Contents

Introduction

This example provides a sample configuration of Cisco Intelligent Services Gateway (ISG) deployed in a service provider's broadband network that is delivering triple-play services to subscribers through DSL, Ethernet, and WiMAX access.

Design

DSL, Ethernet and Fixed WiMAX Access

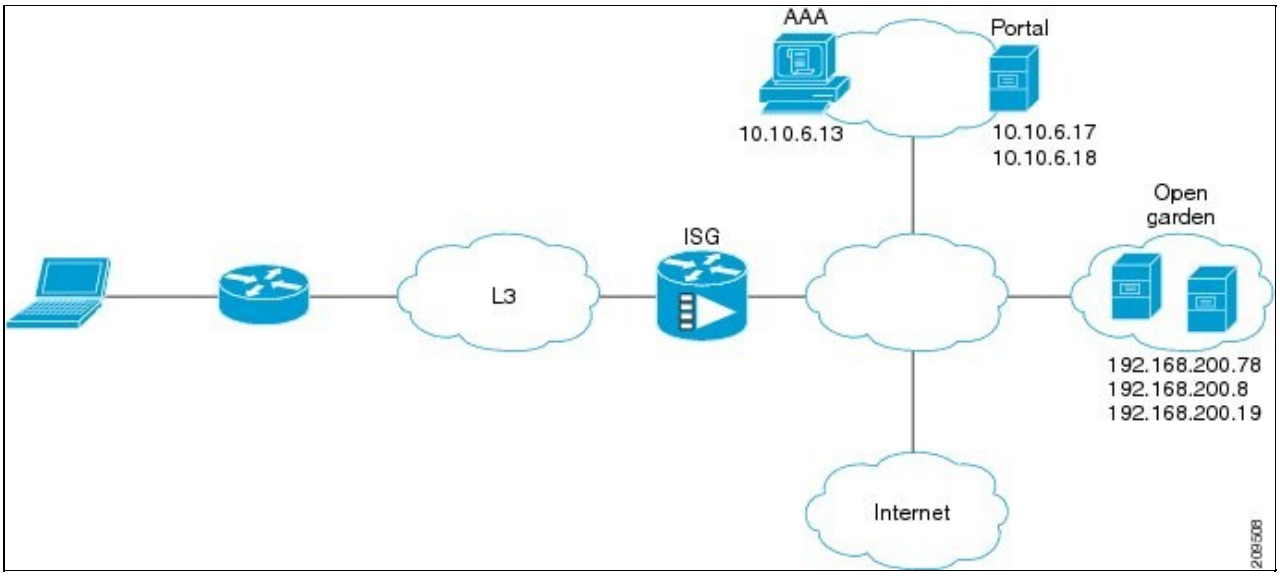
- DSL Forum TR-101 functions
- Metro Ethernet Forum (MEF) 6/10 Ethernet services models
- N:1 and 1:1 VLAN multiplexing models
- Multi VC, trunk and non-trunk user network interface (UNI) options
- Ethernet to the home and business (ETTx) Spanning-Tree Protocol (STP) access rings and hub and spoke
- WiMAX nodes integrated in the ETTx access
- DSL access nodes with redundant connectivity

Transport Functions between Access and Edge

- Intelligent access multiplexing
- MPLS/IP Layer 2 and Layer 3 transport services
- Transparent virtualized Ethernet point-to-point (P2P) and multipoint (MP) transport (EoMPLS and H-VPLS) for services with IP/L3VPN/L2VPN Edge in broadband network gateway (BNG) and multiservice edge (MSE)
- Service-aware IP transport for triple-play services (IPTV, VoD, Voice)
- L2/L3 MPLS/IP transport layer provides flexibility scalability, transparency, virtualization and service awareness when required
- Aggregation network provides the option for implementing L2/L3 business VPN services

