Cisco ISG

Возможности

- Поддержка авторизации и аккаунтинга
- Поддержка нескольких сервисов тарифного плана.
- Пользовательский портал авторизации и управления акаунтом.
- Перенаправление должников на портал с уведомлением о израсходованном балансе.
- Турборежимы. Возможность индивидуального включения, отключения, блокировки.
- Фильтры негативного депозита с возможностью присвоение отдельного сервиса для пользователей с негативным депозитом.
- Авторизация на основе данных DHCP сервера для использования в многосегментных сетях когда мак адрес недоступен для ISG.

ISG Авторизация пользователя

При подключении пользователя к интернету - NAS (Cisco ISG) отправляет запрос на авторизацию к RADIUS, если RADIUS не находит идентификатор пользователя (IP или MAC) тогда пользователя перенаправляет на портал. Там он нажимает кнопку авторизироваться, система через авторизатор ищет его индентификатор, если он не прописан в поле CID прописывает его туда и отправляет запрос авторизировать сессию на Cisco ISG. После получения запроса на повторную авторизацию Cisco ISG отправляет повторно запрос на RADIUS с идентификатором пользователя (IP или MAC) и RADIUS авторизирует его. Идентификатор пользователя прописывается в поле CID.

Если используется многосегментная сеть и Cisco ISG не может идентифицировать MAC клиента, а отправляет только IP то в таком случае ABillS может автоматически определять и авторизировать пользователей по MAC адресу исходя из данных DHCP сервера.

После авторизации абонента Cisco ищет параметры сервиса абонента **Cisco-Service-Info=«ATP_10_0_15»** если данные о сервисе не найдены в кеше системы отправляется запрос на радиус с логинов в в виде названия сервиса **TP_10_0_15** (User-Name=TP_10_0_15). На данный запрос приходят параметры сервиса абонента. **Будьте внимательны при изменении параметров скорости в тарифном плане нужно почистить кешь сессий в Cisco иначе будут присваиваться старые настройки сессий**

Классы трафика

При необходимости система может вести учёт и разделение трафика на разные классы Internet, UA-IX, город и т д.
Для включения данной возможности оператору следует завести классы трафика в биллинге.

При запросе сервиса для тарифного плана 10 и класса трафика 1 (UA-IX) со пропускной скоростью (640kbit/500kbit) RADIUS отправляет следующие параметры.

```
Cisco-Service-Info = QU;640000;80000;160000;D;500000;62500;125000;,
cisco-avpair += ip:traffic-class=input access-group name ACL_IN_INTERNET_1 priority 200,
cisco-avpair += ip:traffic-class=output access-group name ACL_OUT_INTERNET_1 priority 200,
cisco-avpair += ip:traffic-class=out default drop,
cisco-avpair += ip:traffic-class=in default drop,
cisco-avpair += subscriber:accounting-list=BH_ACCNT_LIST_1
```

ACL_IN_INTERNET_1 - является аксеслистом с указанными сетями для данного класса трафика и з более низким приоритетом чем в глобального трафика. **BH_ACCNT_LIST_1** - Является меткой аккаунтинга.

Авторегистрация абонента

При первом подключении абонента перенаправляет на «Пользовательский портал». Абонент заходит в личный кабинет.
При входе в личный кабинет система идентифицирует сессию абонента отправляет RADIUS CoA на сервер доступа. Если сессии найдена абоненту предлагается зарегистрировать MAC для дальнейшего пользования услугой Internet, если сессия абонента не найдена на коммутаторе система предупреждает об этом абонента.
Если сессия найдена абонент нажимает кнопку активировать аккаунт.
С момента нажатия кнопки активируются сервисы абонента и система предоставляет ему доступ к интернету. Если абонент изменил MAC адрес ему нужно по новому пройти процедуру авторегистрации.

ISG Errors

Для более эффективной работы службы поддержки были внедрены следующие коды ошибок возникающих при работе клиента с пользовательским порталом.

