

BDCOM P3310B в IPoE сети со схемой S-VLAN

Предпосылки использования устройства

Разумеется, самое очевидное, это цена устройства. Ни для кого не секрет, что на интернет-рынке в России ситуация с ценами для конечных абонентов далека от идеальной: ежегодно приходится увеличивать каналы, затраты операторов растут, а вот абонентская база совершенно к этому не стремится, уже всё построено до нас. Единственное, куда остается расти, частный сектор. А в чем проблема частного сектора? В том, что там негде поставить узел и классический, всем знакомый ethernet развертывать просто банально сложно. Нужны термошкафы, нужно электричество, нужно место под это всё. Построив пару поселков с "узлами у абонентов" и поняв, что эксплуатировать это совершенно невозможно, практически все приходят к использованию технологии xPON. И, разумеется, начинаются муки выбора. По факту, вендоров, представленных на Связь-Экспоком, либо встретившихся на просторах shop.nag.ru, не так то и много.

- Eltex
- Imaqliq
- Dasan
- BDCOM

Они так и идут по цене, в этом порядке. Конечно же, небольшой оператор выбирает GePON. Почему? Читаем первое предложение - из-за цифры около знака \$. Но цена, это половина беды. Кроме неё есть еще наши любимые, технические нюансы при внедрении и эксплуатации.

Технические возможности и трудности выбора

А вот здесь начинается самое интересное. Сейчас самая популярная технология доступа это IPoE, выдача IP-адресов средствами DHCP. Исторически так сложилось, что наша компания внедрила всю эту модняшную тему до того, как сообщество пришло к самой адекватной схеме "vlan per user", поэтому у нас, так называемый "s-vlan", он же "vlan на дом", "vlan на свитч" и, в случае с PON-ом, "vlan на olt". Это накладывает некоторого рода ограничения на оборудование по его интеллектуальности. В свитчах, это, так называемый, L2+ функционал. Самое главное - dhcp relay opt82, acl или dhcp snooping, для выдачи адреса на конкретный порт и фиксации его против возможной подмены.

Понимая чего мы хотим, начинаем перебирать вендоров:

Eltex - Ок, ребята, мы сейчас дадим вам программера, вы с ним всё решите. Две недели и у нас есть прошивка, в которую дописан dhcp opt 82. Кроме того, в устройстве на тот момент Eltex LTE-8ST, есть dhcp\arp snooping.

Imaqliq - Э-э? Что вам нужно? У нас этого нет, никому вроде не надо. Справедливости ради, отмечу, что они, вроде бы, написали этот функционал через пару лет, но нам стали не интересны. Цена устройства была аналогична новосибирским парням (eltex).

Dasan - 翻译? Что-что? Ах, будем общаться через переводчика? Так, посмотрим... Our RND check your requirement. But, the feedback is negative. Ну что же, спасибо за помощь.

BDCOM - 翻译? Снова переводчик? Здесь хочется остановиться и сказать ребятам из shop.nag.ru "спасибо". Всё-таки саппорт хоть какой-то, но есть. Очень доволен решением не брать устройство на стороне, а обратиться к уже знакомым. Пару проблем решили. Сейчас меня закидают камнями: дескать, наши украинские коллеги обсосали все проблемы по десять раз и все костыли известны. Возможно, вы правы, выбирайте сами. Я прочитал local.com.ua, нашел мало реально полезной информации, разве что "epon dba hardware cycletime 25000 discovery-frequency 60 discovery-length 1024" было полезным (уменьшает время отклика и позволяет работать неким сторонним onu). Ну да я отвлекся. Функционал dhcp opt82 поддерживается, dhcp snooping есть, static acl есть. Прекрасно.

Резюмируем. У нас два вендора, предлагающих примерно одинаковые возможности Eltex и BDCOM. Что нам говорит коммерческий отдел? Он говорит нам:

Элтекс за один порт: 48 тыс. рублей

BDCOM за один порт 15 тыс. рублей

Я ошибся, даже при нынешнем курсе ЭЛТЕКС в ТРИ раза дороже BDCOM!

* **Примечание.** [Цитата](#) от 6 декабря 2014.