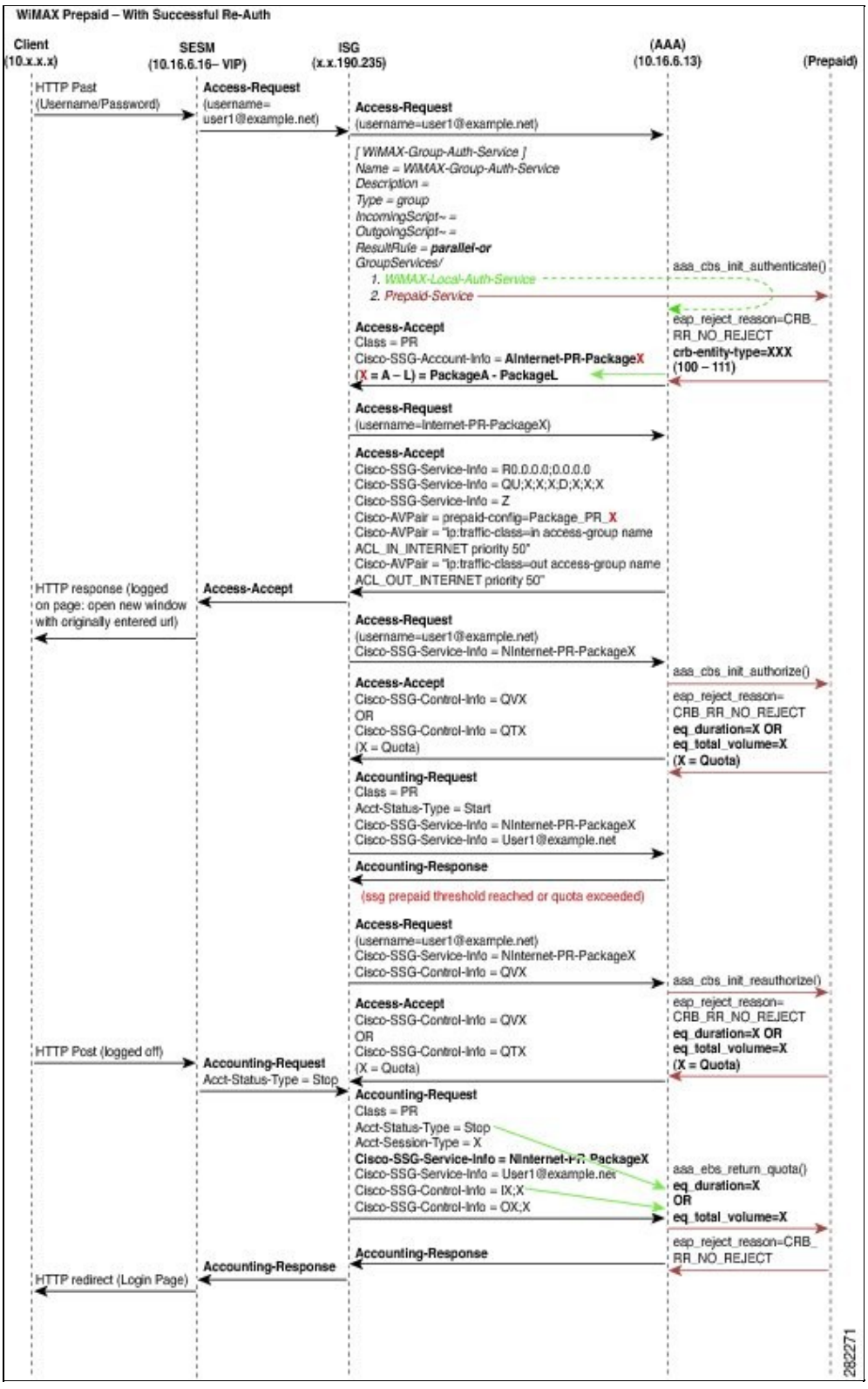
Subscriber and Service Edge

- Residential H.323 signaling interface (HSI) in BNG
- Business L2/3 VPNs in MSE

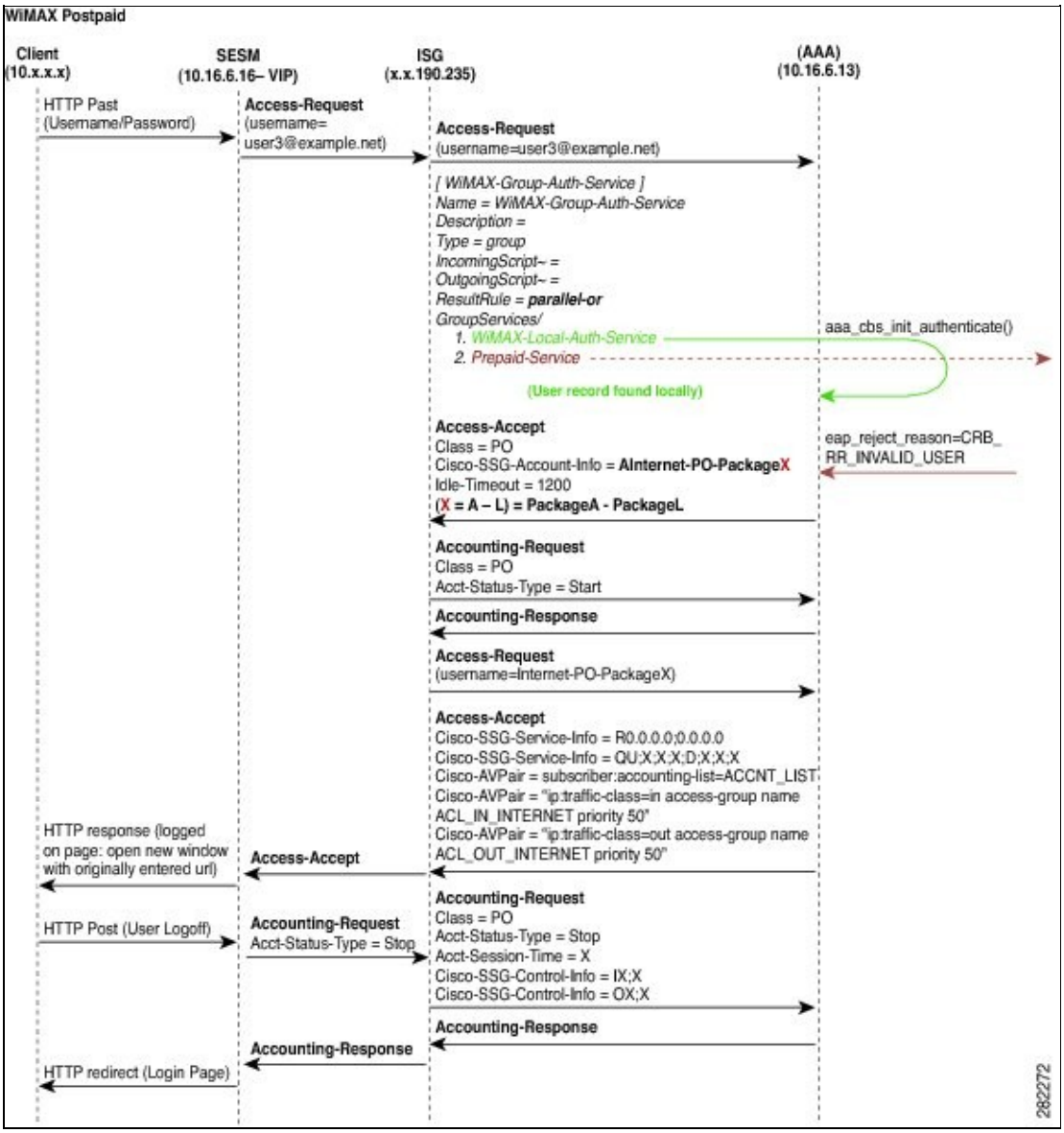


Call Flows