Код	Ошибка	Решение
ISG Errors		
911	Not exist user ID (MAC or IP) on Cisco ISG	Check IP/MAC on Cisco ISG NAS
912	DHCP Error. Can't find User IP in DHCP server.	**Check IP in:** Monitoring→DHCP DHCP leases file. leases2db.pl
913	Not registred IP Address. Can't find your NAS.	Add user IP to NAS IP Pools
914	Negative Deposit	User have negative deposit and can't use service
915	Service Disabled	Service is disabled for user by Administrator
916	Account Disabled	Account is disabled for user by Administrator
917	Not Active Не активизирована услуга	Услуга не включена

Ошибки включения сервиса

Service Activate Errors		
100	Unknow error	Unknow error
101	Turbo mode enable Error	Error in TURBO MODE activation process.
102	User activation Error	System can't add user IP/MAC to CID field
103	IP Discovery mode failed. Unknown error	Can't add user IP to Dhcphosts
104	IP Discovery mode failed. Dublicate IP/MAC	Some of parameters Exists in Dhcphosts table.
106	No responce from CoA server 'xxx.xxx.xxx.xxx'	Нет определения статуса сессии. Запрос управления CoA не проходит.
112	DHCP $_ERROR MAC: $_NOT_EXIST IP: 'xxx.xxx.xxx.xxx'	Система не может определить MAC адрес абонента. Проверте присутствует ли адрес в журнале /Мониторинг/Dhcp/.
114	$ERR_IP_ADDRESS_CONFLICT	Конфликт адресов. адрес прописан статически на другом абоненте
118	$_ERROR: Dublicate	Попытка добавить уже существующий адрес
119	$_ERROR: DHCP add hosts error	Другая ошибка добавления
120	$_ERROR: Can't find assign network IP: 'xxx.xxx.xxx.xxx'	Нельзя найти гостевую сеть для определения рабочей сети. Смотрите параметр $conf{DV_IP_DISCOVERY} на предмет присутствия сети
121	Not active. Не активизирован	MAC абонента не активизирован или отличается от активизированного в системе. Нужно пере активизировать MAC абонента

Настройка Cisco

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISG-1
!
boot-start-marker
boot-end-marker
!
```

```
enable secret 5 $1$WWW/$4otH.1GYuWkFaQp25MJ.V1
!
aaa new-model
!
!
aaa group server radius ISG-RADIUS
 server 10.0.0.1 auth-port 1812 acct-port 1813
!
aaa authentication login default group tacacs+ local
aaa authentication login ISG-AUTH-1 group ISG-RADIUS
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization network ISG-AUTH-1 group ISG-RADIUS
aaa authorization subscriber-service default local group ISG-RADIUS
aaa accounting update periodic 1 jitter maximum 0
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network ISG-AUTH-1 start-stop group ISG-RADIUS
!
!
!
!
! coa interface
aaa server radius dynamic-author
 client 10.0.0.1
 server-key isgcontrol
!
aaa session-id common
clock timezone AZST 5
ip subnet-zero
!
!
ip dhcp relay information policy keep
ip dhcp relay information trust-all
!
ip cef
ip domain name mydomain.com
ip ssh version 2
!
!
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
username letsac privilege 15 secret 5 $1$jHQz$bkaihoHMi6.Eq4ifYnUgH/
!
redirect server-group REDIRECT_NOPAY
   server ip 10.0.0.1 port 80
class-map type traffic match-any CLASS-TO-REDIRECT
 match access-group input 197
 match access-group output 197
!
class-map type control match-all ISG-IP-UNAUTH
 match timer UNAUTH-TIMER
 match authen-status unauthenticated
!
policy-map type service LOCAL_L4R
 ip access-group 197 in
 ip access-group 197 out
 1 class type traffic CLASS-TO-REDIRECT
  redirect to group REDIRECT_NOPAY
 !
!
policy-map type control ISG-CUSTOMERS-POLICY
 class type control ISG-IP-UNAUTH event timed-policy-expiry
  1 service disconnect
 !
```

```
 class type control always event quota-depleted
  1 set-param drop-traffic FALSE
 !
 class type control always event credit-exhausted
  1 service-policy type service name LOCAL_L4R
 !
 class type control always event session-start
  10 authorize aaa list ISG-AUTH-1 password ISG identifier source-ip-address
  20 set-timer UNAUTH-TIMER 1
  30 service-policy type service name SERVICE_L4R
 !
 class type control always event session-restart
  10 authorize aaa list ISG-AUTH-1 password ISG identifier source-ip-address
  20 set-timer UNAUTH-TIMER 1
  30 service-policy type service name SERVICE_L4R
 !
 class type control always event account-logon
  10 authenticate aaa list ISG-AUTH-1
  20 service-policy type service unapply name SERVICE_L4R
 !

