

DAS-3216/3224/3248

Hardware revision B1

IP DSLAM

Руководство пользователя

Rev.2.42(Aug. 2008)



RECYCLABLE

Содержание:

Содержание:	2
Предисловие.....	6
История версий документа.	6
Функциональные возможности DAS-3248.....	7
1. Начальная настройка DAS-3248	9
1.1. Обзор и внешний вид устройства	9
1.2. Способы конфигурирования DAS-3248.....	12
1.3. Настройка параметров IP-интерфейса.....	14
1.3.1. Настройка IP-адреса и маски подсети	15
1.3.2. Настройка управляющего VLAN (Management VLAN)	18
1.4. Настройка синхронизации времени.....	19
1.5. Настройка таблицы маршрутизации	22
1.6. SNMP управление	25
1.6.1. Обзор протокола SNMP	25
1.6.2. Настройка SNMP	28
1.6.3. Remote Monitoring (RMON)	36
1.7. Сохранение конфигурации	40
1.7.1. Виды конфигурационных файлов.....	40
1.7.2. Сохранение конфигурационных файлов на tftp сервере	40
1.8. Вспомогательные команды CLI интерфейса.	41
2. Логическая структура DAS-3248	43
2.1. Структура стека интерфейсов DAS-3248	43
2.2. Файловая структура ОС DAS-3248. Операции с ПО и конфигурациями.	46
2.2.1. Структура внутренней ОС DAS-3248.	46
2.2.2. Порядок загрузки DSLAM. Расположение основных системных файлов.....	47
2.2.3. Каталоги внутренней файловой системы.....	49
2.2.4. Команды работы с файлами.	50
2.2.5. Отображение информации о программном обеспечении. Команды управления загрузкой.....	53
2.2.6. Операции с конфигурациями. Типовые сценарии.....	55
2.2.7. Создание, загрузка и применение скриптового файла команд.....	56
2.2.8. Операции с программным обеспечением. Типовые сценарии.	57
2.2.9. Автоконфигурирование DAS-3248.	58
2.2.10. Удаленная замена ПО устройства.	61
3. Настройка DSL-линий.	63
3.1. Теория и сущность технологии ADSL	63
3.2. Включение/выключение ADSL- порта.....	71
3.4. Использование глобальных DSL-профайлов.....	74
3.5. Включение ATM local loopback.....	78
3.6. Просмотр параметров линии DSL. Оценка параметров линии.	80
3.6.1. Команды просмотра физических параметров линии	80
3.6.2. Команды просмотра параметров буфера канала.....	84
3.6.3. Команды просмотра качества канала	84
3.6.4. Оценка параметров линии по результатам выполненных команд	85
3.7. Параметрические тесты DSL линии.	88

3.7.2. Single End Loop Test (SELT)	88
3.7.1. Dual End Loop Test (DELT)	88
4. Инкапсуляции ATM/AAL5. Настройка стека протоколов на DAS-3248.	92
4.1. Интерфейсы ATM.	98
4.2. Интерфейсы AAL5.	100
4.2.1. Создание, настройка и удаление интерфейса AAL5.	100
4.3. RFC1483 Bridged. (Ethernet over ATM).....	104
4.3.1. Создание, настройка и удаление интерфейса EoA	106
4.3.2. Создание, настройка и удаление bridge порта	108
4.4. Point-to-Point over ATM (PPPoA)	113
4.4.1. Описание и особенности реализации PPPoA to PPPoE internetworking.....	114
4.4.2. Создание, настройка и удаление интерфейса PPPoA Relay	117
4.4.3. Создание, настройка и удаление интерфейса PPPoE	120
4.4.4. Создание, настройка и удаление bridge-порта	123
4.4.5. Пример настройки PPPoA to PPPoE internetworking.....	123
4.5. IP over ATM	125
4.5.1. Описание IPoA to IPoE internetworking.....	126
4.5.2. Основные понятия IPoA to IPoE Tunneling.....	127
4.5.3. Конфигурирование стека интерфейсов IPoA to IPoE Tunneling.	130
4.5.4. Создание, настройка и удаление интерфейса IPoA	131
4.5.5. Создание, настройка и удаление интерфейса IPoE	132
4.5.6. Создание, настройка и удаление bridge-порта на клиентской стороне.....	135
4.5.7. Создание, настройка и удаление bridge-порта на WAN стороне.....	135
4.5.8. Логика работы и конфигурирование Upstream потока в IPoA to IPoE Tunneling..	136
4.5.9. Логика работы и конфигурирование Downstream потока в IPoA to IPoE Tunneling.	140
4.5.10. Логика работы и конфигурирование Proxy ARP в IPoA to IPoE Tunneling.	141
4.5.11. Пример настройки IPoA to IPoE internetworking	144
5. Дополнительные возможности технологий доступа в сетях ADSL	146
5.1. Виды технологий доступа в сетях ADSL	146
5.2. Функция DHCP option 82 (DHCP Relay Agent).	148
5.2.1. Сущность функции DHCP option 82.....	148
5.2.2. Синтаксис команд DHCP option 82 на DAS-3248.....	149
5.2.3. Пример настройки функции DHCP option 82.....	153
5.3. Функция PPPoE Intermediate Agent.	161
5.3.1. Сущность функции PPPoE Intermediate Agent.....	161
5.3.2. Синтаксис команд PPPoE Intermediate Agent	162
5.3.3. Пример настройки PPPoE Intermediate Agent.	165
6. Настройка Uplink Интерфейсов.....	169
6.1. Типы Uplink Интерфейсов.	170
6.2. Настройка скорости/дуплекса.....	172
6.3. Стекирование DAS-3248.	174
7. Способы передачи пакетов	176
7.1. Понятие передачи пакетов. Типы передачи	176
7.2. Настройка функций, связанных с передачей данных.....	177
7.2.1. Таблица коммутации. Port Security.....	177
7.3. Виртуальные локальные сети в DAS-3248	178
7.3.2. Создание, настройка и удаление Static VLAN	179
7.3.3. Настройка GVRP	184
7.4. Стекирование VLAN. Технология Q-in-Q.	186
7.4.1. Использование Q-in-Q. Типовые сценарии.	187
7.4.2. Реализация Q-in-Q на DAS-3248.	189

7.4.3. Приоритезация трафика с Использованием Q-in-Q.....	193
7.4.4. Порядок обработки потока данных при использовании Q-in-Q.....	194
7.4.5.VLAN транкинг (VLAN Trunk).Особенности и ограничения применения услуги E-line.....	197
7.4.6.Совместимость Q-in-Q с другими технологиями, использованными в DAS-3248..	197
7.4.7. Настройки Q-in-Q по умолчанию.....	201
7.4.8. Типовые сценарии Q-in-Q. Примеры использования.....	201
7.5.Групповая рассылка (IGMP Snooping).....	204
7.5.1. Концепция IGMP Snooping.....	205
7.5.2. Особенности реализации IGMP Snooping в DAS-3248.....	206
7.5.3. Настройка IGMP Snooping.....	216
7.5.4. Фильтрация Multicast потоков.....	217
7.5.5. Использование Multicast VLAN Registration (MVLAN Registration).....	218
8.Протокол Spanning Tree.....	221
8.1.Понятие протокола STP (IEEE 802.1D).....	221
8.2.Понятие протокола RSTP (IEEE 802.1w).....	227
8.3.Настройка протокола STP на DAS-3248.....	233
8.4.Настройка протокола RSTP на DAS-3248.....	236
9.Настройка пакетных фильтров.....	239
9.1.Generic Filter.....	239
9.1.1.Общие принципы.....	241
9.1.2.Многоэтапная обработка пакетов.....	245
9.1.3.Несколько действий одного правила (Action Map).....	246
9.1.4.Быстрое изменение последовательности правил.....	246
9.1.5.Обработка логических выражений.....	247
9.1.6. Обработка пакетов в Control Plane.....	248
9.1.7. Расширенные принципы фильтрации. Generic List и.....	250
9.1.8.Примеры использования Generic Filter.....	251
9.2. Access Control List в DAS-3248.....	252
9.2.1.Примеры использования Global ACL.....	252
9.2.2.Пример использования Per Port ACL.....	253
10.Настройка QoS на DAS-3248.....	254
10.1.Теория качества обслуживания (QoS).....	254
10.1.1.Современные требования к качеству обслуживания.....	254
10.1.2.Дисциплины очередей.....	254
10.1.3.Алгоритмы ограничения полосы пропускания.....	258
10.2.Настройки QoS на DAS-3248.....	261
10.2.1.Управление приоритетами и очередями. Scheduling profiles.....	261
10.2.2.Пример конфигурирования QoS на основе Shedulling профилей.....	262
10.2.3.Контроль полосы пропускания по потокам. Flow Based Rate Limiting.....	263
10.2.4.Контроль полосы входного потока (IRL).....	271
10.2.5.Контроль полосы выходного потока (ORL).....	272
10.2.6. Профили очередей (Traffic Class Profile).....	273
11.Упрощенный командный (CLI) режим. Применение. Примеры.....	275
11.1.Назначение упрощенного (пользовательского) командного режима. Принципы и основные команды.....	275
11.2.Дерево команд упрощенного командного режима.....	276
11.3.Синтаксис команд упрощенного командного режима.....	285
11.3.1. Аппаратные команды.....	285
11.3.2. Общие команды управления устройством.....	286
11.3.3. Команды работы с Uplink портами.....	291
11.3.4. Команды управления глобальными профилями DSL.....	293

11.3.5. Команды управления PVC	297
11.3.6. Команды управления VLAN	300
11.3.7. Диагностические команды.....	302
11.3.8. Команды просмотра и управления таблицей коммутации	303
11.3.9. Команды работы с MAC ACL	304
11.3.10. Команды работы с Alarm профилями.....	305
11.3.11. Команды работы с функциями PIA и DRA	310
11.3.12. Команды работы с функцией IGMP Snooping	313
11.3.13. Команды работы с RSTP протоколом	316
11.3.14. Команды просмотра статуса и статистики	319
11.3.15. Управление удаленным DSLAM	320
Приложение А: Соответствие контактов коннекторов TELCO-50 Amphenol портам DAS-3216/3224/3248	322
Приложение В: Внутренний аппаратный тест устройства (POST).....	326
Приложение С: Примеры конфигурирования Generic Filter	327
1.Фильтр для запрета icmp echoсообщений на определенном интерфейсе с определенного ip адреса.....	327
2. Пример анализа заголовка TCP пакета (TCP_SYN_filtering).....	328
3. Фильтр для привязки IP адреса к adsl порту (ATM PVC).....	329
4.Фильтр для привязки IP адреса к adsl порту (ATM PVC) при использовании авторизации пользователя по технологии PPPoE.....	330
5.Использование Generic List в IP-ARP ACL без применения логических выражений.....	331
6.Использование Generic List в IP-ARP ACL с применением логических выражений.....	332
7. FTP filter.	333
8. HTTP filter	334
9.PPTP filter	335
10.PPPoE filter.....	336
11.Non PPPoE filter	337
Приложение D: Настройка некоторых функций DAS-3248 посредством SNMP запросов.	338
1.Индексы интерфейсов на DAS-3248	338
2.Применение основных системных действий на DAS-3224/3248 посредством SNMP запроса.	338
3.Изменение параметров VPI, VCI на DAS-3224/3248 посредством SNMP запроса.	339
4.Изменение Output Rate Limit (ORL) на ATM на DAS-3224/3248 посредством SNMP запроса.	339
5.Изменение параметров Ethernet интерфейсов для DAS-3224/3248 посредством SNMP..	340
6.Изменение параметров VLAN на DAS-3248 посредством SNMP запроса.	341
7.Управление функцией IGMP Snooping на DAS-3224/3248 посредством SNMP запроса...343	
8.Создание и удаление глобального DSL профиля посредством SNMP запроса.	344
9.Получение текущих значений параметров ADSL линии.	346
12.Пример создания и удаления правила Generic Filter посредством SNMP запроса.	348
Приложение Е: Примеры комплексных конфигураций.....	350
1.Пример настройки DAS-3224 DSLAM для предоставления трех сервисов (Интернет, Voice и Видео) с использованием CLI режима	350
2.Пример настройки DAS3 series DSLAM для	350
предоставления трех сервисов (Интернет, Voice и Видео)	404
с использованием упрощенного CLI режима (usermode).	404

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 имеет 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+) и DAS-3216 (имеющего 16 портов ADSL/ADSL2+)

Везде, где для DAS-3248 сказано о 48 портах (интерфейсах), для DAS-3224 и DAS-3216 следует читать 24/16 портов (интерфейсов).

Примечание 2: Данное руководство справедливо **только** для внутреннего программного обеспечения версии **2.42 и выше** устройств **DAS-3216/24/48 HW Rev. B1**

История версий документа.

Номер версии	Описание изменений
2.42	Исходная версия для DAS-3216/3224/3248 rev B1

Функциональные возможности DAS-3248

1. Основные преимущества системы

- 16/24/48 портовый ADSL/ADSL2/ADSL2+ абонентский интерфейс
- 2x10/100/1000BaseT Uplink интерфейсов
- 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 до 3 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
- Встроенный CLI «usermode» режим (режим упрощенных макрокоманд)
- Удаленное встроенное SNMP/TELNET управление
- 2-уровня привилегии пользователя для управления
- SNMP версий: v1, v2c, v3
- Загрузка прошивки через TFTP
- Автоконфигурирование (удаленная автозагрузка конфигурационного файла) через TFTP
- Загрузка прошивки через TFTP (в том числе и удаленно)
- Распределенная система управления AMS - Advanced Management System (поставляется отдельно)
- Локальная система управления LCT - Local Craft Terminal (поставляется бесплатно с устройством)

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 (**отдельная модель DSLAM**)
- Максимальная протяженность линии до 7 км (с использованием READSL2)
- Поддержка ATM OAM- I.610 (F5) Loopback test
- Поддержка Single End Loopback Test (SELT)
- Поддержка Dual End Loopback Test (DELT)
- Расширенные возможности управления мощностью

4. Расширенные функции:

Функции физических интерфейсов

- Поддержка до 8 VC, 128 MAC адресов для каждого ADSL порта
- Поддержка 2К широковещательных MAC адресов на коммутатор DAS-3248
- Настраиваемый размер пакетов (от 64 до 1536)

Функции виртуальных сетей (VLAN)

- Поддержка Port-based VLAN и 802.1q VLAN (до 512 VLANs)
- 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 режима мультиплексирования ATM (LLC/VC mux)

Функции отказоустойчивости:

- Поддержка протокола Spanning Tree (802.1d)
- Поддержка протокола Rapid Spanning Tree (802.1w)

Функции групповых сообщений:

- Поддержка IGMP Snooping v.1,v.2,v3
- Поддержка Multicast VLAN (MVLAN)
- Поддержка фильтрации Multicast групп на портах

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 (802.1p)
- Поддержка ограничения скорости на ATM и Ethernet портах (IRL,ORL)
- Поддержка ограничения скорости по потокам (Flow Based Rate Limiting)

Прочие функции:

- Поддержка SNMP proxy
- Поддержка PPPoE Intermediate Agent (PIA)
- Поддержка DHCP Relay option 82 (DRA)

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-3216/24/3248 производится в двух модификациях:

DAS-3216/24/3248 - имеет питание AC (110-200В)

DAS-3216DC/24DC /3248DC- имеет стационарное питание 48В ВС

Внешний вид других моделей (DAS-3216, DAS-3224) изображен на рис. 1-2 и рис. 1-3



Рисунок 1-2. DAS-3216



Рисунок 1-3. DAS-3224

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



Рисунок 1-4. Расположение органов управления DAS-3248

Как видно из рисунка 1-4 на передней панели имеются светодиодные индикаторы, показывающие текущее состояние системы и статус соединения, модуль с двумя интерфейсами Ethernet 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). Роль портов uplink и downlink могут быть изменены программно, поэтому для общности оба этих порта называют портами Uplink (Uplink1 и Uplink2).

На задней панели имеются также одна (для DAS-3216/3224) 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
ERROR	Красный	Горит в случае возникновения ошибки
1 –48	Зеленый Зеленый/Мерцающий Серый (не горит)	Горит непрерывно, когда соединение ADSL активно Мерцает, когда производится передача через интерфейс Горит, когда обнаружена потеря сигнала или линия административно отключена
Gigabit Ethernet 1-2 10/100/1000	Зеленый	Горит, когда интерфейс активен
Gigabit Ethernet 1-2 LinkAct	Зеленый/Мерцающий	Мерцает, когда производится передача через интерфейс
Reset		Кнопка сброса устройства к настройкам по умолчанию (заводским)

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.
- **SNMP** – конфигурирование устройства может производиться непосредственно по протоколу SNMP через специальные библиотеки функций (MIB), либо посредством поставляемых с устройством графической программы управления (**AMS LCT**). Данная программа рассмотрена в отдельном документе.

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

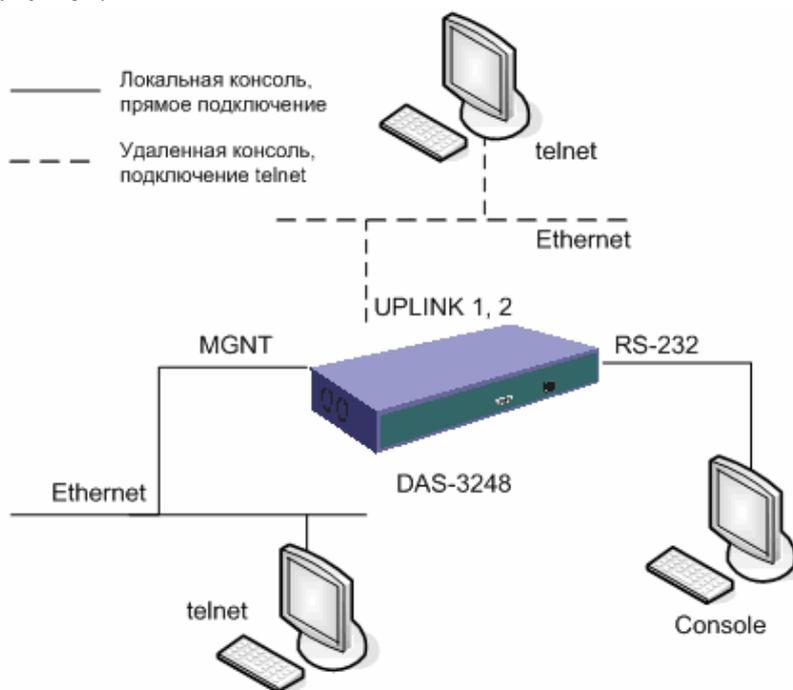


Рисунок 1-6

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

- консольный порт RS-232
- Gigabit Ethernet интерфейс UPLINK1 (eth-1)

Важно: 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:

DSLAM Bootloader

Bootloader Release: R2.42 Date: Jul 21 2008

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-1 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-1")

<управляющее3 значение3>

("status enable")

Примечание: Команда создает bridge port с номером интерфейса 385, именем eth-1 и устанавливает его в активное состояние.

Внимание: Начиная с версии 2.42 командный интерфейс устройства (CLI) имеет два режима : Инженерный и Пользовательский. Смотрите главу 11 настоящего руководства. Переход между режимами осуществляется командами **engmode** и **usermode**

1.3. Настройка параметров IP-интерфейса

В DAS-3248 используются два Ethernet интерфейса:

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



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-1 ip 192.168.1.1, mask 255.255.255.0) . Для подключения убедитесь, что устройство и Ваш компьютер находятся в одной IP подсети.

Eth-2 сконфигурирован по умолчанию как downlink.

1.3.1. Настройка IP-адреса и маски подсети

Изменение IP адресов и маски подсети, производится 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-1 ..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
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
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 downlink	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 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 будут 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	Задаёт 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-1):

Команда	Действие
---------	----------

Шаг 2	<code>\$modify ethernet intf ifname eth-1 ip 192.168.0.50 mask 255.255.255.0</code>	Изменить ethernet интерфейс на порту Uplink 1 (eth-1) с необходимым IP
	<code>\$get ethernet intf</code>	Проверить настройки интерфейсов

Создание ethernet интерфейса UPLINK2 (eth-2):

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-2 в системе как uplink, надо сначала удалить настройки обоих интерфейсов и создать eth-1 как downlink (см.пример).

Примечание: Оба Uplink интерфейса могут быть использованы одновременно 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	<code>\$delete bridge port intf portid 385</code> <code>\$delete filter rule map ifname eth-1 stageid 1 ruleid 1</code> <code>\$delete ethernet intf ifname eth-1</code>	Удалить интерфейс Eth-1
Шаг 2	<code>\$delete bridge port intf portid 386</code> <code>\$delete ethernet intf ifname eth-2</code>	Удалить интерфейс Eth-2
Шаг 3	<code>\$create ethernet intf ifname eth-1 type downlink</code>	Создать Ethernet интерфейс eth-2 как downlink
Шаг 4	<code>\$create bridge port intf portid 385 ifname eth-1 status enable</code>	Создать bridge port 385 на интерфейсе eth-1
Шаг 5	<code>\$create ethernet intf ifname eth-2 ip 192.168.1.50 mask 255.255.255.0 enable</code>	Создать второй ethernet интерфейс на порту Uplink 2 (eth-2)
Шаг 6	<code>\$create bridge port intf portid 386 ifname eth-2 learning disable status enable</code>	Создать bridge port 386 на интерфейсе eth-2
Шаг 7	<code>\$get ethernet intf</code>	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.

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 сдвигку 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 `modify sntp cfg [enable | disable]`
команды:

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

get sntp servaddr

Описание: Получает информацию о текущих значениях работы sntp

Синтаксис команды: create 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

Важно: 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 работоспособности 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.

Экранный вывод:

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	

Примечание: 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.

Внимание: 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 рассматривается в главе 4 данного руководства).

Команды системы:

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 gwip gwip [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

	<p>все потоки описаны в ней. Использование: Create -- Опционально, Delete -- Обязательно Modify -- Обязательно Get -- Опционально</p>
ip ip	<p>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</p>
mask mask	<p>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</p>
gwyip gwyip	<p>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</p>
ifname ifname	<p>Индексное значение, которое однозначно идентифицирует локальный интерфейс, через который может быть достигнут следующий переход для данного маршрута. Использование: Create -- Optional Modify -- Optional</p>
proxyarpstatus enable disable	<p>Указывает, должно ли выполняться Proxy ARP для данной записи таблицы маршрутизации. Использование: Create -- Optional Modify -- Optional По умолчанию: выключен</p>

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

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-1	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-1	DIR	DYI	0
127.0.0.0	255.0.0.0	127.0.0.1	lo-1	DIR	DYI	0
10.90.90.0	255.255.255.0	10.90.90.90	eth-1	DIR	DYI	0
10.90.90.90	255.255.255.255	127.0.0.1	lo-1	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:

Шаг 1
Шаг 2

Команда	Действие
\$ create ip route ip 10.90.80.0 mask 255.255.255.0 gwyp 10.90.91.100	Создать маршрут к подсети 10.90.80.0, через шлюз с ip адресом 10.90.91.100 eth-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-2	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-1	DIR	DYI	0
127.0.0.0	255.0.0.0	127.0.0.1	lo-1	DIR	DYI	0
10.90.90.0	255.255.255.0	10.90.90.90	eth-1	DIR	DYI	0
10.90.90.90	255.255.255.255	127.0.0.1	lo-1	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
- Оповещения SNMP
- Версии 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 DSLAMа 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

1.6.2.Настройка SNMP

- Создание, изменение, удаление community string
- Создание, изменение, удаление snmp host
- Создание, изменение, удаление snmp trap host
- Настройка snmp проху
- 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
<i>community community</i>	Определяет имя Community. Тип: Create -- обязательно Delete -- обязательно Get -- опционально
<i>access ro rw</i>	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
<i>community community</i>	Определяет имя Community.
<i>Access</i>	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
<i>ip ip</i>	Определяет IP-адрес компьютера пользователя, который имеет права доступа. Тип: Create -- обязательно Delete -- обязательно Get – опционально
<i>community community</i>	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
<i>ip ip</i>	Определяет IP-адрес компьютера пользователя, который имеет права доступа.
<i>community community</i>	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
<i>port port</i>	Определяет порт, на который будут отправляться trap. Тип: Create – опционально Get – опционально Modify - опционально Delete – опционально Значение по умолчанию: 162
<i>version v1 v2c</i>	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
<i>Ip Address</i>	Определяет IP-адрес менеджера, на который отправляются trap.
<i>Community</i>	Определяет имя Community, используемое в trap.
<i>Port</i>	Определяет порт, на который отправляются trap.
<i>Version</i>	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
<i>ip ip</i>	Определяет IP-адрес пользователя, который имеет права доступа для CPE для Community, определенной 'NetCommunity'. Тип: Create – обязательно Modify - обязательно Delete – обязательно Get – опционально

<i>netcomm netcomm</i>	<p>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 Proxu, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться.</p> <p>Тип: Create – обязательно Modify - обязательно Delete – обязательно Get – опционально</p>
<i>hostport hostport</i>	<p>Определяет порт UDP менеджера, через который с помощью SNMP Proxu будут передаваться trap. Для запросов и ответов SNMP это поле не используется.</p> <p>Тип: Create – опционально Modify – опционально Значение по умолчанию: 162</p>

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
<i>ip Address</i>	Определяет IP-адрес пользователя, который имеет права доступа для CPE для Community, определенной 'NetCommunity'.
<i>NET Community</i>	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 Proxu, обработка SNMP-агента, соответствующая записи в таблице SNMP Host будет игнорироваться.
<i>Host Port</i>	Определяет порт UDP менеджера, через который с помощью SNMP Proxu 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 string прокси-агента

Синтаксис команды

create snmp proxy comm netcomm netcomm crespcomm crespcomm lowiflowif

Команда **delete snmp proxy comm**

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

Синтаксис команды

delete snmp proxy comm netcomm netcomm

Команда **modify snmp proxy comm**

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

Синтаксис команды

modify snmp proxy comm netcomm netcomm [crespcomm crespcomm]

Параметры

Имя	Описание
<i>netcomm netcomm</i>	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
<i>crespcomm crespcomm</i>	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
<i>lowiflowif</i>	Определяет самое наименьшее имя интерфейса, через

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

Пример \$ create snmp proxy comm netcomm Adsl1 cpecomm Adsl lowif aal5-1

Вывод

Verbose Mode On
 Entry Created
 NET Community : Adsl1
 CPE Community : Adsl
 LowIfName : aal5-1
 Verbose Mode Off:
 Entry Created

Описание полей вывода

Имя	Описание
<i>NET Community</i>	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.
<i>CPE Community</i>	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.
<i>LowIfName</i>	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
<code>status disable enable</code>	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-*, dsif-*, dsli-*.

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 предоставляет 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
<i>rindex rindex</i>	Уникальный идентификатор зонда. Тип: Create – обязательно Delete – обязательно Get - опционально Используемые значения: 0-20
<i>Ifname interface-name</i>	Указывает имя интерфейса. Тип: Create – обязательно Используемые значения: <i>eoal-1 - *</i> , <i>eth-1-*</i>
<i>Owner owner-string</i>	Сущность, которая сконфигурировала этот зонд и

	<p>поэтому использующая его ресурсы. Тип: Create – обязательно Используемые значения: Строка из максимум 64 ASCII символов.</p>
--	---

Пример `$ get srmon probe rindex 1`

Вывод

Verbose Mode On

RMON Probe Index : 1

If-Name : eth-1

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
<i>RMON Probe Index</i>	Уникальный идентификатор зонда.
<i>Ifname</i>	Указывает имя интерфейса. Оно может быть <i>eoal-1 - *</i> , <i>eth-1-*</i>
<i>Stats Owner</i>	Сущность, которая сконфигурировала этот зонд и поэтому использующая его ресурсы.
<i>Total Octets</i>	Общее количество октетов данных (включая «плохие» пакеты), полученных сетью (за исключением битов синхронизации, но включая октеты FCS).
<i>Total Packets</i>	Общее количество полученных пакетов (включая «плохие», широковещательные и многоадресные пакеты).
<i>Total Broadcast Packets</i>	Общее количество полученных хороших широковещательных пакетов.
<i>Total Multicast Packets</i>	Общее количество полученных хороших многоадресных пакетов.
<i>Total 64 Octets</i>	Общее количество полученных пакетов (включая «плохие» пакеты) размером 64 октета (за исключением битов синхронизации, но включая октеты FCS).
<i>Total 65-127 Octets</i>	Общее количество полученных пакетов (включая «плохие» пакеты) размером 65-127 октетов (за исключением битов синхронизации, но включая октеты FCS).
<i>Total 128-255 Octets</i>	Общее количество полученных пакетов (включая «плохие» пакеты) размером 128-255 октетов (за исключением битов синхронизации, но включая октеты FCS).
<i>Total 256-511 Octets</i>	Общее количество полученных пакетов (включая «плохие» пакеты) размером 256-511 октетов (за

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

После применения команды **commit** устройство запоминает конфигурацию в бинарном файле **primcfg**.

reboot config last – команды для загрузки **primcfg**

1.7.2.Сохранение конфигурационных файлов на tftp сервере

Конфигурация устройства **primcfg** может быть выгружена 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 конфигураций. 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 конфигурации] **ip** [ip адрес tftp/ftp 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]

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;

-t| 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

Prompt 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:

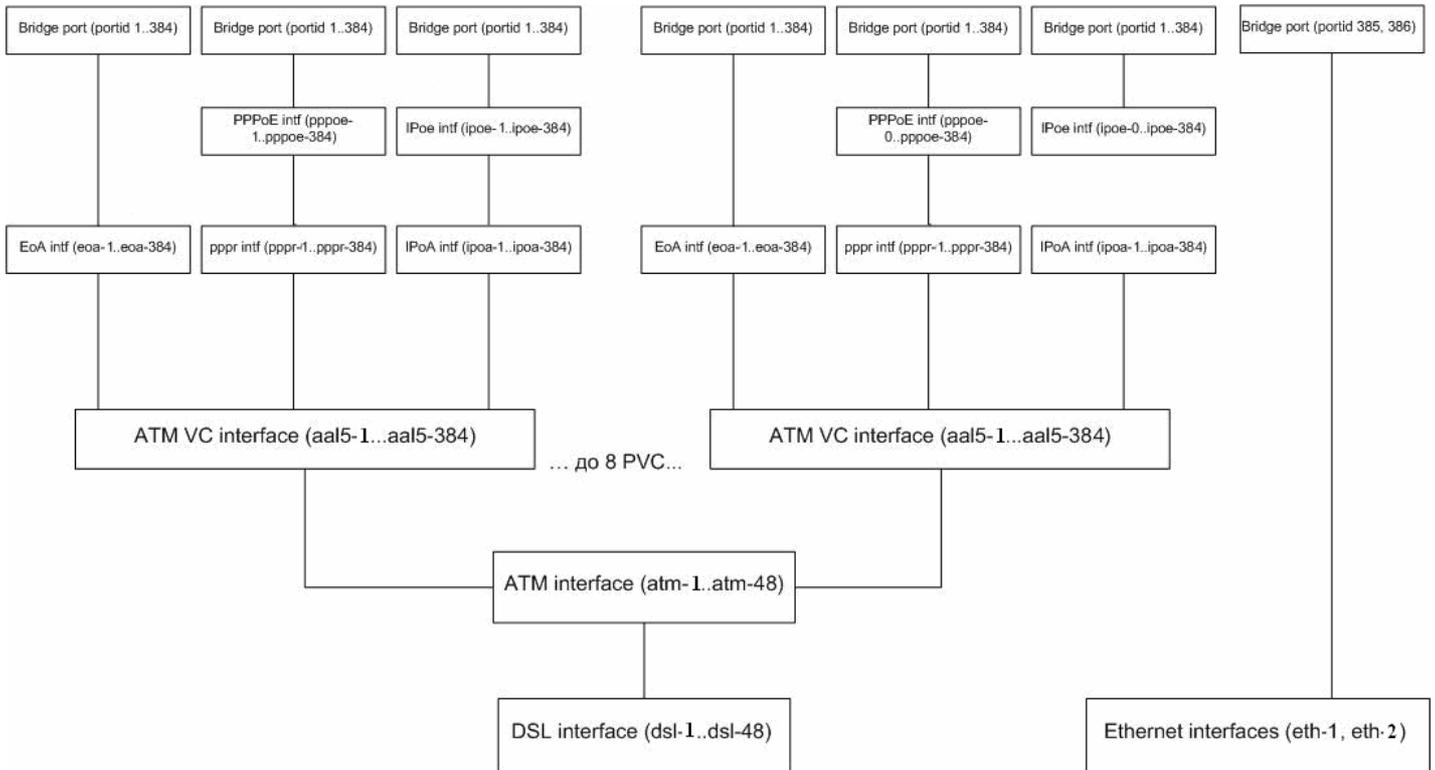


Рисунок 2-1. Логическая структура интерфейсов DAS-3248

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

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

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-1...dsl-48. Интерфейс dsl-1 соответствует 1-ому

ADSL порту, dsl-48 – 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-1...atm-48. Интерфейс atm-1 соответствует 1-ому ADSL порту, atm-48 – 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 aal5-1...aal5-384.

По умолчанию на DSLAM-е созданы 48 ATM VC интерфейсов (aal5-1...aal5-48) – 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 aal5-49...aal5-384. 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-1...eoa-384. По умолчанию созданы 48 EoA интерфейсов с именами eoa-1...eoa-48 (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-1...pppr-384 и pppoe-1...pppoe-384 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-1...ipoa-384 и ipoe-1...ipoe-384 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-1) и Uplink 2 (eth-2) 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 присутствует 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.

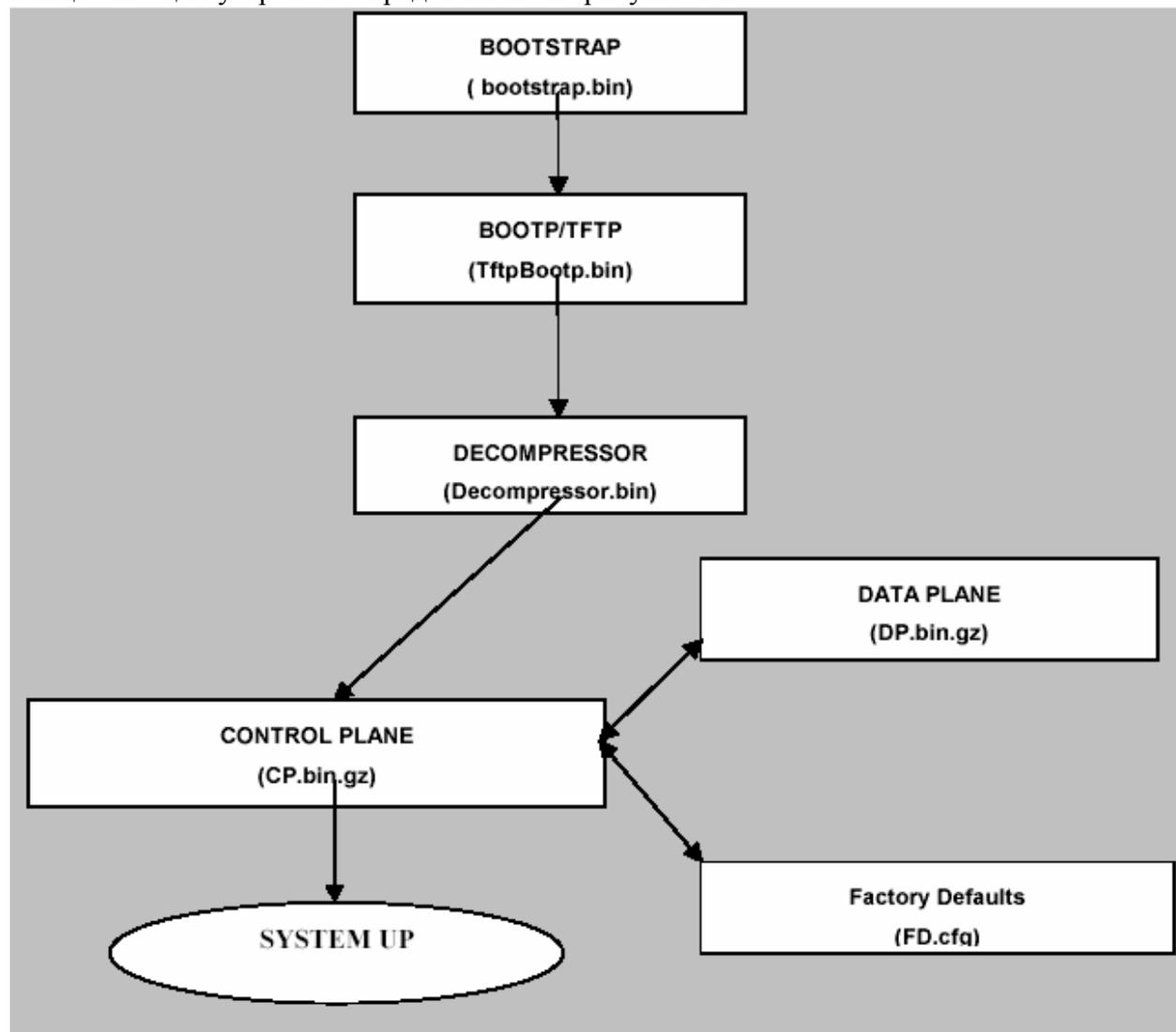


Рисунок 2-2. Порядок инициализации DAS-3248

BOOTSTRAP Загрузчик.

Исполняет роль, аналогичную BIOS. Этот бинарный файл ответственен 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 копии 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 пользовательским интерфейсом.

DataPlane -Часть внутренней ОС, ответственная за связь с пользовательским интерфейсом. Кроме этого она отвечает за АТМ 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
<code>/nvram/bin/control/</code>	Каталог содержит упакованный образ ControlPlane. Может содержать многочисленные версии образов.
<code>/nvram/bin/dataplane/</code>	Каталог содержит упакованный образ DataPlane. Может содержать многочисленные версии образов.
<code>/nvram/bin/dslphy/</code>	Каталог содержит двоичный образ драйвера DSL физического уровня. Может содержать только одну версию файла.
<code>/nvram/cfg/factorydef/</code>	Каталог содержит конфигурацию по умолчанию устройства (FD.cfg). Может содержать многочисленные версии файлов.
<code>/nvram/cfg/manuf/</code>	Каталог содержит специальную информацию изготовителя.
<code>/nvram/user/</code>	Каталог содержит файлы пользователя
<code>/nvram/image/</code>	Временный логический каталог, создающийся при операции загрузки внутреннего ПО. Доступен только в специальном режиме (Safe mode)
<code>/nvram/bootloader/</code>	Каталог, содержащий двоичный файл загрузчика Доступен только в специальном режиме (Safe mode)
<code>/nvram/system/</code>	Каталог, содержащий основную конфигурацию primcfg устройства.

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

Size – 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** true|false] , где:

file-name –имя файла,

version- версия файла (необязательный параметр).

besteffort true|false – 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	: DAS-3248
Name	: customerservice@dlink.com
Location	: No.289, Sinhu 3rd Road, Neihu District, Taipei, Taiwan.
Contact	: Company contact phone/fax number
Vendor	: No.289, Sinhu 3rd Road, Neihu District, Taipei, Taiwan.
LogThreshold	: 0
Object-id	: 1.3.6.1.4.1.3646.1300.300.14
Up Time(HH:MM:SS)	: 1:5:31
HwVersion	: 40
CPSwVersion	: R2.1n_4M_4M
DPSwVersion	: DP_B02_10_28_04_ip1000a
System Time	: Thu Jan 01 01:05:31 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>] [dataplane <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 (secscfg).

clean – загрузка устройства без конфигурации («чистая» конфигурация)

minimum- загрузка устройства с минимальной конфигурацией (сконфигурирован только eth-1 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 конфигурационный файл хранящийся в файловой системе по /nvram/system/primcfg - последняя сохраненная командой commit конфигурация, Конфигурация являются бинарным (двоичным файлом) и может быть выгружена и загружена 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)

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)

4. Введите команду:

```
$reboot config last -для загрузки устройства с текущей 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 файловой системы SDRAM DSLAM-а, в качестве ip указав ip адрес tftp сервера:

Например:

```
$download src dslam2.cfg dest /sdram/user/mycfg.cfg ip 192.168.7.3
```

3. Примените загруженный скриптовый файл командой

```
$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 fname /sdram/user/mycfg.cfg 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 расширением .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 Вам понадобится файл прошивки с расширением bin.gz (в нашем примере он будет называться TEImage.bin.gz) и TFTP сервер.

Порядок обновления ПО:

1. Подключите консольный кабель к DAS-3248, запустите терминальную программу и включите питание DSLAM-а.
2. Дождитесь окончания загрузки, получите доступ к командной строке и введите команду:

```
$reboot config safe
```

Внимание : Логин для safe режима по умолчанию : **root**, пароль: **root**

3. После перезагрузки устройства необходимо настроить Ethernet интерфейс (DAS-3248 должен быть подключен к сети через порт UPLINK 1!!!)

Например:

```
$modify ethernet intf ifname eth-1 ip 192.168.7.13 mask 255.255.255.0
```

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

4. Запустите TFTP сервер, в качестве рабочей директории укажите ту, в которой находится файл TEImage.bin.gz
5. 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
```

6. Дождитесь окончания загрузки файла и обновления flash.

Внимание: **Ни в коем случае не выключайте в это время питание устройства!**

7. После появления приглашения командной строки введите: `reboot`

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.

Пример файла FD.cfg:

```
create ethernet intf ifname eth-1 type uplink ip 192.168.1.1 mask 255.255.255.0
create bridge port intf portid 385 ifname eth-1 status enable
create dsl system
create resvdmac profile param profileid 1 mcastaddr 01:80:C2:00:00:00 action participate
create filter rule entry ruleid 1 action sendtocontrol description IGMP applywhenreq enable
create filter subrule ip ruleid 1 subruleid 1 prototypefrom 2 prototypecmp eq
create filter rule map ifname all stageid 1 ruleid 1 orderId 1
modify filter rule entry ruleid 1 status enable statsstatus enable
create filter rule entry ruleid 2 action copytocontrol description IPOE_CONTROL
applywhenreq enable
create filter subrule ether ethertypefrom 0x806 ethertypecmp eq dstmacaddrfrom ff:ff:ff:ff:ff:ff
dstmacaddrcmp eq ruleid 2 subruleid 1
create filter rule map ifname alleth stageid 1 ruleid 2 orderId 2
modify filter rule entry ruleid 2 status enable statsstatus enable
```

```
create ethernet intf ifname eth-2 type downlink
create bridge port intf portid 386 ifname eth-2 status enable
create snmp comm community public rw
create snmp host ip 192.168.1.2 community public
create user name Admin passwd Admin root
create macprofile global profileid 1 macaddr 00:00:00:00:00:01
wizard deploy all vpi 8 vci 35
wizard modify status all off
create profile entry name adsl2 stdtype adsl2
create profile entry name default
modify profile map port 1 name default
modify profile map port 2 name default
modify profile map port 3 name default
modify profile map port 4 name default
modify profile map port 5 name default
modify profile map port 6 name default
modify profile map port 7 name default
modify profile map port 8 name default
modify profile map port 9 name default
modify profile map port 10 name default
modify profile map port 11 name default
modify profile map port 12 name default
modify profile map port 13 name default
modify profile map port 14 name default
modify profile map port 15 name default
modify profile map port 16 name default
modify profile map port 17 name default
modify profile map port 18 name default
modify profile map port 19 name default
modify profile map port 20 name default
modify profile map port 21 name default
modify profile map port 22 name default
modify profile map port 23 name default
modify profile map port 24 name default
modify adsl alarm profile ifname dsl-1 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-2 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-3 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-4 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-5 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-6 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-7 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-8 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-9 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-10 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-11 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-12 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-13 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-14 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-15 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-16 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-17 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-18 atucgspmstatetrapenable true
```

```
modify adsl alarm profile ifname dsl-19 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-20 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-21 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-22 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-23 atucgspmstatetrapenable true
modify adsl alarm profile ifname dsl-24 atucgspmstatetrapenable true
modify bridge tbg traps bindingStatus enable
wizard modify status all on
end
```

Экраний вывод при автоконфигурировании:

```
$ reboot config network
Transferring 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

User did not request for debugging Control Plane.....Continuing
Primary Ethernet Interface for TFTP :- eth-1
Secondary Ethernet Interface for TFTP :- eth-2
Could not TFTP on eth-2, 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 аппаратной перезагрузке устройства оно опять войдет в режим удаленного конфигурирования.

2.2.10. Удаленная замена ПО устройства.

DAS-3248 позволяет осуществить также удаленную замену программного обеспечения по протоколу BootP/TFTP.

Опишем последовательно эту процедуру:

1. Создаем текстовый скрипт с именем **FD.cfg**, в котором прописываем IP адрес Uplink1(eth-1) интерфейса из нужной нам сети.

Этот файл размещаем в рабочей директории TFTP сервера

Пример скрипта:

```
verbose off
create ethernet intf ifname eth-1 ip 192.168.7.13 mask 255.255.255.0
verbose on
end
```

2. Заходим удаленно на командный интерфейс устройства (по протоколу Telnet).

```
telnet 192.168.7.13
```

3. Запускаем TFTP сервер. IP адрес интерфейса DSLAM должен находиться в одной подсети с tftp сервером.

4. Удаляем текущий файл FD.cfg в файловой системе DSLAM и загружаем с сервера TFTP созданный нами скрипт.

```
$remove fname /nvram/cfg/factorydef/FD.cfg version 1
$download src FD.cfg dest /nvram/cfg/factorydef/FD.cfg ip 192.168.7.13
$upgrade fname /nvram/cfg/factorydef/FD.cfg version 2
```

5. Перезагружаем устройство в safe режим.

```
$reboot config safe
```

Внимание : Логин для safe режима по умолчанию : **root**, пароль: **root**

При этом управление на некоторое время пропадет, но устройство перезагрузится и станет вновь доступно по заданному в скрипте адресу.

6. Загружаем по TFTP новую версию ПО

```
$download src TEImage.bin.gz dest /nvram/image/TEImage.bin ip 192.168.7.13
```

7. Дождитесь окончания загрузки файла и обновления flash.

Внимание: **Ни в коем случае не выключайте в это время питание устройства!**

8. После появления приглашения командной строки введите: **\$reboot**

Внимание: После удаленного обновления ПО устройство загрузится с заводскими настройками.

Если вы хотите загрузить устройство со своими (предварительно сохраненными в текстовом скриптовом файле) **настройками**, переименуйте свой конфигурационный файл в **FD.cfg**, разместите его в рабочем каталоге TFTP сервера и сразу после обновления ПО выполните команду **\$reboot config network** (см. п.2.2.9.Автоконфигурирование DAS-3248).

Не забудьте, что для этой операции в сети необходимо иметь не только TFTP, но DHCP сервер, поскольку **IP адрес**, необходимый для загрузки, **DAS-3248** получает **автоматически с внешнего DHCP сервера** находящего в той же сети, что и DSLAM. **Затем DSLAM загружает скриптовый файл с внешнего TFTP сервера**. Новый файл FD.cfg замещает старый и после проверки синтаксиса всех команд переводится в активное состояние. После этого устройство автоматически перегружается в “нормальный” штатный режим.

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», входящий 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, 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 мультиплектору (DSLAM, АТУС), 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 (АТУР), 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.

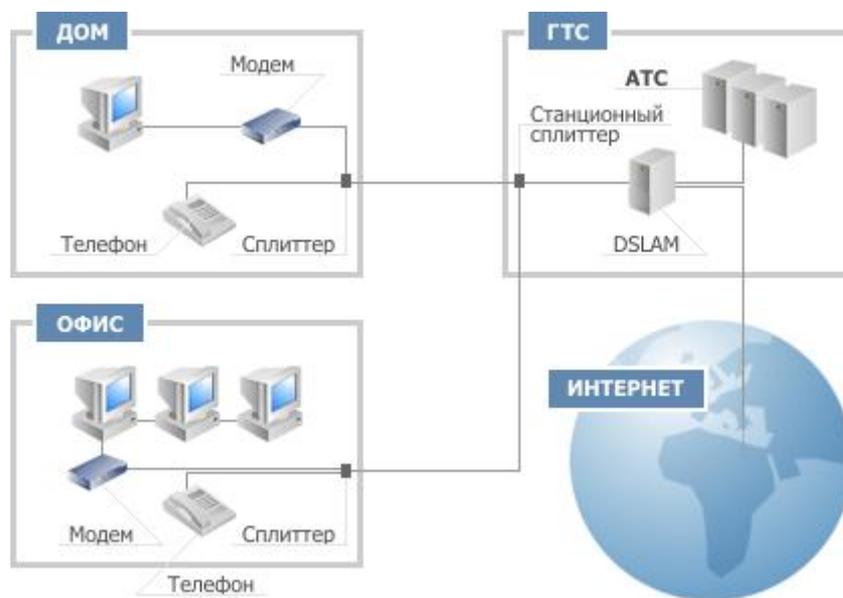


Рисунок 3-1

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

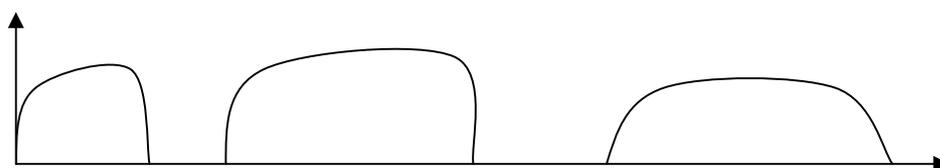
Смысл ее заключается в том, что вся полоса частот в 1.1 МГц делится на 256 подканалов, называемых поднесущими. Каждый канал занимает по 4.3125КГц. Некоторые из подканалов являются специализированными, другие не используются вообще. Нижние подканалы от 1 до 6 резервируются для полосы пропускания аналоговых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

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 ассиметрична, но диапазоны частот для входящего и исходящего потоков частично перекрываются.



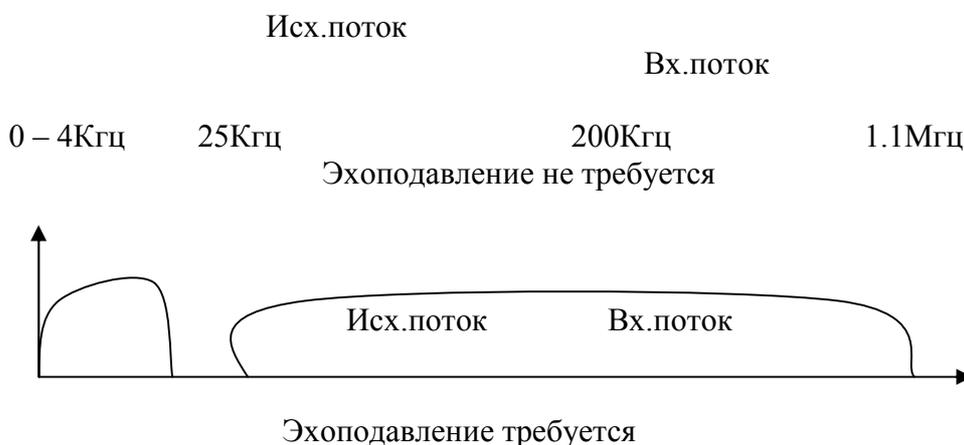


Рисунок 3-2

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 суперкадр 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.

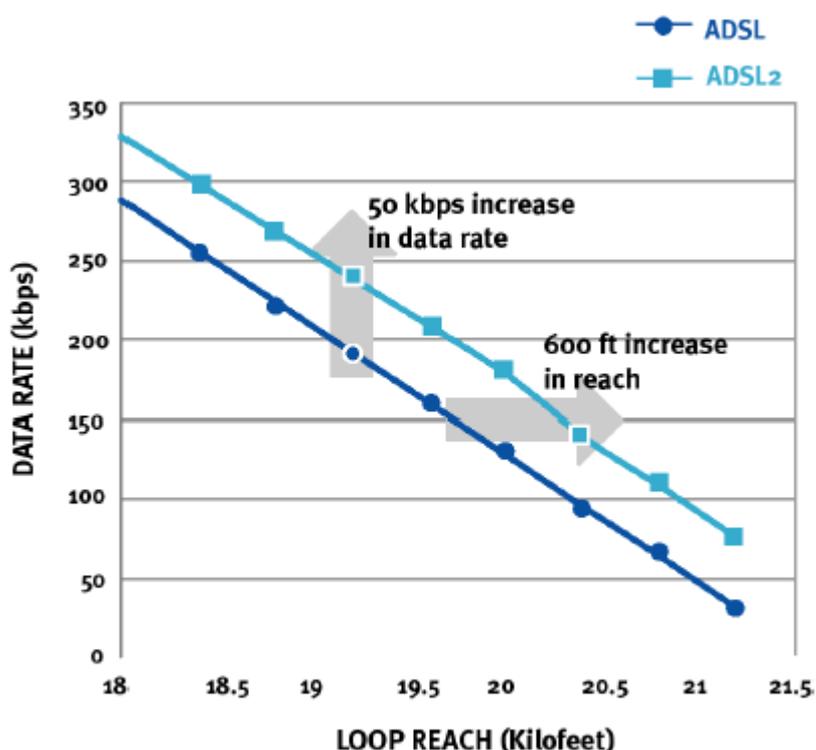


Рисунок 3-3

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.

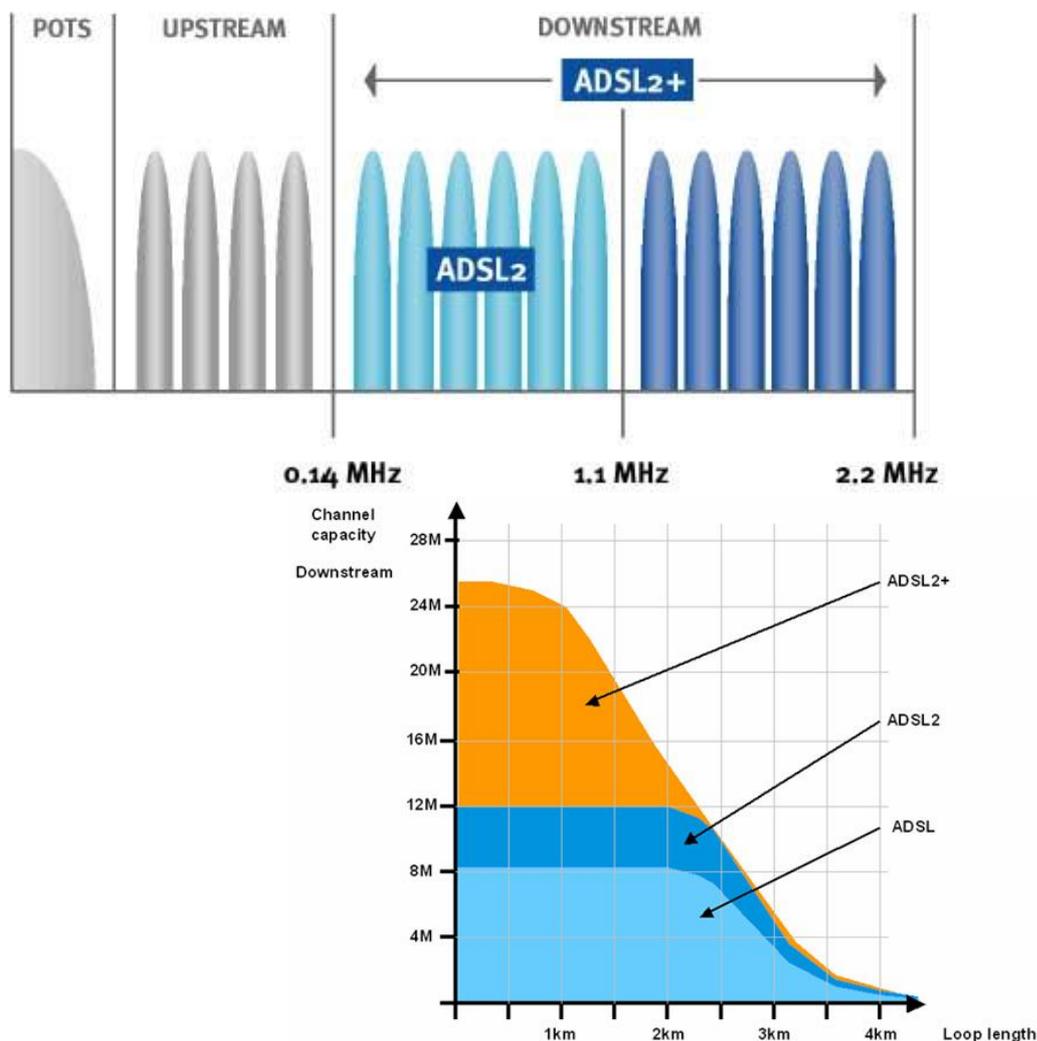


Рисунок 3-5

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.

