Konfiguracja usług szerokopasmowych w oparciu o urządzenie ASR1000

Krzysztof Mazepa

kmazepa@cisco.com

CCIE 18662, JNCIE 137

Opis sesji

Pomimo upływu lat dostep szerokopasmowy w oparciu o sesje PPPoE/PPPoA pozostaje jedną z wielu, dla niektórych operatorów dominujacą metodą oferowania dostepu szerokopasmowego do Internetu. Urzadzenia ASR1000 to wielousługowe, skalowalne routery pozwalajace operatorom budowanie zintegrowanych usług video, głosowych oraz szybkiego dostępu do internetu.

W trakcie sesji przedstawimy przykłady konfiguracji urzadzenia ASR1000 pod kątem takich usług jak PTA (PPPoE/PPPoA), L2TP (LAC/LNS). Omówiona zostanie również konfiguracja usług opartych o rozwiązanie „Intelligent Services Gateway – ISG”. ISG umozliwia operatorom nie tylko migrację od sesji PPP do IP sessions ale również oferowanie zaawansowanych usług normalnie nie dostępnych w typowym modelu PTA.

Agenda

Metody dostępu szerokopasmowego wykorzystujące urządzenie BRAS

- PTA (PPPoA, PPPoE, RA to MPLS)
- LNS (PPPoA, PPPoE)
- IPoE

ASR 1000

- dostępne modele urządzenia
- skalowalność usług szerokopasmowych dziś i jutro
- dostępna funkcjonalność

Konfiguracja usług szerokopasmowych

Rekomendacje (materiał dodatkowy)

Ewolucja sieci dostępowych

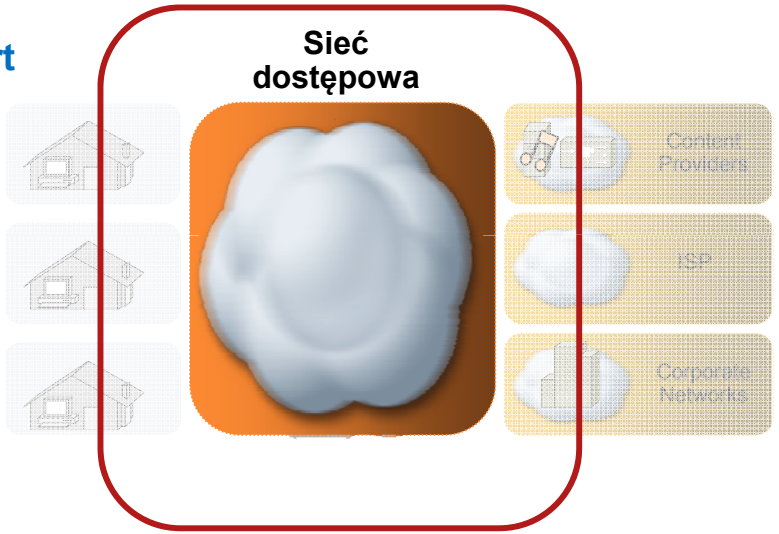
- Trzy raporty organizacji BradbandForum są przykładem ewolucji sieci dostępowych w ciągu ostatnich kilkunastu lat

  TR-25 (1999, **Core Network Architecture for Access to Legacy Data Network over ADSL**)

  TR-59 (2004, **DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services**)

  TR-101 (2006, **Migration to Ethernet-Based DSL Aggregation**)

  (TR-156 (2008))



- W kolejnych latach zmianie ulegały

  - usługi (best effort vs klasy usług)

  - protokoły (od PPPoA poprzez PPPoE do IPoE

  - technologie (od ATM do Ethernetu)

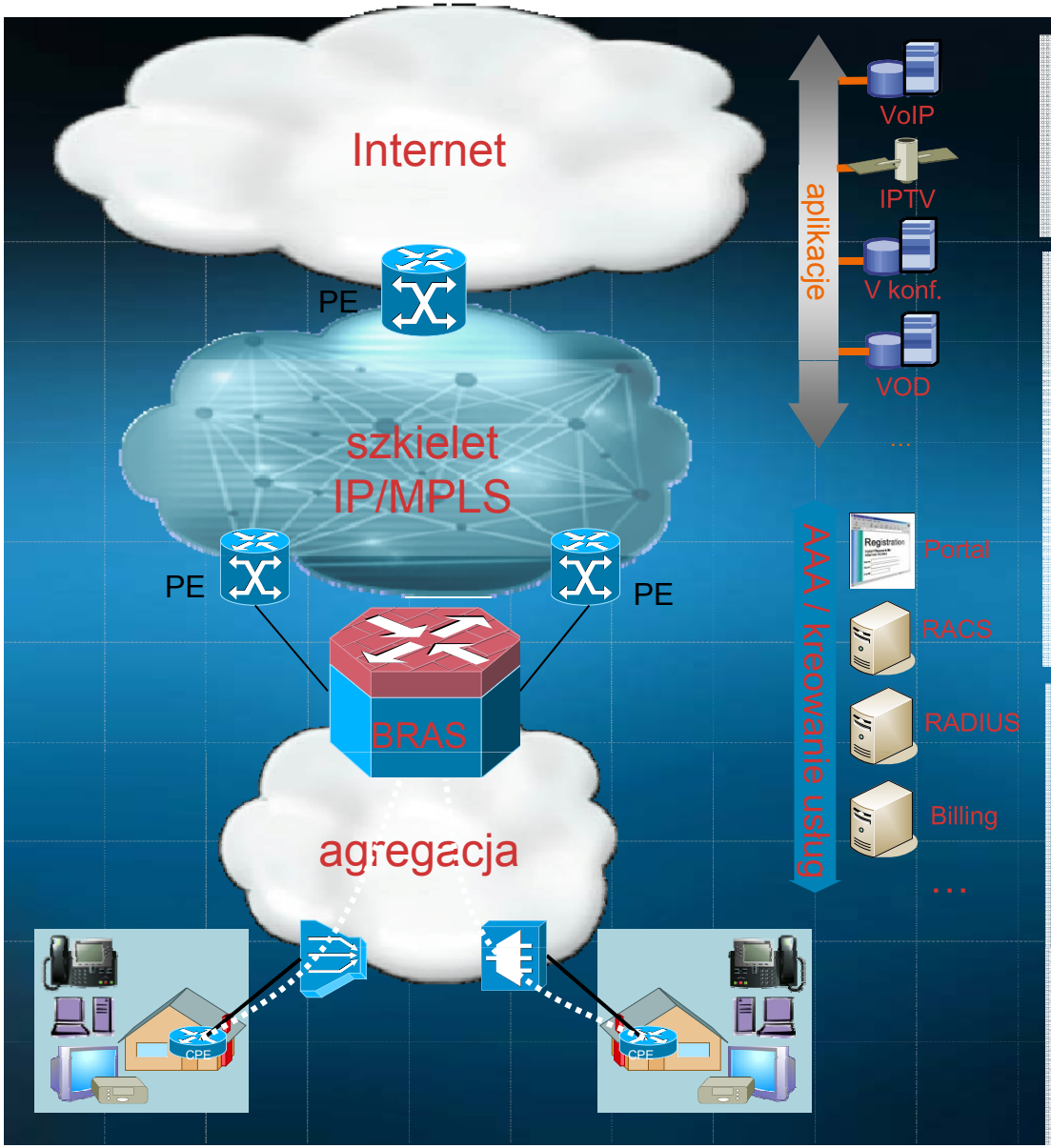
Metody dostępu szerokopasmowego wykorzystujące urządzenie BRAS

Wszystkie podawane w tej prezentacji parametry wydajnościowe **należy traktować jedynie informacyjnie**. Parametry te nie mogą być wyłączną podstawą do zaprojektowania rozwiązania.

Proszę o kontakt z inżynierem Cisco / inżynierem partnera współpracującym z Państwa firmą celem uzyskania dalszych informacji wymaganych w Państwa rozwiązaniu.

ASR1000 jako BNG

PPPoE, PPPoA, PPPoEoA



Podstawowa aplikacja

usługa szybkiego dostępu do internetu dla klientów rezydencjonalnych

Zalety rozwiązania

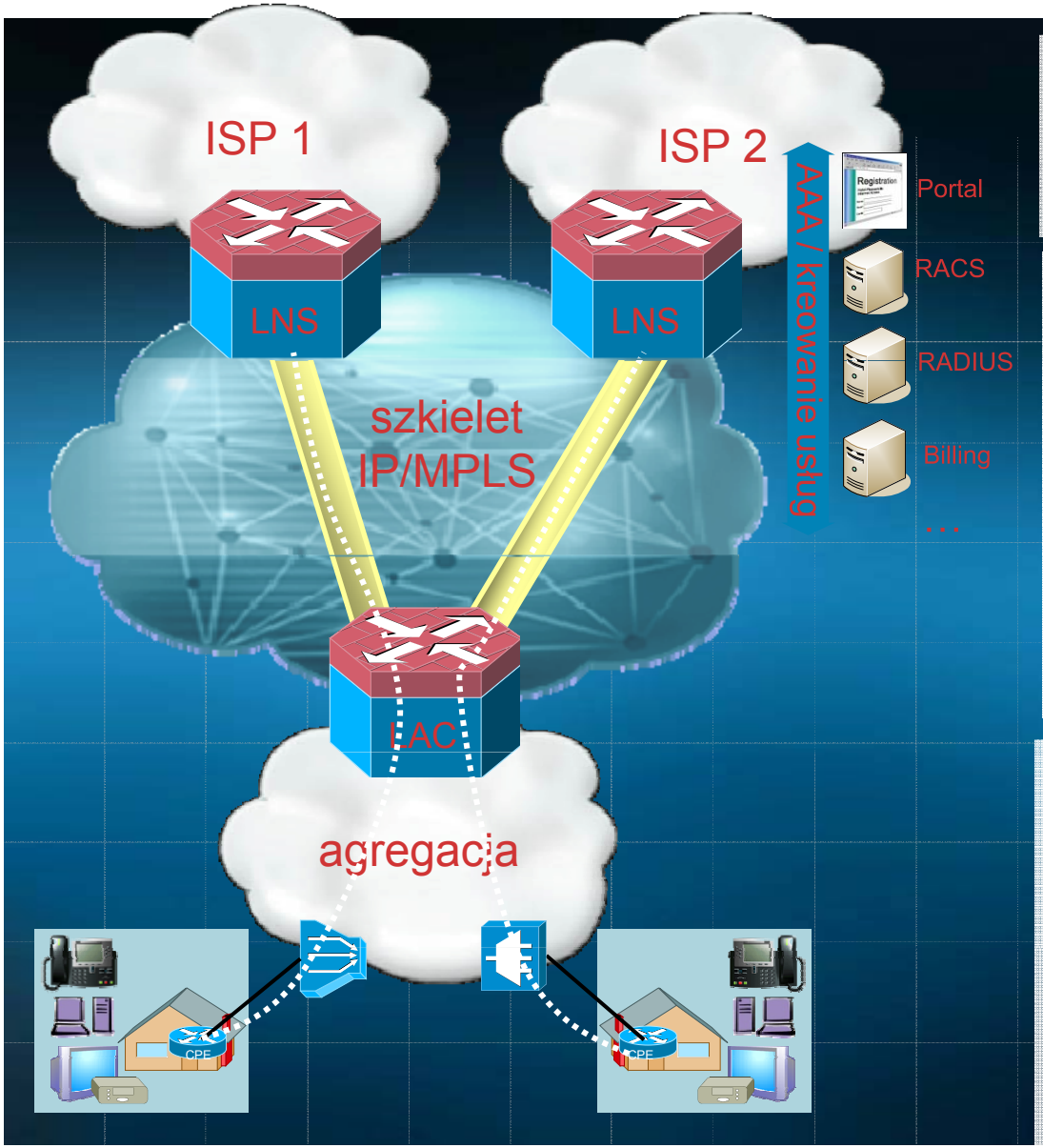
- możliwość sterowania przepustowością łącza
- możliwość wprowadzenia klas QoS
- raportowanie SLA
- często stosowane dodatkowe usługi: VoIP, różne rodzaje Video, zdalny dostęp do VPN

Wybrane zalety ASR1k

- skalowalność do 32/64k abonentów z QoS
- wysoka niezawodność (HA / SSO)
- modularne (carrier-class) chassis
- duża różnorodność dodatkowych funkcjonalności

