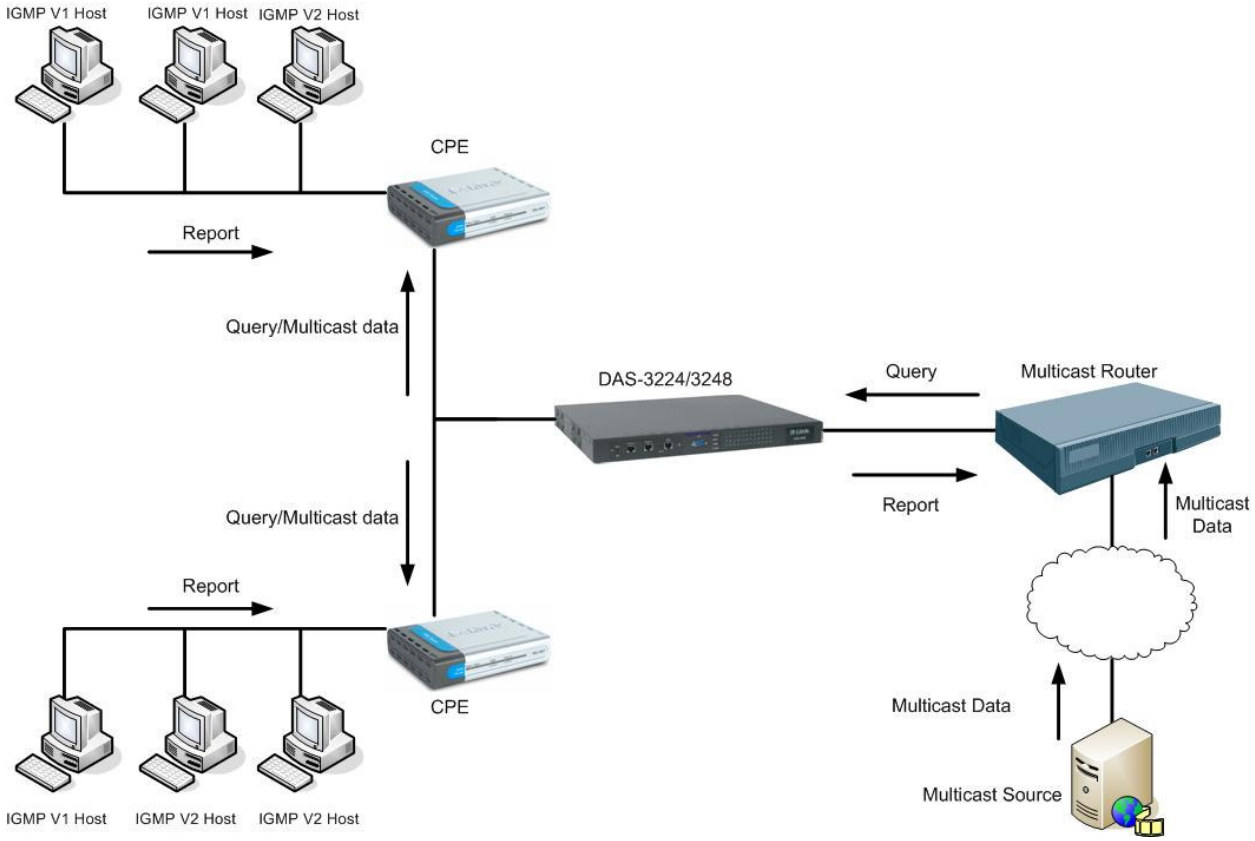


Рисунок 7-3: IGMP Snooping

7.5.1. Концепция IGMP Snooping

Обычный коммутатор рассматривает трафик групповой рассылки как широковещательный и, следовательно, передает копию каждого multicast пакета на каждый из своих портов. Таким образом, multicast данные передаются даже на сегменты локальной сети, которые не содержат членов соответствующей multicast группы, что приводит к уменьшению полезной полосы пропускания.
Коммутатор с поддержкой IGMP Snooping позволяет избежать этого, т.к. он не передает multicast трафик на те порты, которые в нем не заинтересованы. Данная возможность основана на перехвате и анализе IGMP пакетов, передаваемых между хостами и multicast маршрутизаторами. На основании этого анализа DAS-3248 строит базу данных принадлежности к multicast группам и активных портов. На настоящий момент поддерживаются версии 1,2 и 3 протокола IGMP.

7.5.2. Особенности реализации IGMP Snooping в DAS-3248

IGMP Snooping DAS-3248 выполняет следующие функции:

- Перехват multicast ip адресов путем анализа IGMP пакетов
- Преобразование multicast ip адресов в соответствующие MAC адреса.
- Обновление полей VLAN-ID, Multicast MAC address, Port таблицы форвардинга.
- Передача IGMP уведомлений через Uplink порт.
- Подавление нескольких копий уведомлений о членстве в одной группе от разных пользователей.
- Генерация и передача multicast запросов тем портам, которые ранее уведомили в своем членстве в данной multicast группе.
- Удаление по истечению тайм-аута записей из таблицы multicast форвардинга.
- Предоставление статистической информации

7.5.2.1 Перенаправление IGMP пакетов к CPU DAS-3248

Перед включением IGMP Snooping в DAS-3248 требуется создать правило generic фильтра со следующими параметрами:
- action as “sendtocontrol”
- snooplevel as “bridge”
-decsription as “IGMP”
Также необходимо создать для этого правила IP подправило, которое бы соответствовало всем пакетам IP протокола 2 (IGMP). После этого нужно применить данное правило на все порты, с которых возможно получение IGMP уведомлений.
Более подробно процесс создания данного правила будет описан ниже в 7.5.2.10.
Внимание: Данное правило уже сконфигурировано в настройках по умолчанию (заводских).

7.5.2.2. Включение IGMP

В DAS-3248 включение функции IGMP Snooping происходи в два этапа: глобальное включение и включение IGMP Snooping для конкретного порта. Для того чтобы включить IGMP Snooping на определенном порту, нужно сначала включить данную функцию глобально командой **modify igmpsnoop cfg info status enable.**

7.5.2.3.Обработка IGMP Join уведомлений

В режиме Full Bridging DAS-3248 передает полученные уведомления о членстве в группе на все порты, удовлетворяющие следующим условиям:
- для них включен IGMP Snooping;
- с этих портов был получен запрос (Query).

Если DAS-3248 получит уведомление, но при этом он не получал запроса для этой группы, данное уведомление будет передано на порты, удовлетворяющие условиям: данные порты должны выходить либо в группу forward unregistered, либо в группу forward all.

Примечание: список портов, входящих в группы forward unregistered и forward all задается с помощью команд:
modify bridge mcast fwdall [vlanid <dec>] [egressports <Opt>] [forbidegressports <Opt>]

modify bridge mcast fwdunreg [vlanid <dec>] [egressports <Opt>] [forbidegressports <Opt>]

Подробнее список данных команд будет описан далее.

Однако данный процесс связан с неоправданным использованием полосы пропускания. Для того чтобы избежать многократного дублирования уведомлений, пользователь может настроить список портов с подключенными к ним multicast маршрутизаторами.
В режиме half bridging, уведомления всегда передаются на Uplink интерфейс.

7.5.2.4.Обработка уведомлений IGMP Leave

Протокол IGMP имеет три варианта обработки сообщений о прекращении членства в группе множественной рассылки (Leave сообщения): Normal, Fast и FastNormal.
Normal: leave сообщения передаются multicast маршрутизатору, затем базируясь на ответном запросе данного маршрутизатора о членстве в группе, запускается leave процесс.
Fast: порт немедленно удаляется из данной группы множественной рассылки после получения DSLAM-ом сообщения leave. После этого данное сообщение передается multicast маршрутизатору. Данный режим должен использоваться в случае, если к порту подключен только один multicast клиент. Иначе, после получения сообщения leave от одного из нескольких multicast клиентов, остальные клиенты также будут лишены возможности принимать трафик множественной рассылки.
FastNormal: сообщения leave передаются multicast маршрутизатору, после чего немедленно (не ожидая ответа от маршрутизатора), запускается leave процесс. Таким образом, данный вариант уменьшает задержку в обработке leave сообщений.

7.5.2.5. Обработка запросов multicast маршрутизатора (Queries)

Главный IGMP запрос (IGMP General Query) передается всем группам множественной рассылки. Если в поле destination ip address IGMP запроса стоит адрес 224.0.0.1, то этот запрос будет передан на все порты DAS-3248 за исключением того порта, на который он был получен.
IGMP запросы о членстве в группе (IGMP Group Specific Query) передаются всем членам данной группы множественной рассылки в данном VLAN, а также на все multicast маршрутизаторы. Если в базе данных multicast форвардинга нет записей, соответствующих данной группе множественной рассылки и VLAN, то запросы будут переданы на все порты, указанные как fwdunreg и fwdall и на все multicast маршрутизаторы, находящиеся в данном VLAN.

7.5.2.6 Порты multicast запросчиков (Multicast Queriers Ports)

Порты DAS-3248, к которым подключены multicast запросчики, делятся на два типа:

1. Динамически обнаруженные.
2. Статически сконфигурированные.

Динамически обнаруженные порты

Вторая версия протокола IGMP определяет механизм выбора запросчика (Qurier). IGMP первой версии оставляет выбор запросчика за протоколами multicast маршрутизации, причем каждый протокол использует свой собственный механизм, отличный от других, что может привести к появлению в одной сети нескольких запросчиков.
Запросчик – это multicast маршрутизатор, рассылающий IGMP запросы. Остальные multicast маршрутизаторы, подключенные к той же сети, IGMP запросы посылать не будут в целях уменьшения трафика. Запросчиком становится multicast маршрутизатор с наименьшим ip адресом. При появлении в сети multicast маршрутизатора, имеющего меньший адрес, чем у текущего запросчика, будет инициирована новая процедура выборов. Также данная процедура будет инициирована при пропадании текущего запросчика из сети.
В режиме полной коммутации (full bridging) DAS-3248, запросчик может находиться где угодно, в том числе и со стороны одного из adsl портов. Поэтому процедура выбора запросчика необходима. Ранее это было неактуально, т.к. предполагалось, что запросчик только один, и он подключен к Uplink порту DSLAM.

Статически сконфигурированные порты

Порты, к которым подключены запросчики, могут быть также заданы статически. При этом подразумевается, что к данным порта подключены multicast маршрутизаторы, поддерживающие только первую версию протокола IGMP. Порты DAS-3248 IGMP второй версии не могут быть статически сконфигурированными, они обнаруживаются динамически с помощью механизма выборов запросчика.

Команды системы:

create igmpsnoop
querier info

Описание: Создание статической записи о запросчике.
Синтаксис команды: create igmpsnoop querier info vlanid <идентификатор VLAN> portid <идентификатор порта, к которому подключен запросчик>

get igmpsnoop querier info

Описание: Просмотр статичских записей о запросчиках.
Синтаксис команды: get igmpsnoop querier info [vlanid <идентификатор VLAN>] [portid <идентификатор порта, к которому подключен запросчик>]

delete igmpsnoop querier info

Описание: Удаление информации о запросчике.
Синтаксис команды: delete igmpsnoop querier info vlanid <идентификатор VLAN> portid <идентификатор порта, к которому подключен запросчик>

Таблица параметров:

vlanid vlanid	Идентификатор VLAN. **Использование:** Create - Обязательно. Delete - Обязательно. Get – Опционально. **Принимает значения:** 1..4095
portid portid	Идентификатор bridge порта, к которому подключен запросчик. **Использование:** Create – Обязательно. Delete – Обязательно Get – Опционально **Принимает значения:** 1..395

Пример команды: $ create igmpsnoop querier info vlanid 6 portid 6

7.5.2.7. Подавление уведомлений

Механизм передачи IGMP уведомлений может функционировать в двух режимах:

1. подавление уведомлений включено
2. подавление уведомлений выключено

Если источнику множественной рассылки или multicast маршрутизатору не требуется информация обо всех MAC адресах multicast клиентов, то дублирующиеся уведомления о членстве в группе множественной рассылки (например, если к одному порту подключено несколько клиентов одной multicast группы) будут отброшены DAS-3248, т.е. они не будут переданы на Uplink интерфейс, тем самым достигается экономия полосы пропускания. Однако может возникнуть такая ситуация, когда необходимо знать MAC адреса всех multicast клиентов, объявивших о своем членстве в группе множественной рассылки (например, для биллинга). В этом случае подавление уведомлений нежелательно.
В DAS-3248 функция подавления уведомлений применяется на всю систему целиком, а не на конкретную группу множественной рассылки. По умолчанию, данная функция отключена.

Команды системы:

modify igmpsnoop cfg info

Описание: Изменение параметров IGMP Snooping.

Синтаксис команды: modify igmpsnoop cfg info [queryinterval queryinterval] [anxioustimer anxioustimer] [v1hosttimer v1hosttimer] [lastmembqryinterval lastmembqryinterval] [robustness robustness] [versionmask v1|v2|v3] [startupqryinterval startupqryinterval] [lastmemberqrycount lastmemberqrycount] [startupqrycount startupqrycount] [status Enable | Disable] [reportsup Enable | Disable]

get igmpsnoop cfg info

Описание: Просмотр параметров IGMP Snooping.

Синтаксис команды: get igmpsnoop cfg info

Таблица параметров:

queryinterval queryinterval	Таймер Query Interval (в секундах), используемый для удаления устаревших записей. Запись удаляется, если за время истечения таймера DAS-3248 не получил ни уведомлений ни запросов, связанных с этой записью. Значение данного таймера должно быть как минимум в десять раз больше того, которое сконфигурировано на multicast маршрутизаторе. **Использование:** Modify – Опционально. **Принимает значения:** 1..25
anxioustimer anxioustimer	Максимальный промежуток времени (в десятках секундах), по истечении которого модуль IGMP Snooping начнет передавать все полученные IGMP уведомления о членстве в группе множественной рассылки. **Использование:** Modify – Опционально **Принимает значения:** 1..65535
v1hosttimer v1hosttimer	Промежуток времени, в течение которого DAS-3248 ожидает IGMP пакетов первой версии. Измеряется в секундах. **Использование:** Modify – Опционально. **Принимает значения:** 1 – 65535
lastmembqryinterval lastmembqryinterval	Тайм-аут, в течение которого последний член группы множественной рассылки должен ответить на запрос multicast сервера, иначе запись о данной группе будет удалена с Multicast Database.

	Измеряется в десятых долях секунды. **Использование:** Modify – Опционально. **Принимает значения:** 1 – 255
robustness robustness	Ожидаемая вероятность потери пакета для данной подсети **Использование:** Modify – Опционально.
status Enable | Disable	Включение/выключение IGMP Snooping на устройстве. **Использование:** Modify – Опционально.
reportsup Enable | Disable	Включение/выключение подавления уведомлений **Использование:** Modify – Опционально.
versionmask v1|v2|v3	Версии IGMP протокола, которые разрешено использовать на DAS-3224/3248. Пакеты протоколов, не входящих в этот список будут отбрасываться. **Использование:** Modify – Опционально. **Значение по умолчанию**: v1,v2,v3.
startupqryinterval	Тайм-аут, после истечения которого повторные запросы (Queries) при поднятии порта (Port up)
startupqrycount	Количество запросов (Queries) посылаемых при поднятии порта (Port up)
lastmemberqrycount	Количество запросов (Queries) посылаемых последнему члену группы множественной рассылки перед ее удалением из Multicast Database

7.5.2.8 Multicast Database

DAS-3248 имеет базу данных коммутации трафика групповой рассылки – Multicast Database. Данная база данных обновляется модулем IGMP Snooping и Static multicast. Поиск в данной базе данных осуществляется по multicast MAC адресу и VLANID. Результатом поиска будет список портов, являющихся членами данной группы множественной рассылки и входящих в данную VLAN.

7.5.2.9 Совместная работа с VLAN

Модуль IGMP snooping коммутирует IGMP уведомления в соответствии с bridging mode данного VLAN.

Half Bridging – все уведомления передаются только на uplink порты. Если запросчик находится со стороны adsl портов, то все его пакеты будут отброшены.

Full Bridging - все уведомления передаются на uplink порты, а также всем членам данной группы множественной рассылки. Если запросчик находится со стороны adsl портов, все его пакеты будут скоммутированы всем членам данной группы множественной рассылки.

DAS-3248 поддерживает два режима работы multicast с VLAN:

1. Shared VLAN for multicast – информация о multicast группах является общей для всех VLAN.

2. Independent VLAN for multicast – каждый VLAN имеет свою собственную Multicast Database

Выбор одного из этих режимов осуществляется посредством команды глобального системного конфигурирования modify nbsize:

$ modify nbsize mcastcap ivmcapable devcap IVL
$ modify nbsize mcastcap svmcapable devcap SVL

7.5.2.10 Static Multicast

Записи в Multicast database наряду с динамическим добавлением модулем IGMP Snooping могут быть заданы вручную. Данные записи состоят из Multicast MAC адреса, VLANID, списка портов (Egress ports list) и списка запрещенных портов (Forbidden Egress ports list). Список запрещенных портов содержит порты, которые не могут быть использоваться модулем IGMP snooping.

Команды системы:

create bridge static mcast

Описание:	Создание статической записи в multicast database.
Синтаксис команды:	create bridge static mcast vlanid <идентификатор VLAN> mcastaddr <multicast MAC address> [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

modify bridge static mcast

Описание:	Изменение статической записи в multicast database
Синтаксис команды:	modify bridge static mcast vlanid <идентификатор VLAN> mcastaddr <multicast MAC address> [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

get bridge static mcast

Описание:	Просмотр статических записей в multicast database
Синтаксис команды:	get bridge static mcast [vlanid <идентификатор VLAN>] [mcastaddr <multicast MAC address>]

delete bridge static mcast

Описание:	Удаление статической записи в multicast database
Синтаксис команды:	delete bridge static mcast vlanid <идентификатор VLAN> mcastaddr <multicast MAC address>

Таблица параметров:

vlanid vlanid	Идентификатор VLAN. В случае использования опции Shared VLAN for multicast (см. 2.9), информация о multicast MAC адресах едина для всех VLAN. Таким образом, в данном случае VLANID является опциональным параметром. Если включена опция Independent Vlan for multicast, тогда каждая VLAN имеет свою собственную информацию о MAC адресах групповой рассылки, т.е. в этом случае VLANID является обязательным параметром. **Использование:** Create - Обязательно. Delete - Обязательно. Get – Опционально. Modify – Обязательно. **Принимает значения:** 1..4095
mcastaddr mcastaddr	MAC адрес групповой рассылки **Использование:** Create – Обязательно. Modify – Обязательно. Delete – Обязательно Get - Опционально
egressports egressports	Набор портов, являющихся членами данной группы множественной рассылки. Если порт уже указан как FrobiddenEgressPort, его необязательно включать в данный набор. **Использование:** Create - Опционально. Modify – Опционально. **Принимает значения:** 1 – 395
forbidegressports forbidegressports	Набор портов, являющихся членами данной группы. Динамическая конфигурация IGMP Snooping не распространяется на данные порты. **Использование:** Create - Опционально. Modify – Опционально. **Принимает значения:** 1 – 395

Пример команды: **$ create bridge static mcast vlanid 7 mcastaddr 01:00:5e:00:00:01 egressports 10 forbidegressports 20**

По умолчанию, чтобы избежать нежелательного использования полосы пропускания, DAS-3248 не коммутирует трафик групповой рассылки на ADSL порты. Вы можете изменить данное поведение, настроив форвардинг всего multicast трафика или трафика тех групп, которые не имеют членов среди портов DAS-3248 на список заданных портов.

Команды системы:

modify bridge
mcast fwdall

Описание: Конфигурирования списка портов, которые будут получать трафик групповой рассылки всех групп.

Синтаксис команды: modify bridge mcast fwdall [vlanid <идентификатор VLAN>] [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

get bridge static mcast

Описание: Просмотр списка портов, получающих весь multicast трафик.

Синтаксис команды: get bridge mcast fwdall [vlanid <идентификатор VLAN>]

Таблица параметров:

vlanid vlanid	Идентификатор VLAN. В случае использования опции Shared VLAN for multicast (см. 2.9), информация о multicast MAC адресах едина для всех VLAN. Таким образом, в данном случае VLANID является опциональным параметром. Если включена опция Independent Vlan for multicast, тогда каждая VLAN имеет свою собственную информацию о MAC адресах групповой рассылки, т.е. в этом случае VLANID является обязательным параметром. **Использование:** Create - Обязательно. Delete - Обязательно. Get – Опционально. Modify – Обязательно. **Принимает значения:** 1..4095
egressports egressports	Набор портов данной VLAN, на которые будет коммутироваться весь трафик множественной рассылки. Может быть указано несколько значений, разделенных пробелами. **Использование:** Modify – Опционально.
forbidegressports forbidegressports	Набор портов данной VLAN, для которых атрибут Forward All Multicast Groups может динамически не регистрироваться протоколом GMRP. Может быть указано несколько значений, разделенных пробелами. **Использование:** Modify – Опционально.

Пример команды: $ get bridge mcast fwdall

Экранный вывод:

```
VLAN Index                  : 1
Forward All Ports           : 34
Forward All Static Ports    : 1 2 3 5
Forward All Forbidden Ports : 4 9 10 11

VLAN Index                  : 2
Forward All Ports           : 50
Forward All Static Ports    : 50
```

Forward All Forbidden Ports : None

Команды системы:

modify bridge mcast fwdunreg

Описание: Конфигурирования списка портов, которые будут получать трафик групповой рассылки тех групп, которые не имеют членов на DAS-3248

Синтаксис команды: modify bridge mcast fwdunreg [vlanid <идентификатор VLAN>] [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

get bridge static mcast

Описание: Просмотр списка портов.

