Cisco Expo 2008

Применение Cisco ISG для расширенного контроля над абонентскими сессиями

Сергей Гусаров

Системный инженер

segusaro@cisco.com

Содержание

1. Обзор ISG
2. Модели внедрения ISG
3. Примеры конфигураций ISG

Обзор ISG

Эволюция сети оператора связи

Разделенные сети для каждой услуги

Единая сеть «все в одном»

Снижение затрат на управление и обслуживание нескольких сетей

Сеть, обращенная к пользователю

Увеличение дохода с абонента:

- персонализированные услуги
- быстрое внедрение новых услуг
- самостоятельная подписка на услуги и их изменение

Составляющие персонализации

Идентификация

Идентификация пользователя по многим параметрам.
Идентификация происходит:

- **по разным источникам и событиям**
- **сохраняется на все время сессии**

Разнообразные сервисы

Сервисы и политики применяются на основе того:

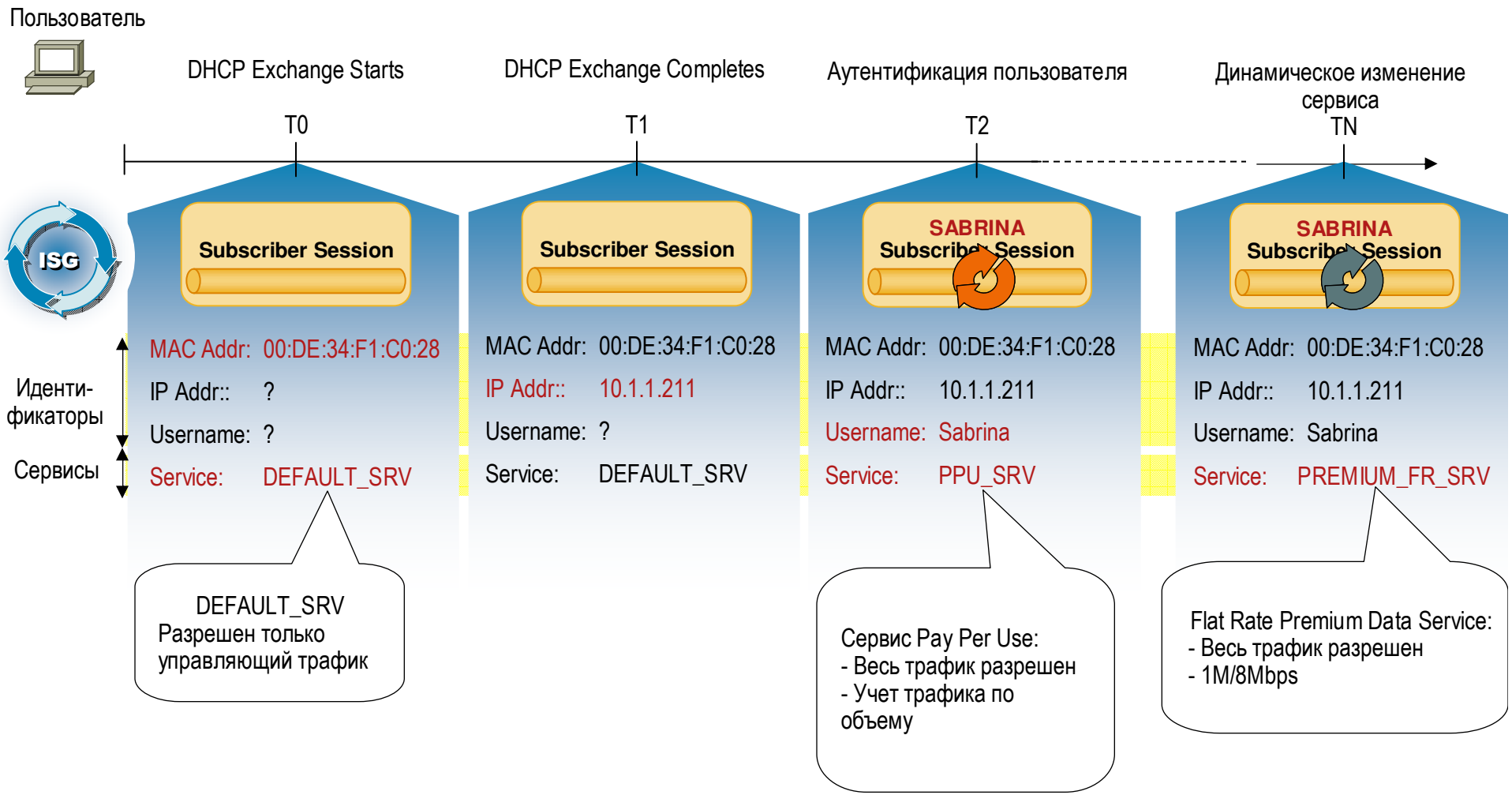
- **Кто этот пользователь**
- **Где он находится**
- **Что ему нужно**

Управление сервисами

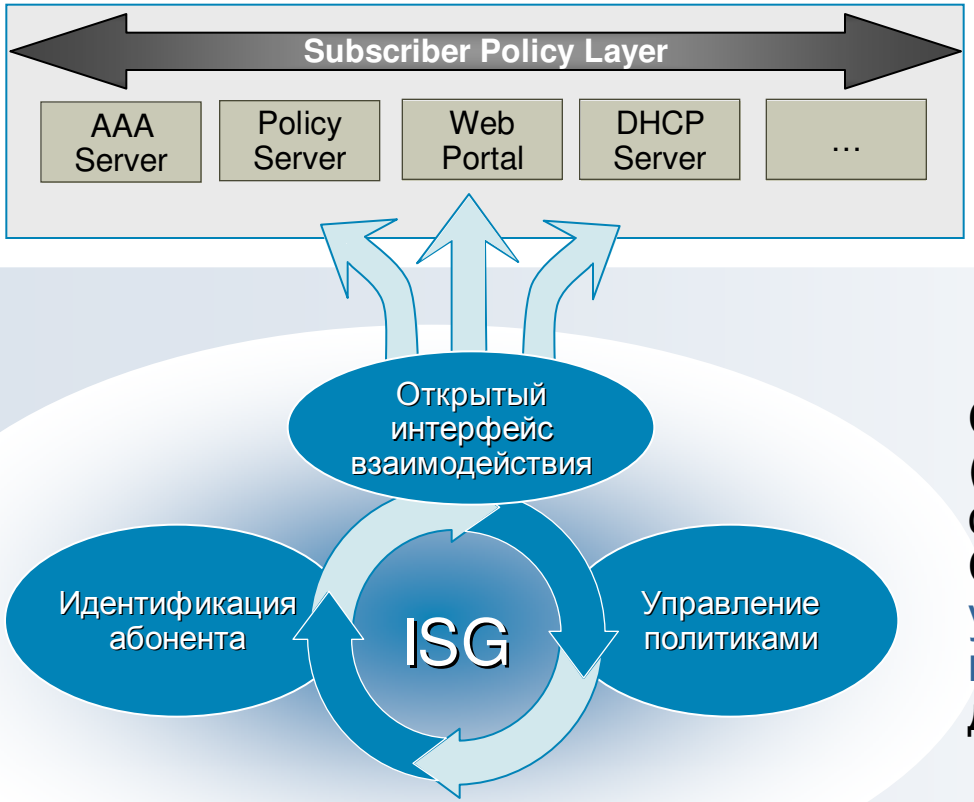
Сервисы и политики изменяются на основе:

- **поведения пользователя**
- **что ему требуется сейчас**

Пример идентификации и применения сервисов



Обзор ISG



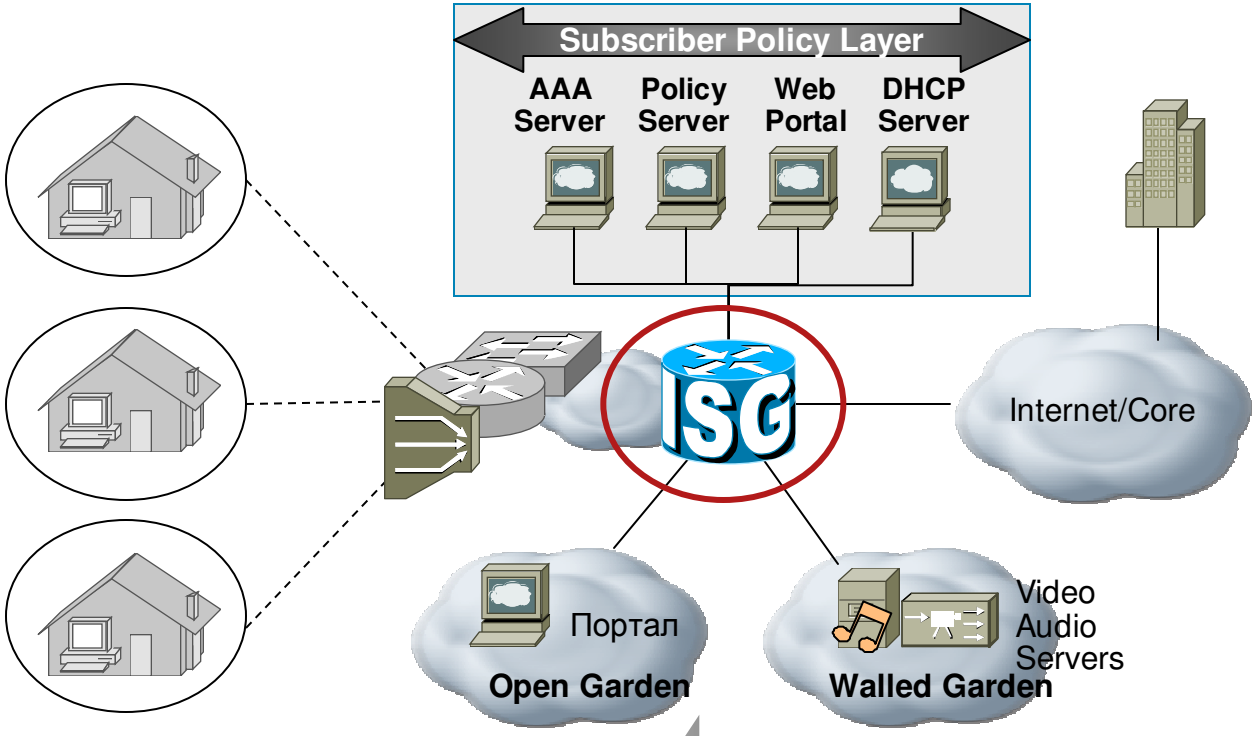
Cisco Intelligent Services Gateway (ISG) – это лицензируемый функционал маршрутизаторов Cisco, обеспечивающий управление сессиями, политиками и сервисами для различных сетей доступа

Устройство, выполняющее эти функции, называется Intelligent Service Gateway router или просто “ISG”

Примеры использования ISG

Разные услуги QoS	Услуга QoS, применяемая к абонентской сессии – Class Based Policers and Shapers, Marking, Queuing
Пакеты услуг	Ограничение полосы пропускания и учет трафика по направлениям
Турбо кнопка	Полоса по запросу, увеличение полосы пропускания на заданное время
Broadband-Lite	Миграция пользователей Dial-up. Для эмуляции низкоскоростных сервисов
Услуги на основе квотирования трафика	Снижение полосы пропускания абонента после исчерпания им квоты, уведомление абонента с помощью веб-портала
Самостоятельная подписка на услуги	Позволяет новым абонентам самостоятельно зарегистрироваться и подписаться на услуги
Аутентификация на веб-портале	Обязательная аутентификация на веб-портале для неаутентифицированных абонентов
Самостоятельное управление услугами	Позволяет абоненту изменять свои услуги с помощью веб-портала
Самостоятельный выбор VPN	Абонент выбирает к какому VPN подключиться
Open Garden	Ограниченный (гостевой) доступ к ресурсам для неаутентифицированных абонентов
Walled Garden	Доступ к привилегированным ресурсам для аутентифицированных абонентов

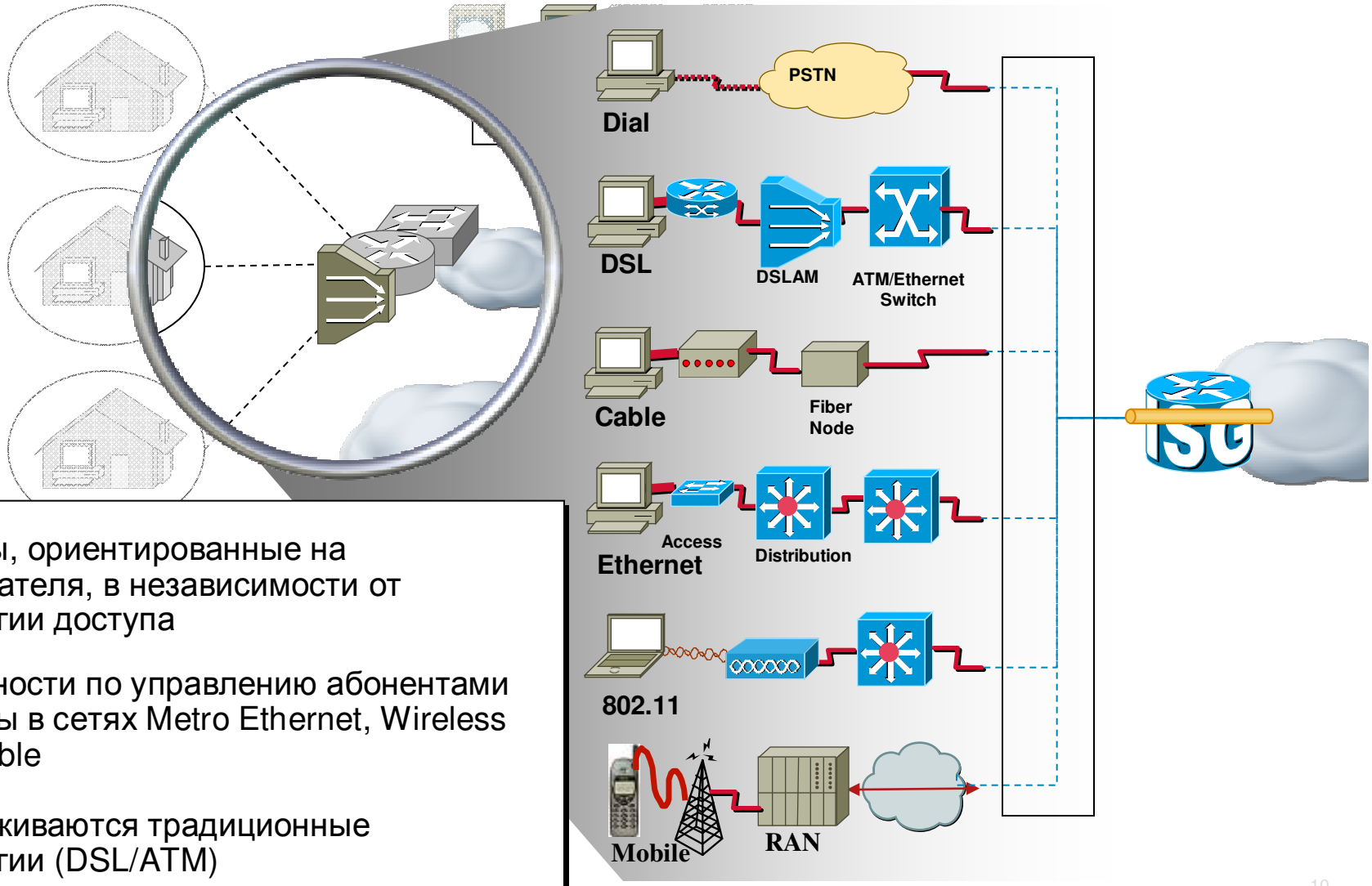
Размещение ISG в сети и задачи ISG



1. На границе сети
2. Взаимодействует с другими устройствами и системами для обеспечения контроля сессии абонента
3. Единая точка взаимодействия

