CLIPS how to…

Что такое CLIPS?

Термин CLIPS означает Connectionless IP Session, т.е. абонент, работающий без установки соединения как в случае с PPP, например. CLIPS абонент подразумевает, в общем случае, тип инкапсуляции IPoE (IP over Ethernet). SmartEdge различает два способа работы с IPoE абонентами:

1. DHCP абонент, т.е. абонент получающий IP адрес по протоколу DHCP, при этом SmartEdge обязательно является непосредственным участником DHCP диалога. Такой способ в SmartEdge называется Dynamic CLIPS.
2. Абонент уже имеющий статичный IP-адрес. Основным отличием такого типа CLIPS доступа является то, что SmartEdge не участвует в назначении IP адреса для абонента. Но сам IP адрес для данного абонента всегда известен и не меняется. Такой способ доступа в SmartEdge называется Static CLIPS.

С точки зрения архитектуры операционной системы SEOS, абонент CLIPS является одним из типов абонентских circuit.

OK, а что такое Circuit?

На уровне операционной системы, SmartEdge вводит универсальную единицу измерения – circuit. Все действия связанные с применением различных полиси, списков доступа, QoS, манипуляций с адресами (вплоть до привязки IP адресов) и пр., осуществляются на уровне circuit. Circuit – это не только абонент, но и порт, VLAN, стэкированный VLAN, тоннель GRE и т.п. Данная архитектурная особенность позволяет полностью абстрагироваться от способов инкапсуляции и осуществлять обработку пакетов на универсальном уровне. Что это означает на практике? Например, раньше был тип доступа DSL с ATM аплинками, потом аплинки стали делать на базе Ethernet, сегодня ШПД строят на Ethernet коммутаторах и т.д. Меняются инкапсуляции и порты на BRAS-е/маршрутизаторе но на фундаментальном уровне в системе не происходит никаких изменений, т.к. для SmartEdge вся обработка пакетов и правил реализуется на уровне circuit. Это также позволяет организовать максимальную прозрачность функционала для абонентов с различным типом доступа, например, а также наделяет систему прочими полезными качествами.

SmartEdge, Dynamic CLIPS и DHCP

Как уже отмечалось ранее, Dynamic CLIPS означает, что IPoE абонент получает IP адрес по протоколу DHCP, при этом SmartEdge участвует в этом процессе. В свою очередь это означает три возможных режима работы SmartEdge с точки зрения DHCP взаимодействия:

1. SmartEdge как DHCP Proxy. В этом режиме SmartEdge проксирует все сообщения между клиентом и сервером т.е. участвует во всех стадиях: обнаружение (Discover/Offer), получение (Request/Replay) и обновление/завершение (Renew/Release).
2. SmartEdge как DHCP Relay. В таком режиме SmartEdge ведет себя как обычный DHCP Relay, т.е. участвует во всех стадиях обнаружения и получения, за исключением стадии обновление/завершение (Renew/Release).
3. SmartEdge как DHCP Server. В этом режиме SmartEdge выполняет роль DHCP сервера.

На практике наиболее применяемыми являются два режима работы SmartEdge – DHCP Proxy и DHCP Server.

Отличительной особенностью SmartEdge является возможность работы с DHCP абонентами как через L2 сеть, так и через L3 сеть доступа. Участвуя в DHCP диалоге непосредственно, SmartEdge самостоятельно определяет то, как физически абонент взаимодействует с сетью: через L2 или через L3. В случае если сеть доступа L2, то единственное, что нужно гарантировать в сети доступа, это доставку посылаемых абонентами

широковещательных запросов DHCP Discover до интерфейсов SmartEdge, т.е. SmartEdge и DHCP клиент должны находится в одном бродкастовом домене. SmartEdge для DHCP клиента в этом случае является IP шлюзом. В случае если есть доступа L3, то доставка DHCP Discover от клиента до SmartEdge осуществляется обычно при помощи L3 Relay-ев. Т.е. сеть доступа сегментирована L3 устройствами, клиент взаимодействует по L2 с сетью доступа как обычно, посылая бродкастовый DHCP Discover, который транслируется в юникаст ближайшим устройством L3 Relay, и доставляется до SmartEdge. С точки зрения DHCP, для клиента, L3 Relay является IP шлюзом, а IP адрес SmartEdge указывается в качестве DHCP сервера в настройках самого L3 Relay.