Синтаксис команды: get bridge mcast fwdunreg [vlanid <идентификатор VLAN>]

Таблица параметров:

vlanid vlanid	Идентификатор VLAN. В случае использования опции Shared VLAN for multicast (см. 2.9), информация о multicast MAC адресах едина для всех VLAN. Таким образом, в данном случае VLANID является опциональным параметром. Если включена опция Independent Vlan for multicast, тогда каждая VLAN имеет свою собственную информацию о MAC адресах групповой рассылки, т.е. в этом случае VLANID является обязательным параметром. **Использование:** Create - Обязательно. Delete - Обязательно. Get – Опционально. Modify – Обязательно. **Принимает значения:** 1..4095
egressports egressports	Набор портов данной VLAN, на которые будет коммутироваться тот трафик множественной рассылки, для которого нет другой информации о его пересылке. Может быть указано несколько значений, разделенных пробелами. **Использование:** Modify – Опционально.
forbidegressports forbidegressports	Набор портов данной VLAN, для которых атрибут Forward Unregistered Multicast Groups может динамически не регистрироваться протоколом GMRP. Может быть указано несколько значений, разделенных пробелами. **Использование:** Modify – Опционально.

Пример команды: ***$*** **get bridge mcast fwunregl vlanid 1**

VLAN Index : 1 Forward Unregistered Ports : 45 Forward Unregistered Static Ports : 1 2 3 6 Forward Unregistered Forbidden Ports : 4 9 10

7.5.3. Настройка IGMP Snooping

7.5.3.1 Включение

Перед использованием, IGMP snooping должен быть глобально включен на устройстве:

modify igmpsnoop cfg info status enable

Передача пакетов центральному процессору для анализа

create filter rule entry ruleid 1 action sendtocontrol description IGMP snooplevel bridge

create filter subrule ip ruleid 1 subruleid 1 prototypefrom 2 prototypecmp eq

modify filter rule entry ruleid 1 status enable statsstatus enable

create filter rule map ifname all stageid 1 ruleid 1

Замечание*:* данное правило создано в системе по умолчанию.

7.5.3.3. Обработка сообщений leave

modify igmpsnoop port info portid < идентификатор порта**> [leavemode Normal | Fast | FastNormal]**

7.5.3.4. Подавление уведомлений

modify igmpsnoop cfg info [reportsup enable | disable]

7.5.3.5. Включение IGMP snooping на порту

Помимо включения IGMP snooping в целом на устройстве, необходимо также включить IGMP snooping на каждом порту, к которому подключено multicast устройство.

modify igmpsnoop port info portid <идентификатор порта> **status [enable | disable]**

7.5.3.6. Ограничение количества мультикаст-групп на порту

modify igmpsnoop port info portid <идентификатор порта> **maxgrpallowed** < количество групп>

7.5.3.7. Фильтрация мультикаст потока по груповому и IP источника.

create igmpsnoop mvlan config grpipaddr grpipaddr **srcipaddr** srcipaddr **vlanid** vlanid **| none [mcastvlanstag** mcastvlanstag | none **] [mcastvlanctag** mcastvlanctag | invlan | none **] [portlist** portlist | none **]**

Пример : $ create igmpsnoop mvlan config grpipaddr 224.0.0.7 srcipaddr 12.23.34.45 vlanid 6 portlist 5 6 10

Внимание: параметр **srcipaddr** сущесвеннен только при использовании IGMP v.3

7.5.3.8 Просмотр Multicast Database

get bridge mcast forwarding [vlanid <идентификатор VLAN**>]** [**macaddr <**multicast MAC адрес>]

8.Протокол Spanning Tree

8.1.Понятие протокола STP (IEEE 802.1D)

Этот раздел описывает работу протокола STP:

Обзор IEEE 802.1D STP

Spanning Tree Protocol (STP, протокол связующего дерева) - это протокол канального уровня модели OSI, который обеспечивает резервирование каналов связи в коммутируемых сетях, предотвращая возникновение петель.

При создании отказоустойчивой сети, между всеми ее узлами должен существовать единственный активный маршрут. Множество активных маршрутов может привести к возникновению петель. Если в сети существует петля, конечные станции могут получать дубликаты сообщений, а сетевые устройства могут изучить MAC-адрес сетевого узла на нескольких портах, что приведет к нестабильной работе.

Алгоритм *Spanning Tree Algorithm (STA)*, на котором основан протокол, позволяет автоматически определять древовидную структуру связей в сети свободную от петель при произвольном соединении портов между собой. Такая структура называется *покрывающим деревом* - Spanning Tree (иногда ее называют *остовым деревом*).

Конфигурация покрывающего дерева строится устройствами коммутируемой сети автоматически с использованием обмена служебными пакетами.

Понятие Bridge ID

Алгоритм STA требует, чтобы каждому мосту сети был присвоен уникальный идентификатор. *Идентификатор моста (Bridge ID)*– 8-байтное поле, которое состоит из 2-х частей: 2-байтного приоритета, назначенного администратором и 6 байтного MAC-адреса его блока управления.

Каждому порту моста также назначается уникальный в пределах устройства идентификатор как правило, это его MAC-адрес и ставится в соответствие стоимость маршрута, соответствующая затратам на передачу кадра по сети через данный порт.

Выборы корневого моста (Root Bridge)

Процесс вычисления остового дерева начинается с выбора *корневого моста (Root Bridge)*, который является его логической вершиной. В качестве корневого моста выбирается сетевое устройство с наименьшим значением идентификатора Bridge ID. Если все устройства сконфигурированы со значением приоритета по умолчанию равным 32768, корневым мостом станет устройство с наименьшим MAC- адресом. Меняя значения приоритетов сетевых устройств, администратор сети может влиять на процесс выбора корневого моста. Наименьшее значение приоритета повышает вероятность выбора устройства корневым мостом, наибольшее – уменьшает.

Роли портов STP

Следующий этап работы STP – выбор *корневого порта (root port)* для каждого из остальных устройств коммутируемой сети. Корневой порт– это порт, который имеет кратчайшее по сети расстояние до корневого моста.

Последний этап – определение назначенных портов.

Каждый сегмент в коммутируемой сети имеет один *назначенный порт (designated port)*. Этот порт функционирует как единственный порт моста, т.е. принимает пакеты от сегмента и передает их в направлении корневого моста через корневой порт данного сетевого устройства. Устройство, содержащее назначенный порт для данного сегмента называется *назначенным мостом (designated bridge)* этого сегмента. Назначенный порт сегмента имеет наименьшее расстояние до корневого моста, среди всех портов, подключенных к данному сегменту. Назначенный порт у сегмента может быть только один. У корневого моста все порты являются назначенными, а их расстояние до корня полагается равным нулю. Корневого порта у корневого моста нет.

При построении покрывающего дерева важную роль играет понятие расстояния. По этому критерию выбирается единственный порт, соединяющий каждое сетевое устройство с корневым мостом, и единственный порт, соединяющий каждый сегмент сети с корневым мостом. Все остальные порты переводятся в резервное состояние, то есть такое, при котором они не передают обычные кадры данных. При таком выборе активных портов в сети исключаются петли и оставшиеся связи образуют покрывающее дерево.

В качестве расстояния в STA используется метрика *стоимость пути* (Path Cost) – она определяется как суммарное условное время на передачу данных от порта данного сетевого устройства до порта корневого моста. *Условное время сегмента* рассчитывается, как время передачи одного бита информации через канал с определенной полосой пропускания. В таблице приводятся типичные стоимости пути в соответствии со стандартом IEEE 802.1D:

Таблица 8-1

Параметр	**Скорость канала**	**Рекомендованное значение**	**Рекомендованный диапазон**	**Диапазон**
Стоимость пути	4 Мбит/с	250	100-1000	1-65535
Стоимость пути	10 Мбит/с	100	50-600	1-65535
Стоимость пути	16 Мбит/с	62	40-400	1-65535
Стоимость пути	100 Мбит/с	19	10-60	1-65535
Стоимость пути	1 Гбит/с	4	3-10	1-65535
Стоимость пути	10 Гбит/с	2	1-5	1-65535

Понятие Bridge Protocol Data Units

Вычисление остового дерева происходит при включении сетевого устройства и при изменении топологии. Эти вычисления требуют периодического обмена информацией между устройствами связующего дерева, что достигается при помощи специальных пакетов, называемых блоками данных протокола моста - *BPDU (Bridge Protocol Data Unit)*.

Пакеты BPDU содержат следующую информацию, необходимую для построения топологии сети без петель:

- Идентификатор Bridge ID, на основании которого выбирается корневой мост

- Расстояние от моста-источника до корневого моста (стоимость корневого маршрута)
- Идентификатор порта

Пакеты BPDU помещаются в поле данных кадров канального уровня, например, кадров Ethernet.

Сетевые устройства обмениваются BPDU через равные интервалы времени (обычно 1-4с). В случае отказа моста (что приводит к изменению топологии) соседние устройства, не получив пакет BPDU в течение заданного времени (Max Age), начинают пересчет остового дерева.

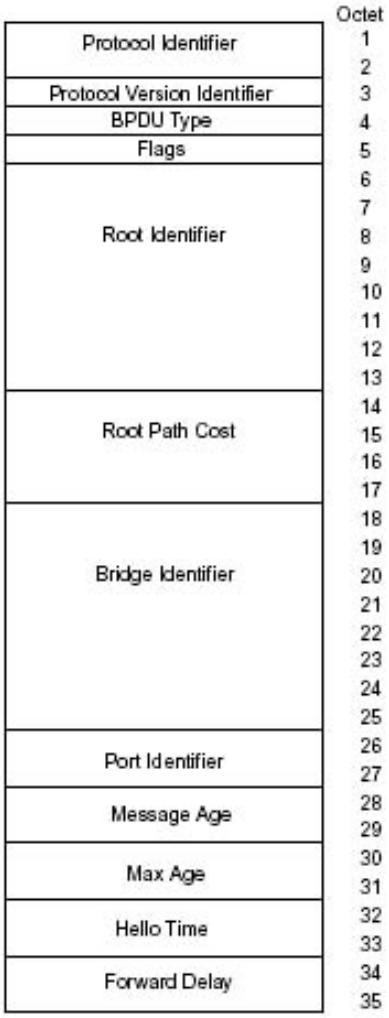


Рисунок 8-1. Формат BPDU.

Пакет BPDU имеет следующие поля:

- Идентификатор версии протокола STA (Protocol Identifier)- 2 байта. Сетевые устройства должны поддерживать одну и ту же версию протокола STA, иначе может установиться активная конфигурация с петлями.
- Версия протокола STP (Protocol Version Identifier) – 1 байт.
- Тип BPDU (BPDU Type) - 1 байт. Существует два типа BPDU - конфигурационный BPDU, то есть заявка на возможность стать корневым мостом, на основании которой происходит определение активной конфигурации, и BPDU уведомления о реконфигурации, которое посылается устройством, обнаружившим событие, требующее проведения реконфигурации - отказ линии связи, отказ порта, изменение приоритетов устройств или портов.

- Флаги (Flags) - 1 байт. Один бит содержит флаг изменения конфигурации, второй бит - флаг подтверждения изменения конфигурации.
- Идентификатор корневого моста (Root Identifier)- 8 байтов.
- Расстояние до корня (Root Path Cost)- 2 байта.
- Идентификатор моста (Bridge Identifier)- 8 байтов.
- Идентификатор порта (Port Identifier)- 2 байта.
- Время жизни сообщения (Message Age) - 2 байта. Измеряется в единицах по 0.5 с, служит для выявления устаревших сообщений. Когда пакет BPDU проходит через коммутатор, тот добавляет ко времени жизни пакета время его задержки данным коммутатором.
- Максимальное время жизни сообщения (Max. Age)- 2 байта. Если пакет BPDU имеет время жизни, превышающее максимальное, то он игнорируется коммутаторами.
- Интервал hello (Hello Time, время приветствия), через который посылаются пакеты BPDU.
- Задержка смены состояний (Forward Delay) - 2 байта. Минимальное время перехода портов коммутатора в активное состояние. Такая задержка необходима, чтобы исключить возможность временного возникновения альтернативных маршрутов при неодновременной смене состояний портов во время реконфигурации.
  Пакет BPDU уведомления о реконфигурации имеет следующие поля:
- Идентификатор версии протокола STA - 2 байта.
- Версия протокола STP – 1 байт.
- Тип BPDU - 1 байт с установленным флагом реконфигурации топологии.

Построение остового дерева

В качестве примера рассмотрим три DSLAM, подключенные с образованием петли (рисунок 8-2).

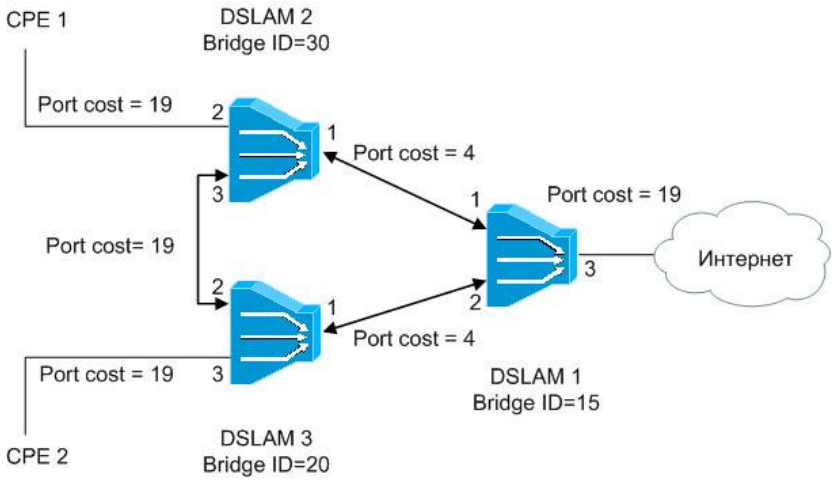


Рисунок 8-2. Перед применением протокола Spanning Tree.

После включения питания и загрузки каждый DSLAM начинает считать себя корневым мостом. Когда мультиплексор генерирует BPDU (через интервал *hello*), он помещает свой идентификатор в поле «идентификатор корневого моста» (Root Identifier), расстояние до корня (Root Path Cost) устанавливается в 0, а в качестве идентификатора порта (Port Identifier) указывается идентификатор того порта, через который будет передаваться BPDU.

Как только DSLAM получает BPDU, в котором имеется идентификатор корневого моста, меньше его собственного, он перестает генерировать свои собственные кадры BPDU, и начинает ретранслировать только кадры нового претендента на звание корневого моста. При ретрансляции кадров устройство наращивает расстояние до корня, указанное в пришедшем BPDU, на условное время сегмента, через который принят данный кадр.

В рассматриваемом примере корневым мостом становится DSLAM 1, т.к. имеет наименьший среди всех устройств идентификатор Bridge ID.

При ретрансляции кадров каждый DSLAM для каждого своего порта запоминает минимальное расстояние до корня. При завершении процедуры установления конфигурации покрывающего дерева, каждый мультиплексор находит свой корневой порт - это порт, который ближе других портов находится по отношению к корню дерева.

Рассмотрим выборы корневых портов DSLAM на примере рисунка 1.

Когда DSLAM 1 посылает BPDU, они содержат стоимость пути к корневому мосту (Root Path Cost) равную 0. Когда DSLAM 2 получает эти BPDU, он прибавляет стоимость пути порта 1 (Port cost = 4) к стоимости, указанной в полученном BPDU (0) и посылает BPDU со стоимостью пути к корню равной 4 через порт 3 и порт 2.

Когда DSLAM 3 получает BPDU от DSLAM 2, он увеличивает стоимость пути к корню до 23 (4 + 19). Однако DSLAM 3 также получает BPDU от корневого моста DSLAM 1 через порт 1. Стоимость пути к корню в этом BPDU равна 0 и DSLAM 3 увеличивает ее до 4 (Port cost его порта 1 равна 4). Теперь DSLAM 3 должен выбрать единственный корневой порт. Сравнивая расстояния до корневого моста портов 1 и 2 DSLAM 3 выбирает в качестве корневого порта порт1, так как его стоимость пути к корню меньше. После этого DSLAM 3 начинает объявлять стоимость пути до корня равную 4 нижележащим устройствам.

Выборы корневого порта DSLAM 2 происходят аналогично, и корневым портом для него становится порт 1 со стоимостью 4.

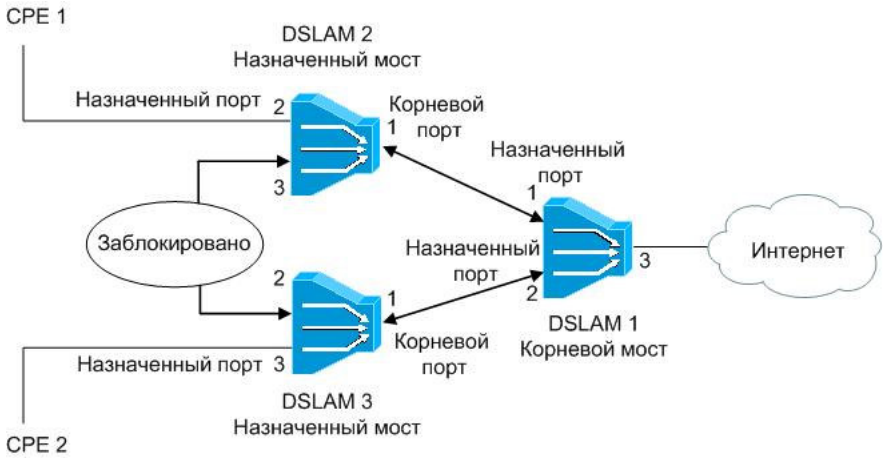


Рисунок 8-3. После применения протокола Spanning Tree.

Кроме этого, мультиплексоры выбирают для каждого сегмента сети назначенный порт. Для этого они исключают из рассмотрения свои корневые порты, а для всех оставшихся портов сравнивают принятые по ним минимальные расстояния до корня. Назначенный портом для каждого сегмента сети становится порт с наименьшим значением стоимости пути к корню (Root Path Cost). Когда имеется несколько портов с одинаковым кратчайшим расстоянием до корневого моста, то при выборе назначенного

порта сегмента протокол STP принимает решение на основе последовательного сравнения идентификаторов мостов (Bridge ID) и идентификаторов портов (Port ID).

Все порты, кроме назначенных переводятся в заблокированное состояние и на этом построение покрывающего дерева заканчивается.

Поскольку DSLAM 1 является корневым мостом, то все его порты являются назначенными.

В сегменте DSLAM 2 – DSLAM 3 порт 3 и порт 2 имеют одинаковую стоимость пути, равную 23. В этом случае STP выберет назначенный порт сегмента на основе сравнения идентификаторов мостов. Поскольку идентификатор DSLAM 3 (20) меньше идентификатора DSLAM 2 (30), то назначенным портом для этого сегмента станет порт 2 DSLAM 3. Порт 3 на DSLAM 2 будет заблокирован.

Состояния портов STP

В процессе построения топологии остового дерева сети каждый порт сетевого устройства проходит несколько стадий:

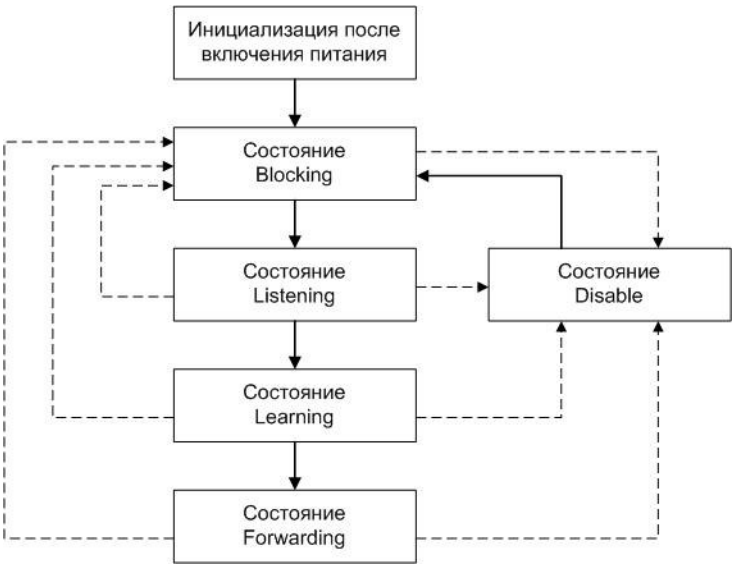


Рисунок 8-4. Состояния портов.

- **Blocking** – Заблокирован. Порт переходит в состояние Blocking сразу после процесса инициализации сетевого устройства или из состояния Disable. В этом состоянии порт не участвует в продвижении пакетов, тем самым предотвращая дублирование кадров возникающее из-за существования множества маршрутов между узлами коммутируемой сети. Кадры, принимаемые от подключенных сегментов или других портов сетевого устройства, будут отбрасываться. MAC-адреса конечных станций изучаться не будут. Порт принимает и обрабатывает только пакеты BPDU, требуемые алгоритмом STP для вычисления активной топологии.
  При истечении таймера протокола STP или получения конфигурационного сообщения (Configuration Message) порт перейдет в состояние Listening. При административном отключении порта он перейдет в состояние Disable.

- **Listening** – Прослушивание. В этом состоянии порт продолжает отбрасывать кадры данных. Изучение MAC-адресов запрещено, т.к. изменения активной топологии могут привести к занесению некорректной информации в таблицу MAC-адресов. Порт будет принимать, обрабатывать и ретранслировать только пакеты BPDU.

Из этого состояния порт может перейти в состояние Blocking, если получит BPDU с лучшими параметрами, чем его собственные (расстояние, идентификатор моста или порта) или в состояние Disable, при административном отключении. При истечении таймера смены состояний или получения конфигурационного сообщения порт перейдет в состояние Learning.