ASR1000 jako BNG

LAC/LNS



Podstawowa aplikacja

- Bit Strem Access
- usługi hurtowego dostępu do internetu

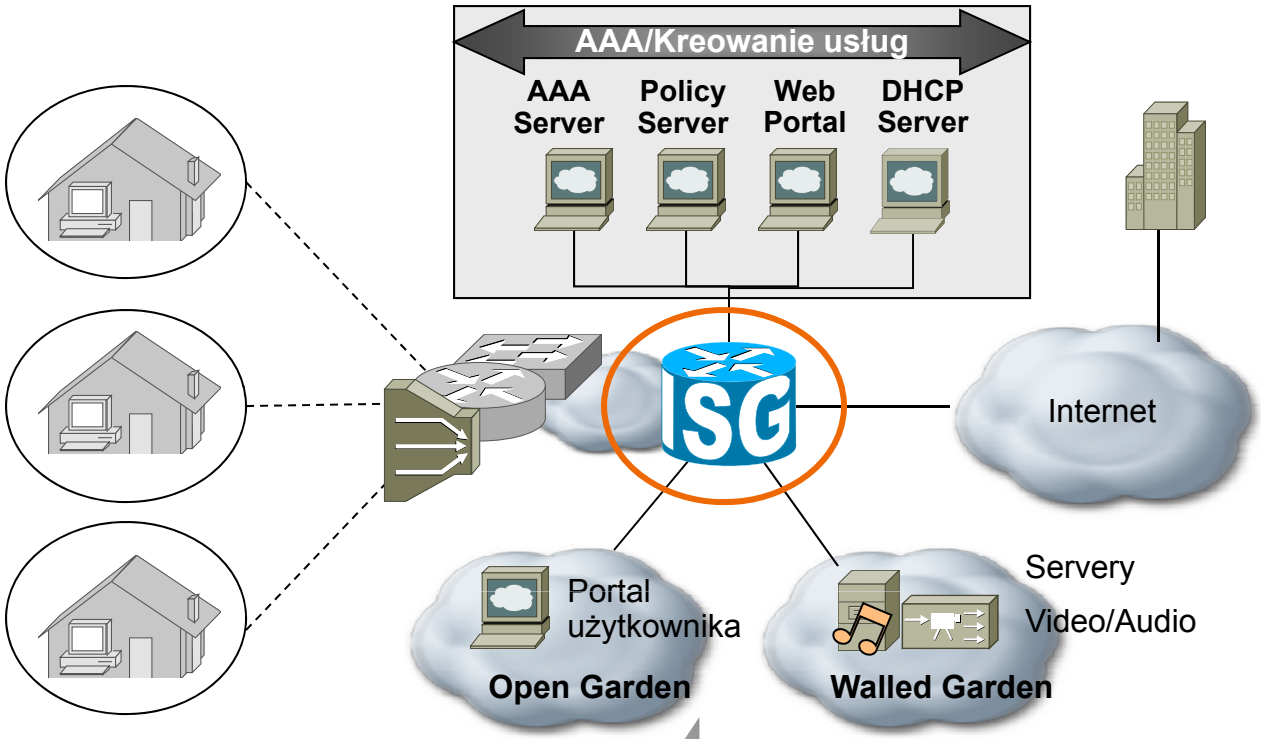
Zalety rozwiazania

- tunelowanie sesji PPP poprzez L2TP
- mozliwość authentykacji na urządzeniu LAC
- możliwość wyboru tunelu (NAS-Port ID, NAI, AVP z Radius)
- dynamiczne przydzielanie adresu IP
- redundancja LNS
- raportowanie SLA

Wybrane zalety ASR1k

- skalowalność do 16k tuneli i 32k sesji PPP z QoS (od wersji 3.3 48/64k sesji PPP)
- wysoka niezawodność (HA/SSO)
- modularne (carrier-class) chassis
- wspierana funkcjonalność ~ 7200

ASR1000 – Inteligent Solution Gateway



- ISG stosowany jest na brzegu sieci
- Współpracuje z innymi urządzeniami kontrolując pasmo i kierunek przesyłania ruchu klienta

- Identyfikacja i autentykacja klienta
- Określenie oferowanej usługi
- Dynamiczna zmiana usługi (na podstawie żądania klienta lub operatora)

Nowoczesny BNG - ASR 1000

(modele, skalowalność, funkcjonalność)

Routery Cisco serii ASR 1000

Przepustowość od 2.5 Gbps do 40Gbps dziś, w przyszłości do 360Gbps

Niewielki, wydajny router

- Przełączanie sprzętowe, wydajność od 2.5Gb/s, 128k kolejek sprzętowych
- Modularna konstrukcja (karty RP, ESP, karty liniowe SIP i SPA
- oprogr. IOS XE, IOS CLI

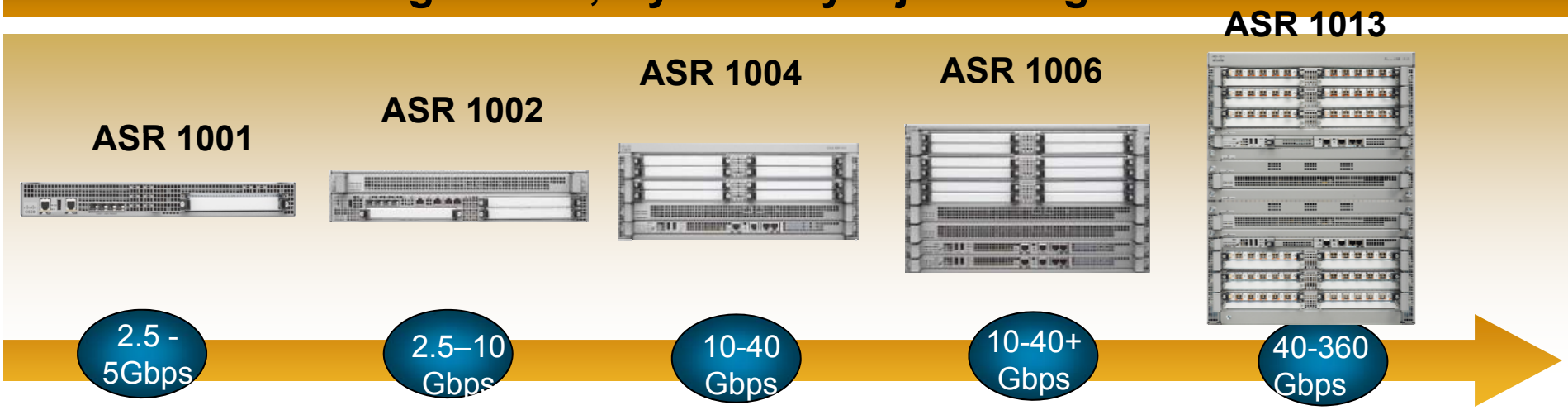
Wysoka niezawodność

- Rozdzielona warstwa kontrolna i przełączająca
- Redundancja sprzętowa i programowa
- Bezprzerwowa wymiana oprogramowania (ISSU)

Zintegrowane usługi

- Zintegrowany firewall, VPN, encrypcja, NBAR, CUBE-ENT,CUBE-SP
- Zwiększenie funkcjonalności porzez dodatkowe licencje

Zintegrowane, wysoko wydajne usługi



Porównanie dostępnych chassis ASR 1000

	ASR1001	ASR 1002	ASR 1004	ASR 1006	ASR 1013
					
Sloty SPA	1 slot	3 sloty	8 slotów	12 slotów	24 slot
Karty ESP	zintegrowane	zintegrowane	1	2	2
Sloty SIP	zintegrowane	zintegrowane	2	3	6
Redundancja IOS	programowa	programowa	programowa	sprzętowa	sprzętowa
Wbudowane porty GE	4	4	N/A	N/A	N/A
Wysokość	1.75” (1RU)	3.5” (2RU)	7” (4RU)	10.5” (6RU)	22.7” (13RU)
Pasmo	2.5 do 5 Gbps	5 do 10 Gbps	10 do 40 Gbps	10 do 40 Gbps	40+ Gbps
Max. moc wyj ściowa	400W	470W	765W	1275W	3200W
Wentylacja	przód - tył	przód - tył	przód - tył	przód - tył	przód - tył
Wbudowany moduł I/O	1 (opcja)				

ASR1001

- Idealny do oferowania usług związanych z bezpieczeństwem (dostęp), jako RR oraz router usług zarządzanych (IP VPN)
- Małe wymiary (1RU)
- Wydajność od 2.5 Gbps do 5 Gbps
- Pamięc DRAM 4G & 8G & 16G
- Enkrypcja wspierana sprzętowo z wydajnością do 1.8 Gbps
- Integracja kart ESP, RP i SIP
- Porty wejściowe
  - 4 wbudowane porty GigE
  - 1 moduł SPA
  - zintegrowana karta interfejsów
- Wysoka niezawodność sprzetowa z opcją redundancji programowej

ASR1K – skalowalność (nie dotyczy ISG)

Dane dla wersji IOS EX 3.2S

Chassis	RP	ESP	Sesje PPP	Tunele L2TP
1001	zintegrowane	zintegrowane ESP-2.5G/5G	8k	4k
1002-F	zintegrowane RP1	zintegrowane ESP-2.5G	brak wsparcia	brak wsparcia
1002	zintegrowane RP1	ESP-5G	12K	6K
1002	zintegrowane RP1	ESP-10G	24K	12K
1004	RP1	ESP-10G	24K	12K
1004	RP1	ESP-20G	24K	12K
1004	RP2	ESP-10G	brak wsparcia	brak wsparcia
1004	RP2	ESP-20G	32K	16K
1004	RP2	ESP-40G	32k	16k
1006	RP1	ESP-10G	24K	12K
1006	RP1	ESP-20G	24K	12K
1006	RP2	ESP-10G	brak wsparcia	brak wsparcia
1006	RP2	ESP-20G	32K	16K
1006	RP2	ESP-40G	32K	16K
1013	RP2	ESP-40G	32K	16K

Proszę o kontakt z inżynierem Cisco przy próbach określenia maksymalnej wydajności urządzenia ASR1000.

Rekomendowane **maksymalne** ilości sesji/tuneli zależą od użytego **chassis/RP/karty ESP** oraz **zastosowanej funkcjonalności.**

ASR1006/1013 z kartą RP2 i modułem ESP40G są rekomendowanymi konfiguracjami

Dla większych wartości zobacz slajd dotyczący „**profili usługowych**”

Dane dla wersji IOS EX 3.2S

ASR1K – skalowalność dla usługi ISG

Chassis	RP	ESP	PPP Sess	IP Sess	ISG TCs
1001	zintegrowane	zintegrowane ESP-2.5G/5G	8k	8k	24k
1002-F	zintegrowane RP1	Zintegrowane ESP-2.5G	brak wsparcia	brak wsparcia	brak wsparcia
1002	zintegrowane RP1	ESP-5G	12K	12K	36K
1002	zintegrowane RP1	ESP-10G	20K	24K	72K
1004	RP1	ESP-10G	20K	24K	72K
1004	RP1	ESP-20G	20K	24K	72K
1004	RP2	ESP-10G	brak wsparcia	brak wsparcia	brak wsparcia
1004	RP2	ESP-20G	32k	32k	96k
1004	RP2	ESP-40G	32k	32k	96k
1006	RP1	ESP-10G	20K	24K	72K
1006	RP1	ESP-20G	20K	24K	72K
1006	RP2	ESP-10G	brak wsparcia	brak wsparcia	brak wsparcia
1006	RP2	ESP-20G	32k	32k	96k
1006	RP2	ESP-40G	32K	32K	96K
1013	RP2	ESP-40G	32K	32K	96K

Proszę o kontakt z inżynierem Cisco przy próbach określenia maksymalnej wydajności urządzenia ASR1000.

Rekomendowane **maksymalne** ilości sesji/tuneli zależą od użytego **chassis/RP/karty ESP** oraz **zastosowanej funkcjonalności.**

ASR1006/1013 z kartą RP2 i modułem ESP40G są rekomendowanymi konfiguracjami

ASR1K – profile usługowe

	Przykładowy profil	Uwagi do przykładowego wdrożenia
1	32K ATM BRAS+ISG	PPPoEoA + PPPoA, ISG, ANCP, dynamiczny QoS, LI,PTA+LAC
2	32K ETH BRAS+ISG	PPPoE, ISG, ANCP, dynamiczny QoS, LI, PTA+LAC
3	32K ETH BRAS + MPLS + ISG	PPPoE, ISG, QoS, PTA, usługi ISG, MPLS-VPN
4	32K ETH BRAS – IPoE	BRAS z sesjami IPoE, usługi ISG, QoS
5	32K ETH BRAS-PPPoE+IPoE	BRAS obsługujący sesje PPPoE i IPoE, usługi ISG, QoS
6	48K ETH BRAS	Sesje PPPoE, hierarchiczny QoS, HA, brak ISG (od wersji 3.3)
7	64K ETH BRAS	Sesje PPPoE, prosty QoS (policing) , HA, brak ISG (od wersji 3.3)
8	8K LNS+ISG	Mały LNS, ASR1001 or ASR1002
9	32K LNS+ISG+MPLS	Duży LNS z usługami ISG, QoS i MPLS-VPN
10	32K PTA+LNS+ISG	Połączenie funkcjonalności LNS + BRAS (PPPoE) z usługami ISG, QoS
11	48K LNS	Duży LNS, hierarchiczny QoS, HA, brak ISG (od wersji 3.3)
12	64K LNS	Duża liczna tunel L2TP, pojedyńcze sesje PPP w tunelu, brak QoS, brak HA, brak ISG (od wersji 3.3)
13	PWLAN -L2	Usługi ISG dla PWLAN – pracuje jako warstwa dostępowa L2 , portal www (logowanie)
14	PWLAN -L3	Usługi ISG dla PWLAN – pracuje jako dostęp L3. Wykorzystuje sesje proxy Radius
15	8K ETH BRAS + ISG	Mały BRAS, ASR1001 lub ASR1002

Wszystkie podawane w tej prezentacji parametry wydajnościowe należy traktować jedynie informacyjnie.
Parametry te nie mogą być wyłączną podstawą do zaprojektowania rozwiązania.

Konfiguracja usług szerokopasmowych

Podstawowa konfiguracja PPPoE (1)
autentykacja z wykorzystaniem serwera Radius

```
aaa new-model
aaa authentication default group radius
aaa authorization network default group radius
aaa accounting network ACCT_LIST default group radius


bba-group pppoe CUSTOMER_A
        virtual-template 1
!
interface Gigabitethernet (slot/card/port)
      pppoe enable group  CUSTOMER_A
!
interface virtual-template 1
      ip unnumbered loopback1
      peer default ip address pool POOL_1
      ppp authentication chap
      ppp accounting ACCT_LIST
!
interface loopback1
ip address 192.168.1.1 255.255.255.255

ip local pool POOL_110.1.1.1 10.1.1.100

!
radius-server host 172.1.1.1 auth-port 1645 acct-port 1646 key cisco
```

Użytkownik zdefiniowany na serwerze Radius (na przykładzie Merit Radius)

```
"test"  Password = "test"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Cisco-AVPair = "ip:addr-
pool=POOL_1"
```

Podstawowa konfiguracja PPPoE (2)
autentykacja z wykorzystaniem serwera Radius

Przykład konfiguracji PPPoEoVLAN.