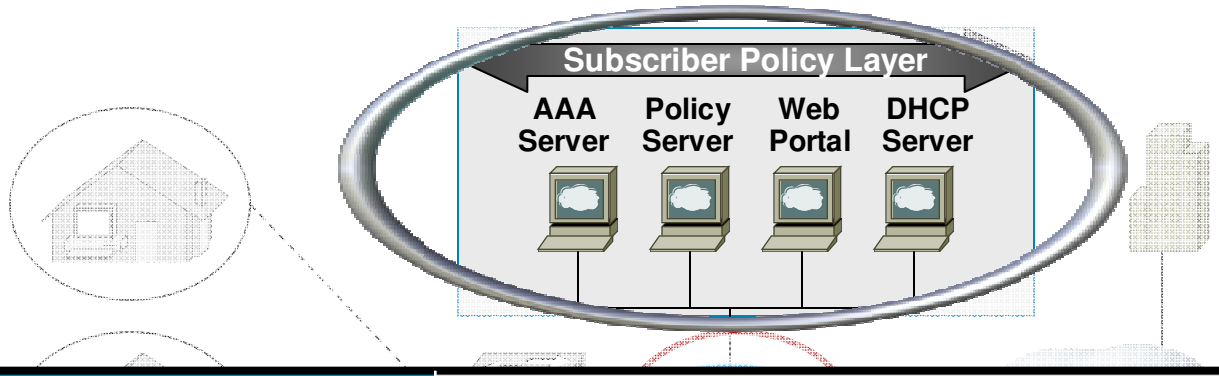
1. Идентификация абонента
2. Аутентификация
3. Назначение сервисов абоненту
4. Динамическое изменение сервисов
5. Учет трафика абонентской сессии и сервисов

Технологии доступа, используемые с ISG



- Сервисы, ориентированные на пользователя, в независимости от технологии доступа
- Возможности по управлению абонентами доступны в сетях Metro Ethernet, Wireless LAN, Cable
- Поддерживаются традиционные технологии (DSL/ATM)

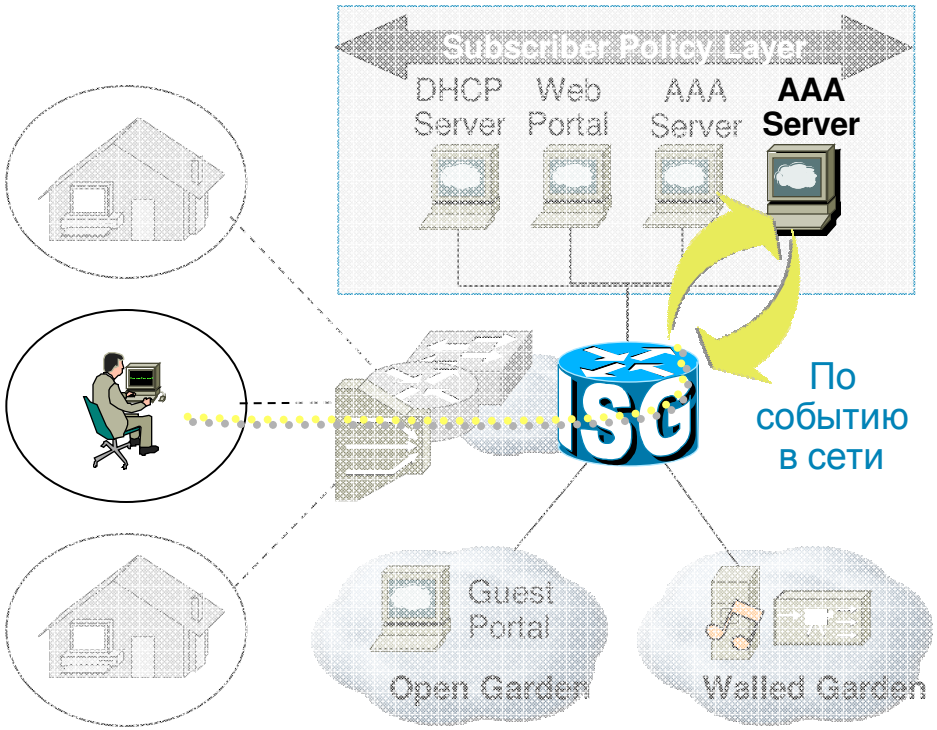
Элементы уровня политик



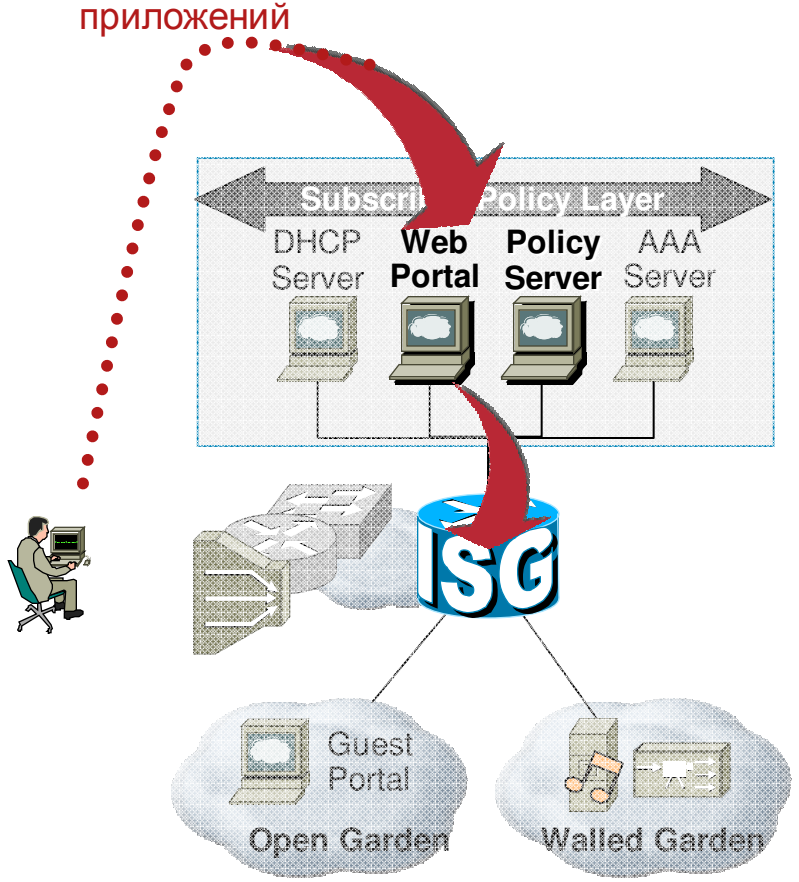
AAA сервер	Аутентификация абонента Авторизация абонента Хранение профилей абонентов и сервисов Сбор Accounting записей Взаимодействие с биллингом
Сервер политик	Динамическое изменение сервисов и политик
Веб-портал	Аутентификация абонента Самостоятельная подписка Изменение сервисов
DHCP сервер	Выдача IP адресов абонентам Выдача IP адресов абонентов по классам

Динамическое применение политик в ISG

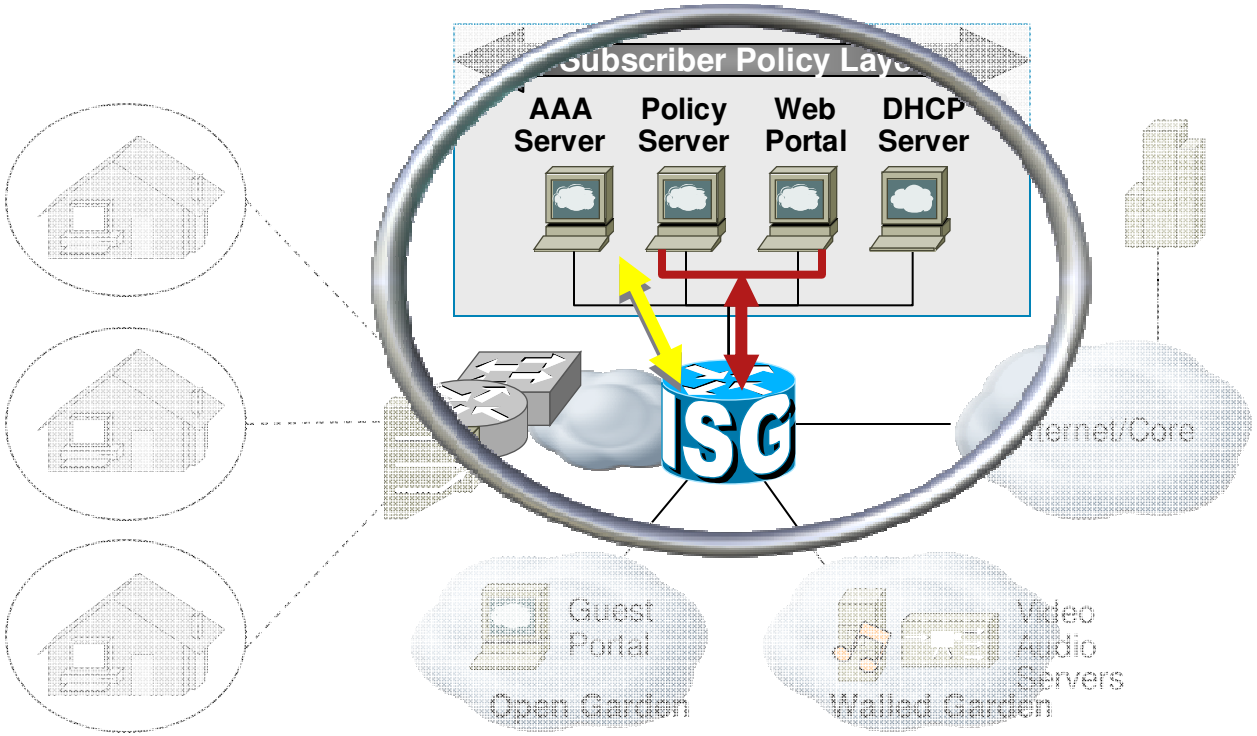
pull
(например, автоматический запрос сервисного профиля при установлении сессии)



push
(например, «турбо кнопка»)



Интерфейс с внешними системами



Протокол RADIUS для аутентификации абонентов и загрузки сервисов

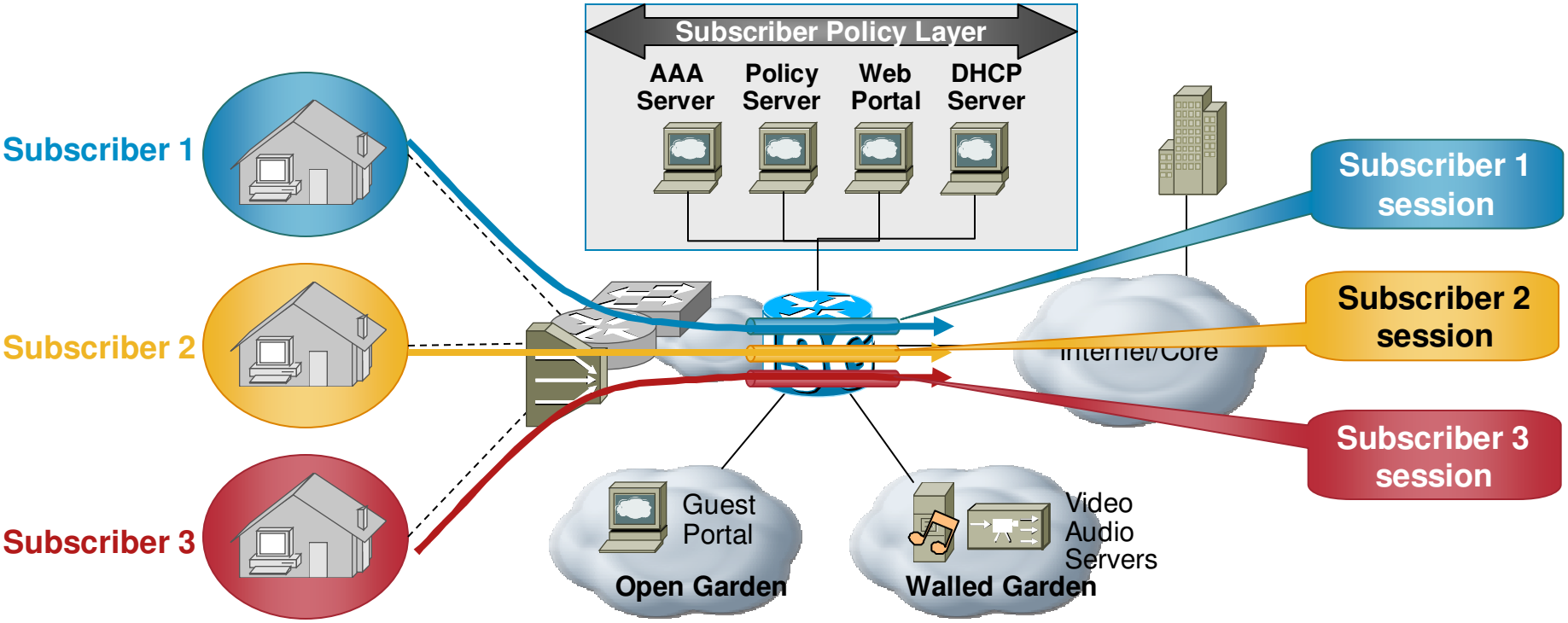
Policy PULL

Расширение протокола RADIUS (Change of Authorization, **RFC 3576**) и основанный на **XML** интерфейс **SGI**(*). **Открытые интерфейсы** для динамического изменения политик, сервисов.