- **Learning** – Обучение. В этом состоянии порт готовится участвовать в процессе продвижения кадров. Пакеты данных от подключенных сегментов и других портов устройства все еще отбрасываются. Изучение MAC-адресов конечных станций разрешено, и адресная информация узлов заносится в таблицу MAC-адресов. Порт продолжает принимать, обрабатывать и передавать пакеты BPDU.
  Из этого состояния порт может перейти в состояние Blocking, если получит BPDU с лучшими параметрами, чем его собственные или в состояние Disable, при административном отключении. При истечении таймера смены состояний или получения конфигурационного сообщения порт перейдет в состояние Forwarding.

- **Forwarding** – Продвижение. В этом состоянии порт принимает и передает пакеты данных и продолжает строить таблицу MAC-адресов. Также продолжают приниматься, передаваться и обрабатываться пакеты BPDU.
  Из этого состояния порт может перейти в состояние Blocking, если получит BPDU с лучшими параметрами, чем его собственные или в состояние Disable, при административном отключении.

- **Disable** – Отключен. В состояние Disable порт может перейти из любого состояния при его административном отключении. Отключенный порт не участвует ни в работе протокола STP, ни в продвижении пакетов данных. После включения порт перейдет в состояние Blocking.

В процессе нормальной работы корневой мост продолжает генерировать служебные пакеты BPDU, а остальные устройства продолжают их принимать своими корневыми портами и ретранслировать назначенными. Если по истечении максимального времени жизни сообщения (по умолчанию — 20 с) корневой порт любого моста сети не получит служебный пакет BPDU, то он инициализирует новую процедуру построения связующего дерева.

Таймеры протокола STP

Таблица 2 описывает таймеры протокола STP, которые влияют на его производительность.

Таблица 8-2. Таймеры протокола STP

Таймер	Описание
Hello Timer	Этот таймер определяет интервал между пересылками сетевым устройством hello- пакетов другим сетевым устройствам.
Forward Delay Timer	Этот таймер определяет время пребывания порта в состояниях Listening и Learning перед тем как перейти в состояния Learning и Forwarding соответственно.
Maximum Age Timer	Определяет время, в течение которого информация протокола, полученная портом, хранится сетевым устройством.

8.2.Настройка протокола STP на DAS-3248.

Команды глобальной настройки STP на DAS-3248

Команды системы:

modify stp info

Описание: Настройка глобальных параметров STP протокола
Синтаксис команды: modify stp info [priority priority-value] [maxage maximum-age] [htime hello-time] [fdelay forward-delay] [enable|disable]

get stp info

Описание: Просмотр глобальных настроек STP протокола на DAS-3248
Синтаксис команды: get stp info

reset stp stats

Описание: Сброс счетчиков STP статистики
Синтаксис команды: reset stp stats

Таблица параметров:

priority priority-value	Приоритет устройства в STP (8 бит идентификатора Bridge ID, доступная для изменения пользователем). **Использование:** Get – Опционально. Modify – Обязательно. **Принимает значения:** 1..65535
maxage maximum-age	Максимальное время (в секундах), в течение которого информация протокола STP, полученная любым портом, хранится сетевым устройством. **Использование:** Modify – Опционально. Get – Опционально
htime hello-time	Максимальные время (в секундах), через которое любой порт, использующий протокол STP должен послать уведомления другим сетевым устройствам. **Использование:** Modify- Опционально. Modify – Опционально.
fdelay forward-delay	Максимальное время (в секундах), после которого любой порт переходит состояние продвижения пакетов (Forwarding).

	Использование: Modify - Опционально. Get – Опционально.
enable|disable	Глобальное включение протокола STP

Пример команды: $ modify stp info priority 0x20 maxage 25 htime 5 fdelay 20 enable
По умолчанию, протокол STP выключен.

Команды настройки протола STP на отдельных Bridge портах.

Команды системы:

modify stp port

Описание: Конфигурирование настроек STP на отдельном порту
Синтаксис команды: modify stp port info portid portid [enable|disable] [pcost pcost] [priority priority] [pktpriority pktpriority]

get stp port
Описание: Просмотр настроек STP на отдельном порту
Синтаксис команды: get stp port info portid portid

reset stp port
Описание: Сброс счетчиков STP
Синтаксис команды: reset stp port info portid portid

Таблица параметров:

portid portid	Номер Bridge интерфейса, на котором производится настройка STP **Использование:** Get – Опционально. Modify – Обязательно. **Принимает значения:** 1..386
Enable/disable	Включение протокола STP на отдельном Bridge интерфейсе. **Использование:** Modify – Опционально.
pcost pcost	Path Cost (стоимость) порта . **Использование:** Modify – Опционально.
priority priority	Приоритет порта в STP (6 битная часть Port ID, доступная для изменения пользователем). **Использование**: Modify – Опционально.
pktpriority pktpriority	Для STP PDU этот приоритет используется в случае выбора очереди пакетов на входящем или исходящем интерфейсе. В случае, когда Bridge интерфейс создан

	поверх ATM PVC интерфейса, этот приоритет также используется для идентификации PVC, с которого пакет был послан. **Использование:** Modify – Опционально.

Пример команды: **$ modify stp port portid 1 disable pcost 1000 priority 0x10**

Экранный вывод:

```
Port ID : 1 Priority : 0x0

State : Forwarding PortStatus : Enable
Path Cost : 100 Desig Cost : 0
Desig Root:80:00:00:10:5A:6C Desig Bridge:80:00:00:10:5A:6C
Desig Port : 0x8000 Fwd Transitions : 1
STP Status : Enable
Set Done
Port ID : 1 Priority : 0x0
State : Forwarding PortStatus : Enable
Path Cost : 100 Desig Cost : 0
Desig Root:80:00:00:10:5A:6C Desig Bridge:80:00:00:10:5A:6C
Desig Port : 0x8000 Fwd Transitions : 1
STP Status : Enable STP PacketsPrio : 2
```

9.Настройка пакетных фильтров

DAS-3248 обладает широкими возможностями по фильтрации и маркированию пакетов. Данный функционал достигается путем использования двух технологий: Generic Filter и Access Control Lists. Ниже будут рассмотрены особенности функционирования данных технологий и приведены примеры настройки.

9.1.Generic Filter

Generic Filter является абстрактным уровнем над интерфейсом-классификатором и покрывает поля наиболее часто используемых протоколов в заголовках пакетов, что открывает широкие возможности по фильтрации и обеспечению QoS. В отличие от деревьев классификатора, generic фильтры могут быть применены как на входящие, так и на исходящие интерфейсы с некоторыми ограничениями. Порядок обработки пакетов для входящих и исходящих интерфейсов с помощью Generic Filter показан на рисунках 9-1 и 9-2

Generic Filter является удобной в использовании абстракцией и удовлетворяет большинству потребностей пользователя. Поддерживаются следующие уровни протоколов:

- Ethernet Layer
  - Source MAC address
  - Destination MAC address
  - EtherType
  - VLAN ID
  - Service VLANID (только для функции Q-in-Q).
  - Priority Tag
  - Service Priority Tag (только для функции Q-in-Q).
  - Destination Service Access Point (DSAP) 802.2 LLC кадра
  - Source Service Access Point (SSAP) 802.2 LLC кадра

- IP Layer
  - Destination IP Address
  - Source IP Address
  - IP Protocol Type
  - TOS

- TCP Layer
  - Destination Port
  - Source Port

- UDP Layer
  - Destination Port
  - Source Port

- ICMP Layer
  - ICMP Type
  - ICMP Code

- IGMP Layer
  - IGMP Type
  - IGMP Code
  - Group Address

- PPP Layer
  - PPP Protocol Type

- ARP Layer
  - Source MAC Address
  - Destination MAC Address
  - Source IP Address
  - Destination IP Address

Кроме этого Generic Filter может производить анализ пакетов по смещениям от начала заголовков Ethernet, PPP, PPPoE, IP, TCP, UDP, IGMP, ICMP.

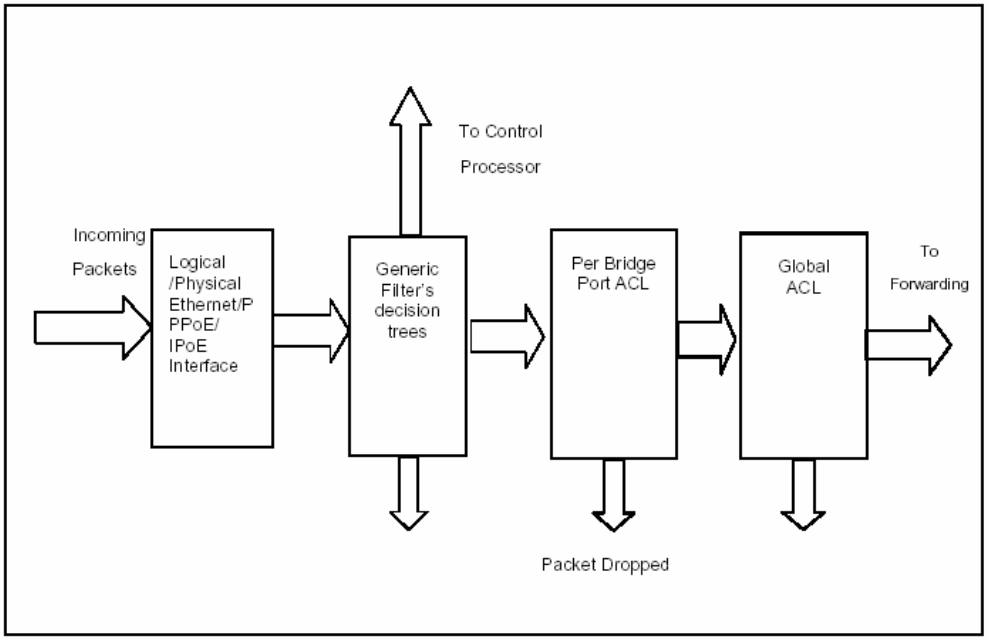


Рисунок 9-1: Порядок применения Generic Filter на входящих интерфейсах

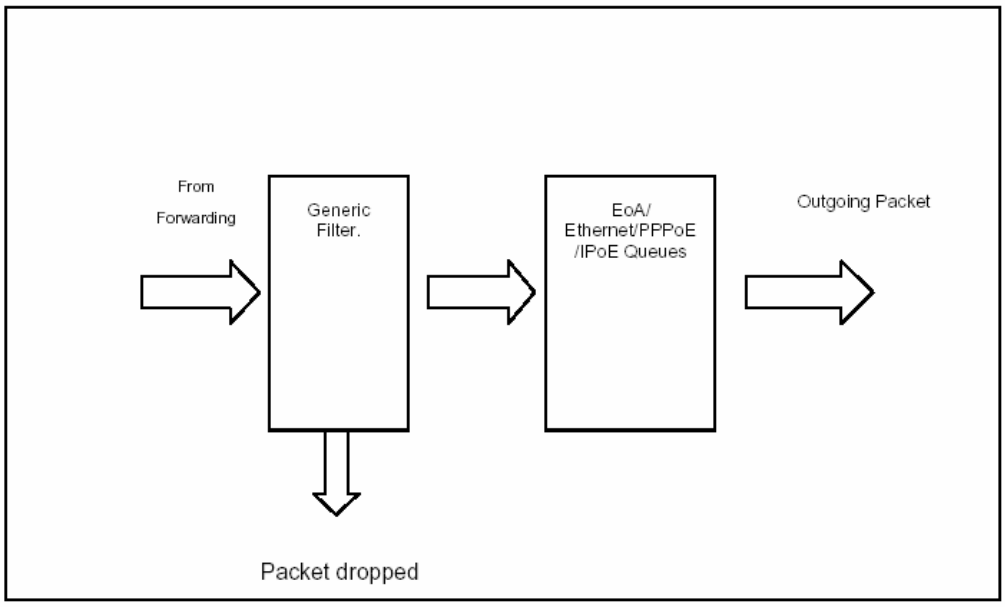


Рисунок 9-2: Порядок применения Generic Filter на исходящих интерфейсах

9.1.1.Общие принципы

9.1.1.1.Generic Filter Rule

Правило – это набор подправил, используемых для классификации пакетов. Правило может быть применено к одному или нескольким интерфейсам (eth-xx, eoa-xx).

К данному интерфейсу может быть применено одно или несколько правил Generic Filter. Во время привязки правила к интерфейсу необходимо указать OrderID. OrderID задает порядок выполнения правил в случае, если к одному и тому же интерфейсу применено несколько правил. Правила с меньшим OrderID будут выполнены раньше, чем те, что имеют больший OrderID. create filter rule map

Каждое правило имеет свой уникальный идентификатор RuleID.

OrderID привязывается к RuleID командой **create filter rule map**.

После того, как найден пакет, соответствующий какому-либо правилу, к пакету может быть применено одно из следующих действий (устанавливается командой **create filter rule actionmap**):

- **Forward exit (forwardexit):** передать пакет в выходную очередь. Игнорировать все последующие этапы. Этапы обработки пакетов будут описаны ниже в данном документе.
- **Allow:** пакет прошел данный этап обработки и будет передан первому правилу следующего этапа на данном интерфейсе.
- **Drop:** отбросить пакет
- **Go To Next Rule (gonextrule):** передать пакет следующему правилу данного интерфейса.
- **Set Output Priority (setprio):** установить внутренний приоритет для пакета который будет использоваться совместно с traffic class mapping table egress порта для определения выходной очереди для данного пакета.
- **Retag Priority (retagprio):** установить тег приоритета (802.1p) для выходящего пакета. Данное значение приоритета будет использоваться совместно с traffic class mapping table egress порта для определения выходной очереди для данного пакета.

- **Retag Service Priority (retaservicegprio):** установить тег приоритета (802.1p) для выходящего пакета Service VLAN (при использовании функции Q-in-Q).Данное значение приоритета будет использоваться совместно с traffic class mapping table egress порта для определения выходной очереди для данного пакета.
- **Packet VlanID (pktvlanid):** устанавливает тег 802.1q VLAN на выходящем из устройства пакете. Величина VLANID лежит в пределах 0-4094.
- **Retag VLANID (retagvlanid):** изменяет тег 802.1q VLAN на выходящем из устройства пакете. Величина VLANID лежит в пределах 0-4094.
- **Packet Service VlanID (pktvlanid):** устанавливает тег Service-VLAN на выходящем из устройства пакете (при использовании функции Q-in-Q). Величина VLANID лежит в пределах 0-4094.
- **Retag VLANID (retagvlanid):** изменяет тег Service-VLAN на выходящем из устройства пакете (при использовании функции Q-in-Q). Величина VLANID лежит в пределах 0-4094.
- **Rate Limiter (ratelimiter)**: Используется для того, чтобы выделить пакеты для последующего ограничения скорости их передачи (Flow based Rate Limiting) .Более подробно смотрите Главу 10.
- **Modify TOS (modifytos)**. Модифицирует поле TOS в заголовке IP пакетов. Имеет аргументами новую величину TOS и битовую маску. Новая Величина TOS может лежать в пределах 0-255.Маска позволяет изменять поле TOS побитово. Более подробно смотрите в Главу 10 (пункт 10.2.3.3).
- **Set BAC Level (setbaclevel**).Включает или выключает функцию Buffer Admission Control, которая используется для контроля перегрузки выходных очередей устройства. Принимает величины 0 или 1. Пороговая величина заполненности очереди, при которой срабатывает BAC, устанавливается для каждого класса трафика (очереди) отдельно через Traffic Class Parameters Table.
- **Send to Control (sendtocontrol)**: Посылает пакеты в ControlPlane для обработки приложениями, зарегистрированными в нем. Имеет аргументом имя приложения (description). Подробнее концепцию обработки в Control Plane смотрите ниже в данной главе.
- **Copy to Control (copytocontrol):** Посылает копию пакетов в ControlPlane, при этом пакеты могут форвардится дальше.Имеет аргументом имя приложения получателя пакетов, зарегистрированного в Control Plane (description). Подробнее концепцию обработки в Control Plane смотрите ниже в данной главе.
- **Expression Defined (expdef):** Данное действие означает применение определенного действия по результатам логического выражения над подправилами. Имеет аргументом ID логического выражения (ExpID).Логическое выражение – выражение, имеющее уникальный ExpID и отражающее срабатывание правила в результате определенной логической комбинации истинности или ложности подправил. Например, выражение (1|(2&3)):drop означает отбрасывание пакетов (действие Drop правила) в случае, когда 1 подправило истинно, либо 2 и 3 подправило одновременно истинны. Подробнее концепцию обработки логических выражений смотрите ниже в данной главе (пункт 9.1.5)

ЗАМЕЧАНИЕ: каждое правило может иметь несколько действий в добавлении к тому, которое указано как часть правила. Концепция нескольких действий для одного правила будет описана далее в этом документе.

Кроме RuleID правило может иметь еще ряд дополнительных параметров (устанавливаются командой **create filter rule entry**):

- Направление правила (параметр **ruledir**). In – для входящих интерфейсов Out– для исходящих интерфейсов.
  Максимальное количество правил типа In=275, типа Out=25.
- Приоритет правила (параметр **ruleprio)**.Данный приоритет определяет тип памяти, которая будет использована для хранения правила. DAS-3248 поддерживает следующие приоритеты:
  - High: высокоскоростная память
  - Low: низкоскоростная память

  Правила, ожидаемая частота срабатывания которых велика, должны создаваться как High priority.
- Признак динамической (условной) обработки правила – параметр **ApplyWhenReq enable/disable**. Если данный параметр выключен (значение по умолчанию), то правило вступает в работу сразу после его включения. Если параметр находится в состоянии enable, то правило неэффективно на интерфейсе до тех пор, пока корреспондирующее приложение не зарегистрирует его на интерфейсе. Приложение может также дерегистрировать правило на интерфейсе, и тогда оно снова становится неэффективным. Регистрация и дерегистрация правил производится через пакетный фильтр, используя описание правила (description) данное ему при создании.
- Признак необходимости сбора статистики срабатывания правила – параметр **statstatus enable/disable.**
- Признак выбора типа пакетов (параметр **pkttype Bcast/Mcast/Ucast**). Позволяет выбрать тип передачи пакетов, на который будет распространяться правило (действителен только для исходящих правил).
- Уровень прослушивания (параметр **snooplevel interface/bridge**). Действителен только для действий SendtoControl и Copytocontrol. Позволяет установить, производится ли пересылка пакетов в ControlPlane со входящего интерфейса или после применения bridging функционала, что позволяет произвести с ними определенные типы фильтрации и преобразований до попадания пакетов в Generic Filter (например, Ingress Vlan filtering) (параметр может изменяться только при выключенном правиле).

9.1.1.2.Generic Filter Subrule

Подправило определяет поле пакета, которое будет использоваться при фильтрации. DAS-3248 поддерживает следующие типы подправил:

- ARP
- Ethernet
- IP
- PPP
- TCP
- UDP
- ICMP
- IGMP
- Generic (на основе смещений)
- Context (основывается не на полях пакета, а на свойствах пакета). Применяется только для функции Q-in-Q для режима VLAN Trunk (E-line).

Существуют следующие типы операций сравнения, поддерживаемых в правилах:

- Equal (равно)

- Not equal (не равно)
- Less than (меньше, чем)
- Less than equal (меньше или равно)
- Greater than (больше чем)
- Greater than equal (больше или равно)
- In range (находится в интервале)
- Ex range (находится вне интервала)
- In Generic List (используется только для Generic подправил и адресов IP source и IP destination IP подправила)
- Not In Generic List (используется только для Generic подправил и адресов IP source и IP destination IP подправила)
- In Named List (только для Generic подправила)
- Not In Named List (только для Generic подправила)

Во время создания подправила пользователь может задать его приоритет. Данный приоритет определяет тип памяти, которая будет использоваться для хранения данного подправила. DAS-3248 поддерживает следующие приоритеты:

- High: высокоскоростная память
- Low: низкоскоростная память
- As in Rule: использовать настройки родительского правила

Рекомендуется для часто срабатывающих правил использовать высокий приоритет. По умолчанию в системе можно создать максимально **75 подправил High Proirity** и **425 подправил Low Priority** для правил типа **ruledir=In** и **25 подправил High Proirity** и **175 подправил Low Priority** для правил типа **ruledir=Out.**

Для подправил третьего уровня и выше (IP, TCP, UDP, ICMP и IGMP) пользователь может указать тип протокола второго уровня: Ethernet или PPPoE.

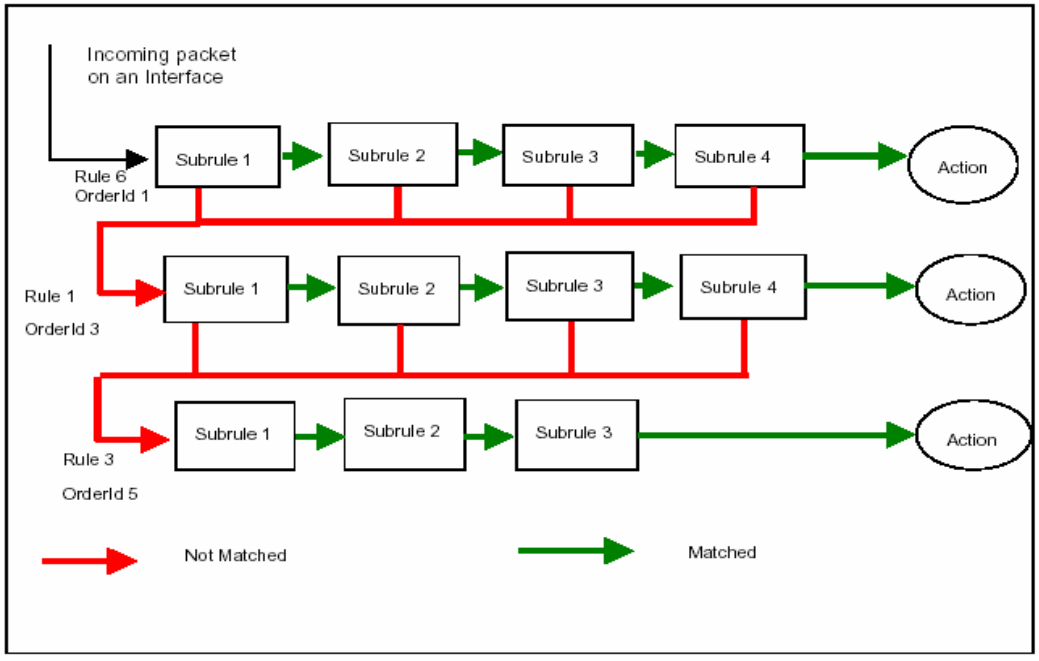


Рисунок 9-3: Порядок исполнения правил и подправил

9.1.1.3.Порядок действий при создании правила Generic Filter

- Создать правило generic фильтра (**create filter rule**)
- Добавить одно или несколько подправил фильрации нужного типа пакетов (IP,UDP,PPP,ARP и.т.д.) к правилу (**create filter subrule**)
- Включить правило (**modify filter rule entry ruleid x status enable**
- Применить правило к интерфейсу/ интерфейсам (**create filter rule map ifname xxx).** Правило может привязываться одной командой как к одному интерфейсу (по выбору пользователя), так и ко всем однотипным интерфейсам (**all-** все интерфейсы, **alleoa**- все интерфейсы EoA,**alleth-** все интерфейсы ethernet, **allpppoe** –все интерфейсы pppoe).