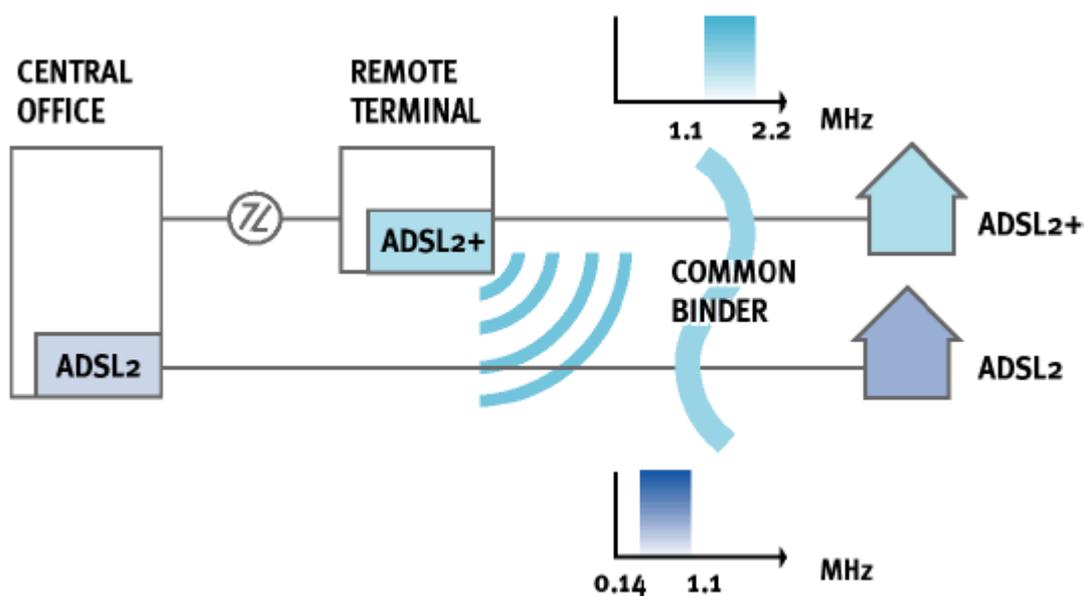


Рисунок 3-6

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 позволяет 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 теоретической скорости 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.

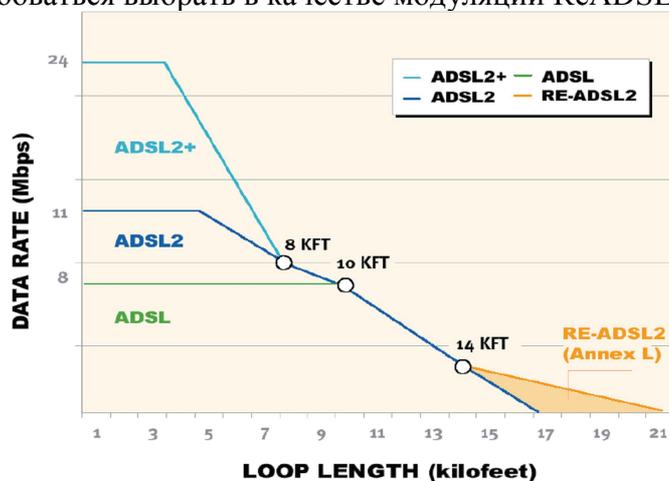


Рисунок 3-7

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 отдельных устройствах серии DAS, и только со специальным ПО (прошивкой) устройства. Annex B несовместим с другими Annex.

Обращайтесь в представительства компании D-link за более подробной информацией.

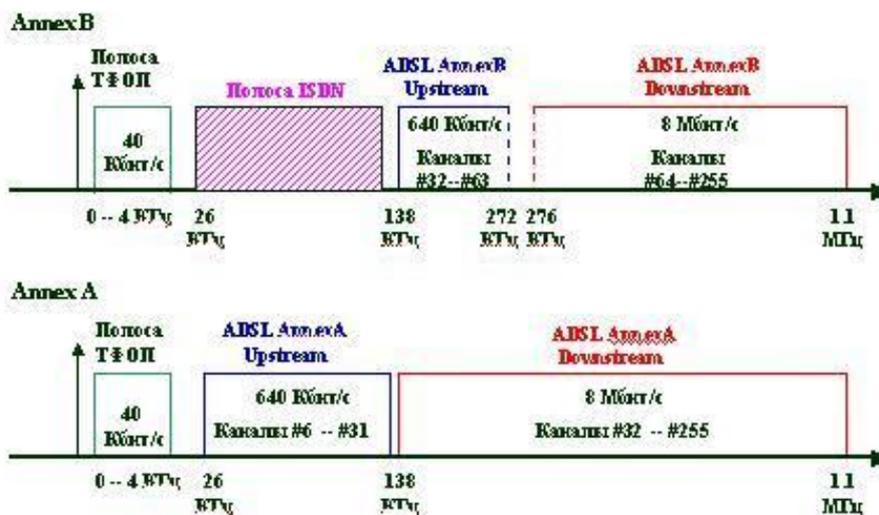


Рисунок 3-8

Управление мощностью ADSL линии (Power management)

В стандартах G.992.3 and G.992.5 определена функция управления мощностью линии. Оператор может определить вручную или автоматически мощность передачи сигнала (Tx) по ADSL линии (ADSL line Transmission).

В первом поколении стандартов ADSL предполагалось, что ADSL-устройства работают в режиме максимального энергопотребления круглосуточно, то есть даже тогда, когда по абонентской линии трафик не передается. В спецификациях ADSL2 этот режим обозначен как L0, а помимо него предусмотрены два более экономичных режима. В L2 уровень энергопотребления снижается оборудованием центрального офиса статистически, то есть с учетом текущей интенсивности передаваемого трафика, а в L3 устройства на обоих концах соединения переходят в спящий режим в случае длительного «простоя» линии. Переходы между L2 и L0 осуществляются без прерывания сервиса и каких-либо потерь пакетов, то есть с точки зрения пользователя, выполняются прозрачно. Повторная инициализация соединения и выход на стационарную скорость передачи из состояния L3 занимает около 3с.

Автоматическое управление мощностью – это функция, которая позволяет автоматически изменять состояние ADSL линии с L0 (full-on, полная мощность) на L2 (low power, режим с низким энергопотреблением) в том случае, скорость Downstream потока данных ниже определенного порога. И наоборот, менять состояние с L2 на L0 в том случае, если DSLAM начнет отбрасывать пакеты Downstream данных.

3.2. Включение/выключение ADSL- порта

Интерфейсы DSL служат для непосредственного управления соответствующими ADSL портами DAS-3248. Названия dsl интерфейсов лежат в диапазоне dsl-1...dsl-48. Интерфейс dsl-1 соответствует 1-ому ADSL порту, dsl-48 – 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-1 disable

Административно включить 1 порт ADSL

\$modify adsl line intf ifname dsl-1 enable

3.3.Изменение параметров порта DSL. Просмотр статуса порта

Для изменения параметров порта DSL используется команда.

modify adsl line intf

Описание: изменение параметров ADSL порта.

Синтаксис команды:

```
modify adsl line intf ifname ifname [ linetransatucconfig ansit1413 | etsi |  
q9921PotsNonOverlapped | q9921PotsOverlapped | q9921IsdnNonOverlapped |  
q9921IsdnOverlapped | q9921tcmIsdnNonOverlapped | q9921tcmIsdnOverlapped |  
q9922potsNonOverlapped | q9922potsOverlapped | q9922tcmIsdnNonOverlapped |  
q9922tcmIsdnOverlapped | q9921tcmIsdnSymmetric | adslPlusPotsNonOverlapped |  
q9921GspanPlusPotsNonOverlapped | q9921GspanPlusPotsOverlapped | q9923Adsl2PotsOverlapped  
| q9923Adsl2PotsNonOverlapped | q9925Adsl2PlusPotsOverlapped |  
q9925Adsl2PlusPotsNonOverlapped | q9923Readsl2PotsOverlapped |  
q9923Readsl2PotsNonOverlapped | adslPlusPotsOverlapped |  
q9921GspanPlusPlusPotsNonOverlapped | q9921GspanPlusPlusPotsOverlapped |  
q9923IsdnNonOverlapped | q9923IsdnOverlapped | q9925IsdnNonOverlapped |  
q9925IsdnOverlapped | q9923AnnexMPotsExtUsNonOverlapped |  
q9923AnnexMPotsExtUsOverlapped | q9925AnnexMPotsExtUsNonOverlapped |  
q9925AnnexMPotsExtUsOverlapped ] [ dsbinsrupdate 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 модуляций ADSL. Подключения всех не выбранных 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

q9922potsNonOverlapped 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-1 disable

**\$ modify adsl line intf ifname dsl-1 LineTransAtucConfig q9925Adsl2PlusPotsNonOverlapped
q9925Adsl2PlusPotsOverlapped**

\$modify adsl line intf ifname dsl-1 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-1

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

Экранный вывод:

```
IFName          : dsl-1
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 q9922potsNonOverlapped q9923Reads12PotsNonOverlapped
pped q9925Ads12PlusPotsNonOverlapped q9925Ads12PlusPotsOverlapped q9923Ads12PotsNonOverlapped q9923AnnexMPotsExtUsNonOverlapped q992
5AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
Trans Atuc Actual : -
Trans Atuc Config : ansit1413 q9921PotsNonOverlapped q9923Reads12PotsNonOverlapped q9925Ads12PlusPotsOverlapped q9923Ads1
2PotsNonOverlapped q9923AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsNonOverlapped q9925AnnexMPotsExtUsOverlapped
GsDmtTrellis    : trellisOn
Trans Atur Cap  : ansit1413 q9921PotsOverlapped q9921tcMIsdnOverlapped ads1PlusPotsOverlapped q9923Reads12PotsNonOverlapped
pped q9925Ads12PlusPotsNonOverlapped q9925Ads12PlusPotsOverlapped q9923Ads12PotsNonOverlapped 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 глобальных DSL-профайлов

Глобальные DSL профайлы используются для быстрой смены основных DSL параметров (например, скоростей Upstream и Downstream потоков) на ADSL портах устройства.

Глобальные DSL профайлы изначально могут быть свободно «привязываться» и «отвязываться» от портов устройства при помощи консольных команд.

Это существенно облегчает администратору сети изменение параметров ADSL, так как профайлы с необходимыми наборами параметров (например, с разными скоростями) могут быть созданы на устройстве заранее и при необходимости быстро «привязываться» к портам устройства.

Однако, следует отметить, что количество таких профайлов ограничено (не более 10).

Синтаксис команд глобальных профайлов ADSL

create profile entry

Описание: создание глобального профайла

Синтаксис команды:

```
create profile entry name <name> [stdtype gdm|glite|t1413|ads12|ads12plus|reads12 ]
[ annexM off|on ] [ mode fix|ra|dynamic ] [ type interleave|fast ] [ dstgtsnr <dec> ]
[ dsminsnr <dec> ] [ dsmaxsnr <dec> ] [ dsminrate <dec> ] [ dsmaxrate <dec> ] [ dsdelay
<dec> ] [ ustgtsnr <dec> ] [ usminsnr <dec> ] [ usmaxsnr <dec> ] [ usminrate <dec> ]
[ usmaxrate <dec> ] [ usdelay <dec> ][ pmmode disable|l2|l3|l2l3 ] [ l2entryrate
<dec> ][ l2entrytime <dec> ][ l2exitrate <dec> ][ l2minrate <dec> ]
```

Таблица описания параметров команд:

name <name>	Имя профиля Обязательный параметр.
stdtype gdm glite t1413 adsl2 adsl2plus readsl2	Стандарт ADSL (тип модуляции) Необязательный параметр
annexM off on	Включение или выключение Annex M Необязательный параметр
mode fix ra dynamic	Определяет форму адаптации скорости передачи. Fix - фиксированная скорость. Не может изменяться . Ra, Dynamic - скорость определяется динамически из выбранного диапазона скоростей. <u>Ссылка</u> : ADSL Forum TR- 005 для получения большей информации. Необязательный параметр
type interleave fast	Параметр используется для настройки режима физической ADSL линии. (только Fast или только Inreleave) Необязательный параметр
dsminrate <dec>	Настройка минимальной скорости передачи Downstream потока данных (от DSLAM к абоненту). Скорость указывается в Кбит/с Необязательный параметр
dsmaxrate <dec>	Настройка максимальной скорости передачи Downstream. Скорость указывается в Кбит/с Необязательный параметр
usminrate <dec>	Настройка минимальной скорости передачи Upstream потока данных Скорость указывается в Кбит/с. Необязательный параметр
usmaxrate <dec>	Настройка максимальной скорости передачи Upstream потока данных Скорость указывается в Кбит/с. Необязательный параметр
dstgtsnr <dec>	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
dsminsnr <dec>	Настройка минимально допустимого отношения сигнал/шум (ОСШ). Если значение шума выше, то модем

	<p>должен оптимизировать мощность излучения до приемлемого уровня. Необязательный параметр Допустимые значения: 0 - 310</p>
dsmaxsnr <dec>	<p>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</p>
ustgtsnr <dec>	<p>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</p>
usminsnr <dec>	<p>Настройка минимально допустимого отношения сигнал/шум (ОСШ). Если значение шума выше, то модем должен оптимизировать мощность излучения до приемлемого уровня. Необязательный параметр Допустимые значения: 0 - 310 Необязательный параметр</p>
usmaxsnr <dec>	<p>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</p>
dsdelay <dec>	<p>Конфигурируемое максимальное значение задержки интерливинга в downstream направлении Необязательный параметр</p>
usdelay <dec>	<p>Конфигурируемое максимальное значение задержки интерливинга в upstream направлении</p>
pmmode disable 12 13 1213	<p>Принудительная смена состояния линии (режима управления мощностью ADSL линии на ближнем конце (ATU-C)</p>
l2entryrate <dec>	<p>Минимальная скорость (в килобитах в секундах) линии, при которой идет переход из состояния L0 в L2.</p>

l2entrytime <dec>	Определяет временной интервал (в секундах), в течение которого скорость ADSL линии должна находиться ниже порога, определенного в l2entryrate , чтобы произошел переход из состояния L0 в L2
l2exitrate <dec>	скорость (в килобитах в секундах) линии, при которой идет переход из состояния L2 в L0
l2minrate <dec>	скорость (в килобитах в секундах) линии во время режима L2.

get profile entry

Описание: просмотр параметров глобального профайла

Синтаксис команды:

get profile entry [**name** <name>]

modify profile map

Описание: изменения привязки глобальных профилей ADSL к портам устройства

Синтаксис команды:

modify profile map [**name** <name>] **port** <dec>

Где [**name** <name>] – имя профайла DSL

port <dec>- список портов, к которым прикреплен данный профиль

По умолчанию в системе определено два глобальных профайла ADSL .Профиль с именем **default** “привязан” ко всем интерфейсам устройства.

```

name      : adsl2          stdtype   : adsl2
annexM    : off            mode       : ra          type      : interleave
DS target snr : 60        DS min snr  : 0          DS max snr   : 310
DS min rate  : 64        DS max rate : 28000     DS interleave delay : 16
US target snr : 60        US min snr  : 0          US max snr   : 310
US min rate  : 64        US max rate : 1088      US interleave delay : 16
pmmode     : l2l3        l2 entry rate : 256        l2 entry time  : 1800
l2 exit rate : 512        l2 min rate  : 1024

```

```

name      : default       stdtype   : adsl2plus
annexM    : off            mode       : ra          type      : interleave
DS target snr : 60        DS min snr  : 0          DS max snr   : 310
DS min rate  : 64        DS max rate : 28000     DS interleave delay : 16
US target snr : 60        US min snr  : 0          US max snr   : 310
US min rate  : 64        US max rate : 1088      US interleave delay : 16
pmmode     : l2l3        l2 entry rate : 256        l2 entry time  : 1800
l2 exit rate : 512        l2 min rate  : 1024

```

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, 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 производиться, 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 <i>ifname</i>	Имя AAL-5 интерфейса, лежит в диапазоне aal5-1..aal5-384. Обязательный параметр
e2e seg	Вариант проверки. Необязательный параметр
lbid <i>lbid</i>	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 aal5-1
```

```
$ get oam lpbk vc ifname aal5-1
```

Экранный вывод:

```
IfName      : aal5-1      VPI : 1      VCI : 1
LB Type     : e2e
OAM Location Id : 0xffffffffffffffffffffffffffff
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 Upstream направлении

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

Пример: **get adsl atur physical ifname dsl-1**

Экранный вывод:

```

Ifname                : dsl-1
Serial Number         : C0123456
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 0 255 0 0 15 0 0 0
[16]          7 0 0 0 0 15 0 0 0 0 0 0 0 0 128 0 0
[32]          0 0 0 0 0 0 128 0 0 0 0 128 0 0 0 0 0
[48]          0 0 0 0 0 2 0 0 0 0 0 0 0 0 32 0 0
[64]          0 0 0 0 0 17 0 0 0 0 0 0 0 0 2 0 0
[80]          0 0 0 0 0 0 0 0 0 2 0 0 0 64 0 0
[96]          1 0 0 0 0 60 0 0 0 0 0 0 0 120 0 0
[112]         0 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 0 2 3 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 0 0
[304]         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
[336]         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
[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
[400]         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
[432]         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
[464]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[480]         0 0 0 0 0 48 48 48 48 48 48 48 53 50 0 0
[496]         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
[528]         12 32 0 0 172 84 143 2 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
[560]         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
[592]         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
[624]         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
[656]         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
[688]         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

```

```

[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  0

```

```

[ 8]  0  0  0  0  0  0  0  0  0

```

```

[16]  0  0  0  0  0  0  0  0  0

```

```

[24]  0  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 мощностью АТУ и общей полученной мощностью АТУ интерфейсом (текущее затухание)
CurrAttainable Rate(bps)	Отображает максимальную достижимую текущую скорость передачи данных АТУ интерфейса. Это значение будет равно, или больше текущего значения линейной скорости.
Curr Output Pwr(dB/10)	Измеренная общая мощность, переданная интерфейсом АТУ. 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 АТМ ячейки счетчика.
GsRxA tmCellCounter	Предоставляют Rx АТМ 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
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: dsl1 (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 ifname- наименование подинтерфейса dsl (dsl1 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 ifname- наименование подинтерфейса dsl (dsl1 или dslf)

Пример 1: Параметры буфера Downstream потока (режим Interleave)

```
$ get adsl atuc channel ifname dsl1-23
Ifname           : dsl1-23
Interleave Delay(ms) : 5
Prev Tx Rate(kbps) : 23126900
Gs Curr Atm Status : OK
GsRsDepth        : 64
AtucChanPerfAtmCD : 792738873
AtucChanGsINPdn  : 26
AtucChanGsM0dn   : 1
AtucChanGsB0dn   : 248
Curr Tx Rate(kbps) : 23017900
Crc Block Length(byte) : 47430
GsSymbolsPerRsWord : 34
GsRedundantBytesPerRsCode : 6
AtucChanPerfAtmCU : 0
AtucChanGsL0dn    : 5905
AtucChanGsT0dn    : 2
```

Пример 2: Параметры буфера Downstream потока (режим Interleave)

```
$ get adsl atur channel ifname dsl1-23
Ifname           : dsl1-23
Interleave Delay(ms) : 14
Prev Tx Rate(kbps) : 1008000
Gs Curr Atm Status : OK
GsRsDepth        : 8
AturChanPerfAtmCD : 670933895
AturChanGsINPup   : 180
AturChanGsM0up    : 8
AturChanGsB0up    : 28
Curr Tx Rate(kbps) : 1022400
Crc Block Length(byte) : 2511
GsSymbolsPerRsWord : 701
GsRedundantBytesPerRsCode : 16
AturChanPerfAtmCU : 5342873
AturChanGsL0up    : 283
AturChanGsT0up    : 1
```

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-1**

```

Ifname          : dsl-1
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 превышающий 10 секунд
Perf Stat UASL	Количество секунд за 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 (соответствуют 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 присутствует 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 **atucgsrcfastovrhdup** и **atucgsrcfastovrhddn** 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 – задержку данных в режиме интерливинга (параметры **atucmaxintldelay** и **aturmaxintldelay**), Correction Time- время коррекции данных (параметры **atucgsrcsintcorrectionup** и **atucgsrcsintcorrectiondn**) и Maximum Interleave Depth- максимальная глубина интерливинга (параметр **atucgsrcmaxdco**). Maximum Interleave Depth принимает значения равные - 64,128,256.

Исходя из этих параметров, количество RS байт и другие параметры подсчитывается автоматически.

Общее правило: чем больше Correction Time, и чем больше Interleaving Delay при неизменной Maximum Interleave Depth ,тем больше избыточность информации (количество RS байт).

Формулы для интерливинг параметров:

$Interleaving\ Delay = (D * S) / 4$

$Correction\ time = (S * D * R) / (8 * NI)$,

Где NI = [Number of Bytes] + 1 + R

Параметры :

- S – Число DMT символов в одном кодовом слове
- D - Реальная Interleaving depth
- R – Число избыточных байт в одном кодовом слове
- NI - Количество байт в одном RS фрейме (размер буфера)

Например, для выставленных значений Maximum Interleave Depth= 64, Interleave Delay =16мс, Correction Time= 1мс и размера буфера 65, получаем количество избыточных байтов R=16, S=2 и реальную Interleaving depth =32 (смотрите формулы ниже).

Результирующая вычисленная Interleave Delay =16мс и Correction Time= 0.985 мс.

Примечание: Допускается скорость 4 DMT символа в секунду. Это значит что задержка 16 мс соответствует 64 DMT символам.

3.7. Параметрические тесты DSL линии.

Параметрические тесты в IP DSLAM является одним из многих методов, с помощью которые позволяют операторам связи и телефонным компаниям понизить расходы на ввод и эксплуатацию линий ADSL для своих клиентов. SELT и DELT достигают этой цели уменьшением времени и затрат, необходимых для развертывания новых ADSL2+ линий, так же как и эффективным поиском проблем с линией. SELT и DELT очень отличаются.

SELT, или Single End Loop Test (тест линии с одной стороны) - это возможность ADSL2+ DSLAM. SELT - это тест с одного конца линии, что означает, что медная линия может проверяться только с помощью DSLAM без необходимости в каком-либо внешнем тестирующем оборудовании на центральной станции или на дальнем конце линии.

DELT, или тест на обоих концах линии - возможность, которую имеют и ADSL2+ DSLAM как и ADSL2+ CPE (на стороне клиента) оборудования. Чтобы выполнение DELT было возможным, необходимо, чтобы на обоих концах кабеля было оборудование, поддерживающее данный тест. Это не позволяет использовать DELT на линиях, где CPE оборудование еще не установлено. Но он предлагает полный набор тестов линии и может предоставить очень значащую информацию о состоянии медной линии.

3.7.2. Single End Loop Test (SELT)

SELT - это Single End Loop Test (тест линии с одной стороны), и служит для УПРЕЖДАЮЩИХ тестов медной линии, когда оборудование на дальнем конце не установлено (то есть CPE еще не установлено в доме у клиента). SELT позволяет сделать простую предварительную оценку линии, во время ее монтажа к новому клиенту.

SELT может определить текущие характеристики линии, длину линии, присутствие шумов и потери сигнала на линии, общее качество медной линии и возможность ее использования для доставки сервисов.

Преимущество SELT в том, что это возможность ADSL2+ IP DSLAM и не требуется внешнего оборудования для тестирования. Это может существенно сократить затраты на оборудование, сократив или устранив надобность в дорогом тестирующем оборудовании.

Внимание: тест SELT не доступен с командного интерфейса. Пользуйтесь утилитой AMS LCT для проведения SELT теста.

3.7.1. Dual End Loop Test (DELT)

DELT - это тест на обоих концах (Dual End Loop Test) линии. В отличие от SELT, который тестирует не терминированную медную линию с помощью ADSL2+ IPDSLAM, DELT использует и DSLAM и удаленное ADSL2+ оборудование, чтобы выполнять реактивные тесты в обоих направлениях. Это позволяет иметь гораздо более высокую степень анализа линии, чем просто один SELT.

DELT предоставляет больше информации, чем SELT, но DELT требует совместимый модем на другом конце линии, подразумевая использование этого теста только после того, как CPE будет установлено, что делает DELT очень мощным инструментом диагностики. SELT не требует CPE, что делает этот тест уникальным инструментом для предварительной оценки.

DELT может определить ADSL2+ затухание (вход/исход), сигнал/шум, шум.

DELT является частью промышленного стандарта, который поддерживают производители ADSL2+ чипсетов. Следовательно, ADSL2+ IPDLAM компании D-link могут производить DELT тест в паре с любым ADSL2+ CPE оборудованием, если оно поддерживает DELT.

Пример проведение DELT теста с командного режима:

```
$modify adsl line intf ifname dsl-1 disable  
$modify adsl line intf ifname dsl-1 linedeltconflsf force  
$modify adsl line intf ifname dsl-1 enable
```

Внимание: После тестирования DELT параметр профиля интерфейса, отвечающий за тест, а необходимо вернуть назад в исходное состояние, поскольку в режиме DELT линия не способна передавать пользовательские данные.

Это достигается командами:

```
$modify adsl line intf ifname dsl-1 disable  
$modify adsl line intf ifname dsl-1 linedeltconflsf inhibit  
$modify adsl line intf ifname dsl-1 enable
```

Результаты тестирования доступны по командам просмотра физических параметров линии (результат доступен не ранее чем через 1-2 мин после включения интерфейса)

Максимально достижимая скорость данной линии, определенная в ходе тестирования DELT, показывается командами в параметре **CurrAttainable Rate** командами :

Для Downstream потока

```
$get adsl atuc physical ifname dsl-1 showview concise
```

Для Upstream потока

```
$get adsl atur physical ifname dsl-1 showview concise
```

Шумовые характеристики линии показываются командами:

```
$get adsl atuc physical ifname dsl-1 showview DELT  
$get adsl atur physical ifname dsl-1 showview DELT
```

Результат представляет собой массив значений параметров (значение шума, сигнал/шума, затухания для каждого тона (поднесущей) ADSL:

Delt HLIN= Выводит характеристическую функцию канала, представленную в линейном формате масштабным коэффициентом и комплексным числом. В этом поле отображаются максимальные масштабные коэффициенты для восходящего и нисходящего канала, участвующие в характеристической функции. Результаты диагностики позволяют анализировать неполадки при работе физической ADSL-линии.

Delt HLOG = Выводит характеристики канала в формате, основанном на логарифмической шкале уровней. Эти данные могут применяться при оценке физического состояния ADSL-линии.

Delt QLN = Выводит показатель шума на "тихой" линии – среднее квадратичное значение уровня шума на линии на частотах DMT при отсутствии ADSL-сигналов. Он измеряется в дБм/Гц. Этот показатель может применяться для анализа перекрестных наводок.

Delt DMT Bin SNR = Выводит отношение "сигнал-шум" (в дБ) при передаче от абонента и к абоненту. Соотношение "сигнал-шум" для тонального диапазона DMT – это количественное соотношение мощности принимаемого сигнала к мощности принимаемого шума. Отношение сигнал/шум может использоваться при анализе изменяющихся со временем перекрестных помех и затухания сигнала на линии (например, из-за изменения температуры и влажности).

Signal Atn(dB/10)- суммарное затухание сигнала по всем поднесущим

Пример экранного вывода:

```
$get adsl atuc physical ifname dsl-1 showview DELT
Ifname : dsl-1
Delt HLINSCus   : 32767
Delt HLOGMTus   : 4000   Delt QLNMtus   : 4000
DELT Last Tx State : dmtatucshowtime
Delt SnrmtUs    : 4000   DELT Curr Status : Success
Delt HLINpsus
-----
[0]    32768 32768 32768 32768 32768 32768 32768 32768 32768
[8]    32768 32768 32768 32768 601  64867 1600  738
[16]   367  62427 4679  64332 5213  61659 6015  4144
[24]   58396 62942 7486  1336  58179 65138 270  7083
[32]   6617 64800 59453 1002  5481  64466 64533 60656
[40]   868  4344  64934 61725 3375  65168 65426 62561
[48]   65460 2599  63275 65256 65068 1939  64942 1662
[56]   684  64148 735  64432 64761 789  413  780
Delt HLOGpsus
-----
[0]    1023 1023 1023 1023 1023 1023 372  314
[8]    264  226  200  190  187  187  189  193
```

[16] 198 205 213 223 234 246 257 268

[24] 280 291 303 313 325 338 354 374

Delt QLNpsus

[0] 255 255 255 255 255 255 178 182 174 177 180 175 179 181 176 179

[16] 180 179 181 181 180 181 179 180 181 181 180 180 179 179 180 180

Delt DMT Bin SNR

[0] 255 255 255 255 255 255 119 131 140 146 151 154 158 160 163 166

[16] 168 168 168 168 168 168 167 165 160 159 155 149 145 137 129 64

[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

Signal Atn(dB/10) : 54

4. Инкапсуляция ATM/AAL5. Настройка стека протоколов на DAS-3248.

Основные понятия ATM .

Asynchronous Transfer Mode (ATM) - это метод передачи информации между устройствами в сети маленькими пакетами, называемыми ячейками (cells). ATM служит основной транспортной технологией в сетях ADSL.

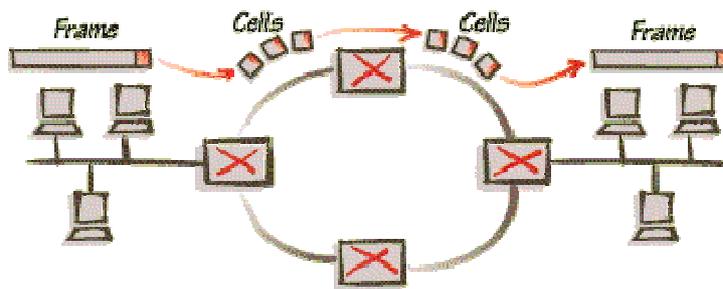


Рисунок 4-1

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 АТМ "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 АТМ. Понятие ААL уровня.

АТМ имеет трехуровневую модель, состоящую из следующих уровней:

- физического;
- уровня АТМ;
- уровня адаптации АТМ.

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



Рисунок 4-2

Наиболее важным является уровень адаптации (АТМ Adaptation Layer, ААL). Он представляет собой набор протоколов ААL1-ААL5, которые преобразуют сообщения протоколов верхних уровней сети АТМ в ячейки АТМ нужного формата. Протоколы ААL при передаче пользовательского трафика работают только в конечных узлах сети (см. рис 3), как и транспортные протоколы большинства технологий.

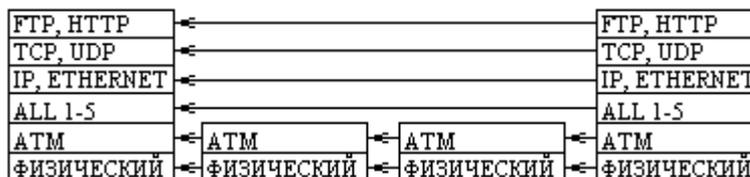


Рисунок 4-3

Уровень адаптации состоит из нескольких подуровней (см. рис.2). Нижний подуровень ААL называется подуровнем сегментации и реассемблирования (Segmentation And Reassembly, SAR). Эта часть не зависит от типа протокола ААL 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 передаче по сети ATM коммутируемых (Bridged) протоколов.

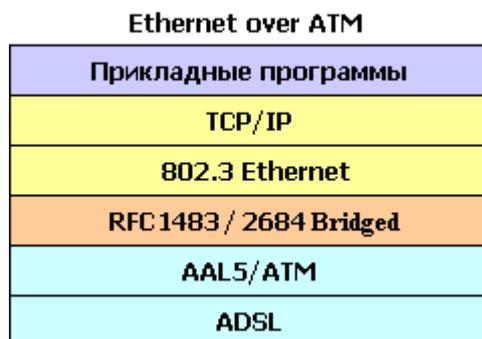


Рисунок 4-4

- **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.

IP over ATM



Рисунок 4-6

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

IP over ATM



Рисунок 4-7

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

PPP over ATM



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 АТМ существует **два** подхода к мультиплексированию данных по каналам АТМ.

Первый метод заключается в мультиплексировании множества протоколов поверх **одного** виртуального канала АТМ. 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

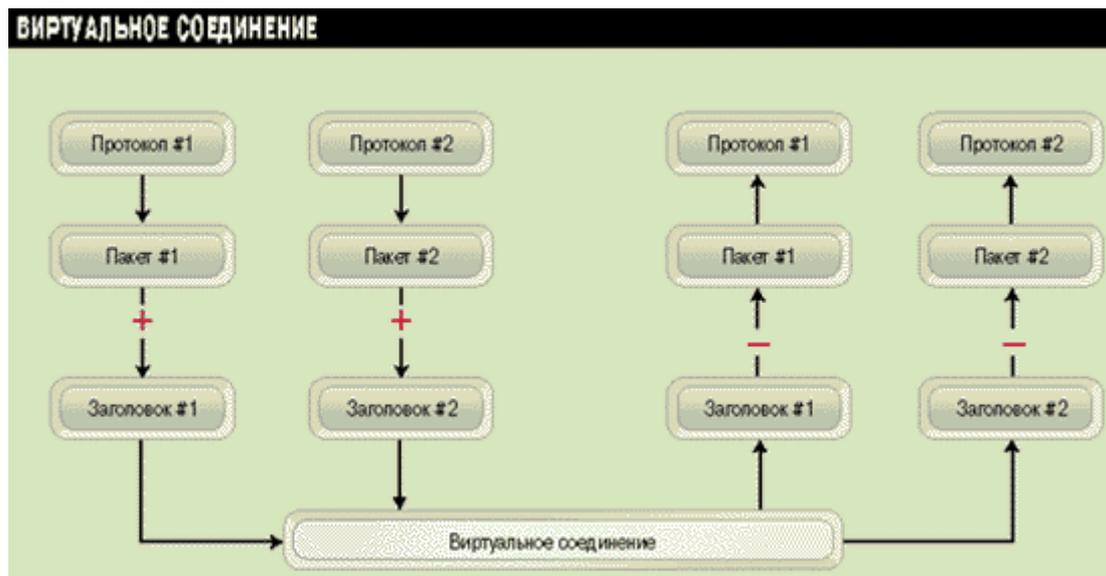


Рисунок 4-9

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 АТМ. 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 АТМ.

Используются для управления АТМ функционалом DAS-3248. Названия АТМ интерфейсов лежат в диапазоне atm-1...atm-48. Интерфейс atm-1 соответствует 1-ому ADSL порту, atm-48 – сорок восьмому. АТМ интерфейсы являются вышележащими над DSL интерфейсами и нижележащими для АТМ VC интерфейсов.

create atm port

Описание: Используется для создания АТМ порта.

Синтаксис команды: **create atm port ifname** interface-name **lowif** dsl-portinterface-name [enable | disable] [**Maxvpibits** maxvpibits][**Maxvcibits** maxvcibits] [**Orl** Or1]

modify atm port

Описание: используется для включения/выключения АТМ порта.

Синтаксис команды: **modify atm port ifname** interface-name [enable | disable] [**maxvcs** maxvcs] [**Maxvpibits** maxvpibits] [**Maxvcibits** maxvcibits][**Orl** Or1]

delete atm port

Описание: используется для удаления АТМ порта.

Синтаксис команды: **delete atm port ifname** interface-name

get atm port

Описание: используется для получения информации по одному определенному АТМ порту либо по всем АТМ портам.

Синтаксис команды: **get atm port [ifname** interface-name]

Таблица описания параметров команд:

ifname ifname	Имя DSL интерфейса, лежит в диапазоне dsl-1..dsl-48. Обязательный параметр.
lowif dsl-port-interfacename	Идентификатор DSL интерфейса, для которого настраивается АТМ Необязательный параметр.
enable disable	Статус АТМ 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 АТМ интерфейса.

	Значения параметров: от 1 до 8. Необязательный параметр.
maxvc <i>max-num-vccs</i>	Максимальный номер идентификатора виртуального пути (канала), поддерживаемого ATM интерфейсом. Необязательный параметр.
Maxvpibits <i>max-vpi-bits</i>	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-1

Экраниый вывод:

```

IfName: atm-1:
LowIfName : dal-
Class0thrshld :
MaxVccs: 4
MaxVpiBits : 9
RowStatus
Class1thrshld
Class0thrshld :UnknownVCI : 3
MaxVciBits : 10
Class0thrshld :Class1thrshld
Class0thrshld :
OAMSrc : 0xffffffffffffffffffffffffffff
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 (aal5-1...aal5-48) – на каждый ATM порт по одному VC. Имена данных PVC интерфейсов лежат в интервале: aal5-1 -aal5-48, где aal5-1 соответствует первому adsl порту, а aal5-48 – 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 aal5-49...aal5-384. 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-interface-name
[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 <i>ifname</i>	имя ATM VC интерфейса, лежит в диапазоне aal5-1..aal5-384. Обязательный параметр.
vpi <i>vpi</i>	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 <i>vci</i>	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 <i>atm-port-interfacename</i>	Имя ATM интерфейса, на котором будет создан данный VC интерфейс. Обязательный параметр.
enable disable	Административный статус VC интерфейса. Оptionальный параметр. Значение по умолчанию enable.
aal5	Тип AAL, используемый в VC. Поддерживается только AAL5. Оptionальный параметр. Значение по умолчанию aal5.
a5txsize <i>aal5-cpcs-tx-sdu-size</i>	Максимальный размер передаваемого CPCS SDU. Оptionальный параметр. Значение по умолчанию 1536.
a5rxsize <i>aal5-cpcs-rx-sdu-size</i>	Максимальный размер принимаемого CPCS SDU. Оptionальный параметр. Значение по умолчанию 1536.
vcmux lscmux auto	Метод мультиплексирования. Оptionальный параметр. Значение по умолчанию lscmux.
pvc	Тип PVC. Поддерживается только PVC. Оptionальный параметр. Значение по умолчанию pvc.
channel <i>fast interleaved</i>	Тип канала, по которому будут передаваться/приниматься ячейки данного PVC. Оptionальный параметр. Значение по умолчанию interleaved.
mgmtmode <i>data mgmt DataAndMgmt raw</i>	Определяет Management Mode данного ATM PVC. <ol style="list-style-type: none"> Data - через данное PVC будет передаваться только data пакеты. Mgmt – через данное PVC можно управлять CPE устройством. В случае Mgmt PVC поверх него не может быть создан EOA интерфейс. DataAndMgmt – по одному ATM PVC может осуществляться как передача

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

Пример:

Команда для создания нового ATM VC LLC based поверх порта atm-24 (24 порт ADSL) с параметрами VPI 8, VCI 35:

create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-24

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-24
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.

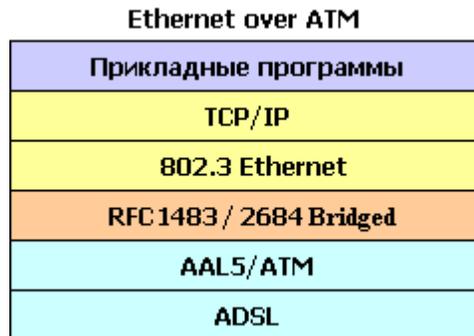


Рисунок 4-10

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 протокола PPPoE для прозрачной передачи пакетов от клиентских устройств к серверу авторизации PPPoE (BRAS- Broadband Remote Access Server).

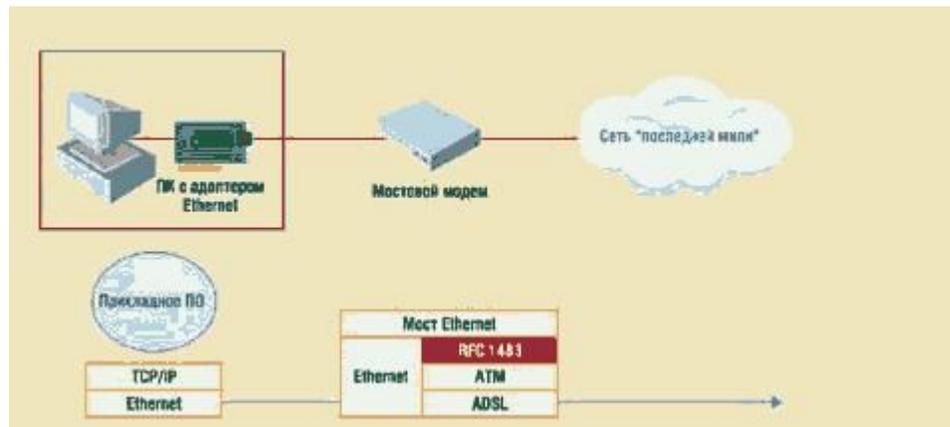


Рисунок 4-11

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

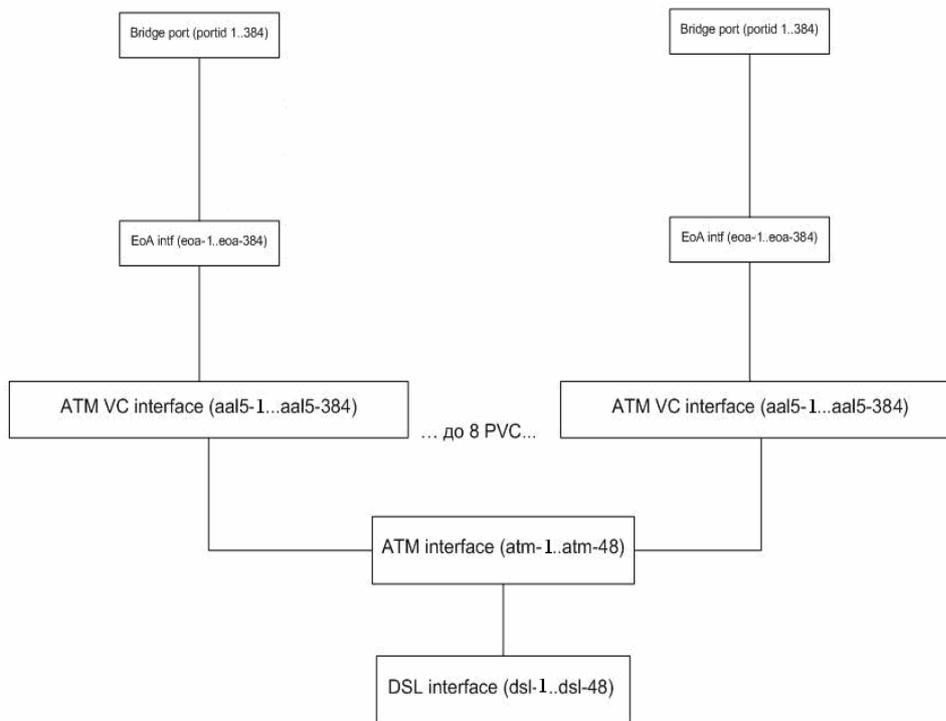


Рисунок 4-12

Внимание:

По умолчанию в системе уже созданы 48 ЕоА интерфейсов с именами eoa-1...eoa-48 (поверх каждого АТМ VC).

Кроме того, поверх каждого из интерфейсов ЕоА 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 АТМ VC интерфейса.

То есть:

- 1) Создать АТМ VC интерфейс;
- 2) Создать ЕоА интерфейс;
- 3) Создать Bridge интерфейс.

Пример:

```

create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-24
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-1..eoa-384. По умолчанию созданы 48 EoA интерфейсов с именами eoa-1...eoa-48 (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 <i>ifname</i>	имя EoA интерфейса, лежит в диапазоне eoa-1..eoa-384. Обязательный параметр.
lowif <i>lowif</i>	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, проверяться 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 только 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 **pktype** интерфейса eoa-51 на новые значения (pktype bcast):

modify eoa intf ifname eoa-51 pktype bcast

delete atm eoa intf

Описание: удаляет ЕоА интерфейс

Синтаксис команды:

delete eoa intf ifname ifname

Пример:

команда удаления ЕоА интерфейса eoa-51

delete eoa intf ifname eoa-51

get eoa intf

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

Синтаксис команды:

get eoa intf [ifname ifname]

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

Пример: Просмотр статуса интерфейса eoa-51

get eoa intf ifname eoa-51

Экранный вывод:

IfName	:eoa-	LowIfName	:
51		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 диапазоне 1–384. 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. Оptionальный параметр. Значение по умолчанию 16.
learning enable disable	Включает и выключает режим обучения MAC адресам. Оptionальный параметр. Значение по умолчанию enable.
status enable disable	Административный статус Bridge интерфейса. Оptionальный параметр. Значение по умолчанию enable.
stickystatus enable disable	Включает режим постоянной привязки MAC адресов к bridge порту. В состоянии enable запись о MAC адресе не устаревает, поэтому однажды обученный определенному MAC

	<p>адресу, порт сохраняет запись и не дает «обучиться» данному MAC другой порт. Запись о MAC может быть стерта административным выключением интерфейса или переводом данной настройки в состояние disable(по истечению таймаута)</p> <p>В состоянии disable запись о MAC устаревает через некоторое время, поэтому другой bridge port может «обучиться» MAC через определенное время (по таймауту)</p> <p>Внимание : При использовании режима sticky необходимо выключить floodsupport (для запрещения хождения пакетов от неизвестных источников) глобально командой \$modify bridge tbg info floodsupport disable</p> <p>Или на отдельном VLAN :</p> <p>\$modify vlan static vlanid xx floodSupport disable.</p> <p>Опциональный параметр. Значение по умолчанию disable.</p>
<p>fdbmodify enable disable</p>	<p>Определяет, может ли порт самостоятельно изменять базу данных MAC адресов (fdb)</p> <p>Опциональный параметр. Значение по умолчанию enable.</p>
<p>aclGlbDenyApply enable disable</p>	<p>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.</p> <p>Enable- глобальный список применим к порту.</p> <p>Disable- не применим.</p> <p>Опциональный параметр. Значение по умолчанию enable.</p>
<p>aclGlbTrackApply Enable Disable</p>	<p>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.</p>

	<p>Enable- глобальный список применим к порту.</p> <p>Disable- не применим.</p> <p>Опциональный параметр. Значение по умолчанию enable.</p>
--	--

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 (learning 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	:	eo-a-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

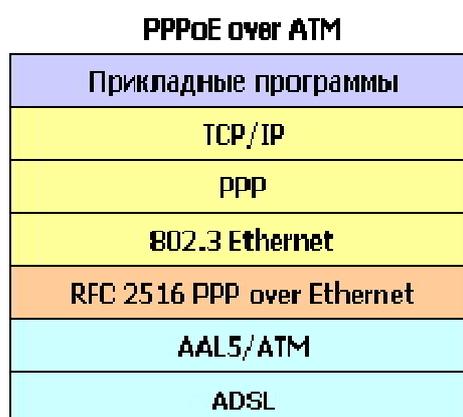


Рисунок 14

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

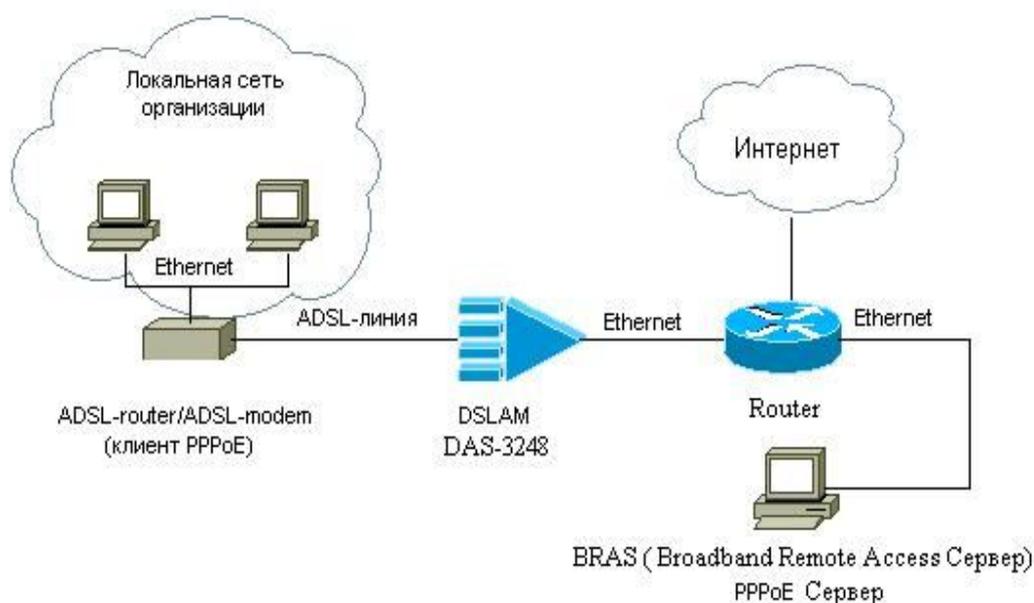


Рисунок 4-15

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).

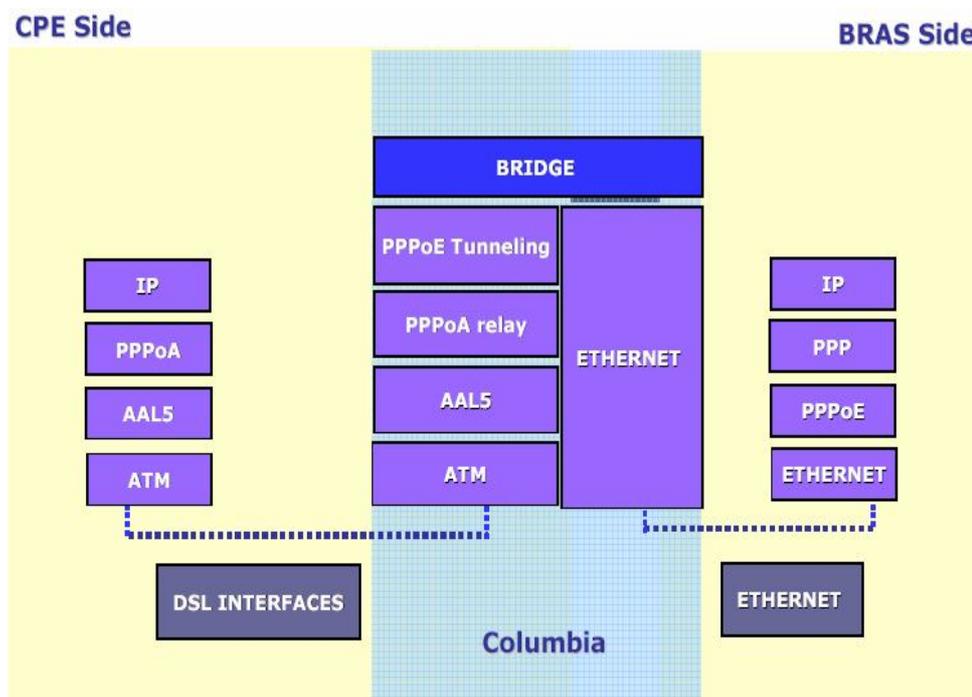


Рисунок 4-16: Стек протоколов для PPPoA to PPPoE Internetworking

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 завершении 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.

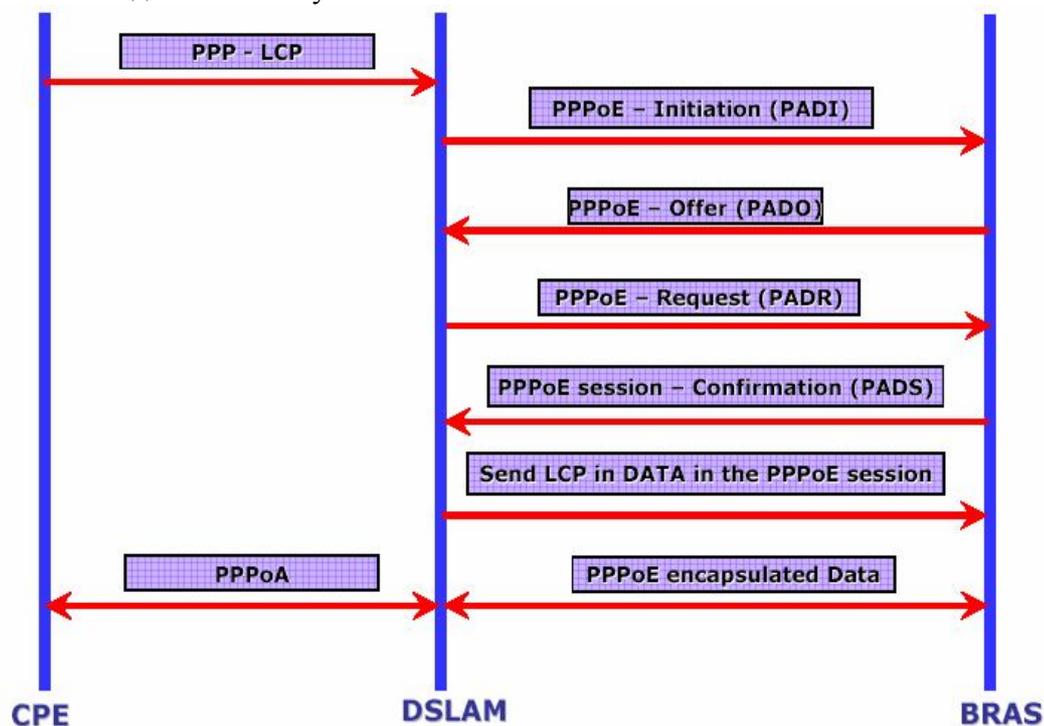


Рисунок 4-17: Инициирование PPPoA to PPPoE

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

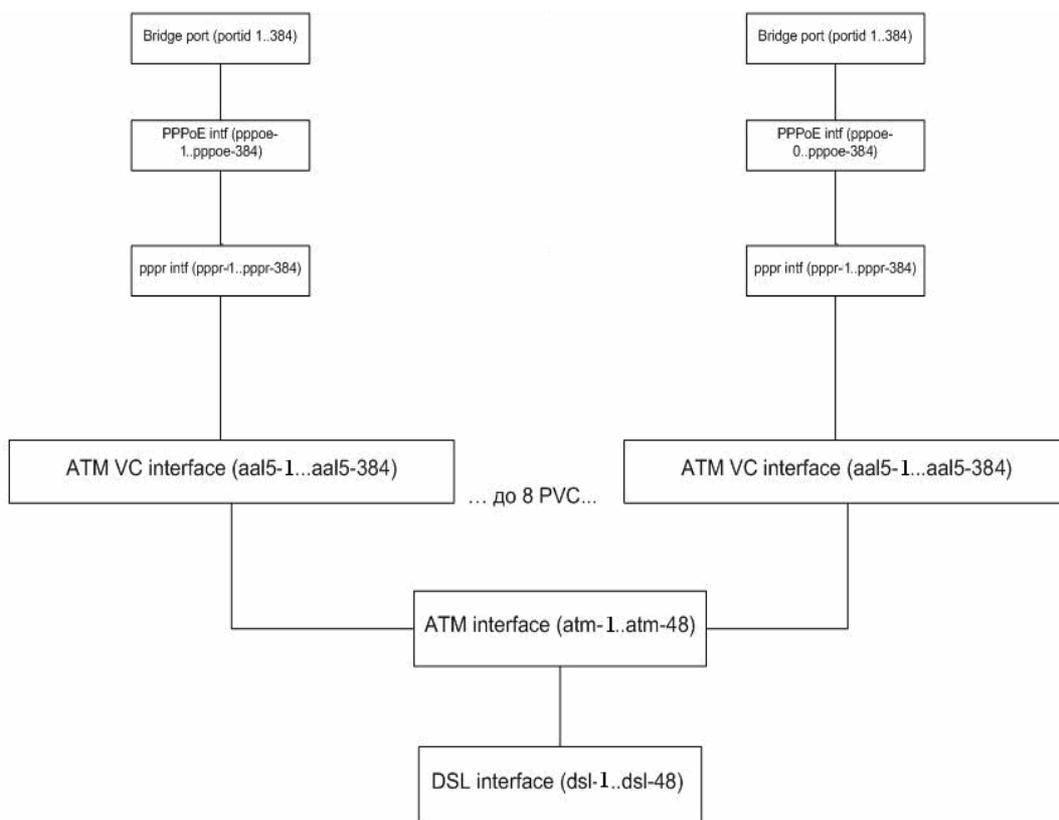


Рисунок 4-18

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-1...pppr-384.

create pppr intf

Описание: создает новый PPPR интерфейс.

