

BRAS. L2 WiFi -

- 1.
- 2.
 - 2.1 BRAS
 - 2.2
- 3. ESR BRAS
- 4. SoftWLC c ESR
 - 4.1.
 - 4.2.
 - 4.3. ,
- 5. firewall ESR
- 6.
 - 6.1. ESR
 - 6.2

1.

BRAS ESR-10/20/100/200/1000/1200/1500/1700. Wi-Fi, . BRAS :

- , ;
- , , , (SMS,);
- , , BRAS , ;
- BRAS .

BRAS , , SoftWLC, , BRAS. SoftWLC BRAS 2 : PCRF .

, BRAS- -, . MAC . , BRAS , MAC- . BRAS L2- , BRAS VPN L3- . , L2, BRAS vlan L2- . ESR BRAS L3 : [BRAS](#) /[BRAS](#) vrf. [L3 WiFi](#) -

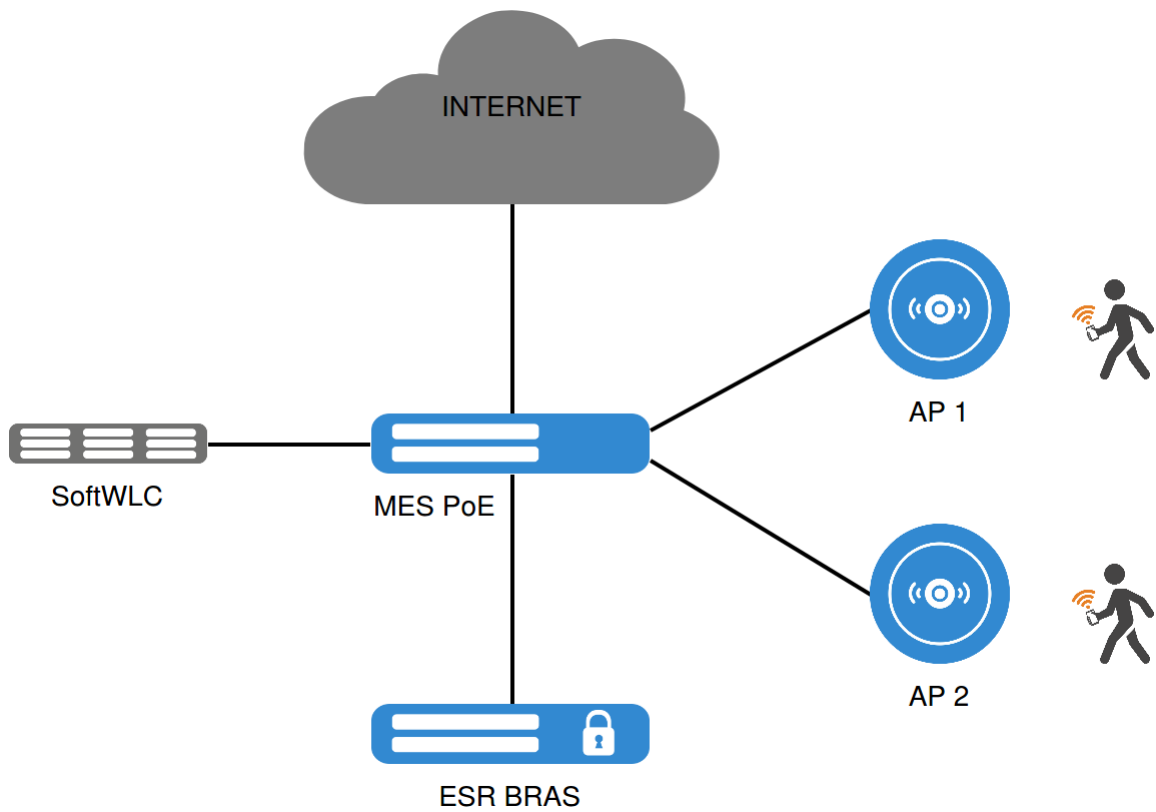
, ESR 1.11.3, SoftWLC 1.18.

2.

, BRAS SoftWLC , L2 (vlan) SSID.

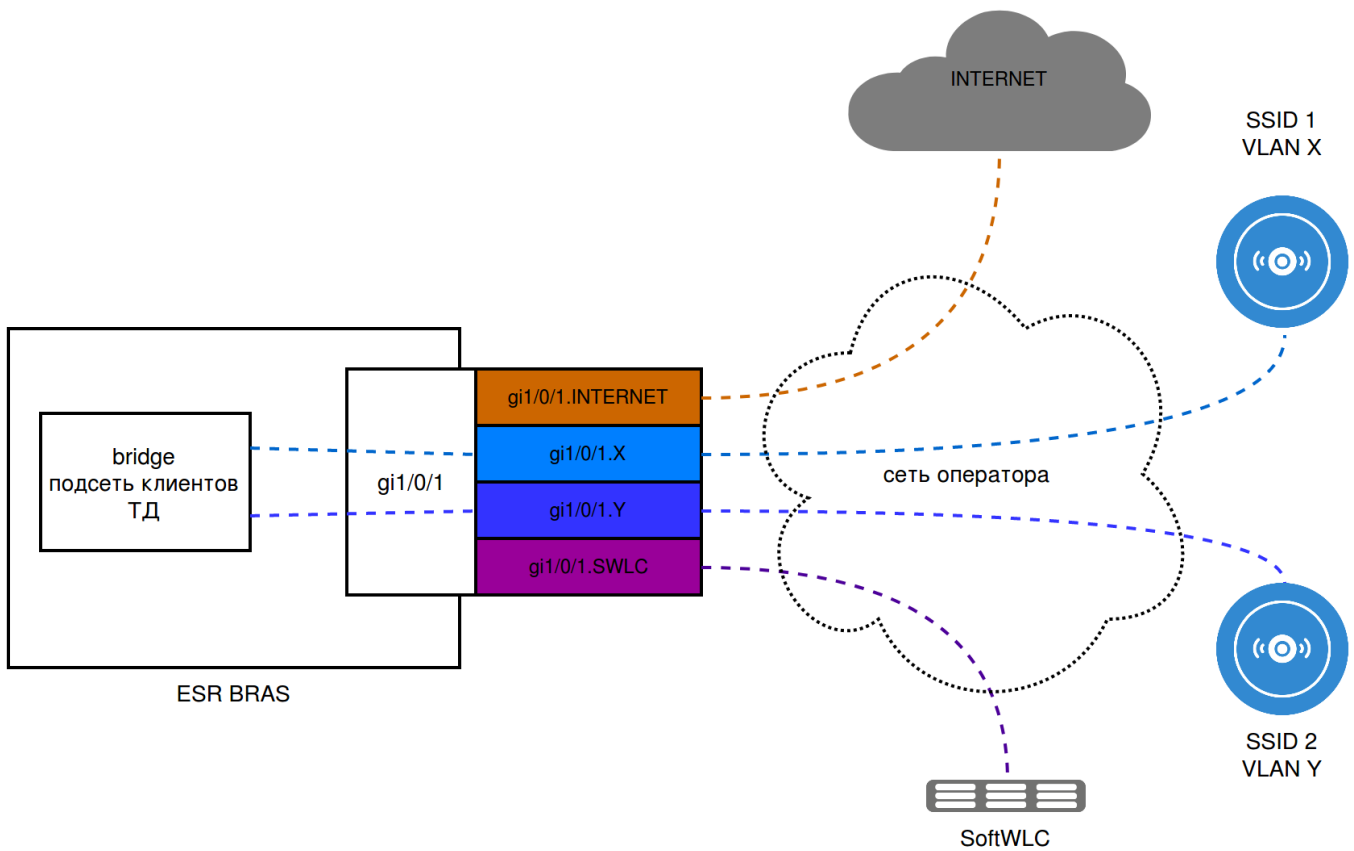
2.1 BRAS

. 2.1, , SSID vlan, ESR. , SoftWLC . .