9.1.2.Многоэтапная обработка пакетов

Иногда возникает необходимость осуществлять фильтрацию в несколько этапов. Например, первый этап может использоваться для отбрасывания неавторизованных пакетов, а на втором этапе может осуществляться приоритезация. Для того чтобы удовлетворять этим требованиям, фильтрация и приоритезация пакетов в DAS-3248 может быть разделена на несколько этапов. Этап, во время которого будет работать данное правило, определяется во время его приложения к конкретному интерфейсу.

Этапы выполняются согласно их StageID. Т.е. правила меньших этапов будут выполнены перед правилами этапов с большим значением StageID.

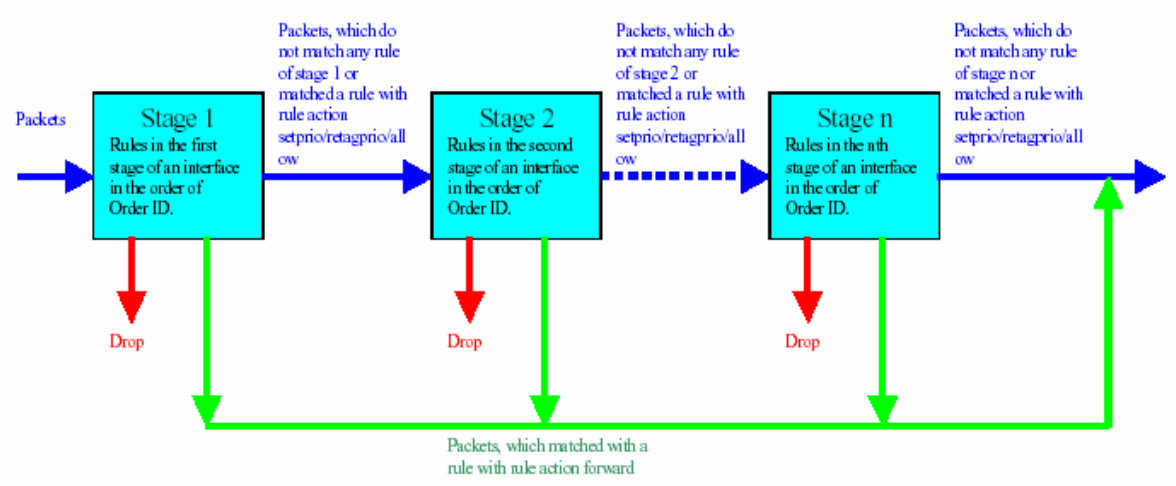


Рисунок 9-4: Многоэтапность обработки пакетов.

Пакет не будет передан на следующий этап если:

- на текущем этапе пакет соответствует правилу с действием Drop. В этом случае пакет будет отброшен, никаких правил к нему больше применяться не будет.

Пакет будет передан на следующий этап если:

- если текущий этап является последним, пакет будет поставлен в исходящую очередь
- пакет не совпал ни с одним из правил на текущем этапе
- пакет совпал с правилом allow. В этом случае к данному пакету на текущем этапе больше ни одного правила применено не будет.
- пакет совпал с правилом setprio или retagprio. В этом случае к данному пакету на текущем этапе больше ни одного правила применено не будет.

Максимальное число этапов во входящем и выходящем направлениях может быть различно.

9.1.3.Несколько действий одного правила (Action Map)

В DAS-3248 одно и то же правило может иметь несколько действий (allow, setprio, etc). Все эти действия будут выполнены в случае соответствия пакета данному правилу. Это очень полезно, если над некоторым типом пакетов нужно произвести сразу несколько действий. Дополнительные действия ассоциируются с правилом уже после того, как оно создано. Каждое действие имеет свой orderindex, который определяет порядок выполнения всех действий, ассоциированных с правилом.

Причем:

- в первую очередь выполняются действия из action map в порядке возрастания их Order Index
- после этого выполняется действие, указанное при создании правила

Итак, для того, чтобы ассоциировать несколько действий с одним правилом нужно:

1. Создать правило Generic Filter
2. Создать соответствие действия правилу (rule to action map) для данного правила Generic фильтра:

create filter rule actionmap ruleid 1 orderindex 1 action copytocontrol
create filter rule actionmap ruleid 1 orderindex 2 action retagprio priority 2

3. Создать подправила данного правила
4. Включить правило
5. Приложить правило на интерфейс

9.1.4.Быстрое изменение последовательности правил

Пользователь DAS-3248 может заменить последовательность выполнения правил одного этапа путем выполнения всего одной команды. То же самое можно получить путем изменения значений OrderId всех правил. Однако в этом случае, в процессе изменения порядка следования правил, возможно, появление ошибочной их последовательности, которая может повлечь нарушения в работе сети. Для того чтобы этого избежать, в DAS-3248 пользователь может заменить целиком одну последовательность применения правил другой последовательностью.

Generic Filter Sequence – последовательность выполнения правил. Логически она состоит из Generic Filter Sequence Information (задает идентификатор данной последовательности) и Generic Filter Sequence entries (набор правил данной последовательности).

Для примера рассмотрим следующую ситуацию:

Пусть к интерфейсу eoa-2 приложены следующие правила во входящем направлении:

ruleid 1 Orderid 1

ruleid 3 Orderid 2
ruleid 5 Orderid 3
ruleid 6 Orderid 4

Требуется сменить данную последовательность на:

ruleid 5 Orderid 1
ruleid 2 Orderid 2
ruleid 7 Orderid 3

Для того чтобы сменить последовательность надо:

1. Создать sequence information путем задания sequence ID

   create filter seq info seqid 1

2. Создать членов искомой последовательности

   create filter seq entry seqid 1 ruleid 2 orderid 2
   create filter seq entry seqid 1 ruleid 5 orderid 1
   create filter seq entry seqid 1 ruleid 7 orderid 3

3. Применить получившуюся последовательность

   modify filter seq entry seqid 1 ifname eoa-2 stageid 1 seqdir in

9.1.5.Обработка логических выражений.

В стандартном правиле все подправила как бы объединены оператором AND ,то есть только при соблюдении всех подправил (признаков) правило сработает. Но данное ограничение можно легко обойти, применяя логические выражения.
Логическое выражение – строка, определяющая отношения между подправилами (Subrule) в правиле (Rule). Логическое выражение состоит из нескольких составляющих:

- ID подправила (Subrule ID)
- Логических операторов (OR/AND/NOT)
- Действия правила (Action), отделяемого от комбинации логических операндов и Subrule ID двоеточием «:»

Каждое определенное выражение должно быть закреплено своим ExpID .
Например: $create filter expr entry exprid 1 exprstring “(1|2): drop”
Данное выражение означает, что правило основанное на этом логическом выражении сработает (то есть пакет будет отброшен), если будет истинно хотя бы одно из подправил (пакет удовлетворит хотя бы одному из двух выбранных признаков).
Определенное один раз ExpID может применено к правилам с помощью действия **exprdef** ко многим правилам.
Например: $create filter rule entry ruleid 1 action exprdef exprid 1
Количество ExpID в системе ограничено и должно быть меньше 256.
Одно и тоже Subrule ID может повторяться в логическом выражении многократно. Так, например, логическое выражение (1&2)|(2&3) является корректным, и означает, что правило сработает при одновременном удовлетворении пакетом признаков, указанных в подправилах 1 и 2 или 2 и 3.
Применяемые к логическому выражению могут действия (Action) могут любые из перечисленных выше для входящих правил и любые, кроме ratelimiter для исходящих правил.

В случае применения неправильного действия (не совместимого направлением правила) при попытке включения его устройство будет выдавать ошибку.
Действия не могут быть соотнесены с частью логического выражения. Таким образом, выражения “(1 | 2 : drop)” и “(1| (2 & 3):drop): allow” являются неправильным, тогда как правильными являются выражения “(1 | (2 & 3)) “ и “(1 & 2): modifytos actionval 0xff actionmask 0xff”.
К логическому выражению могут быть применены многочисленные действия (до 4 действий одновременно), при этом Action Map не используется, а действия перечисляются через запятую “,”
В случае применения многочисленных действий, последующие действия не могут быть применены после терминирующих действий (drop, allow, gotonextrule, forwardexit and sendtocontrol).
В случае применения многогочисленных действий, включающих Sendtocontrol и Copytocontrol, в выражениях может присутствовать только одно описание приложения, зарегистрированного в Control Plane, и его имя обязательно должно присутствовать в правиле (параметр description). Подробнее смотрите ниже пункт 9.1.7.
Примеры логических выражений:

- Subrule1 OR Subrule 2) AND (subrule 3 OR subrule 4). Пропустить пакет (Allow) **“((1 | 2) & (3 | 4)): allow”**.

- (Subrule1 AND Subrule2) OR (subrule3 AND (subrule4 OR subrule5)). Переопределить приоритет пакета (retagprio 2) и пропустить. **“((1 & 2) | (3 & (4 | 5))): retagprio 2”**

- Subrule1 AND (Subrule2 OR NOT Subrule3). Отбросить пакет (Drop). **“(1 & (2 | (!(3)))): drop”**

9.1.6. Обработка пакетов в Control Plane.

Некоторые типы обработки данных, такие как IGMP Snooping, не могут быть осуществлены только с помощью интерфейса пользователя и DataPlane, а обязательно с участием ядра внутренней ОС DAS-3248 ControlPlane.

Процессы которые хотят осуществить обработку данных в ControlPlane, называются пользовательскими приложениями по отношению к ControlPlane.
Кроме пользовательских приложений и непосредственно самого ControlPlane в передаче данных ControlPlane участвует пакетный фильтр (Packet Filter).

Packet Filter представляет собой абстрактный уровень, который используется, чтобы зарегистрировать приложения, которые могут посылать данные в Control Plane, используя действия SendtoControl и CopytoControl правил Generic filter, а также для возвращения обработанных данных обратно.
Регистрация пользовательских приложений осуществляется по имени приложения (description), указанному в параметрах действий SendtoControl и CopytoControl правил Generic filter.
Например: В случае, если производится классификация и обработка пакетов протокола IGMP, правило должно иметь описание IGMP.

Примечание: Приложения по умолчанию (например Snooping), уже зарегистрированы в системе соответствующим правилом по умолчанию, но в данном пункте мы разбираем концепцию применения действий с ControlPlane.

Пользователь может также определить для действий SendtoControl и CopytoControl должны ли пакеты поступать на Control Plane на уровне входного интерфейса или после осуществления Bridging функционала.

Осуществление правил с ControlPlane не мешает работе других правил Generic Filter.

Кроме имени пользовательского приложения действия с ControlPlane могут иметь следующие параметры:

- Traps enabled/disabled.
  Раньше, все пакеты потоков, которые помечены действием sendtocontrol и copytocontrol передавались в ControlPlane зарегистрированным в них приложениям. Эта схема обработки потока имела две проблемы:
  - На обработке этих пакетов значительно терялась мощность системы (в том числе процессора);
  - ControlPlane и DataPlane очереди могли быть переполнены пакетами единственного потока. Большой поток этих пакетов мог вызывать отказ в обслуживании пакетов другого типа, также приходящих для обработки в ControlPlane, что являлось особенно серьезным, если данный поток представлял собой атаку (злонамеренно сформированный поток).
  Для того чтобы решить эти проблемы, был введен новый параметр trap level для действий sendtocontrol и copytocontrol. Эта ловушка работает следующим образом:
  - Если Traps disabled, то все пакеты из потоков с действиями sendtocontrol и copytocontrol передаются ControlPlane.
- Если Traps enabled, только по одному пакету из потоков с действиями sendtocontrol и copytocontrol передаются ControlPlane. Остальные пакеты передаются вызывающему приложению только тогда, когда процесс показывает свою готовность к получению новых пакетов через запрос к ControlPlane через пакетный фильтр. Если приложение пока не готово к получению новых данных, пакеты или молча отбрасываются (в случае sendtocontrol действия) или обрабатываются отдельно (в случае copytocontrol действия).
- Control Flow ID . Идентификатор потока. Все потоки в Control Plane попадают в одну и туже очередь с дисциплиной DP-SP. Это сильно затрудняет проведение приоритезации потоков в Control Plane.Для решения этой проблемы и дифференции потоков данных с действиями SendtoControl и CopytoControl проблемы был введен параметр Control flow ID

Применение действия SendtoControl на примере IGMP Snooping:
В этом примере, мы проиллюстрируем, используя команды CLI правила Generic Filter классификацию пакетов протокола IGMPv2.

Данная задача включает в себя 3 этапа:
1. Создание правила классификации для IGMP пакетов. На основании действия этого правила классифицированные пакеты протокола IGMP будут посылаться для обработки в ControlPlane.
2. Прикрепить правило к интерфейсу.
3. Зарегистрировать приложение в Packet Filter для приема пакетов.

1.Создать правило
$create filter rule entry ruleid 1 action sendtocontrol description “IGMP”
Создать подправило для выделения пакетов с типом протокола IGMP в заголовке IP пакета
$create filter subrule ip ruleid 1 subruleid 1 prototypefrom 2 prototypecmp eq
Включить правило
$modify filter rule entry ruleid 1 status enable
2. Прикрепить правило к интерфейсу.
$create filter rule map ifname eoa-0 stage 1 ruleid 1 orderid 1
3.Зарегистрировать пользовательское приложение, используя Packet Filter, для приема пакетов из ControlPlane.
$igmpsnoop cfg info status enable
$igmpsnoop port info portid 1 status enable

9.1.7. Расширенные принципы фильтрации. Generic List и Named List.

9.1.6.1. Generic List.

Generic List позволяет пользователю определить список (list) 32-битных целочисленных параметров для интерфейсов EoA, Ethernet, PPPoE и IPoE. Этот список будет использован для сравнения с полем в пакете данных.
Основное назначение Generic List: используя его, пользователь может легко реализовать IP Access Control List. В этом случае, список используется как IP адрес или набор IP адресов, пакеты которых должны быть отброшены или пропущены. Generic list может быть использован, наряду с Generic Filter правилами при фильтрации пакетов IP и ARP протокола.
Примечание: Величины параметров Generic List должны быть указаны в шестнадцатеричном виде (например,0x12345678).Для перевода IP адреса в вид, необходимый для представления в DAS-3248, преобразуйте каждый октет IP адреса в шестнадцатиричный вид и запишите полученое число без разделителей (точек). Например, 0x12345678 соответствует IP адресу 18.52.86.120.
Пример. Создать Generic List
$create filter list genentry ifname eoa-0 value 0x12345678

9.1.6.1. Named List.

Named List отличается от Generic List тем, что он не ассоциируется с одним конкретным интерфейсом, а идентифицируется ListID, и, таким образом, может быть применен к различным типам интерфейсов. Named List может иметь дискретные параметры или диапазонные параметры. Named List может быть ассоциирован с Generic Filter правилом (в этом случае Named list используется в правиле Generic Filter с действием (Action) «Match in Named List»), или может быть использован для создания Generic List путем применения к интерфейсу. Named List может иметь до 8 записей entry (параметров).

Пример:
1. Создать Named List
$create filter namedlist info listid 1 listtype discrete
2. Создать дискретную запись в Named List
$create filter namedlist genentry listid 1 value 0x1234567
2. Создать диапазонную запись в Named List

$create filter namedlist genentry listid 1 value 0x12345678 valueto 0x56781234
4. Применить Named List к интерфейсу.
$create filter namedlist map ifname eoa-0 listid 1

9.1.8.Примеры использования Generic Filter

Пример 1:Фильтр для запрета icmp echo (type 8 code 0) сообщений на определенном интерфейсе (eoa-x, eth-x)

$create filter rule entry ruleid 2 action drop ruleprio high

Создаем главное правило:
action drop - отбрасывать
ruleprio high - правило будет загружаться в высокоприоритетную память (рекомендуется для "часто срабатывающих" правил)

$create filter subrule icmp ruleid 2 subruleid 1 icmptype 8 icmptypecmp eq subruleprio asinrule

Создаем подправило, в котором указываем, что же все-таки фильтровать:
ruleid 2 subruleid 1 - первое подправило второго правила
icmptype 8 icmptypecmp eq - все icmp type 8 пакеты
subruleprio asinrule - приоритет подправила такой же, как у правила

$create filter rule map ifname eoa-23 stageid 1 ruleid 2

Применяем правило к конкретному интерфейсу (eoa-xx, eth-x)

$modify filter rule entry ruleid 2 status enable

Включаем фильтр в работу

Примечание: Другие примеры использования Generic Filter приведены в Приложении С настоящего руководства.

9.2. Access Control List в DAS-3248

Access Control List позволяет задать пользователю список MAC адресов, которым будет разрешен или наоборот запрещен доступ. Данные списки могут быть созданы для каждого bridge порта в отдельности или для всего DSLAM-а в целом.

- Per port ACL: данный список создается для конкретного bridge порта. MAC адресам, указанным в этом списке, доступ разрешен.
- Global ACL: данный список создается целиком для устройства. Если выбрана опция Deny, MAC адресам, находящимся в этом списке доступ запрещен.

Per Port ACL

- Создается для конкретного bridge порта
- Все входящие пакеты, у которых source MAC адрес совпадает с одним из адресов, перечисленных в списке, имеют доступ к данному bridge порту. Все остальные входящие пакеты доступа к данному bridge порту не имеют, т.е. отбрасываются.
- Если список MAC адресов пуст, любые адреса имеют доступ на данный Bridge порт.
- Только unicast MAC адреса могут быть добавлены в список.

Global ACL

- Создается на глобальном уровне (целиком на DAS-3248)
- Всем пакетам, имеющим source MAC адрес, совпадающий с одним из адресов, перечисленных в списке, может быть запрещен доступ путем выбора опции Deny.
- Данный список может быть использован для отслеживания содержащихся в нем MAC адресов. В этом случае при перемещении MAC адреса на другой порт будет сгенерирован SNMP Trap.
- Только unicast MAC адреса могут быть добавлены в список.

Замечание: ACL применяется после классификаторов и правил Generic Filter.

9.2.1.Примеры использования Global ACL

- Добавление MAC адреса в глобальный список MAC адресов и включение опции deny:

  create acl global macentry macaddr 00:11:95:90:26:46 deny enable

- Добавление MAC адреса в глобальный список MAC адресов и включение опции слежения:

  create acl global macentry macaddr 00:11:95:90:26:46 track enable

- Добавление MAC адреса в глобальный список MAC адресов и включение обеих опций deny и слежения:

  create acl global macentry macaddr 00:11:95:90:26:46 deny enable track enable

- Создание bridge порта с включенными опциями Global ACL (по умолчанию данные опции включены)

  create bridge port intf ifname eoa-0 portid 1 aclGlbDenyApply enable aclGlobalTrackApply enable

Созданную запись в глобальном списке MAC адресов можно удалить командой:

delete acl global macentry macaddr xx:xx:xx:xx:xx:xx

например:

delete acl global macentry macaddr 00:11:95:90:26:46

9.2.2.Пример использования Per Port ACL

- Соответствующий bridge порт должен существовать до создания ACL
- Добавление MAC адреса в список для данного порта:

  create acl port macentry portid 2 macaddr 00:50:34:8D:AF:76:4A

10.Настройка QoS на DAS-3248

10.1.Теория качества обслуживания (QoS).

10.1.1.Современные требования к качеству обслуживаниия

Современные требования к качеству обслуживания (QoS):

- Система должна обеспечивать ограничение полосы пропускания (sustained rate), необходимой для доступа в Internet. Не разрешается выходить за рамки пропускной способности, определенные провайдером.
- Система должна предоставлять механизмы, позволяющие классифицировать трафик в различные потоки (голос, STB control, Video и Data) и расставлять приоритеты каждому потоку. Высокоприоритетные потоки должны иметь преимущество над менее приоритетными.
- Система должна поддерживать ограничение по доступной полосе пропускания для более, чем одного (макс. 4) потока.

Для того, чтобы предоставить пользователю полную гибкость в деле обеспечения egress приоритезации на основе очередей, когда он имеет полный контроль за тем, как он хочет чтобы вел себя алгоритм приоритезации, релиз 2.10 и выше программного обеспечения DSLAM DAS-3248 определяет новый настраиваемый алгоритм. Новый механизм приоритезации применим только для ATM очередей.

10.1.2.Дисциплины очередей.