Механизм Binding, а также взаимоотношения между Context, Interface, Port и Circuit

Прежде чем переходить к конкретным примерам по настройке SmartEdge, следует несколько слов уделить деталям того, как соотносятся друг с другом интерфейсы, порты и IP адреса в SmartEdge.

Context в SmartEdge представляет собой виртуальный маршрутизатор, т.е. это полноценный маршрутизатор в котором могут быть определены свои собственные интерфейсы, IP адреса, абоненты, запущены свои протоколы маршрутизации, определены свои администраторы, запущены действующие только в рамках этого контекста дебаги и т.п.

В традиционном маршрутизаторе понятия порт и интерфейс обычно означают одно и тоже. В SmartEdge это не так. Например, у нас есть порт Ethernet 1/5, и я хочу прописать ему IP адрес 192.168.1.1/24. Для этого я сначала должен выбрать/создать context (т.е. виртуальный маршрутизатор) где будет жить этот IP, а потом «привязать» (т.е. сделать bind) данный порт с IP адресом к этому контексту. Именно для этого в SmartEdge существуют интерфейсы, более того, названия этим интерфейсам придумывает сам администратор ☺. Итак, обратимся к описанному примеру, вот так это выглядит в CLI:

```
!
context Router-A        <= Создаем контекст и придумываем ему имя
!
 interface inf-to-the-core        <= Придумываем имя интерфейса
  description Bound to port eth1/5
  ip address 192.168.1.1/24
!
!
! ** End Context **
!
port ethernet 1/5
 no shutdown
 bind interface inf-to-the-core Router-A     <= Тут осуществляется «привязка»
!
```

Таким образом, получается, что традиционное понятие port в SmartEdge весьма условное и служит для того, чтобы не загромождать CLI непонятными сущностями, и дать общее представление о том, где контрено, находится этот port физически в шасси, т.к. port eth 5/1 – это тоже circuit (см. описание circuit выше). Т.е. в общем случае виртуальный маршрутизатор на момент создания не имеет вообще никаких интерфейсов, администратор сам создает интерфейсы, давая им удобные для его понимания названия, назначает этим интерфейсам IP адреса и прочие параметры, а потом делает привязку физических портов, VLAN-ов, PVC и прочих circuit-ов, к этим интерфейсам и контекстам. Этот процесс называется binding. Работая со SmartEdge, всегда следует помнить одно правило, каждый конкретный circuit может быть

привязан только к одному контексту в каждый момент времени, т.е. сделать bind для circuit-а в два и более контекста одновременно невозможно.

Статический и динамический Bind

Привязка или bind того или иного circuit к контексту и интерфейсу с IP адресом может быть статичной или динамичной. Пример в параграфе выше описывает статичный способ привязки. Это характерно, например, для интерфейсов аплинков, если говорить о BRAS-овом применении SmartEdge. Также в BRAS-овом приложении SmartEdge используется динамичный bind, в основном для так называемых абонентских circuit. На сегодняшний день в SmartEdge различают следующие основные типа абонентских circuit: PPPoE/PPPoA, DHCP CLIPS, L2TP LNS, Static CLIPS. Динамичный bind означает, что привязка абонента выполняется не администратором, как в случае привязки аплинков, например, а по наступлению определенных событий. Самый простой пример – это абонент PPPoE, так до того как SmartEdge услышал PADI отправленный с определенного MAC адреса, такого абонента нет в системе, а, следовательно, и нет соответствующего circuit. В этот момент SmartEdge начинает создавать circuit для данного абонента и, основываясь на конфигурации, а также информации получаемой от AAA соответственно выполняет bind. После завершения сессии, circuit разрушается и bind удаляется из памяти.

