ericsson.com

Базовая настройка

AAA,RADIUS,CoA,PPPoE,L2TP

Rev

ERICSSON

Содержание

1 RFC, протоколы, базовые понятия

Мультисервисный маршрутизатор SmartEdge в полной мере поддерживает протоколы RADIUS и CoA для аутентификации, авторизации и аккаунтинга(AAA) широкополосных абонентов и администраторов для управления через протоколы Telnet и SSH.

Список RFC(по состоянию на 18 января 2011г.):

RFC 2058	Remote Authentication Dial In User Service (RADIUS)
RFC 2059	RADIUS Accounting
RFC 2138	Remote Authentication Dial In User Service (RADIUS)
RFC 2139	RADIUS Accounting
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting Client MIB
RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 3162	RADIUS and IPv6
RFC 3576	Dynamic Authorization Extensions to Remote Authentication for Dial In User Service (RADIUS)
RFC 4679	DSL Forum Vendor-Specific RADIUS Attributes
RFC 4818	RADIUS Delegated-IPv6-Prefix Attribute

2 Ограничения

Минимальный интервал, с которым SmartEdge отсылает сообщения Accounting Update(Acct-Interim-Interval)
в RADIUS:
для сессии составляет 600 секунд(10 минут),
для сервиса составляет 900 секунд(15 минут).
Максимальный - 604,800 секунд(7 дней).

Количество одновременно обрабатываемых соединений:
XCRP3 (установлен в SE100) – до 150 соединений в секунду
XCRP4 (актуальный RP для SE600/1200) – до 300 соединений в секунду

Количество CoA серверов – до 5(до SEOS 6.4), до 36(после SEOS 6.4)

Доступные протоколы аутентификации – PAP, CHAP
(протоколы MS-CHAP, MS-CHAPv2 и другие отсутствуют)

3 Базовая настройка AAA (для абонентов)

В данном разделе кратко рассмотрим конфигурирование подсистемы AAA(аутентификация, авторизация и аккаунтинг) для абонентов с использованием RADIUS сервера.

Существует 2 режима работы AAA: контекстный и глобальный.
В первом режиме для каждого контекста можно определить свои параметры AAA, во втором режим параметры определяются глобально и задаются в указанном контексте.

Настройка в глобальном режиме

Следующая строчка глобально включает аутентификацию абонентов через RADIUS в контексте local

```
[local]Redback(config)#aaa global authentication subscriber radius context local
```

Настройка в режиме контекста.

Переключитесь в нужный контекст (для каждого контекста можно задать свои параметры AAA), для этого наберите в режиме конфигурирования CLI:

```
[local]Redback(config)#context local
```

Включите аутентификацию абонентов через RADIUS в контексте:

```
[local]Redback(config-ctx)#aaa authentication subscriber radius
```

Включите аккаунтинг абонентов через RADIUS в контексте:

```
[local]Redback(config-ctx)#aaa accounting subscriber radius
```

Пример:

```
[local]Redback(config)#aaa global authentication subscriber radius context local
[local]Redback(config)#context local
[local]Redback(config-ctx)#aaa authentication subscriber radius
[local]Redback(config-ctx)#aaa accounting subscriber radius
[local]Redback(config-ctx)#commit
```

4 Базовая настройка RADIUS

Переключитесь в нужный контекст(для каждого контекста можно задать свой набор RADIUS серверов), для этого наберите в режиме конфигурирования CLI:

```
[local]Redback(config)#context local
```

Задайте адрес RADIUS сервера для аутентификации(порт по умолчанию – 1812) и секретный ключ

```
[local]Redback(config-ctx)#radius server 10.43.32.56 key Secret
```

Задайте адрес RADIUS сервера для аккаунтинга(порт по умолчанию - 1813) и секретный ключ

```
[local]Redback(config-ctx)#radius accounting server 33.44.55.66 key Secret
```

Задайте параметр max-entries – количество попыток обращения к RADIUS серверу

```
[local]Redback(config-ctx)#radius max-retries 5
```

Задайте параметр timeout – время в течение которого SmartEdge будет ждать ответ от RADIUS сервера при каждой попытке соединения

```
[local]Redback(config-ctx)#radius timeout 30
```

Создайте новый интерфейс, задайте адрес, на котором будет являться адресом NAS для биллинга:

```
[local]Redback(config-ctx)#interface mgmt loopback

[local]Redback(config-if)#ip address 11.200.1.1/32
```

Важная строка, говорит о том что с этого адреса SmartEdge будет обращаться в биллинг:

```
[local]Redback(config-if)#ip source-address radius
```