. 2.1.

, . 2.2, ESR. gi1/0/1 (). SoftWLC .vlan SSID1 SSID2 . NAT ESR.

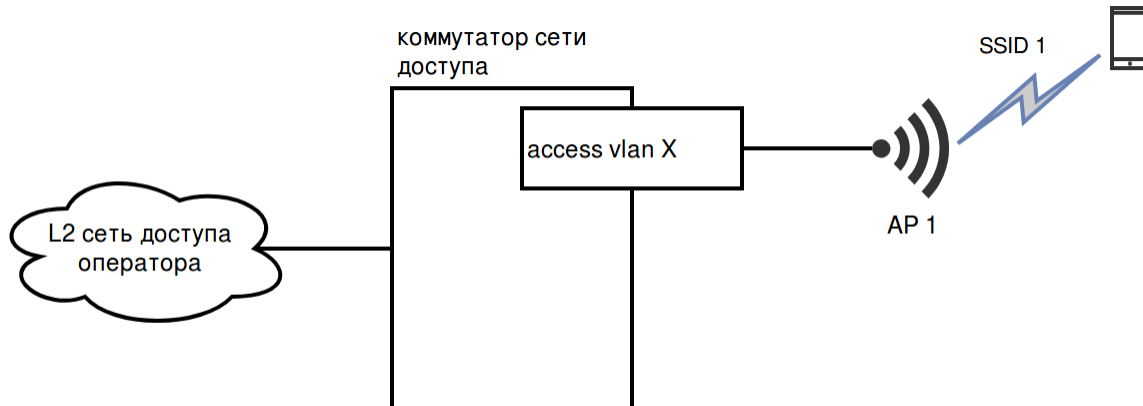


. 2.2.

, .. - vlan, vlan (, SSID vlan). , SSID, vlan. ESR BRAS SoftWLC L3 .

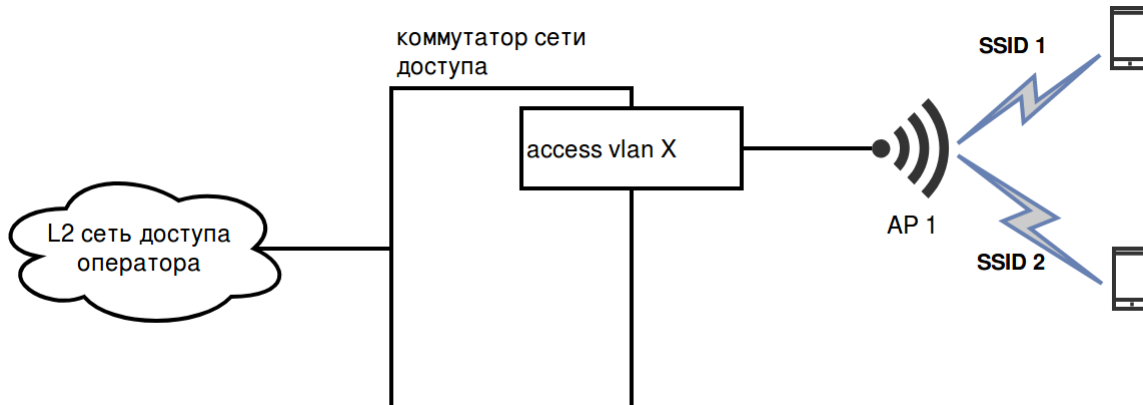
2.2

1) 1- 1 SSID.



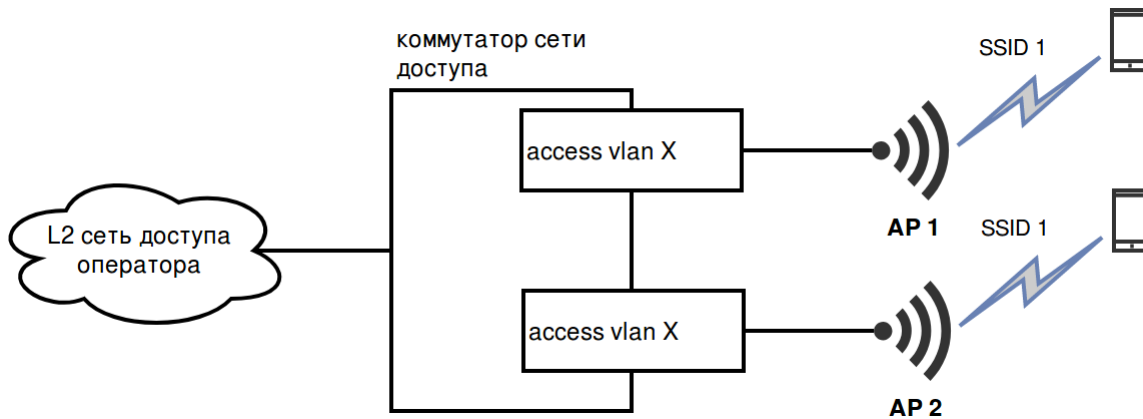
SSID. access , L2 ESR BRAS vlan. , SSID .

2) 1 2 SSID ().



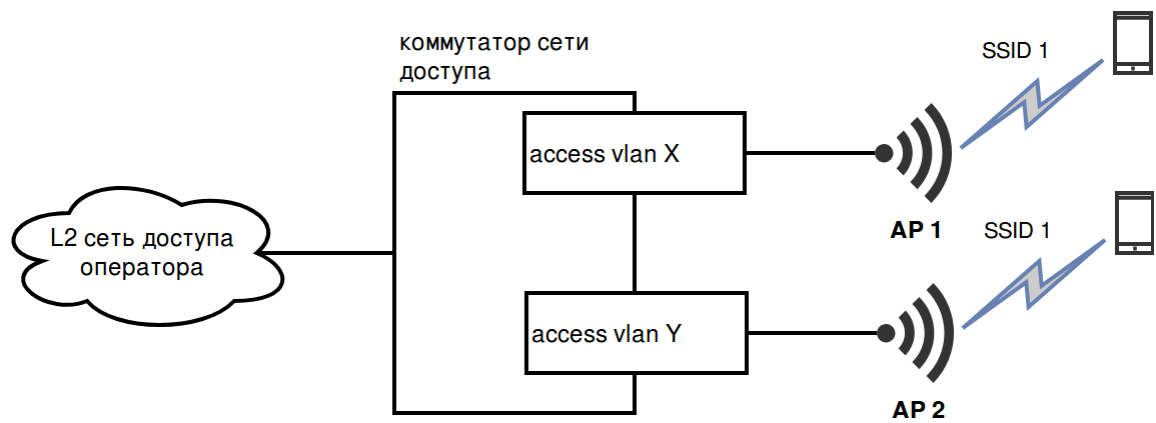
2 SSID . untagged access , L2 ESR BRAS vlan. , SSID, . **SSID** .

3.1) 2- () 1 SSID.



