Cisco Expo 2009

conf t:Intelligent Services Gateway (ISG)

Đorđe Vulovic, Systems Engineer, CCIE #16582

Cisco Expo 2009

conf t:ISG

Uvod

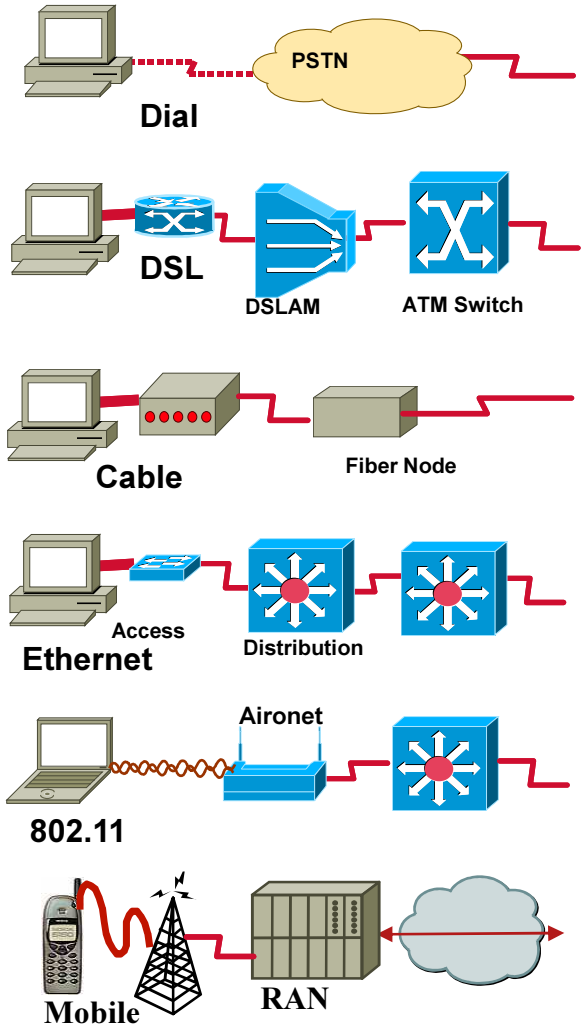
Intelligent Services Gateway (ISG)

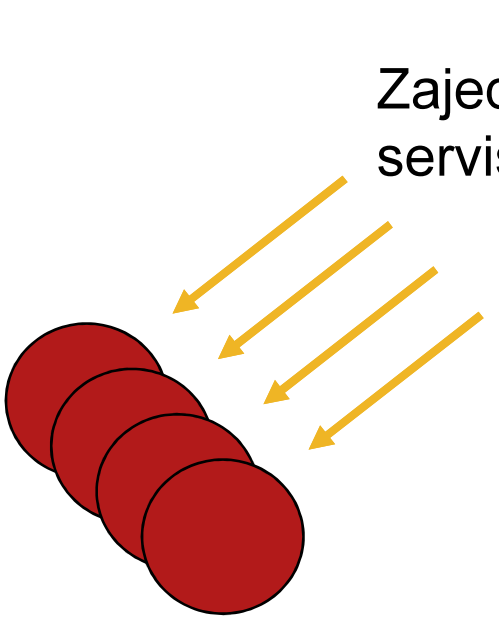
- Funkcionalnost IOS-a koja upravlja korisničkim sesijama:
  - Identifikacija korisnika
  - Određivanje servisa i polise za korisnika
  - Izvršavanje polise na korisničkom saobraćaju
  - Upravljanje životnim vekom sesije
  - Izveštavanje o korišćenju servisa
  - Nadzor statusa sesija
  - Dinamička aktivacija servisa kroz otvorene interfejse
- Dostupan na sledećim platformama/softverskim verzijama (različite platforme mogu imati različit skup implementiranih ISG funkcionalnosti):
  - Cisco 7200/7300 (12.2SB)
  - Cisco 10000 (12.2SB)
  - Cisco ASR 1000
  - Cisco 7600 (12.2SR)

Ključne ISG funkcionalnosti

Service Selection / Self-Care	Reduced CAPEX and OPEX with an integrated edge for MPLS and Broadband Aggregation with Service Selection
Flexible Accounting	Per session and per service accounting, QoS Accounting, Pre-paid (volume), Pre-paid (Time-Based), Tariff-Switching (Pre-Paid and Post-paid)
Authentication / Authorization	L4 redirect for Web-Based Authentication, Transparent Auto Logon, PPP Authentication, RADIUS Proxy for EAP Authentication
Dynamic Policy Push	Policies for session bandwidth, security and accounting that can be pushed dynamically in real time while session is still active – using standardized protocols (e.g. RADIUS, RFC3576 CoA)
Flexible Session Type	PPP and IP-Sessions - using different session initiators; access protocol agnostic
Policy based rules – "Control Policy"	Event triggered conditional actions: Association of actions based on events
"Domain Switching" MPLS integration – VRF-Switching	Map user to VRF Dynamic VPN Selection
Multidimensional Identity	Policy determination based on all aspects of subscriber identity
Timeouts	Idle Timeout, Session Timeouts
Conditional debugging	Debugging based on any subscriber, service or any other identifier