Strict Priority (SP) Discipline

Strict Priority – дисциплина освобождения очередей, применяемая как для upstream, так и для downstream потоков. Данная дисциплина порождает полную остановку трафика низкоприоритетных очередей при высокой нагрузке высокоприоритетных

Для каждого цикла обслуживания во время обработки данного порта выходной планировщик проверяет процесс прихода пакетов в каждую очередь. Даже если в менее приоритетной очереди есть пакеты, ждущие обслуживания, первыми будут обслужены пакеты высокоприоритетных очередей. Результатом может стать переполнение низкоприоритетных очередей.
Дисциплина SP не ассоциирует пропускную способность с какой-либо конкретной очередью. Поэтому, данные, находящиеся в наиболее приоритетной очереди, имеют максимально доступную полосу пропускания.
SP профайл задает веса для всех очередей в виде максимальных значений (для DAS-3248 - 100). Т.е. для 4-х классов трафика (ATM интерфейс) SP профайл будет {100,100,100,100}

Значения SA профайла лежат в интервале от 1 до 100 для каждого класса трафика. Сетевой вес рассчитывается, исходя из процентного соотношения текущего веса по отношению к общему. Например:

- SA профайл {90,80,10,20} будет {45,40,5,10}
- SA профайл {10,20,30,40} будет {10,20,30,40}
- SA профайл {10,20,100,100} будет {33,66,100,100}

Замечание: последние два класса трафика будут иметь SP поведение. Это является истиной только в случае PP, но не в случае custom priority. Таким образом, это выполняется только в случае Ethernet интерфейса.

Probabilistic Priority (PP) Discipline

Probabilistic Priority – избегает полной остановки трафика путем улучшения существующей дисциплины SP. PP ставит в соответствие каждой очереди некий параметр, называемый весом. Согласно этим весам определяется процент пакетов (за длительный временной интервал), которые имеют право покинуть данную очередь. Данная дисциплина легко может быть превращена в SP путем соответствующего задания весов для каждой очереди. PP также получила название SP-SA (Strict priority with starvation avoidance)

Дисциплина PP ставит в соответствие атрибут bandwidth каждой очереди на порту. Результатом является разделение между всеми очередями всей доступной полосы пропускания. Доля доступной полосы из общего значения называется весом и лежит в интервале от 1 до 100.
Если у нас имеется n классов трафика, и каждому назначен приоритет w1, w2,…,wn, тогда каждый класс трафика получит:

$R(i) = \frac{w(i) * 100}{\sum w(i)}$, где i=1…n полосы пропускания

Обозначим n – число активных очередей на порт и m – число неактивных. В этом случае мы имеем незанятую свободными m очередями полосу пропускания, которая может быть использована теми очередями, которые содержат пакеты:

$O(i) = R(i) + \frac{\sum w(j)}{j}$ где j=1…m

Данное взвешенное распределение рассчитывается при каждом приходе в одну из очередей нового пакета, т.к. активность очередей – непрерывный процесс. **O(i) –** портовое взвешенное распределение для процесса прихода пакетов.
Управляемая, предрассчитанная случайная таблица весов используется во время распределения пропускной способности порта между очередями на основе их весов. Данная случайная таблица используется для рандомизации отправки пакетов среди очередей данного класса, для того чтобы пакеты из очереди данного класса не накапливались во время отправки.

Описание

Для каждого цикла обслуживания выполняются следующие шаги:

1. Во время планирования для данного порта выходной планировщик контролирует процесс прихода пакетов в каждую очередь.
2. После этого планировщик использует полученную информацию о процессе прихода пакетов для расчета взвешенного распределения (Port Weight Distribution) для каждого цикла прихода пакета.
3. Исходя из рассчитанного взвешенного распределения, рассчитывается вес наиболее приоритетной очереди, в которую пришел пакет (port-class-weight).

4. Затем происходит проверка текущего слота случайной таблицы весов на предмет того, может ли очередь данного класса быть обслужена на текущем шаге. Такая возможность определяется путем сравнения port-matching-weight с данным случайным весом – проверяется совпадение данного и случайного весов.

Например, если port-matching-weight равен 50 и текущий глобальный случайный вес больше или равен 50, то данная очередь подлежит обслуживанию.

- Если данная очередь подлежит обслуживанию, то первый пакет будет обслужен, а процесс расчета весов повторится, с учетом прихода новых пакетов.
- Если данная очередь не подлежит обслуживанию, тогда будет произведено сравнение веса следующей, более приоритетной очереди. Данный процесс будет повторяться до тех пор, пока не будет найдена очередь, подлежащая обслуживанию.

Замечание: случайная таблица обновляется в течение каждой итерации обслуживания.

Если какой-нибудь из port-matching-weight соответствует максимальному весу, тогда для данного класса дисциплина превращается в SP. Соответствующая очередь будет являться подлежащей обслуживанию пока в ней есть хотя бы один пакет. Остальные очереди получат полосу пропускания, равную их весам. Например, если веса 10, 20, 100, 70, то класс 3 получит (100-(10+20)) единиц полосы пропускания в SP, а класс 4 не будет обслужен вообще до тех пор, пока предыдущая очередь третьего класса содержит трафик.

Рисунок 10-1 иллюстрирует PP дисциплину.

Как показано на рисунке, 1, 0 и 1 в процессе прихода пакетов представляют активность или ее отсутствие в очереди. Таблица весов классов отражает распределение полосы пропускания в зависимости от активности очереди. Случайная таблица весов рассчитана для случайных весов в интервале от 1 до 100, принимая во внимание, что весовое значение используется более одного раза.

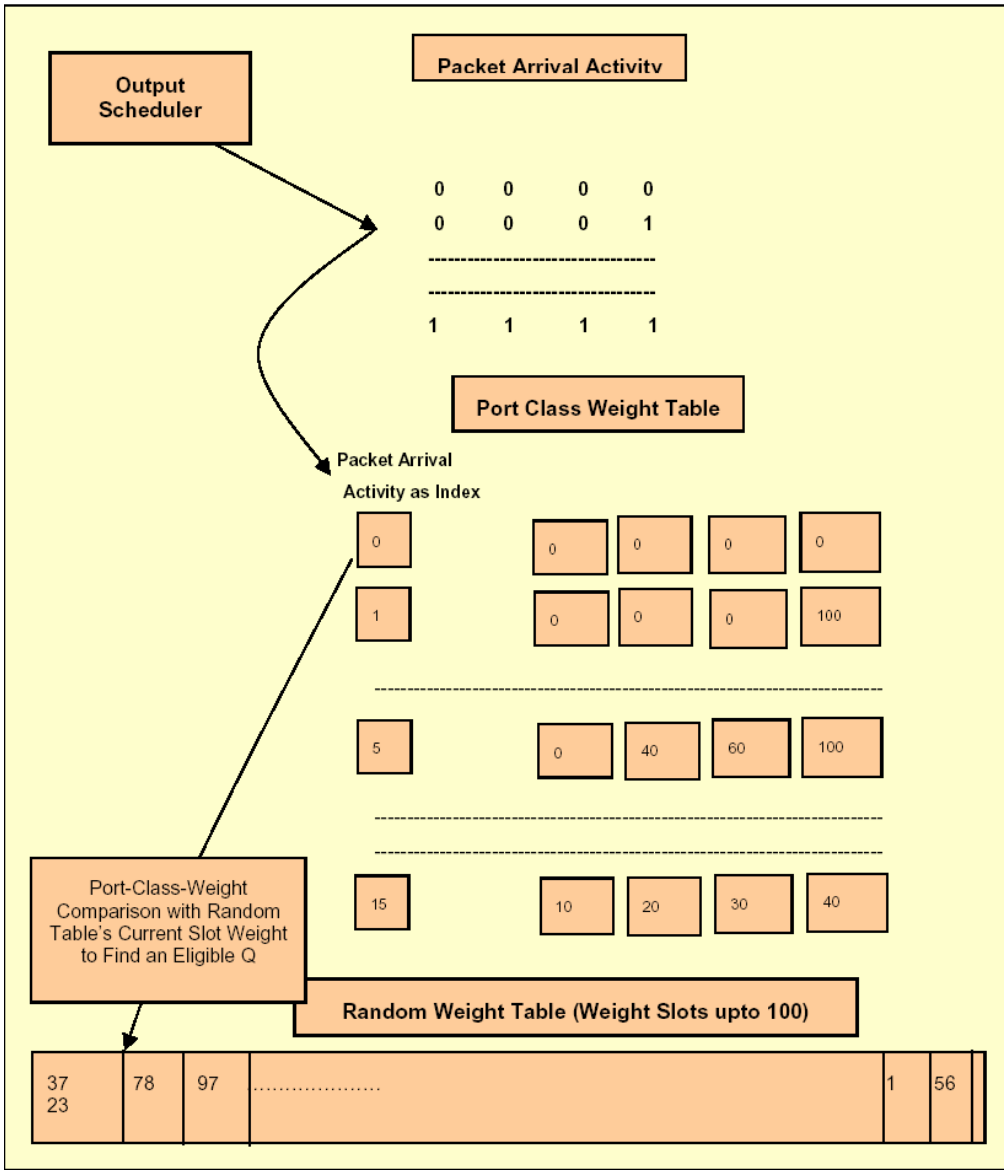


Рисунок 10-1

Customized Scheduling

Данный алгоритм может быть применен только к ATM очередям. Пользователь может настроит следующие параметры:

- Excess bandwidth sharing weight
- Minimum bandwidth (in Kbps)
- Maximum bandwidth (in Kbps)

Ниже описаны три типа профайлов, которые пользователь может описать, используя данный алгоритм:

1. Приоритетный (SP): означает строгие приоритеты, использует следующие параметры для каждой очереди:
   - Excess bandwidth sharing weight = 100 (для всех очередей)
   - Minimum bandwidth = Maximum bandwidth =0 (для всех очередей)

2. Приоритезированный min-max:
    - Excess bandwidth sharing weight = 100 (для всех очередей)
    - Minimum bandwidth: min значение полосы пропускания, требуемое для данной очереди. Указывается в Кбит/с.
    - Maximum bandwidth: max значение полосы пропускание, которое данная очередь может использовать. Указывается в Кбит/с. Ноль значит отсутствие ограничений.
3. Взвешенный:
    - Excess bandwidth sharing weight = размер избыточной полосы пропускания, которую данная очередь хочет занять.
    - Minimum bandwidth: min значение полосы пропускания, требуемое для данной очереди. Указывается в Кбит/с.
    - Maximum bandwidth: max значение полосы пропускание, которое данная очередь может использовать. Указывается в Кбит/с. Ноль значит отсутствие ограничений.

.

10.1.3.Алгоритмы ограничения полосы пропускания

10.1.3.1.Token Bucket Filter

Контроль полосы пропускания в DAS-3248 производится на основе алгоритма Token Bucket Filter (TBF).

TBF- это дисциплина очереди, которая передает поступающие пакеты со скоростью, не превышающей административно заданный порог, но с возможностью превышающих его коротких всплесков.

Реализована TBF в виде буфера, постоянно заполняющегося некими маркерами (токенами) с заданной скоростью. Наиболее важным параметром буфера является его размер, определяющий количество хранимых токенов.

Каждый прибывающий токен сопоставляется с одним пакетом данных из очереди, после чего удаляется. Связав этот алгоритм с двумя потоками - токенов и данных, получим три возможные ситуации:

- Данные прибывают со скоростью равной скорости входящих токенов. В этом случае каждый пакет имеет соответствующий токен и проходит очередь без задержки.
- Данные прибывают со скоростью меньшей скорости поступления токенов. В этом случае лишь часть существующих токенов будет уничтожаться, потому они станут накапливаться до размера буфера. Далее, накопленные токены могут использоваться при всплесках для передачи данных со скоростью, превышающей скорость пребывающих токенов.
- Данные прибывают быстрее, чем токены. Это означает, что в буфере скоро не останется токенов, что заставит дисциплину приостановить передачу данных. Эта ситуация называется "превышением". Если пакеты продолжают поступать, они начинают уничтожаться.

Последняя ситуация очень важна, поскольку позволяет административно ограничивать доступную полосу пропускания.

Накопленные токены позволяют пропускать короткие всплески, но при продолжительном превышении пакеты будут задерживаться, а в крайнем случае - уничтожаться.

Параметры TBF:

Burst Size

Размер буфера в байтах или пакетах. Максимальное количество байт или пакетов, для которых токены могут быть доступны мгновенно. В целом, чем больше граничная скорость, тем больше должен быть размер буфера. Если буфер слишком мал, пакеты могут уничтожаться. Это связано с тем, что каждый тик таймера будет генерироваться больше токенов, чем может поместиться в вашем буфере.

Rate

Ограничение скорости (байтах в секунду или пакетах в секунду)
Задает скорость, с которой элемент может проходить очередь. Это достигается организацией достаточной задержки между проходящими пакетами.

10.1.3.2.Алгоритмы TBF на DAS-3248. SRTCM и TRTCM.
В DAS-3248 определено два алгоритма функционирования Rate Limiter:
SRTCM (RFC 2697) и TRTCM (RFC 2698).

Single Rate Two Color Marking (SRTCM) – одна скорость, два цвета.
Данный алгоритм имеет одну скорость продвижения токенов, то есть представляет собой классический TBF, рассмотренный в предыдущем пункте. Прошедшие Rate Limiter на основе SRTCM данные помечаются зеленым цветом (действие Conform), отброшенные помечаются красным (действие Violate). Сущность алгоритма SRTCM представлена на рисунке 10-2.

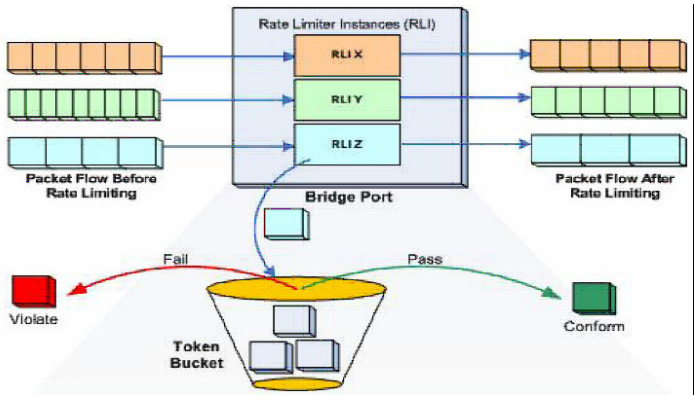


Рисунок 10-2. Single Rate Two Color Marking (SRTCM)

Two Rate Three Color Marking (TRTCM) - две скорости, три цвета.
Является вторым алгоритмом Rate Limiting . Данный алгоритм представляет собой объединение двух буферов TBF, в котором поток данных, прошедших первый буфер, попадает на вход второго. Скорости продвижения токенов первого и второго буферов отличаются.

Таким образом, данные классифицируются TRTCM алгоритмом на три группы:
Прошедшие оба буфера – зеленый цвет (действие Conform).
Прошедшие первый буфер, но отброшенные вторым – желтый цвет (действие Exceed).
Отброшенные первым буфером – красный цвет (действие Violate).
Сущность TRTCM представлена на рисунке 3.

Алгоритм TRTCM дает возможность задавать два порога скорости для потока данных и три разных действия, в зависимости от их превышения.
Это позволяет, например, до превышения первого порога пропускать все пакеты определенного протокола (к примеру, ARP), после превышения первого порога - осуществлять выборочную фильтрацию пакетов потока, например, пропускать пакеты, адресованные только определенным сетевым адресам, после превышения второго порога – полный запрет передачи потока.

Параметры TRTCM:

Peak Rate -Ограничение скорости первого буфера
Peak Burst Size- Размер первого буфера.
Commited Rate-Ограничение скорости второго буфера
Commited Burst Size-Размер второго буфера

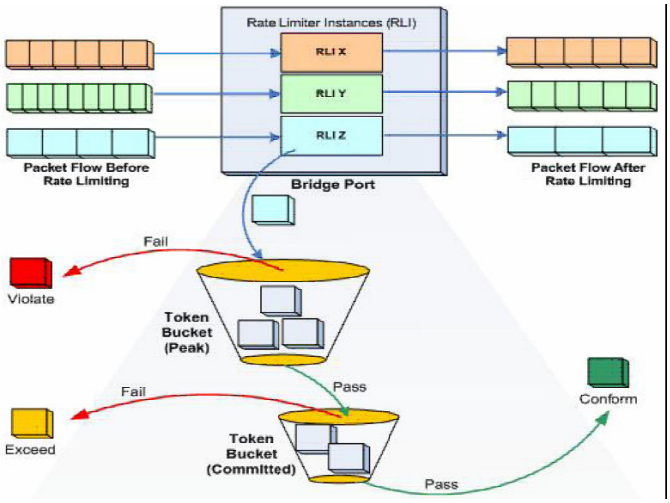


Рисунок 10-3. Two Rate Three Color Marking (TRTCM)

10.2.Настройки QoS на DAS-3248.

Обеспечение качества обслуживания является комплексной задачей, которая включает в себя:

1. управление политикой очередей
2. управление тегами 802.1p
3. определение соответствия приоритетов 802.1p очередям
4. IRL (Input Rate limiting) - на AAL5 интерфейсах
5. ORL (Output Rate Limiting) – на ATM интерфейсах и Ethernet интерфейсах
6. Flow based rate-limiting – на Bridge интерфейсах

10.2.1.Управление приоритетами и очередями. Scheduling profiles.

Дисциплины очередей в DAS-3224/3248 конфигурируются посредством scheduling profiles. Для Ethernet интерфейса доступен только PP профайл. В зависимости от интерфейса (ATM или Ethernet), с которым будет ассоциирован профайл, профайлы могут быть двух типов – Ethernet или ATM. ATM профайлы имеют 4 класса трафика (4 очереди), ethernet профайлы имеют 8 классов трафика. По умолчанию в системе созданы два профайла (ATM и ethernet) с именем SPPROFILE и SP дисциплиной.

10.2.1.1.Создание/удаление/настройка/просмотр статуса schedule profile

create sched profile info name name **[algo** pp | custom **] iftype** eth | atm – создание scheduling профайла (значение весов – по умолчанию).
delete sched profile info name name – удаление профайла
get sched profile info name name – просмотр параметров профайла
get sched profile class [name name**] [classid** classid**] –** просмотр параметров политик очередей
modify sched profile class name name **classid** classid **[param 1** param1**] [param2** param2**] [param3** param3**] [param 4** param4 **] [param5** param5**] –** для PP применим только param 1 (вес). Для Custom применимы параметры param1 (вес), 2 (min bandwidth), 3 (max bandwidth).

10.2.1.2.Привязка schedule profile к ethernet или ATM порту.

modify ethernet intf ifname ifname **profilename** profilename
modify atm port ifname ifname **profilename** profilename

10.2.1.3.Настройка соответствия между очередями и приоритетами

Пакеты помещаются в очереди в соответствии со своим «внутренним» приоритетом 802.1p (в DAS-3248 это называется regenprio) и таблицей соответствия приоритета очереди. Под «внутренним» приоритетом понимается приоритет пакета внутри DAS-3224/3248. Назначение этого «внутреннего» приоритета рассматривается в следующем разделе. Таблица соответствия regenprio и очередей настраивается с помощью команды **bridge port trfclassmap**

modify bridge port trfclassmap portid portid **regenprio** regenprio **[trfclass** trfclass **]**

где: portid – идентификатор порта
regenprio – “внутренний” приоритет пакета
trfclass – номер очереди

Замечание: по умолчанию данная таблица настроена в соответствии со стандартом 802.1d.

10.2.1.4.Определение «внутреннего» приоритета пакета

может производиться тремя способами (рассмотрим их в порядке возрастания их приоритетов):

a. С помощью фильтра пакетов:

create filter rule entry ruleid ruleid **action setprio priority <**value**>**

Данное правило необходимо привязать к нужному bridge порту и включить

b. С помощью значения 802.1p в теге входящего пакета (если пакет помечен):

modify bridge port priomap portid portid **usrprio** usrprio **[regenprio** regenprio **]**

где: portid – идентификатор порта
usrprio – приоритет входящего пакета
regenprio – “внутренний” приоритет пакета

c. Default приоритет того порта, с которого данный пакет попал в систему.

modify bridge port prioinfo portid portid **[defprio** defprio **] [numtrfclass** numtrfclass **]**

где: portid – идентификатор нужного порта, defprio – приоритет по умолчанию для всех ingress пакетов этого порта, numtrfclass – число очередей для данного порта (этот параметр можно не указывать)

10.2.1.5.Назначение выходного приоритета.

Если пакет высылается через tagged порт, необходимо выставить ему соответствующий приоритет для корректной обработки на приемной стороне. Для этого используется egress правило фильтра пакетов с действием retagprio.

10.2.2.Пример конфигурирования QoS на основе Shedulling профилей.

Пусть на 24-ом adsl порту создано два bridge порта 24 и 50, причем на каждый приходит не тегированный трафик. Пусть, к примеру, по 50-ому порту передается multicast видео поток с постоянной скоростью 2 Мбит/с, которому нужно предоставить наибольший приоритет и гарантированную полосу пропускания.

1. Изменяем дефолт приоритет для 50-го порта:

   $ **modify bridge port intf portid 50 status disable**
   $ **modify bridge port prioinfo portid 50 defprio 7**
   $ **modify bridge port intf portid 50 status enable**

2. По умолчанию 7 приоритет помещается в 7-ую очередь. В этом можно убедиться командой
   $ **get bridge port trfclassmap portid 50**

3. Настроим профайл отправки так, чтобы, во-первых, обеспечить 7 очереди высший строгий приоритет и, во-вторых, ограничить ее полосу пропускания 2 Мбит/с.

4. Создаем scheduling профайл для атм порта
   $ **create sched profile info name VOD algo custom iftype atm**

5. Указываем для 8-ой самой приоритетной очереди все 100 (т.е. для нее будет выполняться SP) и фиксированную полосу пропускания в 2048Кбит/с. Все остальные очереди будут делить оставшуюся полосу по PP в долях: 10/20/30/40/50/60/70. В нашем случае периодически пакеты будут проходить через вторую очередь (т.к. по умолчанию нулевой приоритет направляется во вторую очередь)

   $ **modify sched profile class name VOD classid 8 param1 100 param2 2048 param3 2048**

6.связываем созданный schedule профайл с нужным ATM интерфейсом
   $ **modify atm port ifname atm-23 profilename VOD**

10.2.3.Контроль полосы пропускания по потокам. Flow Based Rate Limiting.