Możliwe jest podanie **zakresu VLAN** na których spodziewamy się przychodzących sesji **PPPoE**

```
bba-group pppoe CUSTOMER_A
      virtual-template 1


interface gigabitethernet 0/0/0.0
no ip address
no ip mroute-cache
duplex half
vlan-range dot1q 20 30
pppoe enable group CUSTOMER_A
exit-vlan-config
```

Przykład dla interfajsu QinQ z dowolnym S-VLAN'em

```
!
interface g1/0/0.10
      encapsulation dot1q 20 second-dot1q any
      pppoe enable group CUSTOMER_A
      pppoe max-sessions 1000
```

Konfiguracja PPPoEoA z dynamicznym kreowaniem interfejsów (AutoVC)

```
vc-class atm pvcr_bba_vc_class
 protocol pppoe group bba_group1
 vbr-nrt 1000 1000 1
 create on-demand
 idle-timeout 30
!
interface ATM0/0/0
 no ip address
 atm clock INTERNAL
 no atm enable-ilmi-trap
!
interface ATM0/0/0.65000 multipoint
 no atm enable-ilmi-trap
 range pvc 1/32 1/48
 encapsulation aal5snap
 protocol pppoe group bba_group1
 class-vc pvcr_bba_vc_class
```

Co to jest vc-class ?

vc- class definiuje parametry przypisane do grupy VC/PVC

Co zyskujemy używając komendę „create on-demand”?

Co zyskujey stosując komendę range-pvc ?

Cisco-AVPair – narzędzie przy konfiguracji usług

protocol : attribute sep value *

cisco-avpair= ”ip:addr-pool=first“

Przykładowe avpair

cisco-avpair= ”ip:inacl=INPUT_ACCESS_LIST_TEST_1”

cisco-avpair= ”ip:outacl=OUTPUT_ACCESS_LIST_TEST_2”

cisco-avpair = “ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet”,

cisco-avpair = “ip:inacl#4=deny icmp any any”,

cisco-avpair = “ip:route#5=10.0.0.0 255.0.0.0”,

cisco-avpair = “ip:route#6=10.10.0.0 255.0.0.0”

cisco-avpair = “atm:vc-qos-policy-in=<in policy name>”

cisco-avpair = “atm:vc-qos-policy-out=<out policy name>”

cisco-avpair = “ip:sub-qos-policy-in=<in policy name>”

cisco-avpair = “ip:sub-qos-policy-out=<out policy name>”

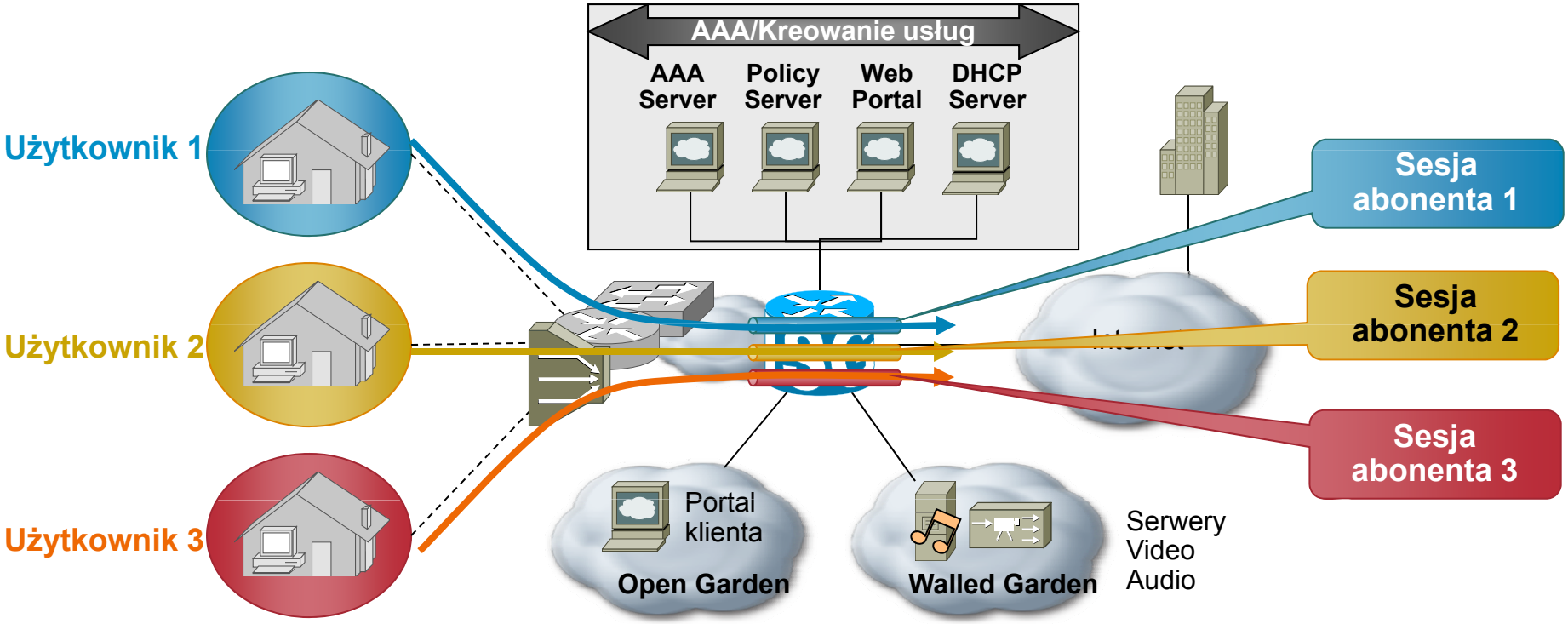
Podstawowa konfiguracja LAC i LNS
autentykacja lokalna ☺

```
!
! Router LAC
!
vpdn enable
!
vpdn-group isp_tylko_przykład.com
  request-dialin
    protocol l2tp
  domain isp.com
   initiate-to ip 10.0.0.13
     local name LAC1
     l2tp tunnel password cisco
!
bba-group pppoe customerA
  virtual-template 1
!
interface g1/0/0
  pppoe enable group customerA
!
interface virtual-template 1
  ppp authentication pap chap
```

```
!
! Router LNS
!
vpdn enable
!
vpdn-group isp_inny_przykład.com
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname LAC1
 l2tp tunnel password 0 cisco
!
Interface Loopback100
Ip address 100.1.1.1 255.255.255.255
!
interface Virtual-Template2
 ip unnumbered Loopback100
 peer default ip address pool POOL_1
 ppp authentication chap
!
username user@isp.com pass cisco
!
ip local pool  POOL_1 10.1.1.1
10.1.1.100
```

Uwaga
Jeżeli authentykujemy użytkownika korzystając
z serwera RADIUS to wówczas definiujemy użytkownika następująco (przykład)
"user@isp.com" Password = "cisco"
    Service-Type = Framed-User,
    Cisco-AVPair = "ip:addr-pool=POOL_1"

IPoE z wykorzystaniem rozwiązania ISG



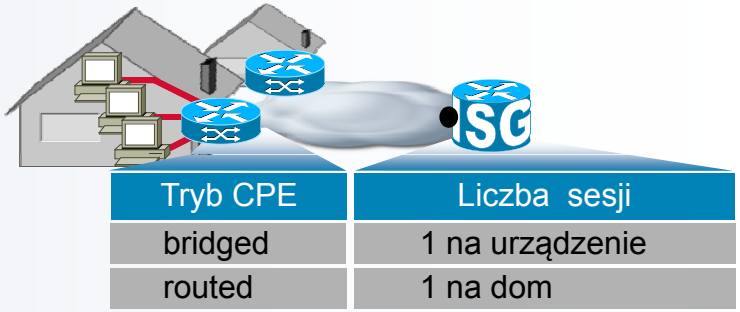
- Sesja utworzona jest automatycznie reprezentując pojedynczego abonenta usługi
- Sesja tworzona jest w momencie pojawienia się ruchu klienta (**FSOL** = First Sign Of Life)

Rodzaje sesji

Sesje tworzone dynamicznie

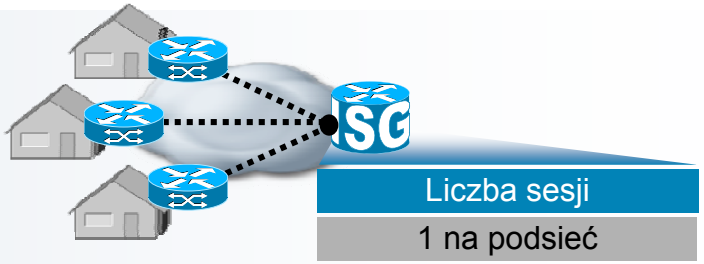
sesje PPP

sesje IP



sesja IP reprezentująca podsieć

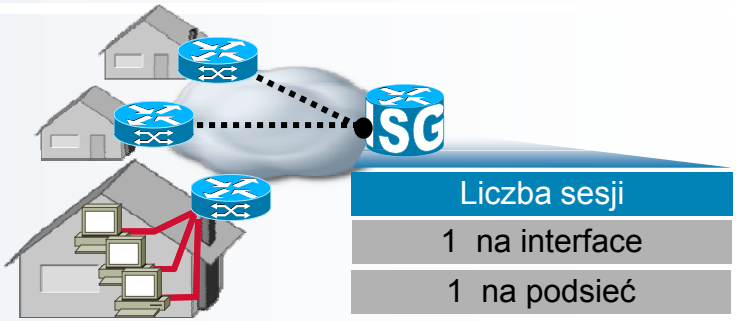
- Przynależność do sesji określona podczas autentykacji
- Autentykacja jest obowiązkowa w tego rodzaju konfiguracji



Sesje utworzone statycznie

możliwe tylko dla sesji IP

wymagana ręczna konfiguracja po stronie operatora



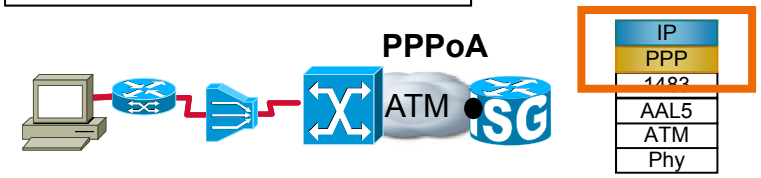
Sesje tworzone dynamicznie

ISG Session

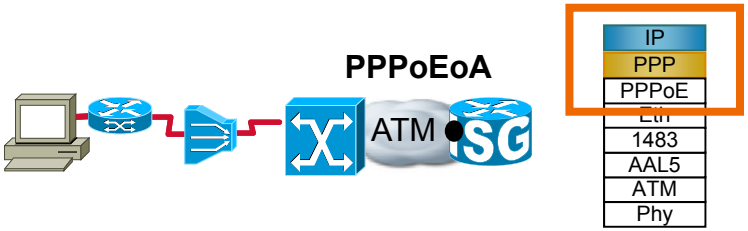
Sesje PPP

Interface Virtual Template
(sub)interface Virtual Access

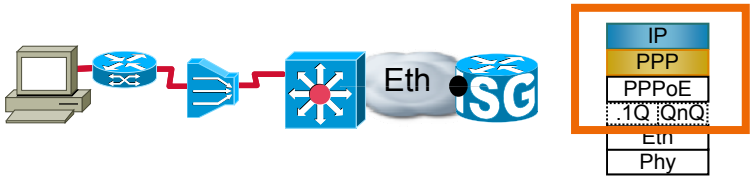
PPPoA



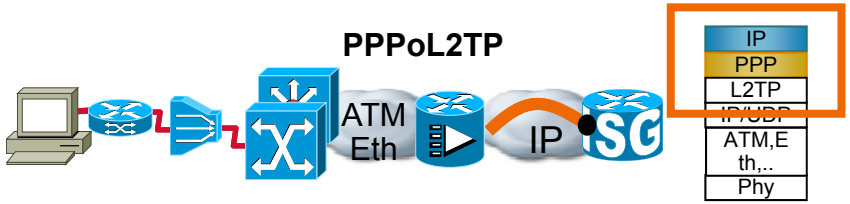
PPPoEoA



PPPoEoE / PPPoEoVLAN/PPPoEoQnQ

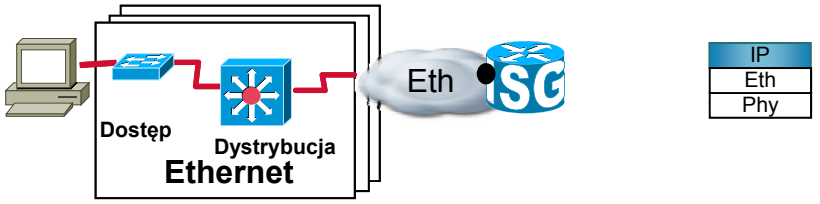


PPPoL2TP

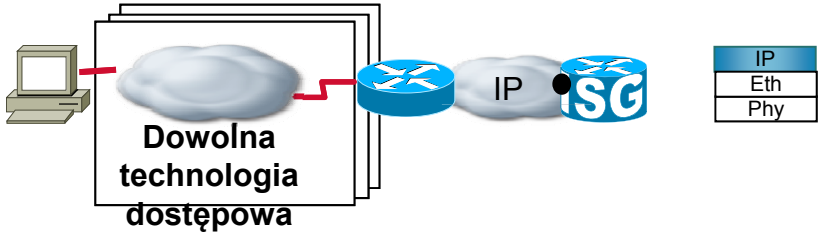


Sesje IP

IP (stosując wartwę 2)



IP (stosując warstwę 3)



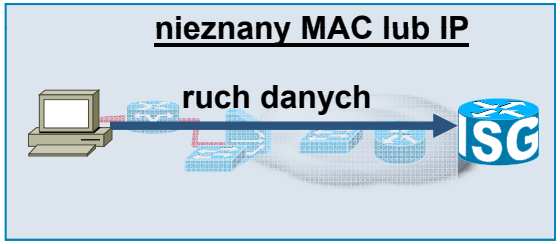
Utworzenie sesji

- Sesje ISG są utworzone w momencie rozpoczęcia ruchu klienta (First Sign of Life - FSOL)
- FSOL zależy od typu sesji

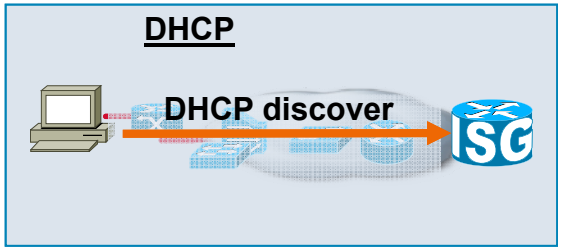
FSOL – sesje PPP

FSOL – sesje IP

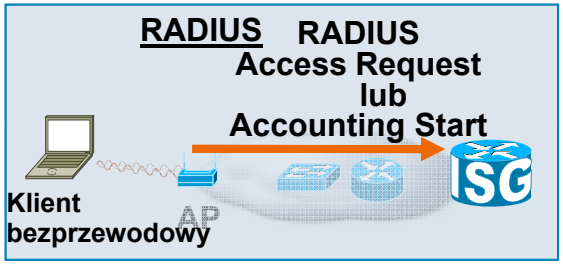
.... mozliwe są następujące opcje .....