interface GigabitEthernet0/1.40
 description SUBSCRIBERS SUBNET 10.0.0.2/24
 encapsulation dot1Q 40
 ip dhcp relay information trusted
 ip address 10.0.0.2 255.255.255.0
 ip helper-address 10.0.0.1
 service-policy type control ISG-CUSTOMERS-POLICY
 ip subscriber routed
  initiator unclassified ip-address
!
logging trap notifications
logging origin-id hostname
logging 10.0.0.1
logging host  10.0.0.1 transport udp port 6032
!Billing
access-list 195 permit ip host 10.0.0.1 any
access-list 195 permit ip any host 10.0.0.1
access-list 195 deny   ip any any
! Without billing
access-list 196 deny   ip host 10.0.0.1 any
access-list 196 deny   ip any host 10.0.0.1
access-list 196 permit ip any any
! Redirect rules
access-list 197 permit tcp any any eq www
access-list 197 permit tcp any eq www any
access-list 197 permit udp any any eq domain
access-list 197 permit udp any eq domain any
access-list 197 deny   ip any any
! Acces rule for guest users
access-list 198 permit tcp any any eq www
access-list 198 permit tcp any eq www any
access-list 198 permit udp any any eq domain
access-list 198 permit udp any eq domain any
access-list 198 permit tcp any any eq 9443
access-list 198 permit tcp any eq 9443 any
access-list 198 deny ip any any
!
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 31 mac format unformatted
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 key radisg
radius-server vsa send cisco-nas-port
radius-server vsa send accounting
radius-server vsa send authentication
!
```

RADIUS Server	10.0.0.1
WEB server	10.0.0.1
DHCP server	10.0.0.1

ABillS

Настройка сервера доступа

файл настройки **config.pl**

включение модуля авторизации

```
$AUTH{cisco_isg} = 'Mac_auth2';
$ACCT{cisco_isg} = 'Acct2';
```

Включение поддержки Cisco ISG в пользовательском портале

```
$conf{INTERNET_ISG}=1;
```

$conf{ISG_SERVICES}='NTURBO_SPEED1;NTURBO_SPEED1;ABILLING_ACCESS';	Описание дополнительных сервисов авторизации. Первая буква сигнализирует запускать ли сервис при старте сессии (A)
$conf{ISG_ACCOUNTING_GROUP}='ISG-AUTH-1';	аккаунтинг группа. По умолчанию ISG-AUTH-1
$conf{DHCPHOSTS_ISG}=1;	При использовании Freeradius DHCP сессии для DHCP вести только в лизес мониторинге
$conf{DHCP_LEASES_NAS}='NAS_ID';	Список серверов которые используются для ведения dhcp leases. Данная опция указывается если для выдачи ISG IP используется ABillS Freeradius DHCP

Настройка сервера доступа / Система/ Сервер доступа/

IP:	IP адрес маршрутизатора
Название:	Название
Тип:	указать тип: cisco_isg

:Управление:

IP:PORT:	адрес и порт для отправки RADIUS CoA команд. (По умолчанию 1700)
Пароль:	пароль для отправки RADIUS CoA команд

Проверяю состояние сессии на роутере:

```
Router#sh sss session
Current Subscriber Information: Total sessions 1

Uniq ID Interface    State         Service      Identifier           Up-time
179     IP           authen        Local Term   123.123.244.194       00:16:27
```

Более детально информация о учитываемом траффике

```
#sh sss session detail
.... пропущено ....