Синтаксис команды:

```
create pppr intf ifname ifname lowif lowif  
[ maxpdu maxpdu ] [ ppprackto ppprackto]  
[ lowiftoggetimerto lowiftoggetimerto ] [nature dynamic | static ]  
[configstatus Normal | Config ] [enable | disable]
```

Таблица описания параметров команд:

ifname <i>ifname</i>	имя PPPR интерфейса, лежит в диапазоне pppr-1..pppr-384. Обязательный параметр.
lowif <i>lowif</i>	Имя AAL5 интерфейса, на котором будет создан данный PPPR интерфейс. Обязательный параметр.
maxpdu <i>maxpdu</i>	Максимальный размер блока данных ATM PDU (Protocol Data Unit) Оptionальный параметр. Значение по умолчанию 1492.
ppprackto <i>ppprackto</i>	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. Оptionальный параметр.
lowiftoggetimerto <i>lowiftoggetimerto</i>	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-1...pppoe-384.

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 <i>if-name</i>	имя PPPoE интерфейса, лежит в диапазоне pppoe-1..ppoe-384. Обязательный параметр.
lowif <i>lowif</i>	Имя PPPR интерфейса, на котором будет создан данный PPPoE интерфейс. Обязательный параметр.
wanbridgeport <i>wanbridgeport</i>	Определяет WAN bridge порт, привязанный к интерфейсу.0 означает, что доступен любой bridge порт. Поддерживается только значение 0. Оptionальный параметр. Значение по умолчанию 0.
sessionid <i>sessionid</i>	Идентификатор сессии pppoe (session id). Данный параметр принимается только в случае статической сессии pppoe. Оptionальный параметр. Диапазон значений 0-65535. Значение по умолчанию 0.
acmacaddr <i>acmacaddr</i>	AC (Access Concentrator) MAC- MAC адрес BRAS сервера, который будет использовать DAS-3248 для установления PPPoE сессии. Оptionальный параметр.
macaddrprof <i>macaddrprof</i>	Profile id (идентификатор профиля), в котором указан MAC адрес интерфейса DAS-3248 для установления PPPoE сессии. Обязательный параметр
servicenameprof <i>servicenameprof</i>	Profile id (идентификатор профиля), в котором указано Service Name (имя сервиса) BRAS сервера, который будет

	использоваться DAS-3248. Значение <i>any</i> обозначает, что нет необходимости использовать AC Name. Значение <i>anyconfigured</i> означает, что любое значение AC будет принято. Опциональный параметр. Значение по умолчанию any
acnameprof <i>acnameprof</i>	Profile id (идентификатор профиля), в котором указано AC Name (Access Concentrator Name)- имя BRAS сервера, которое будет использоваться DAS-3248. Значение <i>any</i> обозначает, что нет необходимости использовать AC Name. Значение <i>anyconfigured</i> означает, что любое значение AC будет принято Опциональный параметр. Значение по умолчанию any
ethpkttype <i>type2 802_3</i>	Определяет тип передаваемых пакетов Ethernet (802.3 или Type2). Опциональный параметр.
nature <i>dynamic static</i>	Определяет, является ли интерфейс статическим или динамическим. Dynamic-динамический Static-статический. Опциональный параметр.
enable 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** Type2|802_3] [**nature** dynamic | static] [**enable|disable**]

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	<pre>\$create atm vc intf ifname aal5-51 vpi 8 vci 35 lowif atm-24</pre>	Создать новый ATM VC интерфейс поверх 24 ADSL порта с параметрами VPI 8, VCI 35
Шаг 2	<pre>\$create pppr intf ifname pppr-51 lowif aal5-51</pre>	Создать PPPoA Relay интерфейс непосредственно над AAL5 интерфейсом:
Шаг 3	<pre>\$ create macprofile global profileid 1 macaddr 00:0E:7F:61:C1:BE</pre>	Указывать MAC адрес, который будет использовать DAS-3248 для установления PPPoE сессии:
Шаг 4	<pre>\$create pppoe global serviceprofile profileid 1 servicename ISP1</pre>	Указать Service Name, который будет использоваться DAS-3248 (необязательный параметр)
Шаг 5	<pre>\$create pppoe intf ifname pppoe-51 lowif pppr-51 servicenameprof 1 macaddrprof 1</pre>	Создать PPPoE интерфейс
Шаг 6	<pre>\$create filter rule entry ruleid 2 action sendtocontrol ruledir in applywhenreq enable description PPPR_CONTROL</pre>	Создать правило Generic фильтра так, чтобы все пакеты LCP передавались управляющему процессу. Это необходимо для обнаружения PPPoA сессии со стороны CPE.
Шаг 7	<pre>create filter subrule ppp ruleid 2 subruleid 1 prototypefrom 0xc021 prototypecmp eq</pre>	Создать подправило с указанием LCP протокола (тип протокола 0xc021)
Шаг 8	<pre>modify filter rule entry ruleid 2 status enable</pre>	Включить созданное правило
Шаг 9	<pre>create filter rule map ifname allpppoe stageid 1 ruleid 2</pre>	Привязать данное правило ко всем PPPoE интерфейсам
Шаг 10	<pre>create bridge port intf portid 52 ifname pppoe-51</pre>	Создать bridge port поверх ранее созданного PPPoE интерфейса

Шаг 11	<pre>\$modify pppr intf ifname pppr-51 enable \$modify pppoe intf ifname pppoe-51 enable \$modify bridge port intf portid 52 status enable</pre>	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 передаче 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

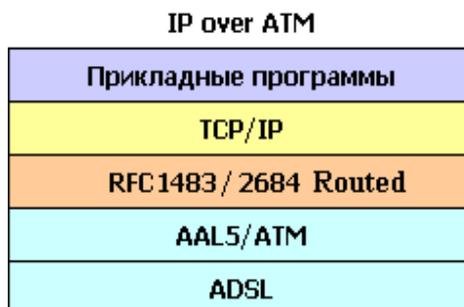


Рисунок 4-20

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).

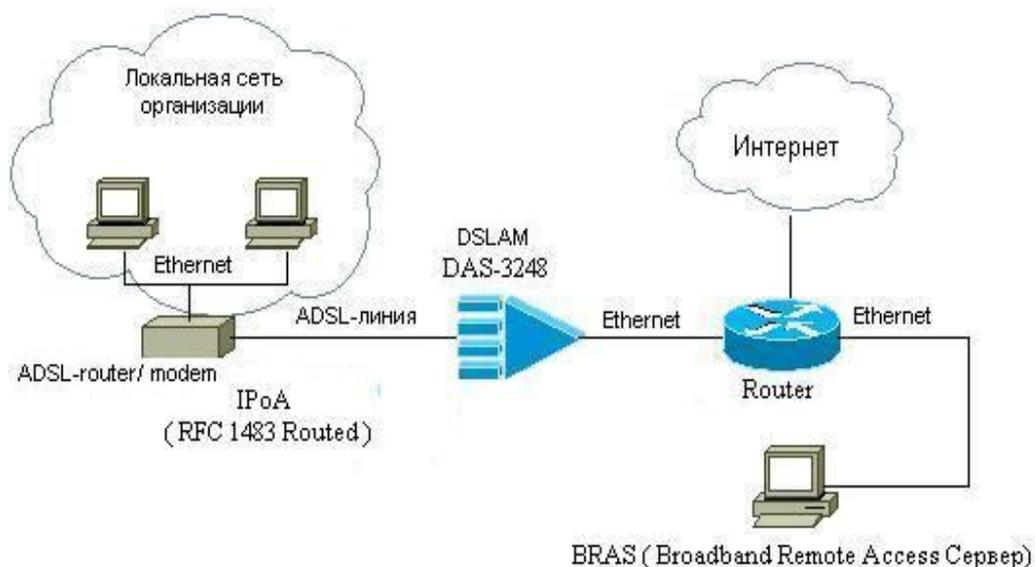


Рисунок 4-21

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).

Upstream трафик, протекающий от DSL к Ethernet интерфейсам DAS-3248, показан на рисунке 4-22 жирной стрелкой, начинающейся на CPE стороне DSLAM (DSL интерфейс). 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 интерфейс).

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.

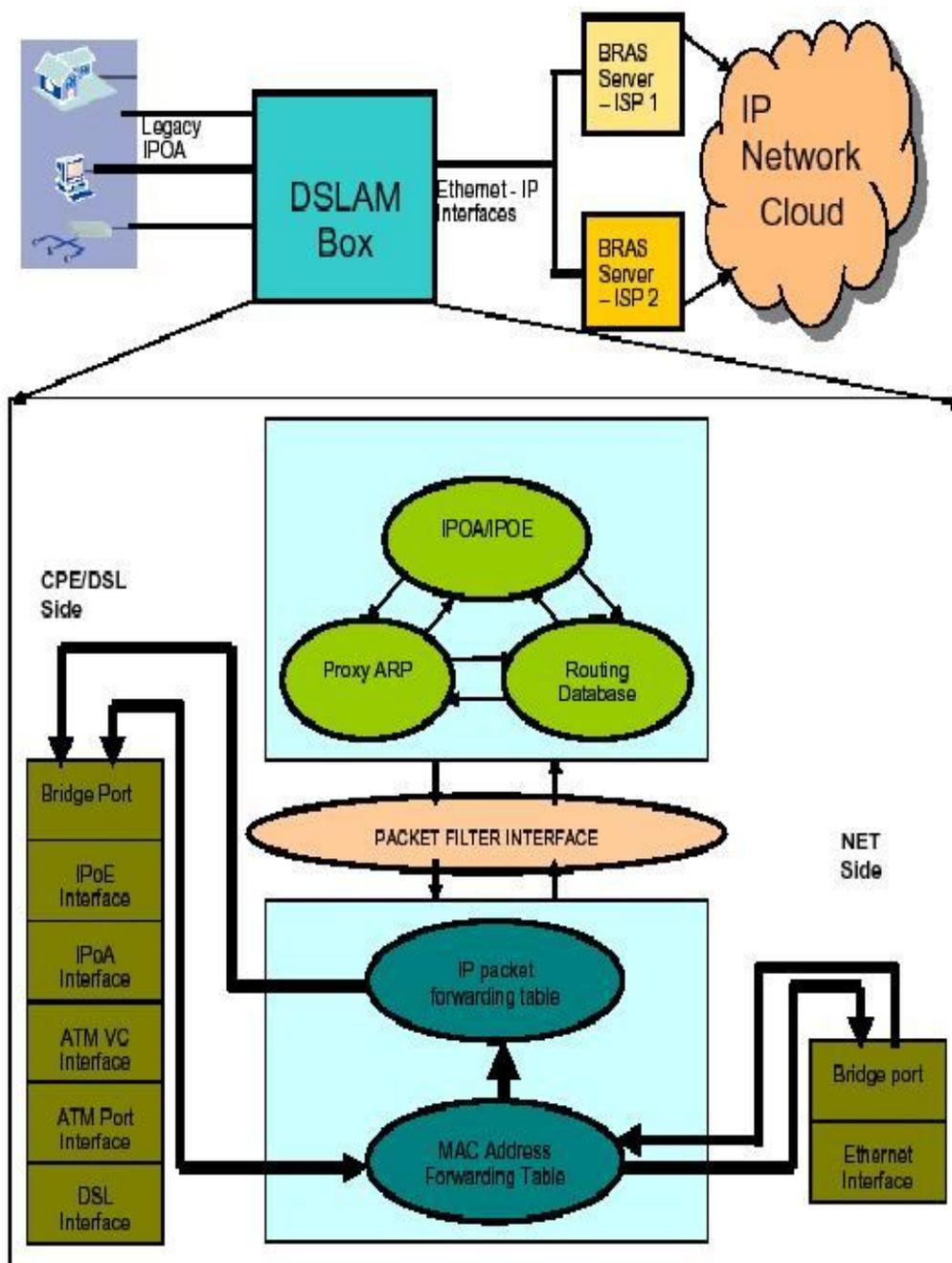


Рисунок 4-22.

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 используются 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 (Proxu ARP Module)

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

Управление ARP записями;

Генерация ARP запросов для разрешения соответствий IP-МАС. В случае IPoE это разрешение APR соответствий для BRAS серверов;
Обновление ARP кеша после обработки ARP ответов;
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:

- 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;
конфигурирование Bridge порта над IPoE интерфейсом;
3) обработка триггеров от модулей ARP Proxu 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 ответственна 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:

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.

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).

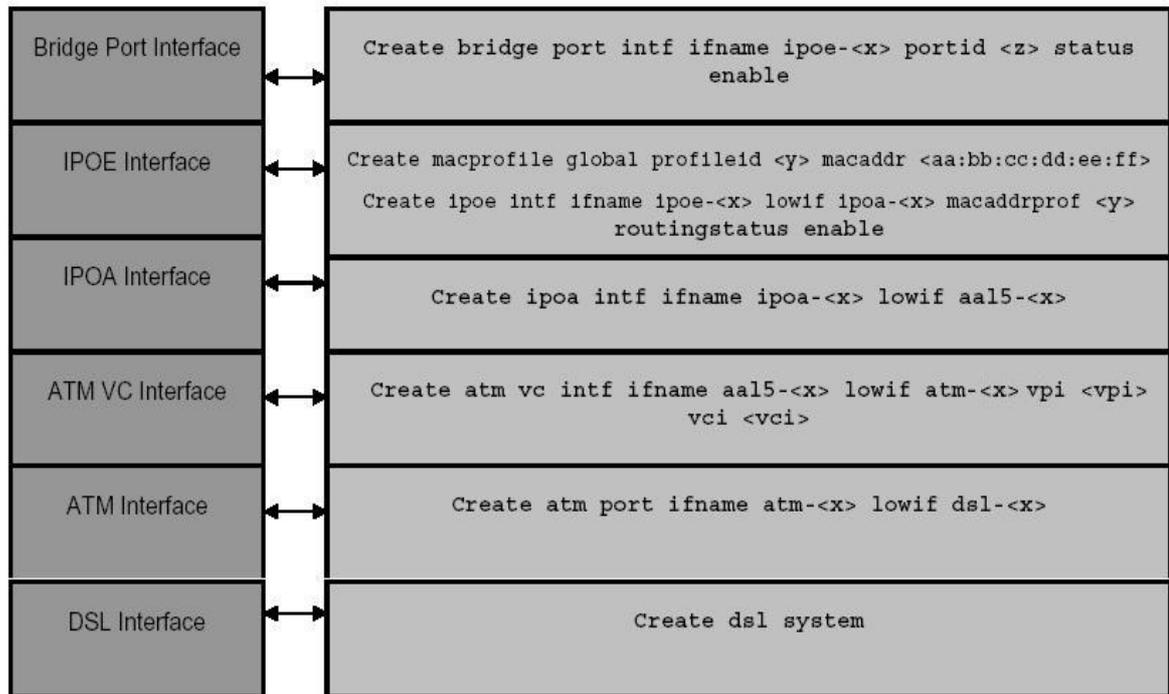


Рисунок 4-23

4.5.3.2 WAN/NET Сторона DAS-3248.

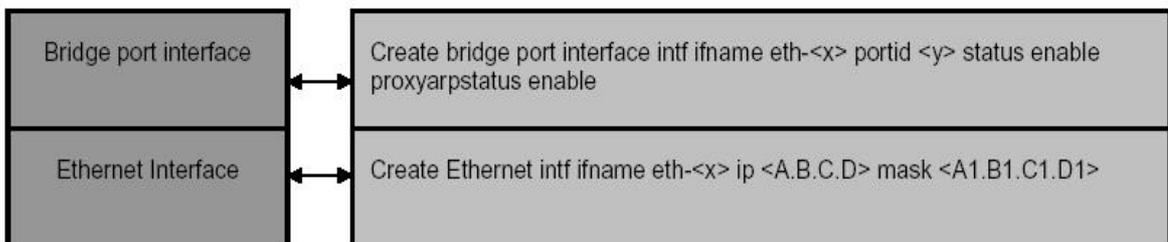


Рисунок 4-24

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 <i>ifname</i>	имя EoA интерфейса, лежит в диапазоне ipoa-1..ipoa-384. Обязательный параметр.
lowif <i>lowif</i>	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. Оptionальный параметр. Поддерживается только значение Normal. Значение по умолчанию Normal.
enable disable	Административный статус EoA интерфейса. Оptionальный 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 <i>ifname</i>	имя IPoE интерфейса, лежит в диапазоне eoa-1..eoa-384. Обязательный параметр.
lowif <i>lowif</i>	Имя IPoA интерфейса, на котором будет создан данный IPoE интерфейс. Обязательный параметр.
macaddrprof <i>macaddrprof</i>	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 Оptionальный параметр. Значение по умолчанию Type2.
inactivitytmrintrvl <i>inactivitytmrintrvl</i>	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 другим 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-1 или eth-2 интерфейс.

Кроме того, в контексте IPoA to IPoE Tunneling, вводится дополнительный параметр для Bridge порта.

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

Пример:

```
create bridge port intf ifname eth-1 portid 53 status enable proхуarpstatus 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 gwypip <A.B.C.D> ifname ANYWAN
```

Шлюз (gwypip)- 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 .

```
$create vlan static vlanid <m> vlnname <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 конфигурирование 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 .

```
$create vlan static vlanid <m> vlnname <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 разрешаться динамически.

```
$create ip route rid <X> ip <E.F.G.H> mask 255.255.255.255 gwyp <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

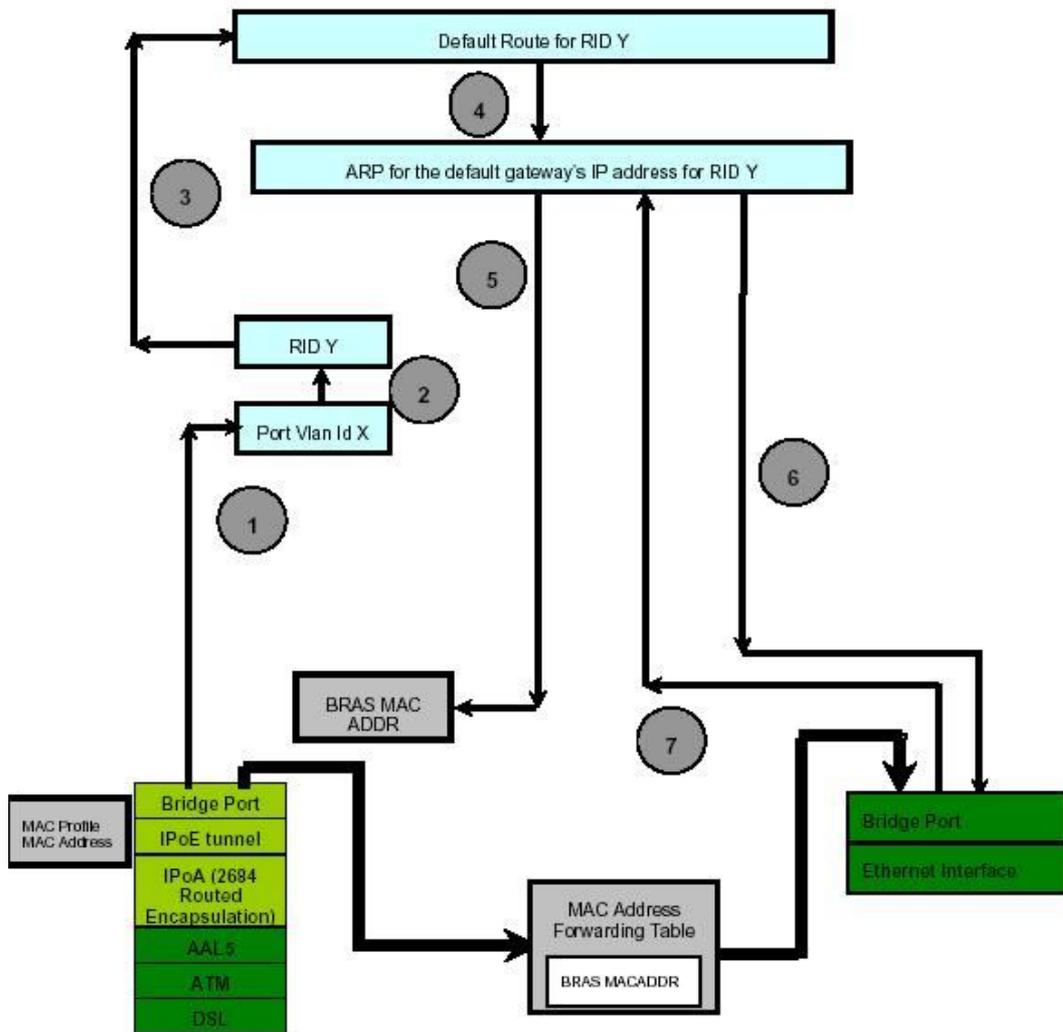


Рисунок 4-25. Алгоритм IPoA to IPoE в Upstream направлении

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 туннелироваться 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.

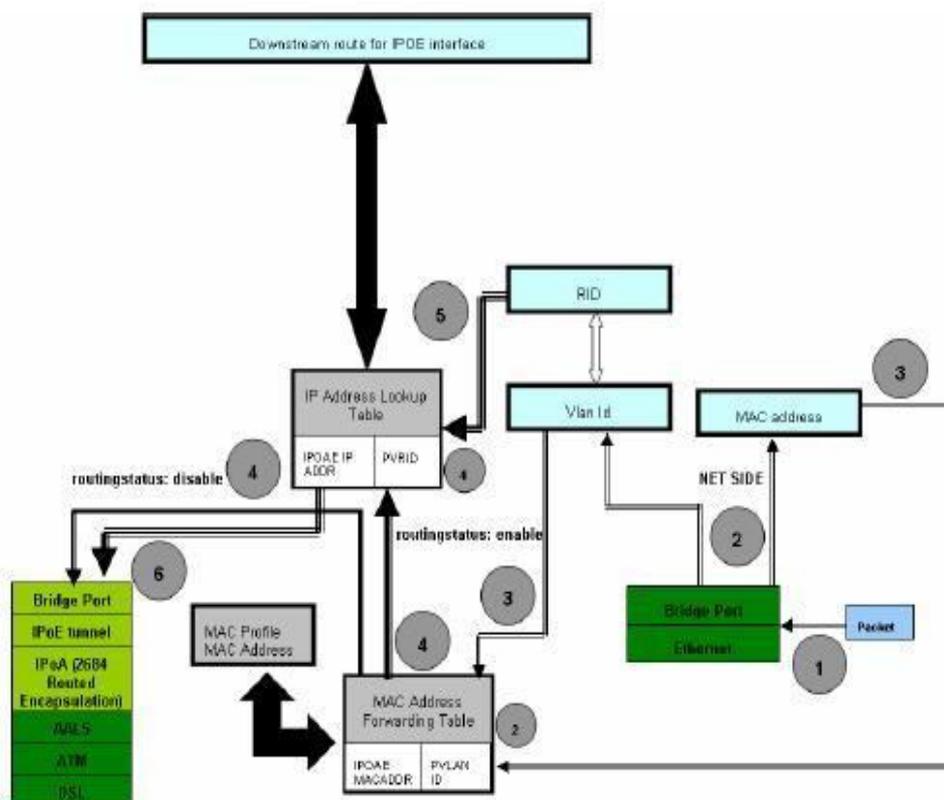


Рисунок 4-26. Алгоритм работы IPoA to IPoE в Downstream направлении

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, базирясь 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 устанавливается 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 членами 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

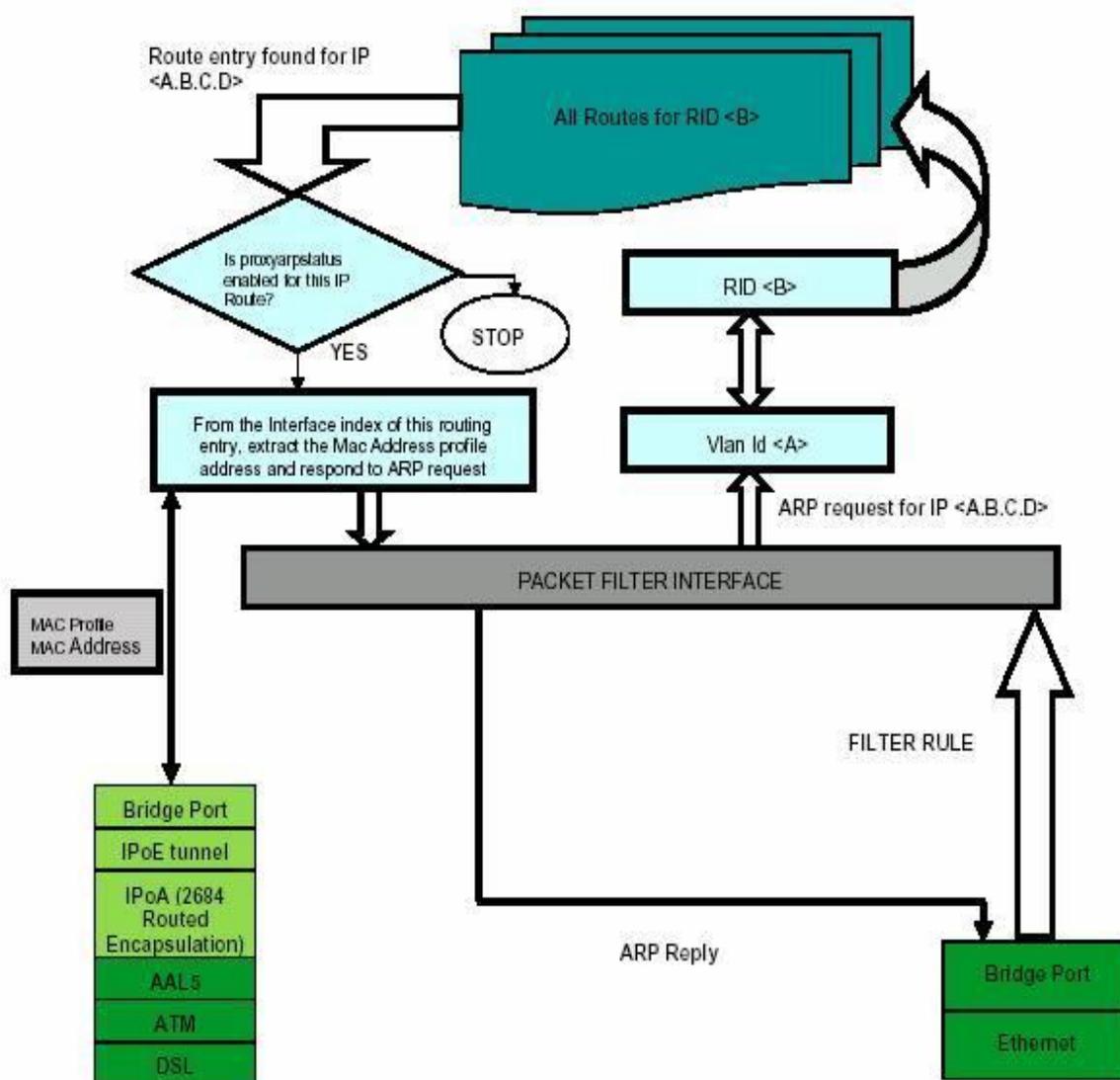


Рисунок 4-27. Алгоритм работы ARP-прокси

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 `prohуarpstatus` 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`.

Следующие CLI команды показывают конфигурирование ARP-прокси:

1. `$modify bridge port intf portid <X> prohуarpstatus enable`
Эта команда показывает, что ARP запросы, полученные с WAN интерфейса DSLAM, соответствующего этому порту моста будут разрешаться, используя ARP-прокси.
2. `$modify ip route rid <Z> ip <A.B.C.D> mask <E.F.G.H> prohуarpstatus 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 были 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-1 (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 Проху ARP.

BRAS сервер имеет IP 192.168.100.1 и MAC адрес 00:0E:7F:61:C1:BE

	Команда	Действие
Шаг 1	<code>\$vlan static vlanid 3 vlanname IPoE_1</code>	Создать соответствующий VLAN
Шаг 2	<code>\$create rid static rid 3</code>	Создать RID
Шаг 3	<code>\$create ip route rid 3 ip 0.0.0.0 mask 0.0.0.0 gwyp 192.168.100.1 ifname anywan</code>	Создать default route для этого RID
Шаг 4	<code>\$create atm vc intf ifname aal5-51 vpi 1 vci 50 lowif atm-24</code>	Создать новый ATM VC интерфейс поверх 24 ADSL порта с параметрами VPI 1, VCI 50
Шаг 5	<code>\$create ipoa intf ifname ipoa-51 lowif aal5-51</code>	Создать IPoA интерфейс непосредственно над AAL5 интерфейсом.
Шаг 6	<code>\$create macprofile global profile id 1 macaddr 00:0E:7F:61:C1:BE</code>	Указать MAC профиль, который будет использоваться IPoE интерфейсом
Шаг 7	<code>\$create ipoe intf ifname ipoe-51 lowif ipoa-51 macaddrprof 1 routingstatus enable</code>	Создать IPoE интерфейс
Шаг 8	<code>\$create bridge port intf ifname ipoe-51 portid 52</code>	Создать bridge интерфейс поверх IPoE интерфейса
Шаг 9	<code>\$modify vlan static vlanname IPoE_1 egressports 52 385</code>	Сделать CPE bridge порт и WAN bridge порт членами соответствующего VLAN
Шаг 10	<code>\$modify gvrp port info portid 52 portvlanid 3</code>	Включить CPE bridge порт в VLAN
Шаг 11	<code>\$create ip route rid 3 ip 192.168.100.200 mask 255.255.255.255 gwyp 192.168.100.200 ifname ipoe-51 ProxyArpStatus enable</code>	Присвоить IPoE интерфейсу IP и создать маршрут с этим IP и соответствующим RID (Проху ARP включен)
Шаг 12	<code>\$modify bridge port intf portid 385 proxyarpstatus enable</code>	Включить Проху ARP на WAN bridge интерфейсе
Шаг 13	<code>\$create filter rule entry ruleid 2 action copytocontrol description IPOE_CONTROL applywhenreq enable</code>	Создать правило с действием 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 ethertype from 0x806 ethertype cmp eq dstmacaddr from ff:ff:ff:ff:ff:ff dstmacaddr cmp 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 были 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

5. Дополнительные возможности технологий доступа в сетях ADSL

5.1. Виды технологий доступа в сетях ADSL

Схема со статическими (фиксированными) IP адресами.

Данная схема является самой простой, но и самой негибкой.

В такой схеме DSLAM и модем выполняют роль прозрачного моста и по сути своей являются как бы “удлинителем” обычной сети Ethernet посредством технологии ADSL. IP адрес присваивается на конечном компьютере пользователя, а все устройства находятся в одной «плоской» сети.

Вариантом такой схемы является случай, когда модем клиента выполняет роль маршрутизатора. В этом случае статический IP адрес жестко присваивается уже на WAN интерфейсе модема, а за модемом может скрываться несколько локальных компьютеров пользователей.

Тем не менее, даже в этой схеме DSLAM выполняет роль прозрачного моста.

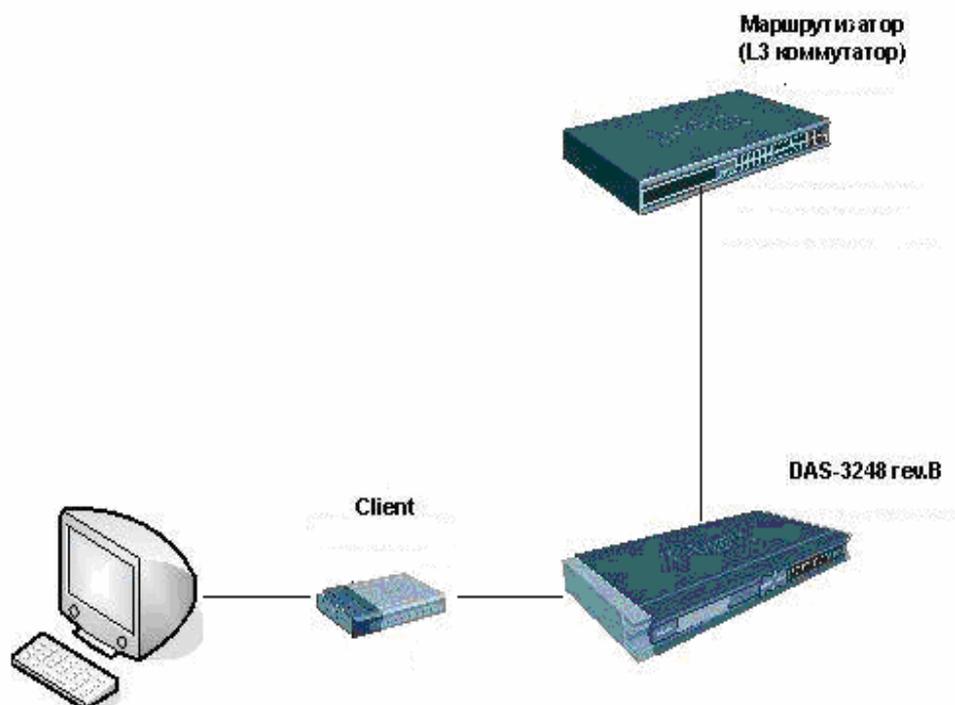


Рисунок 4-28. Схема ADSL доступа с фиксированными IP адресами

DHCP. Сущность DHCP – централизованная раздача IP адресов клиентам с сервера DHCP. Данная схема является более управляемой и позволяет управлять раздачей IP адресов абонентам в соответствии с политиками безопасности и управления, настроенными на DHCP сервере.

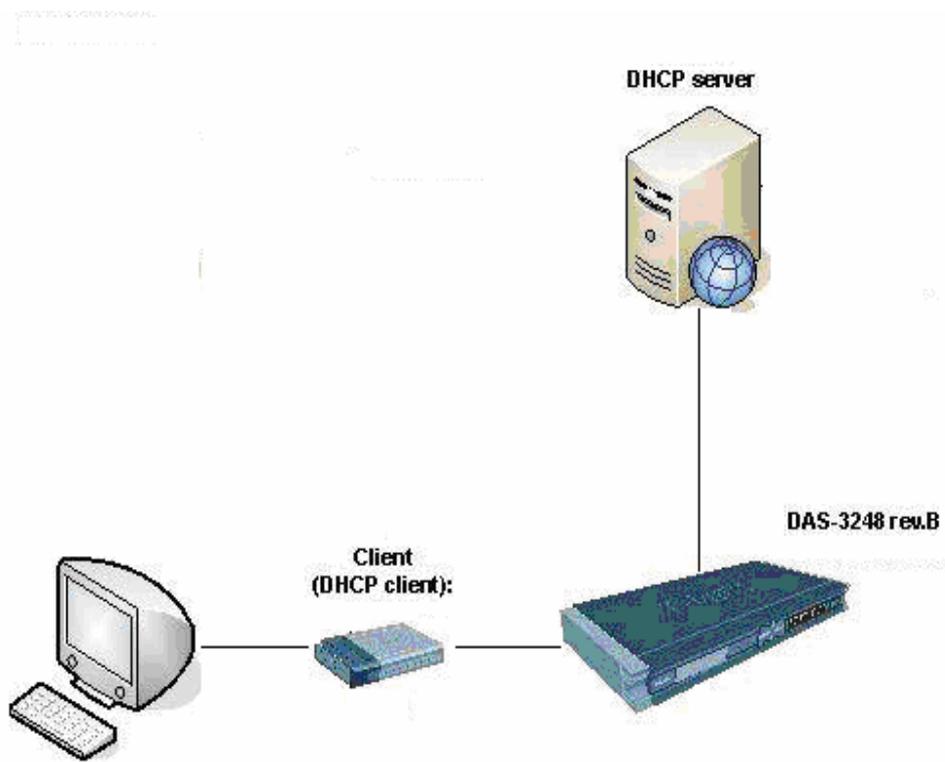


Рисунок 4-29. Схема ADSL доступа по DHCP технологии

2.PPPoE. Сущность PPPoE- простая аутентификация пользователя на основе связки логин/пароль, хранящийся на PPPoE сервере. Также как и DHCP, данная схема является управляемой и позволяет управлять раздачей IP адресов в соответствии с политиками безопасности и управления, настроенными на PPPoE сервере.

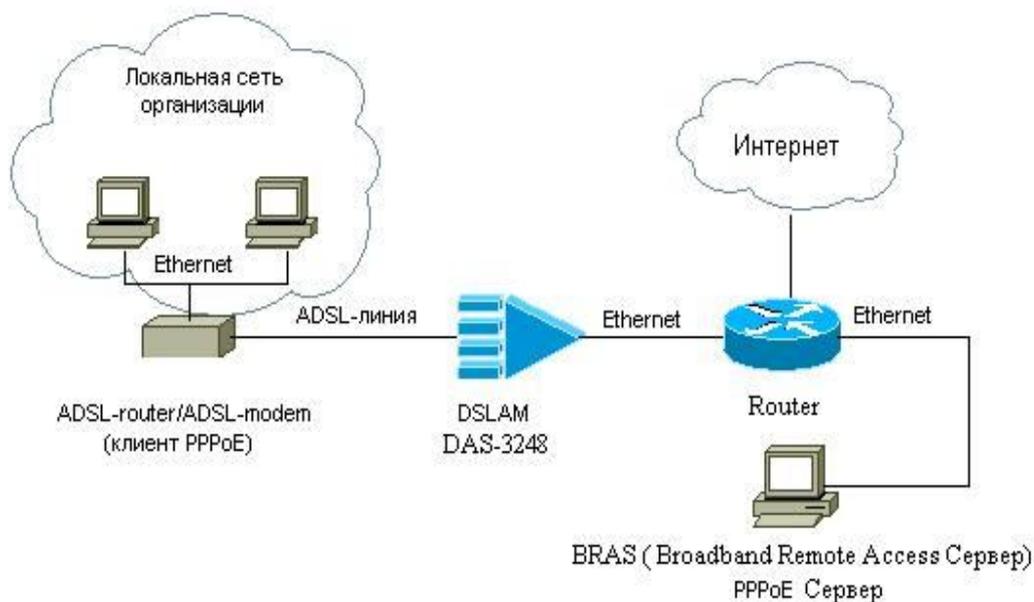


Рисунок 4-30. Схема ADSL доступа по PPPoE технологии

5.2. Функция DHCP option 82 (DHCP Relay Agent).

5.2.1. Сущность функции DHCP option 82.

Функция Option 82 используется Relay Agent (агентом перенаправления запросов) для добавления дополнительной информации в DHCP – запрос клиента. Эта информация может быть использована для применения политик, направленных на увеличение уровня безопасности и эффективности сети. Эта технология описана в стандарте RFC 3046. DSLAM может быть сконфигурирован в качестве агента DHCP relay, что значительно расширяет возможности использования DHCP серверов в сети, позволяя использовать один DHCP сервер для нескольких подсетей. DSLAM, работающий в качестве DHCP relay агента перенаправляет DHCP запрос от клиента в локальной сети на удаленный DHCP сервер. DHCP сервер идентифицирует клиента с использованием параметров Circuit ID и Remote ID, после чего выдает нужный IP адрес в аренду клиенту, пославшему запрос.

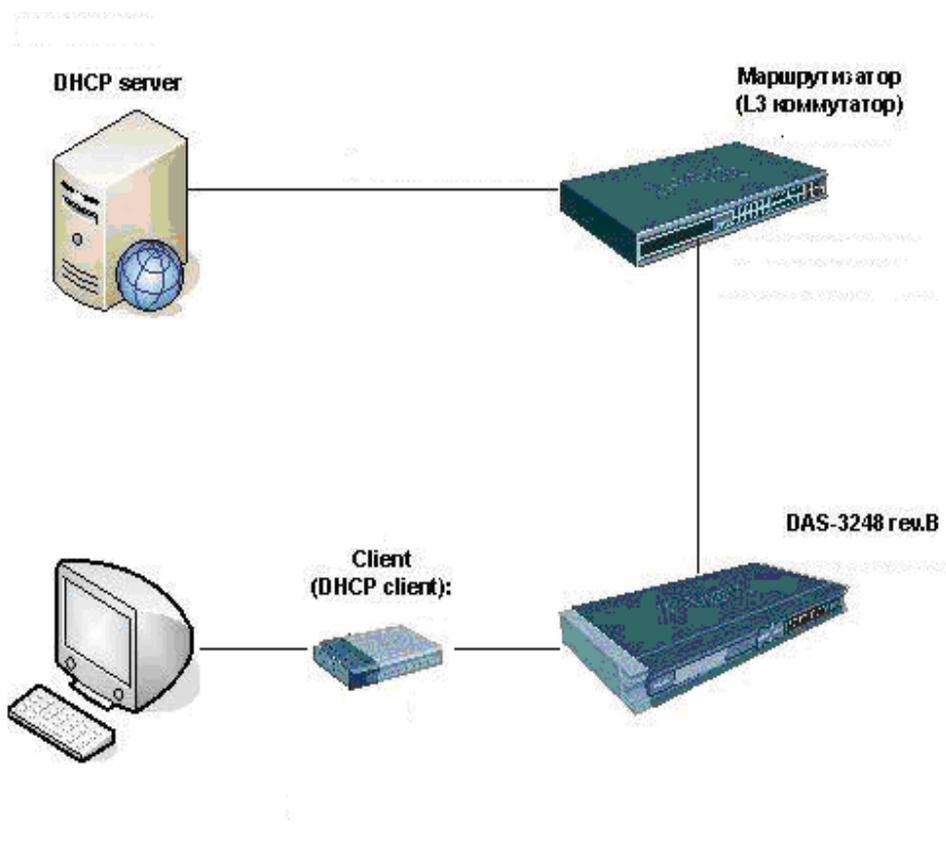


Рисунок 4-31. Пример схемы доступа с использованием DHCP Relay

5.2.2. Синтаксис команд DHCP option 82 на DAS-3248.

modify dra global config

Описание: Глобальное включение функции DHCP option 82 (DRA) на DSLAMе

Синтаксис:

modify dra global config [status Enable|Disable]

Для Функции DHCP option 82 обязательным является сначала создание профиля Intermediate agent (IA) . Профиль IA указывается физические параметры включаемы в теги DRA. Поэтому приведем его синтаксис:

create ia profile entry

Описание: Создание профиля Intermediate Agent (IA)

Синтаксис:

create ia profile entry profileid <dec> [anitype auto|config] [anival <name>]
[aciprefixstr "<name>"]
[acifieldlist AniVal|Chassis|Rack|Frame|Slot|SubSlot|L2Type|Port|Vpi|Vci|VlanTag }+|None]
[suboption Aci|Rai|EncapType|AccessLoopChar }+|None]
[chassisval <name>] [rackval <name>][frameval <name>][slotval <name>]
[subslotval <name>]

Таблица описания параметров команд:

profileid <dec>	Обязательный параметр. Номер профиля IA в системе. Может использоваться для многих правил PIA и DRA
anitype auto config	Метод генерации профиля IA (автоматически или вручную пользователем). Оptionальный параметр. Значение по умолчанию: Auto
anival <name>	Текстовое значение используемое в качестве параметра anival. Существенен только при anitype config Оptionальный параметр.
aciprefixstr "<name>"	Текстовое значение, которое вставляется в качестве префикса в Circuit Id. Это может быть строка пробелов или даже специальных символов. Существенен только при anitype config Оptionальный параметр.
acifieldlist AniVal Chassis Rack Frame Slot SubSlot L2Type Port	Список аппаратных параметров DSLAM, добавляемых в Circuit Id.

Vpi Vci VlanTag}+ None	Существенен только при anitype config Опциональный параметр.
suboption Aci Rai EncapType AccessLoopChar}+ None	Параметры подопций участвующие в функциях PIA и DRA. Aci - Circuid ID Rai - Remote ID EncapType - Тип АТМ инкапсуляции AccessLoopChar -Параметры DSL None - Не добавлять Существенен только при anitype config Опциональный параметр.
chassisval <name>	Номер шасси. Для DAS-3216/24/48 не имеет смысла. Опциональный параметр.
rackval <name>	Номер шкафа. Для DAS-3216/24/48 не имеет смысла. Опциональный параметр.
frameval <name>	Номер полки. Для DAS-3216/24/48 не имеет смысла. Опциональный параметр.
slotval <name>	Номер слота (платы). Для DAS-3216/24/48 не имеет смысла. Опциональный параметр.
subslotval <name>	Номер подслота. Для DAS-3216/24/48 не имеет смысла. Опциональный параметр.

create dra global instance

Описание: Создание профиля DHCP option 82 (DRA)

Синтаксис:

```
create dra global instance portid <dec> vlan <dec> profileid <dec> ]
[ status disable|client|server ] [ op82 disable|AddAlways|AddIfNotExists ]
[ configsuboption {aci|Portid}+|None} ]
[ acival "<name>" ] [ raival "<name>" ]
[ syncratefields {ActualDataRateupstrm|ActualDataRatednstrm|MinDataRateupstrm|
MinDataRatednstrm|AttainableDataRateupstrm|AttainableDataRatednstrm|
MaxDataRateupstrm|MaxDataRatednstrm|MinLpDataRateupstrm|MinLpDataRatednstr|
MaxDelayupstrm|ActualDelayupstrm|MaxDelaydnstrm|ActualDelaydnstrm}+|None]
[ op82fromclientact drop|forward ] [ learning disable|enable ]
[ portno <name> ] [ draaddop82tounicast disable|enable ]
```

Таблица описания параметров команд:

portid <dec>	Обязательный параметр. Номер Bridge порта, к которому привязано правило DRA.
vlan <dec>	Виртуальный VLAN для передачи трафика правила DRA внутри DSLAM. Всегда равен 4097. Обязательный параметр.
profileid <dec>	Номер профиля (profile id) Intermediate Agent, с которым связано данное правило DRA. Обязательный параметр.
status disable client server	Опциональный параметр. Статус DRA в данном правиле: Disable - административно отключен. Client - данное правило добавляет теги CircuitID и RemoteID в пакеты Server - данное правило производит изъятие теги CircuitID и RemoteID из пакетов. Значение по умолчанию :disable
op82 disable AddAlways AddIfNotExists	Условие добавления тегов DHCP option в пакеты: Disable - не добавлять AddAlways - добавлять всегда AddIfNotExists - добавлять только ,если тег DHCP option 82 еще не присутствует в пакете. Опциональный параметр. Значение по умолчанию : AddAlways.
configsuboption {aci Portid}+ None}	Вид добавляемого тега в CircuitID параметр Аci – добавляется текстовое значение, указанное в параметре acival . Portid – добавляется номер ATM порта (смотрите параметр portno). None - ничего не добавляется. Опциональный параметр. Значение по умолчанию : None
acival "<name>"	Текстовое значение, которая добавляется в пакеты как указатель DSLAM (параметр CircuitID). Опциональный параметр. Значение по умолчанию : «\0»

raival "<name>"	<p>Текстовое значение, которая добавляется в пакеты как указатель клиентского порта DSLAM (параметр Remote ID)</p> <p>Опциональный параметр. Значение по умолчанию : «\0»</p>
syncratefields {ActualDataRateupstrm ActualDataRatednstrm MinDataRateupstrm MinDataRatednstrm AttainableDataRateupstrm AttainableDataRatednstrm MaxDataRateupstrm MaxDataRatednstrm MinLpDataRateupstrm MinLpDataRatednstr MaxDelayupstrm ActualDelayupstrm MaxDelaydnstrm ActualDelaydnstrm}+ None	<p>Перечень для синхронизируемых по DHCP option 82 параметров DSL. См. подробнее указание TR-101 DSL Forum.</p> <p>Опциональный параметр.</p>
op82fromclientact drop forward	<p>Действие предпринимаемое с пакетом, в случае, если в нем уже содержится тег DHCP option 82.</p> <p>Значение по умолчанию: Drop. Опциональный параметр.</p>
learning disable enable	<p>Параметр показывающий, включено ли обучение таблицы коммутации DSLAM от приходящих по DHCP option 82 пакетов.</p> <p>Опциональный параметр.</p>
portno <name>	<p>Значение, которое добавляется в качестве номера порта ATM в параметр CircuitID (если в параметре configsuboption присутствует Portid).</p> <p>Опциональный параметр. Значение по умолчанию : «\0»</p>
draaddop82tounicast disable enable	<p>Параметр, показывающий добавляются ли DHCP option 82 в Unicast пакеты.</p> <p>Опциональный параметр. Значение по умолчанию :enable</p>

5.2.3. Пример настройки функции DHCP option 82

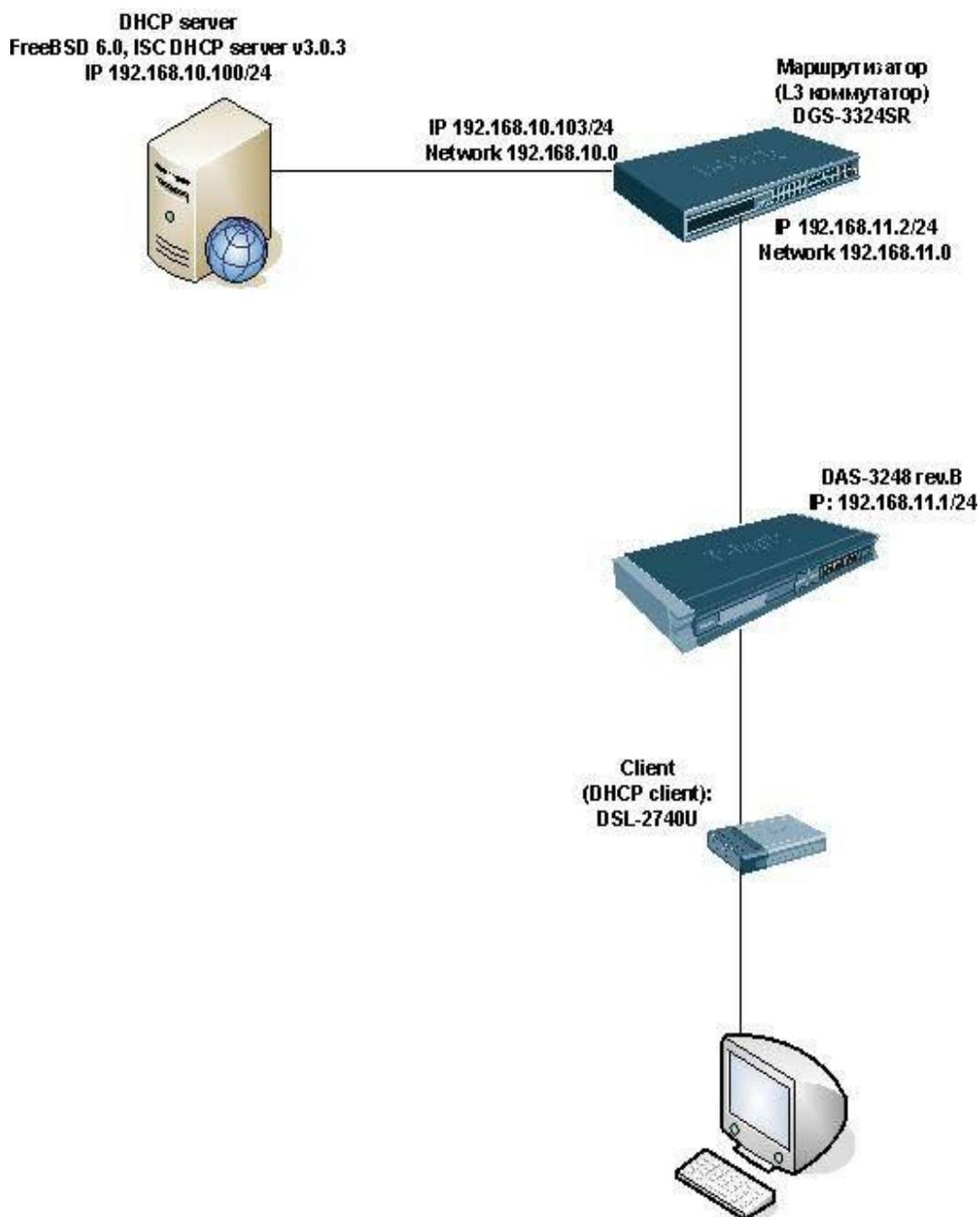


Рисунок 4-32. Пример схемы доступа с использованием DHCP Relay

Шаг 1.Настройка DHCP сервера:

В качестве DHCP сервера использовалась машина с установленной ОС FreeBSD 6.0 и ISC DHCP 3.0.3 сервером.

1.Пример конфигурации dhcpd.conf:

```
option domain-name-servers 192.168.100.1;
default-lease-time 600;
max-lease-time 7200;
authoritative;
ddns-update-style none;
log-facility local7;
```

```
class "client1" {
match if option agent.remote-id = "modem1" and option agent.circuit-id = "dslam";
}
```

```
shared-network test {
  subnet 192.168.10.0 netmask 255.255.255.0 { not authoritative; }
  subnet 192.168.11.0 netmask 255.255.255.0 {
    option routers 192.168.11.2;
  }
  pool {
    range 192.168.11.95 192.168.11.95;
    allow members of "client1";
  }
}
```

2.Добавление маршрута к 192.168.11.0 подсети:

```
$ sudo route add 192.168.11.0/24 192.168.10.103
```

Шаг 2.Настройка маршрутизатора:

В качестве маршрутизатора использовался L3 коммутатор D-Link DGS-3324SR (здесь предполагается, что коммутатор находится в настройках по умолчанию). К первому порту коммутатора подключен DHCP сервер (подсеть 192.168.10.0), ко второму порту – DSLAM (подсеть 192.168.11.0).

1.Удаление 1-го и 2-го портов из default VLAN:

```
DGS-3324SR:4#config vlan default delete 1:1-1:2
Command: config vlan default delete 1:1-1:2
```

Success.

2.Создание двух новых VLAN:

DGS-3324SR:4#create vlan vlan2 tag 2
Command: create vlan vlan2 tag 2

Success.

DGS-3324SR:4#create vlan vlan3 tag 3
Command: create vlan vlan3 tag 3

Success.

DGS-3324SR:4#

3.Добавление нужных портов в VLAN:

DGS-3324SR:4#config vlan vlan2 add untagged 1:1 advertisement enable
Command: config vlan vlan2 add untagged 1:1 advertisement enable

Success.

DGS-3324SR:4#config vlan vlan3 add untagged 1:2 advertisement enable
Command: config vlan vlan3 add untagged 1:2 advertisement enable

Success.

DGS-3324SR:4#

4.Создание IP интерфейсов для каждого VLAN:

DGS-3324SR:4#create ipif vlan2 192.168.10.103/24 vlan2
Command: create ipif vlan2 192.168.10.103/24 vlan2

Success.

DGS-3324SR:4#create ipif vlan3 192.168.11.2/24 vlan3
Command: create ipif vlan3 192.168.11.2/24 vlan3

Success.

DGS-3324SR:4#

5.Сохранение настроек:

DGS-3324SR:4#save
Command: save

current box_id: 1 is AUTO

Do you want to change current box id from AUTO mode to STATIC mode?(y/n) y
Saving all configurations to NV-RAM..... Done.

На этом конфигурация коммутатора закончена.

Шаг 3.Настройка DSLAM (здесь предполагается, что DSLAM находится в настройках по умолчанию):

1.Изменение IP адреса в настройках ЕТН-1 интерфейса:

```
$modify ethernet intf ifname eth-1 disable
```

```
$modify ethernet intf ifname eth-1 ip 192.168.11.1 mask 255.255.255.0 enable
```

```
Interface      : eth-1
Type           : Uplink      UseDhcp    : False
IP Address     : 192.168.1.1  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 : Down
```

Set Done

```
Interface      : eth-1
Type           : Uplink      UseDhcp    : False
IP Address     : 192.168.11.1  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
$
```

Thu Jan 01 00:01:45 1970 : STATUS ALARM : ETHER Interface Up : Interface - eth-1

2.Создание маршрута к 192.168.10.0 подсети:

```
$create ip route ip 192.168.10.0 gwyip 192.168.11.2 mask 255.255.255.0
```

Entry Created

Destination	Net Mask	Gateway	If-name	Route	Route	Route Age(sec)
-------------	----------	---------	---------	-------	-------	----------------

Type Orig

192.168.10.0 255.255.255.0 192.168.11.2 eth-1 IND LCL 0

3.Проверка доступности DHCP сервера посредством команды ping:

\$ping 192.168.10.100

64 bytes of data from 192.168.10.100, seq=0 ttl=63 rtt =30 msec

64 bytes of data from 192.168.10.100, seq=1 ttl=63 rtt =10 msec

64 bytes of data from 192.168.10.100, seq=2 ttl=63 rtt =10 msec

64 bytes of data from 192.168.10.100, seq=3 ttl=63 rtt =10 msec

----- Ping Statistics -----

4 packets transmitted, 4 packets received, 0 percent packet loss

4.Создание фильтрующего правила для отправки DHCP Discovery пакетов ControlPlane устройства на обработку:

\$create filter rule entry ruleid 301 ruledir in ruleprio high applywhenreq disable snooplevel interface
description DRA_CNTRL action sendtocontrol statsstatus enable

Entry Created

Rule Id : 301 Rule Action : sendtocontrol
Set Priority : - Admin status : disable
Stats admin status : enable Rule Priority: high
Rule Direction : in ApplyWhenReq : disable
Pkt Type : Ucast
Application Description : DRA_CNTRL
Snoop Level : interface
Expression Id: 0
Action Value : 0x0
Action Mask : 0xffffffff

5.Создание подправила для фильтрующего правила:

\$create filter subrule udp ruleid 301 subruleid 1 srportcmp any dstportfrom 67 dstportcmp eq
subruleprio asinrule transporthdr ethernet

Entry Created

Rule Id : 301 Subrule Id : 1
Start source port : - End source port : -
Start destination port : 67 End destination port : -
Source port comparison : any Destination port comparison : eq
Subrule Priority : asinrule
Transport Header : ethernet

6.Привязка созданного правила ко всем еоа интерфейсам:

\$create filter rule map ruleid 301 stageid 1 orderid 301 ifname alleoa

Entry Created

Interface : alleoa Stage Id : 1
Rule Id : 301 Order Id : 301

7.Включение созданного правила в работу:

\$modify filter rule entry ruleid 301 status enable

Rule Id : 301 Rule Action : sendtocontrol
Set Priority : - Admin status : disable
Stats admin status : enable Rule Priority: high
Rule Direction : in ApplyWhenReq : disable
Pkt Type : Ucast
Application Description : DRA_CNTRL
Snoop Level : interface
Expression Id: 0
Action Value : 0x0
Action Mask : 0xffffffff

Set Done

Rule Id : 301 Rule Action : sendtocontrol
Set Priority : - Admin status : enable
Stats admin status : enable Rule Priority: high
Rule Direction : in ApplyWhenReq : disable
Pkt Type : Ucast
Application Description : DRA_CNTRL
Snoop Level : interface
Expression Id: 0
Action Value : 0x0
Action Mask : 0xffffffff

8.Включение DRA (выполняется глобально на устройстве):

\$modify dra global config status enable

DRA global Status

Disable

Set Done

DRA global Status

Enable

9.Создание профиля Intermediate agent (IA):

Примечание: как правило, данный профиль используется при создании всех PIA и DRA профилей.