Начинаем интеграцию

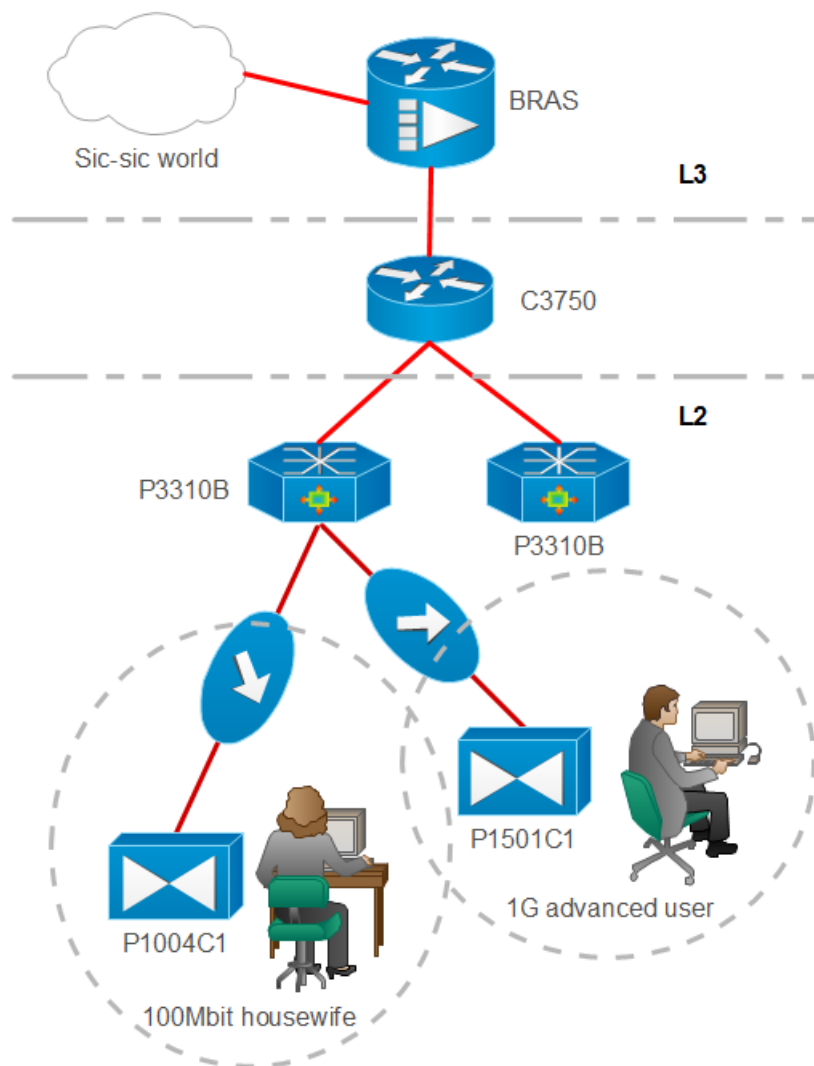
Лирика заканчивается, начинается реальная работа. Устройство P3310B на столе, в комплекте две ONU P1501C1 и P1004C1, гигабитная с одним портом, и 100-мбитная с четырьмя.



Как я уже отмечал, у нас “s-vlan”. Схема элементарная. Есть роутер, где кучка вланов с L3-интерфейсами, они приходят на OLT и пробрасываются прямо до порта, куда включен абонент. Далее ему выдается IP и всё это уходит на L3-connected BRAS. Выданный ip фиксируется на ONU. Все счастливы.

Разумеется, первым делом мы обновляем OLT до последней FW. На момент написания статьи это [10.1.0B 21324](#).

```
#copy tftp: flash: x.x.x.x
Source file name[]?bdcom/3314_en_21324.bin
Destination file name[bdc0m/3314_en_21324.bin]?Switch.bin
#reboot
```



Базовый конфиг устройства

! ### Необходимые базовые сервисы

```
service timestamps log date
service timestamps debug date
service password-encryption
```

!

! ### Задаем адрес syslog-сервера

```
logging 172.16.0.2
logging buffered 131072
logging buffered informational
```

!

```
hostname BDTEST
```

!

```
ip default-gateway 172.16.12.1
```

!

```
no spanning-tree
```

!

! ### Нафиг нетбиос и dhcp-серверы со стороны клиентов

```
ip access-list extended subs.filter
deny tcp any any eq 135
deny tcp any any eq 136
deny tcp any any eq 137
deny tcp any any eq 138
deny tcp any any eq 445
deny udp any any eq 68
permit ip any any
```

!