- Pakiet IP z nieznanym adresem MAC lub źródłowym adresem IP
  Stosujemy MAC dla sesji IP tzw. L2-connected
  stosujemy adres IP dla sesji IP L3



- Pakiet DHCP Discover
- ISG musi pracować jako DHCP Relay lub server DHCP



- RADIUS Access/Accnt Start
- ISG musi pracować jako Radius Proxy
- Zastosowanie typowe w konfiguracjach PWLAN i WiMAX

Autentykacja sesji

Autentykacja - zezwala na dostęp do zasobów sieciowych tylko dla znanych użytkowników

Wspierane sposoby autentykacji

- **powiązane z protokołami wykorzystanymi w warstwie dostępowej:**
  - PPP: CHAP/PAP
  - IP: EAP dla klientów sieci bezprzewodowych
  - autentykacja DHCP
- **Transparent Auto Logon (TAL):**
  - autentykacja użytkownika wykorzystujaca identyfikatoy sieciowe abonenta
  - np. adres MAC/IP, DHCP Option 82, tagi PPPoE ...
- **Portal użytkownika - Web Logon**

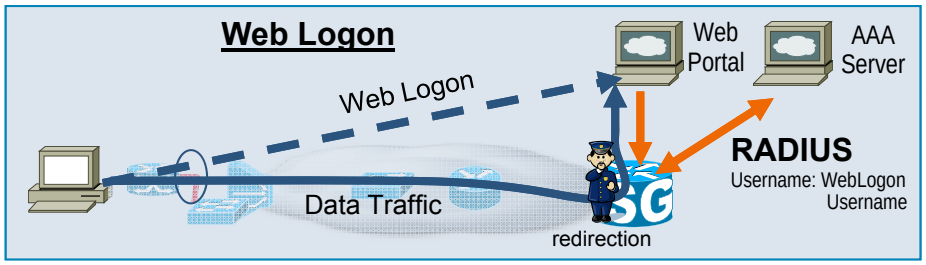
Autentykacja choć nie jest obowiązkowa, zwykle jest zastosowana

Autentykacja dla sesji IP

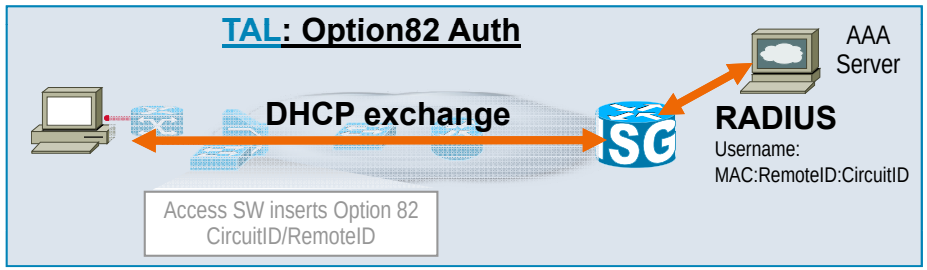
ISG Session

Możliwe scenariusze

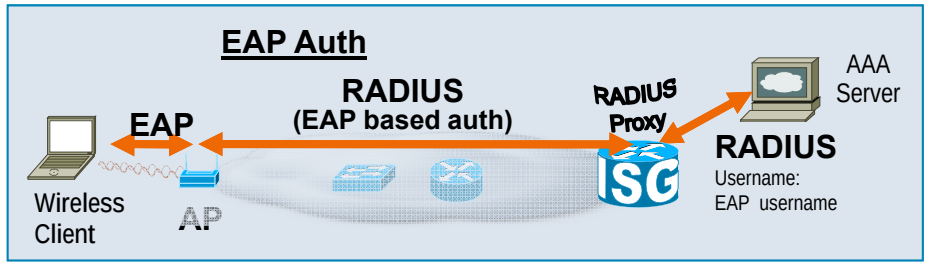
Prawdopodobieństwo zastosowania



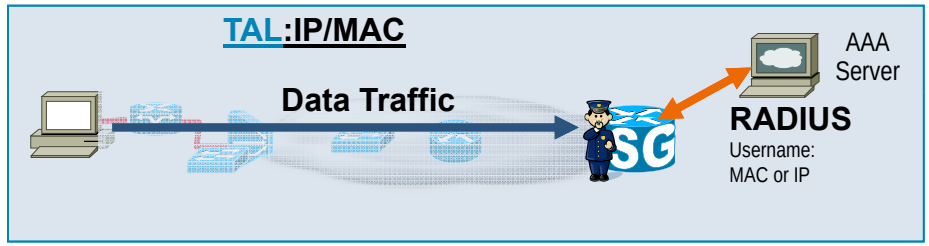
- Użytkownik zostaje przekierowany do portalu celem autentykacji
- Dane użytkownika przekazane są do urządzenia ISG
- ISG autentykuje użytkownika



- Przełącznik dostępowy uzupełnia żadanie DHCP Requests o parametr „Option82 Circuit” i „Remote ID”
- ISG dokonuje autentykacji tworząc nazwę użytkonika z połączenia parmetrów „Option 82 Circuit” i „remoteID”
- Wymaganie – sesja ISG jest zainicjowana stosując DHCP



- Użytkonik rozpoczna autentykację EAP dołączając się do punktu dostępowego (AP)
- ISG wciela się w rolę serwera RADIUS w kierunku AP, klienta RADIUS w kierunku rzeczywistego serwera
- Sesja ISG musi być skonfigurowana jako „RADIUS initiated”



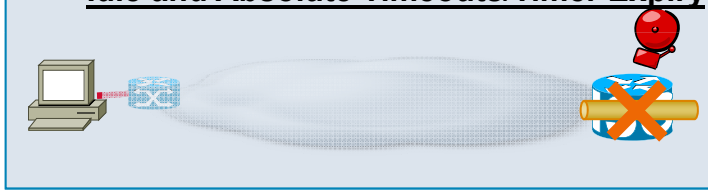
- ISG dokonuje autentykacji wykorzystując źródłowy adres MAC/IP jako identyfikatory klienta.
- Adres MAC jet stosowany typowo dla warstwy dostępowej L2, adres IP dla topologi L3.

Zakończenie sesji

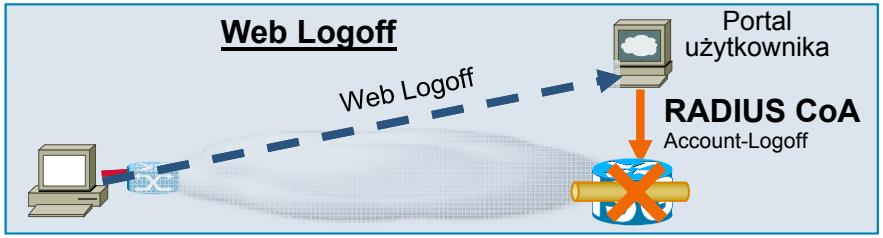
ISG Session

Sesje IP i PPP

Idle and Absolute Timeouts/Timer Expiry

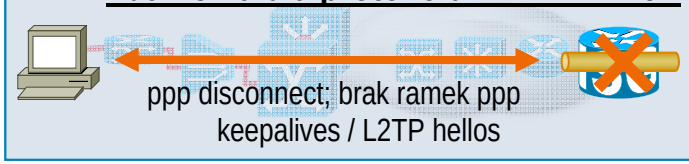


Web Logoff



Unikalne dla sesji PPP

Zdarzenia dla protokołu PPP i PPPoX



RADIUS PoD (Packet Of Disconnect)

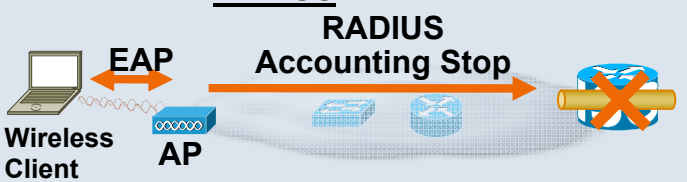
Unikalne dla sesji IP

ICMP/ARP keepalive failure

ICMP Keepalives j est stosowany dla sesji L3
ARP keepalives jest stosowany dla l2-connected sessions

DHCP

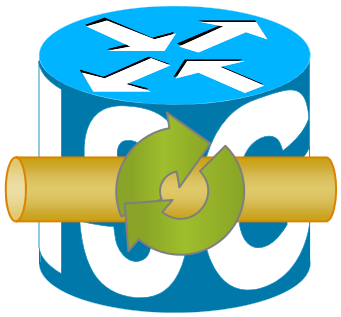
RADIUS



Dotycy sesji „DHCP initiated”

Usługi ISG

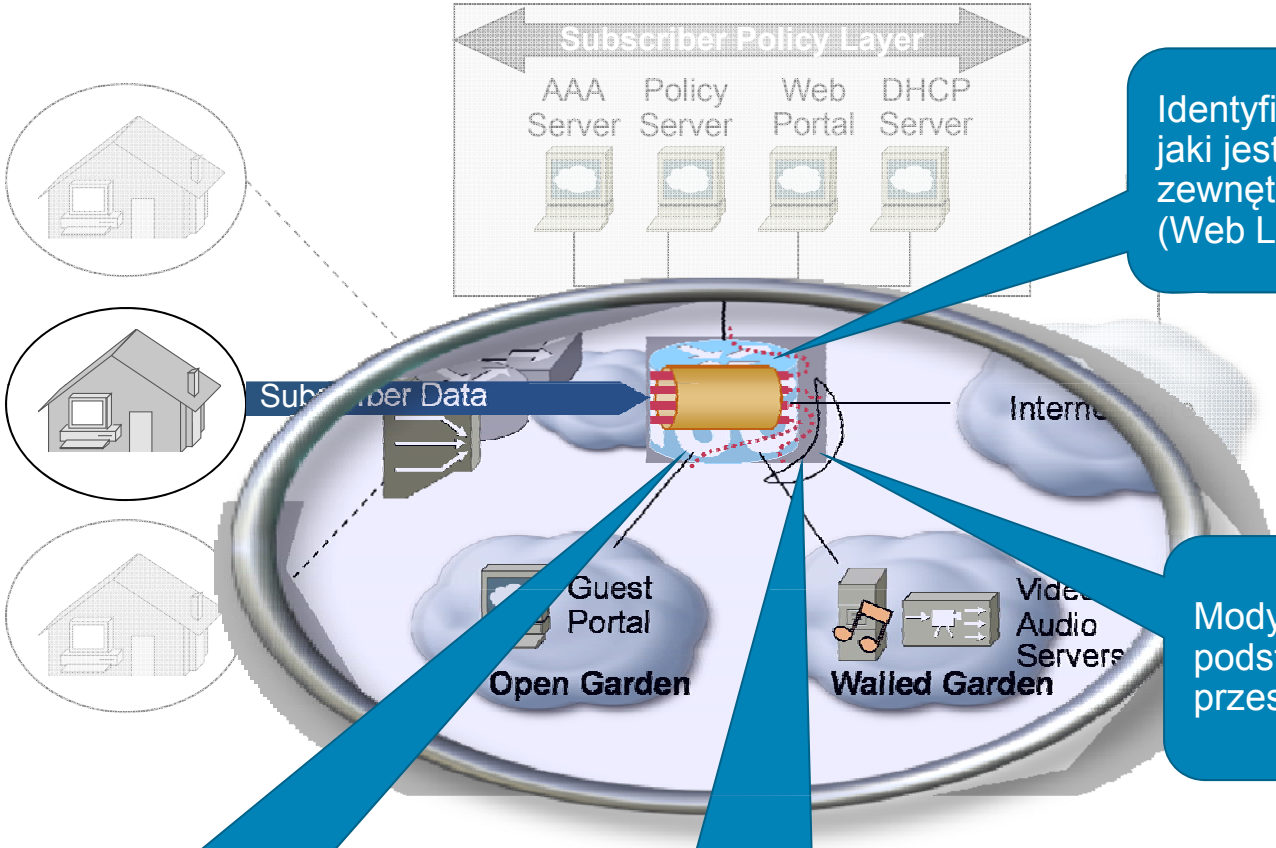
Definicja usługi zbiór funkcjonalności mających zastosowanie dla sesji klienta (usługa 1, usługa 2, usługa 3, usluga n)



Usługi		
	Zarządzanie sesją	Portbundle (PBHK) Keepalives: ICMP oraz ARP Timeouts: Idle, Absolute
	Kształtowanie ruchu	QoS: Policing, MQC Security: Per User ACLs
	Przesyłanie ruchu	Kontrola adresu przydzielonego klientowi Przekierowanie: początkowe, stałe, okresowe przydzielenie do VRF (początkowe, okresowe)
	Accounting	PostPaid Prepaid: Time/Volume based Tariff Switching Interim Broadcast

Jak wykorzystywać mozliwe usługi ?