Abstrakcija pristupne tehnologije

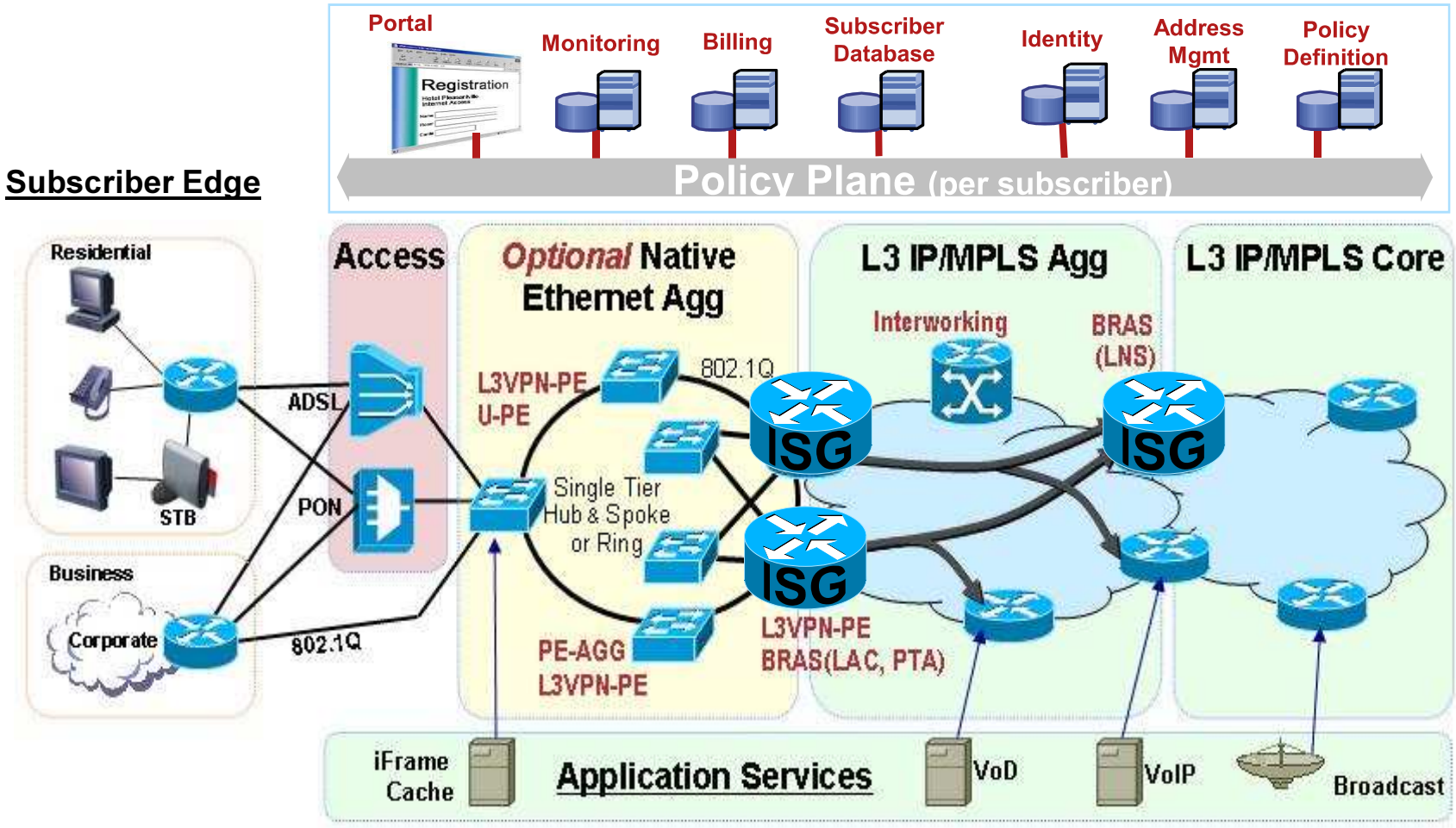




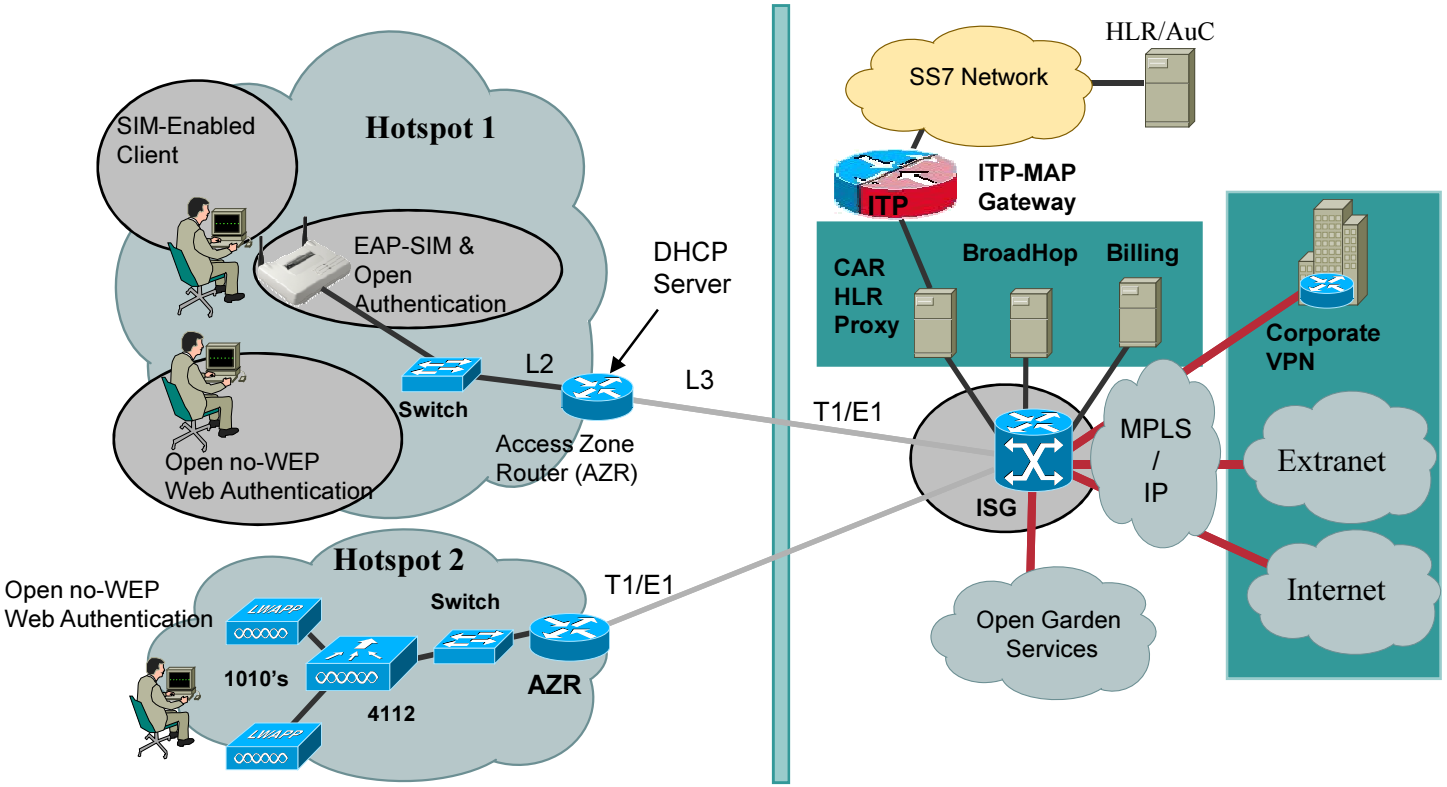
Zajednički servisi

Zajednički tipovi korisničkih sesija

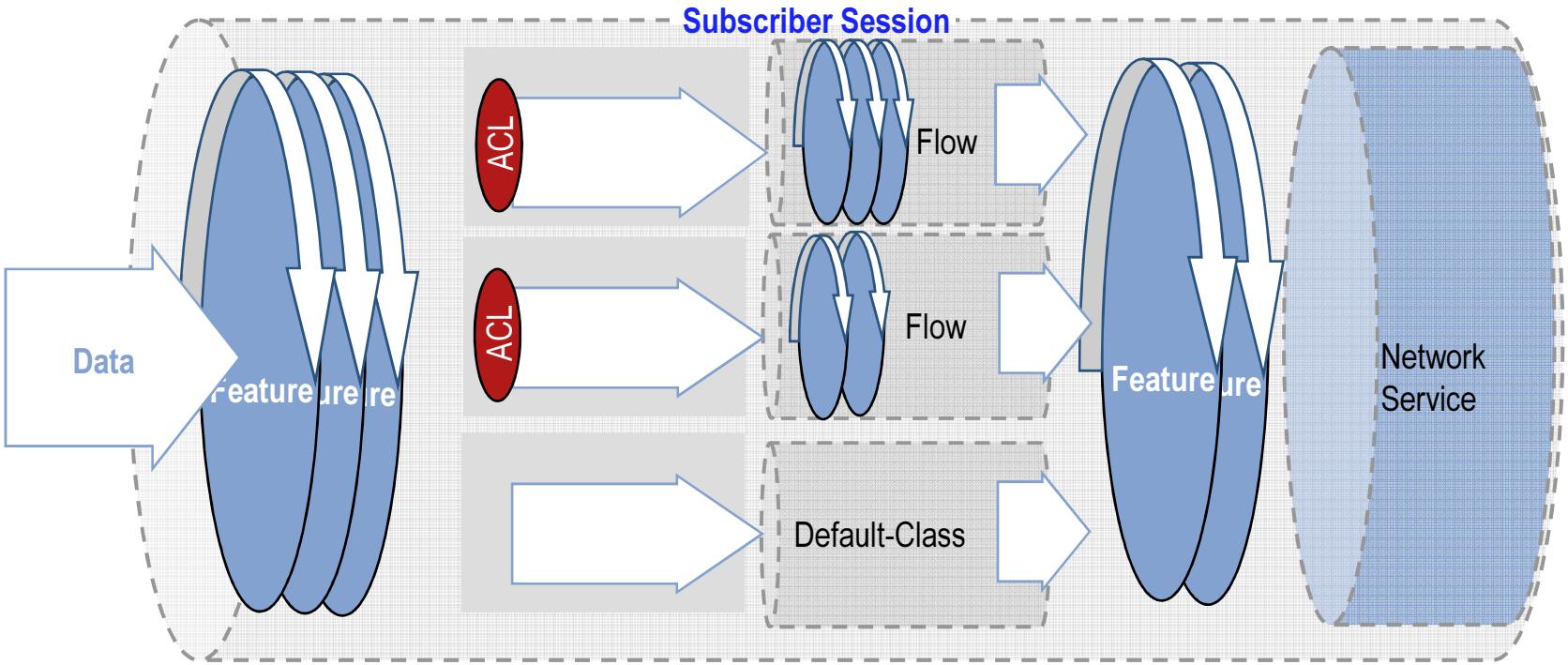
Primer korišćenje ISG-a: Wireline



Primer korišćenje ISG-a: Public WLAN



Funkcionisanje ISG-a



Session-Features:
Apply to the entire session
e.g. per-session-ACL, Policing, MQC, Accounting

Traffic Classification
(using traffic classes: class-map type traffic)

Flow-Features:
Apply to the classified flow
(a portion of the entire session data)

Session-Features:
Apply to the entire session
e.g. PBHK

Network Service:
Forwarding (at L2, e.g. L2TP) or
Routing (L3, e.g. connection to a VRF)
Mutually exclusive

Cisco Expo 2009

conf t:ISG

Kontrola pristupa korisnika

PPP sesija