! ### По умолчанию разрешим людям получать адреса по DHCP

```
ip access-list extended sub-DUMMY
```

```

permit udp any eq 68 any eq 67
deny ip any any
!
! ### Уменьшает пинг, разрешает работу некоторых сторонних ONU
epon dba hardware cycletime 25000 discovery-frequency 60 discovery-length 1024
!
aaa authentication login default local
aaa authentication enable default none
aaa authorization exec default local
!
username admin password password
!
! ### Базовый конфиг ONU, который будет применен к свежеподключенным ONU
epon onu-config-template ots
! ### Разрешим максимум 10 маков на абонентском порту
cmd-sequence 1 switchport port-security mode dynamic
cmd-sequence 2 switchport port-security dynamic maximum 10
! ### Гостевой-блокировочный vlan по умолчанию, тут можно и s-vlan указать по сути.
! ### Это специфика нашей сети.
cmd-sequence 3 epon onu all-port ctc vlan mode tag 1261
! ### Мальтикаст vlan, максимум 5 групп на порт
cmd-sequence 4 epon onu all-port ctc mcst mc-vlan add 1251
cmd-sequence 5 epon onu all-port ctc mcst tag-stripe enable
cmd-sequence 6 epon onu all-port ctc mcst max-group-number 5
! ### Ловим петли
cmd-sequence 7 epon onu all-port loopback detect
! ### Блокируем всё, кроме DHCP по-умолчанию
cmd-sequence 8 epon onu all-port ip access-group sub-DUMMY
!
!
interface GigaEthernet0/1
description Uplink Copper
switchport trunk vlan-allowed 1201,1251,1261,2201,3201
switchport trunk vlan-untagged none
switchport mode trunk
! ### Это очень важный момент, здесь обязательно нужно указать мальтикаст vlan!
switchport pvid 1251
dhcp snooping trust
no shutdown
!
interface GigaEthernet0/2
!
interface GigaEthernet0/3
description Uplink Fiber
switchport trunk vlan-allowed 1201,1251,1261,2201,3201
switchport trunk vlan-untagged none
switchport mode trunk
switchport pvid 1251
dhcp snooping trust
no shutdown
!
interface GigaEthernet0/4
interface GigaEthernet0/5
interface GigaEthernet0/6
!
interface EPON0/1
! ### По умолчанию будем применять профиль с именем ots для всех свежеподключенных ону
epon pre-config-template ots binded-onu-llid 1-64
! ### Кинем туда все вланы кроме управляющего
switchport trunk vlan-allowed 1251,1261,2201,3201
switchport mode trunk
! ### Фильтруем всю левоту
ip access-group subs.filter
no shutdown
!
! ### Аналогично
interface EPON0/2
interface EPON0/3

```

```

interface EPON0/4
! ### Аналогично
!
interface VLAN1201
description Management Interface
ip address 172.16.12.10 255.255.255.0
!
vlan 1201
name vlan1201
!
vlan 1251
name vlan1251
!
vlan 1261
name vlan1261
!
vlan 2201
name vlan2201
!
vlan 3201
name vlan3201
!
vlan 1,1201,1251,1261,2201,3201
!
ip mcst enable
ip mcst timer router-age 600
ip mcst timer response-time 120
ip mcst series-connection
!
! ### Перечисляем используемые нами multicast-группы в iptv
ip mcst mc-vlan 1251 range 237.5.1.7 - 237.5.1.9 , 237.5.1.11 - 237.5.1.17 , 237.5.1.19 - 237.5.1.22 ,
237.5.1.25 - 237.5.1.27
ip mcst mc-vlan 1251 range 237.5.1.29 - 237.5.1.30 , 237.5.1.50 , 237.5.1.60 , 237.5.1.70
!
! ### Включим снупинг для истории. Фактически, работать он не будет
ip dhcp-relay snooping
ip dhcp-relay snooping vlan 1261,2201,3201
ip dhcp-relay snooping database-agent 172.16.0.2
ip dhcp-relay snooping db-file bdcom/fc:fa:f7:c9:fc:1c-leases
!
! ### /srv/tftp/bdcom/fc:fa:f7:c9:fc:1c-leases ; chmod 666 /srv/tftp/bdcom/fc:fa:f7:c9:fc:1c-leases
!
ip dhcp-relay snooping write-immediately
! ### Будем перехватывать запросы абонентов к DHCP-серверу и перенаправлять на наш локальный
relay, где уже умная система сама выдаст правильный адрес. Формат опции см. ниже
ip dhcp-relay snooping information option format hn-type host
ip dhcp-relay agent
ip dhcp-relay helper-address 172.16.0.3 vlan 1261,2201,3201
!
! ### Выше везде указываем абонентские vlan-ы. Если классический s-vlan, то он будет один. У нас
три из-за специфики
!
! ### Первым делом это выключается на всех устройствах. Не заходил даже.
ip http language english
no ip http server
!
!
snmp-server community 0 community RW
!
!
time-zone Moscow 3 0
snmp master 3
snmp server 172.16.0.2
no snmp master
!