ISG services



Identyfikuje rodzaj ruchu, jaki jest przekierowany do zewnętrznego serwera (Web Logon, reklama)

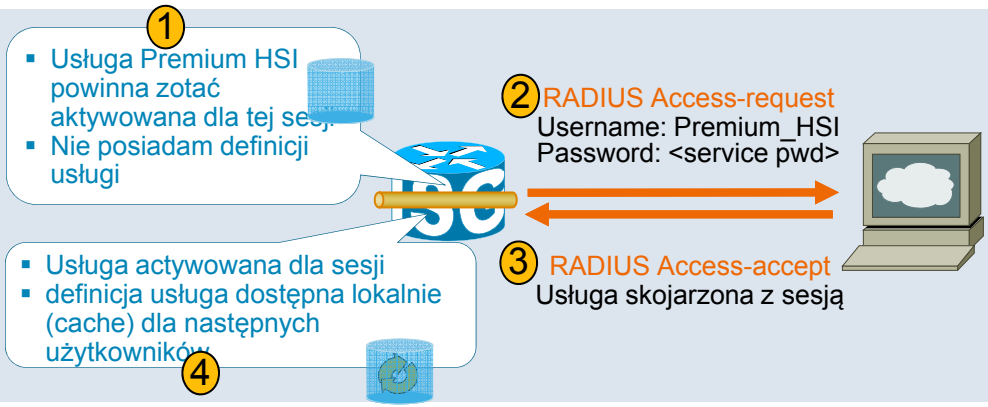
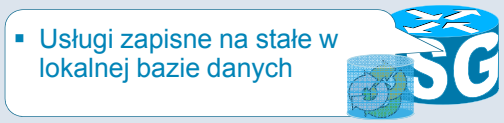
Modyfikacja bilingu na podstawie rodzaju przesyłanych danych

Zezwala na ruch wyłacznie w obszarze Open Garden dla nieznanego użytkownika

Umozliwia konfigurację QoS dla róznych klas ruchu

Definiowanie usług

ISG services

	Miejsce	Sposób otrzymania definicji usługi
	**Server AAA** ▪ Usługi zdefiniowane w **Profilach usługowych** ▪ Wykorzystanie standardowych i Vendor Specific atrybutów RADIUS ▪ Przesyłane do ISG na żądanie	
	**Policy Manager** **(wspierający interface SGI)** ▪ Usługi zdefiniowane w XML ▪ ISG ma lokalną kopię wszystkich usług	
	**ISG** ▪ Usługi wstępnie skonfigurowane stosując CLI ▪ Usługi są zdefiniowane w **Service Policies:** policy-map type service <name>	

Cisco Policy Language CLI

Control policy-map	Conditional class of events	Actions
policy-map type control <*name*>	event 1 class type control <*conditions*> event <*event type*>	action1 action2 more actions for event .....
	event 2	
	more events	

Element typopwo skonfigurowany na interface

Definiuje wszystkie aspekty związane z sesją klienta

Zdarzenia są identyfikowane poprzez ich rodzaj

Typowe przykłady:

- Session-start: zauważono nową sesję
- Account-logon: wiadomość Account-Logon msg. Otrzymana z zewnętrznego źródła
- Service-start: otrzymano żądanie „new service start” z zewnętrznego źródła
- Service-stop: otrzymanao żądanie „Service termination req.” z zewnętrznego źródła
- Timed-policy-expiry: ustawiony czas upłynął

Akcje przypisane do zdarzeń są wykonane tylko wówczas jeżeli spelnione są zdefiniowane warunki

Akcje są wykonywane zgodnie ze zdefiniowaną listą

Typowe przykłady akcji to:

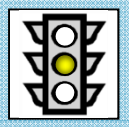
- Service: uruchomienie nowej usługi
- Service Unapply: wyłączenie aktywnej usługi
- Authenticate: wykonanie autentykacji użytkownika
- Set-Timer: umożliwia wykonanie innego zdarzenia po upływie zdefiniowanego czasu

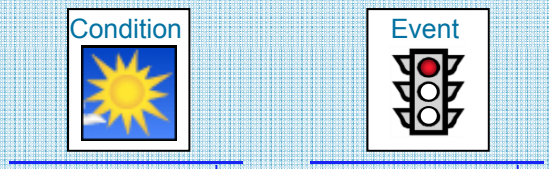
Definicja Control Policy

policy-map type control

Control Policy

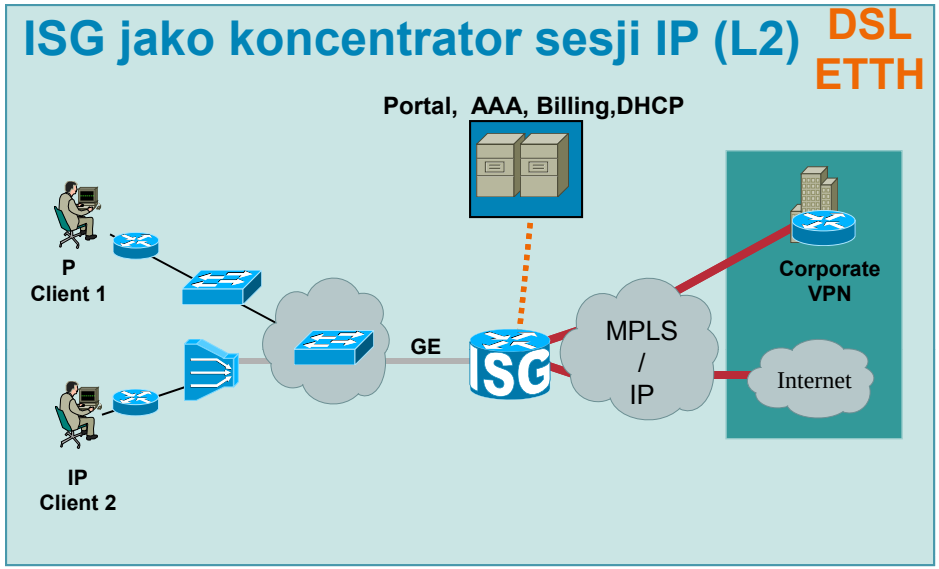
Powiązanie zdarzeń i warunków w listę wykonywanych akcji

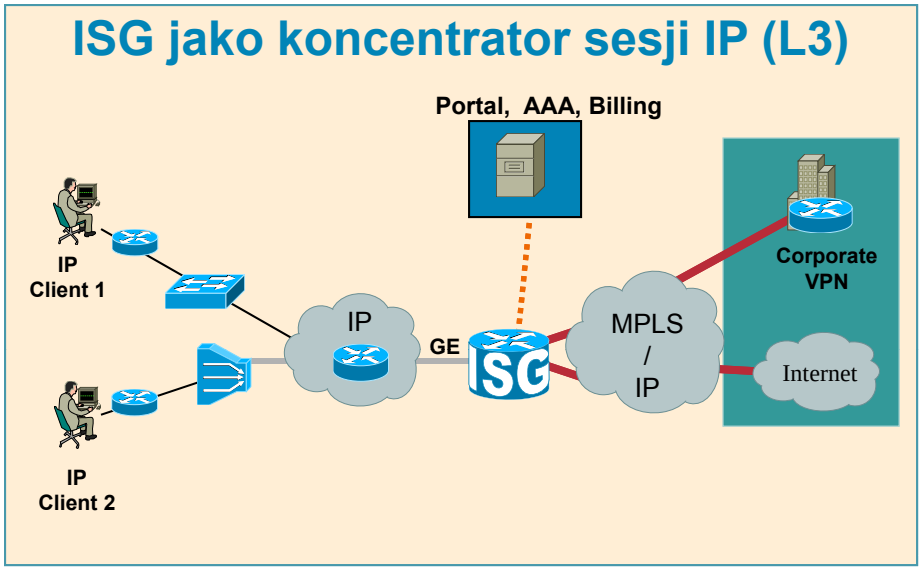
Condition	Event	Condition	Event	Condition	Event
					
Control Class: *List of Actions*		**Control Class:** *List of Actions*		**Control Class:** *List of Actions*	
1. Disable Service B 2. Enable Service A		1. Enable Service X 2. Enable Service Y 3. Take Action R		1. Enable Service PBHK 2. Take action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




```
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 IP_UNAUTH_TIMER 15
 !
 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 CND_U event timed-policy-expiry
  10 service disconnect
!
```

Przykład zastosowania sesji IP

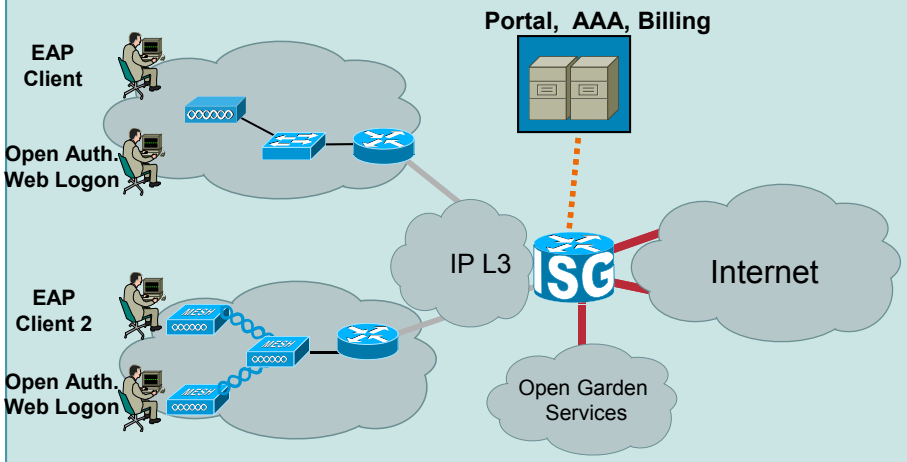




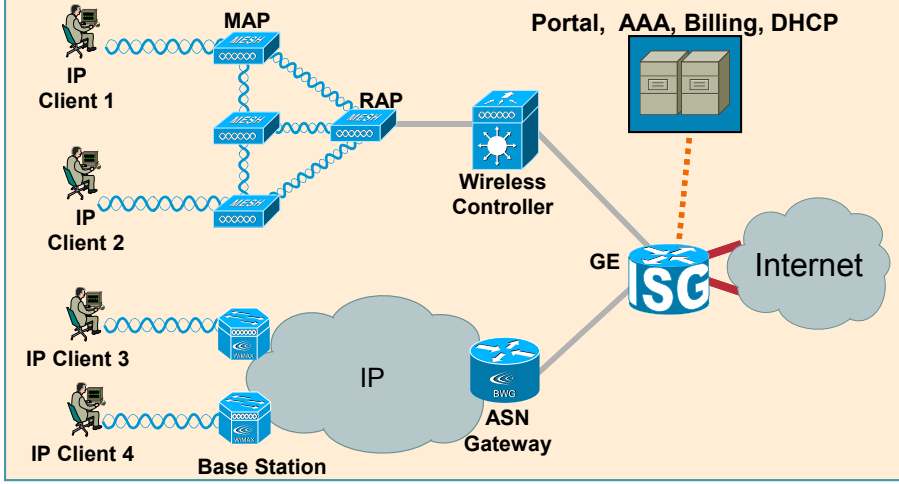
	Przydzielenie adresu	Inicjacja sesji poprzez	Interface	Autentykacja
L2–IP aggregator	ISG iako DHCP Relay lub Server	DHCP	GE (.1Q)	L4R w kierunku portalu TAL (Option-82)
			ATM GE (QinQ)	L4R w kierunku portalu TAL (Nas_Port_ID)
	ISG nie jest powiązany z usługą DHCP	MAC	GE (.1Q)	L4R w keruku portalu TAL (MAC address)
			ATM GE (QinQ)	L4R w kierunku portalu TAL (Nas_Port_ID)
L3–IP aggregator	ISG jako DHCP Server	DHCP	GE	L4R w kieruku portalu TAL (Option-82)
	ISG nie jest powiązany z usługą DHCP	IP	GE	L4R w kierunku portalu TAL (IP//MAC Address)