- Sesija koja obuhvata saobraćaj sa jedne PPP konekcije
- Detekcija početka i kraja sesije se vrši pomoću poruka iz samog PPP protokola

IP sesija (1)

- Sesija koja obuhvata saobraćaj prema/od jedne IP ili MAC adrese
- Sesija može biti *L2-connected* ili *Routed*:
  - Kod *L2-connected* sesije korisnik i ISG imaju L2 vezu
  - Kod *Routed* sesije korisnik i ISG imaju L3 vezu
- Sesija se detektuje na jedan od sledećih načina:
  - Bez kontrolnih protokola:
    - ISG na osnovu korisničkih paketa uspostavlja/raskida sesiju
  - Pomoću kontrolnih protokola:
    - DHCP (ISG je DHCP server ili DHCP Relay)
    - Radius (ISG je Radius Proxy)
    - Saobraćaj sa nepoznate IP/MAC adrese se odbacuje!
  - Moguće je aktivirati više načina odjednom

IP sesija (2)

- Događaji za detekciju početka sesije (*First Sign Of Life* – FSOL):
  - Paket sa do tada neprepoznatom izvorišnom IP/MAC adresom
  - DHCP *Discover* paket
  - Radius *Access-Request* paket
- Detekcija kraja sesije:
  - DHCP *Release* zahtev od klijenta
  - Istek dodeljene DHCP adrese (*lease expiry*)
  - Radius *Accounting-Stop* paket

Konfiguracija *L2-connected* IP sesije

FSOL=DHCP DISCOVER

```
interface GigabitEthernet0/1.401
  ip subscriber l2-connected
    initiator dhcp class-aware
```

FSOL=UNKNOWN MAC

```
interface GigabitEthernet0/1.401
  ip subscriber l2-connected
    initiator unclassified mac-address
```

FSOL=RADIUS ACCESS REQUEST

```
interface GigabitEthernet0/1.401
  ip subscriber l2-connected
    initiator radius-proxy
```


Konfiguracija *Routed* IP sesije

FSOL=DHCP DISCOVER

```
interface GigabitEthernet0/1.401
  ip subscriber routed
    initiator dhcp class-aware
```