```

Что делать после регистрации абонента

Применив этот базовый конфиг с небольшими изменениями под себя, мы получаем рабочий вариант системы. Как только мы подключим первую ONU, то получим нижеследующее. Для простоты возьмем гигабитную ONU.

```
!  
interface EPON0/1:1  
onu-configuration  
switchport port-security dynamic maximum 10  
switchport port-security mode dynamic  
epon onu port 1 ctc vlan mode tag 1261  
epon onu port 1 loopback detect  
epon onu port 1 ip access-group sub-DUMMY  
epon onu port 1 ctc mcst tag-stripe enable  
epon onu port 1 ctc mcst mc-vlan add 1251  
epon onu port 1 ctc mcst max-group-number 5  
!!onu-configuration-end  
!
```

Т.е. применится наш шаблон с именем 'ots'.

Как только мы это увидим, можем начинать донастройку. В частности, нам требуется переключить vlan с гостевого на абонентский, и повесить правильный access-list на клиентский порт.

```
!  
ip access-list extended sub-FCFAF7D8BC92  
permit ip 10.228.17.5 255.255.255.255 any  
permit ip 10.143.0.0 255.255.0.0 any  
permit udp any eq 68 any eq 67  
!  
interface EPON0/1:1  
epon onu port 1 ctc vlan mode tag 2201  
epon onu port 1 ip access-group sub-FCFAF7D8BC92  
!
```

Все эти операции реально автоматизировать через snmp или телнет. Таких деталей я раскрывать не буду, скажу лишь, что это вполне реально.

Формат опции 82

В ходе посиделок со снифером был разобран формат опции 82 в типе 'hn-type host'. В скобках фактические байты пакета, начиная с самой опции 82. Мы определяем абонента по mac-адресу ONU, поэтому этот формат нам подходит больше всего.

```
[52] - Опция 82  
[27] - Длина данных опции 82  
[01] - Под-опция номер 1 (agent circuit id) опции 82  
[05] - Длина под-опции 1  
[0001000702] - Данные о номере "порта" на OLT, точно не знаю как распарсить  
[02] - Подопция номер 2 (agent remote id) опции 82  
[06] - Длина подопции 2  
[fcfaf7d854b7] - MAC ONU  
[09] - Подопция номер 9 опции 82  
  
[15] - Длина данных всей подопции  
[00000cf8] - Код вендора (3320)  
[10] - Длина данных хоста  
[01] - Код 1  
[00] - Длина данных в коде 1  
[02] - Код 2  
[06] - Длина данных в коде 2  
[424454455354] - hostname устройства (BDTEST)  
[03] - Код 3  
[04] - Длина данных в коде 3  
[ac100c0a] - IP-адрес хоста (172.16.12.10)
```

Как побегать вокруг ARP\DHCP Snooping-a

Чисто теоретически, идея хорошая. Через внутренний DHCP-relay проходит запрос DHCPACK, и

устройство OLT узнает, что конкретному абоненту выдан конкретный адрес. Ничего не мешает начать блокировать остальные пакеты, в которых отличается либо ip, либо mac. Очень удобно. В теории. На практике порождает ряд проблем:

- Нельзя использовать статические адреса. Только DHCP. Всякие хитрые (кривые) роутеры идут лесом, пользователи с windows 98 туда же. Это редко бывает проблемой, но если вы любите цеплять юриков в обычную абонентскую сеть, то может ею стать.
- После перезагрузки OLT нужно помнить какие адреса были кому выданы, иначе у клиентов всё сломается, трафик перестанет ходить, в саппорте увеличится кол-во звонков и так далее.