Dostęp do sieci publicznych

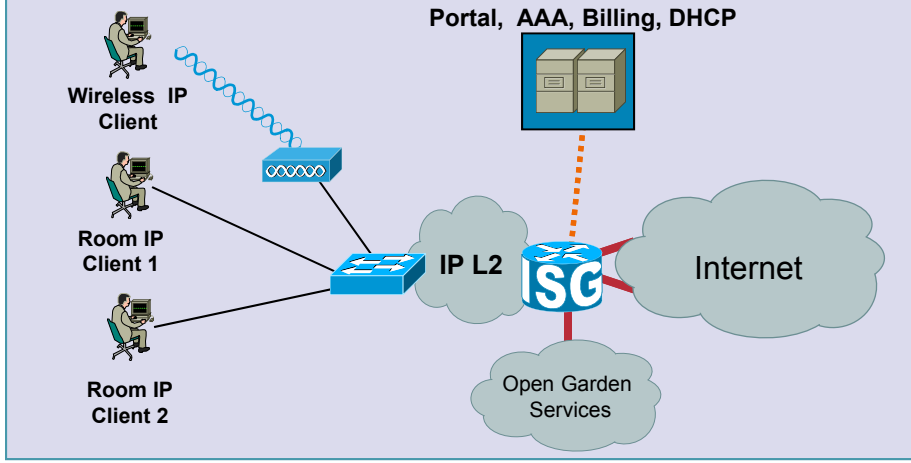
ISG w rozwiązaniach PWLAN



ISG for Municipal/ResidentialWireless Access



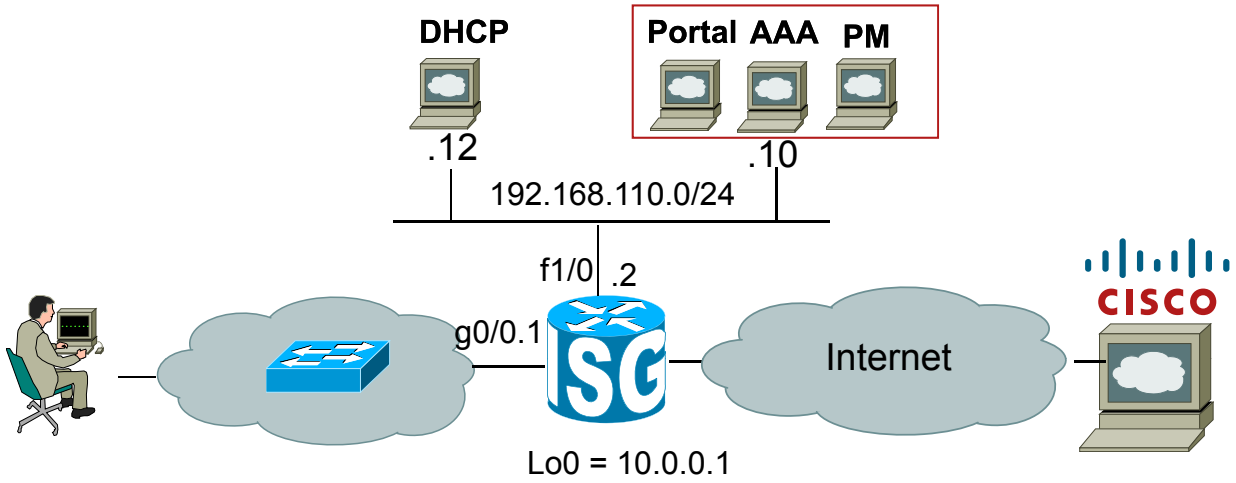
ISG for Hospitality



	Address Assignm.	Session Initiator	Interf	Authentication
PWLAN	AZR (ISG not in DHCP path)	RADIUS/ IP	L3	L4R to portal RADIUS (EAP clients)
Municipal Access (WiFi only)	ISG is DHCP Server	DHCP	.1Q or L3	L4R to portal
		RADIUS		RADIUS (EAP clients)
	ISG not in DHCP path	MAC	.1Q	TAL (IP Address) then L4R
		MAC		TAL (MAC)
		RADIUS	L3	L4R to portal
		RADIUS		RADIUS (EAP clients)
Hospita-lity	ISG is DHCP Relay or Server	DHCP	L2	TAL (Option82)
		DHCP		L4R to portal

Przykład
ISG jako koncentrator sesji IP

ISG jako koncentrator sesji IP (L2)



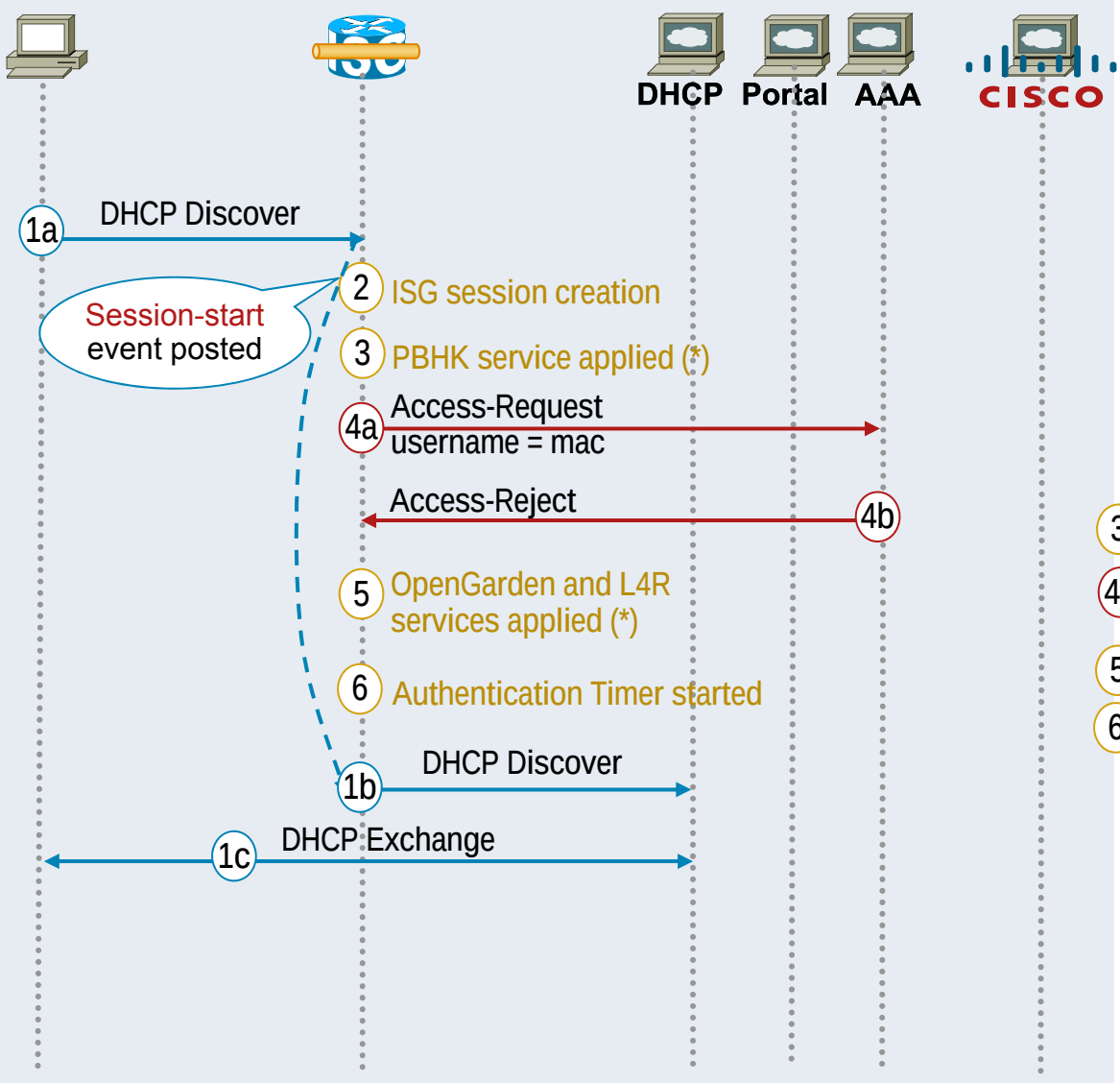
Przydział adresów	Inicjalizacja sesji	Interf.	Autentykacja
DHCP ISG jest DHCP Relay	DHCP	GE (.1Q)	TAL (mac address) oraz Web Logon

- Po zalogowaniu abonent uzyskuje dostęp do zasobów ze standardowo zdefiniowaną usługą szybkiego dostępu do internetu
- - 256Kbps upstream/ 768Kbps downstream poprzez policing relaizowany na ISG

  - accounting

  - idle timeout (10 min)

Jak to działa w detalach ☺

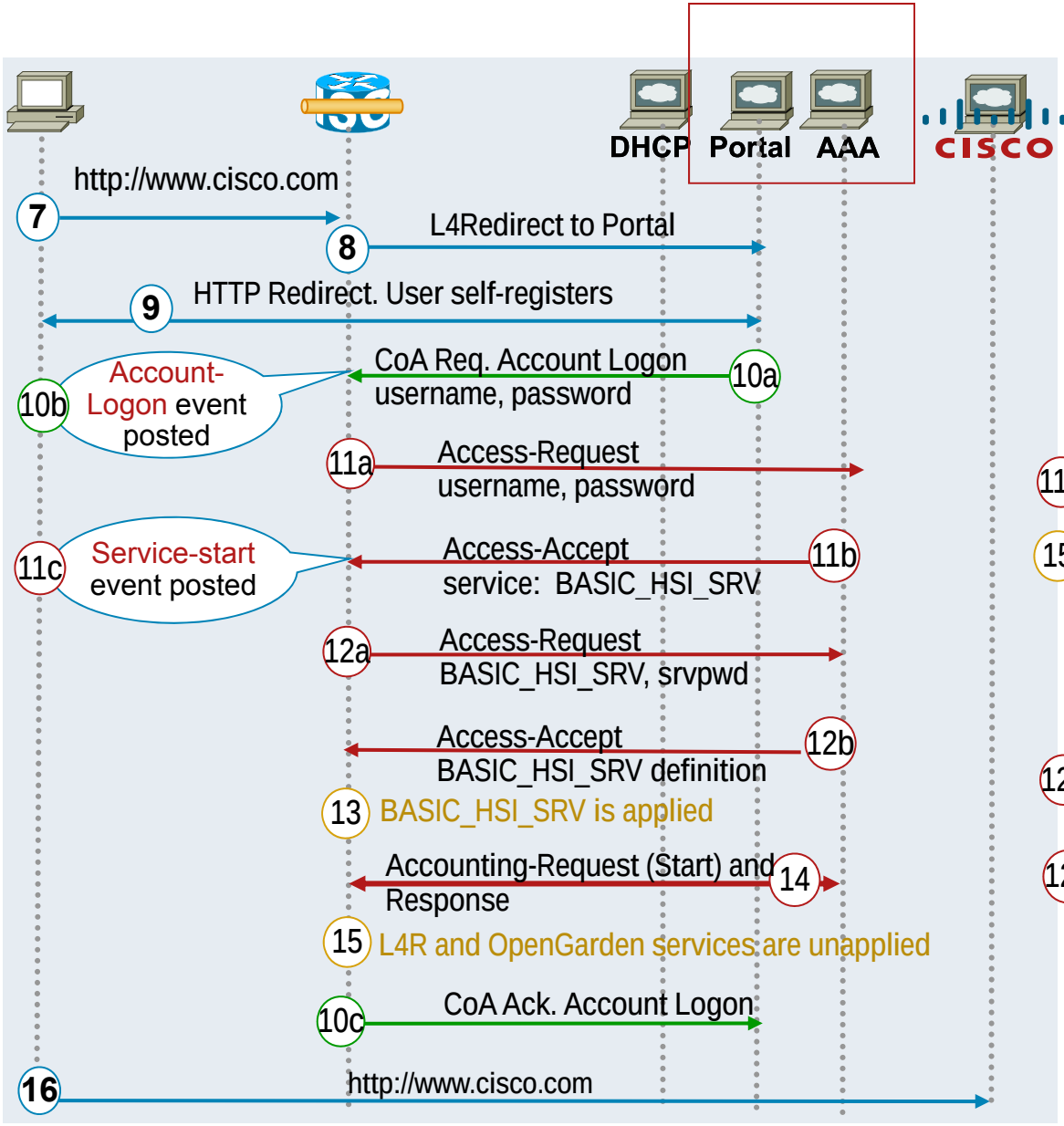



```
interface GigabitEthernet 0/0.1
  encapsulation dot1Q 10
  ip address ...
  service-policy type control IP_SESSION_RULE1
  ip subscriber l2-connected                    (2)
       initiator DHCP
```

```
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
```

(*) assumes that the definition of PBHK, L4R and OpenGarden are already available on the ISG

Jak to działa w detalach ☺



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   10b
11a 10 authenticate aaa list IP_AUTHEN_LIST
    20 service-policy type service unapply
15                              name L4R_SRV
    30 service-policy type service unapply
                                name OG_SRV
  !
  class type control BASIC_HSI_SRV event
                                service-start   11c
12a 10 service-policy type service identifier service-
                                name
```

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;

Przykładowa konfiguracja (1)

NorthBound Interfaces

I.

RADIUS interface configuration

```
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
```

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

RADIUS Extensions interface configuration

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

Przykładowa konfiguracja (2)

Services

AAA Server configuration

```
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.

Cfg required on ISG

OpenGarden service associated configurations

```
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
```

L4R service associated configurations

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

PBHK service associated configurations

```
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
```

Basic HSI service Associated configurations

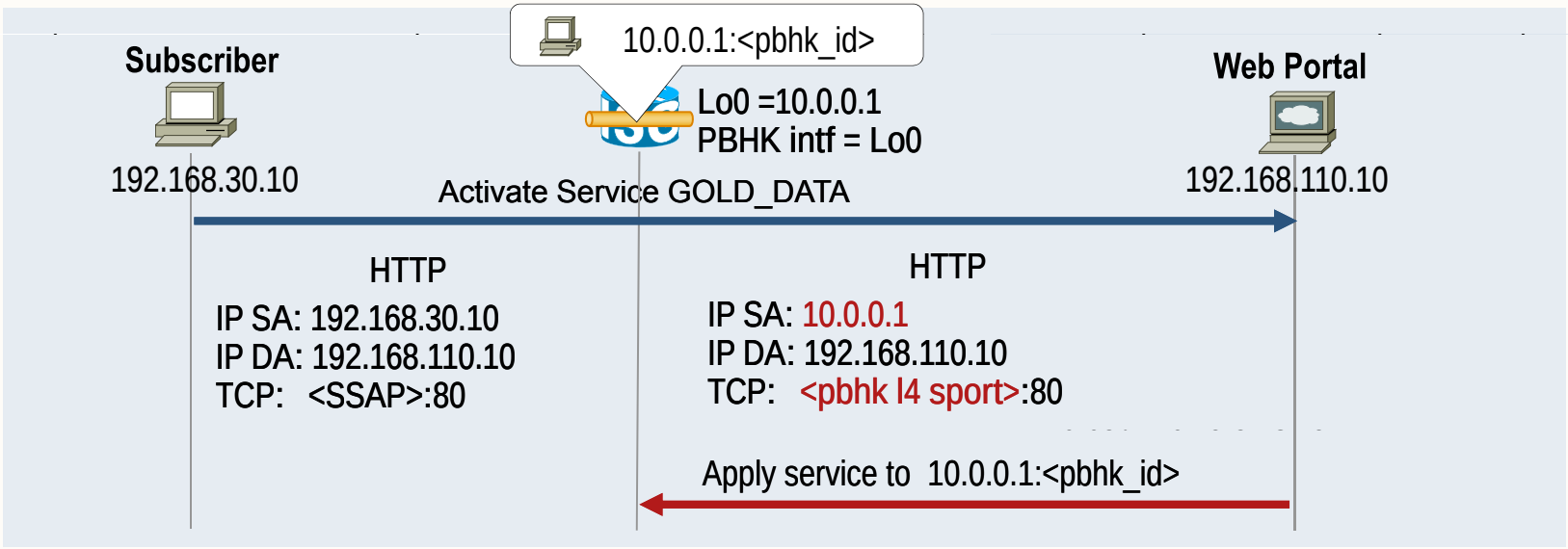
```
aaa accounting network IP_ACCNT_LIST group SERVER_GROUP1
```