Пример:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius server 10.43.32.56 key Secret
[local]Redback(config-ctx)#radius max-retries 5
[local]Redback(config-ctx)#radius timeout 30
[local]Redback(config-ctx)#interface mgmt loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#ip source-address radius
[local]Redback(config-if)#commit
```

5 Базовая настройка CoA

Переключитесь в нужный контекст(для каждого контекста можно задать свой набор CoA серверов), для этого наберите в CLI:

```
[local]Redback(config)#context local
```

Задайте набор серверов CoA с собственными секретными ключами и портами:

```
[local]Redback(config-ctx)#radius coa server 1.1.1.1 key coacoa port 3799
[local]Redback(config-ctx)#radius coa server 1.1.1.2 key coacoa port 3800
[local]Redback(config-ctx)#radius coa server 1.1.1.3 key coacoa port 3801
[local]Redback(config-ctx)#radius coa server 1.1.1.4 key coacoa port 3802
[local]Redback(config-ctx)#commit
```

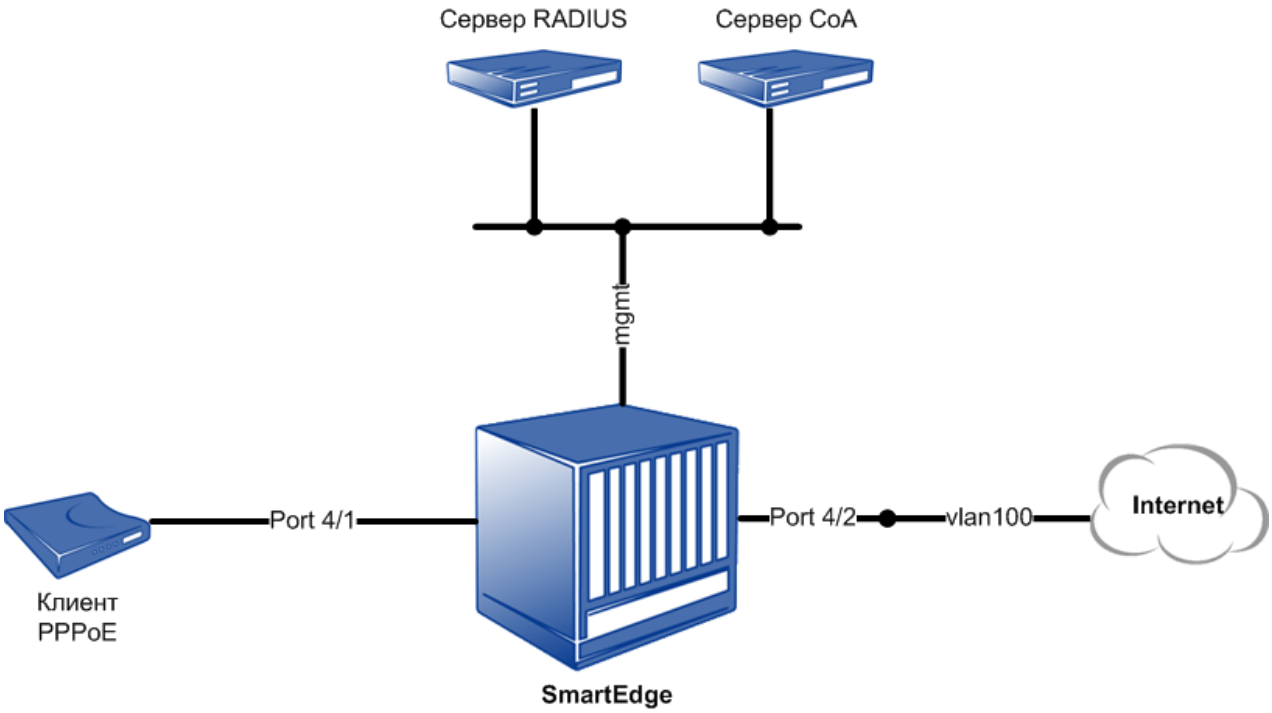
Пример:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#radius coa server 1.1.1.1 key coacoa port 3799
[local]Redback(config-ctx)#radius coa server 1.1.1.2 key coacoa port 3800
[local]Redback(config-ctx)#radius coa server 1.1.1.3 key coacoa port 3801
[local]Redback(config-ctx)#radius coa server 1.1.1.4 key coacoa port 3802
[local]Redback(config-ctx)#commit
```

6 Базовая настройка PPPoE

Следующий пример рассматривает конфигурацию, в которой SmartEdge терминирует PPPoE соединения с аутентификацией пользователей через RADIUS сервер.