Flow Based Rate Limiting позволяет выделять из входящего трафика, поступающего на устройство, отдельные потоки данных, основываясь на определенном признаке, и дифференцированно контролировать их полосу пропускания (гарантирует, что заданная скорость передачи пакетов заданного типа не будет превышена).
Для Upstream потока данных (рис.10-4) это позволяет дифференцированно производить ограничение скорости определенных типов предустановленных и пользовательских потоков данных, что снижает нагрузку на устройство (за счет уменьшения скорости или полного прекращения передачи нежелательных потоков), а также позволяет оператору связи строить различные типы сервиса, основываясь на данной технологии.
Для Downstream данная технология также позволяет избавиться от паразитной и нежелательной нагрузки на устройство, приходящей по Uplink порту с Backbone сети.
Применяется на Bridge интерфейсах устройства.

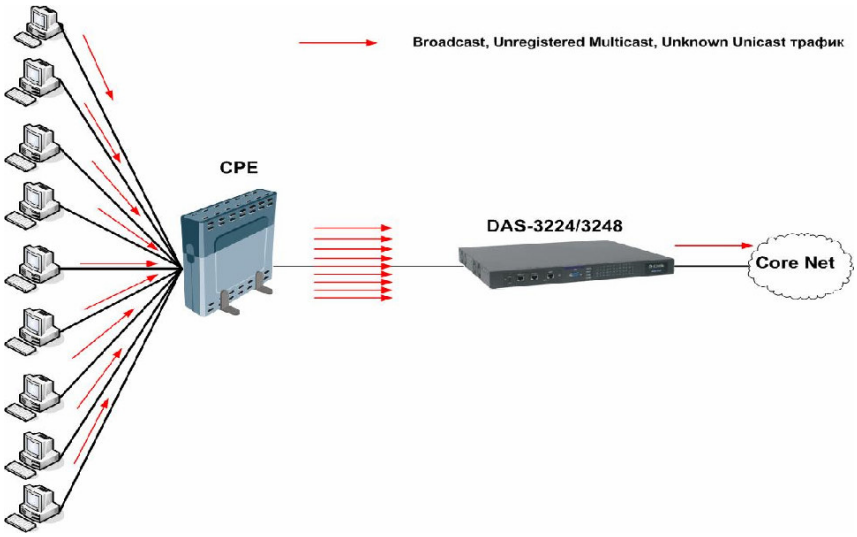


Рисунок 10-4

10.2.3.1.Контроль предопределенных потоков.

Контроль потоков в DAS-3248 разделяется на два типа: для предопределенных в системе потоков и для установленных пользователем потоков (рис.10-5).

Примечание: В версиях внутреннего ПО DAS-3248 1.xx существовал упрощенный Rate Limiting (алгоритм только SRTCM и дейтвия над потоком только Allow (пропустить) и Drop (отбросить).

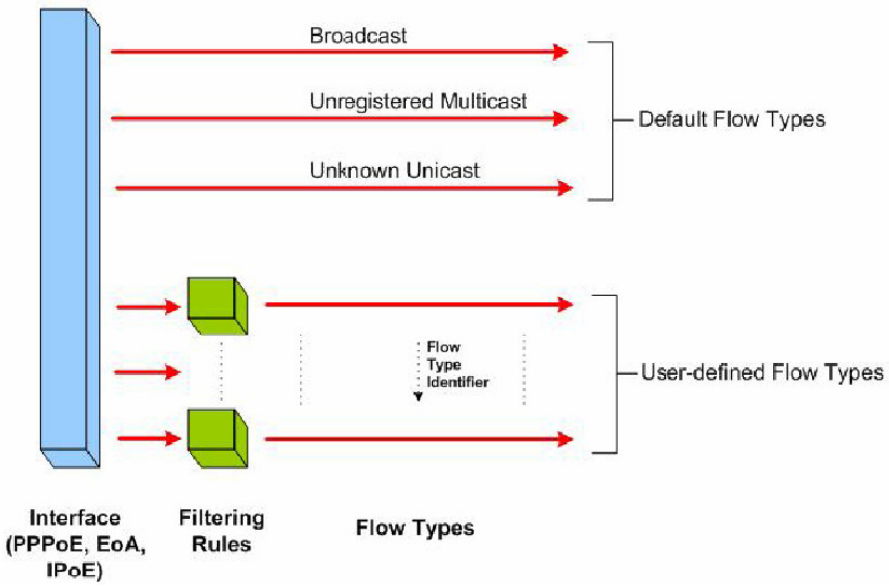


Рисунок 10-5

В системе имеется три предустановленных типа потоков трафика, по которым ведется контроль:
Broadcast – широковещательный поток данных;
Unregistered Multicast – пакеты от неизвестных системе групповых адресов;
Unknown Unicast – пакеты от неизвестных эникаст адресов.
Алгоритм конфигурирования контроля полосы пропускания для предопределенных типов:

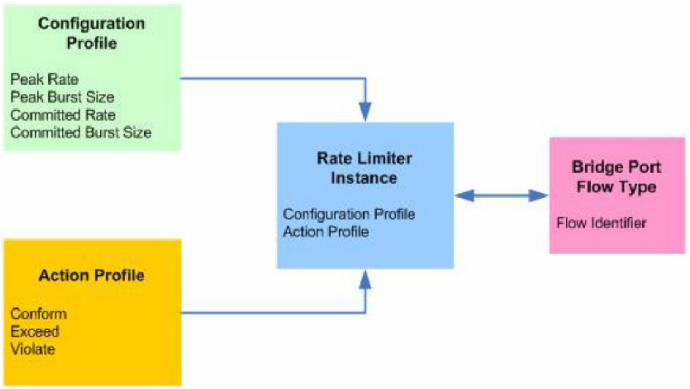


Рисунок 10-6. Алгоритм конфигурирования предопределенных типов потока

1. Создать RL профиль командой **create rl profile**

На первом этапе задаются параметры TBF.Также в этом пункте указывается единица измерения TBF (байты в секунду или пакеты в секунду)

Синтаксис команды для SRTCM:

create rl profile info profileid profileid [rate rate] [mbs mbs] [level packet| byte] [type sr2cm **]**

где

type sr2cm –выбор алгоритма (SRTCM)

level packet| byte – единица измерения для параметров rate и burst (в пакетах или байтах);

rate – полоса пропускания;

mbs- размер буфера (burst);

Для TRTCM команда **create rl profile** имеет расширенный синтаксис:

create rl profile info profileid profileid [rate rate **] [mbs** mbs **] [level** packet | byte **] [type** sr2cm | trtcm **] [peakrate** peakrate **] [pbs** pbs **] ,**где

peakrate – Ограничение скорости первого буфера (Peak Rate)

pbs- Размер первого буфера (Peak Burst Size).

rate – Ограничение скорости второго буфера (Commited Rate)

mbs – Размер второго буфера Commited Burst Size

level packet| byte- единица измерения для параметров rate и burst (в пакетах или байтах)

type sr2cm| trtcm –переключатель режима SRTCM или TRTCM

2. Создать RL Action Profile

На втором этапе указывается, какие действия необходимо предпринять с пакетами, которые прошли Rate Limiter (действие Conform) ,
или были отброшены (действие Violate) и Exceed (для TRTCM)

Действия настраиваются командой **create rl actionprofile info**

Синтаксис команды:
create rl actionprofile info profileid profileid [**result** conform|exceed|violate] [**action** drop|allow] [**description** <name>][**actionval** actionval] [**actionmask** actionmask]

Синтаксис команды:
create rl actionprofile info profileid profileid [**result** conform |violate] [**action** drop|allow]**,**где

profileid - Идентификатор Action Prolile
result – результат алгоритмов SRTRM и TRTCM
action – действие (Allow - пропустить, Drop – отбросить, другие действия будут рассмотрены ниже.
description <name> **actionval** actionval **actionmask** actionmask – расширенные параметры Action (расширенные действия Action смотрите ниже).
Примечание: параметры **actionval и actionmask обязательно** задавать в шестнадцатиричном виде (0x1,0x10 и т д).

3. Создать RL instance (связывает RL Profile с RL Action профиль) командой
create rl instance
Третий этап связывает параметры TBF с действиями, которые будут предприняты с потоком.

Синтаксис команды:
create rl instance instanceid instanceid **profileid** profileid **actionprofileid** actionprofileid ,
где instanceid, profileid, actionprofileid- идентификаторы RL Instance, RLProfile и RL Action Profile.

4. Приложить RL instance к требуемому Bridge интерфейсу командой
create bridge rlinstance map

Синтаксис команды:
create bridge rlinstance map [portid all| portid] [**flowtype** bcast|unregmcast|unknownucast][**instanceid** instanceid]
portid all| portid – идентификатор бридж интерфейса, на который прикладывается RL Instance (либо на все порты),
flowtype bcast|unregmcast|unknownucast – идентификатор потока
instanceid – идентификатор RL Instance

10.2.3.2.Контроль пользовательских потоков.

Кроме предустановленных типов в DAS-3248 возможен контроль полосы информационных потоков, тип которых определяется пользователем.

Различие в конфигурировании данной функции с контролем предопределенных потоков заключается лишь в том, что Rate Limiter используется для контроля только определенные пользователем потоки, выделенные с помощью фильтров (Generic Filter) на входном интерфейсе. Для этого используются правила Generic Filter с действием **action ratelimiter.**

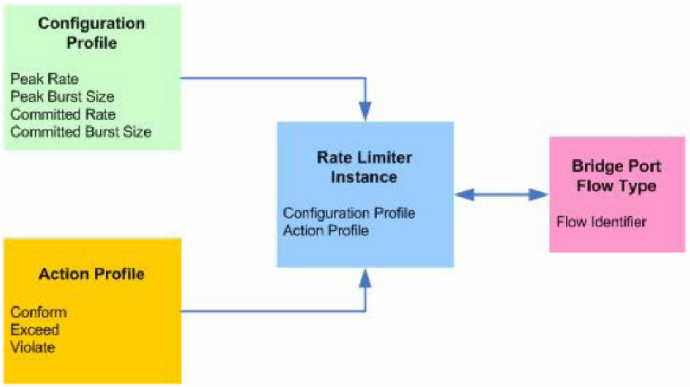


Рисунок 10-7. Алгоритм конфигурирования пользовательских типов потоков

Алгоритм конфигурирования контроля полосы пропускания для предопределенных типов отражен на рисунке 10-7.

Порядок действий алгоритма:

1.Создать правило фильтрации (Generic Filter) для выделения нужного потока данных и включить его в работу командой **create filter rule** (см. Главу 9)

2.Привязать правило к интерфейсу, на котором будет осуществляться Rate Limiting командой
$create filter rule map (см. Главу 9).

3.Создать Rate Limiter (RL) Profile
$create rl profile info

Синтаксис команды для SRTCM:
create rl profile info profileid profileid [rate rate] [mbs mbs] [level packet| byte] [type sr2cm | trtcm **]**
где
type sr2cm| trtcm –переключатель режима SRTCM или TRTCM
level packet| byte – единица измерения для параметров rate и burst (в пакетах или байтах);
rate – полоса пропускания;
mbs- размер буфера (burst);

Для TRTCM команда **create rl profile** имеет расширенный синтаксис:

create rl profile info profileid profileid [rate rate **] [mbs** mbs **] [level** packet | byte **] [type** sr2cm | trtcm **] [peakrate** peakrate **] [pbs** pbs **] ,**где

peakrate – Ограничение скорости первого буфера (Peak Rate)
pbs- Размер первого буфера (Peak Burst Size).
rate – Ограничение скорости второго буфера (Commited Rate)
mbs – Размер второго буфера Commited Burst Size
level packet| byte- единица измерения для параметров rate и burst (в пакетах или байтах)
type sr2cm| trtcm –переключатель режима SRTCM или TRTCM

4.Создать RL Action Profile
$create rl actionprofile info

Синтаксис команды:
create rl actionprofile info profileid profileid [**result** conform|exceed|violate] [**action** drop|allow|sendtocontrol|copytocontrol|modifytos|setbaclevel] [**description** <name>] [**actionval** actionval] [**actionmask** actionmask] **,**где
profileid - Идентификатор Action Prolile
result – результат алгоритмов SRTRM и TRTCM
action – действие (Allow - пропустить,Drop – отбросить, другие действия будут рассмотрены ниже.
description <name> **actionval** actionval **actionmask** actionmask – расширенные параметры Action (расширенные действия Action смотрите ниже).

5.Связать RLProfile и RL Action Profile путем создания RL Instance
create rl instance info

Синтаксис команды:
create rl instance instanceid instanceid **profileid** profileid **actionprofileid** actionprofileid ,
где instanceid, profileid, actionprofileid- идентификаторы RL Instance, RLProfile и RL Action Profile.

6.Связать RL Instance с портом и его типом
create bridge rlinstance map

Синтаксис команды:
create bridge rlinstance map [portid all| portid] [**flowtype** flotypeid][**instanceid** instanceid], где
portid all| portid – идентитфикатор бридж интерфейса на который прикалдывается RL Instance (либо на все порты),
flowtype flotypeid – идентификатор потока (должен совпадать с параметром actionval действия ratelimiter в правиле Generic Filter).

instanceid – идентификатор RL Instance

10.2.3.3.Расширенные действия Action.
Кроме простых действий: allow (пропустить данные потока для дальнейшей обработки) или drop (отбросить данные) в алгоритмах SRTCM и TRTCM можно указывать более сложные действия:

Sendtocontrol- Передает поток в ControlPlane, что дает возможность дополнительной обработки потока приложениями (процессами), зарегистрированными в Control Plane (например, IGMP Snooping). При конфигурировании действия **Sendtocontrol** вы должны определить следующие параметры:

- Имя приложения, которое получает пакеты. Ее имя должно определяться в правиле фильтра Generic Filter (см. Главу 9).
- Traps enabled/disabled.
  Раньше, все пакеты потоков, которые помечены действием sendtocontrol и copytocontrol передавались в ControlPlane зарегистрированным в них приложениям. Эта схема обработки потока имела две проблемы:
  - На обработке этих пакетов значительно терялась мощность системы (в том числе процессора);

- ControlPlane и DataPlane очереди могли быть переполнены пакетами единственного потока. Большой поток этих пакетов мог вызывать отказ в обслуживании пакетов другого типа, также приходящих для обработки в ControlPlane, что являлось особенно серьезным, если данный поток представлял собой атаку (злонамеренно сформированный поток).
  Для того чтобы решить эти проблемы, был введен новый параметр trap level для действий sendtocontrol и copytocontrol. Эта ловушка работает следующим образом:
  - Если Traps disabled, то все пакеты из потоков с действиями sendtocontrol и copytocontrol передаются ControlPlane.
  - Если Traps enabled, только по одному пакету из потоков с действиями sendtocontrol и copytocontrol передаются ControlPlane. Остальные пакеты передаются вызывающему приложению только тогда, когда процесс показывает свою готовность к получению новых пакетов через запрос к ControlPlane через пакетный фильтр. Если приложение пока не готово к получению новых данных, пакеты или молча отбрасываются (в случае sendtocontrol действия) или обрабатываются отдельно (в случае copytocontrol действия).
- Control Flow ID . Идентификатор потока. Все потокаи попадают в однуи туже очередь с дисциплиной DP-SP на интерфейсе. Это сильно затрудняет проведение приоритезации потоков в Control Plane.Для решения этой проблемы и дифференции потоков данных с действиями Sendto Control и CopytoControl проблемы был введен параметр Control flow ID.

Copytocontrol- Копирует поток в ControlPlane. Имеет те же параметры и тоже назначение, что и Sendtocontrol, за исключением того, что поток не перенаправляет, а только копируется в Control Plane, что дает возможность его дальнейшего форвардинга.
(подробнее см. Главу 9).

Modifytos- Изменяет поле TOS в заголовке IP пакета.
Требует задания нового значения TOS и битовой маски.
В маске если битовая позиция содержит 1, то соответствующий бит в области TOS переписывается соответствующим битом нового значения. Если битовая позиция содержит 0, то соответствующий бит в поле области TOS остается неизменным.

8 битовое поле TOS в заголовке IP пакета используется в различных целях и в различных ситуациях.
Например, при использовании в DiffServ ,где DSLAM ведется себя как оконечное устройство (edge), Вам нужно модифицировать первые 6-битовый области TOS (которые формирует DSCP область) в классификации потока.
В некоторых других сценариях, каждый отдельный бит TOS может иметь свое назначение. Кроме того, в сети передачи данных операторов связи могут быть введены свои уникальные реализации, обеспечивающие прогрессивные способы интерпретации области TOS.

Setbaclevel- уставливает Buffer Admission Control (BAC).

BAC level является механизмом исключения перегрузки в DAS-3248. В этом механизме, пакеты могут быть выборочно отброшены выборочно в выходных очередях системы в зависимости от уровня загруженности очереди.
Существует два уровня BAC:

- BAC уровень 0 -означает, что пакет не должен быть отброшен прежде, чем буфер очереди не переполнится.

- BAC уровень 1 -означает, что пакет должен был отброшен, если уровень занятости очереди выше сконфигурированного порога. Этот порог сконфигурирован для каждого типа трафика, используя Traffic Class Parameters Table.

10.2.3.4.Примеры конфигурирования Flow Based Rate Limiting

Пример 1. Конфигурирование контроля предопределенного (широковещательньного) потока данных на основе SRTCM:

1.Создать RL профиль:
$ create rl profile info profileid 2 rate 2 mbs 4 level packet

2.Создать RL Action Profile
$ create rl actionprofile info profileid 2 result conform action allow
$ create rl actionprofile info profileid 2 result violate action drop

3.Связать rl profile и rl action profile путем создания RL instance
$ create rl instance info instanceid 2 profileid 2 actionprofileid 2

4. Приложить rl instance к Bridge интерфейсу
$create bridge rlinstance map portid 1 flowtype bcast instanceid 2

Пример 2. Использование Flow-based Rate Limiting с применением SRTCM для пользовательского типа потока.

1.Создать правило фильтрации (Generic Filter) для выделения нужного потока данных и включить его в работу

$ create filter rule entry ruleid 4 action ratelimiter actionval 0x10
$ create filter subrule ip ruleid 4 subruleid 1 srcipaddrfrom 192.168.100.1 dstipaddrfrom 192.168.100.253 srcaddrcmp eq dstaddrcmp eq
$ modify filter rule entry ruleid 4 status enable

2.Привязать правило к интерфейсу, на котором будет осуществлятся Rate Limiting
$ create filter rule map ifname eth-0 stageid 1 ruleid 4

3.Создать Rate Limiter (RL) Profile
$ create rl profile info profileid 3 rate 32768 mbs 4096 level byte

4.Создать RL Action Profile
$ create rl actionprofile info profileid 3 result conform action allow
$ create rl actionprofile info profileid 3 result violate action drop

5.Связать RLProfile и RL Action Profile путем создания RL Instance
$ create rl instance info instanceid 3 profileid 3 actionprofileid 2

6.Связать RL Instance с портом и его типом
$ create bridge rlinstance map portid 385 flowtype 16 instanceid 2

Пример3. Использование Flow-based Rate Limiting с применением TRTCM для контроля пользовательского типа потока.
1. Создать правило фильтрации (Generic Filter) для выделения нужного потока данных и включить его в работу
$ create filter rule entry ruleid 4 action ratelimiter actionval 0x10
$create filter subrule ip ruleid 4 subruleid 1 srcipaddrfrom 192.168.100.17 dstipaddrfrom 192.168.100.253 srcaddrcmp eq dstaddrcmp eq
$ modify filter rule entry ruleid 4 status enable

2.Привязать правило к интерфейсу, на котором будет осуществлятся Rate Limiting
$ create filter rule map ifname eoa-0 stageid 1 ruleid 4

3.Создать Rate Limiter (RL) Profile
$ create rl profile info profileid 3 rate 32768 mbs 4096 level byte type trtcm peakrate 65535 pbs 8192

4.Создать RL Action Profile
$ create rl actionprofile info profileid 3 result conform action allow
$ create rl actionprofile info profileid 3 result exceed action setbaclevel actionval 0x1
$ create rl actionprofile info profileid 3 result violate action drop

5.Связать RLProfile и RL Action Profile путем создания RL Instance
$ create rl instance info instanceid 3 profileid 3 actionprofileid 3

6.Связать RL Instance с портом и его типом
$ create bridge rlinstance map portid 1 flowtype 16 instanceid 3

10.2.4.Контроль полосы входного потока (IRL).

Input Rate Limiting (IRL) применяется для обеспечения заданного контрактным соглашением оператора связи (провайдера) с клиентом скорости Upstream потока данных и/или защиты очередей устройства от перегрузки несанкционированными потоками данных.
Данная функция применяется, поскольку регулирование потока данных с помощью профилей dsl портов (рассмотрены в главе 3) не является правильным поведением для оператора связи (провайдера). DSL порты и профили характеризует параметры линии на физическом уровне и полоса, заданная им, не является достаточным основанием для констатации факта обеспечения контрактной скорости, заявленной оператором связи клиенту.

Часто контрактные обязательства провайдера распространяются только на определенные типы протоколов, пакетов и т. д.
Таким образом, передача других типов пакетов может быть или осуществлена ими с низшим приоритетом или вообще не осуществляться.

Для реализации этого функционала используется совместное использование функции IRL с другими функциями.

Конфигурирование IRL
IRL конфигурируется на ATM VC (AAL5) интерфейсах устройства.

IRL использует технологию TBF и алгоритмы SRTCM и TRTCM, рассмотренные в начале данной главы.