Przykładowa konfiguracja (3)

Services

PBHK – Port Bundle Host Key

* Used to generate a host key -> common identifier that ISG & Portal can use to reference a subs. session
  - Extracted by the Portal from packets sourced by subscriber
  - If PBHK - disabled: *host key: IP Source Address (Subscriber IP Address)*
    - enabled: ISG performs a port NAT (PAT) like operation to subscriber packets destined to portal
      host key: ISG IP address + PBHK ID (L4Source Port (12MSBs))



* PBHK Benefits: Support for overlapping host IP addresses
  Subscribers needn't be routable from Portal
  Portal provisioning much simpler

Przykładowa konfiguracja (4)

Services

AAA Server configuration

```
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.

OpenGarden service associated configurations

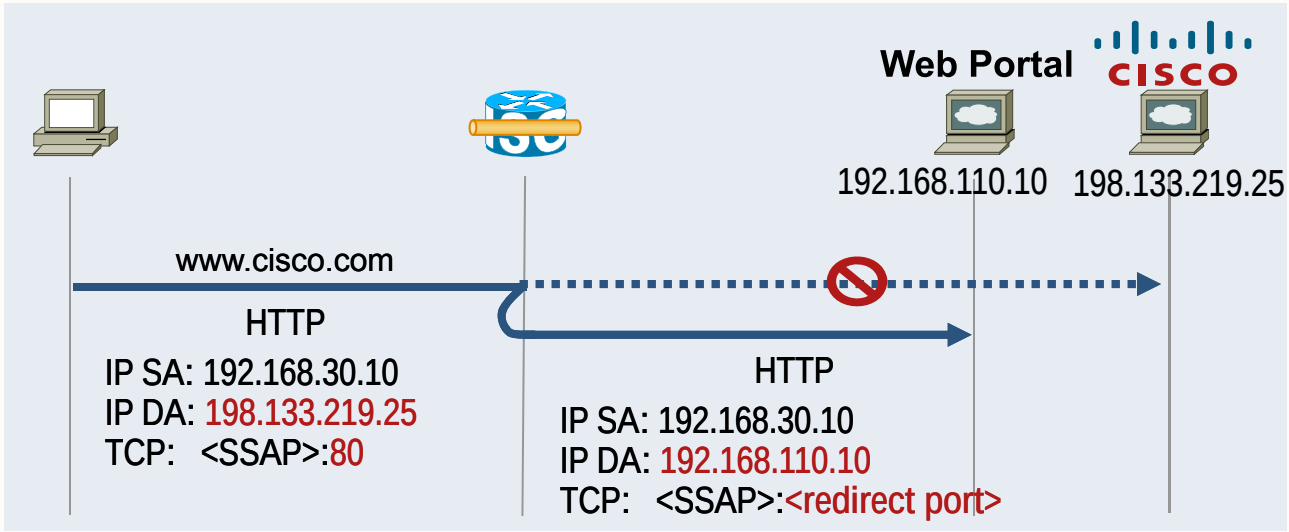
L4R service associated configurations

Cfg required on 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
    permit tcp any any
```

L4 Redirect



- subscriber's traffic, matching a flow description, is redirected to a destination and a L4 port defined on the ISG
- any TCP and UDP traffic can be redirected
- the target server responsible to handle the redirected traffic

Przykładowa konfiguracja (5)

Services

AAA Server configuration

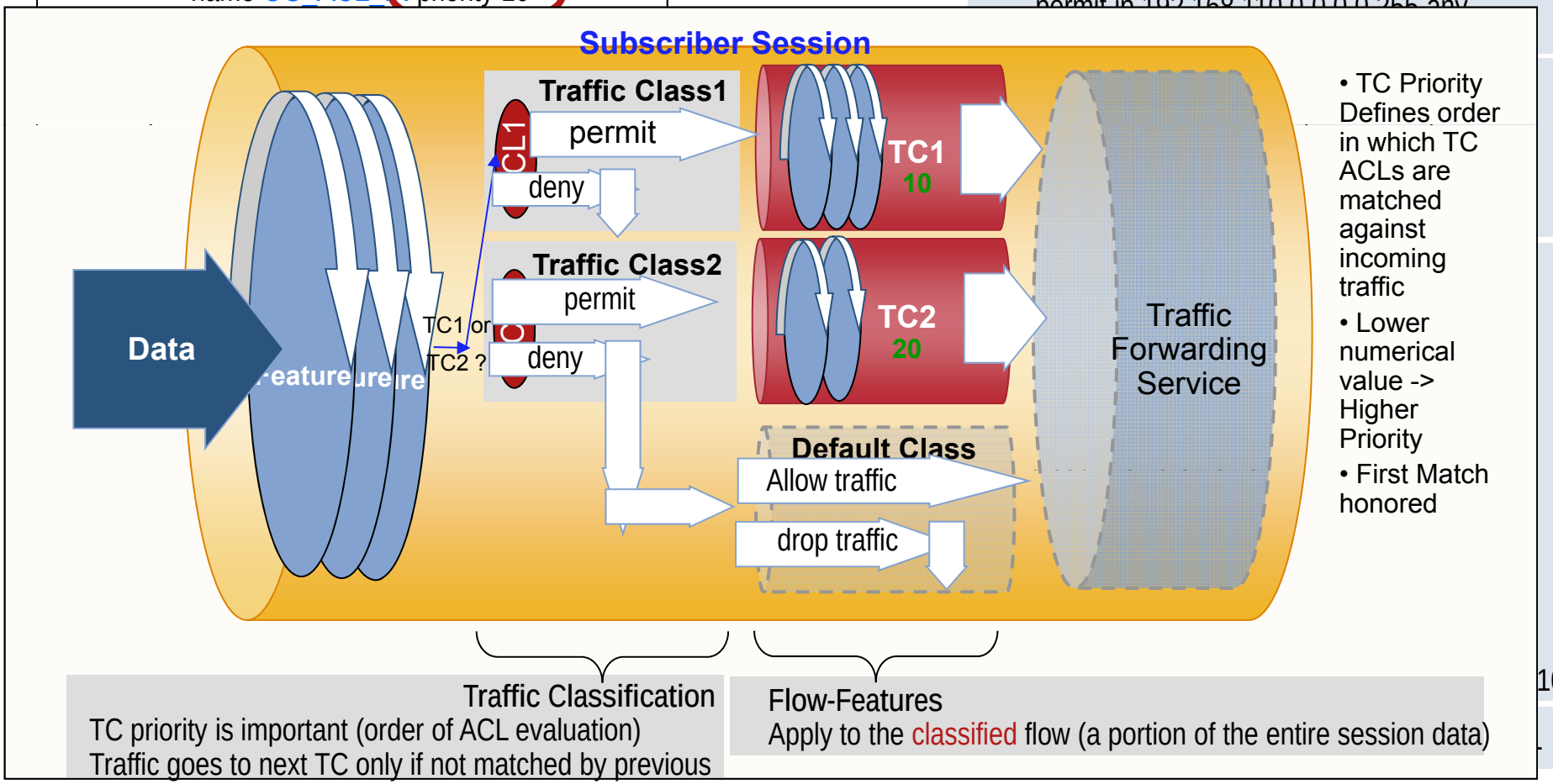
Service-Name = "OG_SRV"
Service Password = "servicecisco"
AVPair: ip:traffic-class=input access-group
name OG_ACL_IN priority 10

II.

OpenGarden service associated configurations

Cfg required on 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
```



Przykładowa konfiguracja (6)

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

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

V. 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 cfg

```
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

Przykładowa konfiguracja (7)

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 cfg

```
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

Rekomendacje – to tylko początek ☺

ASR1K - zalecenia projektowe

1. Pomimo, że karta RP1 pracuje poprawnie przy 24000 sesji nie przekraczaj 16k sesji w przypadku konfiguracji skomplikowanych usług

   Przykładowo, gdy wymagane są usługi ISG i H-QoS zastosuj zamiast karty RP1 kartę RP2...

2. Bądź świadomy, że w dodatkowe usługi wymagają dodatkowej pamięci oraz zasobów procesora.
   Przykładem mogą być usługi zarządzania jak zbieranie statystyk poprzez SNMP.

3. Pamiętaj o ograniczeniach związanymi z kombinacją niektórych komponentów (RP/ESP). Monitoruj zasoby urządzenia regularnie.

   Dla urządzeń z kartą RP1 zwróc uwagę na wykorzystanie zasobów karty RP1. Dla urządzeń z kartąRP2 zwróc uwagę na wykorzystanie zasobów karty ESP (szczególnie w przypadku karty ESP-20)

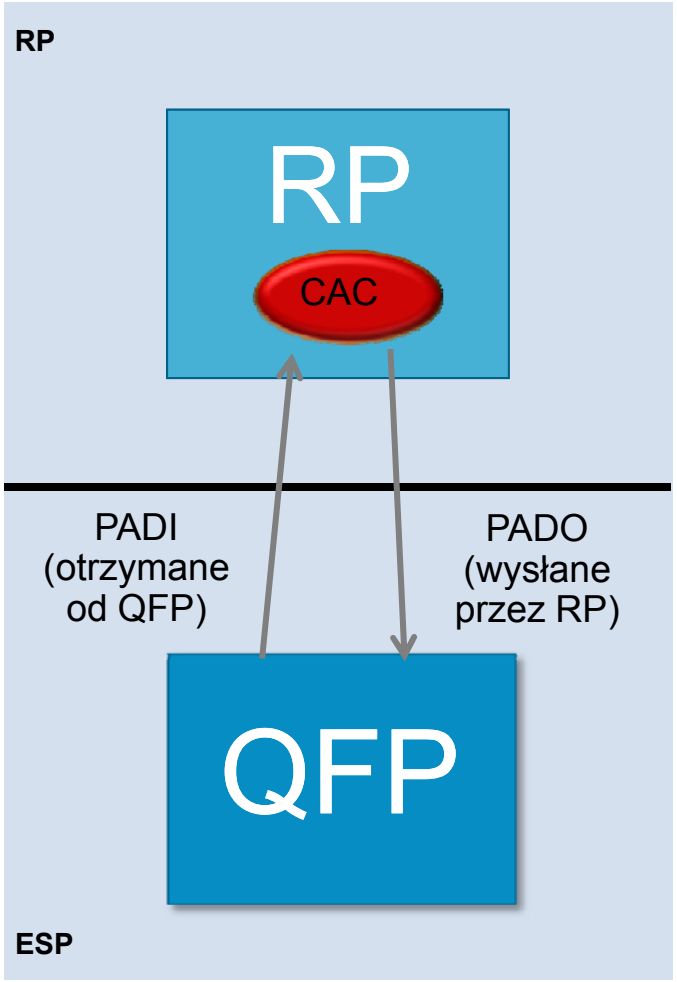
5. Od wersji IOS XE możliwa będzie praca z ilością sesji większą niż 32k. Wymaga to jednak zastosawania kart RP-2 i ESP-40

6. Pamiętaj o stosowaniu 16GB pamięci dla kart RP2 gdy ilość sesji przekracza 32k sesji lub stosowania dual stack IPv4/IPv6...

Zalecane elementy konfiguracji
Usługi szerokopasmowe na routerze ASR1K

Rodzaj konfiguracji	Domyślne ustawienie	Rekomendacja
Call Admission Control	nie skonfigurowane	skonfiguruj , szczegóły na kolejnych slajdach
PPP Keepalives	10 sekund	60 sekund
ograniczenie ilości sesji	nie skonfigurowane	Ustaw następujące limity - globalne ograniczenie ilości sesji - ograniczenie sesji per-VLAN i per-VC (w zależności od twojego otoczenia sieciowego) - ograniczenie sesji „per adres mac” - ograniczenie sesji dla scenariuszy vpdn
Unicast RPF (w trybie „strict mode”) oraz filtrowanie „per-user Access-Lists”	nie skonfigurowane	Uzywaj celem ochrony przed atakami DoS Zmodyfikuj konfigurację interfejsu Virtual-Template (dla wszystkich sesji) lub selektywnie poprzez modyfikację konfiguracji serwera RADIUS
Control Plane Policing	nie skonfigurowane	Skonfiguruj policy tak by ograniczać np. ruch ARP, PPPoE discovery, IP Options, TCP/UDP fragments, ICMP itp.
Monitorowanie zasobów systemu (System Health monitoring)	N/A	Monitor obciążenie CPU oraz zajętość pamięci (CLI, SNMP) . Zwróć uwagę na monitoriawanie zasobów biorących udział w zestawianiu sesji PPP (IOS, RP, ESP)

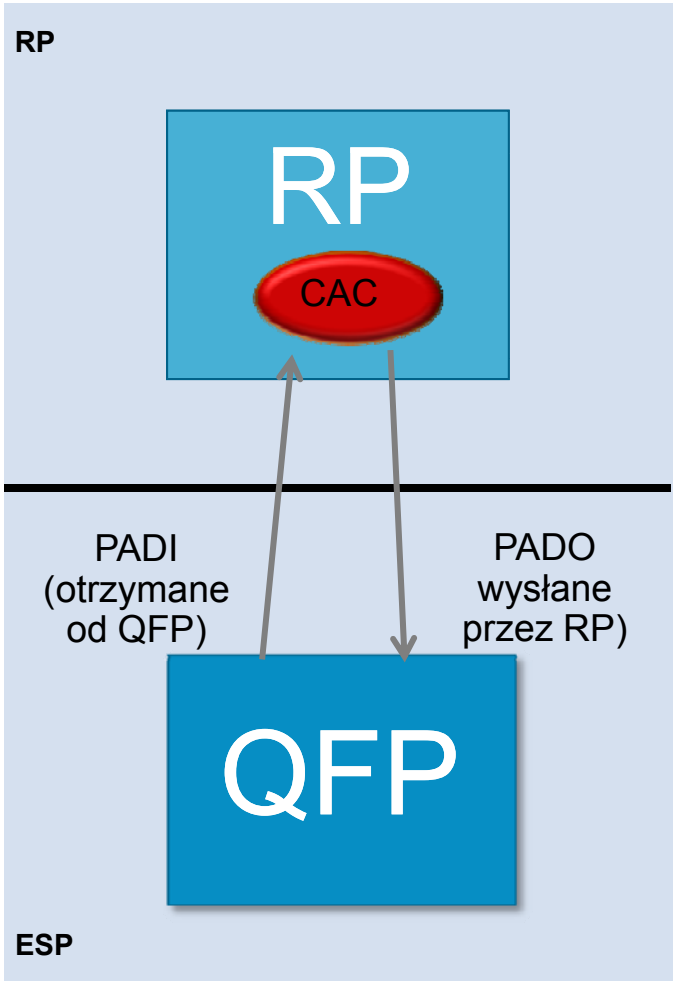
ASR1K Call Admission Control



1. Umożliwia modyfikację szybkości działania BRAS celem dopasawania do możliwości serwera RADIUS
   - Ustawienie maksymalnej akceptowalnej wartości CPS (ang. call per second) umożliwia wyrównanie szybkości działania routera BRAS z wolną infrastrukturą RADIUS)
2. Chroni CPU w sytuacjach gwałtownego wzrostu ilości zestawianych sesji
   - CAC może ochronić IOS CPU przed zbyt dużym obciążeniem, gdy następuje np. usterka interfejsu lub zaburzenia routingu skutkujące masowym ponownym zestawianiem tysięcy sesji PPPoX lub PPP (LAC/LNS)
3. Poprawia współpracę pomiędzy kartami RP i ESP. Komponenty te mają różne maksymalne wartości CPS i CAC je wyrównuje.
4. Przewidywalny czas odtworzenia usługi w przypadku usterki jednego z BRAS (BRAS Clustering)

ASR1K Call Admission Control

Sesje PPPoE



- Dla sesji PPPoE CAC rozpoczyna działanie po otrzymaniu ramki PADI od klienta PPPoE
- Jeżeli CAC zdecyduje, że sesja nie powinna być zestawiona ramka PADO nie jest wysyłana w kierunku klienta PPPoE i zasoby CPU oraz pamięć nie są dodatkowo obciążane.
- CAC działa w oparciu o dwa parametry
  1. aktualne obciążenie sesjami. Sesja nie będzie zestawiona gdy spowoduje ona przekroczenie dopiuszczalnego ustawionego poziomu
  2. aktualna zajętość CPU – jeżeli zajętość CPU jest powyżej ustalonego poziomu nowe połączenia nie będą zestawiane.