Контекст local

Как уже отмечалось ранее, SmartEdge работает с виртуальными маршрутизаторами или контекстами, которые создает администратор. В системе всегда есть как минимум один контекст, а также среди контекстов есть своего рода иерархия. Контекст local – всегда присутствует в системе и не может быть удален.

AAA в SmartEdge

Работая с абонентами, SmartEdge вовлекает RADIUS для аутентификации, авторизации и аккаунтинга. Поскольку может быть несколько контекстов, то в каждом контексте может быть определен свой набор AAA серверов, с которыми он работает. Контекст аутентификации (или контекст в котором прописаны RADIUS сервера) может быть указан непосредственно в конфигурации, например, VLAN-а доступа, тогда все абонентские сессии, приходящие в этом VLAN, будут авторизованы через AAA этого контекста. Если нет явных указаний, то контекст может быть выбран по структурированному username, например ivanov@homenet, в этом случае SmartEdge будет искать контекст homenet и использовать RADIUS сервера этого контекста для авторизации этого пользователя. Если username не структурированный и контекст аутентификации не был указан на уровне порта или VLAN-а дотсупа, то SmartEdge не сможет определить контекст. Для этих целей существует контекст “aaa last resort” в “global” конфигурации. “Global” конфигурация не принадлежит никакому контексту и служит своего рода логическим ресурсом для динамической привязки абонентов к тому или иному контексту в случае условий описанных выше. В этом случае RADIUS возвращает Context-Name VSA на момент аутентификации, сообщая SmartEdge к кому контексту должен быть привязан данный абонентский circuit.

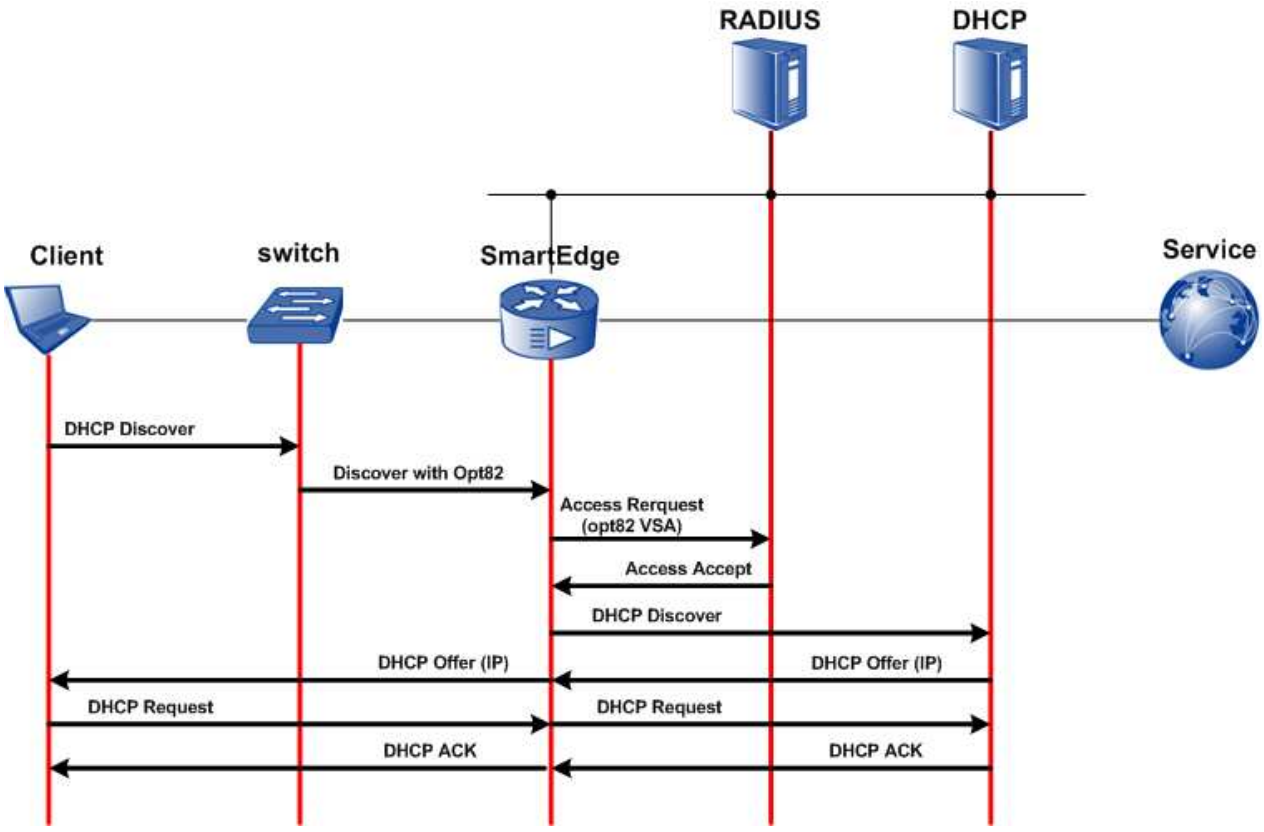
Таким образом, для рассматриваемых ниже примеров будет использоваться следующая конфигурация AAA.

```
!
!*определяем глобальные методы AAA для subscriber, определяя в качестве
!*контекста аутентификации и аккаунтинга контекст local
aaa global authentication subscriber radius context local
aaa global accounting subscriber radius context local
!
!*назначаем контекст local на роль aaa last-resort
```

```
aaa last-resort context local
!
!
context local
!
aaa authentication subscriber global
aaa accounting subscriber global
!
radius accounting server 30.0.0.1 encrypted-key 9B75C092F5241D6F
radius coa server 30.0.0.1 encrypted-key 9B75C092F5241D6F port 3799
radius server 30.0.0.1 encrypted-key 9B75C092F5241D6F
!
!
! ** End Context **
!
```