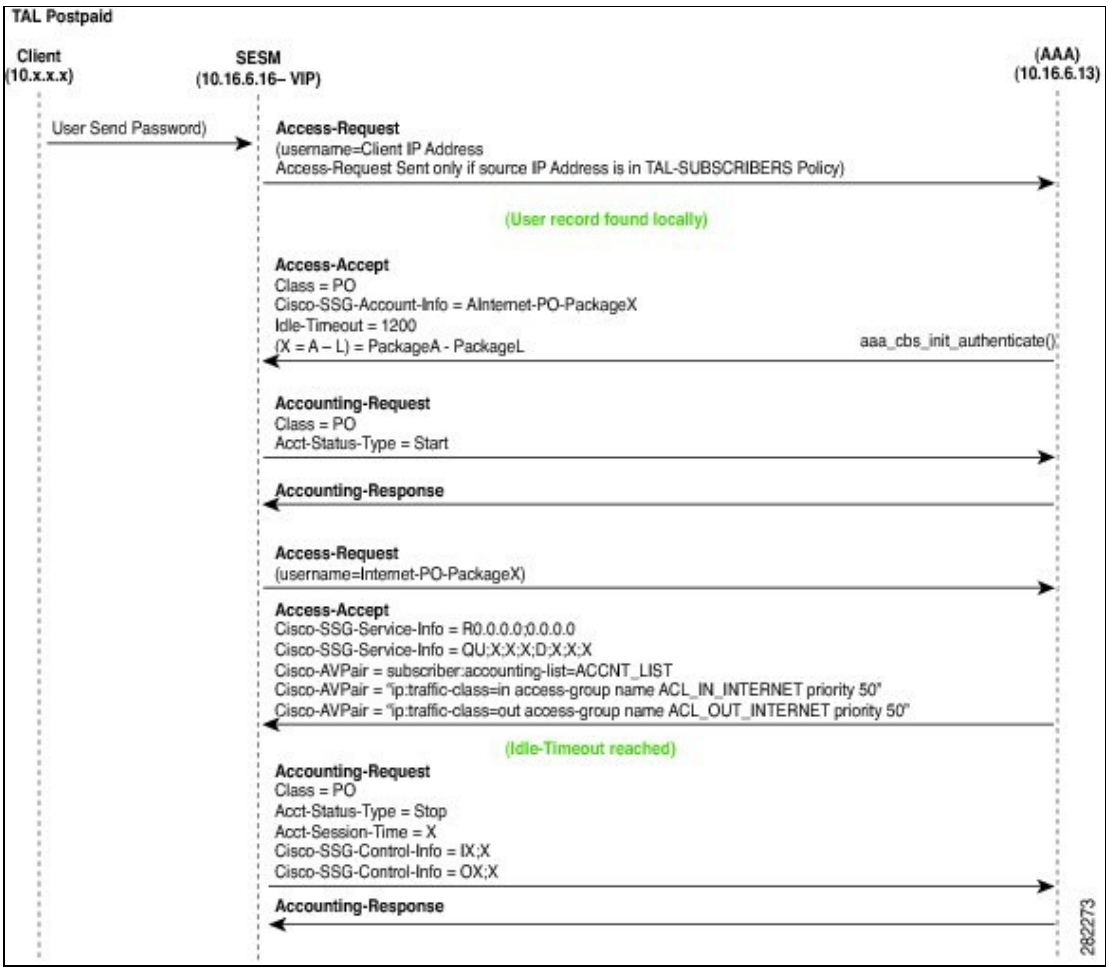
WiMAX Prepaid



WiMAX Postpaid



Transparent Auto-Logon (TAL) Postpaid



Configuration

The following example shows the configuration of a routed subscriber network using the Port-Bundle Host Key (PBHK) and Layer 4 Redirect features. The basic behavior of the ISG is summarized in the control policy that is used when a First Sign of Life (FSOL) is detected. In this example, the FSOL is an unclassified source IP address.