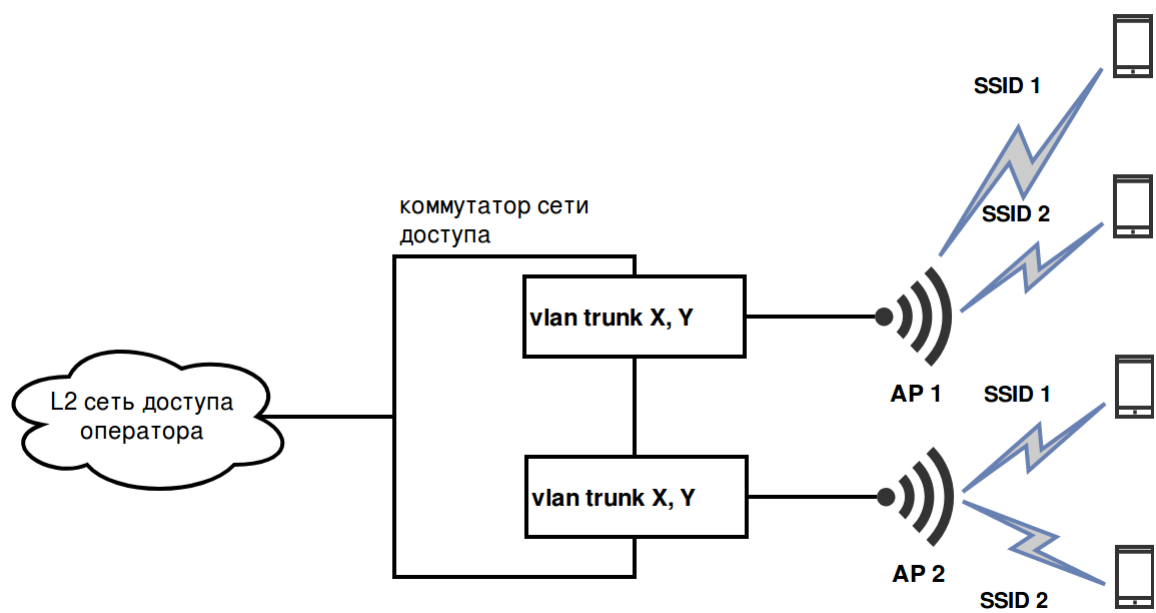
1 SSID. untagged, access (с vlan id) 1, L2 ESR BRAS vlan. , , . .

3.2) 2- () 1 SSID.



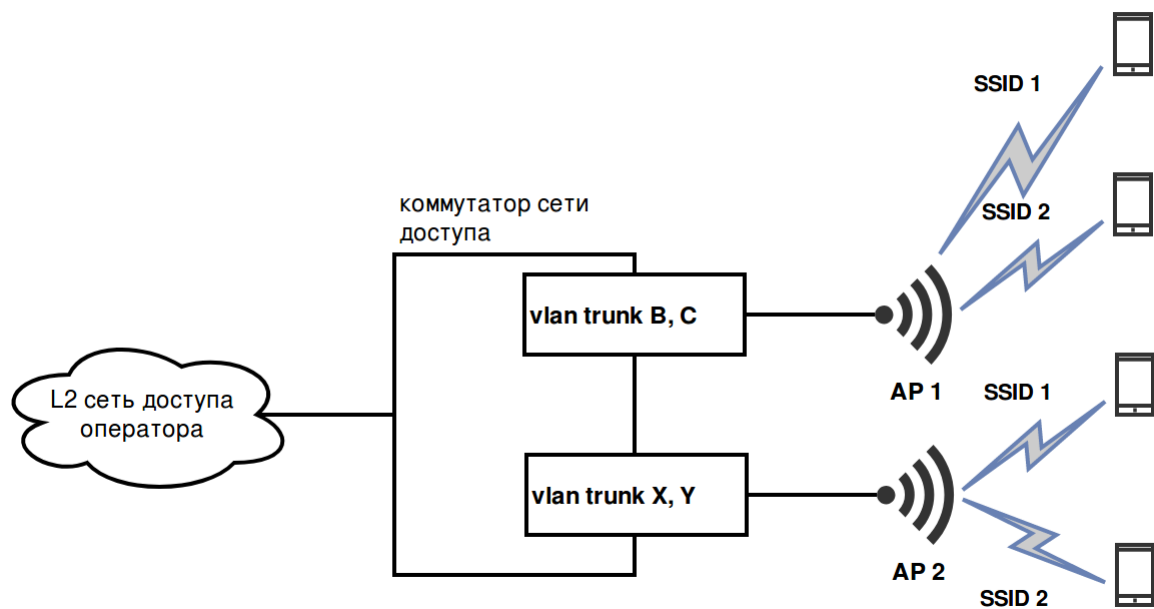
1 SSID. access (с vlan ID), L2 ESR BRAS vlan. , , , .

4.1) 2- () 2 () SSID.



2 () SSID . SSID vlan (vlan), trunk , L2 ESR BRAS. , , SSID, . SSID .

4.2) 2- () 2 () SSID.



2 () SSID . SSID vlan (vlan), trunk , L2 ESR BRAS vlan. , , SSID, , , .

3. ESR BRAS

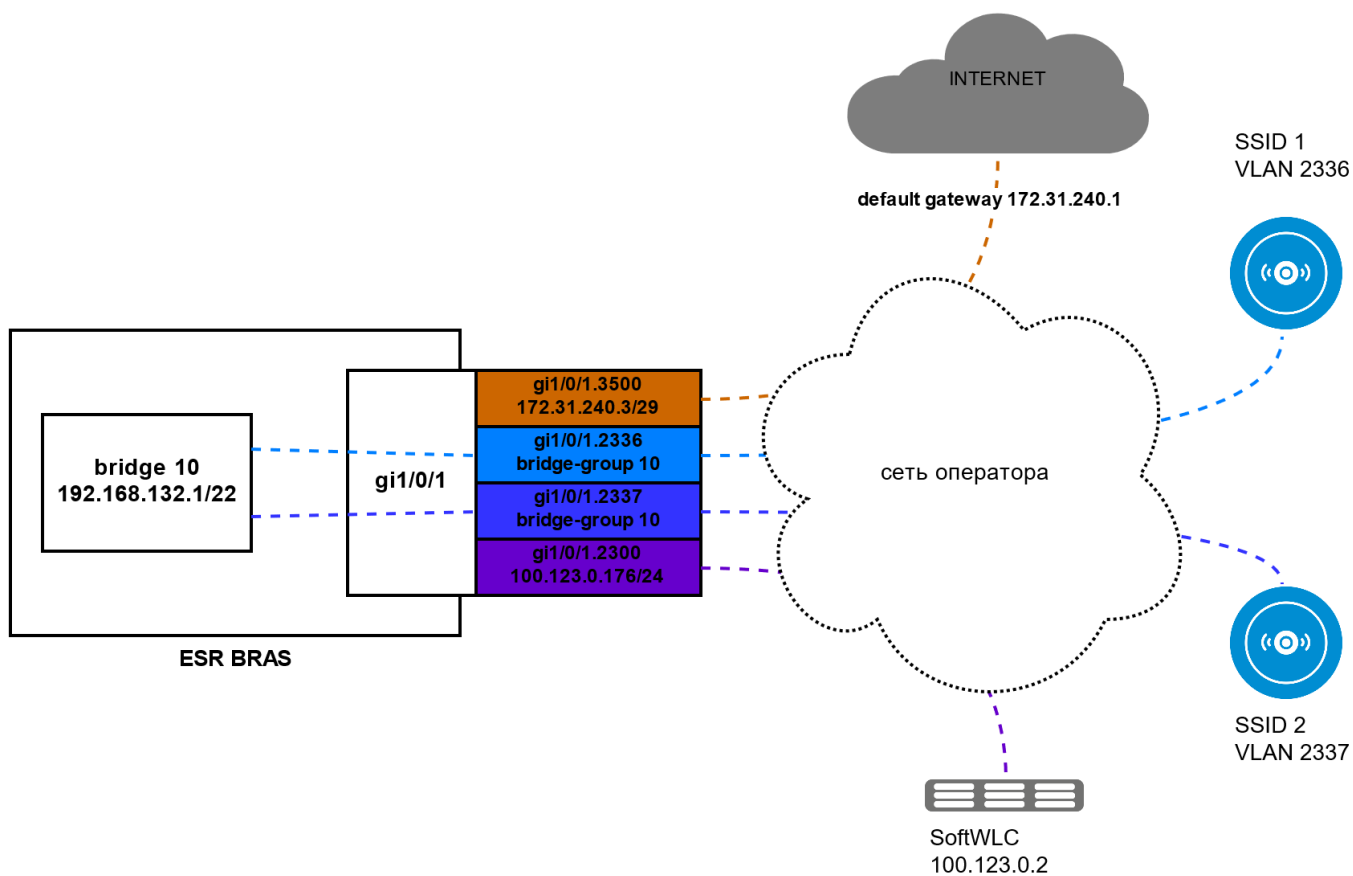
ESR SoftWLC BRAS. , SoftWLC . SoftWLC : [Wi-Fi \(SoftWLC\)](#)

ESR :

	vlan	/
, SoftWLC	2300	100.123.0.176/24
	3500	172.31.240.3/29
		192.168.132.0/22
SSID 1	2336	
SSID 2	2337	

SoftWLC 100.123.0.2. ESR 172.31.240.1.