Сценарий Dynamic CLIPS с динамичными IP

На диаграмме ниже представлено базовое взаимодействие для данного сценария.



Аутентификация выполняется RADIUS сервером, а назначение IP адреса производится посредством внешнего DHCP сервера. Будет рассмотрен случай, когда аутентификация будет осуществляться на базе DHCP Option 82 (т.е. двух ее сабопциях Agent-Circuit-Id и Agent-Remote-Id). Назначение IP адреса контролируется внешним DHCP сервером, и осуществляется для данного примера стандартным для ISC-DHCP сервера способом.

Ниже представлена минимальная конфигурация, которую необходимо сделать на SmartEdge для описанного примера (предполагается, что AAA блок уже настроен, как показано в параграфе выше).

```
!
context local
!
!*создаем multibind интерфейс, это своего рода шаблон для абонентских
!*circuit, здесь же указываем, что этот интерфейс будет работать как
!*Proxy для DHCP запросов
 interface CLIPS-SUBS-001 multibind
  ip address 10.111.255.253/16
  dhcp proxy 65535
!
 interface mgmt
  ip address 30.0.0.10/24
!
 interface uplink0
  ip address 10.0.13.6/30
!
!*указываем IP адрес DHCP сервера
 dhcp relay server 30.0.0.2
!
!
! ** End Context **
!
!
port ethernet 7/1
! XCRP management port on slot 7
 no shutdown
 bind interface mgmt local
!
!
!*включаем на порту 1/3 возможность динамически создавать абонентские
!*circuit, которые будут привязываться к тому или иному контексту и
!*multibind интерфейсу при помощи указаний, получаемых с RADIUS
port ethernet 1/3
 no shutdown
 service clips dhcp
!
port ethernet 1/4
 no shutdown
 encapsulation dot1q
 dot1q pvc 100
  bind interface uplink0 local
!
```

Необходимо также настроить соответствующую запись в радиус сервере. Аутентификация будет выполняться на базе DHCP option 82, а точнее двух ее сабопциях Agent-Remote-Id и Agent-Circuit-Id.
Dynamic CLIPS требует как минимум следующих обязательных атрибутов в access-accept:

- **“IP-Interface-Name”** – определяет имя multibind интерфейса, т.е. то куда приземлить абонента, также SmartEdge перепишет/запишет поле GI_ADDR в пакете DHCP Discover на IP адрес этого multibind интерфейса прежде чем отправить спроксированный Discover в сторону DHCP сервера. Этого нужно также для того, чтобы DHCP сервер посылал Offer обратно в SmartEdge. (не забываем что SmartEdge это DHCP Proxy, а также тот факт, что DHCP север должен иметь route для ip префикса этого multibind интерфейса, если между SmartEdge и сервером есть L3 хопы).
- **“DHCP-Max-Leases”** – для работы Dynamic CLIPS всегда должно быть равно 1 (архитектурное требование).

Также для рассматриваемого примера обязательным атрибутом будет являться атрибут **“Context-Name”**. Т.к. включая dynamic clips на порту eth 1/3, мы не указали явной привязки сервиса clips к какому-либо из контекстов. Т.е. если бы конфиг был `service clips dhcp context local`, то атрибут “Context-Name” в access-accept не нужен. Так для указанного примера запись в RADIUS может выглядеть, например, следующим образом:

```
DEFAULT Cleartext-Password := "Redback", Agent-Circuit-ID == "mtu1-
005:4/11", Agent-Remote-ID == “\024 \007”
      IP-Interface-Name = "CLIPS-SUBS-001",
      DHCP-Max-Leases = 1,
      Context-Name = "local"
```

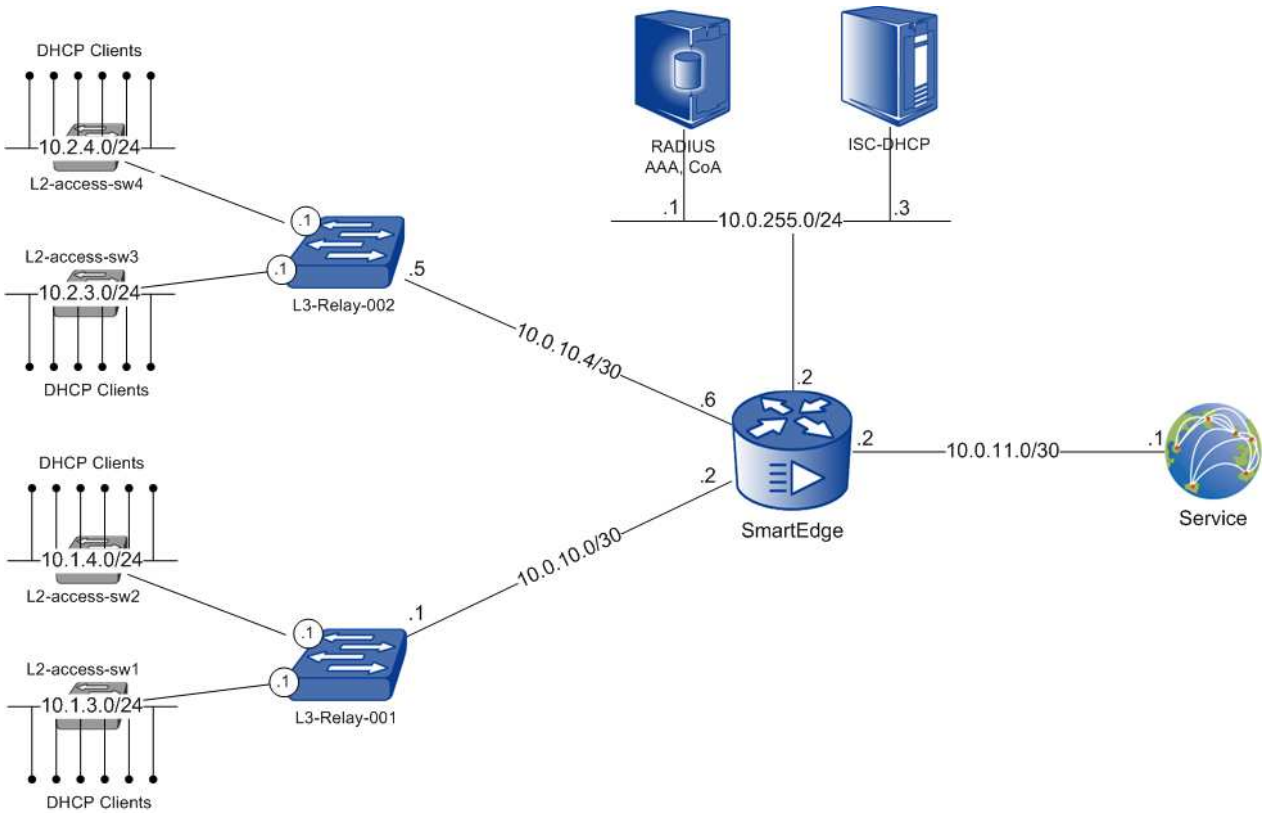
Полезные команды для проверки, что все получилось:

```
show subscribers active all
show dhcp relay hosts
```