Session inbound features:
```

```
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:999999 - Quota:1000000
   Usage(since last update):161828 - Total:161828
   Current states: Start
Session outbound features:
 Feature: Prepaid Idle Timeout
   Timeout configuration: 120 (seconds)
 Feature: Prepaid Volume Monitor
   Threshold:999999 - Quota:1000000
   Usage(since last update):161828 - Total:161828
   Current states: Start
Configuration sources associated with this session:
Service: PREPAID_INTERNET, Active Time = 00:16:39
```

сброс активных сессий

```
# cle sss session all
```

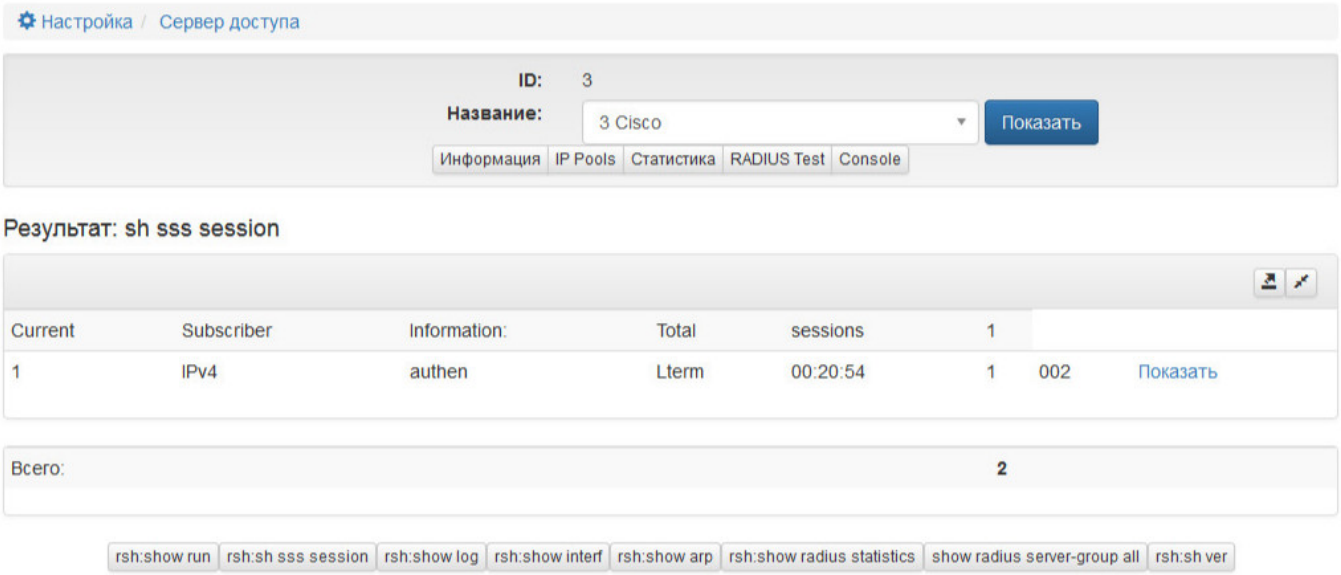
Проверка редиректа

```
sh redirect translations
```

ABillS Console

удобный интерфейс отслеживания и мониторинг сессий абонентов непосредственно на Cisco

/ Настройка / Сервер доступа Активные сессии



Информация по сессии

Результат: sh sss session uid 1

```
Type: IPv4, UID: 1, State: authen, Identity: 002
IPv4 Address: 81.162.119.111
Session Up-time: 00:25:27, Last Changed: 00:25:27
Switch-ID: 4097
Policy information:
  Authentication status: authen
  Active services associated with session:
    name "TP_8", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map ISG-CUSTOMERS-POLICY
      condition always event session-start
        10 authorize aaa list ISG-AUTH-1 identifier source-ip-address
    subscriber rule-map default-internal-rule
      condition always event service-start
        1 service-policy type service identifier service-name
Classifiers:
Class-id    Dir   Packets    Bytes                Pri.  Definition
```

Также доступны команды

- Проверки лога
- Просмотр версии маршрутизатора
- Просмотр конфигурации
- Информация по интерфейсах

Для получения информации используется rsh протокол. Для использования нужно rsh доступ на Cisco для пользователя abills_admin (под которым работает веб сервер).

Включение rsh

```
rsh enable
ip rcmd remote-host abills_admin 10.88.88.1 root enable
username abills_admin privilege 15 nopassword
```

RADIUS Debug

- 10.0.0.2 адрес CISCO ISG
- 10.11.11.1 адрес клиента

Пример гостевого доступа абонента

Запрос авторизации