1.Создать IRL профиль, в котором указать параметры TBF и необходимые алгоритма анализа пакетов. Для этого используется команда **create irl profile.**

Синтаксис команды:
create irl profile profilename profilename [**irltype** sr2cm|trtcm] [**cir** cir][**cbs** cbs] [**pir** pir] [**pir** pir][**conformaction** colorgreen][**exceedaction** drop|coloryellow] [**violateaction** drop|coloryellow], где
profilename – имя IRL профиля
irltype sr2cm|trtcm –выбор алгоритма SRTCM или TRTCM
cir – Commited Rate (Скорость первого буфера)
cbs – Commited Burst Size (Емкость первого буфера)
pbs – Peak Burst Size (Емкость второго буфера)
pir – Peak Rate (Скорость второго буфера).
conformaction colorgreen – действие по результату Conform
exceedaction drop|coloryellow – действие по результату Exceed
violateaction drop|coloryellow – действие по результату Violate

2.Привязать IRL профиль к интерфейсу AAL командой **create irl map**

Синтаксис команды:
create irl map ifname ifname **profilename** profilename, где
ifname- имя AAL интефеса
profilename – имя IRL профиля.

Пример конфигурирования IRL:
1. Создать IRL Profile
create irl profilename gold irltype trtcm cir 1000 cbs 400 pir 2000 pbs 12000 conformaction colorgreen exceedaction coloryellow violation drop
2.Приложить IRL Profile к интерфейсу:
create irl map aal5-3 profilename gold

10.2.5.Контроль полосы выходного потока (ORL)

Является третьим инструментом, контролирующим полосу пропускания, и предназначен для контроля потока данных, выходящего из устройства.
ORL работает на уровне ATM интерфейсов (для контроля полосы пропускания Downstream потока) и на уровне Ethernet интерфейсов (для контроля полосы Upstream потока).

Основное назначением ORL на ATM портах – это регулирование контрактной скорости Downsteam потока данных, передающегося к клиентам.
Функция ORL применяться, поскольку регулирование потока данных с помощью профиля dsl портов (рассмотрены в главе 3) не является правильным поведением для оператора связи (провайдера). DSL порты и профили характеризует параметры линии на физическом уровне и полоса, заданная им, не является достаточным основанием для констатации факта обеспечения контрактной скорости, заявленной оператором связи клиенту.

Основным назначением ORL на Ethernet портах является контроль полосы суммарного потока выходящего из DSLAM. Данный поток является суммой клиентских потоков и позволяет устройству быть более гибким. Кроме того, данная функция может применяться, например, для обеспечения контроля потока в случае использования оператором сторонних каналов связи (когда оператор связи использует ограниченный по скорости платный Uplink канал).

Конфигурирование ORL для ATM интерфейсов вкратце уже было затронуто в главе 3 при создании профиля dsl порта.
ORL конфигурируется параметром ORL в командах:

create atm port [**Orl** Orl]
modify atm port [**Orl** Orl] ,где
Orl Orl – параметр, задающий ORL ограничение скорости потока (задается в Кбит/с).

ORL для Ethernet интерфейсов конфигурируется параметром ORL в командах

create ethernet intf [**Orl** Orl]
modify Ethernet intf [**Orl** Orl] ,где
Orl Orl – параметр, задающий ORL ограничение скорости потока (задается в Мбит/с).

10.2.6. Профили очередей (Traffic Class Profile).

Traffic Class Profile представляет собой профиль для параметров входных очередей устройства.
По умолчанию в системе сконфигурированы Traffic Class Profile с profileid 1 для ATM портов, и Traffic Class Profile с profileid 2 для Ethernet портов.

Traffic Class Profile может использоваться совместно с IRL для контроля перегрузки DSLAM пакетами неприоритетных потоков данных клиента. Для этого конфигурируется порог срабатывания IRL (в процентном отношении от размера очереди). После достижения этого порога, только прошедшие IRL пакеты будут пропускаться в систему, остальные будут отброшены.
Кроме того, возможно условное срабатывание защиты очередей, используя Flow Based Rate Limiting и Generic Filter Rule с действиями Buffer Admission Control (BAC Control). Подробнее читайте об этом в соответствующих разделах, посвященных описанию этих технологий.

Вы можете сконфигурировать свои параметры Traffic Class Profile через команду **modify trfclass profile class**.

Команды Traffic Class Profile:

modify trfclass profile class
Описание команды: Задать параметры класса трафика (очередей устройства)
Синтаксис команды:

modify trfclass profile class profileid profileid **classid** classid **size** size [**thrshld1** thrshld1],
где profileid – ID Traffic Class Profile
classid – ID внутренней очереди
Size – размер класса трафика (очереди). Принимает значения от 1 до 64.По умолчанию 64.

thrshld1 – процентное заполнение очереди, начиная с которого начинает работать IRL.

Пример: Изменить параметры **trfclass profile** профиля по умолчанию (для очередей ATM) на срабатывание IRL при 80 процентном заполнении для 4 очереди. Размер очереди оставить неизменным.

$modify trfclass profile class profileid 1 **classid** 4 **thrshld1** 80

Приложение А: Соответствие контактов коннекторов TELCO-50 Amphenol портам DAS-3248.

разъем Line 1	разъем Line2
24 порт- контакты 1,26	48 порт- контакты 1,26
23 порт- контакты 2,27	47 порт- контакты 2,27
22 порт- контакты 3,28	46 порт- контакты 3,28
21 порт- контакты 4,29	45 порт- контакты 4,29
20 порт- контакты 5,30	44 порт- контакты 5,30
19 порт- контакты 6,31	43 порт- контакты 6,31
18 порт- контакты 7,32	42 порт- контакты 7,32
17 порт- контакты 8,33	41 порт- контакты 8,33
16 порт- контакты 9,34	40 порт- контакты 9,34
15 порт- контакты 10,35	39 порт- контакты 10,35
14 порт- контакты 11,36	38 порт- контакты 11,36
13 порт- контакты 12,37	37 порт- контакты 12,37
12 порт- контакты 13,38	36 порт- контакты 13,38
11 порт- контакты 14,39	35 порт- контакты 14,39
10 порт- контакты 15,40	34 порт- контакты 15,40
9 порт- контакты 16,41	33 порт- контакты 16,41
8 порт- контакты 17,42	32 порт- контакты 17,42
7 порт- контакты 18,43	31 порт- контакты 18,43
6 порт- контакты 19,44	30 порт- контакты 19,44
5 порт- контакты 20,45	29 порт- контакты 20,45
4 порт- контакты 21,46	28 порт- контакты 21,46
3 порт- контакты 22,47	27 порт- контакты 22,47
2 порт- контакты 23,48	26 порт- контакты 23,48
1 порт- контакты 24,49	25 порт- контакты 24,49

разъем Phone 1	разъем Phone2
24 порт- контакты 1,26	48 порт- контакты 1,26
23 порт- контакты 2,27	47 порт- контакты 2,27
22 порт- контакты 3,28	46 порт- контакты 3,28
21 порт- контакты 4,29	45 порт- контакты 4,29
20 порт- контакты 5,30	44 порт- контакты 5,30
19 порт- контакты 6,31	43 порт- контакты 6,31
18 порт- контакты 7,32	42 порт- контакты 7,32
17 порт- контакты 8,33	41 порт- контакты 8,33
16 порт- контакты 9,34	40 порт- контакты 9,34
15 порт- контакты 10,35	39 порт- контакты 10,35
14 порт- контакты 11,36	38 порт- контакты 11,36
13 порт- контакты 12,37	37 порт- контакты 12,37
12 порт- контакты 13,38	36 порт- контакты 13,38
11 порт- контакты 14,39	35 порт- контакты 14,39
10 порт- контакты 15,40	34 порт- контакты 15,40
9 порт- контакты 16,41	33 порт- контакты 16,41
8 порт- контакты 17,42	32 порт- контакты 17,42
7 порт- контакты 18,43	31 порт- контакты 18,43
6 порт- контакты 19,44	30 порт- контакты 19,44
5 порт- контакты 20,45	29 порт- контакты 20,45
4 порт- контакты 21,46	28 порт- контакты 21,46
3 порт- контакты 22,47	27 порт- контакты 22,47
2 порт- контакты 23,48	26 порт- контакты 23,48
1 порт- контакты 24,49	25 порт- контакты 24,49

Приложение B: Внутренний аппаратный тест устройства (POST).

1. В стадии загрузки устройства при появлении сообщения «**Press F1 to enter Interactive Mode, 'Enter' to skip ... 5 seconds left**» нажмите клавишу **F1**.
2. Затем, при появлении строки «**Press 'P/p' to perform POST, 'Enter' to skip .... 5 seconds left**» Нажмите клавишу **P** или **p** на клавиатуре.

3.Дождитесь аппаратной проверки устройства.
При полностью исправном устройстве на экране появятся следующие сообщения:

Validating SDRAM-A..... **Success**
Validating SDRAM-B..... **Success**
Validating SDRAM-D..... **Success**
Validating SDRAM-E..... **Success**
CPLD Ctrl Reg read at addr 0x/4A01C00 = 0x000000FF
CPLD Version read at addr /4A01804 = 00000009
CPLD Status read at addr /4A01800 = 000000FE
CPLD Test..... **Success**
Validating Dsl Device.....

Number of Chips is 2
Chip Type is 0
Chip Type is G24

POST passed for Dsl Device Id 0 [0x000000C8]

POST passed for Dsl Device Id 1 [0x000000C8]

POST passed for Dsl Device Id 2 [0x000000C8]

POST passed for Dsl Device Id 3 [0x000000C8]

POST passed for Dsl Device Id 4 [0x000000C8]

POST passed for Dsl Device Id 5 [0x000000C8]

Validating Dsl Device..... **Success**

Validating Ethernet device access.....

Ethernet Controller 1 Vendor Info 0x102313F0
Ethernet Controller 2 Vendor Info 0x102313F0

Validating Ethernet device access..... **Success**
POST execution..... Done

Приложение C: Примеры конфигурирования Generic Filter

1.Фильтр для запрета icmp echoсообщений на определенном интерфейсе с определенного ip адреса

create filter rule entry ruleid 2 action drop ruleprio high

Создаем главное правило:
action drop - отбрасывать
ruleprio high - правило будет загружаться в высокоприоритетную память (рекомендуется для "часто срабатывающих" правил)

$create filter subrule ip ruleid 2 subruleid 1 srcipaddrfrom 192.168.100.129 srcaddrcmp eq dstaddrcmp any ipsrcaddrmask 0xffffffff subruleprio asinrule

Создаем первое подправило, в котором указываем, что нас интересует трафик от хоста 192.168.100.197:
ruleid 2 subruleid 1 - первое подправило второго правила
srcipaddrfrom 192.168.100.197 - нижнее значение диапазона ip адресов источников трафика (т.к. srcaddrcmp равен eq, верхнее можно не указывать)
dstaddrcmp any - ip адрес назначения любой
ipsrcaddrmask 0xffffffff - маска источника 255.255.255.255
subruleprio asinrule - приоритет подправила такой же, как у правила

$create filter subrule icmp ruleid 2 subruleid 2 icmptype 8 icmptypecmp eq subruleprio asinrule

Создаем подправило, в котором указываем, что из ранее выбранного ip трафика от хоста 192.168.100.197 нас интересуют icmp echo сообщения:
ruleid 2 subruleid 2 - второе подправило второго правила
icmptype 8 icmptypecmp eq - все icmp type 8 пакеты
subruleprio asinrule - приоритет подправила такой же, как у правила

$create filter rule map ifname eoa-23 stageid 1 ruleid 2

Применяем правило к конкретному интерфейсу (eoa-xx, eth-x)

$modify filter rule entry ruleid 2 status enable

Включаем фильтр в работу

2. Пример анализа заголовка TCP пакета (TCP_SYN_filtering).

Создаем правило, включаем сбор статистики срабатываний для него
$create filter rule entry ruleid 2 action drop statsstatus enable

Создаем подправило
offsethdr tcp offset -начинаем считать от заголовка TCP отступаем 12 байт
mask 0x00020000 - задаем маску
valuefrom 0x00020000 – значение в соотвествии с наложенной маской

$create filter subrule generic ruleid 2 subruleid 1 offsethdr tcp offset 12 mask 0x00020000 valuefrom 0x00020000 gencmp eq subruleprio high

прикладываем правило к интерфейсу
$create filter rule map ruleid 2 ifname eth-0 stageid 1

включаем правило
$modify filter rule entry ruleid 2 status enable

3. Фильтр для привязки IP адреса к adsl порту (ATM PVC)

Пояснение: Данное правило позволяет реализовать жесткую привязку IP адреса к порту DSLAM, что может быть полезно при использовании на клиенских устройсвах ADSL статических IP адресов.

$create filter rule entry ruleid 2 action allow

Создаем разрешающее правило для нужного ip адреса:
action allow - принимать пакеты

$create filter subrule ip ruleid 2 subruleid 1 srcipaddrfrom 192.168.100.207 srcaddrcmp eq dstaddrcmp any ipsrcaddrmask 0xffffffff

Создаем подправило, в котором указываем, что нас интересует трафик от хоста 192.168.100.207:
ruleid 2 subruleid 1 - первое подправило второго правила
srcipaddrfrom 192.168.100.207 - нижнее значение диапазона ip адресов источников трафика (т.к. srcaddrcmp равен eq, верхнее можно не указывать)
dstaddrcmp any - ip адрес назначения любой
ipsrcaddrmask 0xffffffff - маска источника 255.255.255.255

$create filter rule entry ruleid 3 action drop

Создаем правило, запрещающее весь остальной трафик.

$create filter subrule ip ruleid 3 subruleid 1 srcaddrcmp any dstaddrcmp any

Подправило, задающее весь трафик.

$create filter rule map ifname eoa-23 stageid 1 ruleid 2
$create filter rule map ifname eoa-23 stageid 1 ruleid 3

Применяем ранее созданные правила к конкретному интерфейсу (eoa-xx, eth-x)

$modify filter rule entry ruleid 2 status enable
$modify filter rule entry ruleid 3 status enable

Включаем фильтр в работу

4.Фильтр для привязки IP адреса к adsl порту (ATM PVC) при использовании авторизации пользователя по технологии PPPoE.

Пояснение: Данное правило позволяет реализовать жесткую привязку IP адреса к порту DSLAM для технологии доступа PPPoE, что может быть полезно при использовании на клиентских устройствах ADSL авторизации PPPoE.
Хотя сам DSLAM не проводит авторизацию PPPoE (данная проверка осуществляется на BRAS- PPPoE сервере), но при использовании этого правила пользователь будет блокирован при использовании чужих авторизационных данных для данной линии (порту DSLAM).

Каким образом это достигается:
PPPoE-BRAS сервер настраивается на полное взаимное соответствие учетных данных PPPoE определенному IP адресу (то есть, BRAS сервер однозначно «привязывает» учетную запись к выдаваемому по технологии PPPoE IP адресу).
Таким образом, за счет привязки IP адреса к порту на DSLAM и IP адреса к учетной записи PPPoE на сервере, как бы реализуется «привязка» учетных данных к порту DSLAM.То есть, пользователь не может входить под «чужой» учетной записью на данном порту DSLAM. Обращаем внимание, что блокировка осуществляется не в период PPPoE авторизации, а сразу после нее при попытке передачи пользовательских данных.

Правило:

$create filter rule entry ruleid 4 action drop statsstatus enable

Создаем запрещающее правило для всех «неправильных» ip адресов:
action drop - отбрасывать пакеты

$create filter subrule ip ruleid 4 subruleid 1 srcipaddrfrom 11.22.33.44 ipsrcaddrmask 0xFFFFFFFF srcaddrcmp neq transportHdr ethernet pppoe

Создаем подправило, в котором указываем, что нас интересует трафик от хоста 11.22.33.44 переданный только по технологии pppoe :
ruleid 4 subruleid 1 - первое подправило второго правила
srcipaddrfrom 11.22.33.44 - нижнее значение диапазона ip адресов источников трафика (т.к. srcaddrcmp равен neq, верхнее можно не указывать)
dstaddrcmp neq - ip адрес назначения любой, не равный заданому выше;
ipsrcaddrmask 0xffffffff - маска источника 255.255.255.255
transportHdr ethernet PPPoE **-** анализ ведется внутри пакета pppoe

$modify filter rule entry ruleid 4 status enable
Включаем правило в работу
$create filter rule map ifname eoa-0 stageid 1 ruleid 4
Привязываем првило к интерфейсу.

5.Использование Generic List в IP-ARP ACL без применения логических выражений.

Пояснение: Данное правило может использовтся для фильтрации нежелательных IP адресов на ADSL интерфейсах. Причем правило является универсальным, то есть работает как для статического присвоения адресов клиентам, так и для технологии PPPoE.

Создать Generic List «черных» адресов, пакеты от которых должны быть отброшены.
$create filter list genentry ifname eoa-0 value 0x11223344
$create filter list genentry ifname eoa-0 value 0x55667788

Создать фильтрующее правило Generic Filter
$create filter rule entry ruleid 1 action drop

Создать подправило анализа заголовка пакета
$create filter subrule ip ruleid 1 subruleid 1 srcaddrcmp ingenlist transportHdr ethernet pppoe
Включить правило в работу
$modify filter rule entry ruleid 1 status enable
Создать 2 правило для отбрасывания ARP пакетов
$create filter rule entry ruleid 2 action drop

$create filter subrule arp ruleid 2 subruleid 1 srcaddrcmp ingenlist
Включить правило в работу
$modify filter rule entry ruleid 2 status enable
Выставить порядок обработки правил
$create filter rule map ifname eoa-0 stageid 1 ruleid 1 orderid 1
$create filter rule map ifname eoa-0 stageid 1 ruleid 2 orderid 2

6.Использование Generic List в IP-ARP ACL с применением логических выражений.

Пояснение: Данное правило представляет собой модификацию предыдущего **с применением логических выражений.**

Создать Generic List «черных» адресов, пакеты от которых должны быть отброшены.
$create filter list genentry ifname eoa-0 value 0x11223344
$create filter list genentry ifname eoa-0 value 0x55667788

Определить логическое выражение
$create filter expr entry exprid 1 exprstring "(1|2):drop"

Применить логическое выражение к правилу
$create filter rule entry ruleid 1 action exprdef exprid 1

Создать подправило анализа заголовка пакета
$create filter subrule ip ruleid 1 subruleid 1 srcaddrcmp ingenlist transportHdr ethernet pppoe

Создать подправило для фильтрации ARP
$create filter subrule arp ruleid 1 subruleid 2 srcaddrcmp ingenlist

Включить правило в работу
$modify filter rule entry ruleid 1 status enable

Ассоциировать правило с интерфейсом
$create filter rule map ifname eoa-0 stageid 1 ruleid 1 orderid 1

7. FTP filter.

$create filter rule entry ruleid 10 action drop ruledir in

Создаем главное правило:
action drop - отбрасывать
ruledir in – направление действия правила относительно интерфейса.

$create filter subrule tcp ruleid 10 subruleid 1 dstportfrom 21 dstportto 23 srcportcmp any dstportcmp inrange subruleprio high

Создаем подправило, в котором указываем, что нас интересуют обращения на TCP порты с 21 по 23.
ruleid 10 subruleid 1 – первое подправило десятого правила
dstportfrom 21 – нижнее значение диапазона портов – получателей
dstportto 23 – верхнее значение диапазона портов – получателей
srcportcmp any – порт источника любой
dstportcmp inrange – любой порт назначения из диапазона 21-23
subruleprio high – приоритет подправила

$create filter rule map ifname eoa-0 stageid 1 ruleid 10

Применяем ранее созданные правила к конкретному интерфейсу (eoa-xx, eth-x)

$modify filter rule entry ruleid 10 status enable

Включаем фильтр в работу

8. HTTP filter

$create filter rule entry ruleid 11 action drop ruledir in

Создаем главное правило:
action drop - отбрасывать
ruledir in – правило для входящего интерфейса (ingress).

$create filter subrule tcp ruleid 11 subruleid 1 dstportfrom 80 srcportcmp any dstportcmp inrange subruleprio high

Создаем подправило, в котором указываем, что нас интересуют обращения на 80 TCP порт.
ruleid 11 subruleid 1 – первое подправило одиннадцатого правила
dstportfrom 80 – нижнее значение диапазона портов – получателей
srcportcmp any – порт источника любой
dstportcmp inrange – любой порт назначения из диапазона (в данном случае 80 порт)
subruleprio high – приоритет подправила

$create filter rule map ifname eoa-0 stageid 1 ruleid 11

Применяем ранее созданные правила к конкретному интерфейсу (eoa-xx, eth-x)

$modify filter rule entry ruleid 11 status enable

Включаем фильтр в работу

9.PPTP filter

Задача : Фильтровать PPTP пакеты

$ create filter rule entry ruleid 23 action drop statsstatus enable ruledir out ruleprio high

Создаем главное правило:
action drop - отбрасывать
statsstatus enable – включение сбора статистики по правилу
ruledir in – правило для входящего интерфейса (ingress).

$ create filter subrule tcp ruleid 23 subruleid 1 srcportfrom 1723 srcportcmp eq dstportcmp any subruleprio asinrule

Создаем подправило, в котором указываем, что нас интересуют обращения с 1723 TCP порта.
ruleid 23 subruleid 1 – первое подправило двадцать третьего правила
srcportfrom 1723 – нижнее значение диапазона портов источника
srcportcmp eq – эквивалент 1723 порта
dstportcmp any – любой порт назначения
subruleprio high – приоритет подправила

$ create filter rule map ifname eoa-22

Применяем созданное правило к конкретному интерфейсу (eoa-xx, eth-x)

$ modify filter rule entry ruleid 23 status enable

Включаем фильтр в работу

10.PPPoE filter

Задача : Фильтровать PPPoE пакеты

$ create filter rule entry ruleid 24 action drop statsstatus enable ruleprio high

Создаем главное правило:
action drop - отбрасывать
statsstatus enable – включение сбора статистики по правилу

$ create filter subrule ether ruleid 24 subruleid 1 ethertypefrom 0x8863 ethertypecmp eq subruleprio asinrule

Создаем подправило, в котором указываем, что нас интересуют все PADI пакеты протокола PPPoE.
ruleid 23 subruleid 1 – первое подправило двадцать третьего правила
ethertypefrom 0x8863 – нижнее значение типа протокола
ethertypecmp – эквивалент 0x8863 типа протокола
subruleprio asinrule – приоритет как у правила

$ create filter rule map ifname eoa-22 stageid 1 ruleid 24

Применяем созданное правило к конкретному интерфейсу (eoa-xx, eth-x)

$ modify filter rule entry ruleid 24 status enable

Включаем фильтр в работу

11.Non PPPoE filter .