Чтобы сбросить dynamic clips абонента, нужно использовать следующую команду:

```
clear dhcp host
```

Сценарий работы Dynamic CLIPS через L3 сеть доступа.
На рисунке ниже представлена топология, на базе которой будет сделана конфигурация и пояснения.




```
!
context local
!
 interface mgmt
  ip address 10.0.255.2/24
   ip source-address radius dhcp-server
!
 interface subnet-10.1.3.0/24 multibind
  ip address 10.1.3.254/24
  dhcp proxy 253
!
 interface subnet-10.1.4.0/24 multibind
  ip address 10.1.4.254/24
  dhcp proxy 253
!
 interface subnet-10.2.3.0/24 multibind
  ip address 10.2.3.254/24
  dhcp proxy 253
!
 interface subnet-10.2.4.0/24 multibind
  ip address 10.2.4.254/24
  dhcp proxy 253
!
 interface to-L3-Relay-001 p2p
```

```
  ip address 10.0.10.2/30
  ip access-group acl-for-l3-relays-only in
!
 interface to-L3-Relay-002 p2p
  ip address 10.0.10.6/30
  ip access-group acl-for-l3-relays-only in
!
 interface to-the-world p2p
  ip address 10.0.11.2/30
!
!
 ip access-list acl-for-l3-relays-only
  seq 10 permit ip 10.0.0.1 0.255.255.0
!
!
 aaa authentication administrator local
 aaa authentication subscriber radius
 aaa accounting subscriber radius
 aaa accounting suppress-acct-on-fail
 radius accounting server 10.0.255.1 encrypted-key 3828082561D6BDD6
 radius coa server 10.0.255.1 encrypted-key 3828082561D6BDD6 port 3799
!
!
 radius server 10.0.255.1 encrypted-key 3828082561D6BDD6
!
subscriber default
   dhcp max-addrs 1
!
 ip route 10.1.3.0/24 10.0.10.1 connected tag 777
 ip route 10.1.4.0/24 10.0.10.1 connected tag 777
 ip route 10.2.3.0/24 10.0.10.5 connected tag 777
 ip route 10.2.4.0/24 10.0.10.5 connected tag 777
!
 dhcp relay option
 dhcp relay server 10.0.255.3
!
!
! ** End Context **
!
port ethernet 1/1
! XCRP management port on slot 1
 no shutdown
 bind interface mgmt local
!
port ethernet 2/1
 no shutdown
 bind interface to-L3-Relay-001 local
 service clips dhcp context local
!
port ethernet 2/2
 no shutdown
 bind interface to-L3-Relay-002 local
```

```
 service clips dhcp context local
!
port ethernet 3/1
 no shutdown
 bind interface to-the-world local
!
```

Отличительной особенностью примера работы через L3 Релеи, в отличие от описанного случая, когда сегмент доступа между абонентом и BRAS-ом является L2, то, что на портах, где включен clips service также живут статические привязки L3 интерфейсов в сторону этих L3 Релеев.

```
!
port ethernet 2/1
 no shutdown
 bind interface to-L3-Relay-001 local
 service clips dhcp context local
!
port ethernet 2/2
 no shutdown
 bind interface to-L3-Relay-002 local
 service clips dhcp context local
!
```