FSOL=UNKNOWN MAC

```
interface GigabitEthernet0/1.401
  ip subscriber routed
    initiator unclassified ip-address
```

ISG mora biti DHCP Server

FSOL=RADIUS ACCESS REQUEST

```
interface GigabitEthernet0/1.401
  ip subscriber routed
    initiator radius-proxy
```


Cisco Expo 2009

conf t:ISG

Interfejs prema AAA serveru

Radius poruke u ISG-u (1)

- *Access Request* poruke se koriste za:
  - Autentifikaciju i autorizaciju sesije
  - Autentifikaciju i autorizaciju servisa
  - Zahtev za učitavanje servisa sa AAA servera
  - Re-autorizacija za *prepaid* korisnike
- *Access Accept* poruke se koriste za:
  - Notifikaciju uspešne autentifikacije
  - Učitavanje korisničkog profila i pridruženih servisa
  - Učitavanje servisa
  - Kvote za *prepaid* korisnike
- *Access Reject* poruke se koriste za:
  - Notifikaciju neuspešne autentifikacije

Radius poruke u ISG-u (2)

- *Accounting Request Start* poruke se koriste za:
  - Početak sesije
  - Početak servisa
- *Accounting Request Stop* poruke se koriste za:
  - Završetak sesije
  - Istek servisa
- *Accounting Request Interim* poruke se koriste za:
  - Ažuriranje brojača sesije za prethodni vremenski interval

CoA/PoD poruke u ISG-u

- *Change of Authorization* (CoA) poruka

  CoA poruke se koriste za dinamičku promenu parametara sesije:

  Logovanje korisnika (Account Logon)

  Izlogovanje korisnika (Account Logoff)

  Upit za parametar sesije (Session Query)

  Aktiviranje servisa (Service Activate)

  Deaktiviranje servisa (Service De-activate)

- *Packet of Disconnect* (PoD) poruka

  PoD poruke se koriste za terminaciju PPP sesija

Konfiguracija AAA servera (1)

Definicija AAA servera

```
aaa new-model
!
aaa group server radius <server-group>
   <ip-address> auth-port <port> acct-port <port>
!
aaa authentication login default none
aaa authentication login <auth-list> group <server-group>
!
aaa authorization network <author-list> group <server-group>
aaa authorization network default group <server-group>
aaa authorization subscriber-service default local group <server-group>
!
aaa accounting update periodic 5
aaa accounting network <acct-list> start-stop group <server-group>
!
aaa session-id common
!
ip radius source-interface <loopback-interface>
!
radius-server host <ip-address> auth-port <port> acct-port <port> <key>
```

Tipični portovi su 1812 i 1813

Konfiguracija AAA servera (2)

Tipična Definicija Radius atributa koji se šalju u *Access Request* i *Accounting Start* porukama

```
radius-server attribute 44 include-in-access-req
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 include-in-acct-req
radius-server attribute 55 access-request include
```

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

Slanje VSA Radius atributa

```
radius-server vsa send accounting
radius-server vsa send authentication
```

Cisco Expo 2009

conf t:ISG

Servisi i AAA servisni profili

Funkcionalnosti, servisi i servisni profili

- Funkcionalnost je komponenta ISG softvera koja vrši specifičnu operaciju na korisničkom saobraćaju:
  - Može biti primenjena na celokupnu sesiju ili na na saobraćaj koji je definisan klasifikatorom saobraćaja
- Servis je skup funkcionalnosti koje se primenjuju na sesiju:
  - Može se startovati automatski po uspostavljanju sesije ili naknadno
- Servisni profil je način definisanja servisa:
  - Lokalno na ISG-u
  - Udaljeno na AAA serveru

Najčešće ISG funkcionalnosti

- *PBHK (Port Bundle Host key)*
- *L4 Redirect*
- *QoS*
- *Idle-Timeout*
- *Session-Timeout*
- *Accounting*
- *Per-session Filter*
- *Prepiad*

Konfiguracija klasifikatora saobraćaja

Definicija klasifikatora saobraćaja

```
class-map type traffic match-any <class-map-name>
   match access-group input <in-acl-name>
   match access-group output <out-acl-name>
```

Lokalna konfiguracija servisnog profila

Definicija servisa na nivou sesije

```
policy-map type service <policy-map-name>
  <session-feature>
```

Definicija servisa na nivou dela saobraćaja

U slučaju da paket zadovoljova više klasifikatora uzima se onaj sa najvišim prioritetom

```
policy-map type service <policy-map-name>
  [<priority>] class type traffic <class-map-name>
     <traffic-class-feature>
```