Схема тестового стенда:



Пример конфигурации:

Определяем имя сервиса PPPoE - Internet, разрешаем принимать соединения с любым именем сервиса, определяем DNS серверы для абонентов, задаём MTU 1492 :

```
!
context local
!
domain isp.ru
domain Internet advertise
!
subscriber default
dns primary 8.8.8.8
dns secondary 8.8.4.4
ppp mtu 1492
!
! ** End Context **
```

В режиме глобальной конфигурации:

```
!
pppoe service-name accept-all
pppoe services marked-domains
!
```

Определяем статичные интерфейсы и маршрут по умолчанию:

```
!
context local
!
 interface Internet
  ip address 10.1.1.1/24
!
 interface mgmt
 ip address 10.2.2.1/24
 ip source-address radius
!
!
ip route 0.0.0.0/0 10.1.1.2
!
```

Привязываем интерфейс mgmt к интерфейсу управления XCRP:

```
!
port ethernet 7/1
! XCRP management ports on slot 7 and 8 are configured through 7/1
 no shutdown
 bind interface mgmt local
!
```

Включаем карту 4x10GE в 4 слоту:

```
!
card 10ge-4-port 4
!
```

Настраиваем второй физический интерфейс 10GE на линейной карте в слоту 4:
Инкапсуляция - 802.1q, VLAN = 100, виртуальный интерфейс – Internet, контекст - local

```
!
port ethernet 4/2
 no shutdown
 encapsulation dot1q
 dot1q pvc 100
  bind interface Internet local
!
```

Динамичные интерфейсы, в данном случае будем использовать PPPoE.

```
!
context local
!
 interface pppoe multibind
  ip address 192.168.1.254/24
  ip pool 192.168.1.0/24
!
! ** End Context **
!
```

Настраиваем первый физический интерфейс 10GE на линейной карте в слоту 4:
Инкапсуляция – PPPoE, протоколы аутентификации – PAP,CHAP,
максимальное количество соединений – 8000

```
!
port ethernet 4/1
 no shutdown
 encapsulation pppoe
 bind authentication chap pap context local maximum 8000
!
```

Пример двойной инкапсуляции – PPPoE и 802.1q

```
!
port ethernet 4/1
 no shutdown
 encapsulation dot1q
 dot1q pvc 100 encapsulation pppoe
  bind authentication chap pap context local maximum 8000
!
```

Определение схемы AAA, CoA и RADIUS сервера.

```
!
aaa last-resort context local
!
context local
!
!
 aaa authentication subscriber radius
 aaa accounting subscriber radius
 radius accounting server 10.2.2.2 encrypted-key 3828082561D6BDD6
 radius coa server 10.2.2.3 encrypted-key 3828082561D6BDD6 port 3799
!
 radius server 10.2.2.2 encrypted-key 3828082561D6BDD6
!
!
! ** End Context **
```

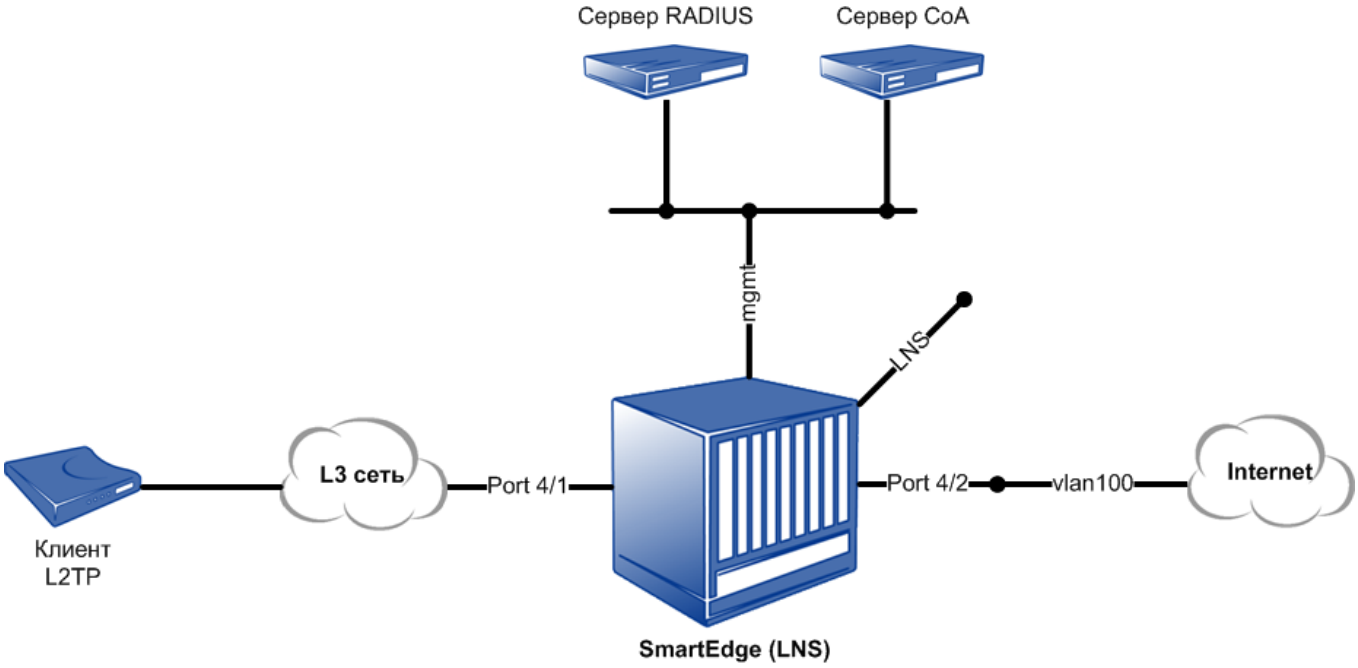
На данном этапе PPPoE абонент может установить сессию и получить IP адрес из пула, для этого необходим следующий вид учетной записи в конфигурации RADIUS сервера.

```
#
user password = "userpass"
      Service-Type= Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 255.255.255.254
#
```