. 3.1 ESR c. ESR "router-on-stick", uplink gi1/0/1.



. 3.1.

ESR :

- 1) - , ESR;
- 2) L3 ESR, , ;
- 3) , : , , ESR SoftWLC - BRAS;
- 4) BRAS , .

ESR factory , :

```
esr1000# copy system:default-config system:candidate-config
Entire candidate configuration will be reset to default, all settings will be lost upon commit.
Do you really want to continue? (y/N): y
|*****| 100% (50B) Default configuration loaded successfully.
```

:

```

security zone trusted
exit
security zone untrusted
exit
security zone users
exit

bridge 10
  description "users"
  security-zone users
  ip firewall disable
  ip address 192.168.132.1/22
  ip helper-address 100.123.0.2
  protected-ports local
  enable
exit

interface gigabitethernet 1/0/1.3500
  description "UpLink"
  security-zone untrusted
  ip address 172.31.240.3/29
exit
interface gigabitethernet 1/0/1.2300
  description "mgmt"
  security-zone trusted
  ip firewall disable
  ip address 100.123.0.176/24
exit
interface gigabitethernet 1/0/1.2336
  bridge-group 10
exit
interface gigabitethernet 1/0/1.2337
  bridge-group 10
exit

ip dhcp-relay

ip route 0.0.0.0/0 172.31.240.1

ip telnet server
ip ssh server

```

(commit/confirm), ssh/telnet.

NAT:

```

object-group network users
  ip prefix 192.168.132.0/22
exit

nat source
  pool nat_addr
  ip address-range 172.31.240.3
exit
ruleset nat_source
  to zone untrusted
  rule 1
    match source-address users
    action source-nat pool nat_addr
  enable
exit
exit
exit

```

- , SoftWLC. DHCP , . (isc-dhcp-server). .

SNMP NTP - ESR EMS:

```

snmp-server
snmp-server system-shutdown
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 100.123.0.2
    source-address 100.123.0.176
exit

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit

```

BRAS :

- 1) BRAS;
- 2) radius;
- 3) access-list, BRAS;
- 4) BRAS .

1.1) :

```

esr1000# sh licence
Active licence not found!

```

. "".

1.2) ESR , :

```

esr1000# copy tftp://100.123.0.2:/NP07000030.lic system:licence
|*****| 100% (678B) Licence loaded successfully. Please reboot system to
apply changes.
esr1000# sh licence
Licence information
-----
Name:      eltex
Version: 1.0
Type:      ESR-1000
S/N:       NP07000030
MAC:       A8:F9:4B:AB:79:A0
Features:
  BRAS - Broadband Remote Access Server

```

1.3) ESR:

```

esr1000# reload system
Do you really want to reload system ? (y/N): y

```

BRAS.

2) :



SoftWLC Eltex-PCRF - ESR

aaa radius-profile! VRRP !

```
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 100.123.0.176
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
radius-server host 100.123.0.3
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 100.123.0.176
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
  radius-server host 100.123.0.3
exit
```

```
object-group network SoftWLC
  ip address-range 100.123.0.2
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 100.123.0.176
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text testing123
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit
```

, 100.123.0.2 31812 31813, testing123. ESR PCRF (, SoftWLC). , PCRF ESR 3799 100.123.0.2, testing123. PCRF ESR.

3) access-list, BRAS:

```

ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port 8443
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
  exit
exit

ip access-list extended INTERNET
  rule 1
    action permit
    enable
  exit
exit

ip access-list extended unauthUSER
  rule 1
    action permit
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit

```

4.1) BRAS , bridge :

```

object-group network bras_users
  ip address-range 192.168.132.2-192.168.135.254
exit

bridge 10
  description "users"
  security-zone users
  ip firewall disable
  ip address 192.168.132.1/22
  ip helper-address 100.123.0.2
  service-subscriber-control object-group bras_users
  location data10
  protected-ports local
  enable
exit

```



"service-subscriber-control object-group bras_users" - , , bras_users. , bridge 10 . "service-subscriber-control any", .

4.2) BRAS:

100.123.0.2 7070 URL 8080 . PCRF.

```
subscriber-control filters-server-url http://100.123.0.2:7070/filters/file
subscriber-control
  aaa das-profile COA
  aaa sessions-radius-profile PCRF
  aaa services-radius-profile PCRF
  nas-ip-address 100.123.0.176
  session mac-authentication
  bypass-traffic-acl unauthUSER
  default-service
    class-map unauthUSER
    filter-name remote gosuslugi
    filter-action permit
    default-action redirect http://100.123.0.2:8080/eltex_portal/
  exit
  enable
exit
```

ESR BRAS. SoftWLC. BRAS , SoftWLC.

4. SoftWLC c ESR

SoftWLC , ESR BRAS; - , ; , .

4.1.

:

- 1) BRAS ;
- 2) URL - welcome gosuslugi;
- 3) WELCOME;
- 3) BRAS ;
- 4) ESR BRAS EMS .
- , 5- - ESR BRAS.

- 1) (. 4.1.1) <http://<ip >:8080/epadmin> " BRAS":

Конструктор порталов
Версия: 1.18-27

Стартовая страница

Галерея

Системные настройки ▾

Конструктор порталов

Уведомления

Доступ к NBI

Доступ к NGW

Взаимодействие с BRAS

Взаимодействие с BRAS

Взаимодействие с BRAS ☒

Сохранить

. 4.1.1.

- " BRAS" - , BRAS ;

"".

! SoftWLC 1.18 ESR BRAS - PCRF BRAS, ESR.

← → ↺ 🏠

100.110.0.148:8080/epadmin/main.htm?menu=bras&vp=default&hl=ru

Конструктор порталов
Версия: 1.15-101 (12.08.19 09:50:27)

Стартовая страница

Галерея изображений

Системные настройки ▾

Конструктор порталов

Уведомления

Доступ к NBI

Доступ к NGW

Взаимодействие с BRAS

Взаимодействие с BRAS

Взаимодействие с BRAS ☒

Секретный ключ RADIUS

Секретный ключ BRAS

Порт CoA

Таймаут подключения (в секундах)

Сохранить

:

- " BRAS" - ;
- " " - testing123;
- " BRAS" - testing123;
- " CoA" - 3799;
- " (") - 10.

"".

2.1) http://<ip >:8080/wifi-cab/ " PCRF" " URL" "" (. 4.2.1):

Создать список URL

Имя *

welcome

Домен *

root

Тип

White

URL: Шаблоны: IP/MASK: IP/MASK (TCP):

Импорт из файла

Кликните дважды для редактирования

Url

Поиск

... http://100.123.0.2:8080/eltex_portal/

Save Cancel

Сохранить Отменить

. 4.2.1.