Konfiguracija servisnog profila na AAA serveru

- Servisni profil se čuva na AAA serveru kao skup Radius atributa:
  - Svaka funkcinalnost se opisuje sa jednim ili više atributa:
    - Cisco-AV-Pair
    - Cisco-Service-Info
    - Cisco-Account-Info
  - Za učitavanje servisnog profila neophodno je definisani lozinku

Definicija lozinke za učitavanje servisnog profila

```
Subscriber service password <password>
```

Primer servisnog profila

Na AAA serveru

```
Service-Name = "DEFAULT_BW_SERVICE"
Service Password = "servicecisco"
AVPair: ip:traffic-class=input access-group name ACL_IN_DEF_BW priority 20
AVPair: ip:traffic-class=output access-group name ACL_OUT_DEF_BW priority 20
AVPair: subscriber:accounting-list=ACCNT_LIST1
Service INFO: QU;512000;256000;5000
Service INFO: QD;512000;256000;5000
```

Na ISG-u

```
class-map type traffic match-any TC_DEF_BW
 match access-group output name ACL_OUT_DEF_BW
 match access-group input name ACL_IN_DEF_BW
!
policy-map type service DEFAULT_BW_SERVICE
 20 class type traffic TC_DEF_BW
        accounting aaa list ACCNT_LIST1
        police input 512000 256000 5000
        police output 512000 256000 5000
```


Aktiviranje servisnog profila

Iz ISG polise

```
policy-map type control <policy-map-name>
  class type control always event session-start
    10 service-policy type service name <service-name>
```

Iz korisničkog profila

```
Radius Attribute 1: User-Name = <username>
Radius Attribute 28: Idle-timeout = <value> secs
Cisco Account-Info: A<service-name>
```


conf t:ISG

Korak 5: ISG polisa

ISG polisa

- ISG polisa definiše ponašanje ISG sistema u slučaju određenih događaja u toku sesije
- ISG polisa se sastoji od niza pravila:
  - Pravilo se definiše za jedan tip događaja i sadrži niz akcija koje se vrše kada događaj nastupi
    - Ukoliko je akcija `authorize`, sledeća pravila u nizu se izvršavaju samo ako akcija nije uspela tj. korisnik nije autorizovan
  - Pravilo se može izvršavati ili bezuslovno (*always*) ili ukoliko je zadovoljen uslov iz kontrolnog klasifikatora

Događaji u ISG polisi

- session-start
- session-default-service
- session-restart
- session-service-found
- service-start
- service-stop
- account-logon
- account-logoff
- timed-policy-expiry
- credit-exhausted
- quota-depleted

Akcije u ISG polisi (1)

- `authenticate aaa list <list-name>`

  Autentifikuje korisnika prema AAA listi za autentifikaciju <list-name>

- `authorize [aaa list <list-name>] [password <password>] [upon network-service-found {continue | stop}] identifier <identifier>`

  Autorizuje korisnika prema AAA listi za autorizaciju <list-name> prema zadatom tipu identifikatora

Akcije u ISG polisi (2)

- `service-policy type service [unapply] [aaa list <list-name> service] {name <service-name> | identifier <identifier>}`

  Aktivira ISG servis sa zadatim nazivom ili sa nazivom dobijenim od vrednosti zadatog tipa identifikatora

- `set-timer <name-of-timer> <minutes>`

  Startuje navedeni tajmer u okviru polise; istek tajmera generiše `timed-policy-expiry` događaj

Konfiguracija kontrolnog klasifikatora

Definicija kontrolnog klasifikatora

```
class-map type control [match-all | match-any | match-none]
<control-class-name>
   <condition>
```

- Primer uslova u kontrolnom klasifikatoru:

```
match authen-status {authenticated |
unauthenticated}

match authenticated-username {<username> |
regexp <regular-expression>

match service-name {<service-name> | regexp
<regular-expression>}

match source-ip-address <ip-address> <subnet-
mask>

match timer {<timer-name> | regexp <regular-
expression>}
```

Konfiguracija ISG polise

Definicija polise

<action-number> je broj od 1 do 254

```
policy-map type control <policy-map-name>
 class type control {<control-class-name> | always} <event>
  <action-number> <action>
```

Primena polise na (pod)interfejs

```
interface GigabitEthernet0/1.401
  service-policy type control < policy-map-name>
```

conf t:ISG

Funkcionalnost redirekcije prema portal serveru

Redirekcija prema portal serveru (1)

- Ukoliko je korisnik neautentifikovan, prva HTTP sesija korisnika se preusmerava na portal server
- Korisnik unosi korisničko ime i lozinku na portal server
- Portal server pomoću Account-Logon CoA poruke obaveštava ISG o unetim podacima
- ISG pokušava da autentifikuje korisnika na AAA serveru i rezultat autentifikacije javlja portal serveru

Redirekcija prema portal serveru (2)