Т.к. коммутаторы, являющиеся L3 Релеями переводят все броадкастовое DHCP взаимодействие в юникаст и при этом используют в качестве source IP адрес из абонентских сегментов, то на SmartEdge необходим маршрут, для того чтобы поддержать такое взаимодействие. Обратимся к нашему примеру, коммутатор L2-access-sw4 обслуживает сегмент с подсетью 10.2.4.0/24. Этот сегмент терминируется на L3 коммутаторе L3-Relay-002, где поднят IP адрес – 10.2.4.1/24. Этот адрес является шлюзом для этого сегмента. Когда в данном сегменте появляется DHCP Discover, L3 коммутатор будет транслировать его на DHCP сервер – 10.0.10.6. В качестве DHCP сервера выступает SmartEdge, которому необходимо отвечать юникастом в IP адрес Релея, т.е. в 10.2.4.1. Именно для этого добавляются статик маршруты на SmartEdge в нашем примере:

```
!
 ip route 10.1.3.0/24 10.0.10.1 connected tag 777
 ip route 10.1.4.0/24 10.0.10.1 connected tag 777
 ip route 10.2.3.0/24 10.0.10.5 connected tag 777
 ip route 10.2.4.0/24 10.0.10.5 connected tag 777
!
```

В данном примере мы повесили на эту статику тэг 777 на будущее, чтобы была возможность легко зафильтровать эти маршруты при редистрибюции, не забивая себе голову префиксами.
Внимательный читатель может задать следующий вопрос. А для чего такие странные ACL на интерфейсах в сторону L3 Релеев? И как вообще будут работать абоненты на этих портах, если все source IP, кроме .1 запрещены (каждый acl имеет последним выражением неявное deny all)?

```
!
 interface to-L3-Relay-001 p2p
  ip address 10.0.10.2/30
  ip access-group acl-for-l3-relays-only in
!
 interface to-L3-Relay-002 p2p
  ip address 10.0.10.6/30
```

```
  ip access-group acl-for-l3-relays-only in
!
 ip access-list acl-for-l3-relays-only
  seq 10 permit ip 10.0.0.1 0.255.255.0
!
```

А это как раз то случай, когда circuit architecture проявляет себя во всей красе. Во-первых, зачем ACL? Ответ: для безопасности. Представьте, что со стороны сети доступа приходит пакет с source IP адресом 10.1.3.150, например, на порт SmartEdge eth2/1, предположим, что при этом такой адрес никогда не выдавался в этом сегменте по DHCP, что в таком случае должен сделать SmartEdge, если к интерфейсу `to-L3-Relay-001` не прикручен указанный acl? Пакет успешно попадет в роутер и будет смаршрутизирован. Так как же все это работает? Все просто, порт eth2/1 это circuit, и если через данный порт проходит DHCP диалог, то согласно нашей конфигурации создается абонентский circuit, в который будут попадать только те пакеты в source IP которых указан адрес, выданный данному клиенту по DHCP. Т.е. получается, что в circuit порта eth2/1 рождаются child circuit-ы абонентов, для которых правила примененные к parent circuit не применяются. Это называется демультиплексированием входящих пакетов на порту SmartEdge, т.е. грубо говоря, работает некий фильтр, который в зависимости от настроек выполненных на порту, понимающий как правильно демультиплексировать пакеты по circuit-ам живущим в этом порту.

Что нужно сделать еще?

Осталось применить стандартные вещи – общие для PPPoE и CLIPS, создать qos полиси для rate-limit-ов в соответствии с тарифами, составить абонентские ACL, http-redirect профили – при необходимости, и прочее… Но об этом в других How to… т.к. в этом документе представлена скромная попытка автора раскрыть базовую механику CLIPS в SmartEdge.
Надеюсь, что документ получился полезным.

Денис Михайловский (с)

Об ошибках и неточностях просьба сообщать по адресу: edenmik@redback.com