:

- "" - welcome;
- "" - root;
- "" - white;
- "URL" -  "http://<ip >:8080/eltex_portal/".

"Save" "" .

2.2) gosuslugi (.4.2.2), BRAS filter-name remote gosuslugi:

Создать список URL

Имя *

gosuslugi

Домен *

root

Тип

White

URL:

Шаблоны:

IP/MASK:

IP/MASK (TCP):

+

-

Импорт из файла

Кликните дважды для редактирования

☐

Url

Поиск

☐

^((https|http):\\)(.+)?gosuslugi\.ru

☐

^((https|http):\\)(.+)?gu-st\.ru

☐

^http://esia-portal1\.test\.gosuslugi\.ru/

☐

^http://esia\.gosuslugi\.ru/

☐

^https://esia-portal1\.test\.gosuslugi\.ru/

☐

^https://esia\.gosuslugi\.ru/

Сохранить

Отменить

. 4.2.2

SoftWLC , : [Wi-Fi \(SoftWLC\)](#).

3) " " , " PCRF" "" (. 4.3.1):

Создать новый сервис

+

×

Имя сервиса *

WELCOME ?

Домен *

root ?

Класс трафика *

WELCOME ?

Квота по времени

? Секунды

Квота по трафику

? Байт

Сброс по часовому поясу домена

Не задан ?

Интервал отправки аккаунтинга, с *

300 ?

Приоритет *

4 ?

Возможность прохождения IP потоков

Разрешить IP поток в оба нап ?

Фильтры URL

Действие по умолчанию *

URL по умолчанию *

redirect

▼

http://100.123.0.2:8080/eltex_portal/welcome

Имя фильтра

welcome ▼

Добавить

Удалить

Действие

permit ▼

Выбранные фильтры

Имя фильтра	Действие	URL
welcome	permit	

Сохранить

Отменить

. 4.3.1.

:

- " " - WELCOME;
- " " - root;
- " " - WELCOME.

! , ESR ip access-list extended WELCOME, , .. access-list ESR . / BRAS ;

- " " - 600;
- " " - 4;
- " IP " - IP ;
- " " - redirect;
- "URL " - http://<ip >:8080/eltex_portal/welcome;
- " " - welcome ();
- " " - permit;
- " " - " ".

" " , " " .

4) " PCRF" "BRAS VRF" (. 4.4.1):

Подсети L2	BRAS VRF	Информация PCRF	CoA log	MAC адреса	Списки url
Обновить	Добавить	Редактировать	Удалить	Экспорт	
<input type="checkbox"/>	VRF	Port	Secret		
<input type="checkbox"/>	1	3799	testing123		

. 4.4.1.

BRAS VRF. VRF , , , CoA- ESR - " " , (. 4.4.2):

Редактировать BRAS VRF

VRF *

1

?

Port *

3799

?

Secret *

testing123


?

Сохранить

Отменить

. 4.4.2.

"" , SoftWLC 1.17 .

5.1) EMS, eltex (), () ESR (. 4.5.1):

Апплет Устройства Управление RADIUS Wireless Netconf События Утилиты Адм

Синхронизация

Сохранить

Применить

Поиск

?

EMS

AllClients

eltex

Добавить объект

Имя объекта

ESR_BRAS_L2

Тип

ESR1000

IP адрес

100.110.0.176

Домен

Добавить

Отменить

Активные аварии

Список устройств

Дата:

Страница: 0 / 0

на страницу

Изменить поля

Обновить

ID

Дата создания

. 4.5.1.

- :
- "" - ESR_BRAS_L2 ();
 - "" - , ESR1000;
 - "IP " - IP , SoftWLC.
- "" .

5.2) ESR (, -  EMS) "" , "" (. 4.5.2):

Описание Мониторинг Конфигурация **Доступ**

Обновить Редактировать

Редактировать 'Доступ'

Описание	нет
IP адрес	100.123.0.176
Nas IP address	
SNMP порт	161
SNMP транспорт	UDP
Файловый протокол	TFTP
Таймаут обмена, мс	60000
Read community / User v3	public11
Write community / Password v3	private1
Версия SNMP	v2c
Регистрация трапов	Accept
Выведено из обслуживания	<input type="checkbox"/>
Дата 'Выведено из обслуживания'	15.08.2019 17:39:52
Статус	WRONG
Время статуса	15.08.2019 17:41:52
Telnet/SSH login	
Telnet/SSH password	
SSH порт	22
MAC адрес	
BRAS сервис	<input checked="" type="checkbox"/>
Режим ESR	Station
OTT (Over-the-top)	None
Режим кластера	None
Дата инициализации устройства	15.08.2019 17:39:52

☒ Принять
 ☒ Заполнить местоположение
 ☒ Заполнить геокоординаты
 ☒ Отменить

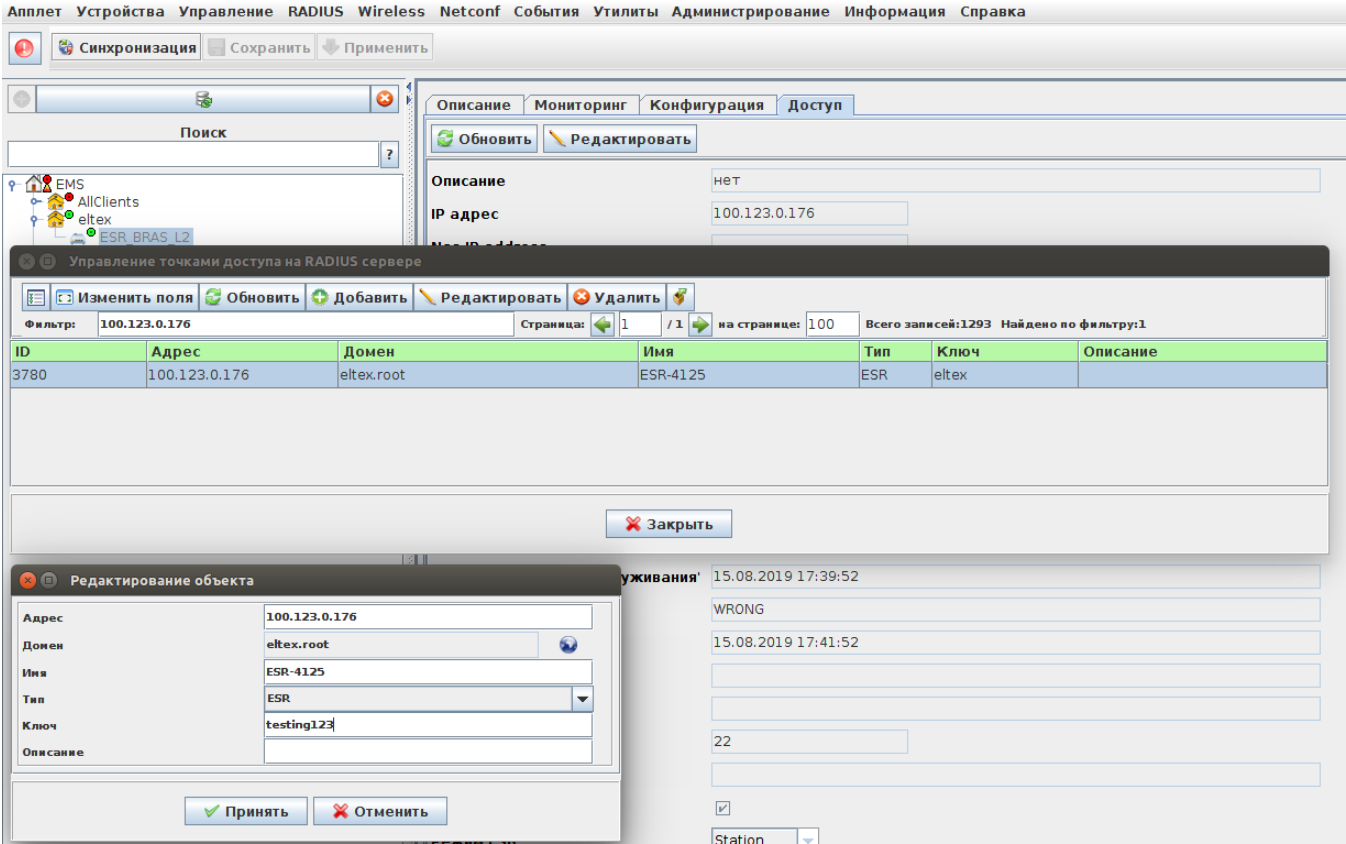
. 4.5.2.