В данном случае абонент получит IP адрес из пула адресов ip pool 192.168.1.0/24

7 Базовая настройка L2TP

Следующий пример рассматривает конфигурацию, в которой SmartEdge терминирует L2TP соединения с аутентификацией пользователей через RADIUS сервер.



Конфигурация:

Настраиваем SmartEdge в режиме LNS, адрес L2TP LNS – 10.3.3.3(loopback интерфейс) определяем DNS серверы для абонентов, определяем MTU 1460:

```
!
context local
!
!
 l2tp-peer unnamed local 10.3.3.3
  session-auth chap context local
  function lns-only
!
subscriber default
dns primary 8.8.8.8
dns secondary 8.8.4.4
ppp mtu 1460
!
```

P2P сеть между SmartEdge и внутренней L3 сетью – 10.4.4.0/30 (10.4.4.1 – адрес Smartedge, 10.4.4.2 – адрес соседнего роутера)
Транспортные адреса клиента L2TP – 10.5.5.0/24(статическая маршрутизация)
Адрес L2TP LNS – 10.3.3.3(loopback интерфейс)

Определяем статичные интерфейсы и маршрут по умолчанию:

```
!
context local
!
 interface Internet
  ip address 10.1.1.1/24
!
 interface mgmt
  ip address 10.2.2.1/24
  ip source-address radius
!
 interface LNS loopback
  ip address 10.3.3.3/32
!
 interface l2tp multibind
  ip address 192.168.1.254/24
  ip pool 192.168.1.0/24
!
 interface wan
  ip address 10.4.4.1/30
!
ip route 0.0.0.0/0 10.1.1.2
ip route 10.5.5.0/24 10.4.4.2
!
!** End Context **
!
```

Привязываем интерфейс mgmt к интерфейсу управления XCRP:

```
!
port ethernet 7/1
! XCRP management ports on slot 7 and 8 are configured through 7/1
 no shutdown
 bind interface mgmt local
!
```

Включаем карту 4x10GE в 4 слоту:

```
!
card 10ge-4-port 4
!
```

Настраиваем второй физический интерфейс 10GE на линейной карте в слоту 4:
Инкапсуляция - 802.1q, VLAN = 100, виртуальный интерфейс – Internet, контекст - local

```
!
port ethernet 4/2
 no shutdown
 encapsulation dot1q
 dot1q pvc 100
  bind interface Internet local
!
```

Настраиваем первый физический интерфейс 10GE на линейной карте в слоту 4: Инкапсуляция - IPoE, контекст - local

```
!
port ethernet 4/1
 no shutdown
 bind interface wan local
!
```

Определение схемы AAA, CoA и RADIUS сервера.

```
!
aaa last-resort context local
!
context local
!
!
 aaa authentication subscriber radius
 aaa accounting subscriber radius
!
 radius accounting server 10.2.2.2 encrypted-key 3828082561D6BDD6
 radius coa server 10.2.2.3 encrypted-key 3828082561D6BDD6 port 3799
!
 radius server 10.2.2.2 encrypted-key 3828082561D6BDD6
!
!
! ** End Context **
```

На данном этапе L2TP абонент может установить сессию и получить IP адрес из пула, для этого необходим следующий вид учетной записи в конфигурации RADIUS сервера.

```
#
user password = "userpass"
      Service-Type= Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 255.255.255.254
#
```

В данном случае абонент получит IP адрес из пула адресов ip pool 192.168.1.0/24