```
call admission new-model
call admission limit 1000
call admission cpu-limit 80
call admission pppoe 10 1
```

ASR1K Call Admission Control

Jak należy rozumieć konfigurację wartości CAC ?

```
call admission new-model
call admission limit 1000
call admission cpu-limit 80
call admission pppoe 10 1
```

- Konfigurację zawsze rozpoczynamy od komendy “**new-model**” ...
- W dalszej kolejności określamy **maksymalną wartość zajętości CPU lub obciążenia zestawianymi sesjami**.
- Komenda “**limit**” określa maksymalne obciążenie routera (o tym jak podana wartośc ma się do cps za chwilę ...), od którego następuje ograniczenie w zestawianiu nowych sesji
- “**call admission pppoe 10 1**” określa obciążenie dla pojedynczej sesji PPPoE
  - 10 = obciążenie sesji, 1 = „extended lifetime” (1s + 1s)
  - dla sesji typu oA użyj “call admission pppoa 10 1”
  - dla konfiguracji LNS zastosuj “call admission vpdn 10 1”
  - dla „IP sessions” zastosuj “call admission ip 10 1” … (to jest komendta ukryta)
- W pokazanym przykładzie router będzie akceptował nowe sesje do momentu, gdy CPS nie przekroczy wartośći 50 CPS { 1000 / (10*2) = 50 CPS }
  - Przybliżona wartość **CPS = (Limit) / (Session Charge * Charge Lifetime)**
- **cpu-limit** (tutaj 80) oznacza, że CAC nie będzie akceptował przychodzących sesji gdy 5-cio sekundowe obciążenie CPU będzie na poziomie 80% lub wyżej
- CAC wykorzystuje zajętość CPU procesu IOSd, nie bierze pod uwagę obciążenia karty RP jak również karty ESP.

ASR1K Call Admission Control
Rozważania projektowe

1. Weź pod uwagę kombinację sprzętu (RP/ESP) oraz zastosowaną funkcjonalność (vide kolejne slajdy)
2. Monitoruj przyczyny odmowy zestawiania sesji (zobacz poniższy przykład) by zrozumieć jak często i dlaczego do tego dochodzi ...
3. Weź pod uwagę, że CAC ma zastosowanie jedynie do procesu zestawiania nowych sesji. Terminowanie sesji oraz informacje CoA (ang. change of authorization).
4. W przypadku topologii „PPPoE Server Selection” upewnij się, że CAC został skonfigurowany w każdym urządzeniu zastosowanym w klastrze...

```
ASR1006-2#show call admission statistics
Cac New Model (SRSM) is ACTIVE
Total call Session charges: 0, limit 1000
Total calls rejected 0, accepted 45
Reject reason: CPU-limit: 0 SessionCharges 0
Current actual CPU: 0%, Limit: 80%
Hardware CAC is currently not active
```

Zalecenia CAC dla routera ASR1K

RP1 – 30 cps

```
call admission new-model
call admission limit 600
call admission cpu-limit 65
call admission pppoe 10 1
call admission pppoa 10 1
call admission vpdn 10 1
call admission ip 10 1
```

RP2 – 50 cps

```
call admission new-model
call admission limit 1000
call admission cpu-limit 80
call admission pppoe 10 1
call admission pppoa 10 1
call admission vpdn 10 1
call admission ip 10 1
```

- Zaproponowane wartości zostały podane dla routerów mających karty kontroli RP1 lub RP2 i są oparte o przeprowadzone dotychczas testy
- Zwróć uwagę, że rzeczywista konfiguracji powinna zawierać ustawienia co najmniej dla stosowanych sesji. Pozostałe rodzaje nie muszą pojawiać się w konfiguracji...
- Podane wartości mogą wymagać zmiany w zależności od rzeczywistych warunków pracy urządzenia oraz wykorzystywanych funkcjonalnośći.

Zalecenia CAC dla routera ASR1K

Co robić gdy podane wartości wymagają korekty ?

- Scenariusz #1: CPU limit jest cały czas na wysokim poziomie (vide komenda “show call admission statistics”)
- Scenariusz #2: ESP CPU jest na wysokim poziomie pomimo, że RP CPU jest w dopuszczalnym zakresie pracy
- W obu przypadkach zalecamy obniżenie wartości „limit”. Odradzamy zmianę wartości określającej obciążenie pojedynczą sesją...

```
call admission new-model
call admission limit 600
call admission cpu-limit 65
call admission pppoe 10 1
call admission pppoa 10 1
call admission vpdn 10 1
call admission ip 10 1
```



```
call admission new-model
call admission limit 500
call admission cpu-limit 65
call admission pppoe 10 1
call admission pppoa 10 1
call admission vpdn 10 1
call admission ip 10 1
```

ASR1K - zalecenia konfiguracyjne
RADIUS oraz interface Virtual-Template

Typowy atrybut **lcp:interface-config** był często używany w profilach użytkownika skonfigurowanych na serwerze RADIUS.
Skutkuje to utworzeniem pełnego interfejsu VAI („full" virtual access interface) w odróżnieniu od dużo bardziej efektywniej wykorzystującego zasoby (co skutkuje większą skalowalnością) subinterfejsu VAI.

ASR1K nie wspiera „full VAI" (w odróznieniu od routerów C10K/72xx)

Metoda postępowania w takiej sytuacji
- skonwertuj stosowane parametry RADIUS do Cisco VSA (zobacz listę parametrów tutaj) ISG Radius CoA Interface Guide: Attribute Definitions
- jeżeli z jakiegoś powodu „full interface" VAI musi być utworzony zastosuj komendę „***aaa policy interface-config allow subinterface***"
- opcjonalnie zrób to poprzez profil użytkownika na serwerze RADIUS ***cisco-avpair="lcp:interface-config allow-subinterface=yes***"

By sprawdzić, czy dana funkcjonalność (skonfigurowana poprzez interface virtual-template) skutkuje utworzeniem „pełnego interfejsu" VAI użyj następującej komendy

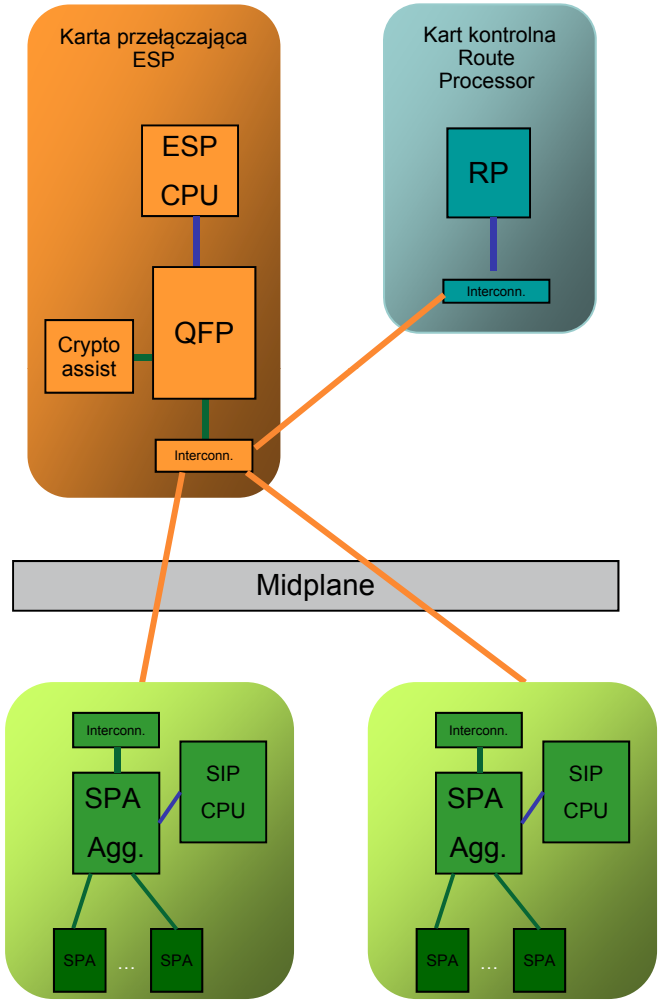
```
ASR1006-2#test virtual-Template 1 subinterface
Subinterfaces may be created using Virtual-Template1
```

ASR1K – monitorowanie zasobów systemowych

- Zwykle administratorzy i operatorzy monitorujący urządzenia sprawdzają zajętość CPU korzystając z komendy “show process cpu” . W przypadku routera ASR1000 oznacza to tylko monitorowanie dla procesu IOS CPU.

- Zalecane jest monitorowanie obciążenia CPU oraz zajętości pamięci dla następujących elementów urządzenia:
  - karta RP - CPU oraz zajętość pamięci
  - karta ESP – CPU, zajętość pamięci, obciążenie QFP

- W praktyce wykonywane jest to poprzez odpytywanie odpowiednich gałęzi MIB
  - CISCO-PROCESS-MIB
  - CISCO-ENTITY-QFP-MIB



ASR1K MIB Specifications Guide

ASR1K – monitorowanie zasobów systemowych

```
ASR1006-2#show platform software status control-processor brief
Load Average
 Slot   Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.00   0.00   0.00
 ESP0 Healthy   0.00   0.01   0.00
 ESP1 Healthy   0.00   0.00   0.00
 SIP0 Healthy   0.00   0.00   0.00
 SIP1 Healthy   0.08   0.02   0.01

Memory (kB)
 Slot   Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  8067464  2266824 (28%)  5800640 (19%)   5365812 (13%)
 ESP0 Healthy  3877064   637920 (16%)  3239144 (84%)   3003240 (77%)
 ESP1 Healthy  3877064   636300 (16%)  3240764 (84%)   3002824 (77%)
 SIP0 Healthy   449784   290728 (65%)   159056 (35%)    256828 (57%)
 SIP1 Healthy   449784   321044 (71%)   128740 (29%)    312280 (69%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   0.09   0.09   0.00  99.70   0.00   0.09   0.00
         1   0.10   0.90   0.00  98.89   0.00   0.10   0.00
 ESP0    0   1.20   3.00   0.00  95.80   0.00   0.00   0.00
 ESP1    0   0.10   0.20   0.00  99.70   0.00   0.00   0.00
 SIP0    0   0.40   0.40   0.00  99.19   0.00   0.00   0.00
 SIP1    0   2.20   3.00   0.00  94.70   0.00   0.10   0.00
```

- Kluczowe parametry wymagające monitorowania przy wdrożeniach typu BB/ISG:
  1. RP/ESP **Load Averages**
  2. **Committed Memory**
  3. RP/ESP **CPU Utilization**

Informacje te dostępne są również poprzez zapytanie SNMP.

Podsumowanie