:

- " " - FTP;
- "Read community / User v3" - public11;
- "Write community / Password v3" - private1;
- "BRAS " - .


" " .

5.3) EMS radius, ESR SoftWLC. "RADIUS" " ", ESR (- IP) , (. 4.5.3):



. 4.5.3.

"" testing123 "", " RADIUS ".

 ESR localhost (127.0.0.1), 127.0.0.1 , .

4.2.

PCRF (),
" " PCRF" - " "(. 4.2.1):

Создать новый сервис

Имя сервиса *

INTERNET

Домен *

root

Класс трафика *

INTERNET

Квота по времени

?

Секунды

Квота по трафику

?

Байт

Сброс по часовому поясу домена

Не задан

Интервал отправки аккаунтинга, с *

300

Приоритет *

10

Возможность прохождения IP потоков

Разрешить IP поток в оба нап

Фильтры URL

Действие по умолчанию *

permit

Имя фильтра

Добавить

Удалить

Действие

permit

Выбранные фильтры

Имя фильтра	Действие	URL

Сохранить

Отменить

. 4.2.1.

- " " - INTERNET (, , " ");
- "" - root;
- "" - INTERNET.

! , ESR ip access-list extended INTERNET, ... access-list ESR . / BRAS ;

- " , " - 300;
- "" - 10;
- " IP " - IP ;
- " " - permit;
- URL .

"".

" " "" "PCRF/BRAS", BRAS (. 4.2.2):

Статистика Hotspot

Статистика Enterprise

Сервисы и тарифы

Тарифы

Сервисы PCRF

PCRF сценарии

Фильтр: PCRF/BRAS

Имя

Домен

Обновить

Очистить

Добавить

Редактировать

Удалить

Экспорт

. 4.2.2.

"" - " " (. 4.2.3):

Создать новый тариф

Наименование *

internet

Описание

Код тарифа *

internet

Домен *

root

Время жизни сессии

12
Часы

Время жизни сессии при бездействии пользователя *

15
Минуты

Интервал отправки аккаунтинга, с *

300

Количество одновременных сессий с одним логином и паролем

Цена, руб.

Состав услуг

Сценарии

Сервисы

☒ INTERNET
☐ WELCOME

Сохранить

Отменить

. 4.2.3.

:

- "" - internet (, , " ");
- "" - internet (, , " ");
- "" - root;
- "" - 12 . , . BRAS , mac ;
- "" - 15 ;
- "" - "INTERNET".

! "WELCOME" ! - BRAS .

"C".

4.3. ,

, SSID, L2. , . SSID ; vlan SSID - . SSID. :

- 1) (-);
- 2) SSID EMS;
- 3) L2 .

1.1) <http://<ip>:8080/epadmin> **Создать новый портал**, (. 4.3.1):

Создать новый виртуальный портал

Имя виртуального портала

eltex

Домен области видимости

eltex.root

Сохранить

Отмена

. 4.3.1.



:

- " " - eltex;
- " " - eltex.root.

"" .

1.2) , "eltex" "" "default", (. 4.3.2):

Тарифы

Русский  admin 

Тарифы

Тарифы для BRAS (реклама, опросы)

Тариф	Код	Домен	Название тарифа на портале	
▼ Работа с ТД				
default	default	root	<div>Default</div>	<div>Удалить</div>

. 4.3.2.

BRAS, " BRAS" - , . Eltex - "" .

1.3) "" (. 4.3.3)

Поиск...

<input checked="" type="checkbox"/>	Тариф	Код	Домен
<input type="checkbox"/>	Работа через BRAS		
<input checked="" type="checkbox"/>	internet	internet	root

Добавить

Отмена

. 4.3.3.

"internet", "", " BRAS".

1.4) "" (. 4.3.4):

Конструктор порталов
Версия: 1.14-75 (30.07.19 15:56:40)

Стартовая страница

Галерея изображений

Системные настройки

Личный кабинет

Порталы

eltex

Общие настройки

Языковые настройки

Рекламные площадки

Работа по расписанию

Сервис оплаты

Тарифные планы

Внешний вид

Создать новый портал

Выбрать другой (доступно: 6)

Тарифные планы




Русский admin

Тариф	Код	Домен	Название тарифа на портале	
Работа с ТД				
Hotspot Default	default	root	Hotspot Default	Удалить
Работа через BRAS				
internet	internet	root	internet	Удалить

. 4.3.4.

., -. SMS-, call : v1.18_

2.1) EMS "Wireless" "SSID" "SSID" "SSID" - SSID (. 4.3.5):

Тип	Hotspot
Имя	★ SSID1
Описание	
Domain	★ eltex.root
Статус SSID	Operational
Дата создания	2020-12-10 07:37:27
Дата изменения	2020-12-10 09:51:02
----- Опции -----	
Bridge Location	data10
VRF	1
Switch Community	<input type="checkbox"/>
Требовать наличие Opt82	<input type="checkbox"/>
Статус VAP	Up
Режим трафика VAP (только для GRE)	Tunnel
Broadcast SSID	<input checked="" type="checkbox"/>
Radio	All
Режим безопасности	Без шифрования
MAC Auth Type	Disable
Статус Client QoS	on
VLAN-ID	<input checked="" type="checkbox"/> 2336
QoS method (down link)	802.1p
VLAN trunk	<input type="checkbox"/>
General Mode	<input type="checkbox"/>
General VLAN-ID	1
802.1p priority (up link)	0
Изоляция клиентов	<input type="checkbox"/>
Band steer	<input checked="" type="checkbox"/>
Support 802.11k	<input type="checkbox"/>
Wireless Multicast Forwarding	<input type="checkbox"/>
Hotspot 2.0	<input type="text"/> 
DiffServ Policy Up	<input type="text"/> 
DiffServ Policy Down	<input type="text"/> 
Bandwidth Limit Up, kbps	0
Bandwidth Limit Down, kbps	0
VAP Limit Up, kbps	0
VAP Limit Down, kbps	0
DPI (Step Logic)	<input type="checkbox"/>
----- Minimal signal -----	
Enabled	<input type="checkbox"/>
----- Captive portal -----	
Enabled	<input type="checkbox"/>
Virtual portal name	eltex
----- Расписание работы ----- ?	
Включить	<input type="checkbox"/>





✓ Принять
✗ Отменить



:

- "" - Hotspot;
- "" - SSID1;
- "Domain" - eltex.root;
- "Bridge, Location" - data10 - location, ESR;
- "Vlan-ID" - 2336;
- "Virtual portal name" - eltex - , .

"".