- Tipovi redirekcije:
  - Permanentna redirekcija
  - Inicijalna redirekcija
  - Periodična redirekcija
- Redirekcija se vrši samo za TCP i UDP saobraćaj
- Aktivira se kao poseban servis u ISG polisi

Konfiguracija servisa za redirekciju (1)

Definicija funkcionalnosti za redirekciju na AAA serveru

```
Cisco-Avpair (26,9,1) = "ip:l4redirect=redirect to {group
<server-group-name> | ip <ip-address> [port <port-number>]}
[duration <seconds>] [frequency <seconds>]"
Cisco-Avpair (26,9,1) = "ip:traffic-class=in access-group
name <in-acl-name> priority <priority>"
```

<in-acl-name> definiše saobraćaj od korisnika prema za koji se vrši redirekcija; to ne sme biti saobraćaj prema portal serveru

Primer ISG polise

```
policy-map type control EXAMPLE
 class type control always event session-start
  1 service-policy type service L4REDIRECT-SVC
```

Konfiguracija servisa za redirekciju (2)

Definicija servisa za redirekciju na ISG-u

```
class-map type traffic match-any <class-map-name>
   match access-group input <in-acl-name>
   match access-group output <out-acl-name>
!
policy-map type service <policy-map-name>
 [<priority>] class type traffic <class-map-name>
   redirect to {group <server-group-name> | ip <ip-address>
   [port <port-number>]} [duration <seconds>] [frequency
   <seconds>]
```

Primer ISG polise

```
policy-map type control EXAMPLE
 class type control L4REDIRECT-CLASS event session-start
  1 service-policy type service L4REDIRECT-SVC
```

Konfiguracija servisa za redirekciju (3)

Definicija portal servera

```
redirect server-group <group-name>
   server ip <ip-address> port <port-number>
```

Definicija AAA interfejsa prema portal serveru

```
aaa server radius dynamic-author
   client {name | ip-address} [vrf vrf-id]
   port port-number
   server-key <key>
   auth-type {all | any | session-key}
   ignore {server-key | session-key}
```

Potrebno samo ako portal server nije ujedno i AAA server

Pre 12.2(31)SB2 neophodan je "`ignore server-key`"

“Open Garden”

- “Open Garden” predstavlja mogućnost pristupa određenim adresama (npr. sajtu provajdera) i od strane neautentifikovanih korisnika
- Aktivira se kao poseban servis u ISG polisi
  - Obavezno pre servisa za redirekciju na portal server

Konfiguracija *"Open Garden"* servisa (1)

Definicija *"Open Garden"* servisa na AAA serveru

```
Cisco-Avpair (26,9,1) = "ip:traffic-class=in access-group
name <in-acl-name> priority 10"
Cisco-Avpair (26,9,1) = "ip:traffic-class=in default drop"
Cisco-Avpair (26,9,1) = "ip:traffic-class=out access-group
name <out-acl-name> priority 10"
Cisco-Avpair (26,9,1) = "ip:traffic-class=out default drop"
```

<in-acl-name> definiše saobraćaj od korisnika prema "Open Garden"-u

<out-acl-name> definiše saobraćaj od "Open Garden"-a prema korisnicima

Primer ISG polise

```
policy-map type control EXAMPLE
 class type control always event session-start
  1 service-policy type service OPENGARDEN-SVC
```

Konfiguracija *"Open Garden"* servisa (2)

Definicija *"Open Garden"* servisa na ISG-u

```
class-map type traffic match-any <class-map-name>
   match access-group input <in-acl-name>
   match access-group output <out-acl-name>
!
policy-map type service <policy-map-name>
  [<priority>] class type traffic <class-map-name>
```

Primer ISG polise

```
policy-map type control EXAMPLE
 class type control OPENGARDEN-CLASS event session-start
  1 service-policy type service OPENGARDEN-SVC
```

Identifikacija sesije na portal serveru

- Korisnička IP adresa (IP Host Key – IPHK)
  - Default metod
- ISG IP adresa + ISG-dodeljeni port (Port Bundle Host Key – PBHK)
  - ISG vrši PAT translaciju HTTP saobraćaja između korisnika i portal servera
  - Prednosti:
    - Podrška za preklapajuće adrese u slučaju više VRF-ova
    - Korisnik ne mora imati L3 vezu sa portalom
    - U portal server ne moraju da se unose korisničke IP adrese
  - Aktivira se kao poseban servis u ISG polisi

Konfiguracija PBHK servisa (1)

Definicija PBHK servisa na AAA serveru

```
Cisco-Avpair (26,9,1) = "ip:portbundle=enable"
```

Definicija PBHK servisa na ISG-u

```
policy-map type service <policy-map-name>
 ip portbundle
```

Primer ISG polise

```
policy-map type control EXAMPLE
 class type control always event session-start
  1 service-policy type service PBHK-SVC
```

Konfiguracija PBHK servisa (2)