```
$create ia profile entry profileid 1
```

Entry Created

```
Profile Id      : 1          ANI Type : auto
ANI value      : -
Aci Prefix Str : -
ACI Field List : AniVal Slot L2Type Port Vpi Vci
Sub Option     : Aci Rai EncapType AccessLoopChar
Chassis       : -          Rack      : -
Frame         : -          Slot      : -
Sub Slot      : -
```

10.Создание профиля DRA (DHCP relay agent) для 15-го порта и задание тегов CircuitID и RemoteID:

```
$create dra instance entry portid 15 vlan 4097 profileid 1 op82 addalways configsuboption aci acival "DSLAM1" raival "Modem15" status client
```

Entry Created

```
Port Id          : 15          VLAN          : 4097
Profile Id       : 1          DRA status    : client
Option82         : AddAlways
Config Sub-Option : aci
Agent Circuit Id : DSLAM1
Remote Agent Id  : Modem15
SyncRateInfoField : ActualDataRateupstrm ActualDataRatednstrm MinDataRateupstrm
MinDataRatednstrm
DRA Act For Op82 From Client : drop
DRA learning     : enable     Port No       : -
VCI              : 35         VPI          : 8
L2 type          : atm        Encap Type   : Llcmux
DRA Add Op82 To Unicast : enable
```

11.Сохранение настроек:

```
$commit
```

12.Настройка абонентского устройства (CPE)

Подключите абонентское устройство (CPE) ко второму DSL порту DSLAM.

WAN интерфейс устройства нужно настроить на использование динамического IP.

После сохранения настроек и перезагрузки устройство получит IP адрес, указанный в конфигурации DHCP сервера, а именно: 192.168.11.95

D-Link
Building Networks for People

DSL-2500U

Home | Advanced | Tools | **Status**

WAN Info

VPI/VCI	Category	Service Name	Interface Name	Protocol	State	Status	IP Address
0/35	UBR	mer_0_35	nas_0_35	MER	Enabled	Up	192.168.11.95

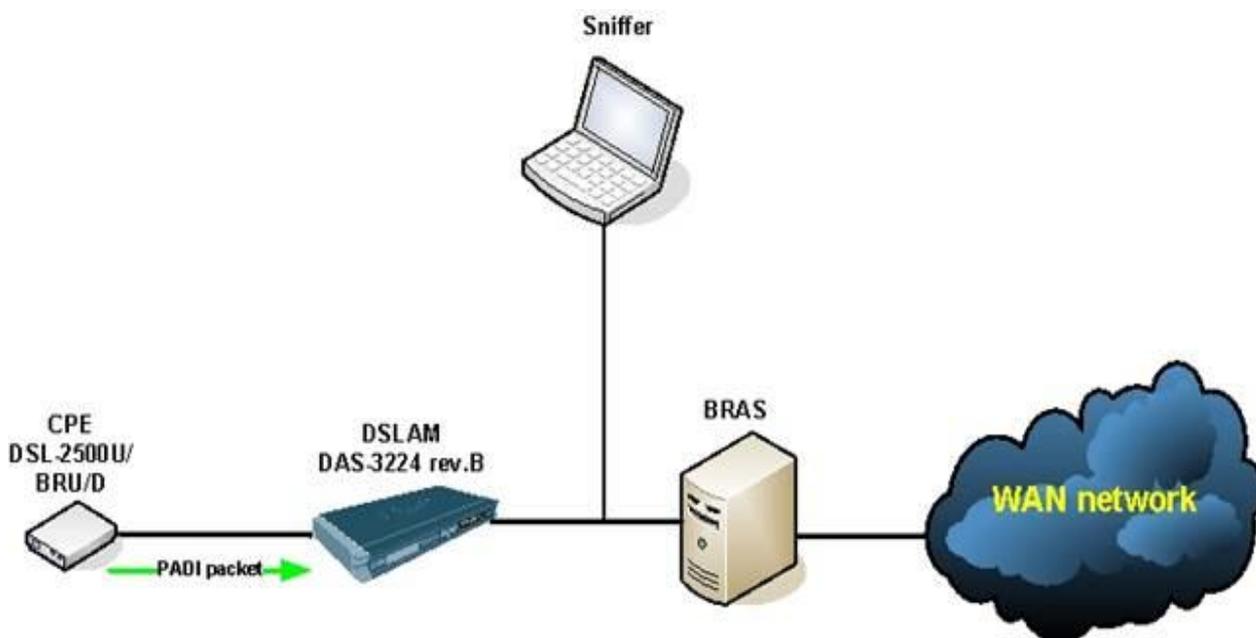
Device Info
DHCP Clients
WAN Info

Рисунок 4-33. Настройка модема

5.3. Функция PPPoE Intermediate Agent.

5.3.1. Сущность функции PPPoE Intermediate Agent.

Функция PPPoE intermediate agent подобна функции DHCP option 82, за тем исключением, что Circuit ID и Remote ID теги посредством DSLAM помещаются во все пакеты PPPoE discovery stage (PADI, PADR и PADT), что позволяет однозначно идентифицировать клиента и с учетом корректности передаваемой информации проводить аутентификацию. Как правило, данная функция используется для «привязки» абонента (получающего доступ во внешнюю сеть с использованием протокола PPPoE) к конкретному порту DSLAM. В случае подключения абонента к другому порту DSLAM (попытка аутентификации с корректным логином/паролем, но с другого порта DSLAM) – в данном случае доступ к услуге будет запрещен, так как связка логин/пароль + Circuit ID + Remote ID неверна.



Модифицированный пакет

Рисунок 4-34. Пример схемы доступа с использованием PPPoE Relay

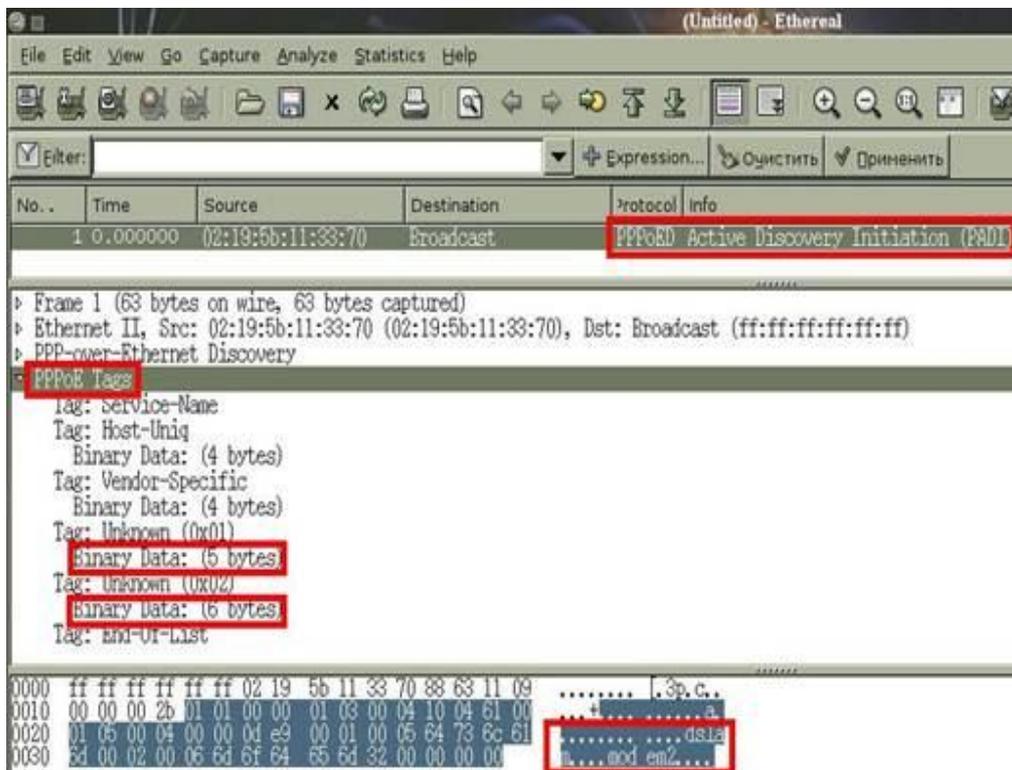


Рисунок 4-35. Перехват измененного пакета с использованием PPPoE Relay

5.3.2. Синтаксис команд PPPoE Intermediate Agent

modify pia global config

Описание: Глобальное включение функции PPPoE Intermediate agent (PIA) на DSLAMе

Синтаксис:

Modify pia global config [status Enable|Disable]

Для функции PPPoE Intermediate agent ,также как для функции DHCP option 82 обязательным является сначала создание профиля Intermediate agent (IA) .синтаксис сохдания этого профиля был рассотрен в разделе DHCP option 82 (см.выше)

create pia instance entry

Описание: Создание профиля PPPoE Intermediate agent (PIA)

Синтаксис:

create pia instance entry portid <dec> vlan <dec> profileid <dec> [status enable|disable] [vsatag disable|AddAlways|AddIfNotExists] [configsuboptionbitmask aci|PortId}+|None] [acival "<name>"] [raival "<name>"] [syncratefields ActualDataRateupstrm|ActualDataRatednstrm|MinDataRateupstrm|MinDataRatednstrm|AttainableDataRateupstrm|AttainableDataRatednstrm|MaxDataRateupstrm|MaxDataRatednstrm|MinLpDataRateupstrm|MinLpDataRatednstrm|Max Delayupstrm|ActualDelayupstrm|MaxDelaydnstrm|ActualDelaydnstrm}+|None] [iwftagfromclientact drop|forward] [insertiwfsupop enable|disable] [portno <name>]

Таблица описания параметров команд:

portid <dec>	Обязательный параметр. Номер Bridge порта, к которому привязано правило PIA.
vlan <dec>	Виртуальный VLAN для передачи трафика правила PIA внутри DSLAM. Всегда равен 4097. Обязательный параметр.
profileid <dec>	Номер профиля (profile id) Intermediate Agent, с которым связано данное правило PIA. Обязательный параметр.
status enable disable	Статус PIA в данном правиле: Disable- административно отключен. Enable- административно включен Оptionальный параметр.
vsatag disable AddAlways AddIfNotExists	Условие добавления тегов PIA пакеты: Disable - не добавлять AddAlways - добавлять всегда AddIfNotExists - добавлять только, если тег DHCP option 82 еще не присутствует в пакете. Оptionальный параметр. Значение по умолчанию : AddAlways
configsuboptionbitmask aci PortId}+ None	Вид добавляемого тега в CircuitID параметр Аci – добавляется текстовое значение, указанное в параметре acival Portid – добавляется номер АТМ порта (смотрите параметр portno). None - ничего не добавляется. Оptionальный параметр. Значение по умолчанию : None
acival "<name>"	Текстовое значение, которая добавляется в пакеты как указатель DSLAM (параметр CircuitID). Оptionальный параметр. Значение по умолчанию : «\0»

raival "<name>"	<p>Текстовое значение, которая добавляется в пакеты как указатель клиентского порта DSLAM (параметр Remote ID)</p> <p>Опциональный параметр. Значение по умолчанию : «\0»</p>
syncratefields ActualDataRateupstrm ActualDataRatednstrm MinDataRateupstrm MinDataRatednstrm AttainableDataRateupstrm AttainableDataRatednstrm MaxDataRateupstrm MaxDataRatednstrm MinLpDataRateupstrm MinLpDataRatednstrm MaxDelayupstrm ActualDelayupstrm MaxDelaydnstrm ActualDelaydnstrm} + None	<p>Перечень для синхронизируемых по PIA параметров DSL. См. подробнее указание TR-101 DSL Forum.</p> <p>Опциональный параметр.</p>
iwftagfromclientact drop forward	<p>Действие, предпринимаемое с пакетом, в случае, если получен пакет PADI с тегом PIA.</p> <p>Опциональный параметр. Значение по умолчанию: drop</p>
insertiwfsubop enable disable	<p>Параметр, разрешающий добавлять тег PIA для PPPoA и PPPoE интерфейсов DSLAM (то есть для функции PPPoA to PPPoE Internetworking)</p> <p>Опциональный параметр. Значение по умолчанию: enable</p>
portno <name>	<p>Значение, которое добавляется в качестве номера порта ATM в параметр CircuitID (если в параметре configsuboption присутствует Portid).</p> <p>Опциональный параметр. Значение по умолчанию : «\0»</p>

5.3.3. Пример настройки PPPoE Intermediate Agent.

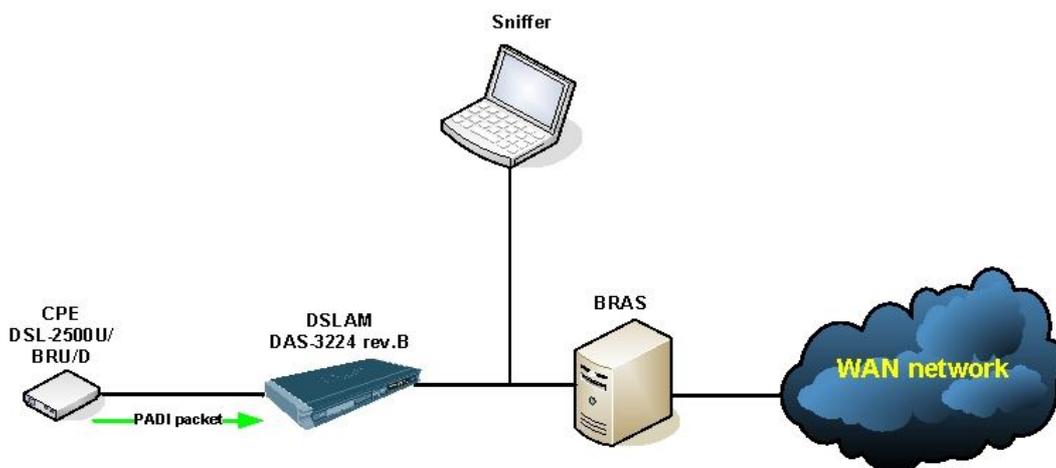


Рисунок 4-36. Пример схемы доступа с использованием PPPoE Relay

1. Создание фильтрующего правила для перенаправления PADI пакетов Control Plane устройства на обработку:

```
$create filter rule entry ruleid 3 action sendtocontrol ruleprio high ruledir in snooplevel bridge  
description PIA_CTRL
```

Entry Created

```
Rule Id      : 3      Rule Action : sendtocontrol  
Set Priority  : -      Admin status : disable  
Stats admin status : disable Rule Priority: high  
Rule Direction : in   ApplyWhenReq : disable  
Pkt Type     : Ucast  
Application Description : PIA_CTRL  
Snoop Level  : bridge  
Expression Id: 0  
Action Value : 0x0  
Action Mask  : 0xffffffff
```

2. Создание подправила, в котором указан идентификатор протокола PPPoE (discovery stage):

```
$create filter subrule ether ruleid 3 subruleid 1 ethertypefrom 0x8863 ethertypecmp eq
```

Entry Created

```

Rule Id          : 3      Subrule Id          : 1
Start source mac address  : -
End source mac address    : -
Start destination MAC address: -
End destination MAC address : -
Start ethernet type      : 0x8863  End ethernet type      : -
Start VLAN Id          : -      End VLAN Id          : -
Start priority tag      : -      End priority tag      : -
Start DSAP             : -      End DSAP             : -
Start SSAP             : -      End SSAP             : -
Source MAC address comparison: any
Destination MAC addr comparison: any
Ether type comparison   : eq
Vlan Id comparison      : any
Priority tag comparison  : any
DSAP comparison         : any
SSAP comparison         : any
Subrule Priority        : asinrule
Start service VLAN Id   :-
End service VLAN Id     :-
Start service priority tag :-
End service priority tag :-
service Vlan Id comparison : any
Service Priority tag comparison : any

```

3. Включение созданного правила в работу:

```
$modify filter rule entry ruleid 3 status enable
```

```

Rule Id          : 3      Rule Action : sendtocontrol
Set Priority      : -      Admin status : disable
Stats admin status : disable  Rule Priority: high
Rule Direction    : in      ApplyWhenReq : disable
Pkt Type          : Ucast
Application Description : PIA_CTRL
Snoop Level       : bridge
Expression Id: 0
Action Value      : 0x0
Action Mask       : 0xffffffff
Set Done

```

```

Rule Id          : 3      Rule Action : sendtocontrol
Set Priority      : -      Admin status : enable
Stats admin status : disable  Rule Priority: high
Rule Direction    : in      ApplyWhenReq : disable
Pkt Type          : Ucast
Application Description : PIA_CTRL
Snoop Level       : bridge
Expression Id: 0

```

Action Value : 0x0
Action Mask : 0xffffffff

4.Привязка созданного правила ко всем eoa интерфейсам:

\$create filter rule map ruleid 3 ifname alleoa stageid 1 orderId 3

Entry Created

Interface : alleoa Stage Id : 1
Rule Id : 3 Order Id : 3

5.Включение функции PPPoE intermediate agent (выполняется глобально на устройстве):

\$modify pia global config status enable

PIA global Status : Disable

Set Done

PIA global Status : Enable

6.Создание профиля Intermediate agent (IA):

Примечание: как правило, данный профиль используется при создании всех PIA и DRA профилей.

\$create ia profile entry profileid 1

Entry Created

Profile Id : 1 ANI Type : auto
ANI value : -
Aci Prefix Str : -
ACI Field List : AniVal Slot L2Type Port Vpi Vci
Sub Option : Aci Rai EncapType AccessLoopChar
Chassis : - Rack : -
Frame : - Slot : -
Sub Slot : -

7.Создание профиля PPPoE intermediate agent (PIA) для 15-го порта и задание тегов CircuitID и RemoteID:

\$create pia instance entry portid 15 vlan 4097 profileid 1 vsatag addalways acival "DSLAM1" raival "Modem15" configsuboptionbitmask aci status enable

Entry Created

Port Id : 15 VLAN : 4097
Profile Id : 1 PIA status : enable
PIAVsaOption : AddAlways
Config Sub Options Bitmask : aci
Agent Circuit Id : DSLAM1
Remote Agent Id : Modem15
SyncRateInfoField Bitmask : ActualDataRateupstrm ActualDataRatednstrm MinDataRateupstrm
MinDataRatednstrm
Act for IWFTag From Client : drop
Insert Iwf Subop : enable
Port No : -
VCI : 35 VPI : 8
L2 type : atm
Encap Type : Llc mux

6. Настройка Uplink Интерфейсов

Uplink интерфейсы – интерфейсы, которые могут быть использованы для подключения к IP backbone (магистрала).

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-1
10/100/1000 BaseT/FX Uplink interface	UPLINK2	eth-2

Таблица 6-1

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

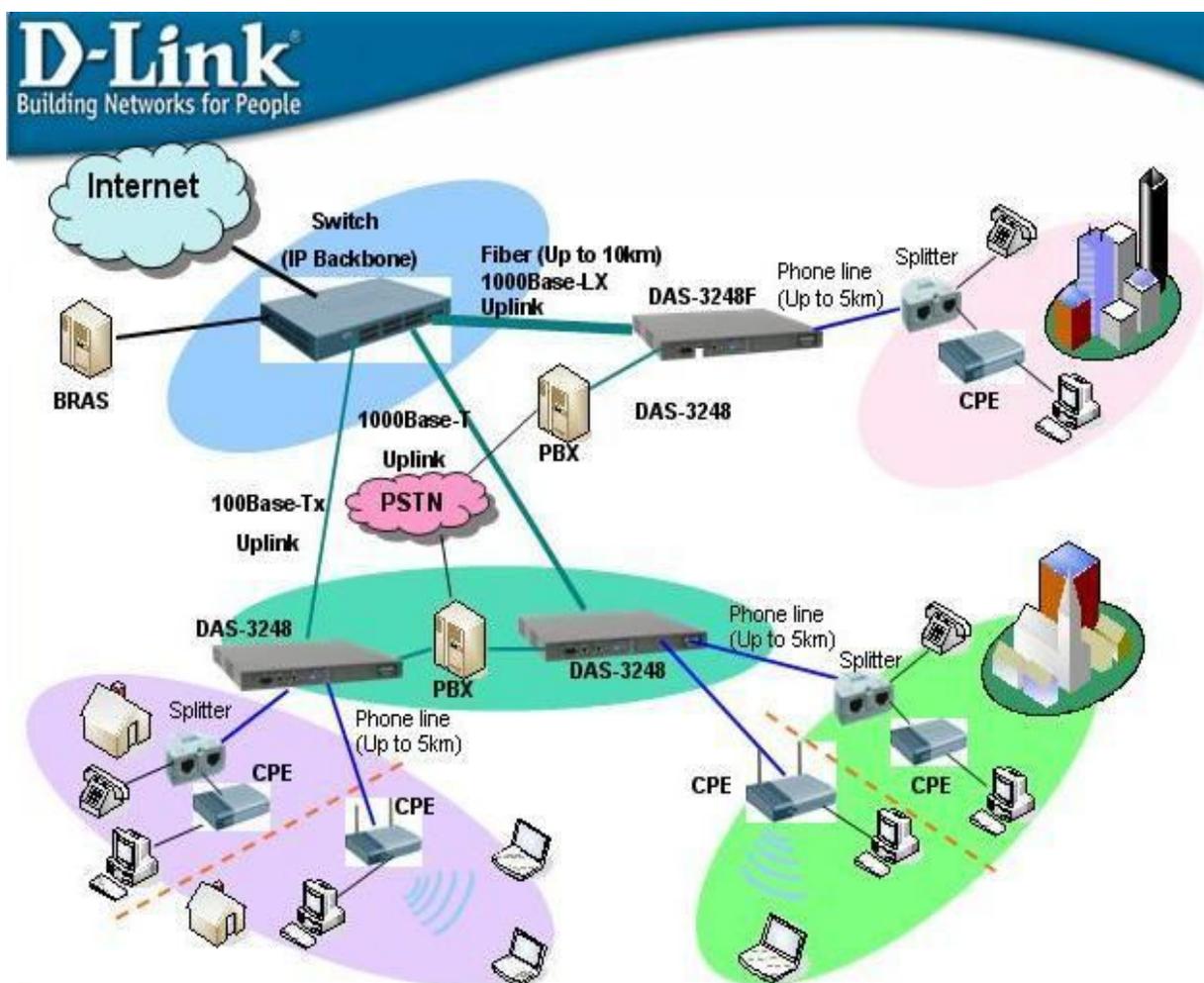


Рисунок 6-1. Пример сети доступа с использованием Uplink интерфейсов

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.

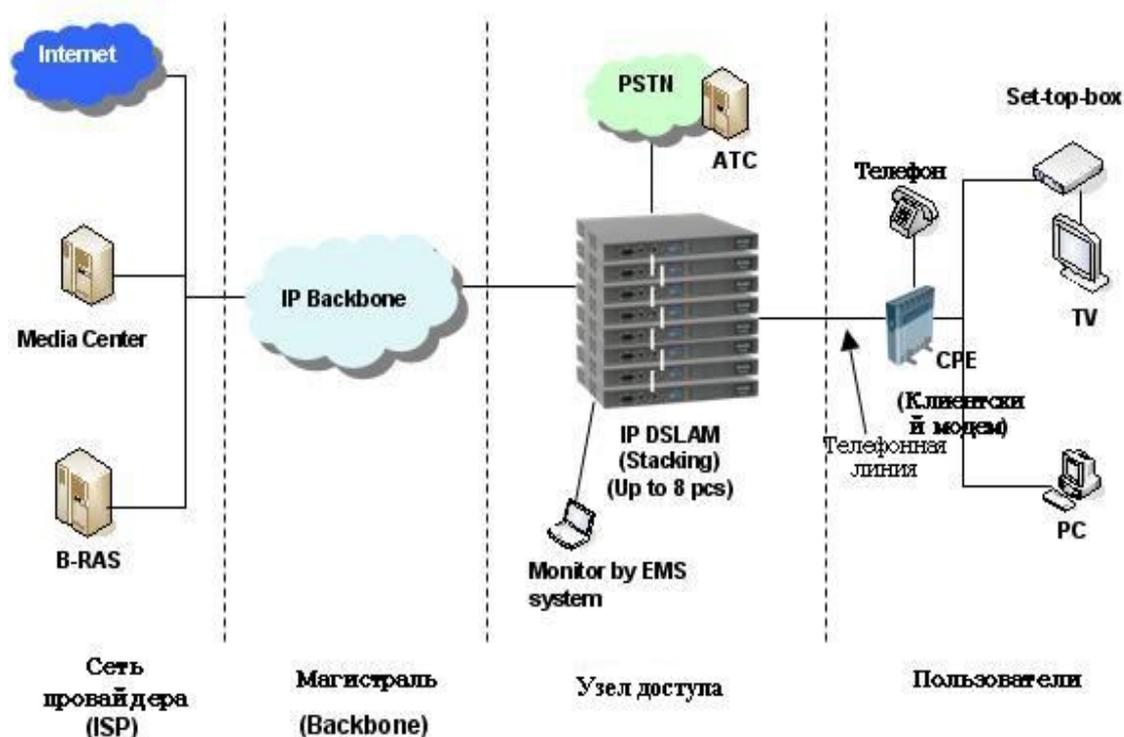


Рисунок 6-2. Пример сети доступа со стекирование DAS-3248

Поскольку для стекирования используются те же самые интерфейсы Uplink1(eth-1) и Uplink 2(eth-2), 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-1 (eth-2) задается параметром **type** при его создании командой **create ethernet intf**

Примечание: по умолчанию тип eth-1- uplink, eth-2- 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-1 с IP 192.168.7.15:

```
$create ethernet intf ifname eth-1 type uplink ip 192.168.7.15 mask 255.255.255.0 enable
```

Экранный вывод:

```
Interface      : eth-1
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-1 и eth-2) 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 настраивать 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-1 duplex half speed 100BT ip 192.168.7.15 mask 255.255.255.0 enable
```

Экранный вывод:

Interface	: eth-1		
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.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-1) 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-1- uplink, eth-2 - downlink. Кроме того, поверх каждого из eth интерфейсов уже создан bridge порт, что позволяет осуществлять L2 Forwarding между устройствами.

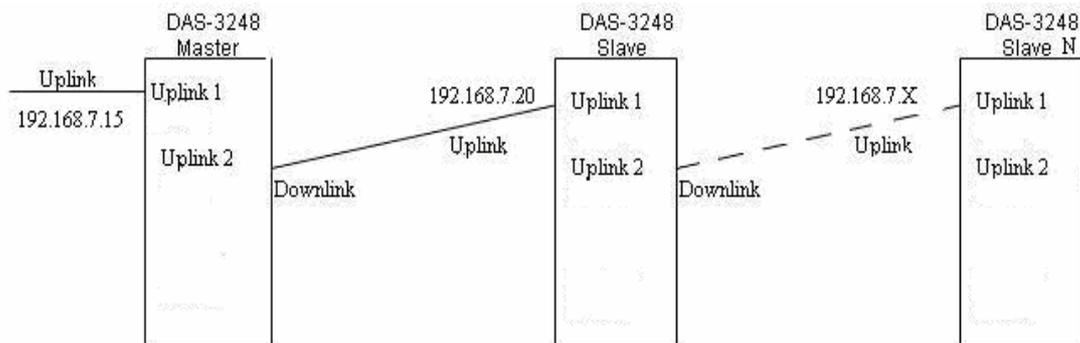


Рисунок 6-17

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-1 192.168.7.15 mask 255.255.255.0
modify ethernet intf ifname eth-1 192.168.7.20 mask 255.255.255.0
.....
modify ethernet intf ifname eth-1 192.168.7.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, соответственно, три типа передачи пакетов:

- unicast:** Одиночная передача. Пакет, посланный по уникастному адресу, доставляется только тому адресу, который указан как адрес назначения в теле пакета. Настройка функций, связанных с Unicast передачей данных, описана в разделе 7.2.
- broadcast:** Широковещательная передача. Пакет, посланный по бродкастному 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 протоколом 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 изменяется 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 входящих 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 коммутации 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 bcasupport support disable - запрещение пересылки широковещательных пакетов

\$ modify bridge tbg info mcasupport support disable- запрещение пересылки групповых пакетов

Чтобы предотвратить перегрузку DSLAM MAC адресами, а также улучшить безопасность сети, применяется функция Port Security, позволяющая порту обучиться 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 окончании 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 bridgingmode 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.

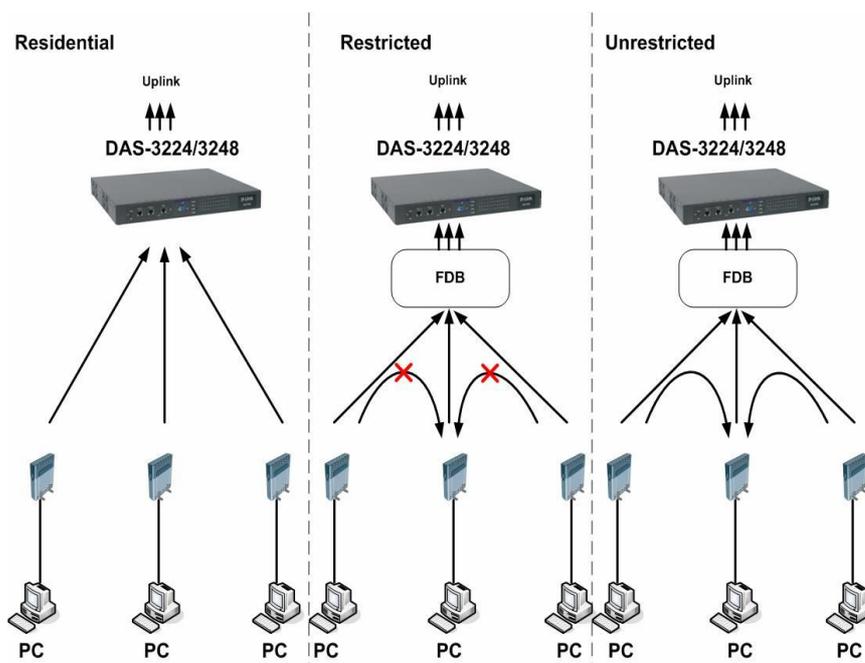


Рисунок 7-1

Также режим коммутации может определяться для каждого созданного в системе VLAN (т.е. локально) через команду :

modify vlan static vlnname bridgingmode Restricted| Unrestricted| Residential

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 оборудование 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** (бroadcast-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 vlnname vlnname 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 (vlnname vlnname | 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 (vlnname vlnname | vlanid vlanid)`

get vlan static

Описание: Получает информацию по vlan.

Синтаксис
команды: `get vlan static [vlnname vlnname | vlanid vlanid]`

Таблица параметров:

Параметр	Описание
----------	----------

vlanname vlanname	<p>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 .</p> <p>Использование: Create – Обязательно Delete – Опционально Get – Опционально Modify – Опционально</p> <p>Принимает значения: любая строка размером до 64 символов .</p>
vlanid vlanid	<p>VLAN идентификатор.</p> <p>Использование: Create – Обязательно Delete – Опционально Get – Опционально Modify – Опционально</p> <p>Для delete, get, modify – может использоваться vlanname или vlanid.</p> <p>Принимает значения: 1 – 4095</p>
egressports egressports none	<p>Устанавливает порты, каждый из которых ассоциирован с типом “egress” (список egress портов) для данного управляющего VLAN. При задании более одного значения, они разделяются пробелами.</p> <p>Использование: Опционально</p> <p>Принимает значения: 1 – 386</p> <p>Значение по умолчанию: none</p>
forbidegressports forbidegressports none	<p>Устанавливает порты, которые запрещены к управлению, будучи включенными, в список “egress” типа портов для данного VLAN.</p> <p>Они могут быть включены в “untagged” тип.</p> <p>Использование: Optional</p> <p>Принимает значения: 1 – 386</p> <p>По умолчанию: none</p>
untaggedports untaggedports none	<p>Устанавливает порты, которые могут передавать “egress” пакеты данного VLAN, как, “untagged” . При задании более одного значения, они разделяются пробелами.</p> <p>Использование: Optional</p> <p>Принимает значения: 1 – 386</p> <p>По умолчанию: none</p>
bridgingmode bridgingmode	<p>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</p>

	<p>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.</p> <p>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”.</p> <p>Использование: Create -- Optional Modify -- Optional</p> <p>Принимает значения: Restricted, Unrestricted, Residential</p> <p>По умолчанию: residential</p>
<p>floodsupport enable disable</p>	<p>Используется если необходимо запретить или разрешить unicast пакеты от неизвестных источников для данного VLAN</p> <p>По умолчанию значение параметра enable.</p> <p>Неизвестные unicast пакеты могут распространяться на все порты VLAN, если глобальное значение (представлено в Dot1dTrInfo) установлено в “enable” или “throtte” и значение на VLAN так же “enable” или “drop”.</p> <p>Использование: Create -- Optional Modify -- Optional</p> <p>Принимает значения: GS_STATE_ENABLE, GS_STATE_DISABLE</p>
<p>bcastsupport enable disable</p>	<p>Параметр определяет распространение broadcast пакетов для данного VLAN. По умолчанию система получает значение enable, когда VLAN создан.</p> <p>Broadcast пакеты могут распространяться через все порты VLAN, если глобальное значение (представлено в Dot1dTrInfo) и значение первичного vlan установлены в “enable”.</p>

	<p>Использование: Create -- Optional Modify -- Optional Принимает значения: GS_STATE_ENABLE, GS_STATE_DISABLE По умолчанию: GS_CFG_DEF_VLAN_BCAST</p>
--	---

Создать VLAN с заданными параметрами:

	Команда	Действие
Шаг 1	\$create vlan static vlnname 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 vlnname Dlink egressports 1 2 23 385 untaggedports 1 2 23 floodSupport disable bcassupport disable	Изменение параметров VLAN По этой команде порты 1 2 23 становятся нетегированными членами Vlan Dlink, порт 385 (Uplink1) тегируемым членом VLAN (транком). <u>Внимание:</u> Тегируемыми являются только те порты, которые присутствуют 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 присваивание PVID Bridge портам, (то есть ассоциирующие входящие в определенный порт кадры с определенным тегом VLAN). Данная команда будет описана подробно в разделе посвященном 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.Настройка GVRP

Данные команды используются для определения входящей (ingress) фильтрации трафика на VLAN, а также для установки PVID.

Команды DAS-3248 для настройки GVRP

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 ] [ restrictedvlanreg False | True ] [ pktpriority pktpriority ] [ psvlanid psvlanid] [ppstatus enable|disable] [ctosprofileid ctosprofileid | None]
```

Параметры команды:

portid <i>portid</i>	Имя Bridge интерфейса, на котором производится настройка параметров. Обязательный параметр.
portvlanid portvlanid	PortVlanID (PVID), ассоциированный с данным Bridge интерфейсом. 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
pktpriority pktpriority	Приоритет, используемый для постановки пакетов в определенную очередь пакетов
psvlanid psvlanid	Определяет PSVID, привязанный к порту DSLAM (для функции 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 окончным портом (disable). Данный параметр изменятся только привключенном bridge интерфейсе. Необязательный параметр По умолчанию :None.
ctosprofileid ctosprofileid None	Содержит привязку CtoS профиля к порту (для функции 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.

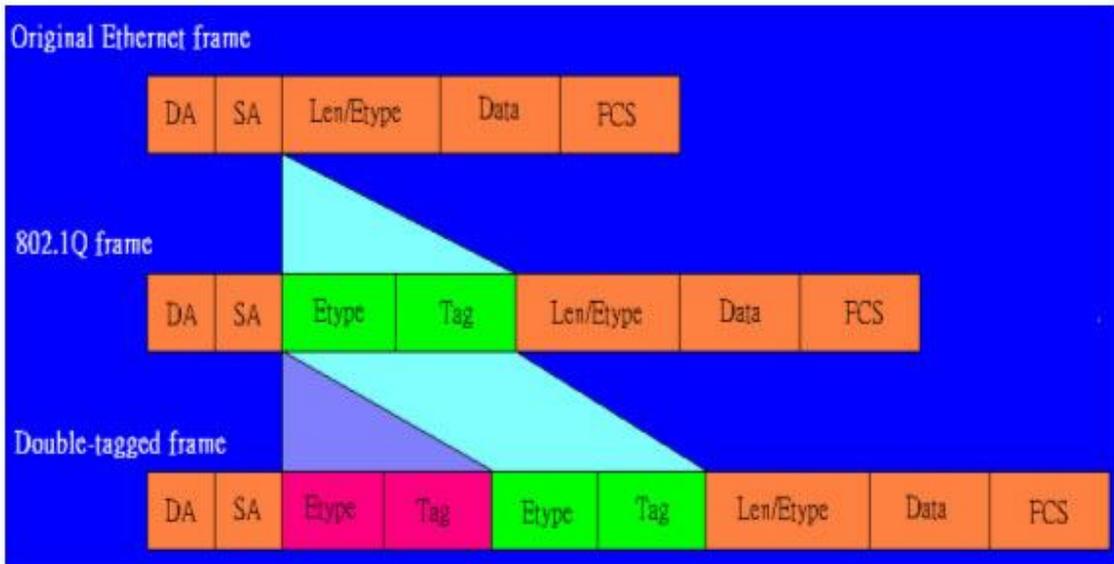


Рисунок 7-3. Структура Ethernet фрейма при использовании Q-in-Q.

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.

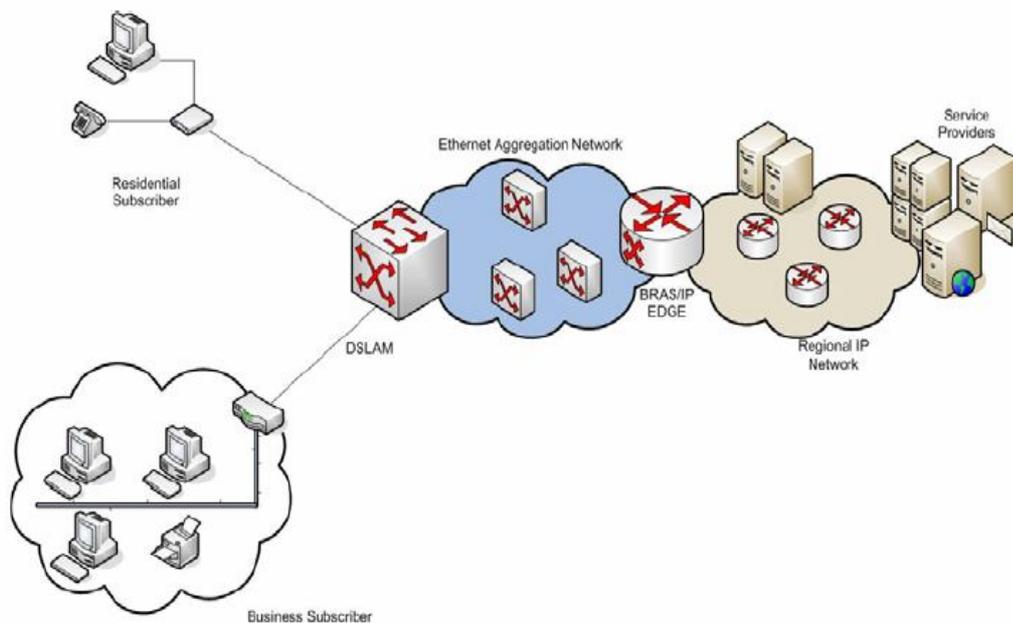


Рисунок 7-4. Схема сети MAN

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:
 - а) Сеть доступа должна обслуживать многочисленных поставщиков услуг (провайдеров).
 - б) 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 передать данные во второй порт, участвующий в услуге E-line. В этом случае данные должны направляться между только двумя участвующими в обмене портами. Данные просто перенаправляются 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 Agreement - 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 выделяется 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 CtoS Profile. В этом случае S-VLAN ID определяется на основании CtoS Profile, а не PSVID.

CtoS профиль создается следующими командами CLI:

1. Создать профиль:

create vlan mapprofile info profileid ctosprofileid profiletype CtoS

2. Определение C-VLAN ID 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 prio info 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 Residential.
В случае резидентных клиентов для фильтрации и пересылки пакетов

используется стандартное Virtual VLAN распределение, то есть взаимоднозначная 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, базирясь 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 тегирования, 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.

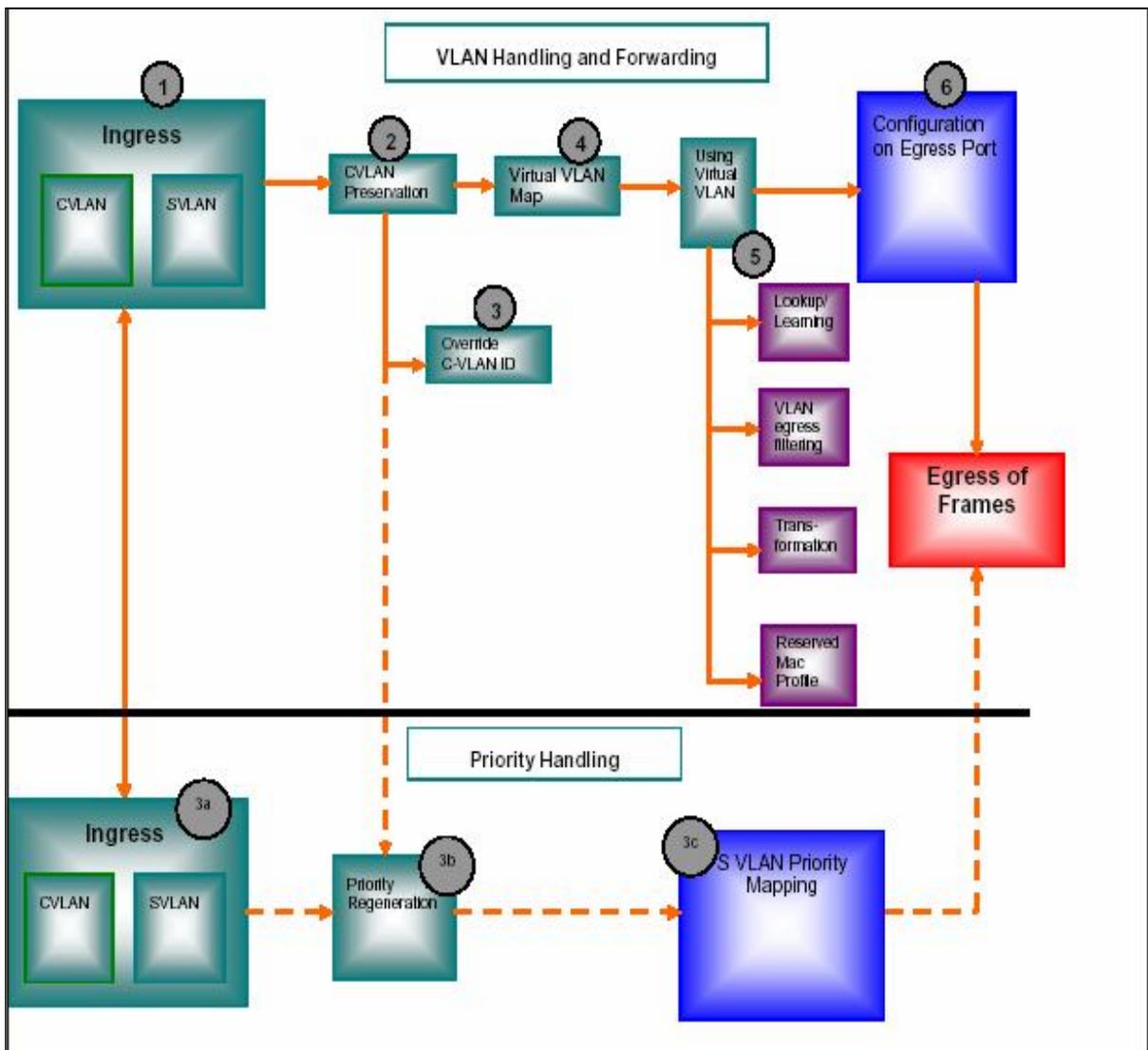


Рисунок 3.Порядок обработки VLAN тегов пакетов в DAS-3248 при использовании Q-in-Q

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 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 в дальнейшем применяется PVID в качестве C-VLAN ID.

3а) 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.

3б) 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.

3с) 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 включаются 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.

Таковыми 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 туннелироваться 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 пользователем 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 resvdmacprofileid 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 resvdmacprofileid resvdmacprofileid

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 -Residential.
- 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 vlannam 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 vlnname 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 mappfile 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 vlnname 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.

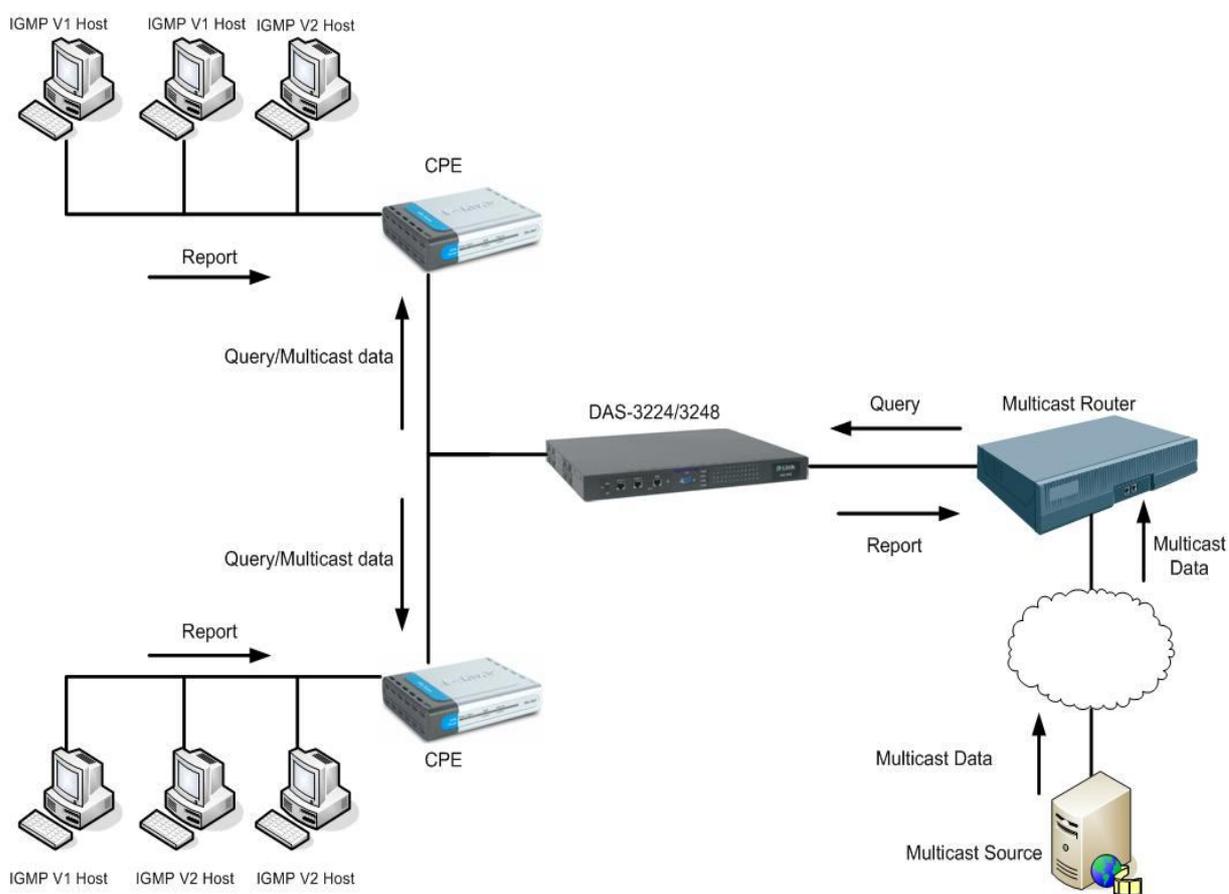


Рисунок 7-3: IGMP Snooping

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"
- description 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 происходит 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 [ vlandid <dec> ] [ egressports <Opt> ] [ forbidegressports <Opt> ]
```

```
modify bridge mcast fwdunreg [ vlandid <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 (Querier). 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 портам 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 create igmpsnoop querier info vlanid <идентификатор VLAN> portid

команды: <идентификатор порта, к которому подключен запросчик>

get igmpsnoop

querier info

Описание: Просмотр статических записей о запросчиках.

Синтаксис `get igmpsnoop querier info [vlanid <идентификатор VLAN>] [portid`

команды: `<идентификатор порта, к которому подключен запросчик>`]

delete igmpsnoop

querier info

Описание: Удаление информации о запросчике.

Синтаксис `delete igmpsnoop querier info vlanid <идентификатор VLAN> portid`

команды: `<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 скомутированы 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 create bridge static mcast vlanid <идентификатор VLAN> mcastaddr

команды: <multicast MAC address> [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

modify bridge static mcast

Описание: Изменение статической записи в multicast database

Синтаксис modify bridge static mcast vlanid <идентификатор VLAN> mcastaddr

команды: <multicast MAC address> [egressports < список multicast портов>] [forbidegressports <список запрещенных multicast портов>]

get bridge static mcast

Описание: Просмотр статических записей в multicast database

Синтаксис get bridge static mcast [vlanid <идентификатор VLAN>] [mcastaddr

команды: <multicast MAC address>]

delete bridge static mcast

Описание: Удаление статической записи в multicast database

Синтаксис delete bridge static mcast vlanid <идентификатор VLAN> mcastaddr

команды: <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 одинакова для всех VLAN. Таким образом, в данном случае VLANID является
----------------------	--

	<p>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.</p> <p>Использование: Create - Обязательно. Delete - Обязательно. Get – Опционально. Modify – Обязательно.</p> <p>Принимает значения: 1..4095</p>
mcastaddr mcastaddr	<p>MAC адрес групповой рассылки</p> <p>Использование: Create – Обязательно. Modify – Обязательно. Delete – Обязательно Get - Опционально</p>
egressports egressports	<p>Набор портов, являющихся членами данной группы множественной рассылки. Если порт уже указан как FrobiddenEgressPort, его необязательно включать в данный набор.</p> <p>Использование: Create - Опционально. Modify – Опционально.</p> <p>Принимает значения: 1 – 395</p>
forbidegressports forbidegressports	<p>Набор портов, являющихся членами данной группы. Динамическая конфигурация IGMP Snooping не распространяется на данные порты.</p> <p>Использование: Create - Опционально. Modify – Опционально.</p> <p>Принимает значения: 1 – 395</p>

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 команд: 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 `get bridge mcast fwdall [vlanid <идентификатор VLAN>]`
команды:

Таблица параметров:

vlanid vlanid	Идентификатор VLAN. В случае использования опции Shared VLAN for multicast (см. 2.9), информация о multicast MAC адресах одина 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 fwunreg 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 (**Внимание:** обязательный пункт для работы функции IGMP Snooping 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.

7.5.3.2. 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

(**Внимание:** обязательный пункт для работы функции IGMP Snooping на устройстве):

```
modify igmpsnoop port info portid <идентификатор порта> status [ enable | disable ]
```

7.5.3.3. Включение IGMP Querier на Uplink1 порту

```
modify igmpsnoop port info portid 385 querierstatus enable
```

(**Внимание:** обязательный пункт для работы функции IGMP Snooping на устройстве):

7.5.3.4. Обработка сообщений leave

```
modify igmpsnoop port info portid <идентификатор порта> [ leavemode Normal | Fast | FastNormal ]
```

Примечание: для уменьшения задержек переключения мультикаст потоков рекомендуется использовать **Leavemode Fast**.

7.5.3.5. Подавление уведомлений

modify igmpsnoop cfg info [reportsup 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 Просмотр Multicast Database

get bridge mcast forwarding [vlanid <идентификатор VLAN> **] [macaddr** <multicast MAC адрес> **]**

7.5.4. Фильтрация Multicast потоков

Часто возникает ситуация когда разным абонентам должны быть предоставлены разные мультикаст потоки (разные например разные пакеты каналов IPTV). Эта функция реализуется посредством команд фильтрации мультикаст потоков.

Фильтрация гарантирует, что в заданный порт попадут только заданные мультикаст потоки и никакие другие.

Синтаксис команды:

create igmpsnoop mvlan config grpipaddr grpipaddr **srcipaddr** srcipaddr **vlanid** vlanid | **none**
[mcastvlanstag mcastvlanstag | **none** **] [mcastvlanctag** mcastvlanctag | **invlan** | **none** **] [portlist**
portlist | **none** **]**

Пример: Необходимо ограничить мультикаст потоки на Bridge порту с portid 3, входящего в VLAN 20:

```
$create igmpsnoop mvlan config grpipaddr 239.30.30.33 srcipaddr 0.0.0.0 vlanid 20  
mcastvlanctag 20 portlist 3
```

```
$create igmpsnoop mvlan config grpipaddr 239.30.30.34 srcipaddr 0.0.0.0 vlanid 20  
mcastvlanctag 20 portlist 3
```

```
$create igmpsnoop mvlan config grpipaddr 239.30.30.36 srcipaddr 0.0.0.0 vlanid 20  
mcastvlanctag 20 portlist 39
```

```
$modify igmpsnoop port info portid 39 mcastvlanstatus enable
```

Теперь на данном порту доступны мультикаст потоки с групповыми IP адресами 239.30.30.33, 239.30.30.34 и 239.30.30.36. Остальные – недоступны.

7.5.5. Использование Multicast VLAN Registration (MVLAN Registration)

MVLAN Registration – это Регистрация Мультикастовых VLAN'ов, которая позволяет серверу передавать мультикастовый поток в одном VLAN'е, в то время как конечные пользователи смогут получать его, находясь в различных VLAN'ах. Пользователи подключаются к мультикастовой рассылке и отсоединяются от нее, отправляя сообщение IGMP Join/Leave на порт вещания. На рисунке 7-4 изображена ситуация, когда без использования MVLAN мультикастовый поток с сервера должен находиться в том же VLAN'е, что и принимающий его пользователь. В этом случае медиа-сервер должен передавать мультикастовый поток на каждый пользовательский VLAN, то есть в данном случае 6 раз. На рисунке 7-5, напротив, поддержка MVLAN позволяет серверу передать поток один раз, при этом пользователи во всех VLAN'ах могут к нему подключиться.



Рисунок 7-4. Вещание мультикаст потоков без использования MVLAN



Рисунок 7-5 Вещание мультикаст потоков с использованием MVLAN

Пример использования MVLAN Registration (для приведенных выше рисунков).