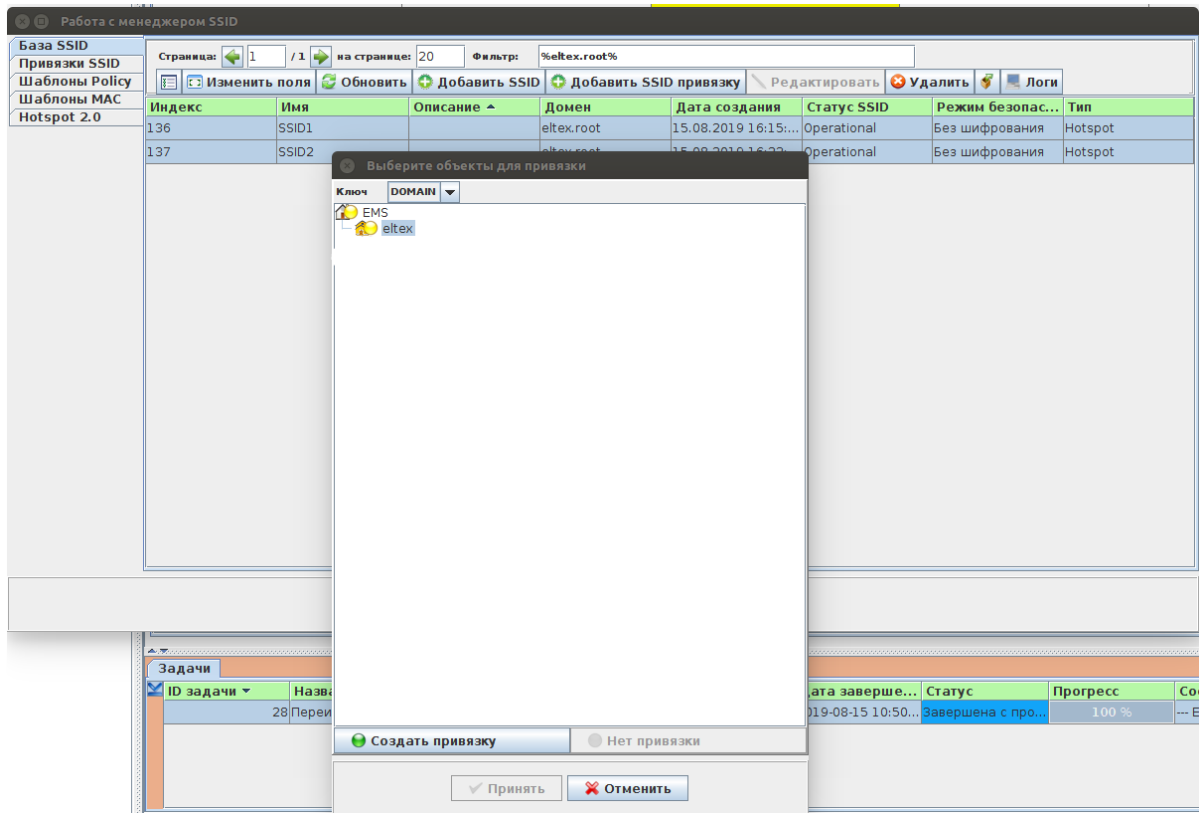
.. SSID - SSID vlan 2337 (. 4.3.6):

Тип	Hotspot
Имя	★ SSID2
Описание	
Domain	★ eltex.root
Статус SSID	Operational
Дата создания	2020-12-10 09:40:45
Дата изменения	2020-12-10 09:51:15
----- Опции -----	
Bridge Location	data10
VRF	1
Switch Community	<input type="checkbox"/>
Требовать наличие Opt82	<input type="checkbox"/>
Статус VAP	Up
Режим трафика VAP (только для GRE)	Tunnel
Broadcast SSID	<input checked="" type="checkbox"/>
Radio	All
Режим безопасности	Без шифрования
MAC Auth Type	Disable
Статус Client QoS	on
VLAN-ID	<input checked="" type="checkbox"/> 2337
QoS method (down link)	802.1p
VLAN trunk	<input type="checkbox"/>
General Mode	<input type="checkbox"/>
General VLAN-ID	1
802.1p priority (up link)	0
Изоляция клиентов	<input type="checkbox"/>
Band steer	<input checked="" type="checkbox"/>
Support 802.11k	<input type="checkbox"/>
Wireless Multicast Forwarding	<input type="checkbox"/>
Hotspot 2.0	<input type="text"/> 
DiffServ Policy Up	<input type="text"/> 
DiffServ Policy Down	<input type="text"/> 
Bandwidth Limit Up, kbps	0
Bandwidth Limit Down, kbps	0
VAP Limit Up, kbps	0
VAP Limit Down, kbps	0
DPI (Step Logic)	<input type="checkbox"/>
----- Minimal signal -----	
Enabled	<input type="checkbox"/>
----- Captive portal -----	
Enabled	<input type="checkbox"/>
Virtual portal name	eltex
----- Расписание работы -----	
Включить	<input type="checkbox"/>

 Принять
  Отменить

vlan SSID.

2.2) SSID - SSID1 SSID2 "SSID". (. 4.3.7):



. 4.3.7.

"" - DOMAIN, eltex, SSID "". "" - .
- "SSID" - "",.. Eltex SSID. EMS .

3.1) "PCRF" "L2" "". "" (. 4.3.8):

Добавить подсеть

Наименование

eltex_2336

Тип

Сервис

NAS IP

100.123.0.176

NAS MAC

VRF

1

Location интерфейса

gi1/0/1.2336

Service домен

eltex.root

Имя Портала

eltex

AP домен

eltex.root

ID ТД

SSID

SSID1:eltex.root

Сохранить
Отменить

. 4.3.8.

:

- "" - eltex_2336 (, , " _");
- "" - ;
- "NAS IP" - 100.123.0.176 (ESR);
- "Location " - gi1/0/1.2336 (-, SSID1);
- "Service " - eltex.root;
- " " - eltex;
- "AP " - eltex.root;
- "SSID" - SSID1:eltex.root



! , SSID "Service " "Domain" SSID.

"".

L2 SSID (. 4.3.9):

Добавить подсеть
×

Наименование

?

Тип *

Сервис ▾

NAS IP *

?

NAS MAC

?

VRF

Location интерфейса *

?

Service домен *

eltex.root

Имя Портала *

eltex ▾

AP домен

eltex.root

ID ТД

?