Policy PUSH

(*) SGI: Service Gateway Interface

Абонентские сессии в ISG



1. Создаются в Cisco IOS для представления абонентов
2. Единый контекст, для которого активируются сервисы
3. Создаются в момент первой активности клиента (**FSOL** = First Sign Of Life)

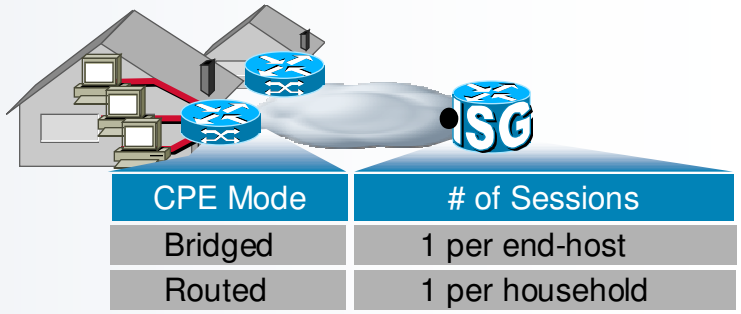
Типы сессий

ISG Session

Динамические сессии:

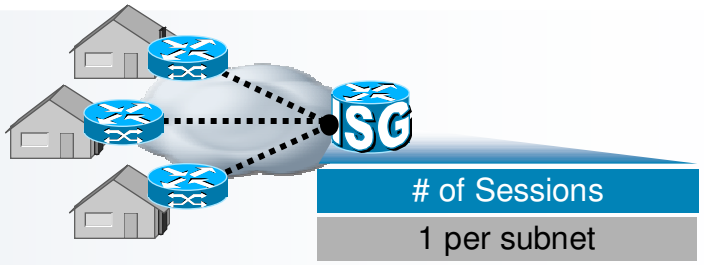
PPP сессии

IP сессии



IP “Subnet” сессии

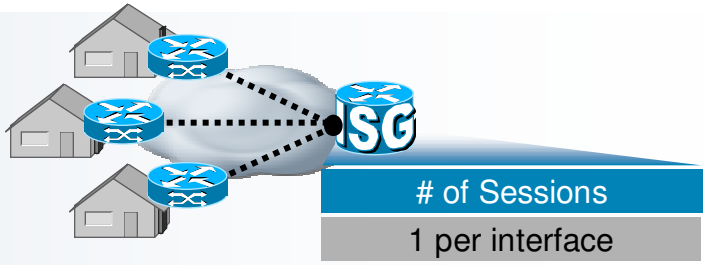
- Привязка сессии к Subnet определяется при аутентификации
- Аутентификация обязательна для таких сессий



Статические сессии:

Интерфейсные сессии –

только IP



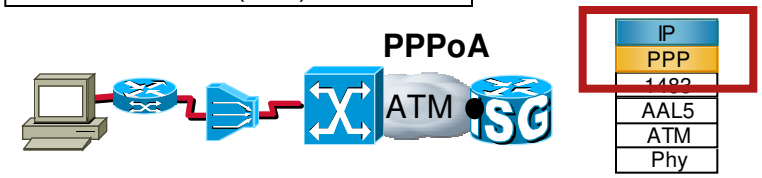
Динамические сессии

ISG Session

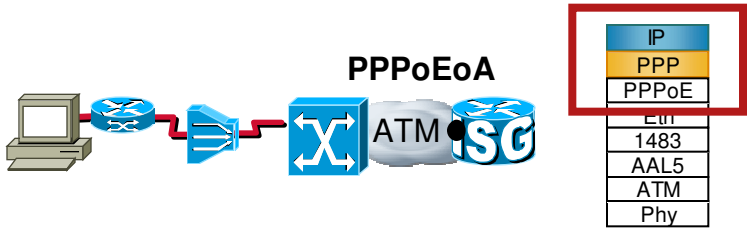
PPP сессии

Virtual Template w/
Virtual Access (sub)Interfaces

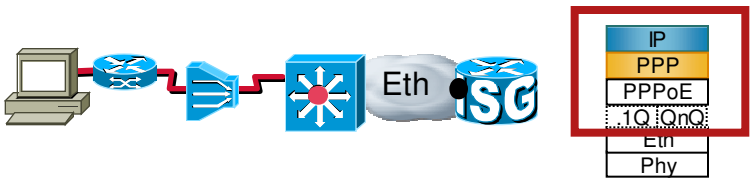
PPPoA



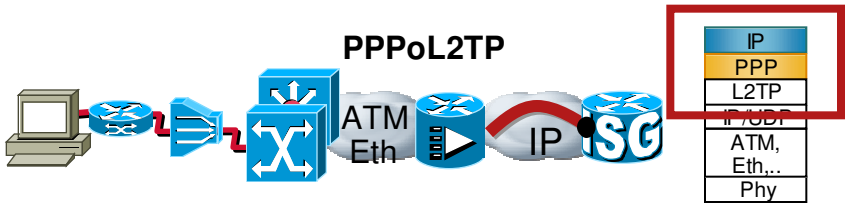
PPPoEoA



PPPoEoE / PPPoEoVLAN/PPPoEoQnQ

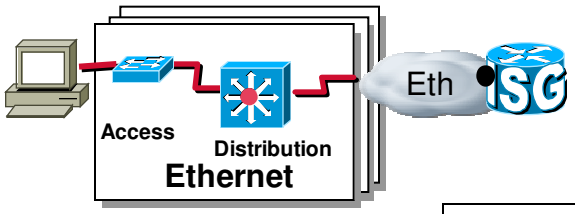


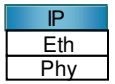
PPPoL2TP



IP сессии

IP–Layer2 Connected

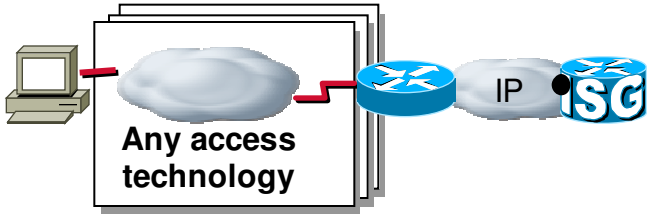


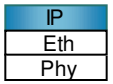


Native IP capable
transport technologies
802.11, 802.16

Main interfaces
Subinterfaces: .1q, QnQ

IP–Routed

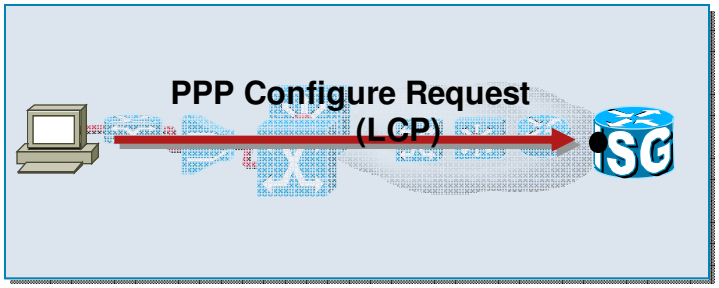




Инициатор для динамических сессий

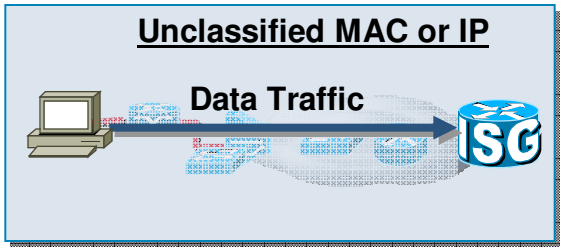
1. ISG сессии возникают по признаку First Sign of Life (FSOL)
2. FSOL зависит от типа сессии

FSOL для PPP сессий

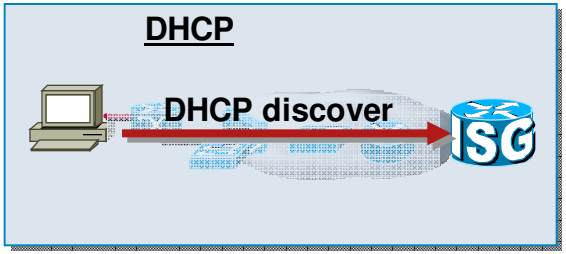


FSOL для IP сессий

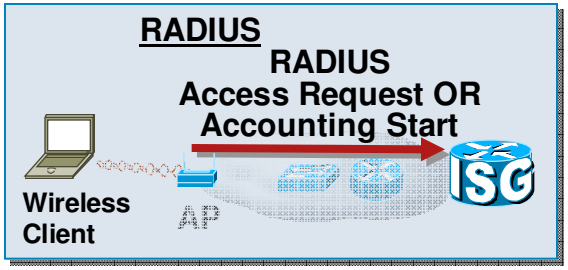
Варианты:



- IP пакет с неизвестным MAC или IP адресом абонента
  - Используйте MAC для L2-connected IP сессий
  - Используйте IP для routed IP сессий



- DHCP Discover message
- ISG должен быть DHCP Relay или DHCP сервером



- RADIUS Access/Accnt Start
- ISG должен быть Radius Proxy
- Обычно используется в PWLAN

Аутентификация сессии

Аутентификация позволяет предоставить доступ к сетевым ресурсам только идентифицированным пользователям

Варианты аутентификации:

1. **Механизмы аутентификации протокола**:
   - PPP: CHAP/PAP
   - IP: EAP для беспроводных клиентов
2. **Transparent Auto Logon (TAL):**
   - Аутентификация на основе сетевых идентификаторов, имеющих отношение к трафику абонента
3. **Web Logon**

Аутентификация не обязательна для сессии, но в большинстве случаев она используется.

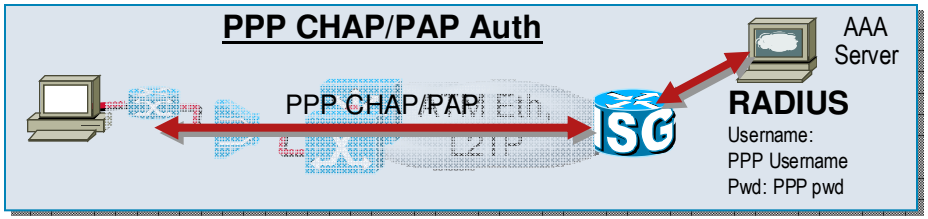
Аутентификация для PPP сессий

ISG Session

PPP – основные сценарии

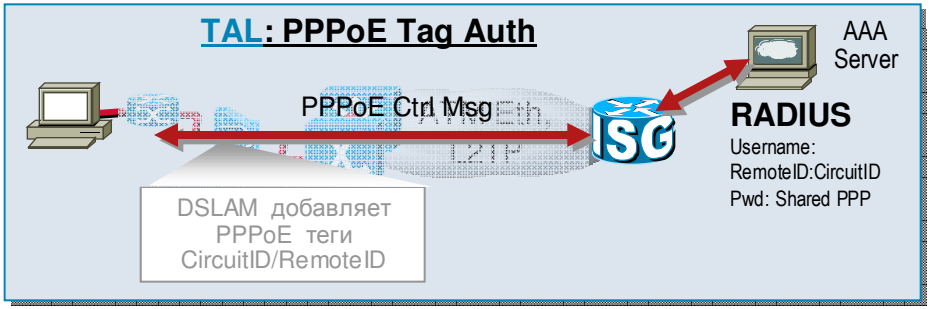
Вероятность использования

PPP CHAP/PAP Auth



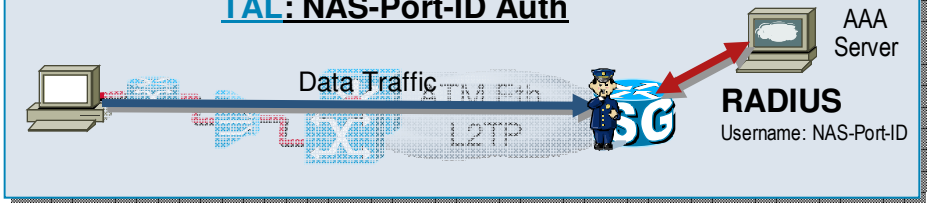
- Использует традиционные протоколы аутентификации PPP
- Применимо для всех типов PPP сессий

TAL: PPPoE Tag Auth



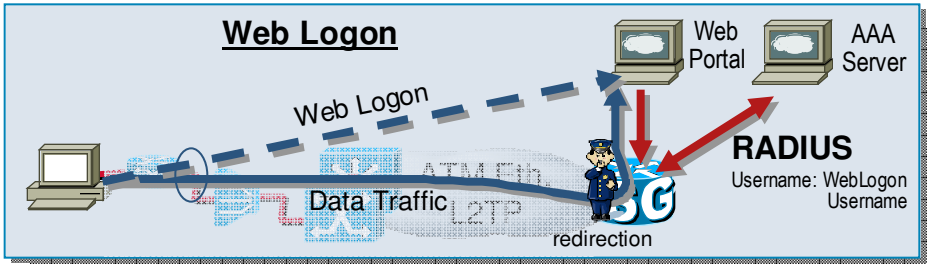
- DSLAM добавляет PPPoE теги, обычно Circuit ID и Remote ID
- ISG выполняет аутентификацию с использованием комбинации Circuit ID и RemoteID в качестве username
- Применимо только для PPPoE сессий

TAL: NAS-Port-ID Auth



- ISG выполняет аутентификацию с использованием NAS-PortID в качестве username
- Обычно используется для PPPoA и PPPoEoQnQ сессий, когда абонент ассоциирован с VC/subif

Web Logon



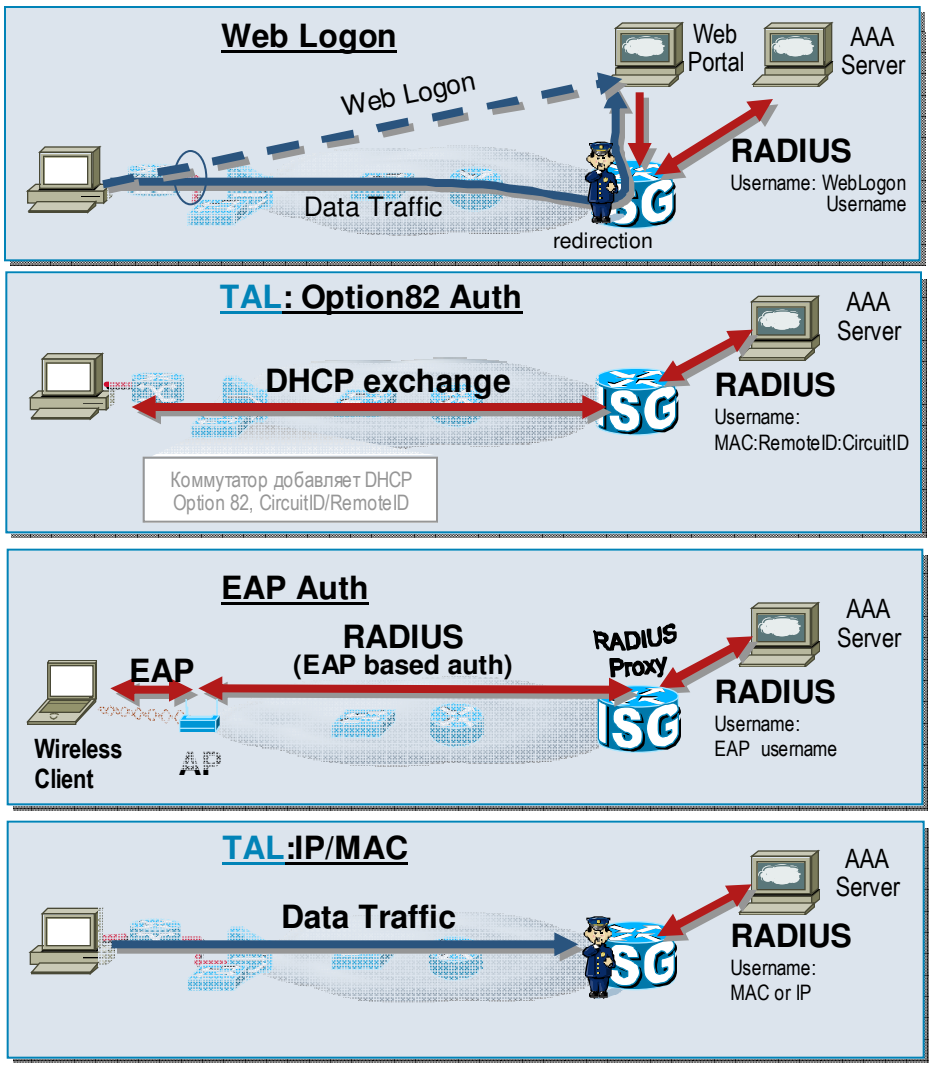
- Трафик пользователя перенаправляется на веб-портал, где он вводит свои данные для аутентификации (username и password)
- Эти данные передаются на ISG
- ISG аутентифицирует пользователя на AAA
- Применимо для всех типов PPP сессий