1. Создаем необходимый VLAN 12 с VID=12 (VLAN1 с VID=1 и именем Default-Vlan создан в системе по умолчанию)

```
$create vlan static vlnname VLAN12 vlanid 12
```

2. Задаем членство портов в VLAN (абонентских входят в VLANы как нетегированные члены, Uplink порт как тегированный):

```
$modify vlan static vlanid 1 untaggedports none egressports none
```

```
$modify vlan static vlnname Default-Vlan egressports 1 385 untaggedports 1
```

```
$modify vlan static vlnname VLAN12 egressports 12 385 untaggedports 12
```

3. Задаем PVID для портов

```
$modify gvrp port info portid 1 portvlanid 1 acceptframetypes all ingressfiltering true
```

```
$modify gvrp port info portid 12 portvlanid 12 acceptframetypes all ingressfiltering true
```

4. Создаем MVLAN с VID100

```
$create vlan static vlnname MVLAN vlanid 100
```

```
$modify vlan static vlnname MVLAN egressports 1 12 385 untaggedports 1 12
```

```
$create igmpsnoop mvlan config vlanid none grpipaddr 0.0.0.0 srcipaddr 0.0.0.0  
mcastvlanctag 100 portlist 1 2 3 4 5 6 7 8 9 10 11 12
```

5. Включаем функцию MVLAN на абонентских портах

```
$modify igmpsnoop port info portid 1 leavemode fast mcastvlanstatus enable
```

```
$modify igmpsnoop port info portid 12 leavemode fast mcastvlanstatus enable
```

6. Включаем функцию IGMP Snooping на клиентских портах

```
$modify igmpsnoop port info portid 1 status enable
```

```
$modify igmpsnoop port info portid 12 status enable
```

7. Включаем функцию MVLAN на Uplink порту

```
$modify igmpsnoop port info portid 385 querierstatus enable leavemode fast status enable
```

8. Включаем функцию IGMP Snooping глобально

```
$modify igmpsnoop cfg info status enable
```

9. Сохраняем настройки

```
$ commit
```

В соответствии с этими настройками PVID портов будет динамически меняться на портах для IGMP репортов, в соответствии с тем, что указано в mvlan в качестве тега (VID=100).

8. Протокол Spanning Tree

8.1. Понятие протокола STP (IEEE 802.1D)

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 стоимости 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.

	Octet
Protocol Identifier	1
	2
Protocol Version Identifier	3
BPDU Type	4
Flags	5
	6
	7
Root Identifier	8
	9
	10
	11
	12
	13
Root Path Cost	14
	15
	16
	17
	18
Bridge Identifier	19
	20
	21
	22
	23
	24
	25
Port Identifier	26
	27
Message Age	28
	29
Max Age	30
	31
Hello Time	32
	33
Forward Delay	34
	35

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 одновременной 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).

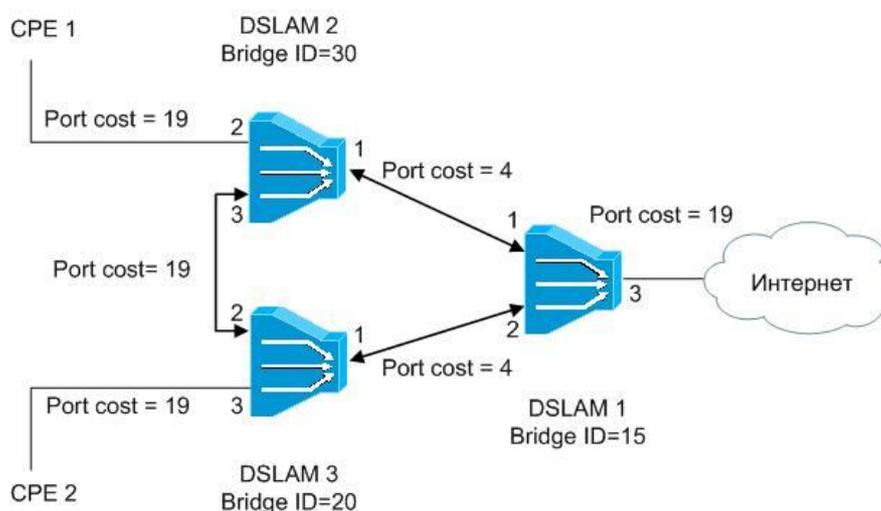


Рисунок 8-2. Перед применением протокола Spanning Tree.

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 корневой порт порт 1, так как его стоимость пути к корню меньше. После этого DSLAM 3 начинает объявлять стоимость пути до корня равную 4 нижележащим устройствам.

Выборы корневой порт DSLAM 2 происходят аналогично, и корневой порт для него становится порт 1 со стоимостью 4.

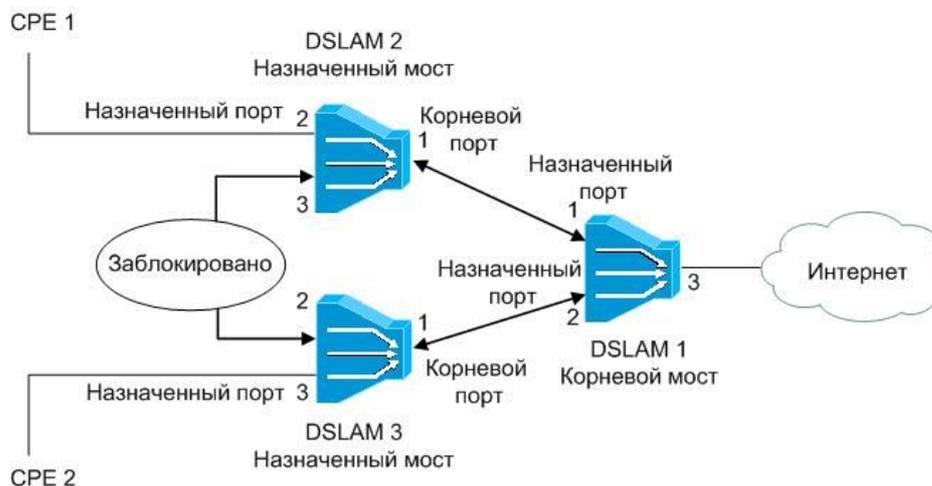


Рисунок 8-3. После применения протокола Spanning Tree.

Кроме этого, мультиплексы 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. Назначенным 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:

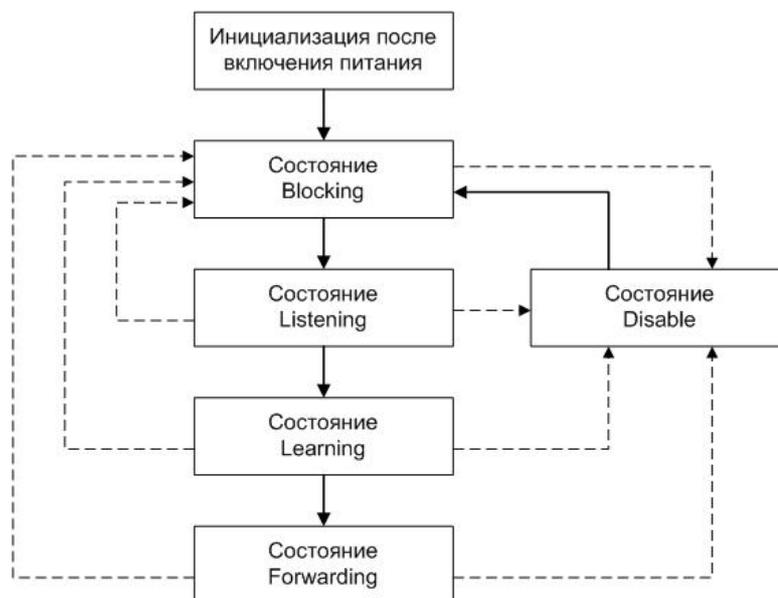


Рисунок 8-4. Состояния портов.

- **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 состоянии 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. Понятие протокола RSTP (IEEE 802.1w)

Обзор IEEE 802.1w RSTP

Протокол IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) является развитием стандарта IEEE 802.1D STP. Он был разработан для преодоления отдельных ограничений протокола STP, связанных с его производительностью. Протокол Rapid Spanning Tree Protocol значительно ускоряет время сходимости коммутируемой сети за счет мгновенного перехода корневых и назначенных портов в состояние продвижения.

Существенным отличием протоколов STP 802.1D и RSTP 802.1w является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии.

Состояния портов RSTP

Протокол RSTP объединяет состояния Disabled, Blocking и Listening, используемые в STP и создает единственное состояние Discarding (Отбрасывание), при котором порт не активен.

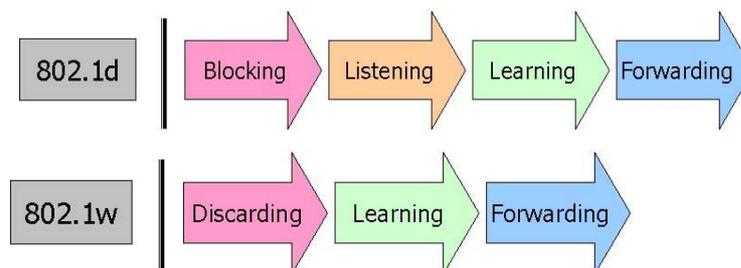


Рисунок 8-5. Состояния портов протоколов STP 802.1D и RSTP 802.1w.

Таблица 3. Различия между состояниями портов в STP и RSTP.

Состояние порта STP	Административное состояние порта сетевого устройства	Порт изучает MAC - адреса?	Состояние порта RSTP	Роль порта в активной топологии
DISABLE	Disabled	Нет	Discarding	Исключен (Disabled)
DISABLE	Enabled	Нет	Discarding	Исключен (Disabled)
BLOCKING	Enabled	Нет	Discarding	Исключен (Alternate, Backup)
LISTENING	Enabled	Нет	Discarding	Включен (Root, Designated)
LEARNING	Enabled	Да	Learning	Включен (Root, Designated)
FORWARDING	Enabled	Да	Forwarding	Включен (Root, Designated)

Роли портов RSTP

Выбор активной топологии завершается присвоением протоколом RSTP определенной роли каждому порту. Эти роли следующие:

- Корневой порт (Root Port)
- Назначенный порт (Designated Port)
- Альтернативный порт (Alternate Port)
- Резервный порт (Backup Port)

Корневой порт – это порт моста, который имеет по сети кратчайшее расстояние (в терминах стоимости пути) до корневого моста.

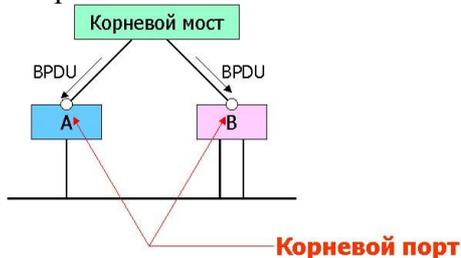


Рисунок 8-6. Корневой порт

Порт является **назначенным**, если он посылает BPDU с наилучшими параметрами в тот сегмент, к которому подключен.

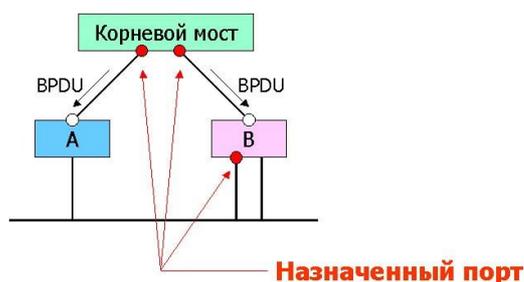


Рисунок 8-7. Назначенный порт.

Роли корневой порт и назначенный порт включают порт в активную топологию.

В RSTP существуют 2 роли – альтернативный порт (*Alternate*) и резервный порт (*Backup*), соответствующие состоянию «Заблокирован» в STP и исключающие порт из активной топологии.

Альтернативный порт предлагает альтернативный основному пути путь в направлении корневой моста и может заменить корневой порт в случае выхода его из строя.

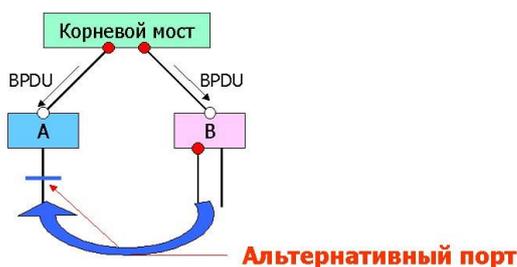


Рисунок 8-8. Альтернативный порт.

Резервный порт предназначен для резервирования пути, предоставляемого назначенным портом в направлении сегментов сети, и не может гарантировать альтернативное подключение к корневому мосту. Резервные порты существуют только в конфигурациях, где есть два или более соединения данного моста с данной сетью (сегментом сети).

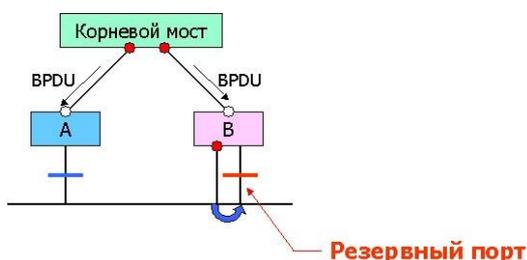


Рисунок 8-9. Резервный порт.

Процесс вычисления связующего дерева у обоих протоколов одинаков.

Однако, при работе RSTP, порт может перейти в состояние продвижения значительно быстрее, т.к. он больше не зависит от конфигурации таймеров. Порты больше не должны ждать стабилизации топологии, чтобы перейти в режим продвижения. Для того чтобы обеспечить быстрый переход в это состояние, протокол RSTP вводит два новых понятия: пограничный порт (*edge port*) и порт типа «точка-точка» (*point-to-point*, P2P).

Пограничным (Edge) портом объявляется порт, непосредственно подключенный к сегменту, в котором не могут быть созданы петли. Например, порт непосредственно подключен к рабочей станции. Порт, который определен как пограничный, мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Пограничный порт теряет свой статус и становится обычным портом связующего дерева в том случае, если получит пакет BPDU.

P2P порт, обычно используемый для подключения к другим мостам, также способен быстро перейти в состояние продвижения. При работе RSTP все порты, функционирующие в полнодуплексном режиме, рассматриваются как порты P2P, до тех пор, пока не будут переконфигурированы вручную.

Сходимость 802.1w

1. Канал связи между мостом А и корневым (Root) мостом заблокирован и оба моста обмениваются BPDU. Как только мост А получит BPDU, он заблокирует свои не пограничные назначенные порты. Эта операция называется синхронизацией (*sync*).

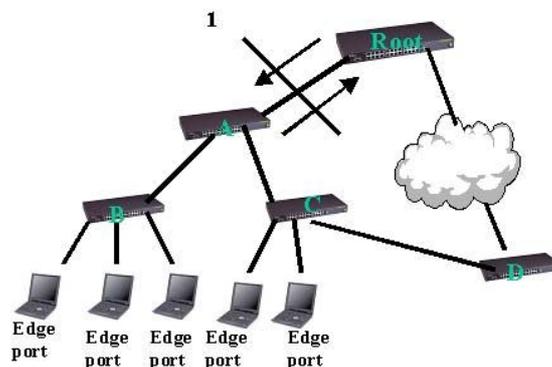


Рисунок 8-10.

2. Как только мост А заблокирует свои не пограничные порты, корневой порт моста А перейдет в состояние продвижения (*forwarding*).

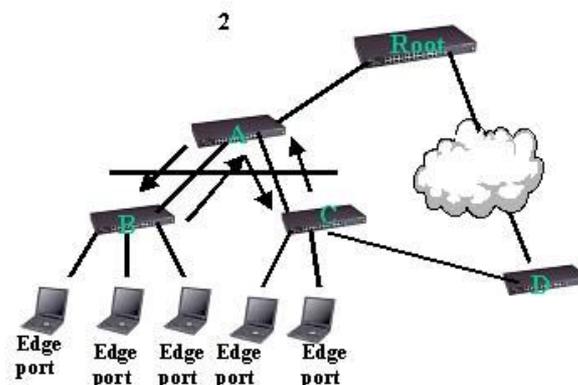


Рисунок 8-11.

3. Теперь сеть заблокирована ниже моста А. По заблокированному отрезку сети через мост А передаются только новые BPDU, порождаемые корневым коммутатором.

4. Заблокированные порты моста А также начинают «вести переговоры» о быстром переходе в состояние продвижения с соседними портами мостов В и С. Эти мосты инициируют операцию синхронизации.
5. Мост В имеет только пограничные назначенные порты (за исключением корневого порта к мосту А). Таким образом не один его порт не блокируется, что дает возможность порту моста А перейти в состояние продвижения.
6. Аналогично, мост С блокирует только свой назначенный не пограничный порт к мосту D.

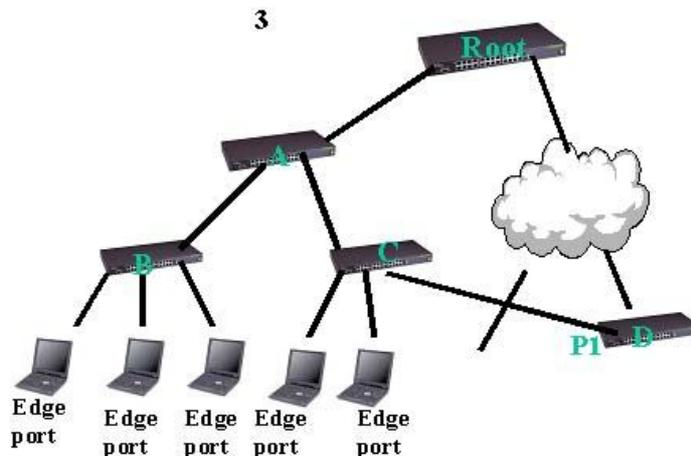


Рисунок 8-12.

7. Порт P1 моста D блокируется. Это означает, что окончательная топология сети сформируется только после прохождения новых BPDU вниз по дереву.
8. Следует отметить, что таймеры в механизме быстрой сходимости не используются. RSTP использует механизм подтверждений (*acknowledgement*), которые мост может отправлять через свой новый корневой порт для получения авторизации на его мгновенный переход в состояние продвижения. Это позволяет избежать вносящих задержку стадий прослушивания (*listening*) и обучения (*learning*).

Последовательность предложений/соглашений

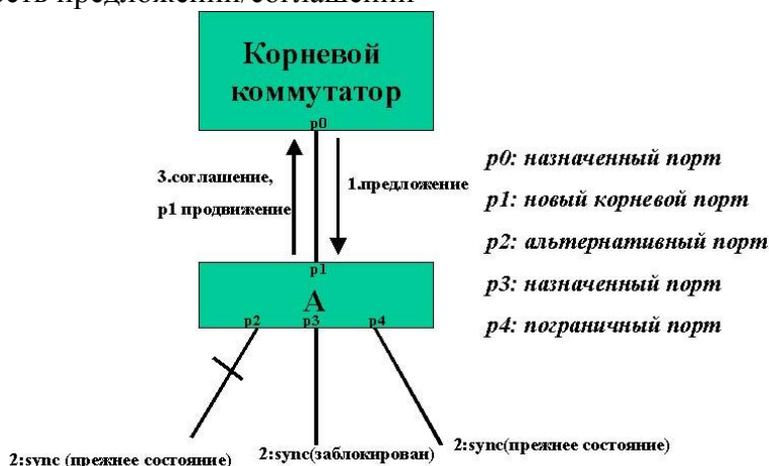


Рисунок 8-13.

Порт является синхронизированным «*in-sync*», если он удовлетворяет следующим критериям:

- Он находится в заблокированном состоянии (это состояние discarding в стабильной топологии)
- Он является пограничным портом

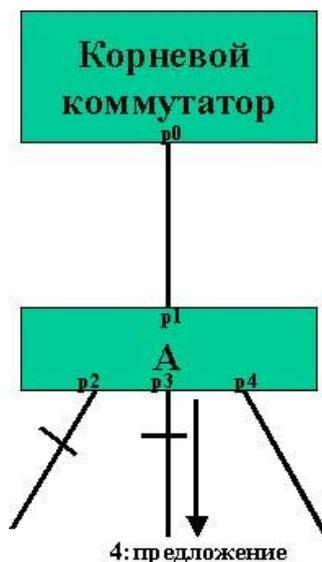


Рисунок 8-14.

Механизм изменения топологии

1. Определение изменений топологии

В протоколе RSTP только не пограничные порты переходят в состояние продвижения при изменении топологии. Это означает, что разрыв соединения больше не рассматривается как изменение в топологии, в отличие от протокола STP (802.1d).

Когда устройство RSTP обнаруживает изменение топологии, происходит следующее:

- Мост устанавливает начальное значение таймера TC While равным удвоенному интервалу hello для всех не пограничных назначенных портов и корневого порта, если необходимо.
- Мост сбрасывает MAC-адреса, ассоциированные со всеми этими портами.
- Поскольку таймер TC While запускается на порте, BPDU, отправляемые с этого порта, имеют установленный бит TC. Пока таймер активен, BPDU также отправляются через корневой порт.

2. Распространение информации об изменении топологии

Когда устройство получает от соседа BPDU с установленным битом TC, происходит следующее:

- Мост сбрасывает все MAC-адреса изученные этими портами, за исключением того, который получил информацию об изменении топологии.
- Мост устанавливает начальное значение таймера TC While и отправляет BPDU с установленным битом TC через все назначенные порты и корневой порт (RSTP больше не использует специальные TCN BPDU, за исключением случаев, когда требуется уведомить коммутатор-источник).

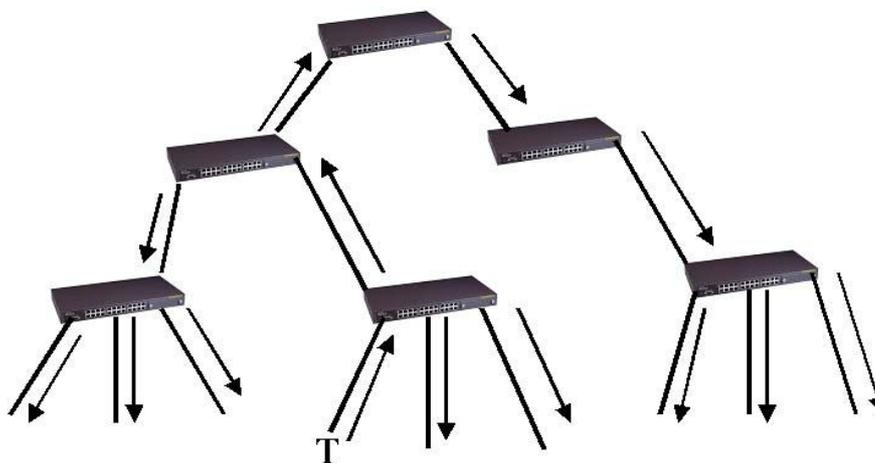


Рисунок 8-15. Новый механизм изменения топологии.
Отправитель BPDU с битом TC непосредственно распространяет информацию об изменении топологии через всю сеть.

8.3.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 modify stp info [priority priority-value] [maxage maximum-age] [htime
 команды: hello-time] [fdelay forward-delay] [enable|disable]

get stp info

Описание: Просмотр глобальных настроек STP протокола на DAS-3248
 Синтаксис get stp info
 команды:

reset stp stats

Описание: Сброс счетчиков STP статистики
 Синтаксис reset stp stats
 команды:

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	Максимальное 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: modify stp port info portid portid [enable|disable] [pcost pcost] [priority
команды: priority] [pktpriority pktpriority]

get stp port

Описание: Просмотр настроек STP на отдельном порту
Синтаксис: get stp port info portid portid
команды:

reset stp port

Описание: Сброс счетчиков STP
Синтаксис reset stp port info portid portid
команды:

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

8.4. Настройка протокола RSTP на DAS-3248.

Команды глобальной настройки RSTP на DAS-3248

Команды системы:

modify rstp info

Описание: Настройка глобальных параметров STP протокола
Синтаксис modify rstp info [rstpEnable disable|enable] [stpVersion
команды: stpCompatible|rstp] [priority <hex>] [maxage maximum-age] [htime
hello-time] [fdelay forward-delay]

get stp info

Описание: Просмотр глобальных настроек STP протокола на DAS-3248
Синтаксис get rstp info
команды:

reset stp stats

Описание: Сброс счетчиков STP статистики
Синтаксис reset rstp stats
команды:

Таблица параметров:

priority priority-value	Приоритет устройства в RSTP (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	Максимальное время (в секундах), через которое любой порт, использующий протокол RSTP 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.

rstpEnable disable enable	Глобальное включение протокола STP
----------------------------------	------------------------------------

Пример команды: \$ modify rstp info priority 0x20 maxage 25 htime 5 fdelay 20
rstpEnable enable

По умолчанию, протокол RSTP выключен.

Команды настройки протокола RSTP на отдельных Bridge портах.

Команды системы:

modify rstp port info

Описание: Конфигурирование настроек STP на отдельном порту
Синтаксис modify rstp port info portid portid [priority <hex>] [portEnable
команды: Enable|Disable] [pcost <dec>] [edge true|false] [migration true|false]

get rstp port info

Описание: Просмотр настроек RSTP на отдельном порту
Синтаксис get rstp port info portid portid
команды:

reset stp port info

Описание: Сброс счетчиков RSTP
Синтаксис reset rstp port info portid portid
команды:

Таблица параметров:

portid portid	Номер Bridge интерфейса, на котором производится настройка RSTP Использование: Get – Опционально. Modify – Обязательно. Принимает значения: 1..386
portEnable Enable Disable	Включение протокола RSTP на отдельном Bridge интерфейсе. Использование: Modify – Опционально.
pcost pcost	Path Cost (стоимость) порта . Использование: Modify – Опционально.
priority <hex>	Приоритет порта в STP (6 битная часть Port ID, доступная для изменения пользователем). Использование: Modify – Опционально.
edge true false	Показывает, является ли порт конечным (Edge)

Пример команды: \$ modify rstp port portid 1 enable pcost 20000 priority 0x80 edge false

Экранный вывод:

```
Port      : 1      PortId   : 0x8001
Priority   : 0x80   State    : disabled
Port Enable : Enable Path Cost : 20000
Desig Root : 0x0000000000000000
Desig Bridge : 0x0000000000000000
Desig Port : 0x8001  Desig Cost : 0
Edge      : false
Migration : false   Role     : Disabled
```

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.

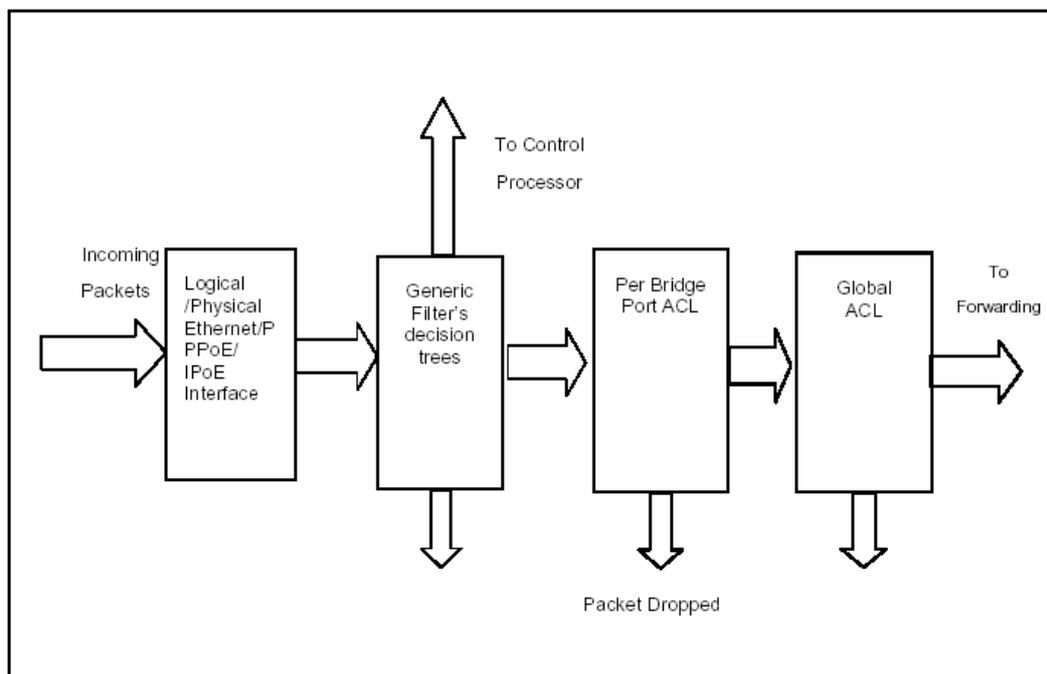


Рисунок 9-1: Порядок применения Generic Filter на входящих интерфейсах

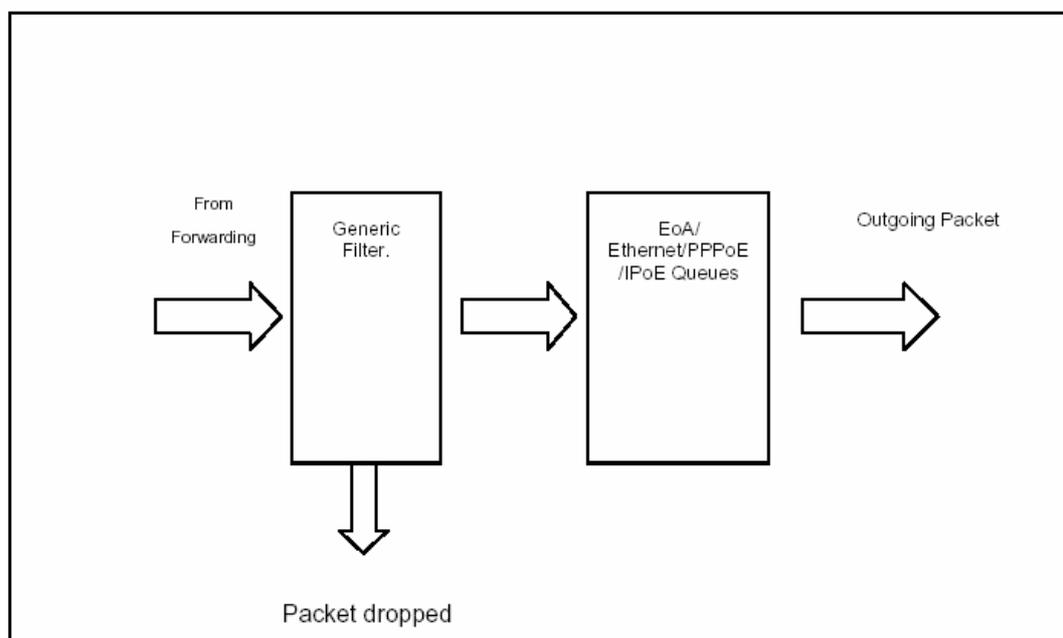


Рисунок 9-2: Порядок применения Generic Filter на исходящих интерфейсах

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 (retaserviceprio):** 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 форвардятся 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 памятьПравила, 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 deregистрировать правило на интерфейсе, и тогда оно снова становится неэффективным. Регистрация и deregистрация 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 **pktype 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 Priority** и **425 подправил Low Priority** для правил типа **ruledir=In** и **25 подправил High Priority** 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.

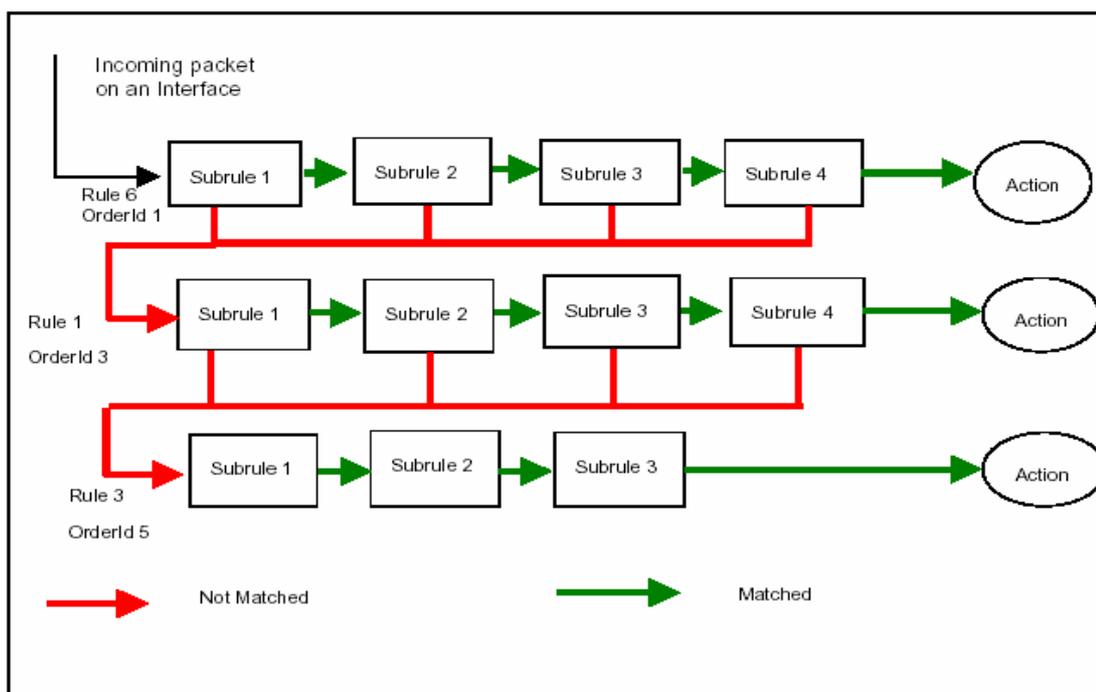


Рисунок 9-3: Порядок исполнения правил и подправил

9.1.1.3. Порядок действий при создании правила Generic Filter

- Создать правило generic фильтра (**create filter rule**)
- Добавить одно или несколько подправил фильтрации 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, **allppoe** –все интерфейсы ppoe).

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.

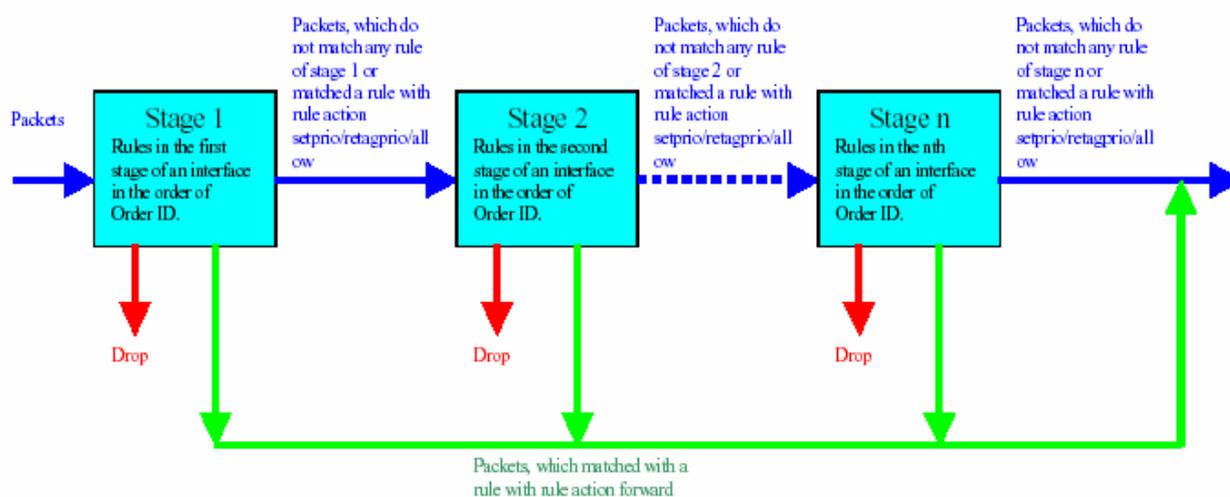


Рисунок 9-4: Многоэтапность обработки пакетов.

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 ExprID .

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 ExprID может применено к правилам с помощью действия **exprdef** ко многим правилам.

Например: `$create filter rule entry ruleid 1 action exprdef exprid 1`

Количество ExprID 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 многочисленных 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 ту же очередь с дисциплиной DP-SP. Это сильно затрудняет проведение приоритизации потоков в Control Plane. Для решения этой проблемы и дифференциации 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 prototype from 2 prototype icmp eq

Включить правило

\$modify filter rule entry ruleid 1 status enable

2. Прикрепить правило к интерфейсу.

\$create filter rule map ifname eoa-1 stage 1 ruleid 1 orderid 1

3. Зарегистрировать пользовательское приложение, используя Packet Filter, для приема пакетов из ControlPlane.

\$sigmpsnoop cfg info status enable

\$sigmpsnoop 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 шестнадцатеричный вид и запишите полученное число без разделителей (точек). Например, 0x12345678 соответствует IP адресу 18.52.86.120.

Пример. Создать Generic List

\$create filter list genentry ifname eoa-1 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-1 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 icmp type 8 icmp type eq subruleprio asinrule

Создаем подправило, в котором указываем, что же все-таки фильтровать:

ruleid 2 subruleid 1 - первое подправило второго правила

icmp type 8 icmp type 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-1 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 обслуживания

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 АТМ 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 (АТМ 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 w_1, w_2, \dots, w_n , тогда каждый класс трафика получит:

$$R(i) = \frac{w(i) * 100}{\sum w(i)}, \text{ где } i=1 \dots n \text{ — полосы пропускания}$$

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:

$$O(i) = R(i) + \frac{\sum_j w(j)}{j} \text{ где } j=1 \dots m$$

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, предрасчитанная 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 получают 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.

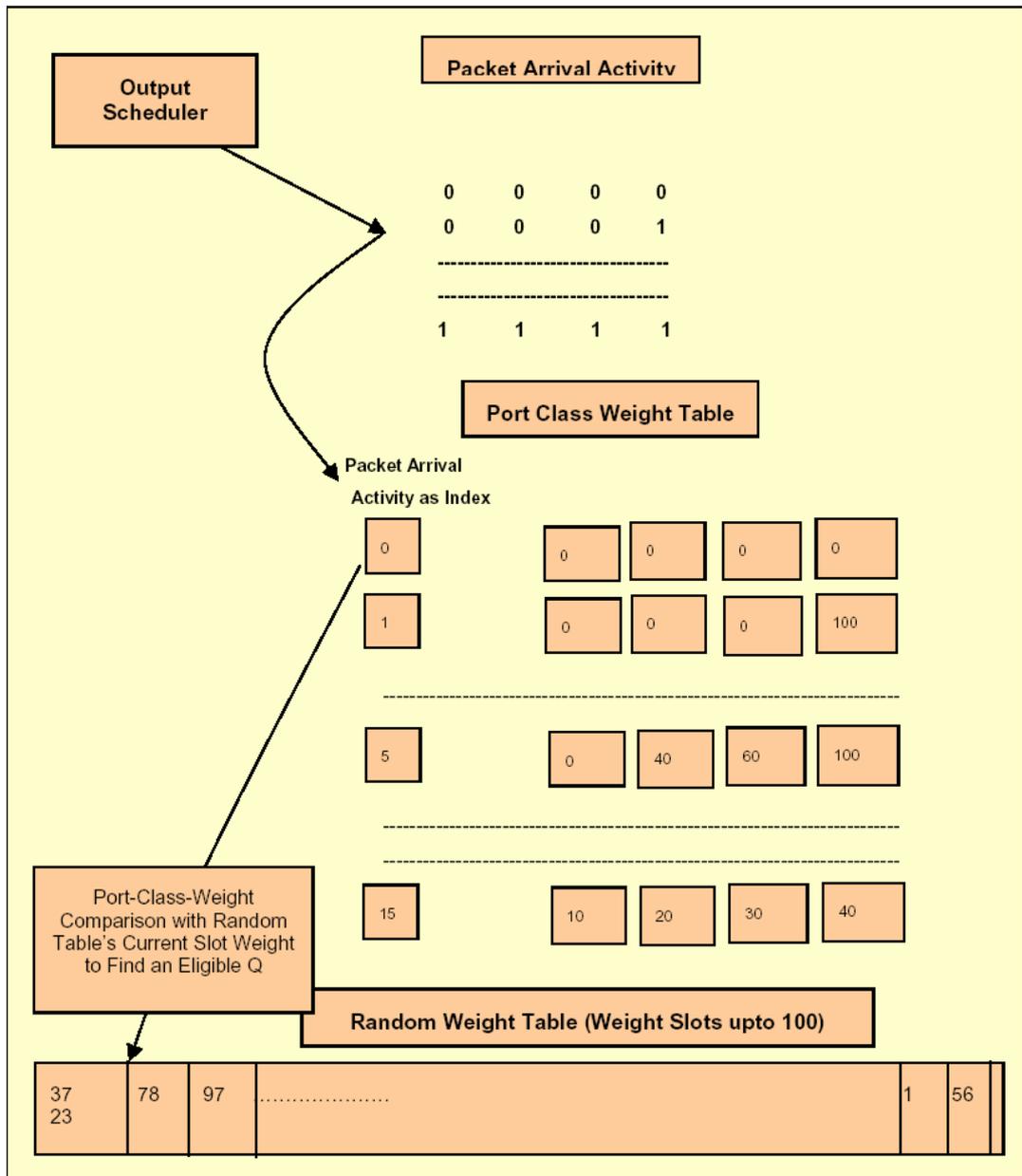


Рисунок 10-1

Customized Scheduling

Данный алгоритм может быть применен только к ATM очередям. Пользователь может настроить 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 пропускания, 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 пропускания, 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 (ТБФ).

ТБФ- это дисциплина очереди, которая передает поступающие пакеты со скоростью, не превышающей административно заданный порог, но с возможностью превышающих его коротких всплесков.

Реализована ТБФ 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)
Задаёт 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.

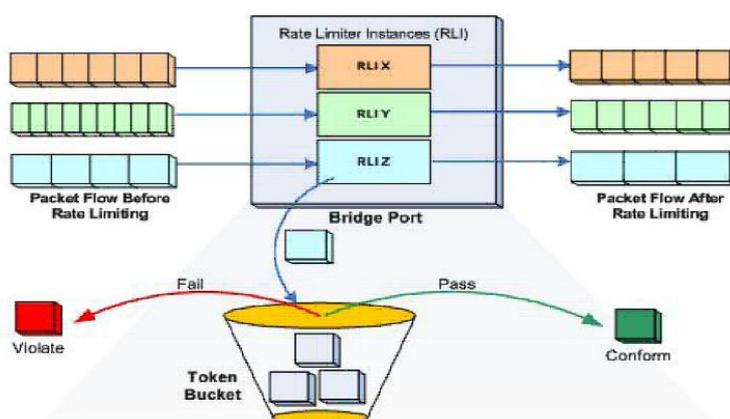


Рисунок 10-2. Single Rate Two Color Marking (SRTCM)

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.
- Committed Rate-Ограничение скорости второго буфера
- Committed Burst Size-Размер второго буфера

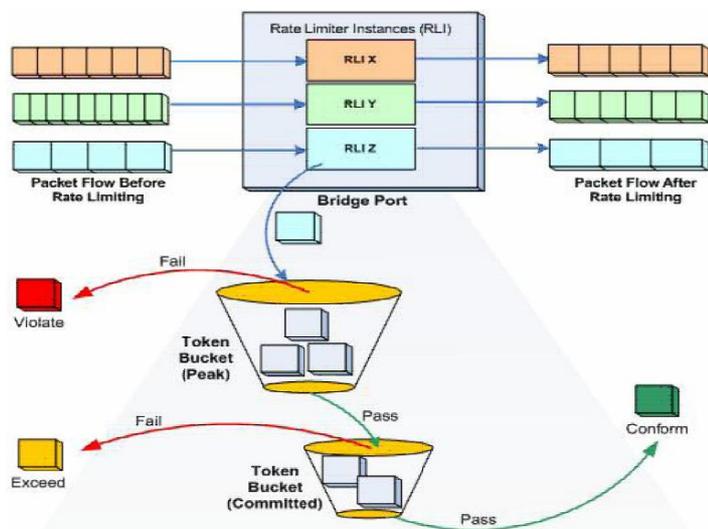


Рисунок 10-3. Two Rate Three Color Marking (TRTCM)

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 АТМ 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.

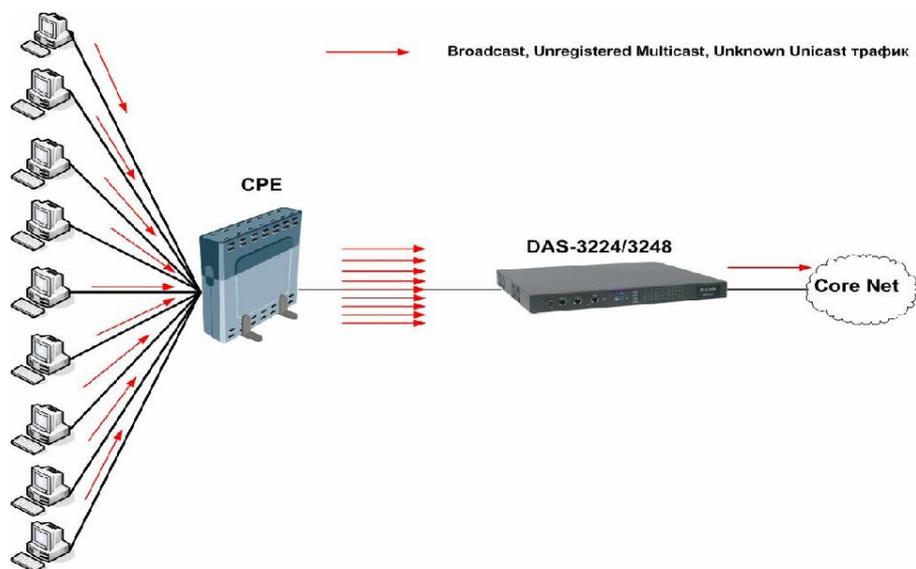


Рисунок 10-4

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)).

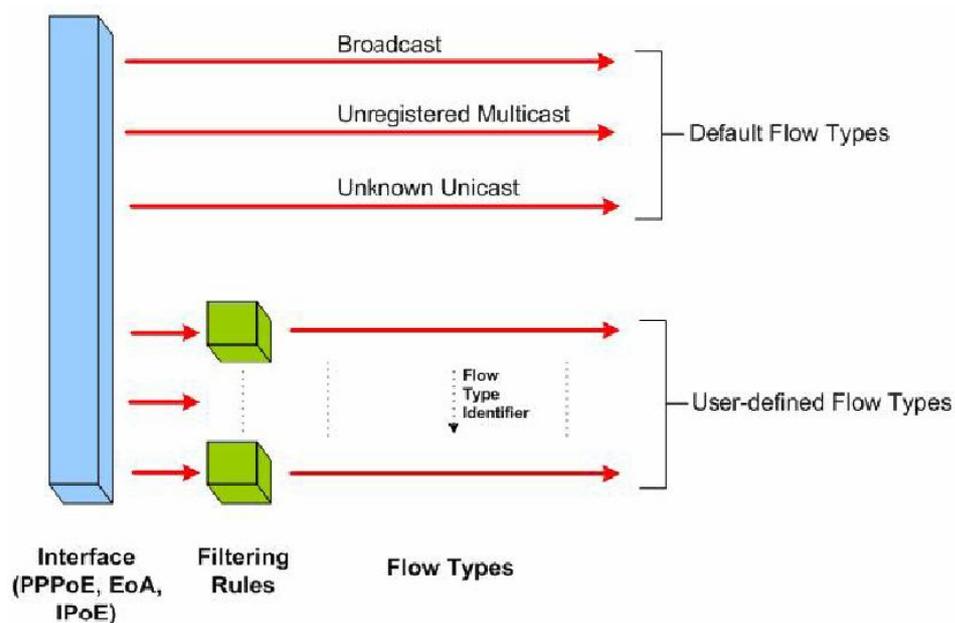


Рисунок 10-5

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 определенных типов:

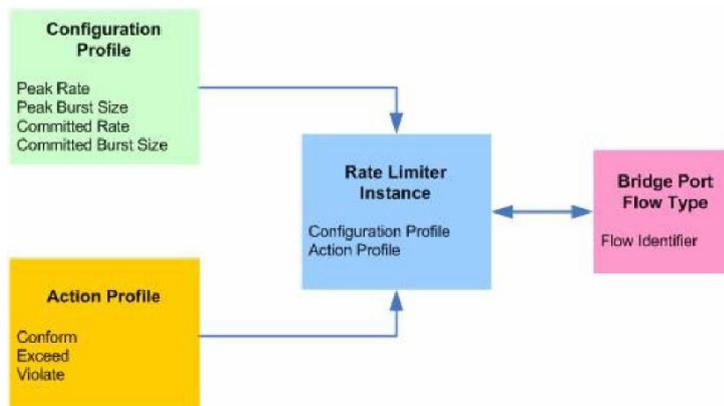


Рисунок 10-6. Алгоритм конфигурирования определенных типов потока

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 (Committed Rate)

mbs – Размер второго буфера Committed 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 Profile

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**.

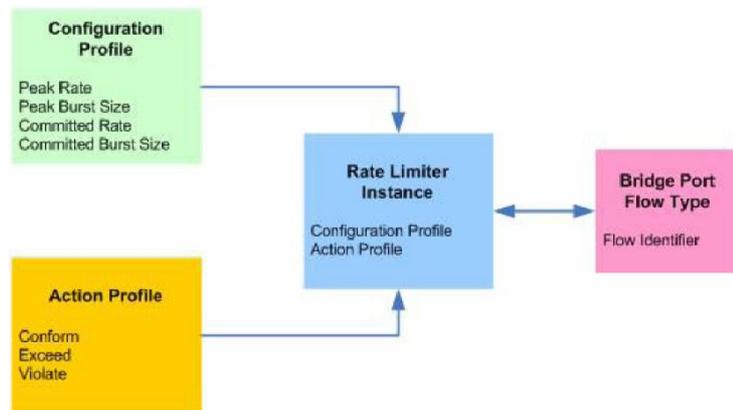


Рисунок 10-7. Алгоритм конфигурирования пользовательских типов потоков

Алгоритм конфигурирования контроля полосы пропускания для predetermined 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 (Committed Rate)

mbs – Размер второго буфера Committed 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 Profile
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 rinstance map

Синтаксис команды:

create bridge rinstance map [portid all| portid] [**flowtype** flotypeid] [**instanceid** instanceid], где
portid all| portid – идентификатор бридж интерфейса на который прикладывается 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 SRTRM 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 потоки попадают в одну и ту же очередь с дисциплиной DP-SP на интерфейсе. Это сильно затрудняет проведение приоритезации потоков в Control Plane. Для решения этой проблемы и дифференциации 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-битовой 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- уставляет 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.