Задача : Фильтровать все не PPPoE пакеты
1. Требуется чтобы в обе стороны проходили только ethertype 0x8863 и 0x8864 - т.е. ТОЛЬКО PPPoE трафик.
2. В сторону клиента блокировать широковещательный трафик
Разрешаем все пакеты с Ethertype 0x8863 и 0x8864 от клиентов:

Запрещаем весь остальной трафик (по Ethertype) от клиентов:
$ create filter rule entry ruleid 23 action allow ruleprio high ruledir in

$ create filter subrule ether ruleid 23 subruleid 1 ethertypefrom 0x8863 ethertypeto 0x8864 ethertypecmp inrange subruleprio asinrule

Создаем подправило, в котором указываем, что нас интересуют все пакеты протокола PPPoE.
ruleid 23 subruleid 1 – первое подправило двадцать третьего правила
ethertypefrom 0x8863 – нижнее значение типа протокола
ethertypefrom 0x8864 – верхнее значение типа протокола
ethertypeinrange – эквивалент 0x8863 типа протокола
subruleprio asinrule – приоритет как у правила

$ create filter rule map ruleid 23 stageid 1 ifname alleoa
Применяем правило ко всем интерфейсам eoa (alleoa)
$ modify filter rule entry ruleid 23 status enable
Включаем правило в работу

$ create filter rule entry ruleid 24 action drop ruledir out pkttype bcast status enable
Запрещаем весь Broadcast трафик в сторону клиентов

$ create filter rule map ruleid 24 stageid 1 ifname alleoa
Включаем фильтр в работу для всех интерфейсов eoa

Приложение D: Настройка некоторых функций DAS-3248 посредством SNMP запросов.

Для всех примеров:
IP DSLAMa -192.168.0.1
snmp RW community string - public

1.Индексы интерфейсов на DAS-3248

snmpwalk -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.2

В результате будет выведены интерфейсы и их индексы (будут использоваться в последующих примерах):

Интерфейсы "eth", индексы интерфейсов с 1 по 3
Интерфейсы "dsl", индексы интерфейсов с 6 по 53
Интерфейсы "atm", индексы интерфейсов с 150 по 197
Интерфейсы "aal5", индексы интерфейсов с 198 по 581
Интерфейс "ppp", индекс интерфейса 582
Интерфейсы "eoa", индексы интерфейсов с 391 по 774
Интерфейсы "dsli", индексы интерфейсов с 54 по 101
Интерфейсы "dslf", индексы интерфейсов с 102 по 149

Оперативный статус интерфейсов
snmpwalk -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.8

Счетчики интерфейсов :
snmpwalk -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.10 – Входящие пакеты (ifInOctets)
snmpwalk -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.16- Исходящие пакты (ifOutOctets)

1.Применение основных системных действий на DAS-3224/3248 посредством SNMP запроса.

Примечание: для всех примеров Read-write SNMP community string – public
IP адрес DSLAM – 192.168.0.1

Задача: Перезагрузка устройства (горячий рестарт)
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.6.6.2.0 i 2**

Задача: Сохранение всех настроек в энергонезависимой памяти (NVRAM).
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.6.6.4.0 i 2**

Задача: Изменение режима коммутации глобально (на всем устройстве) на Unrestricted
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.6.2.15.0 i 2**
Объяснение**:** Значения приведенного OID следующие 1-Restricted, 2-Unrestricted, 3-Residential.

2.Изменение параметров VPI, VCI на DAS-3224/3248 посредством SNMP запроса.

Задача: Изменить VPI интерфейса AAL5-0 на 40, VCI на 10. IP адрес устройства для простоты возьмем 192.168.0.1. Comminity string- public.

Команды:

snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.198 i 2
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.1.5.1.2.198 i 40
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.198 i 1

snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.198 i 2
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.1.5.1.2.198 i 10
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.198 i 1

Объяснение:
Индексы AAL-5 интерфейсов на устройстве начинаются с 198.Таким образом, интерфейс AAL5-0 соответствует ifIndex-198, AAL5-1-199 и.т.д.

Изменение параметров VPI и VCI для каждого интерфейса производится раздельно.
Первые три приведенных команды изменяют VPI ,вторые- VCI.
В каждой группе первая из трех команд административно выключает интерфейс, вторая меняет необходимое значение, третья вновь вводит интерфейс в работу.

3.Изменение параметров Ethernet интерфейсов для DAS-3224/3248 посредством SNMP.

Задача 1: Изменить IP адрес, маску подсети и значение управляющего VLAN для интерфейса Uplink1(eth-0)

Команда:

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.4.2.1.2.1 a 192.168.7.2
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.4.2.1.3.1 a 255.255.255.0
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.4.2.1.13.1 i 1

Объяснение: Первая команда меняет IP адрес Uplink 1(eth-0) на 192.168.7.2. Вторая - команда меняет маску подсети. Третья- управляющий VLAN (это значение по умолчанию равно 0).
Примечание: для интерфейса Uplink 2(eth-1) последняя цифра всех OID меняется на 2 (например, **1.3.6.1.4.1.171.10.65.1.4.2.1.2.2),** для интерфейса MGNT(eth-2)-на 3, (например, **1.3.6.1.4.1.171.10.65.1.4.2.1.2.3**)

Задача 2: Изменить параметры порта Uplink1 (дуплекс с Auto на FullDuplex и скорость порта жестко на 100).
Команда:
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.4.2.1.8.1 i 3
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.4.2.1.4.1 i 2

Объяснение:
1.3.6.1.4.1.171.10.65.1.4.2.1.8.1 i 3- меняет дуплекс порта на Full (значения OID: 1-Auto,2-Half Duplex, 3-Ful Duplex).
1.3.6.1.4.1.171.10.65.1.4.2.1.4.1 i 2- меняет скорость порта на 100Мбит/с (значения OID: 0-auto,1-10,2-100,3-1000).

4.Создание и удаление VLAN на DAS-3248 посредством SNMP запроса.

Задача 1: Создать VLAN с VID=5 и включить в него 1 порт как Untagged, порт Uplink 1-как Tagged. Портам Untagged присвоить PVID=VID.
Внимание: Соответствующие порты (1,385) должны быть до этого момента удалены из default VLAN.

Команда:
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.3.8.1.2.5 s dlink
1.3.6.1.4.1.171.10.65.1.3.8.1.3.5 x
010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
1.3.6.1.4.1.171.10.65.1.3.8.1.4.5 x
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
1.3.6.1.4.1.171.10.65.1.3.8.1.5.5 x
010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
1.3.6.1.4.1.171.10.65.1.3.8.1.6.5 i 1
1.3.6.1.4.1.171.10.65.1.3.8.1.7.5 i 1
1.3.6.1.4.1.171.10.65.1.3.8.1.8.5 i 1
1.3.6.1.4.1.171.10.65.1.3.8.1.10.5 i 4

snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.17.7.1.4.5.1.1.1 i 5

Объяснение:
1) Последняя цифра всех OID задает VID для создаваемого VLAN.

2) **1.3.6.1.4.1.171.10.65.1.3.8.1.2.5 s dlink –**Задаем имя VLAN для VID=5

3) **1.3.6.1.4.1.171.10.65.1.3.8.1.3.5 x**
010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001 –Задаем членство портов в VLAN. Всего шестнадцатеричных разрядов 98 (48 портов/8*8 PVC*2). Установленный бит в октете означает членство данного порта в VLAN.
Каждые два разряда данного шестнадцатеричного параметра обозначают 8 портов. Порты идут по возрастанию от младших к старшим. Это означает, что для 1 порта – членство в VLAN означает значение 01 соответствующих разрядов, для второго -02, для третьего -04…для восьмого порта-80.
Соответствующие биты складываются (то есть членство 1 и 3 порта - 01+04=05 первых двух разрядов). Всего для 1 PVC все порты используются только 12 первых разрядов шестнадцатеричного значения (членство всех портов в VLAN будет выглядеть как FFFFFFFFFFF00…..)
Разряды последних 97 и 98 разрядов обозначают порты Uplink: (для Uplink1-01 Uplink2-02, для MGNT-04)

4) **1.3.6.1.4.1.171.10.65.1.3.8.1.4.5 x**
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 – Задает порты, которые не могут быть добавлены в данный VLAN (Forbinden порты)

5) **1.3.6.1.4.1.171.10.65.1.3.8.1.5.5 x 010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 –**Задает порты, являющиеся Untagged в данном VLAN. Установленный бит в каждом октете означает Untagged порт.

6) **1.3.6.1.4.1.171.10.65.1.3.8.1.6.5 i 1 –**задает режим коммутации данного VLAN (1-Restricted, 2-Unrestricted, 3-Residental)

7) **1.3.6.1.4.1.171.10.65.1.3.8.1.7.5 i 1** – включение функции Flood support для данного VLAN (0-выключение)

8) **1.3.6.1.4.1.171.10.65.1.3.8.1.8.5 i 1 -** включение функции Broadcast support для данного VLAN (0- выключение)

9) **1.3.6.1.4.1.171.10.65.1.3.8.1.10.5 i 4 –** Создание VLAN с вышеуказанными параметрами

10) **snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.17.7.1.4.5.1.1.1 i 5-** Присвоение 1 порту PVID=5

Примечание: изменение параметров существующего VLAN производится с помощью тех же OID.
Однако отличием изменения параметров существующего VLAN от создания нового является, то, что в изменении участвуют не все перечисленные, а **только** те OID, состояние параметров которых меняется.

Задача 2: Удалить VLAN с VID=5.
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.3.8.1.10.5 i 6**

5.Управление функцией IGMP Snooping на DAS-3224/3248 посредством SNMP запроса.

Задача 1: Глобальное включение функции IGMP Snooping.
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.8.1.6.0 i 1**
Объяснение: Значение 1 вышеуказанного OID соответствует включению функции, 0-выключению.

Задача 2: Включение функции IGMP Snooping на отдельном порту (на первом порту)
Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.8.2.1.2.1 i 1**
Объяснение: Последняя цифра OID должна соответствовать номеру Bridge интерфейса (для первого порта -1). Значение OID: 1-включение функции,0-выключение.

5.Управление параметрами ADSL профиля линии посредством SNMP запроса.

Задача 1: Изменить параметры DSL профиля 1 dsl порта (dsl-0). Режим порта Interleave.

Примечание 1:Индексы DSL портов начинаются с 6.

Примечание 2: Перед изменением параметров профиля обязательно выключение порта dsl. После изменения - обратное включение порта в работу.

Примечание 3 :Последние два октета OID параметров профиля порта dsl изменяют с ростом номера порта dsl, начиная со значения 48.Т.е последний октет увеличивается на единицу, начиная со значения 48 для каждого порта. Для каждого восьмого порта значение увеличивается на единицу для предпоследнего октета.
Например: 1 порт (dsl-0) -48.54, 2- 48.55, 3- 48.56, 4- 48.57, 5- 49.48, 6- 49.49, 7- 49.50 8- 49.51, 9- 49.52, 10- 49.53, 11-49.54, 12-49.54, 13-49.55, 14-49.55, 15-49.56, 16-49.57 , 17-50.48 и так до 48- 53.51):

Команда:
s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 2** - Выключение порта DSL-0

snmpset -v2c -c public 192.168.0.1
1.3.6.1.4.1.171.10.65.1.2.11.1.3.48.48.48.48.48.48.48.48.48.48.54 i 3 –Тип линии (1-NoChannel,2-FastOnly,3-InterleaveOnly,4-FastorInterleave,5-FastandInterleave)

1.3.6.1.2.1.10.94.1.1.14.1.2.48.48.48.48.48.48.48.48.48.48.54 i 2 –Режим выбора скорости порта для Downstream потока (1-Фиксированная скорость, 2-Адаптивная настройка скорости)
1.3.6.1.2.1.10.94.1.1.14.1.16.48.48.48.48.48.48.48.48.48.48.54 i 2 - Режим выбора скорости порта для Upstream потока (1-Фиксированная скорость, 2-Адаптивная настройка скорости)

1.3.6.1.2.1.10.94.1.1.14.1.12.48.48.48.48.48.48.48.48.48.48.54 u 32000 –Минимальная скорость Downstream потока (бит/с)
1.3.6.1.2.1.10.94.1.1.14.1.14.48.48.48.48.48.48.48.48.48.48.54 u 12000000 - Максимальная скорость Downstream потока (бит/с)

1.3.6.1.2.1.10.94.1.1.14.1.26.48.48.48.48.48.48.48.48.48.48.54 u 32000 - Минимальная скорость Upstream потока (бит/с)
1.3.6.1.2.1.10.94.1.1.14.1.28.48.48.48.48.48.48.48.48.48.48.54 u 64000 - Максимальная скорость Upstream потока (бит/с)

1.3.6.1.2.1.10.94.1.1.14.1.15.48.48.48.48.48.48.48.48.48.48.54 i 63 –Максимальное время задержки интерливинга для Downstream потока (ms)
1.3.6.1.2.1.10.94.1.1.14.1.29.48.48.48.48.48.48.48.48.48.48.54 i 63 -Максимальное время задержки интерливинга для Upstream потока (ms)
1**.3.6.1.4.1.171.10.65.1.2.11.1.2.48.48.48.48.48.48.48.48.48.48.54 i 3** –Интервал коррекции интерливинга для Upstream потока (IntCorrection Up)(3-125mks,4-250,5-500,6-1ms,7-2ms,8-4ms)
1.3.6.1.4.1.171.10.65.1.2.11.1.16.48.48.48.48.48.48.48.48.48.48.54 i 3- Интервал коррекции интерливинга для Upstream потока (IntCorrection Down)(3-125mks,4-250,5-500,6-1ms,7-2ms,8-4ms)

s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 1** - Включение порта DSL-0

Задача 2: Изменить параметры DSL профиля 1 dsl порта (dsl-0). Режим порта Fast.

Команда:
s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 2** - Выключение порта DSL-0

snmpset -v2c -c public 192.168.0.1
1.3.6.1.4.1.171.10.65.1.2.11.1.3.48.48.48.48.48.48.48.48.48.48.54 i 2 –Тип линии (1-NoChannel,2-FastOnly,3-InterleaveOnly,4-FastorInterleave,5-FastandInterleave)

1.3.6.1.2.1.10.94.1.1.14.1.2.48.48.48.48.48.48.48.48.48.48.54 i 2 - Режим выбора скорости порта для Downstream потока (1-Фиксированная скорость, 2-Адаптивная настройка скорости)
1.3.6.1.2.1.10.94.1.1.14.1.16.48.48.48.48.48.48.48.48.48.48.54 i 2 - Режим выбора скорости порта для Upstream потока (1-Фиксированная скорость, 2-Адаптивная настройка скорости)

1.3.6.1.2.1.10.94.1.1.14.1.11.48.48.48.48.48.48.48.48.48.48.54 u 128000 - Минимальная скорость Downstream потока (бит/с)
1.3.6.1.2.1.10.94.1.1.14.1.13.48.48.48.48.48.48.48.48.48.48.54 u 12000000 - Максимальная скорость Downstream потока (бит/с)
1.3.6.1.2.1.10.94.1.1.14.1.25.48.48.48.48.48.48.48.48.48.48.54 u 32000 - Минимальная скорость Upstream потока (бит/с)
1.3.6.1.2.1.10.94.1.1.14.1.27.48.48.48.48.48.48.48.48.48.48.54 u 64000 - Максимальная скорость Upstream потока (бит/с)

1.3.6.1.4.1.171.10.65.1.2.11.1.15.48.48.48.48.48.48.48.48.48.48.54 i 1-Избыточность данных для увеличения помехозащищенности для Downstream потока (15-disable,1-50%,2-25%.3-12%,4-6%,5-3%,7-1%)
1**.3.6.1.4.1.171.10.65.1.2.11.1.17.48.48.48.48.48.48.48.48.48.48.54 i 1**- Избыточность данных для увеличения помехозащищенности для Upstream потока (15-disable,1-50%,2-25%.3-12%,4-6%,5-3%,7-1%)

s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 1** - Включение порта DSL-0

6.Управление параметрами модуляции ADSL порта посредством SNMP запроса.

Задача 1: Изменить параметры модуляции первого DSL порта на ADSL2+.

В данный набор модуляций входят значения q9925Adsl2PlusPotsOverlapped и q9925Adsl2PlusPotsNonOverlapped параметра LineTransAtucConfig (см Раздел 3.3). Соединения только этих типа модуляций ADSL будут приниматься, остальные отвергаться.

Примечание 1:Индексы DSL портов -с 6 по 53. Интерфейсы "dsli", индексы интерфейсов с 54 по 101 .Интерфейсы "dslf", индексы интерфейсов с 102 по 149

Примечание 2: Перед изменением параметров профиля обязательно выключение порта dsl. После изменения - обратное включение порта в работу.

Команда:
s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 2** - Выключение порта DSL-0

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.2.10.1.11.6 x 0000003000000000 – Тип модуляции.

s**nmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.6 i 1** - Включение порта DSL-0

Пояснение: Всего на модуляцию отводится одно 16 разрядов число. Значения для набора модуляций суммируются поразрядно. Значение по умолчанию (все типы): **A00001180000008C**

Описание типа модуляции	**Значение параметра LineTransAtucConfig**	**Значение SNMP OID**
ADSL ANSI T1.1413	ansit1413	8000000000000000
Не используются в данном типе устройств	etsi	
ADSL G.Dmt	q9921PotsNonOverlapped	2000000000000000
ADSL G.Dmt	q9921PotsOverlapped	1000000000000000
ADSL Annex B (**только для DAS-3224/BE)**	q9921IsdnNonOverlapped	0800000000000000
ADSL Annex B (**только для DAS-3224/BE)**	q9921IsdnOverlapped	0400000000000000
Не используются в данном типе устройств	q9921tcmIsdnNonOverlapped q9921tcmIsdnOverlapped	
G.Lite	q9922potsNonOverlapeed	0080000000000000
G.Lite	q9922potsOverlapped	0040000000000000
Не используются в данном типе устройств	q9922tcmIsdnNonOverlapped q9922tcmIsdnOverlapped q9921tcmIsdnSymmetric q9921GspanPlusPotsNonOverlapped	

	q9921GspanPlusPotsOverlapped	
ADSL 2	q9923Adsl2PotsOverlapped	0000000400000000
ADSL 2	q9923Adsl2PotsNonOverlapped	0000000800000000
ADSL 2+	q9925Adsl2PlusPotsOverlapped	0000001000000000
ADSL 2+	q9925Adsl2PlusPotsNonOverlapped	0000002000000000
READSL 2	q9923Readsl2PotsOverlapped	0000020000000000
READSL 2	q9923Readsl2PotsNonOverlapped	0000010000000000
Не используются в данном типе устройств	adslPlusPotsOverlapped adslPlusPotsNonOverlapped	
Не используются в данном типе устройств	q9921GspanPlusPlusPotsNonOverlapped q9921GspanPlusPlusPotsOverlapped	
ADSL2 Annex B **(только для DAS-3224/BE)**	q9923IsdnNonOverlapped	0000000020000000
ADSL2 Annex B (**только для DAS-3224/BE)**	q9923IsdnOverlapped	0000000010000000
ADSL2+ Annex B **(только для DAS-3224/BE)**	q9925IsdnNonOverlapped	0000000000200000
ADSL2+ Annex B **(только для DAS-3224/BE)**	q9925IsdnOverlapped	0000000000100000
ADSL 2 Annex M	q9923AnnexMPotsExtUsNonOverlapped	0000000000000080
ADSL 2 Annex M	q9923AnnexMPotsExtUsOverlapped	0000000000000040
ADSL 2+ Annex M	q9925AnnexMPotsExtUsNonOverlapped	0000000000000008
ADSL 2+ Annex M	q9925AnnexMPotsExtUsOverlapped	0000000000000004

7.Получение текущих значений параметров ADSL линии.

а) Текущее значение модуляции ADSL, на котором произошло соединение ADSL после его установления (параметр TransAturActual) можно получить через команду:

snmpget -v2c -c public 192.168.0.1 1.3.6.1.4.1.171.10.65.1.2.10.1.5.6

б) Текущая скорость (AturCurrTxRate) (индекс интерфейса dsli-0)
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.4.1.2.54
(ATUC-для Upstream направления)
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.5.1.2.54
(ATUR-для Downstream направления)

в) Текущий сигнал/шум (Curr SNR margin):
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.2.1.4.6
(ATUC-для Upstream направления)

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.3.1.4.6
(ATUR-для Downstream направления)

г) Текущее затухание на линии (CurrAtn):
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.2.1.5.6
(ATUC-для Upstream направления)

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.3.1.5.6
(ATUR-для Downstream направления)

д) Ошибки на ADSL линии

ATUC LoFS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.1.6

ATUR LoFS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.1.6

ATUC LoSS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.2.6

ATUR LoSS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.2.6

ATUC LoLS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.3.6

ATUR LoLS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.3.6

ATUC LPRS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.4.6

ATUR LPRS
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.4.6

ATUC ES
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.5.6

ATUR ES
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.5.6

ATUC Inits
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.6.6

ATUR Inits
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.6.6

ATUC Valid Intervals
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.7.6

ATUR Valid Intervals
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.7.6

ATUC Invalid Intervals
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.8.6

ATUR Invalid Intervals
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.8.6