Аутентификация для IP сессий

ISG Session

IP – основные сценарии

Вероятность использования



- Трафик пользователя перенаправляется на веб-портал, где он вводит свои данные для аутентификации (username и password)
- Эти данные передаются на ISG
- ISG аутентифицирует пользователя на AAA
- Применимо для всех типов IP сессий

- Коммутатор доступа добавляет DHCP Option 82 Circuit и Remote ID в запросы DHCP
- ISG аутентифицирует пользователя по комбинации Circuit и RemoteID в качестве username
- ISG сессия должна быть с DHCP инициатором

- Пользователь начинает EAP аутентификацию
- ISG играет роль RADIUS сервера для AP и RADIUS клиента для настоящего сервера
- ISG выполняет аутентификацию сессии, проксируя RADIUS запросы от настоящего RADIUS клиента к серверу
- ISG сессия должна быть с инициатором RADIUS

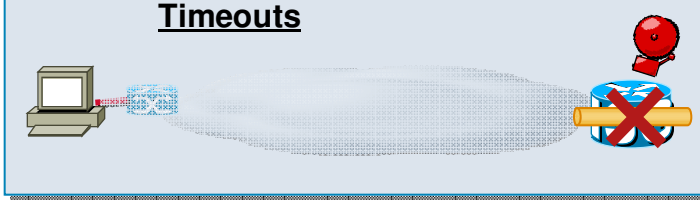
- ISG выполняет аутентификацию с использованием идентификаторов абонентского трафика: IP или MAC адрес абонента
- Обычно используется в IP-L2 connected топологиях для поддержки клиентов со статическим IP адресом или в IP-routed топологиях

Терминация сессий

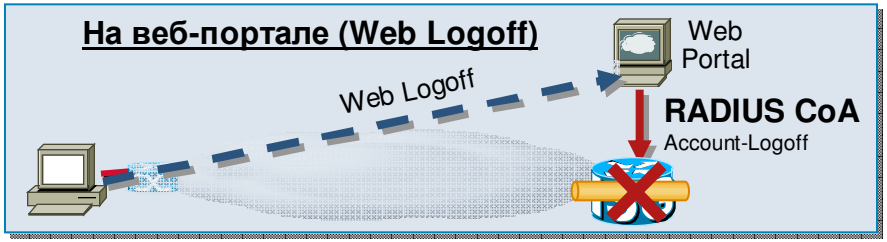
ISG Session

Для IP и PPP сессий

По истечению таймеров Idle или Absolute Timeouts



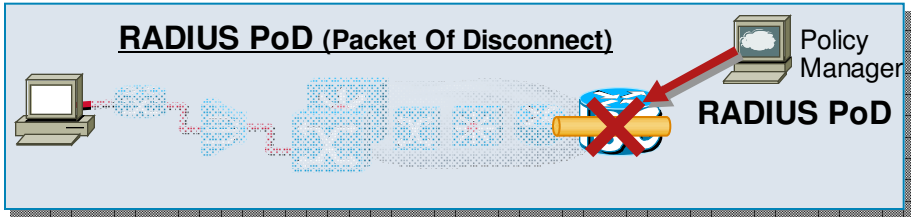
На веб-портале (Web Logoff)



Для PPP сессий

События в протоколе PPP и PPPoX

RADIUS PoD (Packet Of Disconnect)

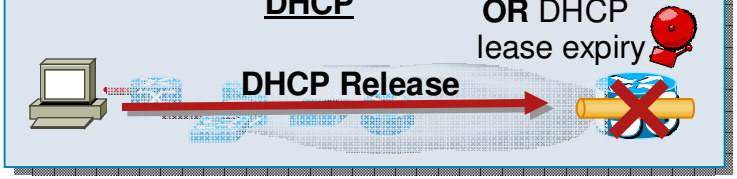


Для IP сессий

ICMP/ARP keepalive

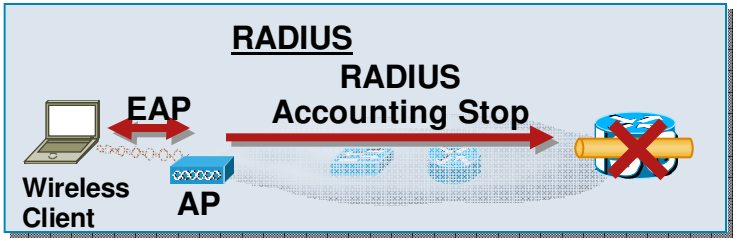
ICMP Keepalives для L3-connected сессий
ARP Keepalives для L2-connected сессий

DHCP



Инициатор DHCP

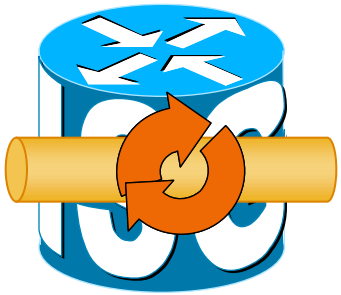
RADIUS



Инициатор RADIUS

ISG сервисы

Сервис – это набор функциональных возможностей (features), которые применяются к абонентской сессии



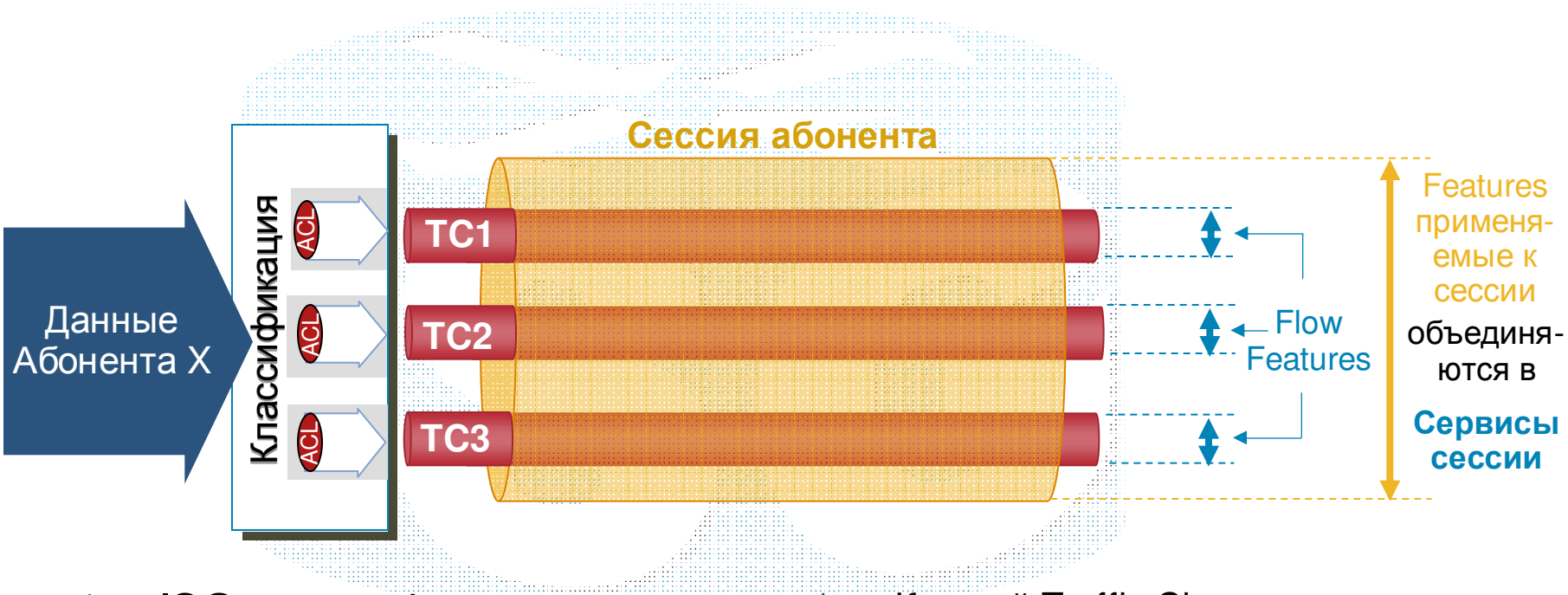
Возможности (features)		
	Управление сессией	Portbundle (PBHK) Keepalives: ICMP и ARP Таймеры: Idle, Absolute
	Профилиро-вание трафика	QoS: Policing, MQC Безопасность: Per User ACLs
	Управление прохождением трафика	Назначение адресов абоненту Перенаправление: первоначальное, постоянное, периодическое Назначение VRF: первоначальное, переключение L2TP
	Учет трафика	PostPaid, промежуточный Prepaid: по времени, по объему

Применим к **Primary Services**

Primary Service: содержит одну возможность управления прохождением трафика и опционально другие возможности. Только один primary service может быть активным у сессии.

Понятие Traffic Class

ISG services

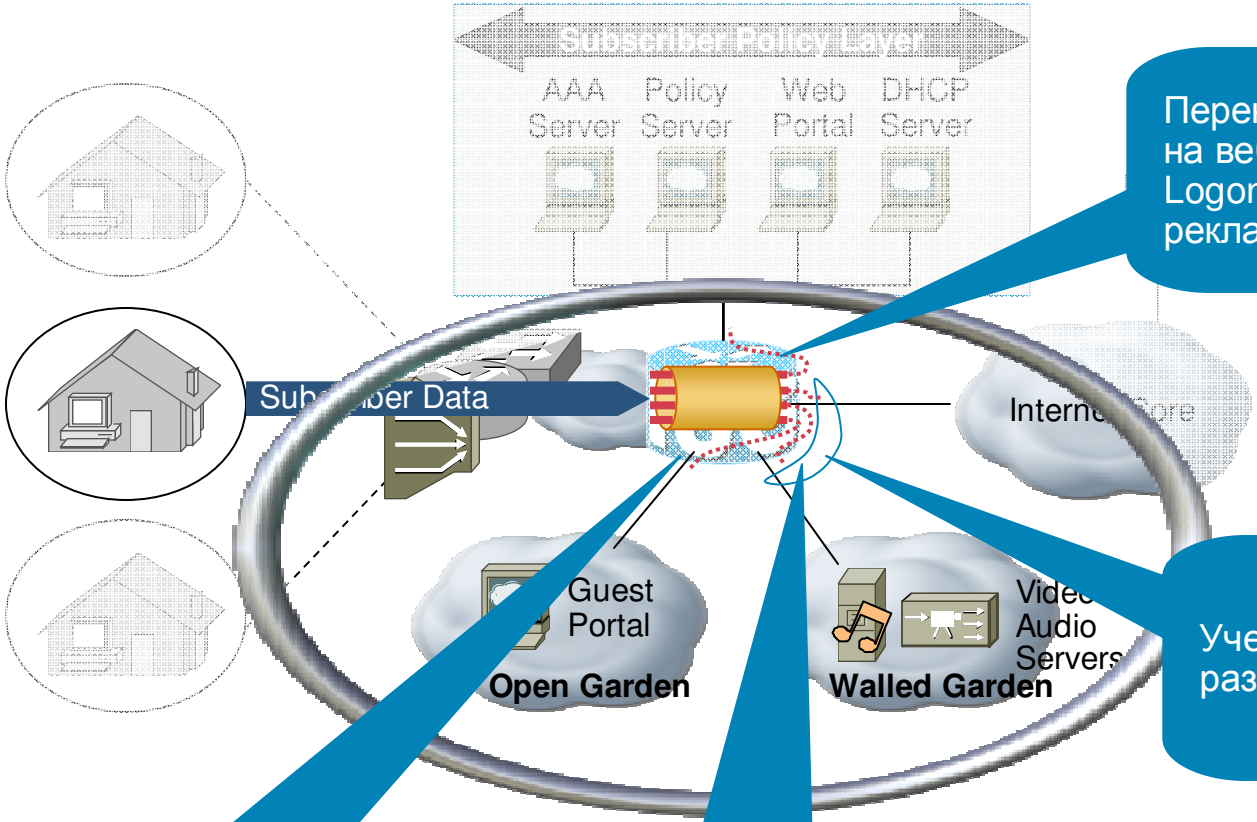


1. ISG классификация похожа на Modular QoS CLI (MQC)
2. Классификация выполняется с помощью списков доступа IP ACL (standard или extended)

1. Каждый Traffic Class может иметь разный набор features
2. Traffic Class и его features называют также TC service
3. Default TC используют для работы с трафиком, который не был классифицирован. К нему обычно применяют drop.

Примеры использования TC Services

ISG services



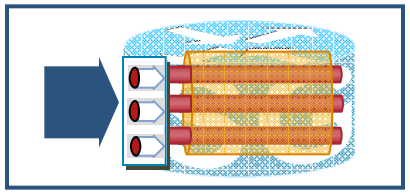
Перенаправить трафик на веб-портал (Web Logon, периодическая реклама)

Учет трафика по разным направлениям

Разрешить трафик к открытым ресурсам (Open Garden) для неаутенти-фицированной сессии, при этом весь остальной трафик дропается.