- ВАС 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 (широковещательного) 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 осуществляется Rate Limiting

```
$ create filter rule map ifname eth-1 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 TRTSM 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 осуществляться Rate Limiting

```
$ create filter rule map ifname eoa-1 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 setbacklevel actionval 0x1
$ create rl actionprofile info profileid 3 result violate action drop
```

5. Связать RL Profile 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 низким 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][**conformation** colorgreen][**exceedaction** drop|coloryellow] [**violateaction** drop|coloryellow], где

profilename – имя IRL профиля

irltype sr2cm|trtcm –выбор алгоритма SRTCM или TRTCM

cir – Committed Rate (Скорость первого буфера)

cbs – Committed Burst Size (Емкость первого буфера)

pbs – Peak Burst Size (Емкость второго буфера)

pir – Peak Rate (Скорость второго буфера).

conformation 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 интерфейса

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
conformation 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 Downstream потока данных, передающегося к клиентам.

Функция ORL применяется, 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 АТМ) на срабатывание IRL при 80 процентном заполнении для 4 очереди. Размер очереди оставить неизменным.

\$modify trfclass profile class profileid 1 classid 4 thrshld1 80

11. Упрощенный командный (CLI) режим. Применение. Примеры

11.1. Назначение упрощенного (пользовательского) командного режима. Принципы и основные команды

Упрощенный командный (пользовательский) режим представляет собой специально созданный для удобства пользователя режим, часть команд в котором представляют собой макрокоманды.

То есть, одна команда упрощенного режима может заменять собой иногда несколько команд обычного (назовем его инженерным) командного режима.

Пример - изменение параметров интерфейсов устройства. Как правило, обычный (инженерный) режим требуется, чтобы статус интерфейса сначала был переведен в состояние `disable` (административно выключен), затем изменены его параметры, затем он будет административно включен. Таким образом, требуется как минимум три команды инженерного режима. Упрощенный (назовем его пользовательским) режим позволяет сделать это изменение одной командой.

Однако следует помнить, что команды пользовательского режима созданы только для осуществления наиболее частых типовых функций.

Тонкие же настройки по-прежнему стоит осуществлять с помощью инженерного режима.

Для переключения между пользовательским и инженерным режимом CLI существуют две команды, которые нигде в устройстве не отображаются (в том числе и в подсказке):

usermode- перевод устройства в пользовательский CLI режим.

Вид приглашения командной строки в этом случае меняется на:

```
/>
```

engmode- перевод устройства в инженерный CLI режим.

Вид приглашения командной строки в этом случае меняется на:

```
$
```

Пользовательский CLI режим представляет собой дерево вложенных меню команд. (дерево команд показано в пункте 11.2)

Для перехода в корень дерева на любом уровне используется команда- **top**

Для перехода на один уровень вверх – **exit**.

Для выхода из CLI- **logout**.

В пользовательском (упрощенном командном) режиме, также как и в инженерном, существует автодобавление команды по первым символам клавишей TAB.

11.2.Дерево команд упрощенного командного режима.

[date-time]	вложенное меню управления временем
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима установить дату и время на устройстве посмотреть дату и время на устройстве
[hw]	вложенное меню аппаратных настроек
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима установить MAC адрес на ethernet порту просмотреть MAC адрес
ping	“пропинговать” IP адрес
reboot	Перезагрузить устройство (либо перезагрузить с настройками по умолчанию либо с последним сохраненным конфигурационным файлом)
logout	выйти из CLI режима
[config]	вложенное меню конфигурирования
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима
[acl]	вложенное меню ACL
exit top logout add del show	подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить список доступа (ACL) Удалить список доступа (ACL) просмотреть список доступа (ACL)
[alarm]	вложенное меню предупреждений
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима
[pm-profile]	вложенное меню
exit top logout set	подняться на уровень выше выйти в корневое меню выйти из CLI режима изменить ADSL PM профиль
profile-15min profile-1day	изменить 15 минутный alarm профиль изменить дневной alarm профиль
show	show alarm profile
[definition]	вложенное меню
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режим установить активный Alarm профиль просмотреть статус активного профиля
[relay]	вложенное меню Relay

<p>exit top logout</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима</p>
<p>[suboption]</p>	<p>вложенное меню</p>
<p>exit top logout set show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима изменить формат suboption для DRA показать формат suboption для DRA</p>
<p>[cidformat]</p>	<p>вложенное меню</p>
<p>exit top logout set show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима установить формат circuid ID для PIA и DRA показать формат circuid ID</p>
<p>[ge]</p>	<p>вложенное меню</p>
<p>exit top logout show enable disable</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима показать статус DHCP Relay на ethernet портах включить DRA на ethernet портах выключить DRA на ethernet портах</p>
<p>[dhcp]</p>	<p>вложенное меню</p>
<p>exit top logout disable enable show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима выключить DRA на устройстве включить DRA на устройстве показать статус DRA на устройстве</p>
<p>[pvc]</p>	<p>вложенное меню</p>
<p>exit top logout set show enable disable</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима установить параметры DRA на отдельном PVC показать статус DHCP relay на отдельном PVC включить DRA на отдельном PVC выключить DRA на отдельном PVC</p>
<p>[pppoe]</p>	<p>вложенное меню</p>
<p>exit top logout disable enable show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима выключить PIA на устройстве включить PIA на устройстве показать статус PIA на устройстве</p>
<p>[pvc]</p>	<p>вложенное меню</p>
<p>exit top logout set show enable disable</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима установить параметры PIA на отдельном PVC показать статус PPPoE relay на отдельном PVC включить PIA на отдельном PVC выключить PIA на отдельном PVC</p>

[igmpsnoop]	вложенное меню управления IGMP Snooping
exit top logout disable enable show	подняться на уровень выше выйти в корневое меню выйти из CLI режима выключить IGMP Snooping на устройстве включить IGMP Snooping на устройстве показать статус IGMP Snooping на устройстве
[ge]	вложенное меню
exit top logout set disable enable show	подняться на уровень выше выйти в корневое меню выйти из CLI режима установить параметры IGMP Snooping на Uplink выключить IGMP Snooping на ethernet порту включить IGMP Snooping на ethernet порту показать статус IGMP Snooping на ethernet порту
[pvc]	вложенное меню
exit top logout set enable disable show	подняться на уровень выше выйти в корневое меню выйти из CLI режима установить режим выхода из мультикаст группы (leavemode) для отдельного PVC включить IGMP Snooping на отдельном PVC выключить IGMP Snooping на отдельном PVC показать статус IGMP Snooping на отдельном PVC
[mvr]	вложенное меню
exit top logout [channel]	подняться на уровень выше выйти в корневое меню выйти из CLI режима вложенное меню
exit top logout add del show	подняться на уровень выше выйти в корневое меню выйти из CLI режима создать мультикаст канал (добавить запись о мультикаст VLAN и групповом IP адресе) удалить мультикаст канал просмотреть доступные мультикаст каналы
[mvlan]	вложенное меню
exit top logout add del clear show	подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить членов в мультикаст VLAN удаление членов из мультикаст VLAN удалить всех членов мультикаст VLAN просмотреть список мультикаст VLAN и их членов
[pvc]	вложенное меню
exit top logout enable	подняться на уровень выше выйти в корневое меню выйти из CLI режима включить MVR (Multicast VLAN Registration) на отдельном PVC

disable show	выключить MVR на отдельном PVC показать статус MVR на отдельном PVC
[mcast-profile]	вложенное меню
exit top logout add del set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить мультикаст профиль удалить мультикаст профиль задать параметры мультикаст профиля показать статус мультикаст профиля
[pvc]	вложенное меню
exit top logout set clear show	подняться на уровень выше выйти в корневое меню выйти из CLI режима “привязать” мультикаст профиль к PVC удалить привязку мультикаст профиля к PVC показать привязку мультикаст профиля к PVC
[ge]	вложенное меню управления ethernet интерфейсами
exit top logout add del set disable enable show	подняться на уровень выше выйти в корневое меню выйти из CLI режима создать Uplink порт удалить Uplink порт задать лимит MAC адресов на Uplink порту административно выключить ethernet порт административно включить ethernet порт показать настройки ethernet порта
[rstp]	вложенное меню управления RSTP
exit top logout disable enable set show [ge]	подняться на уровень выше выйти в корневое меню выйти из CLI режима выключить поддержку RSTP на устройстве включить поддержку RSTP на устройстве задать параметры RSTP на устройстве просмотреть параметры RSTP на устройстве вложенное меню
exit top logout set enable disable show	подняться на уровень выше выйти в корневое меню выйти из CLI режима задать параметры RSTP на ethernet порту включить поддержку RSTP на ethernet порту выключить поддержку RSTP на ethernet порту показать параметры RSTP на ethernet порту
[mgmt]	вложенное меню управления устройством
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима
[user]	вложенное меню управления пользователями
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима

<p>add del show</p>	<p>добавить новый аккаунт пользователя удалить аккаунт пользователя просмотреть всех пользователей</p>
<p>[snmp]</p>	<p>вложенное меню SNMP настроек</p>
<p>[host]</p>	<p>вложенное меню</p>
<p>exit top logout add del show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить доверенный SNMP хост удалить доверенный SNMP хост показать список доверенный хостов SNMP</p>
<p>[traphost]</p>	<p>вложенное меню</p>
<p>exit top logout add del show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить хост получатель SNMP Traps добавить хост получатель SNMP Traps добавить хост получатель SNMP Traps</p>
<p>[community]</p>	<p>вложенное меню</p>
<p>exit top logout add del show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить SNMP community string удалить SNMP community string показать список SNMP community string</p>
<p>[vlan-id]</p>	<p>вложенное меню</p>
<p>exit top logout set show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима установить Management VLAN показать Management VLAN</p>
<p>[default-route]</p>	<p>вложенное меню</p>
<p>exit top logout set show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима установить маршрут по умолчанию показать маршрут по умолчанию</p>
<p>[port]</p>	<p>вложенное меню управления DSL портами</p>
<p>exit top logout disable enable clean dsl-profile set dsl-profile show</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима административно выключить порт административно включить порт удалить “привязку” порта к профилю DSL “привязать” порт к профилю DSL показать “привязку” порта к профилю DSL</p>
<p>[profile]</p>	<p>вложенное меню DSL профилей</p>
<p>exit top logout add del</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима создать новый DSL профиль удалить DSL профиль</p>

set	изменить параметр существующего DSL профиля
show	показать параметры DSL профиля (ей)
[vlan]	вложенное меню управления VLAN
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
[default-vid]	вложенное меню
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
[ge]	вложенное меню
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
set	задать параметры VLAN для ethernet порта
show	показать параметры VLAN для ethernet порта
[pvc]	вложенное меню
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
set	задать параметры VLAN для PVC
show	показать параметры VLAN для PVC
[ge]	вложенное меню
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
add	add vlan
set	включить или выключить тегирование на ethernet порту
stag	установить или удалить SVLAN тег для ethernet порта (для Q-in-Q режима)
del	удалить VLAN
show	показать параметры VLAN на ethernet порту
[mode]	вложенное меню
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
set	задать режим VLAN
show	показать режим VLAN
[pvc]	вложенное меню управления PVC
exit	подняться на уровень выше
top	выйти в корневое меню
logout	выйти из CLI режима
add eoa	добавить PVC и создать стек интерфейсов с вышележащим интерфейсом EOA типа
add ipoa	добавить PVC и создать стек интерфейсов с вышележащим интерфейсом IPoA типа
add pppoa	добавить PVC и создать стек интерфейсов с вышележащим интерфейсом PPPoA типа

del show mac-limit	удалить заданный PVC Просмотреть параметры PVC задать лимит MAC адресов для отдельного PVC
[pppoa-conf]	вложенное меню
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима задать pppoa pvc MAC адрес показать pppoa pvc MAC адрес
[system-info]	вложенное меню
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима set system info show system info
[time-service]	вложенное меню управления временем
exit top logout add del show enable disable	подняться на уровень выше выйти в корневое меню выйти из CLI режима добавить новый сервер времени удалить сервер времени показать список серверов времени включить сервер времени выключить сервер времени
[force-pm]	вложенное меню DSL Power management
exit top logout port	подняться на уровень выше выйти в корневое меню выйти из CLI режима задать принудительный режим DSL Power Management
[route]	вложенное меню маршрутизации
exit top logout add del show	подняться на уровень выше выйти в корневое меню выйти из CLI режима add route delete route show route info
[bridge]	вложенное меню
exit top logout set show	подняться на уровень выше выйти в корневое меню выйти из CLI режима set bridge configuration show bridge configuration
[sntp]	вложенное меню SNTP
exit top logout enable disable add del	подняться на уровень выше выйти в корневое меню выйти из CLI режима включить SNTP выключить SNTP добавить SNTP сервер удалить SNTP сервер

show	показать конфигурацию SNTP
[remote-dslam]	вложенное меню
exit top logout enable disable add del show	подняться на уровень выше выйти в корневое меню выйти из CLI режима включить управление удаленным DSLAM выключить управление удаленным DSLAM добавить ip адрес хоста удаленного управления DSLAM удалить ip адрес хоста удаленного управления remote DSLAM host IP address показать конфигурацию функции удаленного управления DSLAM
save	Сохранить текущие настройки в энергонезависимой памяти
[diag]	вложенное меню диагностики
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима
[delt]	вложенное меню DELT теста
exit top logout start	подняться на уровень выше выйти в корневое меню выйти из CLI режима запустить DELT тест
[atm-oam]	вложенное меню OAM теста
exit top logout start	подняться на уровень выше выйти в корневое меню выйти из CLI режима запустить OAM тест
[show]	вложенное меню
exit top logout	подняться на уровень выше выйти в корневое меню выйти из CLI режима
[fdb]	вложенное меню просмотра FDB
exit top logout unicast ge unicast port	подняться на уровень выше выйти в корневое меню выйти из CLI режим Просмотр таблицы коммутации на ethernet портах Просмотр таблицы коммутации на DSL портах
mcast	Просмотр мультискаст таблицы коммутации
[ethernet]	вложенное меню
exit top logout port	подняться на уровень выше выйти в корневое меню выйти из CLI режима Показать статус ethernet порта
port	Показать статус DSL порта
[stats-counter]	вложенное меню статистики интерфейсов
exit top	подняться на уровень выше выйти в корневое меню

<p>logout dsl atm pvc ge</p>	<p>выйти из CLI режима показать статистику заданных DSL интерфейсов показать статистику заданных ATM интерфейсов показать статистику заданных PVC показать статистику заданных Ethernet интерфейсов</p>
<p>[rstp]</p>	<p>вложенное меню просмотра статистики RSTP</p>
<p>exit top logout ge bridge</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима показать статус RSTP на ethernet портах показать статус RSTP глобально на устройстве</p>
<p>[alarm]</p>	<p>вложенное меню статистики предупреждений</p>
<p>exit top logout log</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима показать лог предупреждений</p>
<p>[active-alarm]</p>	<p>вложенное меню текущих предупреждений</p>
<p>exit top logout port ge system</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима показать предупреждения на DSL портах показать предупреждения на ethernet портах показать текущие системные предупреждения</p>
<p>[pm]</p>	<p>вложенное меню производительности</p>
<p>exit top logout current history-15-min history-1-day</p>	<p>подняться на уровень выше выйти в корневое меню выйти из CLI режима показать статистику производительности в текущий момент времени показать статистику производительности за 15 минутный интервал показать статистику производительности за 1 дневной интервал</p>

11.3. Синтаксис команд упрощенного командного режима.

11.3.1. Аппаратные команды

/hw>show

Описание: Просмотр MAC адресов интерфейсов Uplink

Пример Экранного вывода:

GE-1 MAC Address: 00:bb:cc:dd:ee:f1

GE-2 MAC Address: 00:bb:cc:dd:ee:f2

/hw>set

Описание: сменить MAC адрес на Uplink интерфейсе

Синтаксис команды: set mac1 <mac> mac2 <mac>

Где,

[mac1] MAC адрес eth-1

[mac2] MAC адрес eth-2

Пример: set mac1 00:19:DF:ED:8F:3C

11.3.2. Общие команды управления устройством.

11.3.2.1. Общие команды.

/reboot

Описание: Программная перезагрузка устройства

Синтаксис команды: `reboot [config <config-type>]`

Где,

[config] (default | last) конфигурационный файл, с которым перезагружается устройство (последний или заводской)

Примеры:

reboot

reboot config default

/config>save

Описание: Сохранение текущих настроек устройства в энергонезависимой памяти

/date-time>show

Описание: Показывает текущее время и часовой пояс на устройстве

Экранный вывод:

System Date: 2008-01-01

System Time: 05:01:31

System Timezone: GMT+300

/date-time>set

Описание: Настроить текущее время и часовой пояс на устройстве

Синтаксис команды `set date <date> time <time> timezone <timezone>`

Где:

[date] Дата на устройстве, формат YYYY-MM-DD

[time] Время на устройстве, формат времени: HH:MM:SS

[timezone] Часовой пояс: (GMT-1200 | GMT-1100 | GMT-1000 | GMT-900 | GMT-800

GMT-700 | GMT-600 | GMT-500 | GMT-400 | GMT-330 |
GMT-300 | GMT-200 | GMT-100 | GMT+000 | GMT+100 |
GMT+200 | GMT+300 | GMT+400 | GMT+500 | GMT+530 |
GMT+600 | GMT+630 | GMT+700 | GMT+730 | GMT+800 |
GMT+900 | GMT+930 | GMT+1000 | GMT+1200)

11.3.2.2 Команды управления пользователями.

/config/mgmt/user>show

Описание: Просмотр таблицы пользователей

Экранный вывод:

User Name	Privilege
Admin	admin

/config/mgmt/user>add

Описание: Добавление пользователя

Синтаксис команд: add username <user-name> password <password> privilege <user|admin>

Где:

username	Имя пользователя (максимум 62 символа)
password	Пароль пользователя (максимум 62 символа)
privilege	Уровень привелегий

11.3.2.3 Команды управления SNMP.

/config/mgmt/snmp/community>show

Описание: Просмотр SNMP Community string

Экранный вывод:

Community Name	Access
public	r/w

/config/mgmt/snmp/community>add

Описание: Добавление community string

Синтаксис команд: add community <name> <ro|rw>

Где:

<name>: Имя community string (максимум 62 символа)
<auth>: (ro | rw) права community (ro- только на чтение, rw- чтение и запись)

Пример: add community public rw

/config/mgmt/snmp/community>del

Описание: Удаление community string

Пример: del community public

/config/mgmt/snmp/host>show

Описание: Просмотр списков доверенных хостов SNMP

Экранный вывод:

Host Address	Community Name
192.168.7.121	public

/config/mgmt/snmp/host>add

Описание: Добавление доверенного хоста SNMP

Синтаксис команд: add ip <ip> community <community>

Где:

ip	IP адрес хоста
community	Имя community string

Пример:

add ip 192.168.7.121 community public

/config/mgmt/snmp/traphost>show

Описание: Просмотр списков хостов получателей предупреждений (SNMP Traps)

Экранный вывод:

```
Trap Host      Port Version Community
-----
192.168.7.121  162  v2c   public
```

/config/mgmt/snmp/traphost>add

Описание: Добавление хоста получателя SNMP Traps

Синтаксис команд: add ip <ip> community <community> [version <version>] [port <port>]

Где:

ip IP адрес хоста
community Имя community string
[port] порт назначения (диапазон значений 1~65535, значение по умолчанию 162)
[version] (v1 | v2c), версия протокола snmp, по умолчанию v2c

Пример:

add ip 192.168.7.121 community public version v2c port 155

/config/mgmt/snmp/traphost>del

Описание: Удаление хоста получателя SNMP Traps

Пример:

del ip 192.168.7.121 port 155

11.3.2.4. Команды управления Management Vlan

/config/mgmt/vlan-id>show

Описание: Просмотр параметров Management Vlan

Экранный вывод:

```
Interface: Ge1
Management VLAN ID: 0
Management Priority: 0
```

```
Interface: Ge2
Management VLAN ID: 0
Management Priority: 0
```

/config/mgmt/vlan-id>set

Описание: Изменение параметров Management Vlan

Синтаксис команд: set <eth-port ge1 | ge2> vlanid <vlanid> [priority <priority>]

Где

<eth-port> ethernet port(ge1 | ge2),
vlanid Management vlan id (или cvlanid в Q-in-Q), диапазон: 0~4095, 0 –нет
vlanid
[priority] 802.1q приоритет кадров, диапазон: 0~7

11.3.2.5. Команды управления маршрутами

/config/mgmt/default-route>show

Описание: Просмотр маршрута по умолчанию

Экранный вывод:

Default route: 192.168.7.1

/config/mgmt/default-route>set

Описание: Задать маршрут по умолчанию

Синтаксис команд: set ip <ip>

Где:

ip IP адрес маршрутизатора по умолчанию

Пример: set ip 192.168.7.1

/config/route>add

Описание: Задать маршрут в определенный VLAN

Синтаксис команд: add vlanid <vlanid> gateway-ip <ip>

Где:

vlanid VID VLAN, в который задается маршрут

gateway-ip IP адрес шлюза

11.3.2.6. Автоматическая синхронизация времени устройства по протоколу SNTP

/config/sntp>enable

Описание: Включить SNTP на устройстве

/config/sntp>disable

Описание: Выключить SNTP на устройстве

/config/sntp>add

Описание: Добавить адрес SNTP сервера

Синтаксис команд: add server-ip <ip>

Где:

server-ip IP адрес SNTP сервера

/config/sntp>show

Описание: Просмотр списка SNTP серверов

11.3.2.7. Команды управления портами

/config/port>disable

Описание: Административно выключить определенный порт (порты) устройства

Синтаксис команд: enable <port-range>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример: disable 1-4

/config/port>enable

Описание: Административно включить определенный порт (порты) устройства

Синтаксис команд: enable <port-range>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример: enable 1-4

11.3.3. Команды работы с Uplink портами

/config/ge>show

Описание: Показать конфигурацию ethernet портов

Экраниый вывод:

```
Interface:    ge1
IP Type:      IP
IP Address:   192.168.7.128
Mask Address: 255.255.255.0
Interface Type: uplink
Mgmt VLAN ID: 0
Priority:     0
ORL:         300
Port Speed:  auto
MAC Limit:   256
Admin State: enable
```

```
Interface:    ge2
IP Type:      No IP
IP Address:   0.0.0.0
Mask Address: 0.0.0.0
Interface Type: downlink
Mgmt VLAN ID: 0
Priority:     0
ORL:         300
Port Speed:  auto
MAC Limit:   256
Admin State: enable
```

/config/ge>add

Описание: Добавить ethernet порт

Синтаксис команд: add <ge1 | ge2> ip <ip> mask <mask> type < uplink | downlink > iptype <dhcp|noip|ip>

Где:

<eth-port>	Ethernet порт (ge1 ge2)
[iptype]	Тип получения IP адреса интерфейсом (dhcp noip ip)
[type]	Тип интерфейса uplink или downlink. По умолчанию, порт ge1-uplink, ge2-downlink
[ip]	IP адрес интерфейса
[mask]	Маска подсети интерфейса

/config/ge>set

Описание: Изменить настройки ethernet порта

Синтаксис команд: set <ge1 | ge2 > [maclimit <limit>][iptype <dhcp|noip|ip>][ip <ip>] [mask <mask>] [orl <orl>][portspeed < auto | 100bt | 1000bt >]

Где:

<eth-port>	Ethernet порт (ge1 ge2)
[iptype]	Тип получения IP адреса интерфейсом (dhcp noip ip)
[ip]	IP адрес интерфейса
[mask]	Маска подсети интерфейса
[maclimit]	Количество MAC- адресов на интерфейсе, диапазон значений: 1~2048
[orl]	Значение Output rate limiting (ORL,Mbps), диапазон значений: 0~300
[portSpeed]	Скорость порта (auto 100bt 1000bt)

/config/ge> del

Описание: Удалить ethernet интерфейс

Синтаксис команд: del <eth-port>

Где:

<eth-port> Ethernet порт (ge1 | ge2)

/show/ethernet>port

Описание: Просмотр статус ethernet интерфейсов

Синтаксис команд: port < ge1 | ge2>

Экранный вывод:

```
Interface:          GE-1
Admin Status:      Enable
Oper Status:       Enable
Current Speed:     100BT
Current Duplex Mode: Full
```

```
Interface:          GE-2
Admin Status:      Enable
Oper Status:       Disable
Current Speed:     AnegInProgress
Current Duplex Mode: Not connected
```

11.3.4. Команды управления глобальными профилями DSL

`/config/profile>show`

Описание: Просмотр списка и параметров глобальных DSL профилей

Экранный вывод: (профили, созданные в системе по умолчанию):

Profile name:	adsl2
Standard type:	adsl2
AnnexM:	off
Rate mode:	ra
Line type:	interleaved
Downstream target SNR (db/10):	60
Downstream minimum SNR (db/10):	0
Downstream maximum SNR (db/10):	310
Downstream minimum rate (Kbps):	64
Downstream maximum rate (Kbps):	28000
Downstream interleave delay (ms):	16
Upstream target SNR (db/10):	60
Upstream minimum SNR (db/10):	0
Upstream maximum SNR (db/10):	310
Upstream minimum rate (Kbps):	64
Upstream maximum rate (Kbps):	1088
Upstream interleave delay (ms):	16
PM mode:	L2L3
L2 entry rate (Kbps):	256
L2 entry time (sec):	1800
L2 minimum rate (Kbps):	1024
L2 exit rate (Kbps):	512
Profile name:	default
Standard type:	adsl2plus
Annex:	off
Rate mode:	ra
Line type:	interleaved
Downstream target SNR (db/10):	60
Downstream minimum SNR (db/10):	0
Downstream maximum SNR (db/10):	310
Downstream minimum rate (Kbps):	64
Downstream maximum rate (Kbps):	28000
Downstream interleave delay (ms):	16
Upstream target SNR (db/10):	60
Upstream minimum SNR (db/10):	0
Upstream maximum SNR (db/10):	310
Upstream minimum rate (Kbps):	64
Upstream maximum rate (Kbps):	1088
Upstream interleave delay (ms):	16

PM mode:	L2L3
L2 entry rate (Kbps):	256
L2 entry time (sec):	1800
L2 minimum rate (Kbps):	1024
L2 exit rate (Kbps):	512

/config/profile>add

Описание: Добавить глобальный DSL профиль

Синтаксис команд: add name <profile-name> stdtype < adsl | adsl2 | adsl2plus | all > [annexM <on | off>] [mode < fix | ra | dynamic>][dsminrate <dsminrate>][dsmaxrate <dsmaxrate>] [usminrate <upminrate>][usmaxrate <usmaxrate>] [pmmode < disable | l2 | l3 | l2l3>] [dstgtsnr <dstgtsnr>][ustgtsnr <ustgtsnr>][dsminsnr <dsminsnr>][dsmaxsnr <dsmaxsnr>] [usminsnr <usminsnr>][usmaxsnr <usmaxsnr>][dsdelay <dsdelay>][usdelay <usdelay>] [l2entryrate <l2entryrate>][l2entrytime <l2entrytime>][l2exitrate <l2exitrate>][l2minrate <l2minrate>]

Где:

Profile-name	Имя профиля
[stdtype]	Выбор набора модуляций. По умолчанию adsl2plus.
[annexM]	(on off) включение/выключение annexM. По умолчанию выключено.
[mode]	Режим адаптации скорости (fix ra dynamic). По умолчанию ra
[type]	Тип линии (fast interleaved). По умолчанию interleaved.
[dstgtsnr]	Целевое значение downstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 60.
[dsminsnr]	Минимальное значение downstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 0.
[dsmaxsnr]	Максимальное значение downstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 310.
[dsminrate]	Минимальная скорость downstream, диапазон: 64~28000(Kbps). Значение по умолчанию 64.
[dsmaxrate]	Максимальная скорость downstream, диапазон: 64~28000(Kbps). Значение по умолчанию 28000.
[dsdelay]	Downstream interleave delay, диапазон: 1~64(ms). Для ADSL значения: 1, 2, 4, 8, 16, 32, 64. Для ADSL2/2+, диапазон: 1~63. Значение по умолчанию 16
[ustgtsnr]	Целевое значение upstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 60
[usminsnr]	Минимальное значение upstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 0.
[usmaxsnr]	Максимальное значение upstream SNR, диапазон: 0~310(db/10). Значение по умолчанию is 310.
[usminrate]	Минимальная скорость upstream, диапазон: 64~28000(Kbps). Значение по умолчанию 64.
[usmaxrate]	Максимальная скорость downstream, диапазон: 64~28000(Kbps). Значение по умолчанию 1088.
[usdelay]	Upstream interleave delay, диапазон: 1~16(ms). Значение по умолчанию 16.
[pmmode]	Режим управления мощностью (disable l2 l3 l2l3) .Значение по умолчанию l2l3.
[l2entryrate]	Скорость необходима для вхождения в l2 режим, диапазон: 0~1024(Kbps). Значение по умолчанию 256.

[l2entrytime] Время нахождения в режиме l2, диапазон: 900~65535 (сек). Значение по умолчанию 1800.

[l2exitrate] Скорость выхода из режима l2, диапазон: 32~1024(Kbps) .Значение по умолчанию 512.

[l2minrate] Минимальная скорость для режима l2, диапазон: 32~1024(Kbps).Значение по умолчанию 1024.

Пример: add name dl stdtype adsl2plus annexM on type interleaved mode ra dsminrate 200 dsmaxrate 2000 usminrate 1000 usmaxrate 1000

/config/profile>set

Описание: Изменить параметры существующего DSL профиля

Синтаксис команд: set name <profile-name> stdtype < adsl | adsl2 | adsl2plus | all > [annexM <on | off>] [mode < fix | ra | dynamic>][dsminrate <dsminrate>][dsmaxrate <dsmaxrate>] [usminrate <upminrate>][usmaxrate <usmaxrate>] [pmmode < disable | l2 | l3 | l2l3>] [dstgtsnr <dstgtsnr>][ustgtsnr <ustgtsnr>][dsminsnr <dsminsnr>][dsmaxsnr <dsmaxsnr>] [usminsnr <usminsnr>][usmaxsnr <usmaxsnr>][dsdelay <dsdelay>][usdelay <usdelay>] [l2entryrate <l2entryrate>][l2entrytime <l2entrytime>][l2exitrate <l2exitrate>][l2minrate <l2minrate>]

/config/profile>del

Описание: Удалить глобальный DSL профиль

del name <profile-name>

Где:

name Имя профиля

Пример: del name dl

/config/port>show

Описание: Показать “привязку” DSL профилей к портам устройства

Синтаксис команд: show <port-range>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример: show 1

Port	Admin Status	DSL Profile Name
1	Enable	default

/config/port>set dsl-profile

Описание: Установить “привязку” DSL профилей к портам устройства

Синтаксис команд: set dsl-profile name <profile-name> <port-range>

Где:

<profile-name>: Имя DSL профиля

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример:

set dsl-profile name default 4

/config/port>clean dsl-profile

Описание: Очистить “привязку” DSL профилей к определенным портам устройства

Синтаксис команд: clean dsl-profile <port-range>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример:

clean dsl-profile 4

/config/force-pm>port

Описание: Принудительная установка power management mode на DSL портах.

Синтаксис команд: port <port-range> <l3to10 | l0to12 | l3 | l2to10>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

<pm-mode> режим power management

11.3.5. Команды управления PVC

/config/pvc>show

Описание: Показать список PVC указанных портов и их параметров

Синтаксис команд: show <port-range>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

Пример: show 1

Port	VPI	VCI	Type	VID	Pri	Tag	Other
1	8	35	eoA	1	0	on	MAC limit: 16, Mux: llc
1	8	36	eoA	1	0	off	MAC limit: 16, Mux: llc

/config/pvc>add eoA

Описание: Добавить PVC или группу PVC и создать стек с вышележащим интерфейсом ЕоА типа. (Эта команда создает AAL5 (PVC) интерфейсы с нужными параметрами, поверх них ЕоА интерфейс, поверх ЕоА- bridge интерфейсы. При необходимости создает VLAN с указанным VID и прикрепляет к нему интерфейсы).

Синтаксис команд: add eoA <port-range> <vpi> <vci> vlanid <vlanid> priority <priority> vlantag <on/off> mux <vc/llc> maclimit <limit>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

<vci> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

[vlanid] vlan id (или cvlanid в режиме Q-in-Q), членом которого является создаваемый PVC. Диапазон: 1~4095, значение по умолчанию 1.

[priority] приоритет, диапазон: 0~7, значение по умолчанию 0

[vlantag] показывает тегированным или нетегированным членом VLAN является данный PVC. Значение по умолчанию off.

[mux] тип мультиплексирования. Значение по умолчанию llc.

[maclimit] лимит количества MAC адресов на PVC. Диапазон: 1~16, значение по умолчанию 16.

Пример: add eoA 4-10 8 36 vlanid 2 priority 7 vlantag off mux llc maclimit 10

/config/pvc>add ipoa

Описание: Добавить PVC или группу PVC и создать стек интерфейсов с интерфейсом ipoa типа

Синтаксис команд: add ipoa <port-range> <vpi> <vci> vlandid <vlandid> priority <priority>
ip <ip> mac <mac>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<vci> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
[vlandid] vlan id (или cvlandid в режиме Q-in-Q), членом которого является создаваемый PVC. Диапазон: 1~4095, значение по умолчанию 1.
[priority] приоритет, диапазон: 0~7, значение по умолчанию 0.
[vlantag] показывает тегированным или нетегированным членом VLAN является данный PVC. Значение по умолчанию off.
ip IP адрес
mac MAC адрес

/config/pvc>add pppoa

Описание: Добавить pvc и создать стек интерфейсов с интерфейсом pppoa типа

Синтаксис команд: add pppoa <port-range> <vpi> <vci> vlandid <vlandid> priority <priority>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
[vlandid] vlan id (или cvlandid в режиме Q-in-Q), членом которого является создаваемый PVC. Диапазон: 1~4095, значение по умолчанию 1.
[priority] приоритет, диапазон: 0~7, значение по умолчанию 0
[vlantag] показывает тегированным или нетегированным членом VLAN является данный PVC. Значение по умолчанию off.

/config/pvc>del

Описание: Удалить PVC или группу PVC

Синтаксис команд: del <port-range> <vpi> <vci>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

/config/pvc>mac-limit

Описание: Установить лимит количества MAC адресов на заданных PVC

Синтаксис команд: mac-limit <port-range> <vpi> <vci> maclimit <maclimit>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

<vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

maclimit лимит количества MAC адресов на данном PVC. Диапазон: 1~16, значение по умолчанию 16.

/config/pvc/pppoa-conf>show

Описание: установить PPPoA MAC адреса

Экранный вывод:

PPPoA PVC's MAC address: 00:00:00:00:00:01

/config/pvc/pppoa-conf>set

Описание: установить PPPoA PVC MAC адрес

Синтаксис команд: set mac <macaddr>

Где:

mac MAC адрес

11.3.6. Команды управления VLAN

/config/vlan/mode> show

Описание: Показать текущий режим VLAN на устройстве (802.1q или Q-in-Q)

Экранный вывод:

VLAN Mode: single

/config/vlan/mode> set

Описание: установить текущий режим VLAN на устройстве (802.1q или Q-in-Q)

Синтаксис команд: set single | double

Где:

<vlanmode> single-802.1q режим, double Q-in-Q режим.

Внимание: после введения этой команды DSLAM будет принудительно перезагружен.

/config/vlan/ge>add

Описание: Добавить ethernet порт членом заданного VLAN

Синтаксис команд: add <ge1 | ge2> vlanid <vlanid> tag <on | off>

Где:

<eth-port> ethernet порт

vlanid значение vlan id или cvlanid (для Q-in-Q), диапазон: 1~4095.

[tag] определяет тегированным или не тегированным членом виллана является порт. По умолчанию значение **on** (тегированный).

/config/vlan/ge>del

Описание: удалить ethernet порт из определенного VLAN

Синтаксис команд: del <ge1 | ge2> vlanid <vlanid>

Где:

<eth-port> ethernet порт

vlanid значение vlan id или cvlanid (для Q-in-Q), диапазон: 1~4095.

/config/vlan/ge>show

Описание: показать статус ethernet портов в VLAN

Экранный вывод:

Ethernet port VLAN ID Tag

ge1 1 on

ge1 2 on

ge1 3 on

/config/vlan/ge>set

Описание: Изменить статус членства порта ethernet в определенном VLAN.

В режиме Q-in-Q изменяется статус cvlan tag.

Синтаксис команд: set <ge1 | ge2> vlanid <vlanid> tag <on | off>

Где:

<eth-port> ethernet порт

vlanid значение vlan id или cvlanid (для Q-in-Q), диапазон: 1~4095.

tag определяет тегированным или не тегированным членом виллана является порт.

/config/vlan/default-vid/ge>show

Описание: Показать PVID VLAN ethernet порту

Экраниый вывод:

GE-1
VLAN ID: 1
Frame type: all
Ingress filter: off

GE-2
VLAN ID: 1
Frame type: all
Ingress filter: off

/config/vlan/default-vid/ge>set

Описание: установить PVID VLAN ethernet порту

Синтаксис команд: set < ge1 | ge2t> accept < all | tag-only > ingress-filter < on | off > vlanid <vlanid>

Где:

<eth-port> ethernet порт
[accept] принимать все кадры (all) или только тегированные (tag-only)
[ingress-filter] включает и выключает входной фильтр
[vlanid] значение vlan id или cvlanid (для Q-in-Q), диапазон: 1~4095.

/config/vlan/ge>stag

Описание: изменяет статус порта в SVLAN

Синтаксис команд:stag < ge1 | ge2> <on | off>

Где:

<eth-port> ethernet порт
<on-off> определяет тегированным или не тегированным членом SVLAN является порт.

Описание: Показать PVC PVID и сопутствующие параметры

Экраниый вывод: /config/vlan/default-vid/pvc>show 1

Port	VPI	VCI	Def VID	Frame Type	Ingress Filter
1	8	35	1	all	off
1	8	36	1	all	off

/config/vlan/default-vid/pvc>set

Описание: установить сопутствующие параметры VLAN для PVC

Синтаксис команд:set <port-range> <vpi> <vci> accept < all | tag-only > ingress-filter < on | off >

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

- <vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
- <vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
- [accept] принимать все кадры (all) или только тегированные (tag-only)
- [ingress-filter] включает и выключает входной фильтр

11.3.7. Диагностические команды

/diag/delt/start

Описание: Запустить DELT тест на определенных портах

Пример: start 1

```
Operate State:          delt
Downstream attainable rate (bps): 21584000
Upstream attainable rate (bps): 1088000
```

/diag/atm-oam/start

Описание: запустить OAM тест на определенных портах

Синтаксис команд: start <port> <vpi> <vci>

Где:

- <port> номер DSL порта
- <vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
- <vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

11.3.8. Команды просмотра и управления таблицей коммутации

/config/bridge>set

Описание: задать параметры таблицы коммутации

Синтаксис команд: set dslage <dslage> uplinkage <uplinkage> flood < enable | disable>
broadcast < enable | disable> mode restricted | unrestricted | residential

Где:

[dslage] время жизни пакетов на портах DSL (sec), диапазон: 10~1000000
[uplinkage] время жизни пакетов Uplink (sec), диапазон: 10~1000000
[downlinkage] время жизни пакетов Downlink (sec), диапазон: 10~1000000
[mode] режим коммутации на устройстве (эта настройка будет набрана после сохранения конфигурации перезагрузки устройства).
[flood] включить или выключить защиту от флуда
[broadcast] включить или выключить пропуск широковещательных пакетов
[multicast] включить или выключить пропуск мультикаст пакетов
[multicastdrop] включить или выключить отбрасывание мультикаст пакетов
[fdbfulldrop] включить или выключить отбрасывание пакетов если таблица коммутации полна

Пример: set mode unrestricted

/show/fdb>mcast

Описание: просмотр Multicast таблицы коммутации

Экранный вывод:

Port	VPI	VCI	VLAN ID	Mac Address	Status
1	8	35	1	00:00:ab:b7:09:af	learned

/show/fdb>unicast ge

Описание: просмотр таблицы коммутации на ethernet портах

Экранный вывод:

Port	VLAN ID	Mac Address	Status
ge1	1	00:00:aa:b7:09:ae	learned
ge1	1	00:01:6c:01:3c:ba	learned
ge1	1	00:05:5d:e0:57:05	learned
ge1	1	00:0c:6e:ea:99:8f	learned
ge1	1	00:11:95:cb:ea:eb	learned
ge1	1	00:13:46:26:7f:32	learned
ge1	1	00:13:d4:9d:d1:d4	learned
ge1	1	00:50:ba:ca:87:6c	learned
ge1	3	00:0f:3d:cb:1f:bb	learned

/show/fdb>unicast port

Описание: просмотр таблицы коммутации на PVC

Пример: unicast port 1

Port	VLAN ID	Mac Address	Status
1	1	00:09:fa:b8:09:ae	learned

11.3.9. Команды работы с MAC ACL

/config/acl>show

Описание: просмотр ACL на отдельных портах устройства

Синтаксис команды: show global|pvc|ge port

Где,

global просмотр глобального MAC ACL

pvc просмотр MAC ACL на отдельном PVC

ge просмотр ACL на ethernet порту устройства

port- номер порта или интерфейса устройства

Пример:

/config/acl>show pvc 1

Port VPI VCI MAC Address

1 8 35 00:19:5C:DF:5B:ED

/config/acl>show ge

Ethernet Port MAC Address

1 00:19:5D:45:EF:6D

/config/acl>add global

Описание: добавление MAC в глобальный ACL

Пример: add global 00:19:5D:45:EF:6D

/config/acl>add pvc

Описание: добавление MAC ACL на отдельные PVC

Синтаксис команды: add pvc <port-range> <vpi> <vci> <mac>

Где,

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

<vpi> параметр VPI .Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0)

<vci> параметр VCI .Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0)

<mac> MAC адрес

/config/acl>add ge

Описание: добавление MAC ACL на Uplink порты

Синтаксис команды: add ge <eth-port> <mac>

Где,

<eth-port> (ge1 | ge2)- Uplink интерфейсы

<mac> MAC адрес

11.3.10. Команды работы с Alarm профилями

/config/alarm/pm-profile>show

Описание: Просмотр Alarm профиля на порту

Пример: show 1

Экранный вывод:

Port 1 Alarm Profile 15 Min

Item	ATUC	ATUR
LOFS	0	0
LOSS	0	0
LOLS	0	N/A
LPRS	0	0
ES	0	0
SES	0	0
UAS	0	0

Port 1 Alarm Profile 1 Day

Item	ATUC	ATUR
LOFS	0	0
LOSS	0	0
LOLS	0	N/A
LPRS	0	0
ES	0	0
SES	0	0
UAS	0	0

/config/alarm/pm-profile>set profile-15min

Описание: изменение 15 минутного Alarm профиля

Синтаксис команды: set profile-15min <port-range> <side> LOFS <LOFS> LOSS <LOSS>
LOLS <LOLS> LPRS <LPRS> ES <ES> SES <SES> UAS <UAS>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<side> ближний конец(ne) или дальний конец (fe) линии
[LOFS] Количество Loss of frame second (LOFS) за интервал. Диапазон:
0~900
[LOSS] Количество Loss of signal second (LOSS) за интервал. Диапазон:
0~900
[LOLS] Количество Loss of link second (LOLS), за интервал.
Диапазон:0~900
(только для ближнего конца линии)
[LPRS] Количество Loss of power second (LPRS), за интервал.Диапазон:
0~900
[ES] Количество Error second (ES), за интервал. Диапазон: 0~900
[SES] Количество Severe error (SES), за интервал. Диапазон: 0~900
[UAS] Количество Unavailable second (UAS), за интервал. Диапазон:
0~900

Пример: set profile-15min 1-3 LOFS 3 LOSS 3

/config/alarm/pm-profile>set profile-1day

Описание: изменение 1 дневного Alarm профиля

Синтаксис команды: set profile-1day <port-range> <side> LOFS <LOFS> LOSS <LOSS>
LOLS <LOLS> LPRS <LPRS> ES <ES> SES <SES> UAS <UAS>

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<side> ближний конец(ne) или дальний конец (fe) линии
[LOFS] Количество Loss of frame second (LOFS) за интервал. Диапазон:
0~86400
[LOSS] Количество Loss of signal second (LOSS) за интервал. Диапазон:
0~86400
[LOLS] Количество Loss of link second (LOLS), за интервал.
Диапазон:0~86400
(только для ближнего конца линии)
[LPRS] Количество Loss of power second (LPRS), за интервал.Диапазон:
0~86400
[ES] Количество Error second (ES), за интервал. Диапазон: 0~86400
[SES] Количество Severe error (SES), за интервал. Диапазон: 0~86400
[UAS] Количество Unavailable second (UAS), за интервал. Диапазон:
0~86400

Пример: set profile-1day 1-3 LOFS 3 LOSS 3

/config/alarm/definition>show

Описание: просмотр статуса предупреждений

Синтаксис команды: show <module-id>

Где

<module-id> выбор модуля предупреждений (adsl | adslpm | ge)

Пример1:

/config/alarm/definition>show adsl

Alarm Name	Filter	Severity	Suppressed
LOS	Off	Minor	None
LOF	Off	Minor	None
LPWR	Off	Warning	None
LOSQ	Off	Minor	None
LOL	Off	Minor	None
DATA_INIT_FAIL	Off	Minor	None
CONFIG_INIT_FAIL	Off	Minor	None
PROTOCOL_INIT_FAIL	Off	Minor	None
NO_PEER_DETECTED	Off	Minor	None
OTHER_FAIL	Off	Minor	None
TRAINING	Off	Info	None
PS_L2	Off	Info	None
PS_L3	Off	Info	None
MAC_SPOOFED	Off	Warning	None
DISABLED	Off	Info	None

Пример2:

/config/alarm/definition>show adslpm

Alarm Name	Filter	Severity	Suppressed
LOFS_NE_15_MIN	Off	Minor	None

LOSS_NE_15_MIN	Off	Minor	None
LOLS_NE_15_MIN	Off	Minor	None
LPRS_NE_15_MIN	Off	Minor	None
ES_NE_15_MIN	Off	Minor	None
SES_NE_15_MIN	Off	Minor	None
UAS_NE_15_MIN	Off	Minor	None
LOFS_FE_15_MIN	Off	Minor	None
LOSS_FE_15_MIN	Off	Minor	None
LPRS_FE_15_MIN	Off	Minor	None
ES_FE_15_MIN	Off	Minor	None
SES_FE_15_MIN	Off	Minor	None
UAS_FE_15_MIN	Off	Minor	None
LOFS_NE_1_DAY	Off	Minor	None
LOSS_NE_1_DAY	Off	Minor	None
LOLS_NE_1_DAY	Off	Minor	None
LPRS_NE_1_DAY	Off	Minor	None
ES_NE_1_DAY	Off	Minor	None
SES_NE_1_DAY	Off	Minor	None
UAS_NE_1_DAY	Off	Minor	None
LOFS_FE_1_DAY	Off	Minor	None
LOSS_FE_1_DAY	Off	Minor	None
LPRS_FE_1_DAY	Off	Minor	None
ES_FE_1_DAY	Off	Minor	None
SES_FE_1_DAY	Off	Minor	None
UAS_FE_1_DAY	Off	Minor	None
DISABLED	Off	Info	None

Пример3:

/config/alarm/definition>show ge

Alarm Name	Filter	Severity	Suppressed
SFP_LOS	Off	Major	None
COPPER_LINKDOWN	Off	Major	None
DISABLED	Off	Info	None

/config/alarm/definition>set

Описание: Задать активный ALARM профиль

Синтаксис команды: show <module-id> <alarm-name> filter <filter> severity <severity>

Где:

<module-id> выбор модуля предупреждений (adsl | adslpm | ge)

<alarm-name> **alarm name of alarm list in modules.**

adsl module:

(LOS | LOF | LPWR | LOSQ | LOL | DATA_INIT_FAIL |
 CONFIG_INIT_FAIL | PROTOCOL_INIT_FAIL |
 NO_PEER_DETECTED | OTHER_FAIL | TRAINING | PS_L2 |
 PS_L3 | MAC_SPOOFED | DISABLED)

adslpm module:

(LOFS_NE_15_MIN | LOSS_NE_15_MIN | LOLS_NE_15_MIN |
 LPRS_NE_15_MIN | ES_NE_15_MIN | SES_NE_15_MIN |
 UAS_NE_15_MIN | LOFS_FE_15_MIN | LOSS_FE_15_MIN |
 LPRS_FE_15_MIN | ES_FE_15_MIN | SES_FE_15_MIN |
 UAS_FE_15_MIN | LOFS_NE_1_DAY | LOSS_NE_1_DAY |

LOLS_NE_1_DAY | LPRS_NE_1_DAY | ES_NE_1_DAY |
SES_NE_1_DAY | UAS_NE_1_DAY | LOFS_FE_1_DAY |
LOSS_FE_1_DAY | LPRS_FE_1_DAY | ES_FE_1_DAY |
SES_FE_1_DAY | UAS_FE_1_DAY | DISABLED)

ge module:

(SFP_LOS | COPPER_LINKDOWN | DISABLED)

- [filter]** включение или выключение фильтра сообщений (on | off)
[severity] выбор уровня предупреждений (critical|major|minor|warning|info|none)
[suppressed] подавление других типов предупреждений
<suppressed> Не включает тип <alarm-name>

adsl module:

(LOS | LOF | LPWR | LOSQ | LOL | DATA_INIT_FAIL |
CONFIG_INIT_FAIL | PROTOCOL_INIT_FAIL |
NO_PEER_DETECTED | OTHER_FAIL | TRAINING | PS_L2 |
PS_L3 | MAC_SPOOFED | DISABLED)+ or none.

adslpm module:

(LOFS_NE_15_MIN | LOSS_NE_15_MIN | LOLS_NE_15_MIN |
LPRS_NE_15_MIN | ES_NE_15_MIN | SES_NE_15_MIN |
UAS_NE_15_MIN | LOFS_FE_15_MIN | LOSS_FE_15_MIN |
LPRS_FE_15_MIN | ES_FE_15_MIN | SES_FE_15_MIN |
UAS_FE_15_MIN | LOFS_NE_1_DAY | LOSS_NE_1_DAY |
LOLS_NE_1_DAY | LPRS_NE_1_DAY | ES_NE_1_DAY |
SES_NE_1_DAY | UAS_NE_1_DAY | LOFS_FE_1_DAY |
LOSS_FE_1_DAY | LPRS_FE_1_DAY | ES_FE_1_DAY |
SES_FE_1_DAY | UAS_FE_1_DAY | DISABLED)+ or none.

ge module:

(SFP_LOS | COPPER_LINKDOWN | DISABLED)+ or none.

/show/alarm>log

Описание: просмотр лога предупреждений

Экранный вывод:

Time	Trap
1970-01-01 00:00:38	SNMP-GEN : [SYSTEM_COLDSTART]
1970-01-01 00:00:38	GE ge1 : [COPPER_LINKDOWN]
1970-01-01 00:00:38	GE ge2 : [COPPER_LINKDOWN]
1970-01-01 00:00:39	ADSL port 01 : [TRAINING]
1970-01-01 00:00:39	ADSL port 02 : [TRAINING]
1970-01-01 00:00:39	ADSL port 03 : [TRAINING]
1970-01-01 00:00:39	ADSL port 04 : [TRAINING]
1970-01-01 00:00:39	ADSL port 05 : [TRAINING]
1970-01-01 00:00:39	ADSL port 06 : [TRAINING]
1970-01-01 00:00:40	ADSL port 07 : [TRAINING]
1970-01-01 00:00:40	ADSL port 08 : [TRAINING]
1970-01-01 00:00:40	ADSL port 09 : [TRAINING]
1970-01-01 00:00:40	ADSL port 10 : [TRAINING]
1970-01-01 00:00:40	ADSL port 11 : [TRAINING]
1970-01-01 00:00:40	ADSL port 12 : [TRAINING]
1970-01-01 00:00:40	ADSL port 13 : [TRAINING]
1970-01-01 00:00:41	ADSL port 14 : [TRAINING]
1970-01-01 00:00:41	ADSL port 15 : [TRAINING]

1970-01-01 00:00:41 ADSL port 16 : [TRAINING]
1970-01-01 00:00:41 ADSL port 17 : [TRAINING]
1970-01-01 00:00:41 ADSL port 18 : [TRAINING]
1970-01-01 00:00:41 ADSL port 19 : [TRAINING]
1970-01-01 00:00:41 ADSL port 20 : [TRAINING]
1970-01-01 00:00:42 ADSL port 21 : [TRAINING]
1970-01-01 00:00:42 ADSL port 22 : [TRAINING]
1970-01-01 00:00:42 ADSL port 23 : [TRAINING]
1970-01-01 00:00:42 ADSL port 24 : [TRAINING]
1970-01-01 00:00:42 GE ge1 : [LINK_UP]

11.3.11. Команды работы с функциями PIA и DRA

/config/relay/suboption>show

Описание: Показать типы параметров DSL ,включаемые в Circuit ID

Relay Agent Sub Option:

CircuitID

RemoteID

EncapsulationType

AccessLoopCharacteristic

/config/relay/suboption>set

Описание: Задать типы параметров DSL ,включаемые в Circuit ID

Синтаксис команды: set type (cid | rid | alc | ale)+ none

Пример:

set type cid+rid

set type none

/config/relay/cidformat>show

Описание: Показать аппаратные характеристики DSLAM , включаемые в Circuit ID

Prefix String: --

ANI Type: auto

ANI value: --

ACI Field List: Anival SlotNo L2Type Port Vpi Vci

Chassis No: --

Rack No: --

Frame No: --

Slot No: 0

Sub Slot No: --

/config/relay/cidformat>set

Описание: Задать аппаратные характеристики DSLAM, включаемые в Circuit ID (аналог IA профиля для инженерного режима)

Синтаксис команды:

set prefix <string> chassisno <number> rackno <number> frameno <number>... [l2type enable |disable]

Где:

[prefix] Текстовый префикс (макс. длина 16 символов)

[anitype] Тип конфигурирования (auto | config | none)

[anistr] **disable** или текстовая переменная значения **anitype** (актуально, если anitype=config)

[chassisno] Номер шасси (не имеет значение для DAS-3xxx)

[rackno] Номер шкафа (не имеет значение для DAS-3xxx)

[frameno] Номер полки (не имеет значение для DAS-3xxx)

[slotno] Номер слота (не имеет значение для DAS-3xxx)

[subslotno] Номер блока (не имеет значение для DAS-3xxx)

[l2type] Флаг включения в Circuit ID технологии доступа (L2 типа)

/config/relay/ge>show

Описание: Показать статус DHCP Relay option 82 на ethernet интерфейсах

Ethernet Port DHCP Relay Status

```
-----  
1      Disable  
2      Disable
```

/config/relay/ge>enable

Описание: Включить DHCP Relay option 82 на ethernet интерфейсах

Синтаксис команды: enable <eth-port>

Где

<eth-port> ge1 | ge2 - ethernet интерфейс устройства

/config/relay/dhcp>show

Описание: Показать статус DHCP Relay option 82

/config/relay/dhcp>enable

Описание: Включить DHCP Relay option 82 глобально на устройстве

Пример: /config/relay/dhcp>enable

ОК

/config/relay/dhcp/pvc>show

Описание: Показать статус DHCP Relay option 82 на отдельных pvc

Пример: show 1

```
-----  
Port VPI VCI Status Option82  
      Remote ID  
      Circuit ID  
-----  
1  8  35  Disable N/A  
      N/A  
      00:bb:cc:dd:ee:f1 atm 0/150:8.35  
1  8  36  Disable N/A  
      N/A  
      00:bb:cc:dd:ee:f1 atm 0/150:8.36
```

/config/relay/dhcp/pvc>set

Описание: Установить параметры DHCP Relay option 82 на отдельных PVC

Синтаксис команды: set <port-range> <vpi> <vci> remoteid <rid-string> opt82 <none | auto-add | always-add>

Где,

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

<vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

[remoteid] текстовое значение Remote ID (максимум 62 символа)

[opt82] режим добавления DHCP option 82 (none | auto-add | always-add)

/config/relay/pppoe>show

Описание: Показать статус PPPoE Intermediary Agent Relay глобально на устройстве

Экранный вывод:

PPPoE Relay Status: Disable

`/config/relay/pppoe/pvc>show`

Описание: Показать статус PPPoE Intermediate Agent Relay на отдельном PVC

Пример: `/config/relay/pppoe/pvc>show 1`

```
-----  
Port VPI VCI  Status Option82  
      Remote ID  
      Circuit ID  
-----  
1   8   35   Disable N/A  
      N/A  
      00:bb:cc:dd:ee:f1 atm 0/150:8.35  
1   8   36   Disable N/A  
      N/A  
      00:bb:cc:dd:ee:f1 atm 0/150:8.36
```

`/config/relay/pppoe/pvc>set`

Описание: Установить параметры PIA на PVC

Синтаксис команды: `set <port-range> <vpi> <vci> remoteid <rid-string> opt82 < none | auto-add | always-add >`

Где:

<code><port-range></code>	список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<code><vpi></code>	параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<code><vci></code>	параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<code>[remoteid]</code>	текстовое значение Remote ID (максимум 62 символа)
<code>[opt82]</code>	режим добавления PPPoE Intermediate Agent (none auto-add always-add)

11.3.12. Команды работы с функцией IGMP Snooping

/config/igmpsnoop>show

Описание: Показать статус IGMP Snooping на устройстве

Экранный вывод:

System igmpsnoop status: Disable

/config/igmpsnoop/ge>show

Описание: Показать статус IGMP Snooping на ethernet интерфейсах

Экранный вывод:

Ge1 Igmpsnoop Status: Disable

Ge1 Leavemode: Normal

Ge1 Querier: Off

Ge2 Igmpsnoop Status: Disable

Ge2 Leavemode: Normal

Ge2 Querier: Off

/config/igmpsnoop/pvc>show

Описание: Показать статус IGMP Snooping на отдельном DSL порту

Пример: show 1

Port VPI VCI Igmpsnoop Status Leave Mode

1 8 35 Disable Normal

1 8 36 Disable Normal

/config/igmpsnoop/ge>set

Описание: установить параметры IGMP Snooping для ethernet интерфейсов

Синтаксис команд: Ex: set < ge1 | ge2> [leavemode < normal | fast | fastnormal >] [querier < on/off>]

Где:

<eth-port> ethernet порт

[leavemode] установить режим удаления абонентов из мультикаст групп

[querier] показывает, является ли ethernet порт querier (igmp опросчиком)

Пример: set ge1 leavemode fast querier off

/config/igmpsnoop/pvc>set

Описание: установить режим удаления абонентов из мультикаст групп для PVC

Синтаксис команд: set <port-range> <vpi> <vci> < normal | fast | fastnormal >

Где:

<port-range> список портов или диапазон портов (1, 2, ... ,24 или 1-24)

<vpi> параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

<vci> параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

leavemode режим удаления абонентов из мультикаст групп

Пример: set 4-10 8 35 leavemode fast

/config/igmpsnoop/mvr/channel>add

Описание: Прикрепить мультикаст VLAN к групповому (групповым) IP адресам.

Синтаксис команд: add vlanid <vlanid> groupip <ip>

Где:

vlanid	значение vlan id (cvlanid в режиме Q-in-Q), диапазон: 1~4095
groupip	групповые IP, диапазон: 224~239.X.X.X

/config/igmpsnoop/mvr/channel>show

Описание: Просмотр каналов зарегистрированных в MVR

Экранный вывод:

/config/igmpsnoop/mvr/mvlan>add pvc

Описание: добавить PVC в члены мультикаст VLAN

Синтаксис команд: add <port-range> <vpi> <vci> vlanid <vlanid>

Где:

<port-range>	список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi>	параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<vci>	параметр VCI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
vlanid	значение vlan id (cvlanid в режиме Q-in-Q), диапазон: 1~4095

/config/igmpsnoop/mvr/mvlan>add ge

Описание: добавить PVC в члены мультикаст VLAN

Синтаксис команд: add < ge1 | ge2> vlanid <vlanid>

Где:

<eth-port>	ethernet порт
vlanid	значение vlan id (cvlanid в режиме Q-in-Q), диапазон: 1~4095

/config/igmpsnoop/mcast-profile>add

Описание: Создать мультикаст профиль

Синтаксис команд: add <profile-name> <startip1> <endip1> <startip4> <endip4>

Где:

<name>	Имя мультикаст профиля (максимум 62 символа)
<startip1>	IP адрес начала 1 диапазона мультикаст адресов
<endip1>	IP адрес конца 1 диапазона мультикаст адресов
<startip2>	IP адрес начала 2 диапазона мультикаст адресов
<endip2>	IP адрес конца 2 диапазона мультикаст адресов
<startip3>	IP адрес начала 3 диапазона мультикаст адресов
<endip3>	IP адрес конца 1 диапазона мультикаст адресов
<startip4>	IP адрес начала 4 диапазона мультикаст адресов
<endip4>	IP адрес конца 1 диапазона мультикаст адресов

Пример: add DL 239.0.0.1 239.0.0.9 239.0.1.15 239.0.1.17

/config/igmpsnoop/mcast-profile>set

Описание: Изменить параметры уже существующего мультикаст профиля

Синтаксис команд: set <profile-name> <startip1> <endip1> <startip4> <endip4>

Где:

<name>	Имя мультикаст профиля (максимум 62 символа)
<startip1>	IP адрес начала 1 диапазона мультикаст адресов
<endip1>	IP адрес конца 1 диапазона мультикаст адресов
<startip2>	IP адрес начала 2 диапазона мультикаст адресов
<endip2>	IP адрес конца 2 диапазона мультикаст адресов
<startip3>	IP адрес начала 3 диапазона мультикаст адресов
<endip3>	IP адрес конца 1 диапазона мультикаст адресов
<startip4>	IP адрес начала 4 диапазона мультикаст адресов
<endip4>	IP адрес конца 1 диапазона мультикаст адресов

/config/igmpsnoop/mcast-profile/pvc>set

Описание: Прикрепить мультикаст профиль к PVC.

Ex: set <profile-name> <port-range> <vpi> <vci>

Где:

<name>	имя мультикаст профиля (максимум 62 символа)
<port-range>	список портов или диапазон портов (1, 2, ... ,24 или 1-24)
<vpi>	параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).
<vci>	параметр VPI. Допустимые значения 0~255 (vpi and vci одновременно не могут иметь значение 0).

/config/igmpsnoop/mcast-profile/pvc>show

Описание: Просмотреть список мультикаст профилей на отдельном порту

Пример: show 1

Port	VPI	VCI	Multicast Profile Name
1	8	35	None
1	8	36	None

11.3.13. Команды работы с RSTP протоколом

/config/rstp>show

Описание: Просмотреть статус RSTP на устройстве

```
RSTP Status: Disable
STP Version: RSTP
Bridge Priority: 32768
Bridge Max Age Time(sec): 20
Bridge Hello Time(sec): 2
Bridge Forward Delay Time(sec): 15
Bridge ID: 80:00:00:bb:cc:dd:ee:f1
```

/config/rstp>enable

Описание: Включить RSTP на устройстве

/config/rstp>disable

Описание: Выключить RSTP на устройстве

/config/rstp>set

Описание: Установить параметры RSTP на устройстве

Синтаксис команд: set [stpversion < stpCompatible | rstp>][priority <priority>][maxage<age>][htime <hello-time>][fwdelay <d-time>]

Где:

[stpversion]	версия протокола STP (RSTP или STP)
[priority]	приоритет устройства в RSTP , диапазон: 0~61440с шагом of 4096
[maxage]	максимальное время жизни, диапазон: 6~40(sec)
[htime]	время hello time, диапазон: 1~10(sec)
[fwdelay]	задержка продвижения пакетов, диапазон: 4~30(sec)

/config/rstp/ge>show

Описание: просмотр параметров RSTP на ethernet портах

Экранный вывод:

```
Interface:      ge1
Priority:       128
Port State:    learning
Port RSTP Status:  enable
Port Path Cost:  20000
Port Edge:     false
Designated Bridge: 80:00:00:bb:cc:dd:ee:f1
Designated Root:  80:00:00:bb:cc:dd:ee:f1
Designated Cost:  0
Designated Port ID: 0x8001
RSTP Port ID:   0x8001

Interface:      ge2
Priority:       128
Port State:    disable
Port RSTP Status:  enable
Port Path Cost:  20000
Port Edge:     false
Designated Bridge: 00:00:00:00:00:00:00:00
```

Designated Root: 00:00:00:00:00:00:00:00
Designated Cost: 0
Designated Port ID: 0x8002
RSTP Port ID: 0x800

/config/rstp/ge>set

Описание:

Set ethernet port rstp configuration.

Ex: set < ge1 | ge2> priority <priority> pcost <cost> pedge < true | false >

Где:

<eth-port> ethernet порт
[priority] приоритет порта, диапазон: 0~240 с шагом of 16
[pcost] стоимости пути, диапазон 1~200000000
[pedge] показывает, является ли порт окончательным (edge) или нет

/show/rstp>bridge

Описание: просмотр статистики RSTP на устройстве

Экранный вывод:

RSTP Status: Enabled
STP Version: RSTP
Bridge Priority: 32768
Bridge Max Age(sec): 20
Bridge Hello Time(sec): 2
Bridge Forward Delay(sec): 15
Bridge Id: 80:00:00:bb:cc:dd:ee:f1
Designated Root: 80:00:00:bb:cc:dd:ee:f1
Root Port: 0
STP Max Age(sec): 20
STP Hello Time(sec): 2
STP Hold Time(sec): 3
STP Forward Delay(sec): 15
Topology Chaned Time: 0 day(s) 0 hr. 46 min. 3 sec.

/show/rstp>ge

Описание: просмотр статистики RSTP на ethernet портах

Экранный вывод:

Ifname: ge1
Port Priority: 128
Port Id: 0x8001
Port Status: Enabled
Port State: forwarding
Port Path Cost: 20000
Port Edge: 0
Designated Bridge: 80:00:00:bb:cc:dd:ee:f1
Designated Root: 80:00:00:bb:cc:dd:ee:f1
Designated Cost: 0
Designated Port Id: 0x8001

Ifname: ge2
Port Priority: 128
Port Id: 0x8002
Port Status: Enabled

Port State:	disable
Port Path Cost:	20000
Port Edge:	0
Designated Bridge:	00:00:00:00:00:00:00:00
Designated Root:	00:00:00:00:00:00:00:00
Designated Cost:	0
Designated Port Id:	0x8002

11.3.14. Команды просмотра статуса и статистики

/show>port

Описание: Просмотр статуса DSL портов

Пример: /show>port 1

```
DSL Operation State:  Data
DSL Current Status:  noDefect
DSL Channel:         Interleaved
DSL Standard:        DMT_ADSL2PLUS
DSL PM state:        L0 state
Item                 ATUC    ATUR
-----
Attainable rate (bps) 26292000 1143200
Attenuation (1/10 db) 0         35
Current SNR (1/10 db) 70        63
Output Power (1/10 dam) 153       6
Rate (bps)           23908700 1073000
Interleaved Delay (ms) 0         13
Block Length (byte)  48195    2635
```

/show/stats-counter/dsl

Описание: Просмотр статистики DSL уровня на заданном порту

Пример: /show/stats-counter/dsl 1

```
Item                 ATUC    ATUR
-----
Attainable Rate(bps) 0        0
Interleaved Delay (ms) 0        0
Block Length (byte)  0
Elapsed Time (sec)   18327   N/A
Receive block       0
Transmit block      0
Corrected block     0
Uncorrected block   0
NCD count           0
OCD count           0        N/A
HEC count           0        0
```

/show/stats-counter/atm

Описание: Просмотр статистики АТМ уровня на заданном порту

Пример: /show/stats-counter>atm 1

```
Transmit Cell: 0
Receive Cell:  0
Idle Cell:     0
Delineated Cell: 0
User Cell:
```

/show/stats-counter/pvc

Описание: Просмотр статистики ААL5 (PVC) уровня на заданном порту

Пример: /show/stats-counter/pvc 1

PVC	InPkts	OutPkts	DiscPkts
8/35	0	0	0
8/36	0	0	0

/show/stats-counter>ge 1

Описание: Просмотр статистики на заданном ethernet порту

Пример: /show/stats-counter/ge1

Ifname: ge1
Mac Address: 00:bb:cc:dd:ee:f1
Unknown Protocol: 0
In Octet: 1120041
In Discard: 0
In Error: 0
In Unicast: 107
In Multicast: 3528
In Broadcast: 1015
Out Octet: 93620
Out Discard: 0
Out Error: 0
Out Unicast: 29
Out Multicast: 1373
Out Broadcast: 1

11.3.15. Управление удаленным DSLAM

/config/remote-dslam>enable

Описание: включение управления удаленным DSLAM

config/remote-dslam>disable

Описание: выключение управления удаленным DSLAM

/config/remote-dslam>show

Описание: просмотр статуса управления удаленным DSLAM на устройстве

Remote DSLAM Status: Disable
Remote DSLAM Entries: No entry found

config/remote-dslam>add

Описание: добавить ip адрес удаленного DSLAM

Синтаксис команд: add ip <ip> udp <udp>

Где:

ip IP адрес
udp UDP порт, диапазон: 6001~6010

/config/remote-dslam>del

Описание: удалить ip адрес удаленного DSLAM

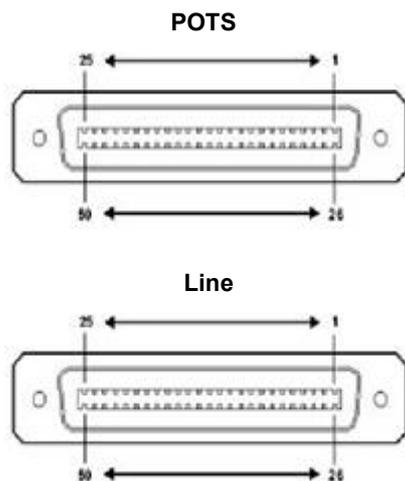
Синтаксис команд: del udp <udp>

Где:

udp UDP порт диапазон, range: 6001~6010

Приложение А: Соответствие контактов коннекторов TELCO-50 Amphenol портам DAS-3216/3224/3248

Схема коммутации портов DAS-3216 rev.B на разъемы TELCO-50 (Amphenol). На рисунке ниже представлено схематическое расположение разъемов на задней панели DAS-3216 rev.B

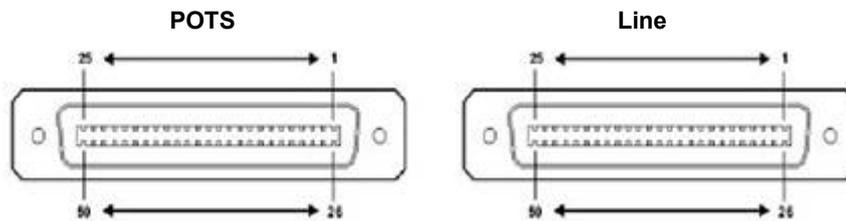


Разъем Line

- 1 порт- контакты 1,26
- 2 порт- контакты 2,27
- 3 порт- контакты 3,28
- 4 порт- контакты 4,29
- 5 порт- контакты 5,30
- 6 порт- контакты 6,31
- 7 порт- контакты 7,32
- 8 порт- контакты 8,33
- 9 порт- контакты 9,34
- 10 порт- контакты 10,35
- 11 порт- контакты 11,36
- 12 порт- контакты 12,37
- 13 порт- контакты 13,38
- 14 порт- контакты 14,39
- 15 порт- контакты 15,40
- 16 порт- контакты 16,41

Остальные контакты – не задействованы на всех разъемах.

Схема коммутации портов DAS-3224 rev.B на разъемы TELCO-50 (Amphenol). На рисунке ниже представлено схематическое расположение разъемов на задней панели DAS-3224 rev.B

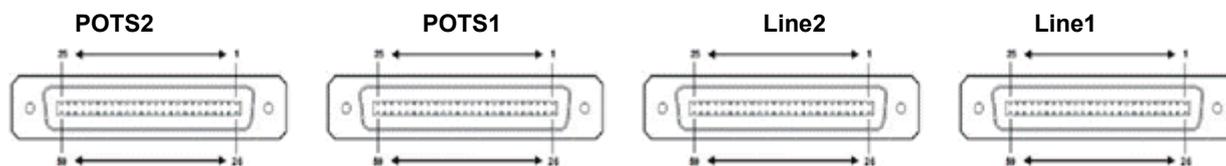


Разъем Line

- 1 порт- контакты 1,26
- 2 порт- контакты 2,27
- 3 порт- контакты 3,28
- 4 порт- контакты 4,29
- 5 порт- контакты 5,30
- 6 порт- контакты 6,31
- 7 порт- контакты 7,32
- 8 порт- контакты 8,33
- 9 порт- контакты 9,34
- 10 порт- контакты 10,35
- 11 порт- контакты 11,36
- 12 порт- контакты 12,37
- 13 порт- контакты 13,38
- 14 порт- контакты 14,39
- 15 порт- контакты 15,40
- 16 порт- контакты 16,41
- 17 порт- контакты 17,42
- 18 порт- контакты 18,43
- 19 порт- контакты 19,44
- 20 порт- контакты 20,45
- 21 порт- контакты 21,46
- 22 порт- контакты 22,47
- 23 порт- контакты 23,48
- 24 порт- контакты 24,49

контакты 25,50 –не задействованы на всех разъемах.

Схема коммутации портов DAS-3248 rev.B на разъемы TELCO-50 (Amphenol). На рисунке ниже представлено схематическое расположение разъемов на задней панели DAS-3248 rev.B



Разъем Line2

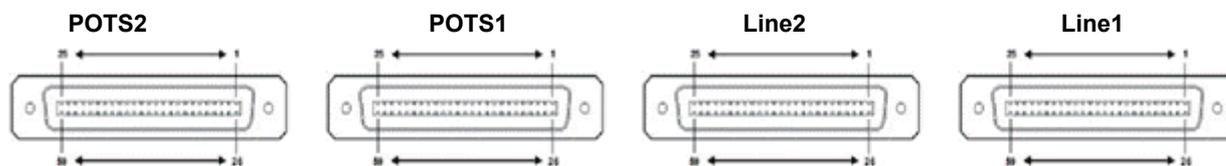
- 25 порт- контакты 1,26
- 26 порт- контакты 2,27
- 27 порт- контакты 3,28
- 28 порт- контакты 4,29
- 29 порт- контакты 5,30
- 30 порт- контакты 6,31
- 31 порт- контакты 7,32
- 32 порт- контакты 8,33
- 33 порт- контакты 9,34
- 34 порт- контакты 10,35
- 35 порт- контакты 11,36
- 36 порт- контакты 12,37
- 37 порт- контакты 13,38
- 38 порт- контакты 14,39
- 39 порт- контакты 15,40
- 40 порт- контакты 16,41
- 41 порт- контакты 17,42
- 42 порт- контакты 18,43
- 43 порт- контакты 19,44
- 44 порт- контакты 20,45
- 45 порт- контакты 21,46
- 46 порт- контакты 22,47
- 47 порт- контакты 23,48
- 48 порт- контакты 24,49

Разъем Line1

- 1 порт- контакты 1,26
- 2 порт- контакты 2,27
- 3 порт- контакты 3,28
- 4 порт- контакты 4,29
- 5 порт- контакты 5,30
- 6 порт- контакты 6,31
- 7 порт- контакты 7,32
- 8 порт- контакты 8,33
- 9 порт- контакты 9,34
- 10 порт- контакты 10,35
- 11 порт- контакты 11,36
- 12 порт- контакты 12,37
- 13 порт- контакты 13,38
- 14 порт- контакты 14,39
- 15 порт- контакты 15,40
- 16 порт- контакты 16,41
- 17 порт- контакты 17,42
- 18 порт- контакты 18,43
- 19 порт- контакты 19,44
- 20 порт- контакты 20,45
- 21 порт- контакты 21,46
- 22 порт- контакты 22,47
- 23 порт- контакты 23,48
- 24 порт- контакты 24,49

контакты 25,50 –не задействованы на всех разъемах

Схема коммутации портов DAS-3248DC rev.B на разъемы TELCO-50 (Amphenol). На рисунке ниже представлено схематическое расположение разъемов на задней панели DAS-3248DC rev.B



Разъем Line2

- 25 порт- контакты 1,26
- 26 порт- контакты 2,27
- 27 порт- контакты 3,28
- 28 порт- контакты 4,29
- 29 порт- контакты 5,30
- 30 порт- контакты 6,31
- 31 порт- контакты 7,32
- 32 порт- контакты 8,33
- 33 порт- контакты 9,34
- 34 порт- контакты 10,35
- 35 порт- контакты 11,36
- 36 порт- контакты 12,37
- 37 порт- контакты 13,38
- 38 порт- контакты 14,39
- 39 порт- контакты 15,40
- 40 порт- контакты 16,41
- 41 порт- контакты 17,42
- 42 порт- контакты 18,43
- 43 порт- контакты 19,44
- 44 порт- контакты 20,45
- 45 порт- контакты 21,46
- 46 порт- контакты 22,47
- 47 порт- контакты 23,48
- 48 порт- контакты 24,49

Разъем Line1

- 1 порт- контакты 1,26
- 2 порт- контакты 2,27
- 3 порт- контакты 3,28
- 4 порт- контакты 4,29
- 5 порт- контакты 5,30
- 6 порт- контакты 6,31
- 7 порт- контакты 7,32
- 8 порт- контакты 8,33
- 9 порт- контакты 9,34
- 10 порт- контакты 10,35
- 11 порт- контакты 11,36
- 12 порт- контакты 12,37
- 13 порт- контакты 13,38
- 14 порт- контакты 14,39
- 15 порт- контакты 15,40
- 16 порт- контакты 16,41
- 17 порт- контакты 17,42
- 18 порт- контакты 18,43
- 19 порт- контакты 19,44
- 20 порт- контакты 20,45
- 21 порт- контакты 21,46
- 22 порт- контакты 22,47
- 23 порт- контакты 23,48
- 24 порт- контакты 24,49

контакты 25,50 –не задействованы на всех разъемах.

Приложение В: 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 С: Примеры конфигурирования Generic Filter

1. Фильтр для запрета icmp echo-сообщений на определенном интерфейсе с определенного ip адреса

```
create filter rule entry ruleid 3 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 3 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 3 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 3 subruleid 2 icmp type 8 icmp type 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 3 subruleid 2 - второе подправило второго правила

icmp type 8 icmp type 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 3
```

Применяем правило к конкретному интерфейсу (eoa-xx, eth-x)

```
$modify filter rule entry ruleid 3 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 3 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 соответствии с наложенной маской

```
$create filter subrule generic ruleid 3 subruleid 1 offsethdr tcp offset 12 mask 0x00020000  
valuefrom 0x00020000 gencmp eq subruleprio high
```

прикладываем правило к интерфейсу

```
$create filter rule map ruleid 3 ifname eth-1 stageid 1
```

включаем правило

```
$modify filter rule entry ruleid 3 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 клиентских устройствах ADSL статических IP адресов.

\$create filter rule entry ruleid 3 action allow

Создаем разрешающее правило для нужного ip адреса:
action allow - принимать пакеты

\$create filter subrule ip ruleid 3 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 3 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 4 action drop

Создаем правило, запрещающее весь остальной трафик.

\$create filter subrule ip ruleid 4 subruleid 1 srcaddrcmp any dstaddrcmp any

Подправило, задающее весь трафик.

\$create filter rule map ifname eoa-23 stageid 1 ruleid 3

\$create filter rule map ifname eoa-23 stageid 1 ruleid 4

Применяем ранее созданные правила к конкретному интерфейсу (eoa-xx, eth-x)

\$modify filter rule entry ruleid 3 status enable

\$modify filter rule entry ruleid 4 status enable

Включаем фильтр в работу

4.Фильтр для привязки IP адреса к adsl порту (АТМ 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 заблокирован при использовании чужих авторизационных данных для данной линии (порту DSLAM).

Примечание: данное правило не требуется при использовании функции PPPoE Intermediate Agent (PIA).

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 ppoe

Создаем подправило, в котором указываем, что нас интересует трафик от хоста 11.22.33.44 переданный только по технологии ppoe :
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 ppoe

\$modify filter rule entry ruleid 4 status enable

Включаем правило в работу

\$create filter rule map ifname eoa-1 stageid 1 ruleid 4

Привязываем правило к интерфейсу.

5.Использование Generic List в IP-ARP ACL без применения логических выражений.

Пояснение: Данное правило может использоваться 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-1 value 0x11223344
```

```
$create filter list genentry ifname eoa-1 value 0x55667788
```

Создать фильтрующее правило Generic Filter

```
$create filter rule entry ruleid 3 action drop
```

Создать подправило анализа заголовка пакета

```
$create filter subrule ip ruleid 3 subruleid 1 srcaddrcmp ingenlist transportHdr ethernet pppoe
```

Включить правило в работу

```
$modify filter rule entry ruleid 3 status enable
```

Создать 2 правило для отбрасывания ARP пакетов

```
$create filter rule entry ruleid 4 action drop
```

```
$create filter subrule arp ruleid 4 subruleid 1 srcaddrcmp ingenlist
```

Включить правило в работу

```
$modify filter rule entry ruleid 4 status enable
```

Выставить порядок обработки правил

```
$create filter rule map ifname eoa-1 stageid 1 ruleid 3 orderid 1
```

```
$create filter rule map ifname eoa-1 stageid 1 ruleid 4 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-1 value 0x11223344
```

```
$create filter list genentry ifname eoa-1 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 3 action exprdef exprid 1
```

Создать подправило анализа заголовка пакета

```
$create filter subrule ip ruleid 3 subruleid 1 srcaddrcmp ingenlist transportHdr ethernet pppoe
```

Создать подправило для фильтрации ARP

```
$create filter subrule arp ruleid 3 subruleid 2 srcaddrcmp ingenlist
```

Включить правило в работу

```
$modify filter rule entry ruleid 3 status enable
```

Ассоциировать правило с интерфейсом

```
$create filter rule map ifname eoa-1 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-1 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-1 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-23
```

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 3 action drop statsstatus enable ruleprio high
```

Создаем главное правило:

action drop - отбрасывать

statsstatus enable – включение сбора статистики по правилу

```
$ create filter subrule ether ruleid 3 subruleid 1 ethertypefrom 0x8863 ethertypesmp eq  
subruleprio asinrule
```

Создаем подправило, в котором указываем, что нас интересуют все PADI пакеты протокола PPPoE.

ruleid 3 subruleid 1 – первое подправило двадцать третьего правила

ethertypefrom 0x8863 – нижнее значение типа протокола

ethertypesmp – эквивалент 0x8863 типа протокола

subruleprio asinrule – приоритет как у правила

```
$ create filter rule map ifname eoa-22 stageid 1 ruleid 3
```

Применяем созданное правило к конкретному интерфейсу (eoa-xx, eth-x)

```
$ modify filter rule entry ruleid 3 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 3 action allow ruleprio high ruledir in

\$ create filter subrule ether ruleid 3 subruleid 1 ethertypefrom 0x8863 ethertypeto 0x8864 ethertypecmp inrange subruleprio asinrule

Создаем подправило, в котором указываем, что нас интересуют все пакеты протокола PPPoE.

ruleid 3 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 3 stageid 1 ifname alleoa

Применяем правило ко всем интерфейсам eoa (alleoa)

\$ modify filter rule entry ruleid 3 status enable

Включаем правило в работу

\$ create filter rule entry ruleid 4 action drop ruledir out pkttype bcast status enable

Запрещаем весь Broadcast трафик в сторону клиентов

\$ create filter rule map ruleid 4 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 2

Интерфейсы "dsl", индексы интерфейсов с 5 по 52

Интерфейсы "atm", индексы интерфейсов с 149 по 196

Интерфейсы "aal5", индексы интерфейсов с 197 по 581

Интерфейсы "eoa", индексы интерфейсов с 582 по 996

Интерфейсы "dsl1", индексы интерфейсов с 53 по 100

Интерфейсы "dslf", индексы интерфейсов с 101 по 148

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 пакеты (ifOutOctets)

2. 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 1.3.6.1.4.1.3646.1300.8.1.6.6.2.0 i 2**

Задача: Сохранение всех настроек в энергонезависимой памяти (NVRAM).

Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.6.6.4.0 i 2**

Задача: Изменение режима коммутации глобально (на всем устройстве) на Unrestricted

Команда: **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.6.2.15.0 i 2**

Объяснение: Значения приведенного OID следующие 1-Restricted, 2-Unrestricted, 3-Residential.

3.Изменение параметров VPI, VCI на DAS-3224/3248 посредством SNMP запроса.

Задача: Изменить VPI интерфейса AAL5-1 на 40, VCI на 10. IP адрес устройства для простоты возьмем 192.168.0.1. Community string- public.

Команды:

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.197 i 2
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.1.5.1.2.197 i 40
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.197 i 1
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.197 i 2
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.1.5.1.3.197 i 10
snmpset -v2c -c public 192.168.0.1 1.3.6.1.2.1.2.2.1.7.197 i 1
```

Объяснение:

Индексы AAL5 интерфейсов на устройстве начинаются с 197. Таким образом, интерфейс AAL5-1 соответствует ifIndex-197, AAL5-1-198 и т.д.

Изменение параметров VPI и VCI для каждого интерфейса производится отдельно. 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.

4.Изменение Output Rate Limit (ORL) на ATM на DAS-3224/3248 посредством SNMP запроса.

```
snmpset -v 2c -c private 192.168.10.201 1.3.6.1.4.1.3646.1300.8.1.1.2.1.3.149 i 20000
```

Объяснение:

Индексы ATM интерфейсов на устройстве начинаются с 149. Таким образом, интерфейс ATM-1 соответствует ifIndex-149, ATM-2-150...ATM-48-196 .

5.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-1)

Команда:

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.4.2.1.2.1 а 192.168.7.2  
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.4.2.1.3.1 а 255.255.255.0  
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.4.2.1.13.1 i 1
```

Объяснение: Первая команда меняет IP адрес Uplink 1(eth-1) 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-2) последняя цифра всех OID меняется на 2 (например, 1.3.6.1.4.1.3646.1300.8.1.4.2.1.2.2).

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 1.3.6.1.4.1.3646.1300.8.1.4.2.1.8.1 i 3  
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.4.2.1.4.1 i 2
```

Объяснение:

1.3.6.1.4.1.3646.1300.8.1.4.2.1.8.1 i 3- меняет дуплекс порта на Full (значения OID: 1-Auto,2-Half Duplex, 3-Ful Duplex).

1.3.6.1.4.1.3646.1300.8.1.4.2.1.4.1 i 2- меняет скорость порта на 100Мбит/с (значения OID: 0-auto,1-10,2-100,3-1000).

7. 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 1.3.6.1.4.1.3646.1300.8.1.8.1.6.0 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 1.3.6.1.4.1.3646.1300.8.1.8.2.1.2.1 i 1**

Объяснение: Последняя цифра OID должна соответствовать номеру Bridge интерфейса (для первого порта -1). Значение OID: 1-включение функции,0-выключение.

8.Создание и удаление глобального DSL профиля посредством SNMP запроса.

Задача 1: Создать DSL профиль со следующими скоростями minUpstream =128кбит/с, minDownstream =256кбит/с, minDownstream=512кбит/с, maxUpstream =1024кбит/с и привязать к нему 1 порт устройства.

Команда:

```
snmpset -v2c -c public 192.168.0.1  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.23.5.100.108.105.110.107 i 4
```

```
snmpset -v2c -c public 192.168.0.1  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.2.5.100.108.105.110.107 i 2  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.3.5.100.108.105.110.107 i 0  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.4.5.100.108.105.110.107 i 1  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.5.5.100.108.105.110.107 i 0  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.9.5.100.108.105.110.107 i 512  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.10.5.100.108.105.110.107 i 1024  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.15.5.100.108.105.110.107 i 128  
1.3.6.1.4.1.3646.1300.8.2.7.1.1.15.5.100.108.105.110.107 i 256
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.2.7.2.1.2.1 s dlink
```

Объяснение:

- 1) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.23.5.100.108.105.110.107 i 4 – Создание DSL профиль с именем **dlink** .

5.100.108.105.110.107- это идентификатор профиля, образующийся по следующему правилу:

Первый индекс (5)- количество символов в названии профиля.

Последующие индексы соответствуют буквам и символам в названии профиля (в данном случае **dlink**).

Индексы символов:

Большие (прописные) буквы английского алфавита имеют индексы, начиная с 65 (то есть А -65, В-66 и т.д.). Малые (строчные) буквы английского алфавита имеют индексы, начиная с 97 (то есть а -97, b-98...d-100 и т.д.). Символы цифр имеют индексы, начиная с 49 (1-49...9-58). Символы нижнего подчеркивания “_” имеет индекс 95, символ дефиса “-” имеет индекс 45.

- 2) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.2.5.100.108.105.110.107 i 08000000 – Задаем тип модуляции (ADSL2+) для создаваемого профиля (смотрите табл ниже)
- 3) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.3.5.100.108.105.110.107 i 0- Задает значение Annex M для профиля (0-выключено, 1-включено)
- 4) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.4.5.100.108.105.110.107 i 1 - Задает типа адаптации линии для профиля (0-фиксированная скорость, 1 – адаптация)
- 5) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.5.5.100.108.105.110.107 i 0 – задает тип линии для профиля (0-interleaved, 1-fast)
- 6) 1.3.6.1.4.1.3646.1300.8.2.7.1.1.9.5.100.108.105.110.107 i 512 – задает минимальную Downstream скорость (в килобитах)

- 7) **1.3.6.1.4.1.3646.1300.8.2.7.1.1.10.5.100.108.105.110.107** i **1024** - задает максимальную Downstream скорость (в килобитах)
- 8) **1.3.6.1.4.1.3646.1300.8.2.7.1.1.15.5.100.108.105.110.107** i **128** - задает минимальную Upstream скорость (в килобитах)
- 9) **1.3.6.1.4.1.3646.1300.8.2.7.1.1.16.5.100.108.105.110.107** i **256** - задает максимальную Upstream скорость (в килобитах)
- 10) **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.2.7.2.1.2.1 s dlink -**
Прикрепляет 1 порт DSL к профилю dlink

Задача 2: Удалить DSL профиль dlink

Команда: **snmpset -v2c -c public 192.168.0.1**

1.3.6.1.4.1.171.10.65.1.3.8.1.23.5.100.108.105.110.107 i **6**

(Внимание : не забудьте “открепить” все порты от этого профиля)

Таблица значений ADSL модуляции

Пояснение: Всего на модуляцию отводится одно 8 разрядов число.

Описание типа модуляции	Значение SNMP OID
ADSL ANSI T1.1413	20000000
ADSL G.Dmt	80000000
G.Lite	40000000
ADSL 2	10000000
ADSL 2+	08000000
READSL 2	04000000

9.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 1.3.6.1.4.1.3646.1300.8.1.2.10.1.5.5
```

б) Текущая скорость (AturCurrTxRate) (индекс интерфейса dsli-0)

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.4.1.2.53
```

(ATUC-для Upstream направления)

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.5.1.2.53
```

(ATUR-для Downstream направления)

в) Текущий сигнал/шум (Curr SNR margin):

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.2.1.4.5
```

(ATUC-для Upstream направления)

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.3.1.4.5
```

(ATUR-для Downstream направления)

г) Текущее затухание на линии (CurrAtn):

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.2.1.5.5
```

(ATUC-для Upstream направления)

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.3.1.5.5
```

(ATUR-для Downstream направления)

д) Ошибки на ADSL линии

ATUC LoFS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.1.5
```

ATUR LoFS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.1.5
```

ATUC LoSS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.2.5
```

ATUR LoSS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.2.5
```

ATUC LoLS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.3.5
```

ATUR LoLS

```
snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.3.5
```

ATUC LPRS

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.4.5

ATUR LPRS

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.4.5

ATUC ES

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.5.5

ATUR ES

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.5.5

ATUC Inits

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.6.5

ATUR Inits

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.6.5

ATUC Valid Intervals

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.7.5

ATUR Valid Intervals

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.7.5

ATUC Invalid Intervals

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.6.1.8.5

ATUR Invalid Intervals

snmpget -v2c -c public 192.168.0.1 1.3.6.1.2.1.10.94.1.1.7.1.8.5

12.Пример создания и удаления правила Generic Filter посредством SNMP запроса.

Задача1 :

Создать фильтр для привязки IP адреса к adsl порту (ATM PVC)

аналогичный следующим консольным командам:

```
$create filter rule entry ruleid 3 action allow description Allow_ip
```

```
$create filter subrule ip ruleid 3 subruleid 1 srcipaddrfrom 192.168.100.207 srcaddrcmp eq  
dstaddrcmp any ipsrcaddrmask 0xffffffff
```

```
$create filter rule entry ruleid 4 action drop description Drop_any_ip
```

```
$create filter subrule ip ruleid 4 subruleid 1 srcaddrcmp any dstaddrcmp any
```

```
$create filter rule map ifname eoa-1 stageid 1 ruleid 3
```

```
$create filter rule map ifname eoa-1 stageid 1 ruleid 4
```

```
$modify filter rule entry ruleid 3 status enable
```

```
$modify filter rule entry ruleid 4 status enable
```

Команды:

```
snmpset -v2c -c public 192.168.0.1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.2.3 i 2
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.3.3 s Allow_ip
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.3 i 2
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.3 i 4
```

```
snmpset -v2c -c public 192.168.0.1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.3.3.1 i 192.168.100.207
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.9.3.1 i 1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.10.3.1 i 7
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.3.1 i 4
```

```
snmpset -v2c -c public 192.168.0.1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.2.4 i 1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.3.4 s Drop_any_ip
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.4 i 2
```

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.4 i 4
```

```
snmpset -v2c -c public 192.168.0.1
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.9.4.1 i 7
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.10.4.1 i 7
```

```
1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.5.1 i 4
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.3 i 4
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.4 i 4
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.3 i 1
```

```
snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.4 i 1
```

Объяснение:

1) snmpset -v2c -c public 192.168.0.1

```
1.3.6.1.4.1.3646.1300.8.1.10.1.1.2.3 i 2 - Действие правила (Allow)
```

1.3.6.1.4.1.3646.1300.8.1.10.1.1.3.3 s **Allow_ip** - Описание (Description) правила
1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.3 i 2- Правило в выключенном состоянии
1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.3 i 4 - Создать правило Generic Filter с ruleid=3

2) **snmpset -v2c -c public 192.168.0.1**

1.3.6.1.4.1.3646.1300.8.1.10.3.1.3.3.1 i **192.168.100.207** –фильтруемый ip адрес
(srcipaddrfrom)

1.3.6.1.4.1.3646.1300.8.1.10.3.1.9.3.1 i 1- srcaddrcmp eq

1.3.6.1.4.1.3646.1300.8.1.10.3.1.10.3.1 i 7- dstaddrcmp any

1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.3.1 i 4 -Создать подправило (Subrule) Generic Filter с Ruleid=3 и subruleid=1

3) **snmpset -v2c -c public 192.168.0.1**

1.3.6.1.4.1.3646.1300.8.1.10.1.1.2.4 i 1 - Действие правила (Drop)

1.3.6.1.4.1.3646.1300.8.1.10.1.1.3.4 s **Drop_any_ip** - описание (Description) правила

1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.4 i 2 - Правило в выключенном состоянии

1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.4 i 4 - Создать правило Generic Filter с ruleid=4

4) **snmpset -v2c -c public 192.168.0.1**

1.3.6.1.4.1.3646.1300.8.1.10.3.1.9.4.1 i 7- srcaddrcmp any

1.3.6.1.4.1.3646.1300.8.1.10.3.1.10.4.1 i 7- dstaddrcmp any

1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.4.1 i 4 - Создать подправило (Subrule) Generic Filter с Ruleid=4 и subruleid=1

5) **snmpset -v2c -c public 192.168.0.1**

1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.3 i 4 - прикрепить интерфейс eoa-1 к ruleid =3

1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.4 i 4 – прикрепить интерфейс eoa-1 к ruleid =4
Индекс 582 в SNMP OID обозначается индекс интерфейса eoa-1.

Если правило прикрепляется более чем к одному интерфейсу, необходимо создать несколько OID каждый со своим индексом интерфейса.

В случае использования закрепленных в системе групповых значений интерфейсов (all, alleth, alleoa) используются следующие индексы:

4294967293- alleth, 4294967294-alleoa, 4294967295 –all.

6) **snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.3 i 1** – включить правило с ruleid=3

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.5.4 i 1 – включить правило с ruleid=4

Задача 2: Удалить вышеописанный фильтр

Команды:

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.3 i 6

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.10.1.5.582.1.4 i 6

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.3.1 i 6

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.3.1.20.4.1 i 6

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.3 i 6

snmpset -v2c -c public 192.168.0.1 1.3.6.1.4.1.3646.1300.8.1.10.1.1.15.4 i 6

Приложение Е: Примеры комплексных конфигураций.

1.Пример настройки DAS-3224 DSLAM для предоставления трех сервисов (Интернет, Voice и Видео) с использованием CLI режима
В данном примере рассматривается конфигурирование DAS-3238 rev.B (f/w ver. 2.43)
В рамках данного примера предполагается, что трафик (три сервиса) с

вышестоящего коммутатора приходит уже тегированным и приоретизированным. Задача DSLAM поместить трафик в соответствии с DSCP приоритетом и внутренним приоритетом 802.1p в нужную приоритетную очередь и определить гарантированную полосу пропускания для каждого из сервисов в направлениях Upstream/Downstream.

Представленный пример является полностью рабочим.

Для Internet VC использовались параметры VPI/VCI 10/40.

VLAN Internet сервиса – VID 21.

Для IPTV VC использовались параметры VPI/VCI 10/50.

VLAN IPTV сервиса – VID 20.

Для Voice VC использовались параметры VPI/VCI 10/60.

VLAN Voice сервиса – VID 1.

Все настройки производились с DSLAM, находящимся в Default конфигурации.

Внимание: кроме ручной настройки данного примера через командный интерфейс вы можете воспользоваться загрузкой и исполнением текстового скриптового файла на устройстве.

1.Изменяем настройки ETH интерфейса (Uplink). В данном случае для управления устройством используется VLAN с VID 21:

```
modify ethernet intf ifname eth-1 disable  
modify ethernet intf ifname eth-1 ip 192.168.10.35 mask 255.255.255.0 mgmtvlanid  
21 enable
```

2.Выключаем созданные в default конфигурации ATM VC интерфейсы, изменяем настройки VPI/VCI и включаем интерфейсы в работу:

```
modify atm vc intf ifname aal5-1 disable  
modify atm vc intf ifname aal5-2 disable  
modify atm vc intf ifname aal5-3 disable  
modify atm vc intf ifname aal5-4 disable  
modify atm vc intf ifname aal5-5 disable  
modify atm vc intf ifname aal5-6 disable  
modify atm vc intf ifname aal5-7 disable  
modify atm vc intf ifname aal5-8 disable  
modify atm vc intf ifname aal5-9 disable  
modify atm vc intf ifname aal5-10 disable  
modify atm vc intf ifname aal5-11 disable  
modify atm vc intf ifname aal5-12 disable  
modify atm vc intf ifname aal5-13 disable  
modify atm vc intf ifname aal5-14 disable  
modify atm vc intf ifname aal5-15 disable  
modify atm vc intf ifname aal5-16 disable  
modify atm vc intf ifname aal5-17 disable
```

modify atm vc intf ifname aal5-18 disable
modify atm vc intf ifname aal5-19 disable
modify atm vc intf ifname aal5-20 disable
modify atm vc intf ifname aal5-21 disable
modify atm vc intf ifname aal5-22 disable
modify atm vc intf ifname aal5-23 disable
modify atm vc intf ifname aal5-24 disable
modify atm vc intf ifname aal5-25 disable
modify atm vc intf ifname aal5-26 disable
modify atm vc intf ifname aal5-27 disable
modify atm vc intf ifname aal5-28 disable
modify atm vc intf ifname aal5-29 disable
modify atm vc intf ifname aal5-30 disable
modify atm vc intf ifname aal5-31 disable
modify atm vc intf ifname aal5-32 disable
modify atm vc intf ifname aal5-33 disable
modify atm vc intf ifname aal5-34 disable
modify atm vc intf ifname aal5-35 disable
modify atm vc intf ifname aal5-36 disable
modify atm vc intf ifname aal5-37 disable
modify atm vc intf ifname aal5-38 disable
modify atm vc intf ifname aal5-39 disable
modify atm vc intf ifname aal5-40 disable
modify atm vc intf ifname aal5-41 disable
modify atm vc intf ifname aal5-42 disable
modify atm vc intf ifname aal5-43 disable
modify atm vc intf ifname aal5-44 disable
modify atm vc intf ifname aal5-45 disable
modify atm vc intf ifname aal5-46 disable
modify atm vc intf ifname aal5-47 disable
modify atm vc intf ifname aal5-48 disable
modify atm vc intf ifname aal5-1 vpi 10 vci 40
modify atm vc intf ifname aal5-2 vpi 10 vci 40
modify atm vc intf ifname aal5-3 vpi 10 vci 40
modify atm vc intf ifname aal5-4 vpi 10 vci 40
modify atm vc intf ifname aal5-5 vpi 10 vci 40
modify atm vc intf ifname aal5-6 vpi 10 vci 40
modify atm vc intf ifname aal5-7 vpi 10 vci 40
modify atm vc intf ifname aal5-8 vpi 10 vci 40
modify atm vc intf ifname aal5-9 vpi 10 vci 40
modify atm vc intf ifname aal5-10 vpi 10 vci 40
modify atm vc intf ifname aal5-11 vpi 10 vci 40
modify atm vc intf ifname aal5-12 vpi 10 vci 40
modify atm vc intf ifname aal5-13 vpi 10 vci 40
modify atm vc intf ifname aal5-14 vpi 10 vci 40
modify atm vc intf ifname aal5-15 vpi 10 vci 40
modify atm vc intf ifname aal5-16 vpi 10 vci 40
modify atm vc intf ifname aal5-17 vpi 10 vci 40
modify atm vc intf ifname aal5-18 vpi 10 vci 40
modify atm vc intf ifname aal5-19 vpi 10 vci 40
modify atm vc intf ifname aal5-20 vpi 10 vci 40
modify atm vc intf ifname aal5-21 vpi 10 vci 40

modify atm vc intf ifname aal5-26 enable
modify atm vc intf ifname aal5-27 enable
modify atm vc intf ifname aal5-28 enable
modify atm vc intf ifname aal5-29 enable
modify atm vc intf ifname aal5-30 enable
modify atm vc intf ifname aal5-31 enable
modify atm vc intf ifname aal5-32 enable
modify atm vc intf ifname aal5-33 enable
modify atm vc intf ifname aal5-34 enable
modify atm vc intf ifname aal5-35 enable
modify atm vc intf ifname aal5-36 enable
modify atm vc intf ifname aal5-37 enable
modify atm vc intf ifname aal5-38 enable
modify atm vc intf ifname aal5-39 enable
modify atm vc intf ifname aal5-40 enable
modify atm vc intf ifname aal5-41 enable
modify atm vc intf ifname aal5-42 enable
modify atm vc intf ifname aal5-43 enable
modify atm vc intf ifname aal5-44 enable
modify atm vc intf ifname aal5-45 enable
modify atm vc intf ifname aal5-46 enable
modify atm vc intf ifname aal5-47 enable
modify atm vc intf ifname aal5-48 enable

3. Выключаем созданные в default конфигурации Bridge интерфейсы:

modify bridge *port* intf portid 1 status disable
modify bridge *port* intf portid 2 status disable
modify bridge *port* intf portid 3 status disable
modify bridge *port* intf portid 4 status disable
modify bridge *port* intf portid 5 status disable
modify bridge *port* intf portid 6 status disable
modify bridge *port* intf portid 7 status disable
modify bridge *port* intf portid 8 status disable
modify bridge *port* intf portid 9 status disable
modify bridge *port* intf portid 10 status disable
modify bridge *port* intf portid 11 status disable
modify bridge *port* intf portid 12 status disable
modify bridge *port* intf portid 13 status disable
modify bridge *port* intf portid 14 status disable
modify bridge *port* intf portid 15 status disable
modify bridge *port* intf portid 16 status disable
modify bridge *port* intf portid 17 status disable
modify bridge *port* intf portid 18 status disable
modify bridge *port* intf portid 19 status disable
modify bridge *port* intf portid 20 status disable
modify bridge *port* intf portid 21 status disable
modify bridge *port* intf portid 22 status disable
modify bridge *port* intf portid 23 status disable
modify bridge *port* intf portid 24 status disable
modify bridge *port* intf portid 25 status disable
modify bridge *port* intf portid 26 status disable
modify bridge *port* intf portid 27 status disable

modify bridge *port* intf portid 28 status disable
modify bridge *port* intf portid 29 status disable
modify bridge *port* intf portid 30 status disable
modify bridge *port* intf portid 31 status disable
modify bridge *port* intf portid 32 status disable
modify bridge *port* intf portid 33 status disable
modify bridge *port* intf portid 34 status disable
modify bridge *port* intf portid 35 status disable
modify bridge *port* intf portid 36 status disable
modify bridge *port* intf portid 37 status disable
modify bridge *port* intf portid 38 status disable
modify bridge *port* intf portid 39 status disable
modify bridge *port* intf portid 40 status disable
modify bridge *port* intf portid 41 status disable
modify bridge *port* intf portid 42 status disable
modify bridge *port* intf portid 43 status disable
modify bridge *port* intf portid 44 status disable
modify bridge *port* intf portid 45 status disable
modify bridge *port* intf portid 46 status disable
modify bridge *port* intf portid 47 status disable
modify bridge *port* intf portid 48 status disable

4.Создаем ATM VC интерфейсы для IPTV услуги:

```
create atm vc intf ifname aal5-49 vpi 10 vci 50 lowif atm-1  
create atm vc intf ifname aal5-50 vpi 10 vci 50 lowif atm-2  
create atm vc intf ifname aal5-51 vpi 10 vci 50 lowif atm-3  
create atm vc intf ifname aal5-52 vpi 10 vci 50 lowif atm-4  
create atm vc intf ifname aal5-53 vpi 10 vci 50 lowif atm-5  
create atm vc intf ifname aal5-54 vpi 10 vci 50 lowif atm-6  
create atm vc intf ifname aal5-55 vpi 10 vci 50 lowif atm-7  
create atm vc intf ifname aal5-56 vpi 10 vci 50 lowif atm-8  
create atm vc intf ifname aal5-57 vpi 10 vci 50 lowif atm-9  
create atm vc intf ifname aal5-58 vpi 10 vci 50 lowif atm-10  
create atm vc intf ifname aal5-59 vpi 10 vci 50 lowif atm-11  
create atm vc intf ifname aal5-60 vpi 10 vci 50 lowif atm-12  
create atm vc intf ifname aal5-61 vpi 10 vci 50 lowif atm-13  
create atm vc intf ifname aal5-62 vpi 10 vci 50 lowif atm-14  
create atm vc intf ifname aal5-63 vpi 10 vci 50 lowif atm-15  
create atm vc intf ifname aal5-64 vpi 10 vci 50 lowif atm-16  
create atm vc intf ifname aal5-65 vpi 10 vci 50 lowif atm-17  
create atm vc intf ifname aal5-66 vpi 10 vci 50 lowif atm-18  
create atm vc intf ifname aal5-67 vpi 10 vci 50 lowif atm-19  
create atm vc intf ifname aal5-68 vpi 10 vci 50 lowif atm-20  
create atm vc intf ifname aal5-69 vpi 10 vci 50 lowif atm-21  
create atm vc intf ifname aal5-70 vpi 10 vci 50 lowif atm-22  
create atm vc intf ifname aal5-71 vpi 10 vci 50 lowif atm-23  
create atm vc intf ifname aal5-72 vpi 10 vci 50 lowif atm-24  
create atm vc intf ifname aal5-73 vpi 10 vci 50 lowif atm-25  
create atm vc intf ifname aal5-74 vpi 10 vci 50 lowif atm-26  
create atm vc intf ifname aal5-75 vpi 10 vci 50 lowif atm-27  
create atm vc intf ifname aal5-76 vpi 10 vci 50 lowif atm-28  
create atm vc intf ifname aal5-77 vpi 10 vci 50 lowif atm-29
```

```
create atm vc intf ifname aal5-78 vpi 10 vci 50 lowif atm-30
create atm vc intf ifname aal5-79 vpi 10 vci 50 lowif atm-31
create atm vc intf ifname aal5-80 vpi 10 vci 50 lowif atm-32
create atm vc intf ifname aal5-81 vpi 10 vci 50 lowif atm-33
create atm vc intf ifname aal5-82 vpi 10 vci 50 lowif atm-34
create atm vc intf ifname aal5-83 vpi 10 vci 50 lowif atm-35
create atm vc intf ifname aal5-84 vpi 10 vci 50 lowif atm-36
create atm vc intf ifname aal5-85 vpi 10 vci 50 lowif atm-37
create atm vc intf ifname aal5-86 vpi 10 vci 50 lowif atm-38
create atm vc intf ifname aal5-87 vpi 10 vci 50 lowif atm-39
create atm vc intf ifname aal5-88 vpi 10 vci 50 lowif atm-40
create atm vc intf ifname aal5-89 vpi 10 vci 50 lowif atm-41
create atm vc intf ifname aal5-90 vpi 10 vci 50 lowif atm-42
create atm vc intf ifname aal5-91 vpi 10 vci 50 lowif atm-43
create atm vc intf ifname aal5-92 vpi 10 vci 50 lowif atm-44
create atm vc intf ifname aal5-93 vpi 10 vci 50 lowif atm-45
create atm vc intf ifname aal5-94 vpi 10 vci 50 lowif atm-46
create atm vc intf ifname aal5-95 vpi 10 vci 50 lowif atm-47
create atm vc intf ifname aal5-96 vpi 10 vci 50 lowif atm-48
```

5.Создаем ЕоА интерфейсы поверх созданных АТМ VC интерфейсов для IPTV услуги:

```
create eoa intf ifname eoa-49 lowif aal5-49
create eoa intf ifname eoa-50 lowif aal5-50
create eoa intf ifname eoa-51 lowif aal5-51
create eoa intf ifname eoa-52 lowif aal5-52
create eoa intf ifname eoa-53 lowif aal5-53
create eoa intf ifname eoa-54 lowif aal5-54
create eoa intf ifname eoa-55 lowif aal5-55
create eoa intf ifname eoa-56 lowif aal5-56
create eoa intf ifname eoa-57 lowif aal5-57
create eoa intf ifname eoa-58 lowif aal5-58
create eoa intf ifname eoa-59 lowif aal5-59
create eoa intf ifname eoa-60 lowif aal5-60
create eoa intf ifname eoa-61 lowif aal5-61
create eoa intf ifname eoa-62 lowif aal5-62
create eoa intf ifname eoa-63 lowif aal5-63
create eoa intf ifname eoa-64 lowif aal5-64
create eoa intf ifname eoa-65 lowif aal5-65
create eoa intf ifname eoa-66 lowif aal5-66
create eoa intf ifname eoa-67 lowif aal5-67
create eoa intf ifname eoa-68 lowif aal5-68
create eoa intf ifname eoa-69 lowif aal5-69
create eoa intf ifname eoa-70 lowif aal5-70
create eoa intf ifname eoa-71 lowif aal5-71
create eoa intf ifname eoa-72 lowif aal5-72
create eoa intf ifname eoa-73 lowif aal5-73
create eoa intf ifname eoa-74 lowif aal5-74
create eoa intf ifname eoa-75 lowif aal5-75
create eoa intf ifname eoa-76 lowif aal5-76
create eoa intf ifname eoa-77 lowif aal5-77
create eoa intf ifname eoa-78 lowif aal5-78
```

```
create eoa intf ifname eoa-79 lowif aal5-79
create eoa intf ifname eoa-80 lowif aal5-80
create eoa intf ifname eoa-81 lowif aal5-81
create eoa intf ifname eoa-82 lowif aal5-82
create eoa intf ifname eoa-83 lowif aal5-83
create eoa intf ifname eoa-84 lowif aal5-84
create eoa intf ifname eoa-85 lowif aal5-85
create eoa intf ifname eoa-86 lowif aal5-86
create eoa intf ifname eoa-87 lowif aal5-87
create eoa intf ifname eoa-88 lowif aal5-88
create eoa intf ifname eoa-89 lowif aal5-89
create eoa intf ifname eoa-90 lowif aal5-90
create eoa intf ifname eoa-91 lowif aal5-91
create eoa intf ifname eoa-92 lowif aal5-92
create eoa intf ifname eoa-93 lowif aal5-93
create eoa intf ifname eoa-94 lowif aal5-94
create eoa intf ifname eoa-95 lowif aal5-95
create eoa intf ifname eoa-96 lowif aal5-96
```

6.Создаем Bridge интерфейсы поверх созданных EoA интерфейсов для IPTV услуги:

```
create bridge port intf portid 49 ifname eoa-49
create bridge port intf portid 50 ifname eoa-50
create bridge port intf portid 51 ifname eoa-51
create bridge port intf portid 52 ifname eoa-52
create bridge port intf portid 53 ifname eoa-53
create bridge port intf portid 54 ifname eoa-54
create bridge port intf portid 55 ifname eoa-55
create bridge port intf portid 56 ifname eoa-56
create bridge port intf portid 57 ifname eoa-57
create bridge port intf portid 58 ifname eoa-58
create bridge port intf portid 59 ifname eoa-59
create bridge port intf portid 60 ifname eoa-60
create bridge port intf portid 61 ifname eoa-61
create bridge port intf portid 62 ifname eoa-62
create bridge port intf portid 63 ifname eoa-63
create bridge port intf portid 64 ifname eoa-64
create bridge port intf portid 65 ifname eoa-65
create bridge port intf portid 66 ifname eoa-66
create bridge port intf portid 67 ifname eoa-67
create bridge port intf portid 68 ifname eoa-68
create bridge port intf portid 69 ifname eoa-69
create bridge port intf portid 70 ifname eoa-70
create bridge port intf portid 71 ifname eoa-71
create bridge port intf portid 72 ifname eoa-72
create bridge port intf portid 73 ifname eoa-73
create bridge port intf portid 74 ifname eoa-74
create bridge port intf portid 75 ifname eoa-75
create bridge port intf portid 76 ifname eoa-76
create bridge port intf portid 77 ifname eoa-77
create bridge port intf portid 78 ifname eoa-78
create bridge port intf portid 79 ifname eoa-79
create bridge port intf portid 80 ifname eoa-80
```

```
create bridge port intf portid 81 ifname eoa-81
create bridge port intf portid 82 ifname eoa-82
create bridge port intf portid 83 ifname eoa-83
create bridge port intf portid 84 ifname eoa-84
create bridge port intf portid 85 ifname eoa-85
create bridge port intf portid 86 ifname eoa-86
create bridge port intf portid 87 ifname eoa-87
create bridge port intf portid 88 ifname eoa-88
create bridge port intf portid 89 ifname eoa-89
create bridge port intf portid 90 ifname eoa-90
create bridge port intf portid 91 ifname eoa-91
create bridge port intf portid 92 ifname eoa-92
create bridge port intf portid 93 ifname eoa-93
create bridge port intf portid 94 ifname eoa-94
create bridge port intf portid 95 ifname eoa-95
create bridge port intf portid 96 ifname eoa-96
```

7.Создаем ATM VC интерфейсы для Voice услуги:

```
create atm vc intf ifname aal5-97 vpi 10 vci 60 lowif atm-1
create atm vc intf ifname aal5-98 vpi 10 vci 60 lowif atm-2
create atm vc intf ifname aal5-99 vpi 10 vci 60 lowif atm-3
create atm vc intf ifname aal5-100 vpi 10 vci 60 lowif atm-4
create atm vc intf ifname aal5-101 vpi 10 vci 60 lowif atm-5
create atm vc intf ifname aal5-102 vpi 10 vci 60 lowif atm-6
create atm vc intf ifname aal5-103 vpi 10 vci 60 lowif atm-7
create atm vc intf ifname aal5-104 vpi 10 vci 60 lowif atm-8
create atm vc intf ifname aal5-105 vpi 10 vci 60 lowif atm-9
create atm vc intf ifname aal5-106 vpi 10 vci 60 lowif atm-10
create atm vc intf ifname aal5-107 vpi 10 vci 60 lowif atm-11
create atm vc intf ifname aal5-108 vpi 10 vci 60 lowif atm-12
create atm vc intf ifname aal5-109 vpi 10 vci 60 lowif atm-13
create atm vc intf ifname aal5-110 vpi 10 vci 60 lowif atm-14
create atm vc intf ifname aal5-111 vpi 10 vci 60 lowif atm-15
create atm vc intf ifname aal5-112 vpi 10 vci 60 lowif atm-16
create atm vc intf ifname aal5-113 vpi 10 vci 60 lowif atm-17
create atm vc intf ifname aal5-114 vpi 10 vci 60 lowif atm-18
create atm vc intf ifname aal5-115 vpi 10 vci 60 lowif atm-19
create atm vc intf ifname aal5-116 vpi 10 vci 60 lowif atm-20
create atm vc intf ifname aal5-117 vpi 10 vci 60 lowif atm-21
create atm vc intf ifname aal5-118 vpi 10 vci 60 lowif atm-22
create atm vc intf ifname aal5-119 vpi 10 vci 60 lowif atm-23
create atm vc intf ifname aal5-120 vpi 10 vci 60 lowif atm-24
create atm vc intf ifname aal5-121 vpi 10 vci 60 lowif atm-25
create atm vc intf ifname aal5-122 vpi 10 vci 60 lowif atm-26
create atm vc intf ifname aal5-123 vpi 10 vci 60 lowif atm-27
create atm vc intf ifname aal5-124 vpi 10 vci 60 lowif atm-28
create atm vc intf ifname aal5-125 vpi 10 vci 60 lowif atm-29
create atm vc intf ifname aal5-126 vpi 10 vci 60 lowif atm-30
create atm vc intf ifname aal5-127 vpi 10 vci 60 lowif atm-31
create atm vc intf ifname aal5-128 vpi 10 vci 60 lowif atm-32
create atm vc intf ifname aal5-129 vpi 10 vci 60 lowif atm-33
create atm vc intf ifname aal5-130 vpi 10 vci 60 lowif atm-34
```

```
create atm vc intf ifname aal5-131 vpi 10 vci 60 lowif atm-35
create atm vc intf ifname aal5-132 vpi 10 vci 60 lowif atm-36
create atm vc intf ifname aal5-133 vpi 10 vci 60 lowif atm-37
create atm vc intf ifname aal5-134 vpi 10 vci 60 lowif atm-38
create atm vc intf ifname aal5-135 vpi 10 vci 60 lowif atm-39
create atm vc intf ifname aal5-136 vpi 10 vci 60 lowif atm-40
create atm vc intf ifname aal5-137 vpi 10 vci 60 lowif atm-41
create atm vc intf ifname aal5-138 vpi 10 vci 60 lowif atm-42
create atm vc intf ifname aal5-139 vpi 10 vci 60 lowif atm-43
create atm vc intf ifname aal5-140 vpi 10 vci 60 lowif atm-44
create atm vc intf ifname aal5-141 vpi 10 vci 60 lowif atm-45
create atm vc intf ifname aal5-142 vpi 10 vci 60 lowif atm-46
create atm vc intf ifname aal5-143 vpi 10 vci 60 lowif atm-47
create atm vc intf ifname aal5-144 vpi 10 vci 60 lowif atm-48
```