Мы давным-давно отказались даже от попыток использовать эту красивую динамику на обычных коммутаторах, и никаких сомнений не осталось при интеграции BDCOM - только статические ACL. Надежно, дубово, но, разумеется, есть нюансы (небольшая ремарка: Eltex до сих пор не может сделать статические acl и, похоже, не собирается этим заниматься).

Как почувствовать нашу любовь

Тот момент, когда я реально не пожалел, что всё-таки обратился в shop.nag.ru. Был написан ACL, открывающий доступ только для нужных мне адресов, который должен быть навешен на оконечный порт ONU:

```
ip access-list extended sub-FCFAF7D8BC92
! ### прибить абонентский ip, с которого он может попасть в интернет
permit ip 10.228.17.5 255.255.255.255 any
! ### разрешить подсеть, в которой висят stb, их может быть много и все авторизации идут на портале.
permit ip 10.143.0.0 255.255.0.0 any
! ### разрешить dhcp-запросы от клиентов
permit udp any eq 68 any eq 67
!
```

И, разумеется, он не заработал. Ни на одной из ONU, ни на гиговой, ни на сотке. Точнее заработал, но частично. Всё, что не /32, не работает, т.е. в примере выше работали правила 1 и 3. Но мне обязательно нужна подсеть! Что делать? Писать в support@nag.ru.

Я очень не люблю туда писать, т.к. имею негативный опыт многочасового переливания из пустого в порожнее, но выбора нет, это лучше чем полностью ничего. Прошло несколько сессий терапии, запросов к китайцам, проверок, и проблема решилась. Чтобы заработало правило 2, подсети 'le /32', нужно перешивать абонентские устройства ONU.

P1004C1 - до версии 10.0.16A 1030
P1501C1 - до версии 10.0.17A 1017

К величайшему сожалению, автоматического обновления прошивок ONU у BDCOM-а нет. В этом плане Eltex снова впереди. Поэтому садимся, и пишем код, который будет делать это автоматически. Ну, или обновляем руками:

```
epon update onu image 1004C1.zblob interface EPON0/1:1
```

Ждем 1.5 минуты и подтверждаем перешивку:

```
epon commit-onu-image-update interface EPON0/1:1
```

Файлы прошивок нужно положить на флешку OLT. По какой-то причине китайцы зажали поставить копеечную флешку на "побольше", поэтому нужные нам файлы умещаются только с прошивкой olt 21324.

```
1 olt.blob <FILE> 626580 WED MAR 12 14:14:52 2014
3 startup-config <FILE> 30092 TUE DEC 16 19:00:08 2014
5 ifindex-config <FILE> 224 TUE DEC 16 19:00:18 2014
4 1004C1.zblob <FILE> 551286 TUE JAN 11 01:08:12 2106
0 Switch.bin <FILE> 5716247 TUE JUN 04 01:37:10 2075
6 1501C1.zblob <FILE> 498486 TUE DEC 16 11:28:24 2014
free space 294912
```

Как попрыгать около multicast vlan

В этом вопросе китайцы тоже отличились. Они считают, что каналов в iptv может быть не больше 256

и мультикаст-группы обязаны идти по порядку. Т.е. вы не можете написать "ip mcst mc-vlan 1251 range 237.1.0.1 - 237.5.1.254".

Придется писать через запятую каждую, фактически, нужную вам группу. Ну, или снова садимся писать код и подставляем костыль. Опять-таки, можно использовать как telnet, так и snmp. Подскажу лишь oid для добавления или удаления - .1.3.6.1.4.1.3320.101.5.1.1.3.'.\$mcastvlan.'.'.\$group

Промежуточные результаты

Появление на российском рынке дешевого PON-решения оказалось существенно более поздним, нежели наше желание построить пассивную сеть, поэтому все быстрые и вкусные поселки висят на Eltex. На текущий момент, на новых OLT от BDCOM количество абонентов на устройство составляет далекое от желаемого число. В силу этой причины, нельзя сказать однозначно о надежности рассматриваемого устройства. Наша статистика говорит ровно об одном обращении в техническую поддержку за 3 месяца эксплуатации 2-х головных станций на сети.

Тишков Андрей
Главный инженер,
<http://www.ots-net.ru>