Предложить разную полосу пропускания для разных потоков данных

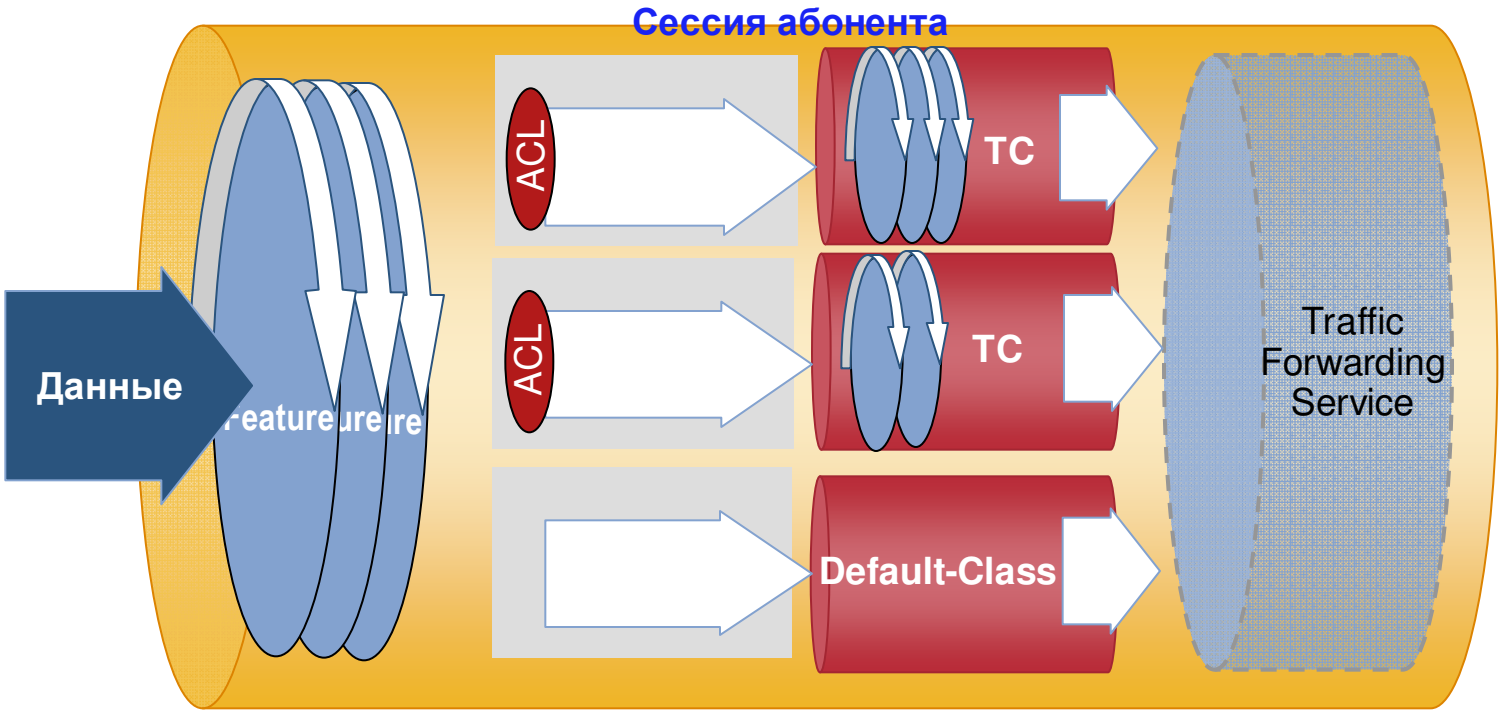
Применение Features к сессии или к TC



ISG services

		Сессия	Traffic Class (TC)
Управление сессией	Portbundle (PBHK)	X	
	Absolute/Idle таймеры	X	X
	ICMP и ARP keepalives	X	
Профилирование трафика	Policing	X	X
	MQC	X	
	Per User ACLs	X	
Управление прохождением трафика	Перенаправление	X	X
	Назначение VRF	X	
	L2TP	X	
Учет трафика	Postpaid Accounting	X	X
	Prepaid Accounting		X

Прохождение трафика через ISG



Session-Features: Применяется ко всей сессии. Например, per-user-ACL, MQC, Accounting

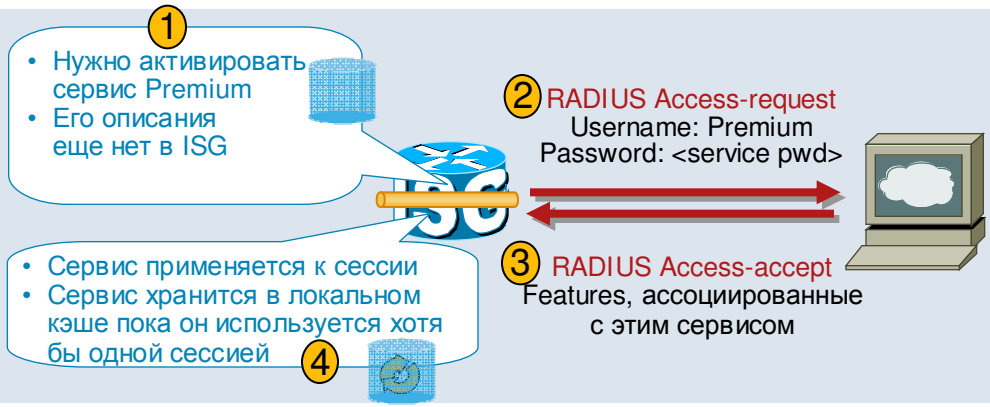
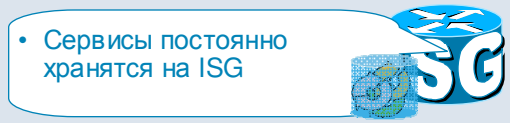
Классификация трафика (с использвоанием Traffic Classes: class-map type traffic)

Flow-Features: Применяется к Traffic Class (часть данных сессии)

Forwarding Service: L2 (L2TP) или маршрутизация (L3, VRF) Взаимно-исключаемые

Определение сервисов

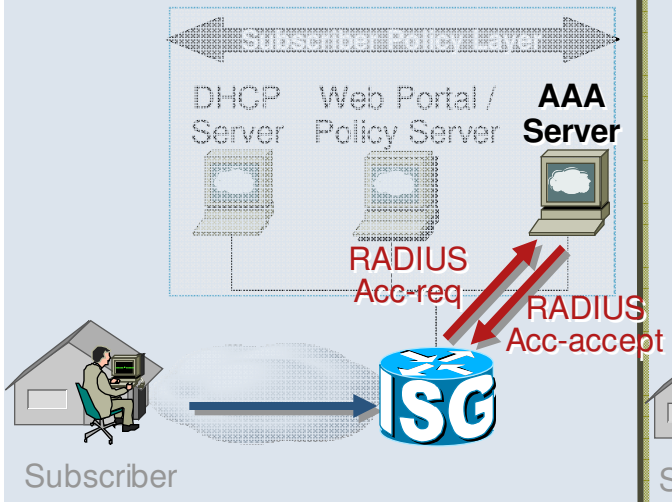
ISG services

Место	Процесс
AAA сервер • Сервисы определяются в **Service Profiles** • Стандартные и Vendor Specific RADIUS attributes • Скачивание сервисов по необходимости	
Сервер политик **(с поддержкой SGI интерфейса)** • Сервисы определены в XML • Предварительное скачивание всех сервисов	
ISG • Сервисы заранее определены на ISG с помощью CLI • Сервисы определяются в разделе **Service Policies:** policy-map type service <name>	

Как активируются сервисы ?

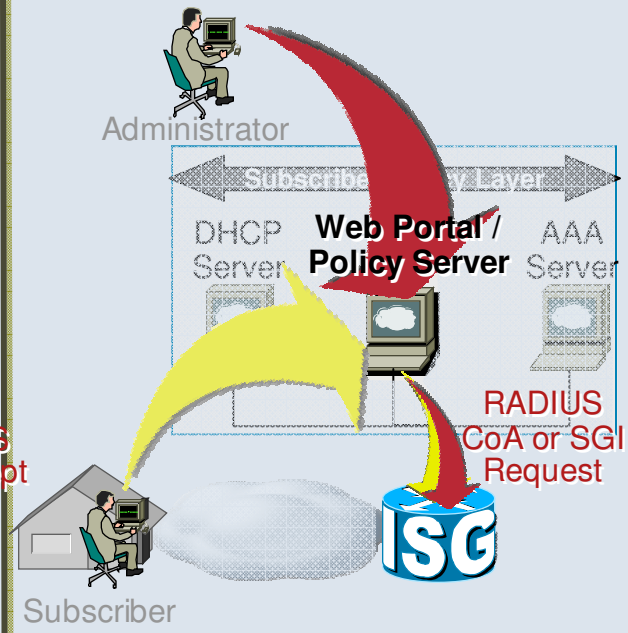
ISG services

Во время аутентификации/ авторизации абонента



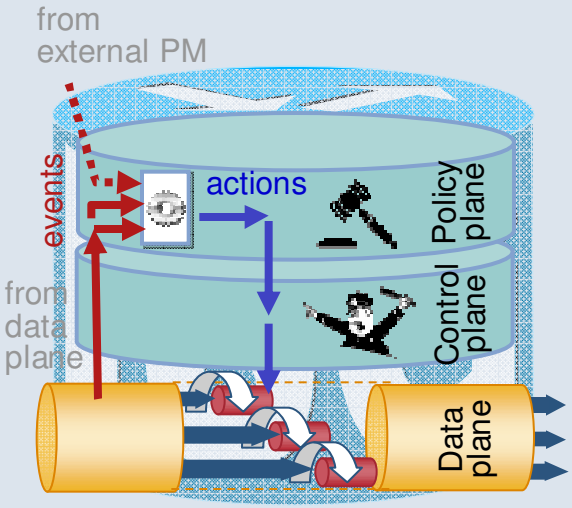
- Абонент успешно аутентифицирован
- RADIUS Response включает сервисы и Features, которые необходимо применить к сессии (информация из User Profile)

С помощью сервера политик, веб-портала



- Запрос на активацию сервисов отправляется сервером политик с помощью запросов RADIUS CoA или SGI

С помощью встроенного в ISG менеджера политик



- **Policy Plane** определяет какие **действия** применить к сессии на основе **событий**

  действия включают в себя применение сервисов

- **Control Plane** обеспечивает исполнение этих действий
- **Data Plane** обеспечивает профилирование трафика сессии

Встроенный в ISG менеджер политик (PM)

Управляет всеми процессами «жизни» сессии абонента,
не только активацией сервисов

«Жизнь» сессии

описывается с помощью

Cisco
Policy
Language

Благодаря CPL и встроенному менеджеру политик
ISG является не только Policy Enforcement Point (PEP),
но и Policy Decision Point (PDP)

Cisco Policy Language CLI

Управляющая policy-map	Условный класс событий	Действия
policy-map type control *<name>*	event 1 class type control *<conditions>* event *<event type>* event 2 другие события	action1 action2 другие действия .....

Обычно применяется к интерфейсу

Определяет все аспекты обслуживания сессии

События определяются их типом

Пример основных типов событий:

- Session-start
- Account-logon
- Service-start
- Service-stop
- Timed-policy-expiry

Действия в событии выполняются только при наличии условий (<conditions>)

- Разные варианты события для разных условий
- Разный набор действий для одного и того же типа события
- Условия учитывают аспекты, сопровождающие события

Действия в упорядоченной последовательности

Разные наборы действий для пары {событие, условие}

Примеры основных действий:

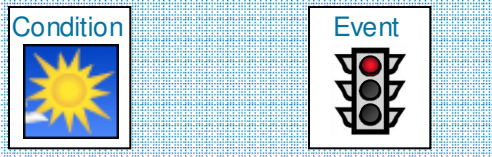
- Service
- Service Unapply
- Authenticate
- Authorize (TAL)
- Set-Timer

Определение Control Policy
policy-map type control

Control Policy
Связывает события и условия
с упорядоченным списком действий

Condition	Event	Condition	Event	Condition	Event
Control Class: *List of Actions*		Control Class: *List of Actions*		Control Class: *List of Actions*	
1. Disable Service B 2. Enable Service A		1. Enable Service X 2. Enable Service Y 3. Take Action R		1. Enable Service PBHK 2. Take action AAA 3. Enable Service L4R 4. Take action: Set Timer	

Пример

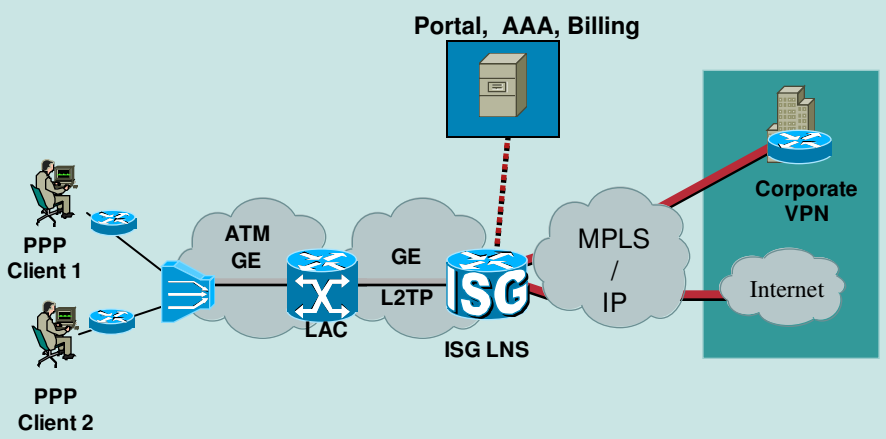



```
policy-map type control SUBSCRIBER_RULE
 class type control always event session-start
  10 service-policy type service name PBHK
  20 authorize aaa password lab identifier mac-addr
  30 service-policy type service name L4R
  40 set-timer TIME1 5
 !
 class type control always event account-logon
  10 authenticate aaa list IP_AUTH_LIST
  20 service-policy type service unapply name L4R
 !
 class type control TIME1_Exp event timed-policy-expiry
  10 service disconnect
 !
```