Definicija PBHK parametara

```
ip portbundle
   match access-list <access-list-number>
   length <bits>
   source <interface>
```

<access-list-number> tipično specificira pakete prema portal serveru

Interfejs u čiju adresu se PAT-uje saobraćaj je tipično Loopback

Primena PBHK translacije na (pod)interfejs

```
interface GigabitEthernet0/2.501
  ip portbundle outside
```

Interfejs prema portal serveru

conf t:ISG

QoS funkcionalnosti

QoS funkcionalnosti

- Session-based/Flow-Based *policing*

  Ograničavanje saobraćaja u *uplink* i/ili *downlink* smeru po sesiji ili delu saobraćaja određenim klasifikatorom saobraćaja

- Per-session QoS

  Primena MQC polise na korisničku sesiju u *uplink* i/ili *downlink* smeru

Konfiguracija *policing* servisa

Definicija *policing* servisa na nivou sesije na AAA serveru

```
Cisco-Avpair (26,9,251) = "QU;<committed-rate>;<normal-
burst>;<excess-burst>;D;<committed-rate>;<normal-
burst>;<excess-burst>"
```

Definicija *policing* servisa na nivou sesije na ISG-u

```
policy-map type service <policy-map-name>
  police input <committed-rate> <normal-burst> <excess-burst>
  police output <committed-rate> <normal-burst> <excess-burst>
```

Konfiguracija *per-session QoS* servisa

Definicija *per-session* QoS servisa na AAA serveru

```
Cisco-Avpair (26,9,1) = "ip:sub-qos-policy-in=<policy name>"
Cisco-Avpair (26,9,1) = "ip:sub-qos-policy-out=<policy name>"
```

Definicija *per-session* QoS servisa na nivou sesije na ISG-u

```
policy-map type service <policy-map-name>
  service-policy input <policy-map-name>
  service-policy output policy-map-name>
```

conf t:ISG

Prepaid funkcionalnost

Prepaid funkcionalnost

- *Prepaid* funkcionalnost omogućava korišćenje servisa od strane korisnika samo ukoliko postoji dostupan kredit
  - Kredit može biti izražen kao saobraćaj (u bajtovima) ili vreme (u sekundama)
- Kredit se administrira od strane biling servera:
  - ISG od biling servera dobija deo kredita u obliku kvote
  - ISG prati korišćenje servisa i smanjuje kvotu
  - Kada kvota padne na definisani limit, ISG od biling servera traži reautorizaciju
  - Ako je reautorizacija uspešna, biling server daje ISG-u novu kvotu
  - Ako je reautorizacija neuspešna, ISG prekida sesiju ili vrši drugu definisanu akciju
- Za komunikaciju između ISG-a i biling servera koristi se Radius protokol

Konfiguracija *prepaid* servisa (1)

Definicija *prepaid* servisa na AAA serveru

```
Cisco-Avpair (26,9,1) = "ip:traffic-class=in access-group
name <in-acl-name> priority 10“
Cisco-Avpair (26,9,1) = "prepaid-config={<name-of-config> |
default"
```

Moguće je koristiti i OUT ACL

Definicija *prepaid* servisa na ISG-u

```
class-map type traffic match-any <class-map-name>
   match access-group input <in-acl-name>
!
policy-map type service <policy-map-name>
  [<priority>] class type traffic <class-map-name>
     prepaid config <name-of-config>
```

Konfiguracija *prepaid* servisa (2)

Definicija *prepaid* parametara

```
subscriber feature prepaid {<name-of-config> | default}
  interim-interval <number-of-minutes>
  method-list {accounting | authorization} <name-of-list>
  password <password>
  threshold {time <seconds> | volume {kilobytes <Kbytes> |
  megabytes <Mbytes> | bytes <bytes>}}
```

`credit-exhausted` i `quota-depleted` događaji

- `credit-exhausted` događaj se dešava kad biling server vrati kvotu 0 tj. kada je korisnik ostao bez kredita

  Tipično, akcija na ovaj događaj je aktiviranje servisa za redirekciju na portal za dopunu kredita

- `quota-depleted` događaj se dešava kada ISG-u istekne kvota za korisnika pri čemu još čeka na odgovor na reautorizaciju:

  U polisi se definiše se da li se korisnički saobraćaj prosleđuje ili odbacuje

ISG dokumentacija na CCO

- Cisco IOS Intelligent Service Gateway Configuration Guide, Release 12.2 SB (http://www.cisco.com/en/US/docs/ios/12_2sb/isg/configuration/guide/isg_c.html)
- Cisco IOS ISG RADIUS CoA Interface Guide, Release 12.2 SB (http://www.cisco.com/en/US/docs/ios/12_2sb/isg/coa/guide/isg_ig.html)

Cisco Networkers
25-28. januar 2010.
Barselona
Registrujte se