8.Создаем ЕоА интерфейсы поверх созданных АТМ VС интерфейсов для Voice услуги:

```
create eoa intf ifname eoa-97 lowif aal5-97
create eoa intf ifname eoa-98 lowif aal5-98
create eoa intf ifname eoa-99 lowif aal5-99
create eoa intf ifname eoa-100 lowif aal5-100
create eoa intf ifname eoa-101 lowif aal5-101
create eoa intf ifname eoa-102 lowif aal5-102
create eoa intf ifname eoa-103 lowif aal5-103
create eoa intf ifname eoa-104 lowif aal5-104
create eoa intf ifname eoa-105 lowif aal5-105
create eoa intf ifname eoa-106 lowif aal5-106
create eoa intf ifname eoa-107 lowif aal5-107
create eoa intf ifname eoa-108 lowif aal5-108
create eoa intf ifname eoa-109 lowif aal5-109
create eoa intf ifname eoa-110 lowif aal5-110
create eoa intf ifname eoa-111 lowif aal5-111
create eoa intf ifname eoa-112 lowif aal5-112
create eoa intf ifname eoa-113 lowif aal5-113
create eoa intf ifname eoa-114 lowif aal5-114
create eoa intf ifname eoa-115 lowif aal5-115
create eoa intf ifname eoa-116 lowif aal5-116
create eoa intf ifname eoa-117 lowif aal5-117
create eoa intf ifname eoa-118 lowif aal5-118
create eoa intf ifname eoa-119 lowif aal5-119
create eoa intf ifname eoa-120 lowif aal5-120
create eoa intf ifname eoa-121 lowif aal5-121
create eoa intf ifname eoa-122 lowif aal5-122
create eoa intf ifname eoa-123 lowif aal5-123
create eoa intf ifname eoa-124 lowif aal5-124
create eoa intf ifname eoa-125 lowif aal5-125
create eoa intf ifname eoa-126 lowif aal5-126
create eoa intf ifname eoa-127 lowif aal5-127
create eoa intf ifname eoa-128 lowif aal5-128
create eoa intf ifname eoa-129 lowif aal5-129
```

```
create eoa intf ifname eoa-130 lowif aal5-130
create eoa intf ifname eoa-131 lowif aal5-131
create eoa intf ifname eoa-132 lowif aal5-132
create eoa intf ifname eoa-133 lowif aal5-133
create eoa intf ifname eoa-134 lowif aal5-134
create eoa intf ifname eoa-135 lowif aal5-135
create eoa intf ifname eoa-136 lowif aal5-136
create eoa intf ifname eoa-137 lowif aal5-137
create eoa intf ifname eoa-138 lowif aal5-138
create eoa intf ifname eoa-139 lowif aal5-139
create eoa intf ifname eoa-140 lowif aal5-140
create eoa intf ifname eoa-141 lowif aal5-141
create eoa intf ifname eoa-142 lowif aal5-142
create eoa intf ifname eoa-143 lowif aal5-143
create eoa intf ifname eoa-144 lowif aal5-144
```

9.Создаем Bridge интерфейсы поверх созданных ЕоА интерфейсов для Voice услуги:

```
create bridge port intf portid 97 ifname eoa-97
create bridge port intf portid 98 ifname eoa-98
create bridge port intf portid 99 ifname eoa-99
create bridge port intf portid 100 ifname eoa-100
create bridge port intf portid 101 ifname eoa-101
create bridge port intf portid 102 ifname eoa-102
create bridge port intf portid 103 ifname eoa-103
create bridge port intf portid 104 ifname eoa-104
create bridge port intf portid 105 ifname eoa-105
create bridge port intf portid 106 ifname eoa-106
create bridge port intf portid 107 ifname eoa-107
create bridge port intf portid 108 ifname eoa-108
create bridge port intf portid 109 ifname eoa-109
create bridge port intf portid 110 ifname eoa-110
create bridge port intf portid 111 ifname eoa-111
create bridge port intf portid 112 ifname eoa-112
create bridge port intf portid 113 ifname eoa-113
create bridge port intf portid 114 ifname eoa-114
create bridge port intf portid 115 ifname eoa-115
create bridge port intf portid 116 ifname eoa-116
create bridge port intf portid 117 ifname eoa-117
create bridge port intf portid 118 ifname eoa-118
create bridge port intf portid 119 ifname eoa-119
create bridge port intf portid 120 ifname eoa-120
create bridge port intf portid 121 ifname eoa-121
create bridge port intf portid 122 ifname eoa-122
create bridge port intf portid 123 ifname eoa-123
create bridge port intf portid 124 ifname eoa-124
create bridge port intf portid 125 ifname eoa-125
create bridge port intf portid 126 ifname eoa-126
create bridge port intf portid 127 ifname eoa-127
create bridge port intf portid 128 ifname eoa-128
create bridge port intf portid 129 ifname eoa-129
create bridge port intf portid 130 ifname eoa-130
create bridge port intf portid 131 ifname eoa-131
```

```
create bridge port intf portid 132 ifname eoa-132
create bridge port intf portid 133 ifname eoa-133
create bridge port intf portid 134 ifname eoa-134
create bridge port intf portid 135 ifname eoa-135
create bridge port intf portid 136 ifname eoa-136
create bridge port intf portid 137 ifname eoa-137
create bridge port intf portid 138 ifname eoa-138
create bridge port intf portid 139 ifname eoa-139
create bridge port intf portid 140 ifname eoa-140
create bridge port intf portid 141 ifname eoa-141
create bridge port intf portid 142 ifname eoa-142
create bridge port intf portid 143 ifname eoa-143
create bridge port intf portid 144 ifname eoa-144
```

10.Создаем IRL профили для обеспечения гарантированной полосы пропускания Upstream для каждого из трех сервисов (Internet – 256Kbit/s, Voice – 256Kbit/s, IGMP - 128Kbit/s):

```
create irl profile profilename Inet irltype sr2cm cir 256 cbs 1000 conformation
colorgreen violateaction drop
create irl profile profilename VoIP irltype sr2cm cir 256 cbs 1000 conformation
colorgreen violateaction drop
create irl profile profilename IGMP irltype sr2cm cir 128 cbs 1000 conformation
colorgreen violateaction drop
```

11.Привязываем созданные IRL профили к нужным aal5 интерфейсам:

```
create irl map ifname aal5-1 profilename Inet
create irl map ifname aal5-2 profilename Inet
create irl map ifname aal5-3 profilename Inet
create irl map ifname aal5-4 profilename Inet
create irl map ifname aal5-5 profilename Inet
create irl map ifname aal5-6 profilename Inet
create irl map ifname aal5-7 profilename Inet
create irl map ifname aal5-8 profilename Inet
create irl map ifname aal5-9 profilename Inet
create irl map ifname aal5-10 profilename Inet
create irl map ifname aal5-11 profilename Inet
create irl map ifname aal5-12 profilename Inet
create irl map ifname aal5-13 profilename Inet
create irl map ifname aal5-14 profilename Inet
create irl map ifname aal5-15 profilename Inet
create irl map ifname aal5-16 profilename Inet
create irl map ifname aal5-17 profilename Inet
create irl map ifname aal5-18 profilename Inet
create irl map ifname aal5-19 profilename Inet
create irl map ifname aal5-20 profilename Inet
create irl map ifname aal5-21 profilename Inet
create irl map ifname aal5-22 profilename Inet
create irl map ifname aal5-23 profilename Inet
create irl map ifname aal5-24 profilename Inet
create irl map ifname aal5-25 profilename Inet
create irl map ifname aal5-26 profilename Inet
create irl map ifname aal5-27 profilename Inet
```



```
create irl map ifname aal5-132 profilename VoIP
create irl map ifname aal5-133 profilename VoIP
create irl map ifname aal5-134 profilename VoIP
create irl map ifname aal5-135 profilename VoIP
create irl map ifname aal5-136 profilename VoIP
create irl map ifname aal5-137 profilename VoIP
create irl map ifname aal5-138 profilename VoIP
create irl map ifname aal5-139 profilename VoIP
create irl map ifname aal5-140 profilename VoIP
create irl map ifname aal5-141 profilename VoIP
create irl map ifname aal5-142 profilename VoIP
create irl map ifname aal5-143 profilename VoIP
create irl map ifname aal5-144 profilename VoIP
```

12. Создаем профили для обеспечения гарантированной полосы пропускания Downstream

потоков для каждого из трех сервисов и указываем необходимые параметры. В данном случае для Интернет трафика выделено 256Kbit/s, IPTV – 12Mbit/s, Voice – 256 Kbit/s:

```
create sched profile info name ThreeServices algo custom iftype atm
modify sched profile class name ThreeServices classid 1 param1 10 param2 256
param3 256
modify sched profile class name ThreeServices classid 2 param1 10 param2 12288
param3 12288
modify sched profile class name ThreeServices classid 3 param1 10 param2 256
param3 256
```

13. Привязываем созданный профиль ко всем ATM интерфейсам DSLAM:

```
modify atm port ifname atm-1 profilename ThreeServices
modify atm port ifname atm-2 profilename ThreeServices
modify atm port ifname atm-3 profilename ThreeServices
modify atm port ifname atm-4 profilename ThreeServices
modify atm port ifname atm-5 profilename ThreeServices
modify atm port ifname atm-6 profilename ThreeServices
modify atm port ifname atm-7 profilename ThreeServices
modify atm port ifname atm-8 profilename ThreeServices
modify atm port ifname atm-9 profilename ThreeServices
modify atm port ifname atm-10 profilename ThreeServices
modify atm port ifname atm-11 profilename ThreeServices
modify atm port ifname atm-12 profilename ThreeServices
modify atm port ifname atm-13 profilename ThreeServices
modify atm port ifname atm-14 profilename ThreeServices
modify atm port ifname atm-15 profilename ThreeServices
modify atm port ifname atm-16 profilename ThreeServices
modify atm port ifname atm-17 profilename ThreeServices
modify atm port ifname atm-18 profilename ThreeServices
modify atm port ifname atm-19 profilename ThreeServices
modify atm port ifname atm-20 profilename ThreeServices
modify atm port ifname atm-21 profilename ThreeServices
modify atm port ifname atm-22 profilename ThreeServices
modify atm port ifname atm-23 profilename ThreeServices
modify atm port ifname atm-24 profilename ThreeServices
```

```
modify atm port ifname atm-25 profilename ThreeServices
modify atm port ifname atm-26 profilename ThreeServices
modify atm port ifname atm-27 profilename ThreeServices
modify atm port ifname atm-28 profilename ThreeServices
modify atm port ifname atm-29 profilename ThreeServices
modify atm port ifname atm-30 profilename ThreeServices
modify atm port ifname atm-31 profilename ThreeServices
modify atm port ifname atm-32 profilename ThreeServices
modify atm port ifname atm-33 profilename ThreeServices
modify atm port ifname atm-34 profilename ThreeServices
modify atm port ifname atm-35 profilename ThreeServices
modify atm port ifname atm-36 profilename ThreeServices
modify atm port ifname atm-37 profilename ThreeServices
modify atm port ifname atm-38 profilename ThreeServices
modify atm port ifname atm-39 profilename ThreeServices
modify atm port ifname atm-40 profilename ThreeServices
modify atm port ifname atm-41 profilename ThreeServices
modify atm port ifname atm-42 profilename ThreeServices
modify atm port ifname atm-43 profilename ThreeServices
modify atm port ifname atm-44 profilename ThreeServices
modify atm port ifname atm-45 profilename ThreeServices
modify atm port ifname atm-46 profilename ThreeServices
modify atm port ifname atm-47 profilename ThreeServices
modify atm port ifname atm-48 profilename ThreeServices
```

14. Настраиваем привязку трафик-классов к приоритетам входящих кадров.

Так как каждый Bridge интерфейс работает в своем VLAN и трафик приоритизирован

вышестоящим устройством (коммутатором) - каждый входящий кадр в конкретном VLAN уже имеет приоритет DSCP (либо 802.1p). Для удобства в рамках данного примера весь трафик (независимо от приоритета) помещается в нужную очередь на DSLAM. Дифференциация для постановки в нужную очередь производится путем включения необходимых Bridge интерфейсов в разные VLAN.

Так, интерфейсы с 1 по 48 используются для Internet сервиса, Bridge интерфейсы с 49 по 96 – для IPTV сервиса, Bridge интерфейсы с 97 по 144 – для Voice сервиса.

```
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 0
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 1
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 2
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 3
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 4
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 5
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 6
modify bridge port trfclassmap portid 1 trfClass 0 regenPrio 7
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 0
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 1
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 2
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 3
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 4
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 5
modify bridge port trfclassmap portid 2 trfClass 0 regenPrio 6
```


modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 7

15. Определяем приоритет (802.1p) для исходящих кадров для нормальной обработки на

приемной стороне (коммутаторе, к которому подключен DSLAM).

Bridge интерфейсы 1-48, service – Inet, VLAN21, 802.1p – 1, queue - 1

Bridge интерфейсы 49-96, service – IPTV, VLAN20, 802.1p – 5, queue - 5

Bridge интерфейсы 97-144, service – Voice, VLAN1, 802.1p – 6, queue – 6

```
modify bridge port prioinfo portid 1 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 2 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 3 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 4 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 5 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 6 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 7 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 8 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 9 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 10 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 11 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 12 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 13 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 14 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 15 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 16 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 17 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 18 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 19 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 20 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 21 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 22 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 23 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 24 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 25 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 26 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 27 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 28 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 29 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 30 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 31 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 32 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 33 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 34 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 35 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 36 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 37 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 38 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 39 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 40 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 41 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 42 defprio 1 numTrfClass 1
modify bridge port prioinfo portid 43 defprio 1 numTrfClass 1
```


16. Включаем все Bridge интерфейсы (с 1 по 144) в работу:

```
modify bridge port intf portid 1 status enable
modify bridge port intf portid 2 status enable
modify bridge port intf portid 3 status enable
modify bridge port intf portid 4 status enable
modify bridge port intf portid 5 status enable
modify bridge port intf portid 6 status enable
modify bridge port intf portid 7 status enable
modify bridge port intf portid 8 status enable
modify bridge port intf portid 9 status enable
modify bridge port intf portid 10 status enable
modify bridge port intf portid 11 status enable
modify bridge port intf portid 12 status enable
modify bridge port intf portid 13 status enable
modify bridge port intf portid 14 status enable
modify bridge port intf portid 15 status enable
modify bridge port intf portid 16 status enable
modify bridge port intf portid 17 status enable
modify bridge port intf portid 18 status enable
modify bridge port intf portid 19 status enable
modify bridge port intf portid 20 status enable
modify bridge port intf portid 21 status enable
modify bridge port intf portid 22 status enable
modify bridge port intf portid 23 status enable
modify bridge port intf portid 24 status enable
modify bridge port intf portid 25 status enable
modify bridge port intf portid 26 status enable
modify bridge port intf portid 27 status enable
modify bridge port intf portid 28 status enable
modify bridge port intf portid 29 status enable
modify bridge port intf portid 30 status enable
modify bridge port intf portid 31 status enable
modify bridge port intf portid 32 status enable
modify bridge port intf portid 33 status enable
modify bridge port intf portid 34 status enable
modify bridge port intf portid 35 status enable
modify bridge port intf portid 36 status enable
modify bridge port intf portid 37 status enable
modify bridge port intf portid 38 status enable
modify bridge port intf portid 39 status enable
modify bridge port intf portid 40 status enable
modify bridge port intf portid 41 status enable
modify bridge port intf portid 42 status enable
modify bridge port intf portid 43 status enable
modify bridge port intf portid 44 status enable
modify bridge port intf portid 45 status enable
modify bridge port intf portid 46 status enable
modify bridge port intf portid 47 status enable
modify bridge port intf portid 48 status enable
modify bridge port intf portid 49 status enable
modify bridge port intf portid 50 status enable
modify bridge port intf portid 51 status enable
```


modify bridge *port* intf portid 104 status enable
modify bridge *port* intf portid 105 status enable
modify bridge *port* intf portid 106 status enable
modify bridge *port* intf portid 107 status enable
modify bridge *port* intf portid 108 status enable
modify bridge *port* intf portid 109 status enable
modify bridge *port* intf portid 110 status enable
modify bridge *port* intf portid 111 status enable
modify bridge *port* intf portid 112 status enable
modify bridge *port* intf portid 113 status enable
modify bridge *port* intf portid 114 status enable
modify bridge *port* intf portid 115 status enable
modify bridge *port* intf portid 116 status enable
modify bridge *port* intf portid 117 status enable
modify bridge *port* intf portid 118 status enable
modify bridge *port* intf portid 119 status enable
modify bridge *port* intf portid 120 status enable
modify bridge *port* intf portid 121 status enable
modify bridge *port* intf portid 122 status enable
modify bridge *port* intf portid 123 status enable
modify bridge *port* intf portid 124 status enable
modify bridge *port* intf portid 125 status enable
modify bridge *port* intf portid 126 status enable
modify bridge *port* intf portid 127 status enable
modify bridge *port* intf portid 128 status enable
modify bridge *port* intf portid 129 status enable
modify bridge *port* intf portid 130 status enable
modify bridge *port* intf portid 131 status enable
modify bridge *port* intf portid 132 status enable
modify bridge *port* intf portid 133 status enable
modify bridge *port* intf portid 134 status enable
modify bridge *port* intf portid 135 status enable
modify bridge *port* intf portid 136 status enable
modify bridge *port* intf portid 137 status enable
modify bridge *port* intf portid 138 status enable
modify bridge *port* intf portid 139 status enable
modify bridge *port* intf portid 140 status enable
modify bridge *port* intf portid 141 status enable
modify bridge *port* intf portid 142 status enable
modify bridge *port* intf portid 143 status enable
modify bridge *port* intf portid 144 status enable

17. Определяем членство портов в VLAN.

VLAN 1 – Voice,

VLAN 20 – IPTV,

VLAN 21 – Internet.

modify vlan static vlanid 1 egressports 385 97 98 99 100 101 102 103 104 105 106
107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126
127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144
untaggedports 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113
114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133

```

134 135 136 137 138 139 140 141 142 143 144 igmpsnoopaction drop
create vlan static vlnname vlan20 vlnid 20 egressports 385 49 50 51 52 53 54
55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81
82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 untaggedports 49 50 51 52 53 54 55
56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82
83 84 85 86 87 88 89 90 91 92 93 94 95 96
create vlan static vlnname vlan21 vlnid 21 egressports 385 1 2 3 4 5 6 7 8 9
10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
37 38 39 40 41 42 43 44 45 46 47 48 untaggedports 1 2 3 4 5 6 7 8 9 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 igmpsnoopaction drop

```

18.Изменяем принадлежность untagged Bridge интерфейсов к VLAN.

Интерфейсы с 1 по 48 – VLAN 21,
Интерфейсы с 49 по 96 – VLAN 20,
Интерфейсы с 97 по 144 – VLAN 1.

```

modify gvrp port info portid 1 portvlanid 21
modify gvrp port info portid 2 portvlanid 21
modify gvrp port info portid 3 portvlanid 21
modify gvrp port info portid 4 portvlanid 21
modify gvrp port info portid 5 portvlanid 21
modify gvrp port info portid 6 portvlanid 21
modify gvrp port info portid 7 portvlanid 21
modify gvrp port info portid 8 portvlanid 21
modify gvrp port info portid 9 portvlanid 21
modify gvrp port info portid 10 portvlanid 21
modify gvrp port info portid 11 portvlanid 21
modify gvrp port info portid 12 portvlanid 21
modify gvrp port info portid 13 portvlanid 21
modify gvrp port info portid 14 portvlanid 21
modify gvrp port info portid 15 portvlanid 21
modify gvrp port info portid 16 portvlanid 21
modify gvrp port info portid 17 portvlanid 21
modify gvrp port info portid 18 portvlanid 21
modify gvrp port info portid 19 portvlanid 21
modify gvrp port info portid 20 portvlanid 21
modify gvrp port info portid 21 portvlanid 21
modify gvrp port info portid 22 portvlanid 21
modify gvrp port info portid 23 portvlanid 21
modify gvrp port info portid 24 portvlanid 21
modify gvrp port info portid 25 portvlanid 21
modify gvrp port info portid 26 portvlanid 21
modify gvrp port info portid 27 portvlanid 21
modify gvrp port info portid 25 portvlanid 21
modify gvrp port info portid 29 portvlanid 21
modify gvrp port info portid 30 portvlanid 21
modify gvrp port info portid 31 portvlanid 21
modify gvrp port info portid 32 portvlanid 21
modify gvrp port info portid 33 portvlanid 21
modify gvrp port info portid 34 portvlanid 21
modify gvrp port info portid 35 portvlanid 21

```



```
modify gvrp port info portid 140 portvlanid 1
modify gvrp port info portid 141 portvlanid 1
modify gvrp port info portid 142 portvlanid 1
modify gvrp port info portid 143 portvlanid 1
modify gvrp port info portid 144 portvlanid 1
```

19.Создаем фильтр для перемаркировки значения DSCP для Internet сервиса (Upstream).

В качестве значения DSCP используется «CS1». В данном примере маркируется весь пользовательский IP трафик (с default ToS значением). Примечание: для маркировки

трафика, инкапсулированного в PPP нужно к подправилу «create *filter* subrule ip ruleid 5 subruleid 1 srcaddrmp any» добавить опцию «transporthdr pppe»:

```
create filter rule entry ruleid 5 description DSCP_Inet_Up action modifytos
actionval 0x20 actionmask 0xff
create filter subrule ip ruleid 5 subruleid 1 toscmp any
modify filter rule entry ruleid 5 statsstatus enable status enable
```

20.Создаем фильтр для перемаркировки значения DSCP для IPTV сервиса (Upstream).

В качестве значения DSCP используется «CS5». В данном примере маркируется весь пользовательский IP трафик (IGMP).

```
create filter rule entry ruleid 6 description DSCP_IGMP_Up action modifytos
actionval 0xA0 actionmask 0xff
create filter subrule ip ruleid 6 subruleid 1 toscmp any
modify filter rule entry ruleid 6 statsstatus enable status enable
```

21.Создаем фильтр для перемаркировки значения DSCP для VoIP сервиса (Upstream).

В качестве значения DSCP используется «CS6». В данном примере маркируется весь пользовательский IP трафик (Voice).

```
create filter rule entry ruleid 7 description DSCP_VoIP_Up action modifytos
actionval 0xC0 actionmask 0xff
create filter subrule ip ruleid 7 subruleid 1 toscmp any
modify filter rule entry ruleid 7 statsstatus enable status enable
```

22.Создаем фильтры для перемаркировки значения DSCP для всех трех сервисов в направлении Downstream. В рамках данного примера предполагается, что трафик приходит с вышестоящего коммутатора уже промаркированным:

Internet: CS1

IPTV: CS5

VoIP: CS6

Далее в соотствии с DSCP значением DSLAM производит перемаркировку значения 802.1p (так называемый «внутренний приоритет»), связывает каждый тип трафика в соответствии с «внутренним» приоритетом 802.1p с нужным классом, после чего трафик

в соответствии с классом получает гарантированную полосу пропускания на АТМ уровне. Таким образом обеспечивается полноценное качество обслуживания.

```
create filter rule entry ruleid 8 description DSCP_Inet_Down action setprio
priority 1 ruledir in
create filter subrule ip ruleid 8 subruleid 1 tosfrom 0x20 tosmask 0xff toscmp eq
```

```

modify filter rule entry ruleid 8 statsstatus enable status enable
create filter rule entry ruleid 9 description DSCP_IGMP_Down action setprio
priority 5 ruledir in
create filter subrule ip ruleid 9 subruleid 1 tosfrom 0xA0 tosmask 0xff toscmp eq
modify filter rule entry ruleid 9 statsstatus enable status enable
create filter rule entry ruleid 10 description DSCP_VoIP_Down action setprio
priority 6 ruledir in
create filter subrule ip ruleid 10 subruleid 1 tosfrom 0xC0 tosmask 0xff toscmp eq
modify filter rule entry ruleid 10 statsstatus enable status enable

```

Дополнение: в качестве значений в правилах нужно указывать ToS в hex формате.

Таблица соответствий:

```

"CS0" = DSCP - 0x00, ToS - 0x00
"CS1" = DSCP - 0x08, ToS - 0x20
"CS2" = DSCP - 0x10, ToS - 0x40
"CS3" = DSCP - 0x18, ToS - 0x60
"CS4" = DSCP - 0x20, ToS - 0x80
"CS5" = DSCP - 0x28, ToS - 0xA0
"CS6" = DSCP - 0x30, ToS - 0xC0
"CS7" = DSCP - 0x38, ToS - 0xE0
"BE" = DSCP - 0x00, ToS - 0x00
"AF11" = DSCP - 0x0a, ToS - 0x28
"AF12" = DSCP - 0x0c, ToS - 0x30
"AF13" = DSCP - 0x0e, ToS - 0x38
"AF21" = DSCP - 0x12, ToS - 0x48
"AF22" = DSCP - 0x14, ToS - 0x50
"AF23" = DSCP - 0x16, ToS - 0x58
"AF31" = DSCP - 0x1a, ToS - 0x68
"AF32" = DSCP - 0x1c, ToS - 0x70
"AF33" = DSCP - 0x1e, ToS - 0x78
"AF41" = DSCP - 0x22, ToS - 0x88
"AF42" = DSCP - 0x24, ToS - 0x90
"AF43" = DSCP - 0x26, ToS - 0x98
"EF" = DSCP - 0x2e, ToS - 0xB8

```

23. После создания и активации правил их необходимо привязать к нужным EoA (Upstream приоритезация) и Uplink (Downstream приоритезация) интерфейсам:

```

create filter rule map ruleid 5 ifname eoa-1 stageid 1
create filter rule map ruleid 5 ifname eoa-2 stageid 1
create filter rule map ruleid 5 ifname eoa-3 stageid 1
create filter rule map ruleid 5 ifname eoa-4 stageid 1
create filter rule map ruleid 5 ifname eoa-5 stageid 1
create filter rule map ruleid 5 ifname eoa-6 stageid 1
create filter rule map ruleid 5 ifname eoa-7 stageid 1
create filter rule map ruleid 5 ifname eoa-8 stageid 1
create filter rule map ruleid 5 ifname eoa-9 stageid 1
create filter rule map ruleid 5 ifname eoa-10 stageid 1
create filter rule map ruleid 5 ifname eoa-11 stageid 1
create filter rule map ruleid 5 ifname eoa-12 stageid 1
create filter rule map ruleid 5 ifname eoa-13 stageid 1
create filter rule map ruleid 5 ifname eoa-14 stageid 1

```



```
create filter rule map ruleid 7 ifname eoa-119 stageid 1
create filter rule map ruleid 7 ifname eoa-120 stageid 1
create filter rule map ruleid 7 ifname eoa-121 stageid 1
create filter rule map ruleid 7 ifname eoa-122 stageid 1
create filter rule map ruleid 7 ifname eoa-123 stageid 1
create filter rule map ruleid 7 ifname eoa-124 stageid 1
create filter rule map ruleid 7 ifname eoa-125 stageid 1
create filter rule map ruleid 7 ifname eoa-126 stageid 1
create filter rule map ruleid 7 ifname eoa-127 stageid 1
create filter rule map ruleid 7 ifname eoa-128 stageid 1
create filter rule map ruleid 7 ifname eoa-129 stageid 1
create filter rule map ruleid 7 ifname eoa-130 stageid 1
create filter rule map ruleid 7 ifname eoa-131 stageid 1
create filter rule map ruleid 7 ifname eoa-132 stageid 1
create filter rule map ruleid 7 ifname eoa-133 stageid 1
create filter rule map ruleid 7 ifname eoa-134 stageid 1
create filter rule map ruleid 7 ifname eoa-135 stageid 1
create filter rule map ruleid 7 ifname eoa-136 stageid 1
create filter rule map ruleid 7 ifname eoa-137 stageid 1
create filter rule map ruleid 7 ifname eoa-138 stageid 1
create filter rule map ruleid 7 ifname eoa-139 stageid 1
create filter rule map ruleid 7 ifname eoa-140 stageid 1
create filter rule map ruleid 7 ifname eoa-141 stageid 1
create filter rule map ruleid 7 ifname eoa-142 stageid 1
create filter rule map ruleid 7 ifname eoa-143 stageid 1
create filter rule map ruleid 7 ifname eoa-144 stageid 1
create filter rule map ruleid 8 ifname eth-1 stageid 1
create filter rule map ruleid 9 ifname eth-1 stageid 1
create filter rule map ruleid 10 ifname eth-1 stageid 1
```

24. Удаляем привязку правила IGMP со всех интерфейсов:
delete *filter* rule map ruleid 1 stageid 1 ifname all

25. Создаем привязку правила IGMP к необходимым интерфейсам (IPTV сервис):

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eth-1
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-49
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-50
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-51
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-52
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-53
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-54
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-55
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-56
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-57
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-58
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-59
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-60
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-61
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-62
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-63
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-64
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-65
```

create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-66
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-67
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-68
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-69
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-70
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-71
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-72
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-73
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-74
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-75
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-76
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-77
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-78
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-79
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-80
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-81
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-82
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-83
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-84
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-85
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-86
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-87
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-88
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-89
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-90
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-91
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-92
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-93
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-94
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-95
create *filter* rule map ruleid 1 stageid 1 orderid 1 ifname eoa-96

26. Включаем IGMP глобально на устройстве:

```
modify igmpsnoop cfg info status enable
```

27. Включаем IGMP в настройках 385-го Bridge интерфейса (Uplink):

```
modify igmpsnoop port info portid 385 querierstatus enable leavemode fast status enable
```

28. Включаем IGMP в настройках абонентских Bridge интерфейсов:

```
modify igmpsnoop port info portid 49 leavemode fast status enable  
modify igmpsnoop port info portid 50 leavemode fast status enable  
modify igmpsnoop port info portid 51 leavemode fast status enable  
modify igmpsnoop port info portid 52 leavemode fast status enable  
modify igmpsnoop port info portid 53 leavemode fast status enable  
modify igmpsnoop port info portid 54 leavemode fast status enable  
modify igmpsnoop port info portid 55 leavemode fast status enable  
modify igmpsnoop port info portid 56 leavemode fast status enable  
modify igmpsnoop port info portid 57 leavemode fast status enable  
modify igmpsnoop port info portid 58 leavemode fast status enable  
modify igmpsnoop port info portid 59 leavemode fast status enable  
modify igmpsnoop port info portid 60 leavemode fast status enable
```

modify igmpsnoop *port* info portid 61 leavemode fast status enable
modify igmpsnoop *port* info portid 62 leavemode fast status enable
modify igmpsnoop *port* info portid 63 leavemode fast status enable
modify igmpsnoop *port* info portid 64 leavemode fast status enable
modify igmpsnoop *port* info portid 65 leavemode fast status enable
modify igmpsnoop *port* info portid 66 leavemode fast status enable
modify igmpsnoop *port* info portid 67 leavemode fast status enable
modify igmpsnoop *port* info portid 68 leavemode fast status enable
modify igmpsnoop *port* info portid 69 leavemode fast status enable
modify igmpsnoop *port* info portid 70 leavemode fast status enable
modify igmpsnoop *port* info portid 71 leavemode fast status enable
modify igmpsnoop *port* info portid 72 leavemode fast status enable
modify igmpsnoop *port* info portid 73 leavemode fast status enable
modify igmpsnoop *port* info portid 74 leavemode fast status enable
modify igmpsnoop *port* info portid 75 leavemode fast status enable
modify igmpsnoop *port* info portid 76 leavemode fast status enable
modify igmpsnoop *port* info portid 77 leavemode fast status enable
modify igmpsnoop *port* info portid 78 leavemode fast status enable
modify igmpsnoop *port* info portid 79 leavemode fast status enable
modify igmpsnoop *port* info portid 80 leavemode fast status enable
modify igmpsnoop *port* info portid 81 leavemode fast status enable
modify igmpsnoop *port* info portid 82 leavemode fast status enable
modify igmpsnoop *port* info portid 83 leavemode fast status enable
modify igmpsnoop *port* info portid 84 leavemode fast status enable
modify igmpsnoop *port* info portid 85 leavemode fast status enable
modify igmpsnoop *port* info portid 86 leavemode fast status enable
modify igmpsnoop *port* info portid 87 leavemode fast status enable
modify igmpsnoop *port* info portid 88 leavemode fast status enable
modify igmpsnoop *port* info portid 89 leavemode fast status enable
modify igmpsnoop *port* info portid 90 leavemode fast status enable
modify igmpsnoop *port* info portid 91 leavemode fast status enable
modify igmpsnoop *port* info portid 92 leavemode fast status enable
modify igmpsnoop *port* info portid 93 leavemode fast status enable
modify igmpsnoop *port* info portid 94 leavemode fast status enable
modify igmpsnoop *port* info portid 95 leavemode fast status enable
modify igmpsnoop *port* info portid 96 leavemode fast status enable

29.Создаем профиль ADSL линии с учетом того, чтобы обеспечить полосу пропускания

для всех трех сервисов.

В качестве ADSL стандарта используется ADSL2+.

Downstream: $256+256+12288 = 13312$ Kbit/s (с некоторым запасом).

Upstream: $256+256+256 = 800$ Kbit/s (с некоторым запасом).

```
create profile entry name NEW stdtype adsl2plus mode dynamic type interleave  
dsmaxrate 13312 usmaxrate 800
```

30.Привязываем созданный профиль ко всем ADSL портам:

```
modify profile map name NEW port 1  
modify profile map name NEW port 2  
modify profile map name NEW port 3  
modify profile map name NEW port 4  
modify profile map name NEW port 5
```

modify profile map name NEW port 6
modify profile map name NEW port 7
modify profile map name NEW port 8
modify profile map name NEW port 9
modify profile map name NEW port 10
modify profile map name NEW port 11
modify profile map name NEW port 12
modify profile map name NEW port 13
modify profile map name NEW port 14
modify profile map name NEW port 15
modify profile map name NEW port 16
modify profile map name NEW port 17
modify profile map name NEW port 18
modify profile map name NEW port 19
modify profile map name NEW port 20
modify profile map name NEW port 21
modify profile map name NEW port 22
modify profile map name NEW port 23
modify profile map name NEW port 24
modify profile map name NEW port 25
modify profile map name NEW port 26
modify profile map name NEW port 27
modify profile map name NEW port 28
modify profile map name NEW port 29
modify profile map name NEW port 30
modify profile map name NEW port 31
modify profile map name NEW port 32
modify profile map name NEW port 33
modify profile map name NEW port 34
modify profile map name NEW port 35
modify profile map name NEW port 36
modify profile map name NEW port 37
modify profile map name NEW port 38
modify profile map name NEW port 39
modify profile map name NEW port 40
modify profile map name NEW port 41
modify profile map name NEW port 42
modify profile map name NEW port 43
modify profile map name NEW port 44
modify profile map name NEW port 45
modify profile map name NEW port 46
modify profile map name NEW port 47
modify profile map name NEW port 48

31.Сохраняем настройки DSLAM:
commit

2.Пример настройки DAS3 series DSLAM для предоставления трех сервисов (Интернет, Voice и Видео) с использованием упрощенного CLI режима (usermode).

Используем ту же задачу, что и в предыдущем примере, но с использованием упрощенного режима (режима макрокоманд) там где это возможно. В остальных случаях также используются команды инженерно CLI режима.

1. Настройка Uplink интерфейсов и management VLAN

```
# usermode
/ config
/config> ge
/config/ge> set ge1 ip 192.168.10.35 mask 255.255.255.0
/config/ge>exit
/config>mgmt
/config/mgmt> vlan-id
/config/mgmt/vlan-id> set ge1 vlanid 21
/config/mgmt/vlan-id> top
```

2.Удаляем созданные в default конфигурации интерфейсы, и создаем стек интерфейсов с новыми VPI/VCI. Заодно создаем VLAN для Bridge интерфейсов 1-48, определяем членство в нем интерфейсов и приоритет 802.1p по умолчанию:

```
/config
/config> pvc
/config/pvc/del 1-48 8 35
/config/pvc/ add eoa 1-48 10 40 vlanid 21 priority 1 vlantag off
```

3.Создаем интерфейсы для IPTV услуги. Заодно создаем VLAN для Bridge интерфейсов 25-48, определяем членство в нем интерфейсов и приоритет 802.1p по умолчанию:

```
/config/pvc/ add eoa 1-48 10 50 vlanid 20 priority 5 vlantag off
```

4.Создаем интерфейсы для Voice услуги:

```
/config/pvc/ add eoa 1-48 10 60 vlanid 1 priority 6 vlantag off
/config/pvc/exit
```

5.Определяем членство Uplink портов в VLAN

```
/config>vlan
/config/vlan>ge
/config/vlan/ge>del ge1 vlanid 1
/config/vlan/ge>del ge2 vlanid 1
/config/vlan/ge>add ge1 vlanid 1 tag on
/config/vlan/ge>add ge1 vlanid 20 tag on
/config/vlan/ge>add ge1 vlanid 21 tag on
```

6. Удаляем привязку правила IGMP со всех интерфейсов:

```
/engmode
```

```
delete filter rule map ruleid 1 stageid 1 ifname all
```

7. Создаем привязку правила IGMP к необходимым интерфейсам (IPTV сервис):

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eth-1
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-49
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-50
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-51
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-52
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-53
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-54
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-55
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-56
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-57
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-58
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-59
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-60
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-61
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-62
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-63
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-64
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-65
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-66
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-67
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-68
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-69
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-70
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-71
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-72
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-73
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-74
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-75
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-76
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-77
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-78
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-79
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-80
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-81
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-82
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-83
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-84
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-85
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-86
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-87
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-88
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-89
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-90
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-91
```

```
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-92
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-93
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-94
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-95
create filter rule map ruleid 1 stageid 1 orderid 1 ifname eoa-96
```

8. Включаем IGMP в настройках 385-го Bridge интерфейса (Uplink):

```
#usermode
/config/igmpsnoop>ge
/config/igmpsnoop/ge> set ge1 leavemode fast querier on
```

9. Включаем IGMP в настройках абонентских Bridge интерфейсов:

```
/config/igmpsnoop/ge>exit
/config/igmpsnoop>pvc
/config/igmpsnoop/pvc>enable 1-48 10 50
/config/igmpsnoop/pvc>set 1-48 10 50 leavemode fast
/config/igmpsnoop/pvc>top
```

10. Включаем IGMP глобально на устройстве:

```
/config
/config> igmpsnoop
/config/igmpsnoop>enable
```

11. Создаем профиль ADSL линии с учетом того, чтобы обеспечить полосу пропускания

для всех трех сервисов.

В качестве ADSL стандарта используется ADSL2+.

Downstream: $256+256+12288 = 13312$ Kbit/s (с некоторым запасом).

Upstream: $256+256+256 = 800$ Kbit/s (с некоторым запасом).

```
/config
/config> profile
/config/profile>add name NEW stdtype adsl2plus mode dynamic type interleaved
dsmaxrate 13312 usmaxrate 800
```

12. Привязываем созданный профиль ко всем ADSL портам:

```
/config/profile>exit
/config> port
/config/port >set dsl-profile name NEW 1-48
```

14. Настраиваем привязку трафик-классов к приоритетам входящих кадров.

Так как каждый Bridge интерфейс работает в своем VLAN и трафик приоритизирован

вышестоящим устройством (коммутатором) - каждый входящий кадр в конкретном VLAN уже имеет приоритет DSCP (либо 802.1p). Для удобства в рамках данного примера весь трафик (независимо от приоритета) помещается в нужную очередь на DSLAM. Дифференциация для постановки в нужную очередь производится путем включения необходимых Bridge интерфейсов в разные VLAN.

Так, интерфейсы с 1 по 48 используются для Internet сервиса, Bridge интерфейсы с 49

modify bridge *port* trfclassmap portid 142 trfClass 2 regenPrio 6
modify bridge *port* trfclassmap portid 142 trfClass 2 regenPrio 7
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 0
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 1
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 2
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 3
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 4
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 5
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 6
modify bridge *port* trfclassmap portid 143 trfClass 2 regenPrio 7
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 0
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 1
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 2
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 3
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 4
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 5
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 6
modify bridge *port* trfclassmap portid 144 trfClass 2 regenPrio 7

15. Определяем приоритет (802.1p) для исходящих кадров для нормальной обработки на

приемной стороне (коммутаторе, к которому подключен DSLAM).

Bridge интерфейсы 1-48, service – Inet, VLAN21, 802.1p – 1, queue - 1

Bridge интерфейсы 49-96, service – IPTV, VLAN20, 802.1p – 5, queue - 5

Bridge интерфейсы 97-144, service – Voice, VLAN1, 802.1p – 6, queue – 6

modify bridge *port* prioinfo portid 1 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 2 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 3 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 4 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 5 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 6 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 7 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 8 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 9 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 10 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 11 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 12 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 13 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 14 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 15 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 16 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 17 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 18 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 19 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 20 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 21 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 22 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 23 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 24 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 25 defprio 1 numTrfClass 1
modify bridge *port* prioinfo portid 26 defprio 1 numTrfClass 1


```
modify bridge port prioinfo portid 131 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 132 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 133 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 134 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 135 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 136 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 137 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 138 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 139 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 140 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 141 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 142 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 143 defprio 6 numTrfClass 6
modify bridge port prioinfo portid 144 defprio 6 numTrfClass 6
```

16.Создаем фильтр для перемаркировки значения DSCP для Internet сервиса (Upstream).

В качестве значения DSCP используется «CS1». В данном примере маркируется весь пользовательский IP трафик (с default ToS значением). Примечание: для маркировки

трафика, инкапсулированного в PPP нужно к подправилу «create *filter* subrule ip ruleid 5 subruleid 1 srcaddrcmp any» добавить опцию «transporthdr pppoe»:

```
create filter rule entry ruleid 5 description DSCP_Inet_Up action modifytos
actionval 0x20 actionmask 0xff
create filter subrule ip ruleid 5 subruleid 1 toscmp any
modify filter rule entry ruleid 5 statsstatus enable status enable
```

17.Создаем фильтр для перемаркировки значения DSCP для IPTV сервиса (Upstream).

В качестве значения DSCP используется «CS5». В данном примере маркируется весь пользовательский IP трафик (IGMP).

```
create filter rule entry ruleid 6 description DSCP_IGMP_Up action modifytos
actionval 0xA0 actionmask 0xff
create filter subrule ip ruleid 6 subruleid 1 toscmp any
modify filter rule entry ruleid 6 statsstatus enable status enable
```

18.Создаем фильтр для перемаркировки значения DSCP для VoIP сервиса (Upstream). В качестве значения DSCP используется «CS6». В данном примере маркируется весь пользовательский IP трафик (Voice).

```
create filter rule entry ruleid 7 description DSCP_VoIP_Up action modifytos
actionval 0xC0 actionmask 0xff
create filter subrule ip ruleid 7 subruleid 1 toscmp any
modify filter rule entry ruleid 7 statsstatus enable status enable
```

18.Создаем фильтры для перемаркировки значения DSCP для всех трех сервисов в направлении Downstream. В рамках данного примера предполагается, что трафик приходит с вышестоящего коммутатора уже промаркированным:

Internet: CS1

IPTV: CS5

VoIP: CS6

Далее в соответствии с DSCP значением DSLAM производит перемаркировку значения 802.1p (так называемый «внутренний приоритет»), связывает каждый тип трафика в соответствии с «внутренним» приоритетом 802.1p с нужным классом, после чего трафик

в соответствии с классом получает гарантированную полосу пропускания на ATM уровне. Таким образом обеспечивается полноценное качество обслуживания.

```
create filter rule entry ruleid 8 description DSCP_Inet_Down action setprio
priority 1 ruledir in
create filter subrule ip ruleid 8 subruleid 1 tosfrom 0x20 tosmask 0xff toscmp eq
modify filter rule entry ruleid 8 statsstatus enable status enable
create filter rule entry ruleid 9 description DSCP_IGMP_Down action setprio
priority 5 ruledir in
create filter subrule ip ruleid 9 subruleid 1 tosfrom 0xA0 tosmask 0xff toscmp eq
modify filter rule entry ruleid 9 statsstatus enable status enable
create filter rule entry ruleid 10 description DSCP_VoIP_Down action setprio
priority 6 ruledir in
create filter subrule ip ruleid 10 subruleid 1 tosfrom 0xC0 tosmask 0xff toscmp eq
modify filter rule entry ruleid 10 statsstatus enable status enable
```

Дополнение: в качестве значений в правилах нужно указывать ToS в hex формате.

Таблица соответствий:

```
"CS0" = DSCP - 0x00, ToS - 0x00
"CS1" = DSCP - 0x08, ToS - 0x20
"CS2" = DSCP - 0x10, ToS - 0x40
"CS3" = DSCP - 0x18, ToS - 0x60
"CS4" = DSCP - 0x20, ToS - 0x80
"CS5" = DSCP - 0x28, ToS - 0xA0
"CS6" = DSCP - 0x30, ToS - 0xC0
"CS7" = DSCP - 0x38, ToS - 0xE0
"BE" = DSCP - 0x00, ToS - 0x00
"AF11" = DSCP - 0x0a, ToS - 0x28
"AF12" = DSCP - 0x0c, ToS - 0x30
"AF13" = DSCP - 0x0e, ToS - 0x38
"AF21" = DSCP - 0x12, ToS - 0x48
"AF22" = DSCP - 0x14, ToS - 0x50
"AF23" = DSCP - 0x16, ToS - 0x58
"AF31" = DSCP - 0x1a, ToS - 0x68
"AF32" = DSCP - 0x1c, ToS - 0x70
"AF33" = DSCP - 0x1e, ToS - 0x78
"AF41" = DSCP - 0x22, ToS - 0x88
"AF42" = DSCP - 0x24, ToS - 0x90
"AF43" = DSCP - 0x26, ToS - 0x98
"EF" = DSCP - 0x2e, ToS - 0xB8
```

19. После создания и активации правил их необходимо привязать к нужным EoA (Upstream приоритезация) и Uplink (Downstream приоритезация) интерфейсам:

```
create filter rule map ruleid 5 ifname eoa-1 stageid 1
create filter rule map ruleid 5 ifname eoa-2 stageid 1
create filter rule map ruleid 5 ifname eoa-3 stageid 1
```



```
create filter rule map ruleid 7 ifname eoa-108 stageid 1
create filter rule map ruleid 7 ifname eoa-109 stageid 1
create filter rule map ruleid 7 ifname eoa-110 stageid 1
create filter rule map ruleid 7 ifname eoa-111 stageid 1
create filter rule map ruleid 7 ifname eoa-112 stageid 1
create filter rule map ruleid 7 ifname eoa-113 stageid 1
create filter rule map ruleid 7 ifname eoa-114 stageid 1
create filter rule map ruleid 7 ifname eoa-115 stageid 1
create filter rule map ruleid 7 ifname eoa-116 stageid 1
create filter rule map ruleid 7 ifname eoa-117 stageid 1
create filter rule map ruleid 7 ifname eoa-118 stageid 1
create filter rule map ruleid 7 ifname eoa-119 stageid 1
create filter rule map ruleid 7 ifname eoa-120 stageid 1
create filter rule map ruleid 7 ifname eoa-121 stageid 1
create filter rule map ruleid 7 ifname eoa-122 stageid 1
create filter rule map ruleid 7 ifname eoa-123 stageid 1
create filter rule map ruleid 7 ifname eoa-124 stageid 1
create filter rule map ruleid 7 ifname eoa-125 stageid 1
create filter rule map ruleid 7 ifname eoa-126 stageid 1
create filter rule map ruleid 7 ifname eoa-127 stageid 1
create filter rule map ruleid 7 ifname eoa-128 stageid 1
create filter rule map ruleid 7 ifname eoa-129 stageid 1
create filter rule map ruleid 7 ifname eoa-130 stageid 1
create filter rule map ruleid 7 ifname eoa-131 stageid 1
create filter rule map ruleid 7 ifname eoa-132 stageid 1
create filter rule map ruleid 7 ifname eoa-133 stageid 1
create filter rule map ruleid 7 ifname eoa-134 stageid 1
create filter rule map ruleid 7 ifname eoa-135 stageid 1
create filter rule map ruleid 7 ifname eoa-136 stageid 1
create filter rule map ruleid 7 ifname eoa-137 stageid 1
create filter rule map ruleid 7 ifname eoa-138 stageid 1
create filter rule map ruleid 7 ifname eoa-139 stageid 1
create filter rule map ruleid 7 ifname eoa-140 stageid 1
create filter rule map ruleid 7 ifname eoa-141 stageid 1
create filter rule map ruleid 7 ifname eoa-142 stageid 1
create filter rule map ruleid 7 ifname eoa-143 stageid 1
create filter rule map ruleid 7 ifname eoa-144 stageid 1
create filter rule map ruleid 8 ifname eth-1 stageid 1
create filter rule map ruleid 9 ifname eth-1 stageid 1
create filter rule map ruleid 10 ifname eth-1 stageid 1
```

20.Создаем IRL профили для обеспечения гарантированной полосы пропускания для каждого из трех сервисов:

```
create irl profile profilename Inet irltype sr2cm cir 256 cbs 1000 conformation
colorgreen violateaction drop
create irl profile profilename VoIP irltype sr2cm cir 256 cbs 1000 conformation
colorgreen violateaction drop
create irl profile profilename IGMP irltype sr2cm cir 128 cbs 400 conformation
colorgreen violateaction drop
```

21.Привязываем созданные IRL профили к нужным aal5 интерфейсам:

```
create irl map ifname aal5-1 profilename Inet
create irl map ifname aal5-2 profilename Inet
create irl map ifname aal5-3 profilename Inet
create irl map ifname aal5-4 profilename Inet
create irl map ifname aal5-5 profilename Inet
create irl map ifname aal5-6 profilename Inet
create irl map ifname aal5-7 profilename Inet
create irl map ifname aal5-8 profilename Inet
create irl map ifname aal5-9 profilename Inet
create irl map ifname aal5-10 profilename Inet
create irl map ifname aal5-11 profilename Inet
create irl map ifname aal5-12 profilename Inet
create irl map ifname aal5-13 profilename Inet
create irl map ifname aal5-14 profilename Inet
create irl map ifname aal5-15 profilename Inet
create irl map ifname aal5-16 profilename Inet
create irl map ifname aal5-17 profilename Inet
create irl map ifname aal5-18 profilename Inet
create irl map ifname aal5-19 profilename Inet
create irl map ifname aal5-20 profilename Inet
create irl map ifname aal5-21 profilename Inet
create irl map ifname aal5-22 profilename Inet
create irl map ifname aal5-23 profilename Inet
create irl map ifname aal5-24 profilename Inet
create irl map ifname aal5-25 profilename Inet
create irl map ifname aal5-26 profilename Inet
create irl map ifname aal5-27 profilename Inet
create irl map ifname aal5-28 profilename Inet
create irl map ifname aal5-29 profilename Inet
create irl map ifname aal5-30 profilename Inet
create irl map ifname aal5-31 profilename Inet
create irl map ifname aal5-32 profilename Inet
create irl map ifname aal5-33 profilename Inet
create irl map ifname aal5-34 profilename Inet
create irl map ifname aal5-35 profilename Inet
create irl map ifname aal5-36 profilename Inet
create irl map ifname aal5-37 profilename Inet
create irl map ifname aal5-38 profilename Inet
create irl map ifname aal5-39 profilename Inet
create irl map ifname aal5-40 profilename Inet
create irl map ifname aal5-41 profilename Inet
create irl map ifname aal5-42 profilename Inet
create irl map ifname aal5-43 profilename Inet
create irl map ifname aal5-44 profilename Inet
create irl map ifname aal5-45 profilename Inet
create irl map ifname aal5-46 profilename Inet
create irl map ifname aal5-47 profilename Inet
create irl map ifname aal5-48 profilename Inet
create irl map ifname aal5-49 profilename IGMP
create irl map ifname aal5-50 profilename IGMP
create irl map ifname aal5-51 profilename IGMP
```



```
create irl map ifname aal5-104 profilename VoIP
create irl map ifname aal5-105 profilename VoIP
create irl map ifname aal5-106 profilename VoIP
create irl map ifname aal5-107 profilename VoIP
create irl map ifname aal5-108 profilename VoIP
create irl map ifname aal5-109 profilename VoIP
create irl map ifname aal5-110 profilename VoIP
create irl map ifname aal5-111 profilename VoIP
create irl map ifname aal5-112 profilename VoIP
create irl map ifname aal5-113 profilename VoIP
create irl map ifname aal5-114 profilename VoIP
create irl map ifname aal5-115 profilename VoIP
create irl map ifname aal5-116 profilename VoIP
create irl map ifname aal5-117 profilename VoIP
create irl map ifname aal5-118 profilename VoIP
create irl map ifname aal5-119 profilename VoIP
create irl map ifname aal5-120 profilename VoIP
create irl map ifname aal5-121 profilename VoIP
create irl map ifname aal5-122 profilename VoIP
create irl map ifname aal5-123 profilename VoIP
create irl map ifname aal5-124 profilename VoIP
create irl map ifname aal5-125 profilename VoIP
create irl map ifname aal5-126 profilename VoIP
create irl map ifname aal5-127 profilename VoIP
create irl map ifname aal5-128 profilename VoIP
create irl map ifname aal5-129 profilename VoIP
create irl map ifname aal5-130 profilename VoIP
create irl map ifname aal5-131 profilename VoIP
create irl map ifname aal5-132 profilename VoIP
create irl map ifname aal5-133 profilename VoIP
create irl map ifname aal5-134 profilename VoIP
create irl map ifname aal5-135 profilename VoIP
create irl map ifname aal5-136 profilename VoIP
create irl map ifname aal5-137 profilename VoIP
create irl map ifname aal5-138 profilename VoIP
create irl map ifname aal5-139 profilename VoIP
create irl map ifname aal5-140 profilename VoIP
create irl map ifname aal5-141 profilename VoIP
create irl map ifname aal5-142 profilename VoIP
create irl map ifname aal5-143 profilename VoIP
create irl map ifname aal5-144 profilename VoIP
```

22. Создаем профили для обеспечения гарантированной полосы пропускания Downstream

потоков для каждого из трех сервисов и указываем необходимые параметры. В данном случае для Интернет трафика выделено 256Kbit/s, IPTV – 12Mbit/s, Voice – 256 Kbit/s:

```
create sched profile info name ThreeServices algo custom iftype atm
modify sched profile class name ThreeServices classid 1 param1 10 param2 256
param3 256
modify sched profile class name ThreeServices classid 2 param1 10 param2 12288
```

param3 12288

modify sched profile class name ThreeServices classid 3 param1 10 param2 256

param3 256

23.Привязываем созданный профиль ко всем АТМ интерфейсам DSLAM:

```
modify atm port ifname atm-1 profilename ThreeServices
modify atm port ifname atm-2 profilename ThreeServices
modify atm port ifname atm-3 profilename ThreeServices
modify atm port ifname atm-4 profilename ThreeServices
modify atm port ifname atm-5 profilename ThreeServices
modify atm port ifname atm-6 profilename ThreeServices
modify atm port ifname atm-7 profilename ThreeServices
modify atm port ifname atm-8 profilename ThreeServices
modify atm port ifname atm-9 profilename ThreeServices
modify atm port ifname atm-10 profilename ThreeServices
modify atm port ifname atm-11 profilename ThreeServices
modify atm port ifname atm-12 profilename ThreeServices
modify atm port ifname atm-13 profilename ThreeServices
modify atm port ifname atm-14 profilename ThreeServices
modify atm port ifname atm-15 profilename ThreeServices
modify atm port ifname atm-16 profilename ThreeServices
modify atm port ifname atm-17 profilename ThreeServices
modify atm port ifname atm-18 profilename ThreeServices
modify atm port ifname atm-19 profilename ThreeServices
modify atm port ifname atm-20 profilename ThreeServices
modify atm port ifname atm-21 profilename ThreeServices
modify atm port ifname atm-22 profilename ThreeServices
modify atm port ifname atm-23 profilename ThreeServices
modify atm port ifname atm-24 profilename ThreeServices
modify atm port ifname atm-25 profilename ThreeServices
modify atm port ifname atm-26 profilename ThreeServices
modify atm port ifname atm-27 profilename ThreeServices
modify atm port ifname atm-28 profilename ThreeServices
modify atm port ifname atm-29 profilename ThreeServices
modify atm port ifname atm-30 profilename ThreeServices
modify atm port ifname atm-31 profilename ThreeServices
modify atm port ifname atm-32 profilename ThreeServices
modify atm port ifname atm-33 profilename ThreeServices
modify atm port ifname atm-34 profilename ThreeServices
modify atm port ifname atm-35 profilename ThreeServices
modify atm port ifname atm-36 profilename ThreeServices
modify atm port ifname atm-37 profilename ThreeServices
modify atm port ifname atm-38 profilename ThreeServices
modify atm port ifname atm-39 profilename ThreeServices
modify atm port ifname atm-40 profilename ThreeServices
modify atm port ifname atm-41 profilename ThreeServices
modify atm port ifname atm-42 profilename ThreeServices
modify atm port ifname atm-43 profilename ThreeServices
modify atm port ifname atm-44 profilename ThreeServices
modify atm port ifname atm-45 profilename ThreeServices
modify atm port ifname atm-46 profilename ThreeServices
modify atm port ifname atm-47 profilename ThreeServices
modify atm port ifname atm-48 profilename ThreeServices
```

24.Сохраняем настройки DSLAM:

```
commit
```