SSID *

SSID2:eltex.root

Сохранить

Отменить

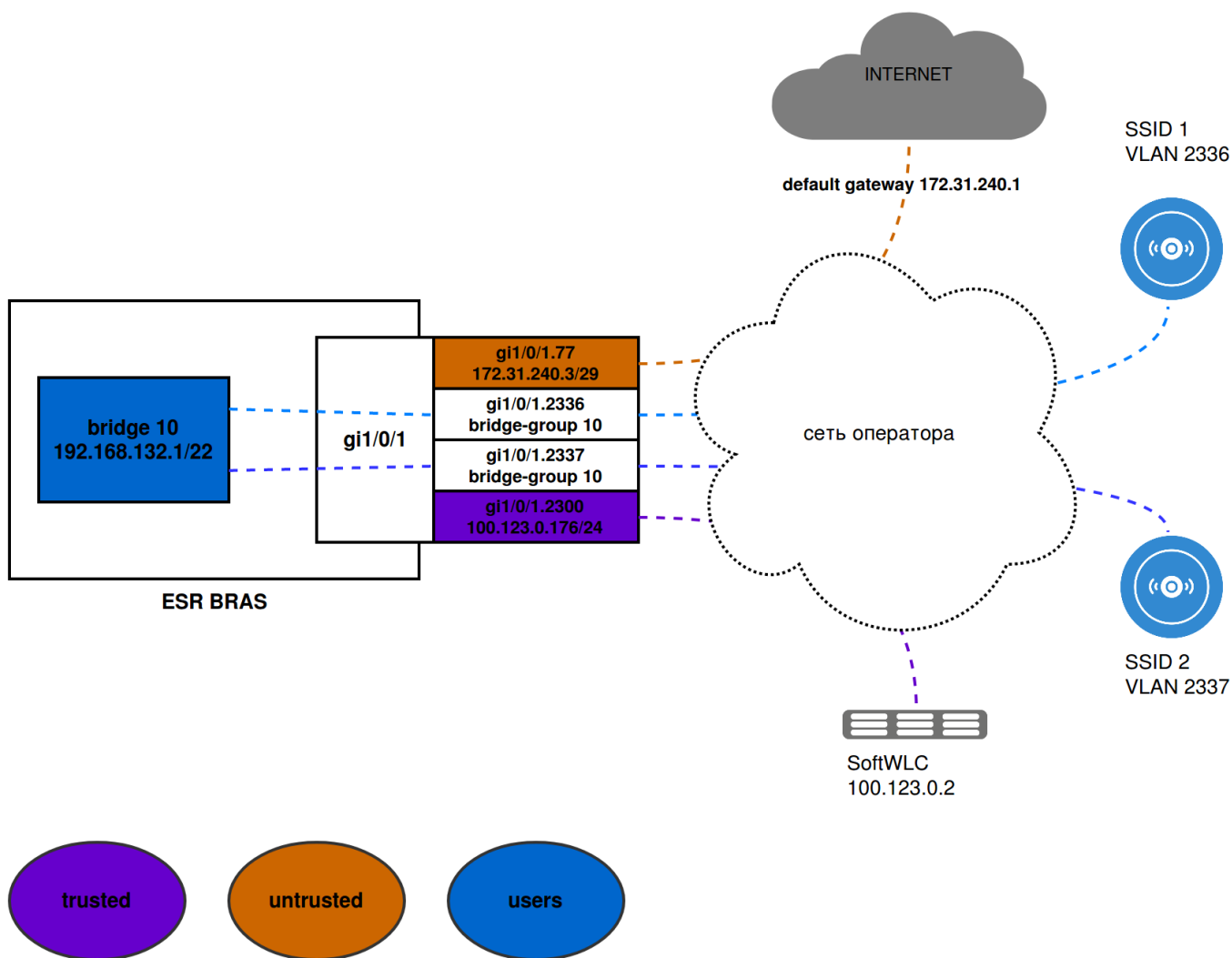
. 4.3.9.

SoftWLC BRAS , vlan , . BRAS : [BRAS. Troubleshooting Guide](#)

5. firewall ESR

ESR . BRAS . - ESR, SoftWLC .

ESR L3 - L3 security zone (). security zone-pair. trusted, untrusted users . , - self all. . 5.1 ESR :



. 5.1.

- Bridge 10 - users.

! - gi1/0/1.2336 gi1/0/1.2337 bridge 10, ip users. security-zone ;

- Gi1/0/1.3500 - untrusted, .. ;
- Gi1/0/1.2300 - trusted, .. ;
- , ESR self.

:

- users untrusted () ;
- ESR trusted self ;
- trusted users , ;
- dhcp-discover users self, ;
- dhcp-request users trusted, DHCP, ;
- DNS users trusted, DNS, ;
- ESR, users self.

ESR.

dhcp, dns:

```
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service dns
  port-range 53
exit
object-group service redirect
  port-range 3128-3159
exit
```



! object-group service redirect , . ESR. [1.4.1](#) [ESR 1.4.0](#) [1.4.1](#)

:

```

security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted self
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted users
  rule 1
    action permit
    enable
  exit
exit
security zone-pair users self
  rule 1
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port redirect
    enable
  exit
exit
security zone-pair users trusted
  rule 1
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match destination-port dns
    enable
  exit
exit

```

, :

```

bridge 10
  no ip firewall disable
exit

interface gigabitethernet 1/0/1.3500
  no ip firewall disable
exit
interface gigabitethernet 1/0/1.2300
  no ip firewall disable
exit

```

.

. ESR BRAS .

6.

6.1. ESR

ESR:

```
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service dns
  port-range 53
exit
object-group service redirect
  port-range 3128-3131
exit

object-group network users
  ip prefix 192.168.132.0/22
exit
object-group network SoftWLC
  ip address-range 100.123.0.2
exit
object-group network bras_users
  ip address-range 192.168.132.2-192.168.135.254
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 100.123.0.176
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

security zone trusted
exit
security zone untrusted
exit
security zone users
exit

ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
```



```

    action permit
    match protocol tcp
    match destination-port 8443
    enable
exit
rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
exit
rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
exit
exit

ip access-list extended INTERNET
    rule 1
        action permit
        enable
    exit
exit

ip access-list extended unauthUSER
    rule 1
        action permit
        match protocol udp
        match source-port 68
        match destination-port 67
        enable
    exit
    rule 2
        action permit
        match protocol udp
        match destination-port 53
        enable
    exit
exit

subscriber-control filters-server-url http://100.123.0.2:7070/filters/file
subscriber-control
    aaa das-profile COA
    aaa sessions-radius-profile PCRF
    aaa services-radius-profile PCRF
    nas-ip-address 100.123.0.176
    session mac-authentication
    bypass-traffic-acl unauthUSER
    default-service
        class-map unauthUSER
        filter-name remote gosuslugi
        filter-action permit
        default-action redirect http://100.123.0.2:8080/eltex_portal/
    exit
    enable
exit

snmp-server
snmp-server system-shutdown
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 100.123.0.2
    source-address 100.123.0.176
exit

bridge 10
    description "users"
    security-zone users

```

```
ip address 192.168.132.1/22
ip helper-address 100.123.0.2
service-subscriber-control object-group bras_users
location data10
protected-ports local
enable
exit

interface gigabitethernet 1/0/1.3500
description "UpLink"
security-zone untrusted
ip address 172.31.240.3/29
exit
interface gigabitethernet 1/0/1.2300
description "mgmt"
security-zone trusted
ip address 100.123.0.176/24
exit
interface gigabitethernet 1/0/1.2336
bridge-group 10
exit
interface gigabitethernet 1/0/1.2337
bridge-group 10
exit
security zone-pair users untrusted
rule 1
action permit
enable
exit
exit
security zone-pair trusted self
rule 1
action permit
enable
exit
exit
security zone-pair trusted users
rule 1
action permit
enable
exit
exit
security zone-pair users self
rule 1
action permit
match protocol udp
match source-port dhcp_client
match destination-port dhcp_server
enable
exit
rule 2
action permit
match protocol tcp
match destination-port redirect
enable
exit
exit
security zone-pair users trusted
rule 1
action permit
match protocol udp
match source-port dhcp_client
match destination-port dhcp_server
enable
exit
rule 2
action permit
match protocol udp
match destination-port dns
enable
exit
```

```

exit

nat source
  pool nat_addr
    ip address-range 172.31.240.3
  exit
  ruleset nat_source
    to zone untrusted
    rule 1
      match source-address users
      action source-nat pool nat_addr
      enable
    exit
  exit
exit

ip dhcp-relay

ip route 0.0.0.0/0 172.31.240.1

ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit

```

6.2

WiFi , , . :

http://<IP- >:< >/eltex_portal/?router=bras&clientIp=<IP- >&clientMac=<MAC- >&nasIp=<NAS-IP >&sessionId=< >&vrf=< VRF>&loc=<location>&L2loc=<L2 location>&origUrl=< , >

ESR:

```

http://100.123.0.2:8080/eltex_portal/?router=bras&clientIp=192.168.132.10&clientMac=a8:9c:ed:53:a9:6d&nasIp=100.123.0.176&sessionId=12393906174523604993&vrf=1&loc=data10&L2loc=gil/0/1.2336&origUrl=http://eltex-co.ru

```