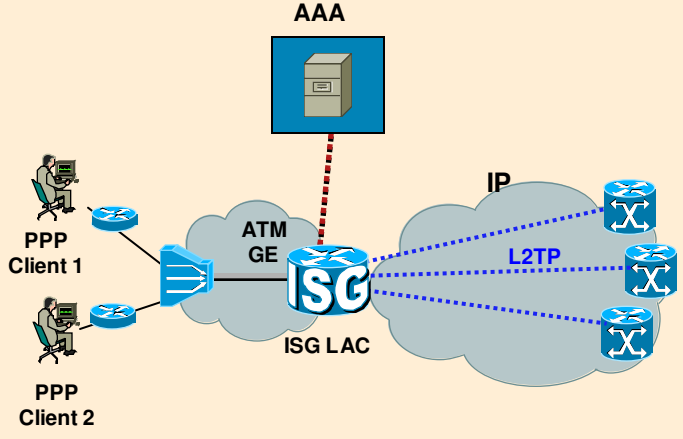
Модели внедрения ISG на сети

Агрегация PPP сессий абонентов

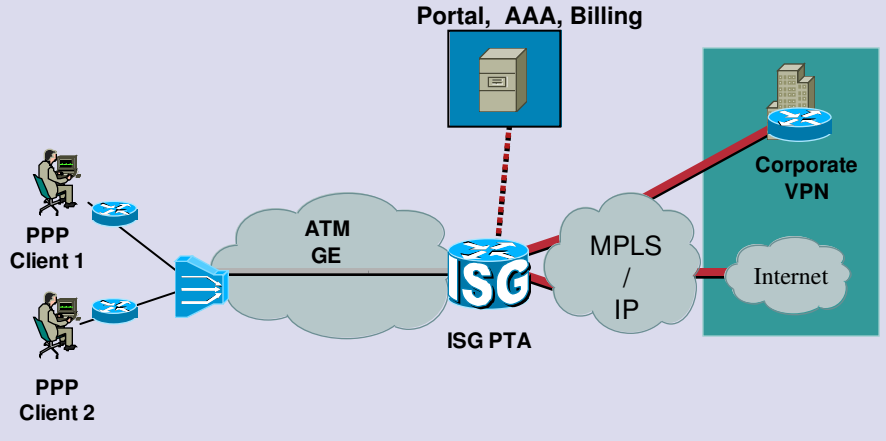
DSL Wholesale – ISG для LNS



DSL Wholesale – ISG для LAC



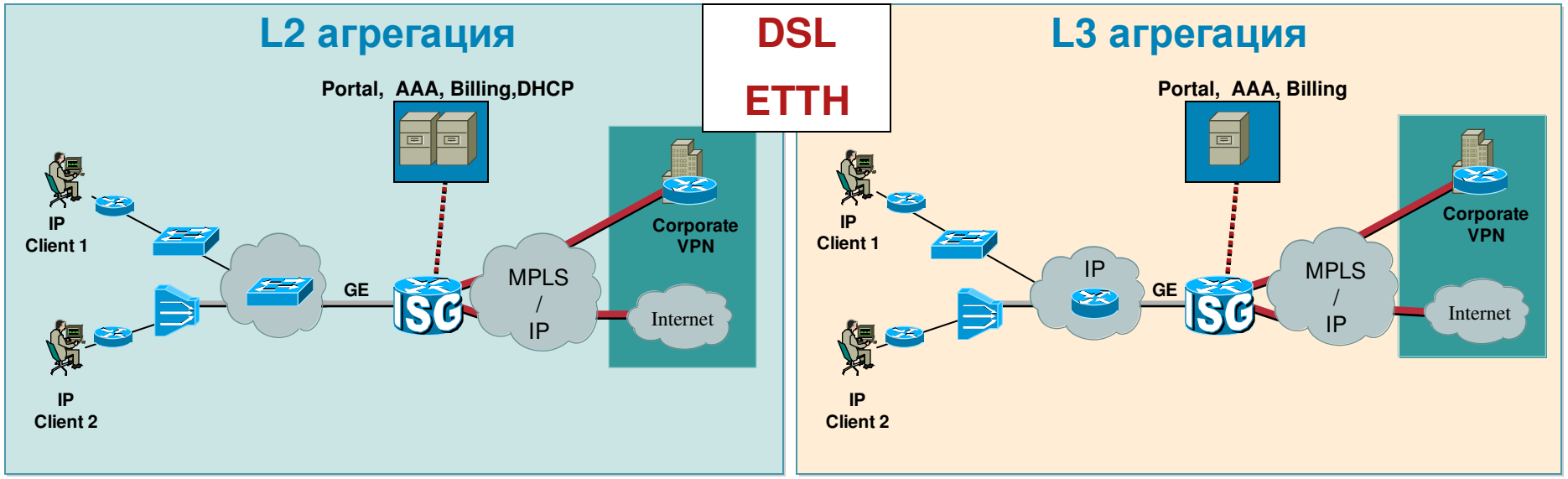
DSL – ISG для PTA



DSL

	Тип сессий	Назначение адреса	Интер-фейс	Аутенти-фикация
LNS	PPPoL2TP	ISP's Radius/ DHCP Servers	GE	PPP CHAP
LAC	PPPoA/ PPPoE	Выполняется ISP	ATM GE (QinQ)	PPP (CHAP) TAL (NAS_Port_ID) None
			GE (.1Q)	PPP (CHAP) TAL (PPPoE Tag) None
PTA	PPPoA/ PPPoE	Локально RADIUS /DHCP	ATM GE (QinQ)	PPP (CHAP) TAL (NAS_Port_ID)
			GE (.1Q)	PPP (CHAP) TAL (PPPoE tag)

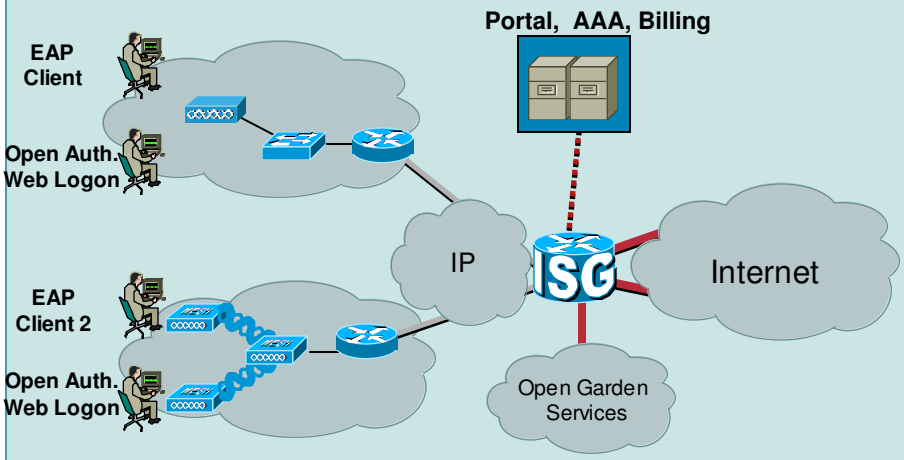
Агрегация IP сессий абонентов



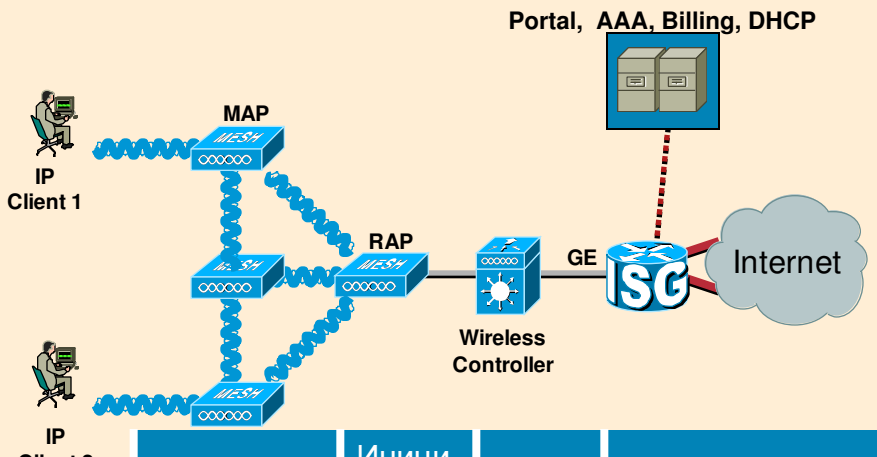
	Назначение адресов	Инициатор сессий	Интерфейс	Аутентификация
L2–IP агрегация	ISG является DHCP Relay или DHCP сервер	DHCP	GE (.1Q)	L4R на портал TAL (Option-82)
			GE (QinQ)	L4R на портал TAL (Nas_Port_ID)
	ISG не обрабатывает DHCP сообщения	MAC	GE (.1Q)	L4R на портал TAL (MAC Address)
			GE (QinQ)	L4R на портал TAL (Nas_Port_ID)
L3–IP агрегация	ISG является DHCP сервером	DHCP	GE	L4R на портал TAL (Option-82)
	ISG не обрабатывает DHCP сообщения	IP	GE	L4R на портал TAL (IP Address)

Публичный беспроводной доступ IP сессии

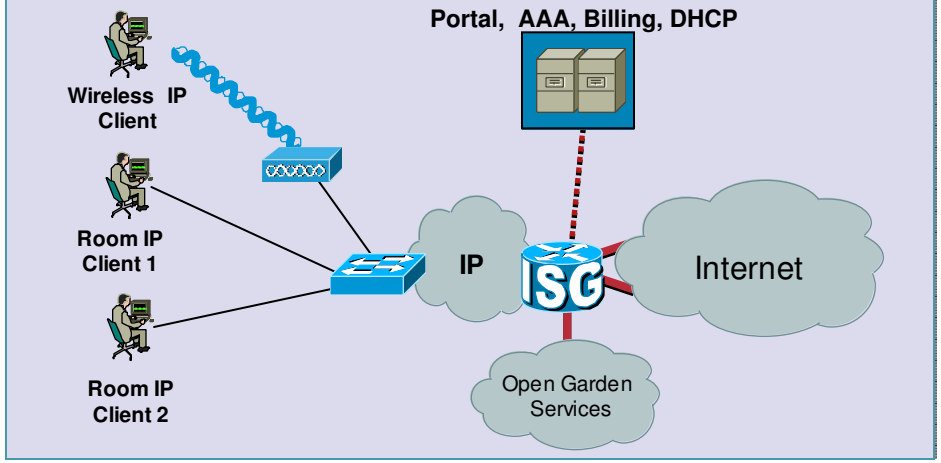
ISG для PWLAN



ISG для доступа Wireless Mesh



ISG для гостиничного бизнеса

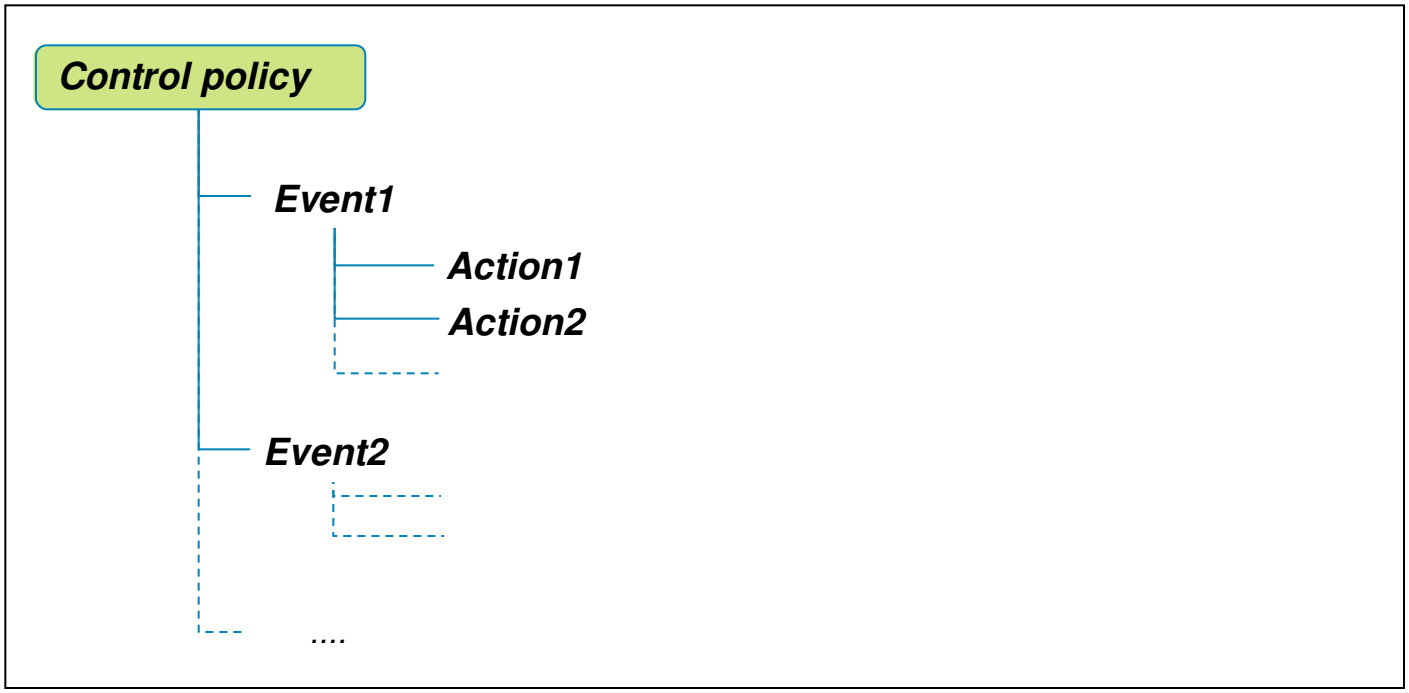


	Назначение адресов	Инициатор сессий	Интерфейс	Аутентификация
PWLAN	AZR (ISG не обрабатывает DHCP сообщения)	RADIUS	L3	L4R на портал RADIUS (EAP clients)
Wireless Mesh	ISG является DHCP сервером	DHCP	.1Q or L3	L4R на портал
		RADIUS		RADIUS (EAP clients)
	ISG не обрабатывает DHCP сообщения	MAC	.1Q	TAL (MAC Address) далее L4R
		MAC		TAL (MAC)
		RADIUS	L3	L4R на портал
		RADIUS		RADIUS (EAP clients)
Гостиницы	ISG является DHCP Relay или сервер	DHCP	L2	TAL (Option82)
		DHCP		L4R на портал

Примеры конфигурации ISG

Основной принцип конфигурирования ISG

1. Конфигурирование ISG главным образом предполагает создание политики управления (control policy)
2. Control policy определяет действия, которые нужно выполнить над сессией при возникновении различных событий



Events:

- Session-start
- Account-logon
- Service-start
- ....

Actions:

- apply/unapply a service
- authenticate (Web Logon)
- authorize (TAL)
- ....

Структура конфигурации ISG

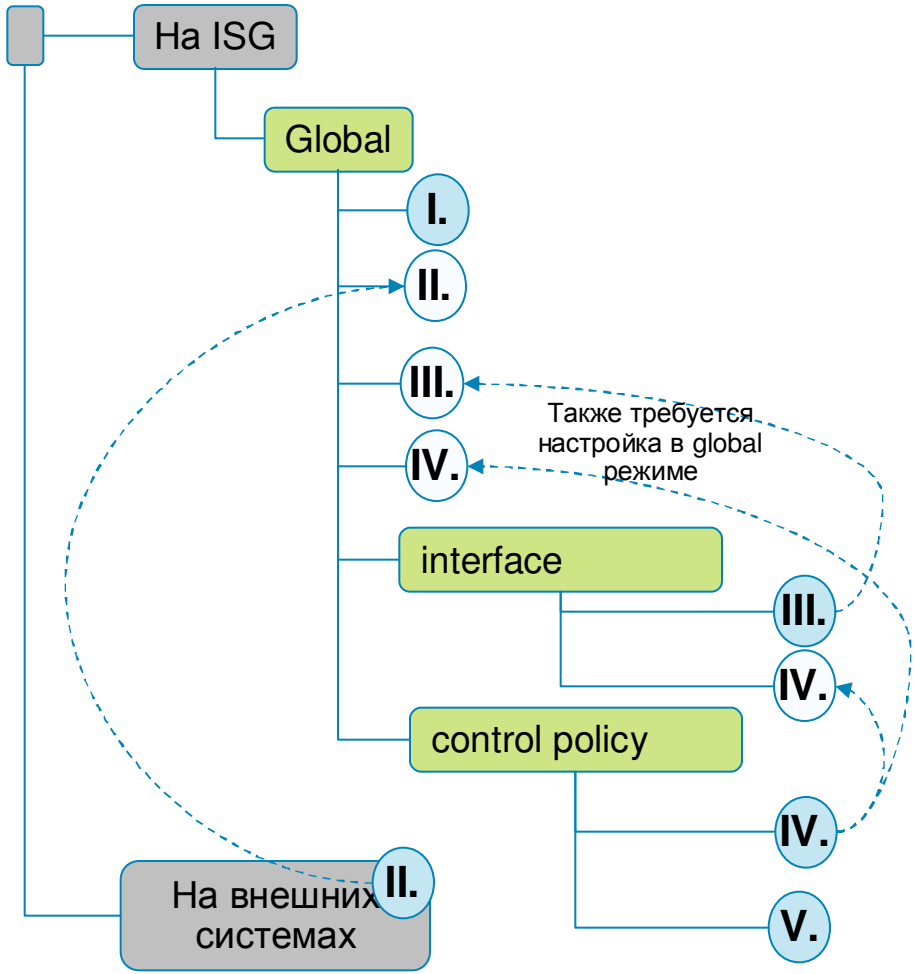
I. Интерфейс взаимодействия
- AAA
- Portal/Policy Server
  - CoA
  - SGI