```
rad_recv: Access-Request packet from host 10.0.0.2 port 1645, id=178, length=121
      User-Name = "10.11.11.1"
      User-Password = "ISG"
      NAS-Port-Type = Virtual
      Cisco-NAS-Port = "0/0/1/40"
```

```
      NAS-Port = 0
      NAS-Port-Id = "0/0/1/40"
      Service-Type = Outbound-User
      NAS-IP-Address = 10.0.0.2
      Acct-Session-Id = "3ED4EBBB00057216"
```

Если абонента не найдено в базе ответ

```
Sending Access-Reject of id 178 to 10.0.0.2 port 1645
      Reply-Message = "User Not Exist '169.254.6.231' /0"
```

Запрос на получение адреса веб портала

```
rad_recv: Access-Request packet from host 10.0.0.2 port 1645, id=179, length=119
      User-Name = "SERVICE_L4R"
      User-Password = "cisco"
      NAS-Port-Type = Virtual
      Cisco-NAS-Port = "0/0/1/40"
      NAS-Port = 0
      NAS-Port-Id = "0/0/1/40"
      Service-Type = Outbound-User
      NAS-IP-Address = 10.0.0.2
      Acct-Session-Id = "3ED4EBBB00057216"
```

ответ:

```
Sending Access-Accept of id 179 to 10.0.0.2 port 1645
      Cisco-AVPair += "ip:l4redirect=redirect list 197 to group REDIRECT_NOPAY"
      Cisco-AVPair += "traffic-class=input access-group 198"
      Cisco-AVPair += "traffic-class=output access-group 198"
      Cisco-AVPair += "ip:traffic-class=out default drop"
      Cisco-AVPair += "ip:traffic-class=in default drop"
      Idle-Timeout = 600
```

Пример PPPoE авторизации

Запрос авторизации

```
rad_recv: Access-Request packet from host 10.0.0.2 port 1645, id=1179, length=119
      Framed-Protocol = PPP
      User-Name = "n9351779"
      CHAP-Password = 0x013d75d54fca0f2f4f189a03a1816b77bf
      NAS-Port-Type = PPPoEoVLAN
      NAS-Port = 0
      NAS-Port-Id = "0/1/1/939"
      Cisco-AVPair = "client-mac-address=0019.dbc7.d1cb"
      Service-Type = Framed-User
      NAS-IP-Address = 10.0.0.2
      Acct-Session-Id = "00D24ADF"
NAS-Identifier = "91.223.105.1"
Event-Timestamp = "Aug  7 2015 06:22:57 MSK"
```

Ответ: успешная авторизация

```
Sending Access-Accept of id 179 to 10.0.0.2 port 1645
  Cisco-Control-Info = QV1000000
  Service-Type = Outbound-User
  Idle-Timeout = 120
  Cisco-Account-Info = NTP_10_0_48
  Cisco-Account-Info = ATP_10_0_48
  Cisco-Account-Info = ABILLING_ACCESS
  User-Name = n9351779
```

```
  Cisco-Service-Info = ATP_10_0_48
```

Абоненту включается услуга тарифного плана с ID **TP_10_0_48** (TP_[ID тарифного плана (tp_id)]-[клас трафика]-[номер временного интервала])

запрос параметров тарифного плана TP_10_0_48

```
rad_recv: Access-Request packet from host 10.0.0.2 port 1645, id=1279, length=119
  User-Name = TP_10_0_48
  NAS-IP-Address = 10.0.0.2
```

ответ по тарифному плану

```
Sending Access-Accept of id 179 to 10.0.0.2 port 1645
  Cisco-Service-Info = QU;1024000;128000;256000;D;1024000;128000;256000;
  Cisco-AVPair = ip:traffic-class=in access-group 196 priority 6
  Cisco-AVPair = ip:traffic-class=out access-group 196 priority 6
  Cisco-AVPair = ip:traffic-class=out default drop
  Cisco-AVPair = ip:traffic-class=in default drop
  Cisco-AVPair = subscriber:accounting-list=ISG-AUTH-1
  Acct-Interim-Interval = 86000
```

Дополнительно

- Очистка кеша сервисов

```
ipconfig /release
```

- Intelligent Service Gateway (ISG) Configuration Library
- Cisco ISG Design and Deployment Guide