II. Сервисы и профили пользователей
- Сервисы сессии
- Traffic Class сервисы
- User Profiles

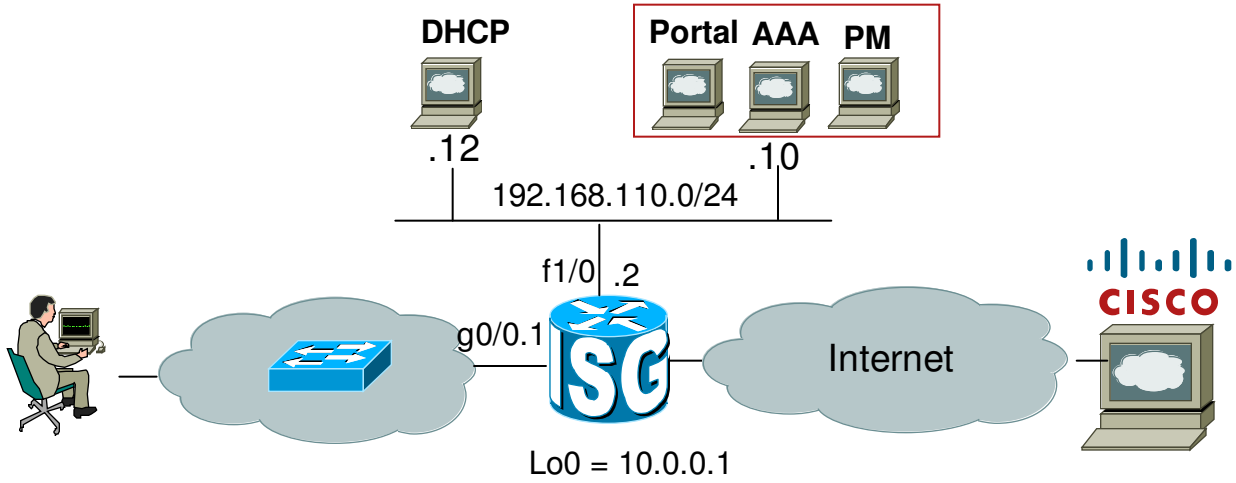
III. Тип доступа абонентов
- Тип сессий и инициатор
- Создание и применение control policy

IV. Аутентификация абонентов

V. Динамическое управление абонентскими сессиями



Пример конфигурации ISG
ISG для агрегации IP сессий (L2)

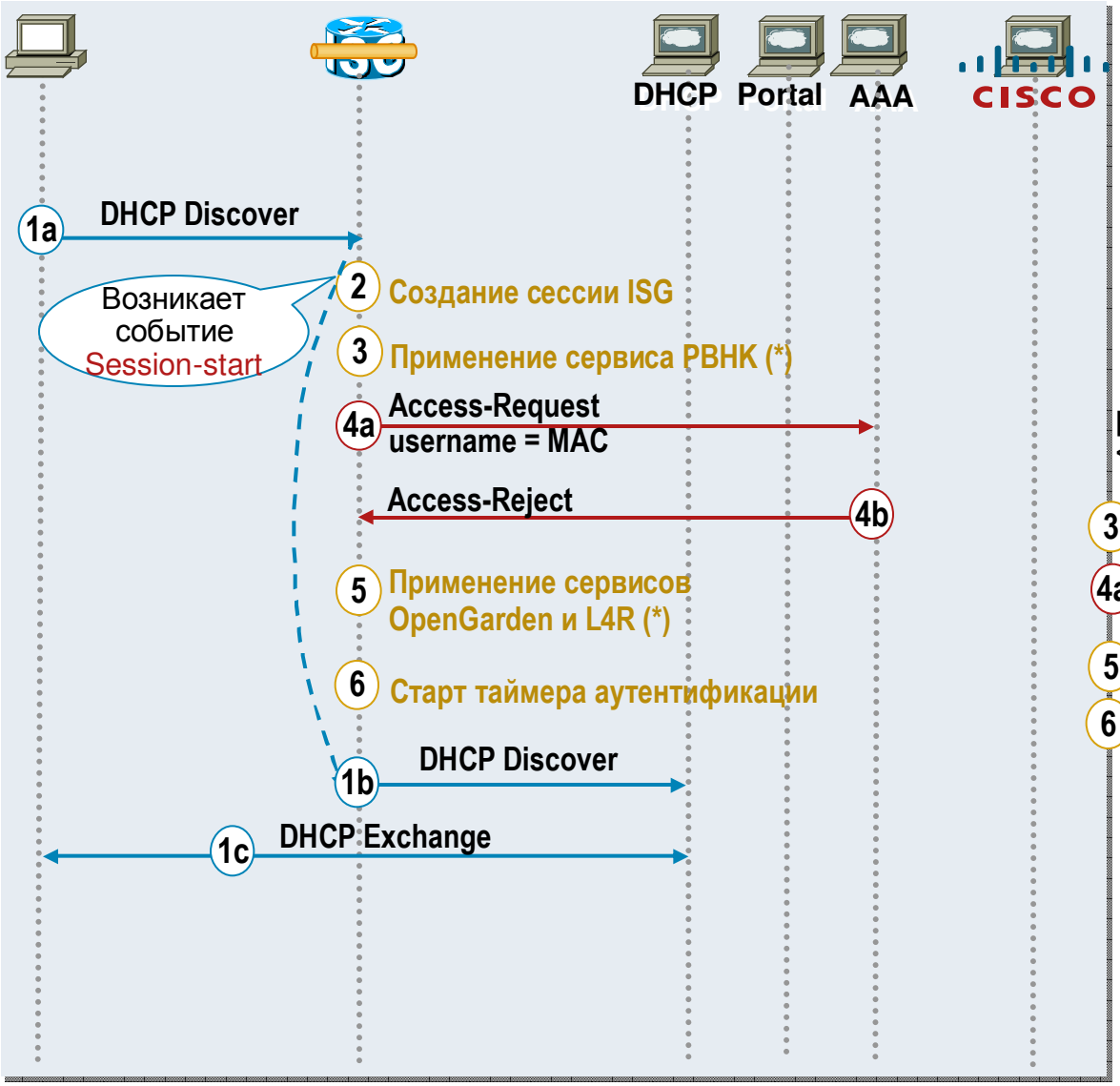


Назначение адресов	Инициатор сессии	Интерфейс	Аутентификация
DHCP ISG - DHCP Relay	DHCP	GE (.1Q)	TAL (MAC address) с использованием Web Logon для самостоятельной подписки

1. После аутентификации абонента ему будет присвоен сервис Pay Per Use Standard High Speed:

   - 256Kbps upstream/ 768Kbps downstream с использованием ISG policing
   - учет трафика
   - idle timeout (10 мин)

Call Flows

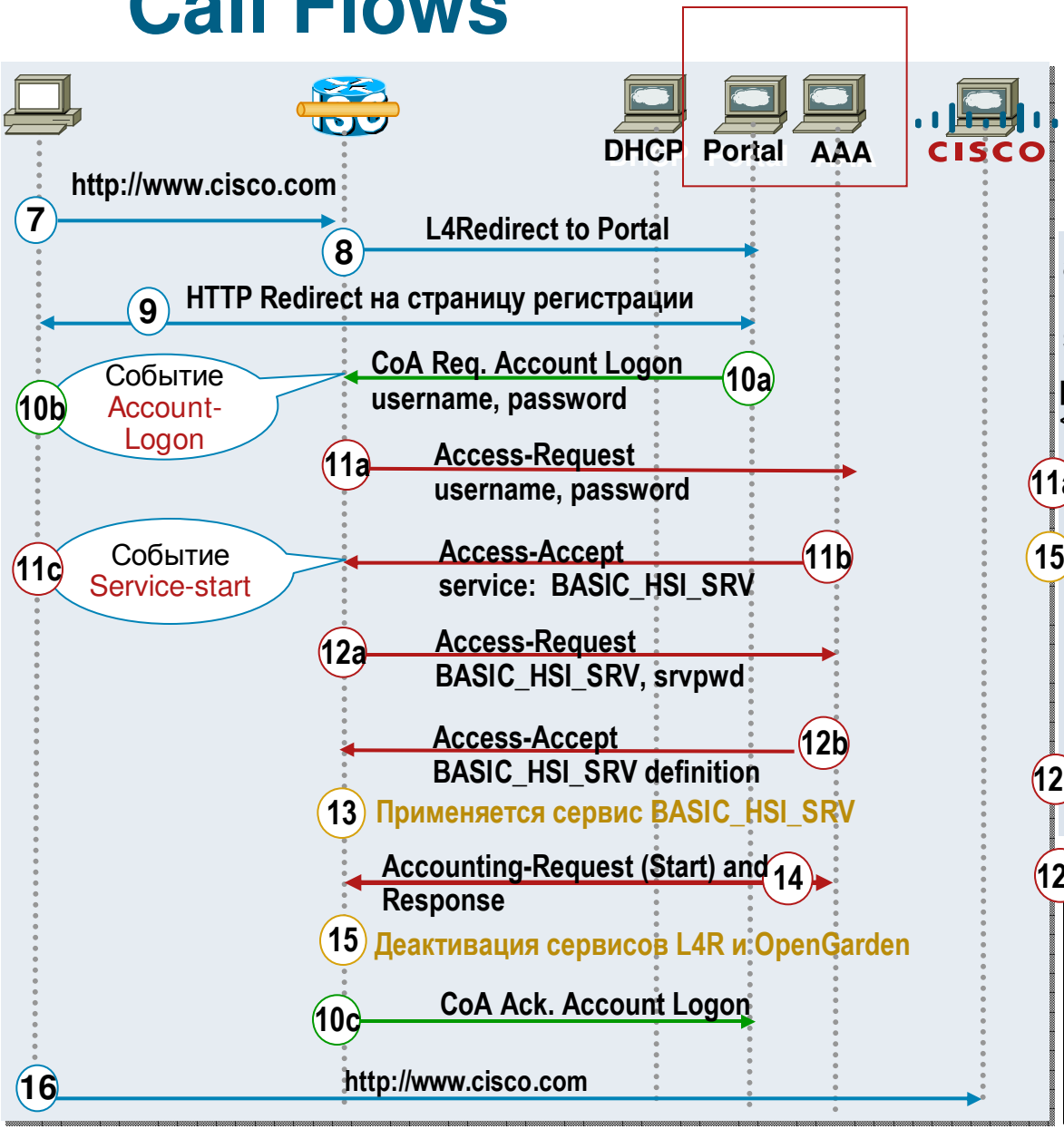



```
interface GigabitEthernet 0/0.1
  encapsulation dot1Q 10
  ip address ...
  service-policy type control IP_SESSION_RULE1
  ip subscriber l2-connected                    (2)
       initiator DHCP
```

```
policy-map type control IP_SESSION_RULE1
<snip>
class type control always event session-start   (2)
(3) 10 service-policy type service name PBHK_SRV
(4a) 20 authorize aaa list IP_AUTHOR_LIST
            password cisco123 identifier mac-addr
(5) 30 service-policy type service name OG_SRV
(6) 40 service-policy type service name L4R_SRV
    50 set-timer AUTHEN_TMR 10
```

(*) подразумевается, что сервисы PBHK, L4R и OpenGarden уже имеются в ISG

Call Flows



Simplified call flow

```
aaa author subscriber-service default
                                SERVER_GRP1
subscriber service password servicecisco
policy-map type control IP_SESSION_RULE1
<snip>
  class type control always event account-logon
    10 authenticate aaa list IP_AUTHEN_LIST
    20 service-policy type service unapply
                                name L4R_SRV
    30 service-policy type service unapply
                                name OG_SRV
  !
  class type control BASIC_HSI_SRV_CM event
                                service-start
    10 service-policy type service identifier service-
                                name
```

10b 11a 15 11c 12a

12b

Service-Name: “**BASIC_HSI_SRV**”
Service-Password: “servicecisco”
Attr 28: idle-timeout = 600
AVPair: “subscriber:accounting-list=
IP_ACCNT_LIST”
ServiceInfo: QU;256000;D;768000;

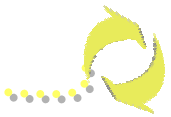
Конфигурация ISG

Интерфейс взаимодействия с внешними системами

Конфигурация RADIUS

```
aaa new-model
aaa group server radius SERVER_GRP1
   server 192.168.110.10 auth-port 1812 acct-port 1813
!
aaa authorization network default group SERVER_GRP1
aaa authorization subscriber-service default group SERVER_GRP1
subscriber service password servicecisco
!
interface Loopback0
   ip address 10.0.0.1 255.255.255.255
!
ip radius source-interface Loopback0
radius-server attribute 4 10.0.0.1
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 access-request include
radius-server attribute 55 include-in-acct-req
radius-server attribute 44 include-in-access-req
radius-server host 192.168.110.10 auth-port 1812 acct-port 1813 key aaacisco
radius-server vsa send authentication
radius-server vsa send accounting
```

I.



Attribute 6 - Service-Type
Attribute 8 - Framed-IP-Address
Attribute 32 - NAS-Identifier
Attribute 44 - Acct-Session-Id
Attribute 55 - Event-Timestamp

Конфигурация RADIUS Extensions (CoA)

```
aaa server radius dynamic-author
 client 192.168.110.10
 server-key cisco
 auth-type any
 port (1700)
```

Конфигурация ISG

Сервисы

Конфигурация AAA сервера

Service-Name = “**OG_SRV**”
Service Password = “servicecisco”
AVPair: ip:traffic-class=input access-group
name **OG_ACL_IN** priority 10
AVPair: ip:traffic-class=output access-group
name **OG_ACL_OUT** priority 10
AVPair: ip:traffic-class=in default drop
AVPair: ip:traffic-class=out default drop

Service-Name = “**L4R_SRV**”
Service Password = “servicecisco”
AVPair: ip:traffic-class=input access-group
name **L4R_ACL_IN** priority 20
AVPair: ip:l4redirect=redirect to group **REDIR_GRP**

Service-Name = “**PBHK_SRV**”
Service Password = “servicecisco”
AVPair: ip:portbundle=enable

Service-Name: “**BASIC_HSI_SRV**”
Service-Password: “servicecisco”
Attr 28: idle-timeout = 600
AVPair: “subscriber:accounting-list= **IP_ACCNT_LIST**”
ServiceInfo: QU;256000;D;768000;

II.

Конфигурация ISG

Конфигурация для OpenGarden сервиса

```
ip access-list extended OG_ACL_IN
   permit ip any 192.168.110.0 0.0.0.255
ip access-list extended OG_ACL_OUT
   permit ip 192.168.110.0 0.0.0.255 any
```

Конфигурация для сервиса L4R

```
redirect server-group REDIR_GRP
 server ip 192.168.110.10 port <TCP port #>
ip access-list extended L4R_ACL_IN
   deny ip any host 192.168.110.10
   permit tcp any any
```

Конфигурация для PBHK сервиса

```
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0
  decription To WebPortal
  ip address 192.168.110.1 255.255.255.0
  ip portbundle outside
!
ip portbundle
  match access-list 198
  source Loopback0
!
access-list 198 permit ip any host 192.168.110.10
```

Конфигурация сервиса Basic HSI

```
aaa accounting network IP_ACCNT_LIST group SERVER_GROUP1
```

Конфигурация ISG

Сервисы

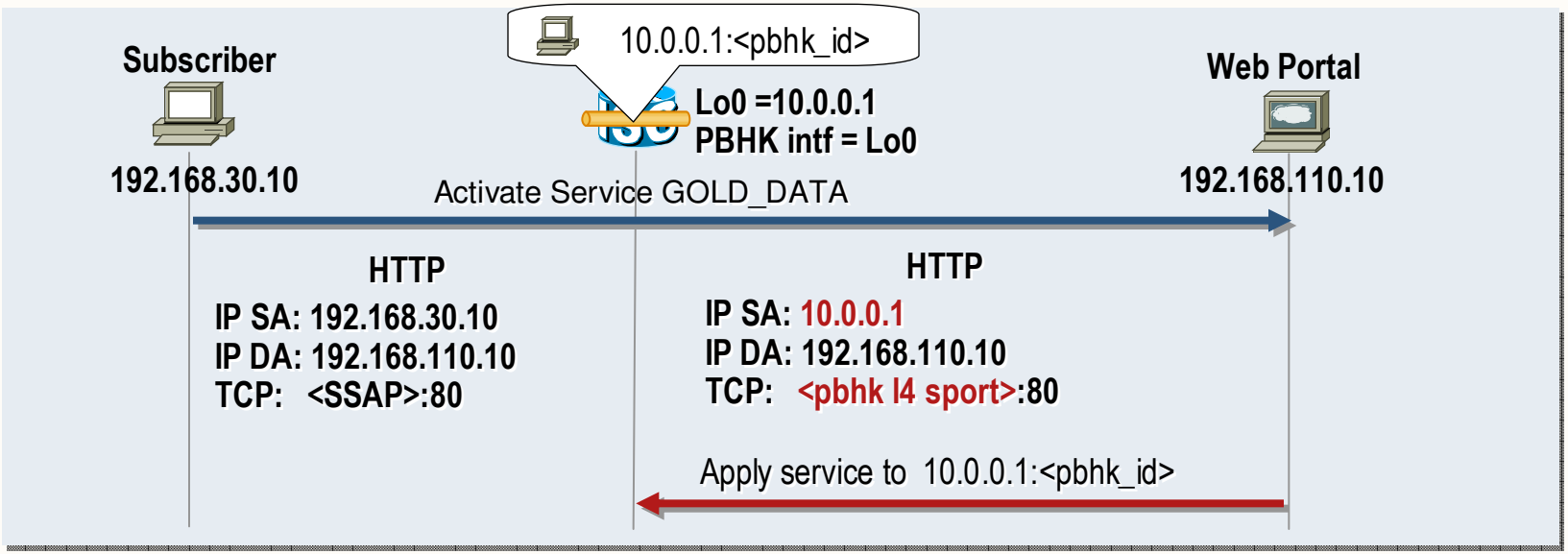
PBHK – Port Bundle Host Key

* Используется для создания host key -> идентификатор, который ISG и Веб-портал может использовать для ссылки на сессию абонента

- Извлекается порталом из пакетов, идущих от абонента
- Если PBHK - выключен: *host key: IP Source Address (IP Address абонента)*

включен: ISG делает PAT для пакетов абонента, идущих на портал

host key: ISG IP address + PBHK ID (L4Source Port (12MSBs))



* **Преимущества PBHK**: поддерживает перекрывающиеся IP адреса абонентов

Портал может не знать реальные абонентские адреса

Упрощается создание портала

Конфигурация ISG

Сервисы

Конфигурация AAA сервера

```
Service-Name = "OG_SRV"
Service Password = "servicecisco"
AVPair: ip:traffic-class=input access-group \
        name OG_ACL_IN priority 10
AVPair: ip:traffic-class=output access-group \
        name OG_ACL_OUT priority 10
AVPair: ip:traffic-class=in default drop
AVPair: ip:traffic-class=out default drop
```

```
Service-Name = "L4R_SRV"
```

II.

Конфигурация OpenGarden сервиса

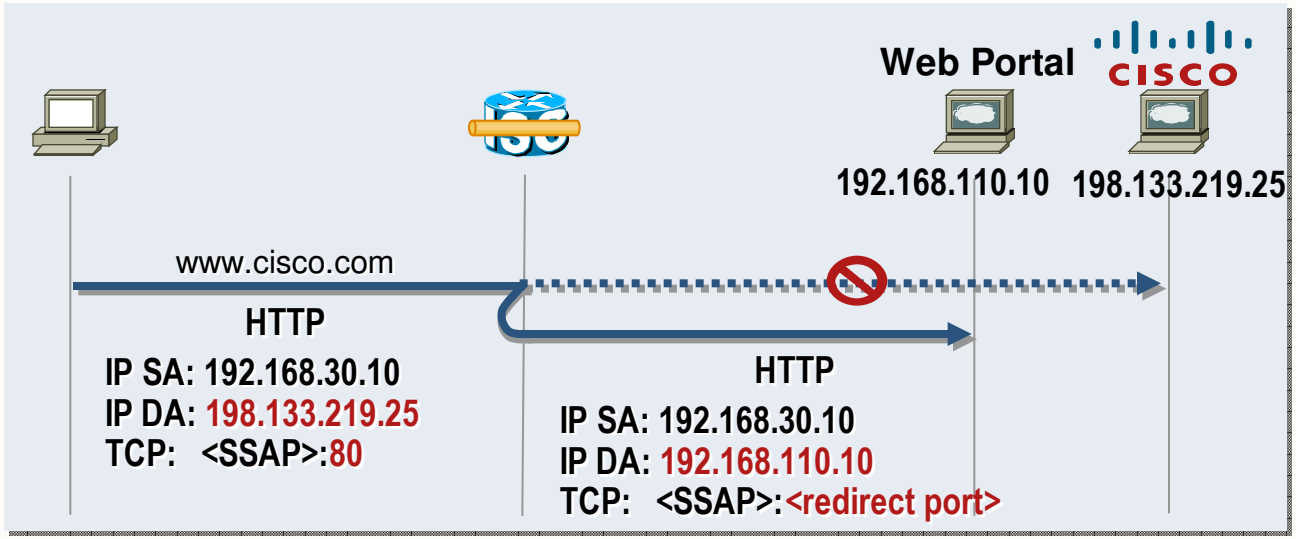
Конфигурация L4R сервиса

Конфигурация ISG

```
ip access-list extended OG_ACL_IN
   permit ip any 192.168.110.0 0.0.0.255
ip access-list extended OG_ACL_OUT
   permit ip 192.168.110.0 0.0.0.255 any
```

```
redirect server-group REDIR_GRP
 server ip 192.168.110.10 port <TCP port #>
ip access-list extended L4R_ACL_IN
  deny ip any host 192.168.110.10
  permit tcp any any
```

L4 Redirect



- трафик абонента, попадающий под описание этого сервиса, перенаправляется на адрес портала и L4-порта, определенного на ISG
- сервер отвечает за обработку перенаправленного трафика

Конфигурация ISG

Сервис

Конфигурация AAA сервера

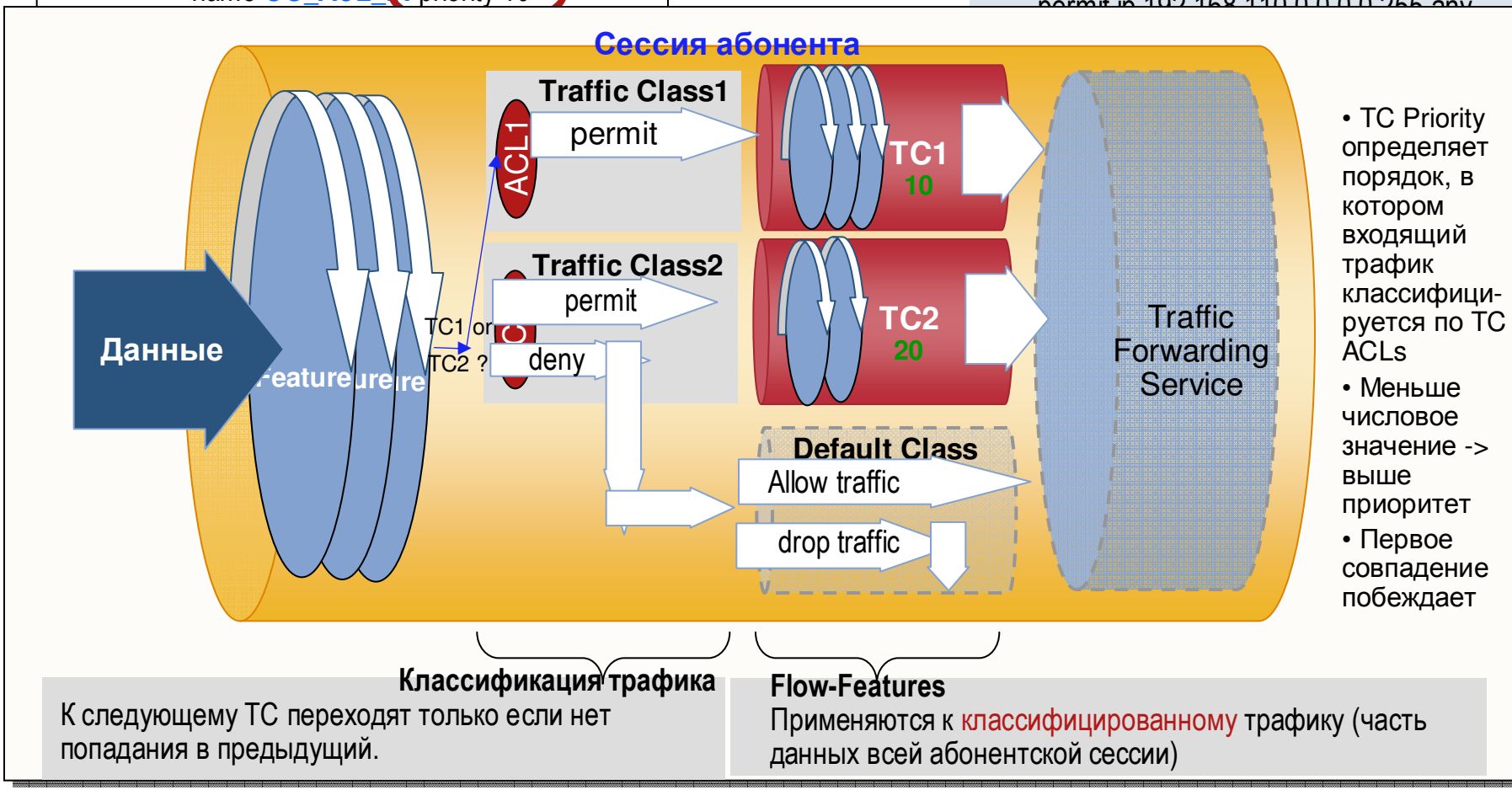
Service-Name = “**OG_SRV**”
Service Password = “servicecisco”
AVPair: ip:traffic-class=input access-group
name **OG_ACL_IN** priority 10

II.

Конфигурация сервиса OpenGarden

Конфигурация ISG

```
ip access-list extended OG_ACL_IN
    permit ip any 192.168.110.0 0.0.0.255
ip access-list extended OG_ACL_OUT
    permit ip 192.168.110.0 0.0.0.255 any
```



- TC Priority определяет порядок, в котором входящий трафик классифици-руется по TC ACLs
- Меньше числовое значение -> выше приоритет
- Первое совпадение побеждает

Классификация трафика

К следующему TC переходят только если нет попадания в предыдущий.

Flow-Features

Применяются к классифицированному трафику (часть данных всей абонентской сессии)

Конфигурация ISG

Управляющая политика (Control Policy)

```
policy-map type control IP_SESSION_RULE1
 class type control AUTH_TMR_CM event timed-policy-expiry
  1 service disconnect
 !
class type control BASIC_HSI_SRV_CM event service-start
 10 service-policy type service identifier service-name
 !
class type control BASIC_HSI_SRV_CM event service-stop
  1 service-policy type service unapply service-name
  10 service-policy type service name L4R_SRV
  20 service-policy type service name OG_SRV
 !
class type control always event session-start
  10 service-policy type service name PBHK_SRV
  20 service-policy type service name OPENGARDEN_SRV
  30 authorize aaa list IP_AUTHOR_LIST password cisco123 identifier
                                                    mac-address
  40 service-policy type service name L4R_SRV
  50 set-timer AUTH_TMR 10
 !
 class type control always event account-logon
  10 authenticate aaa list IP_AUTHEN_LIST
  20 service-policy type service unapply name L4R_SRV
  30 service-policy type service unapply name OPENGARDEN_SRV
 !
 class type control always event account-logoff
  1 service disconnect delay 5
!
```

IV. V. V. IV. IV.

Method Lists:

```
aaa authorization network IP_AUTHOR_LIST group
                                    SERVER_GRP1
aaa authentication login IP_AUTHEN_LIST group
                                    SERVER_GRP1
```

IV.

Control Classes:

```
class-map type control match-any BASIC_HSI_SRV_CM
   match service-name BASIC_HSI_SRV
```

V.

```
class-map type control match-all AUTH_TMR_CM
   match timer AUTH_TMR
   match authen-status unauthenticated
```

IV.

Interface

```
interface GigabitEthernet 0/0.1
     encapsulation dot1Q 10
     ip address 192.168.30.1 255.255.255.0
     service-policy type control IP_SESSION_RULE1
     ip subscriber l2-connected
          initiator DHCP
```

III.

DHCP Relay

```
ip dhcp pool POOL_VLAN10
  relay source 192.168.30.0 255.255.255.0
  relay destination 192.168.110.12
```

III.

DHCP server address

Заключение

Выводы

1. Функционал ISG для агрегации абонентских сессий обеспечивает управление сессиями и политиками
2. Варианты внедрения поддерживают как проводных, так и беспроводных абонентов, PPP и IP доступ

3. Большой выбор вариантов аутентификации абонентов – например: PPP CHAP/PAP, EAP,TAL, Web Logon

4. Открытые и стандартизованные интерфейсы для интеграции с внешними системами

5. Модель конфигурации, основанная на событиях и действиях, предоставляет гибкие и настраиваемые политики для управления сессиями и сервисами абонентов

Приглашаем на демонстрацию решения Cisco SEF в зал «Чехов»