Control Policy

The key to understanding an individual ISG configuration is generally the control policy, which maps out the actions taken by the ISG when different ISG events occur. The following example shows a control policy that allows some source IP address traffic to pass through the ISG without authentication, performing Transparent Auto Logon (TAL) for a set of predefined IP addresses, and performing web (portal) authentication for all other subscribers.

```
policy-map type control isg-control
```

Control policy definition

Session Start Events

```
class type control PASSTHROUGH event session-start
  10 service local-passthrough
```

FSOL traffic that m
map PASSTHROU

```
!
```

through any authen
redirection. It simp
applied to it.

```
class type control TAL_IP_SUBSCRIBERS event session-start
  10 authorize aaa list AUTHOR_LIST1 password svcisco identifier source-ip-address
  20 service-policy type service name DEFAULT_NETWORK_SERVICE
  30 set-timer IP-UNAUTH-timer 5
!
```

FSOL traffic that n
map is sent for auth
authorization fails,
DEFAULT_NETW
is applied, and an a
timer is set.

Any FSOL traffic t
match the previous
handled here.

```
class type control always event session-start
  10 service-policy type service name DEFAULT_NETWORK_SERVICE
  20 service-policy type service name PBHK_SERVICE
  30 service-policy type service name L4_REDIRECT_SERVICE
  40 service-policy type service name OPENGARDEN_SERVICE
  50 set-timer IP-UNAUTH-timer 5
!
```

- Apply defa
- Apply PBH
- Apply L4 R
  service
- Apply Ope
- Set unauth

Account Logon Events

```
class type control always event account-logon
  10 authenticate aaa list AUTHEN_LIST1
  20 service-policy type service unapply name L4_REDIRECT_SERVICE
!
```

On an account-logo
authenticate the su

Upon successful
authentication, una
L4_REDIRECT_S

Account Logoff Events

```
class type control always event account-logoff
  10 service disconnect delay 5
!
```

Upon a
account-logoff
event,
disconnect
after a 5
second delay.
This should
ensure that the
client TCP
sessions close
before
disconnection.

Service Start Event

```
class type control always event service-start
  10 service-policy type service identifier service-name
```

Upon a
service-start
event, apply
the service
defined in
the message.

Service Stop Event

```
class type control always event service-stop
  10 service-policy type service unapply identifier service-name
```

Upon a service-stop event, unapply the service defined in the message.

Timed Policy Expiry Event

```
class type control UNAUTHEN_COND event timed-policy-expiry
  10 service disconnect
```

Upon a timed-policy-expir event, if the class-r UNAUTHEN_CO is true, disconnect session.

Quota Depleted Event

```
class type control always event quota-depleted
  10 set-param drop-traffic TRUE
```

Upon a quota-depleted event, drop the session traffic.

Credit Exhausted Event

```
class type control always event credit-exhausted
  10 service-policy type service name PREPAID_REDIRECT_SERVICE
```

Upon a credit-exhau apply the service PREPAID_REDIRE

Class Maps

In the previous section class maps were used to select which actions would occur for certain events. The following examples show these class-maps.

```
class-map type control match-any PASSTHROUGH
 match source-ip-address 10.10.62.0 255.255.254.0
 match source-ip-address 10.10.28.1 255.255.255.255
 match source-ip-address 10.10.0.111 255.255.255.255
?
class-map type control match-any TAL_IP_SUBSCRIBERS
 match source-ip-address 10.10.52.163 255.255.255.255
```

AAA

Authentication, authorization, and accounting (AAA) is a key part of ISG and ISG cannot operate without a minimum AAA configuration.

This comm is required.

```
aaa new-model
!
aaa group server radius AAA_GROUP
 server 10.10.6.13 auth-port 1812 acct-port 1813
```

Typical ser group definition

```
aaa authentication login AUTHEN_LIST group AAA_GROUP
aaa authorization network AUTHOR_LIST group AAA_GROUP
aaa authorization subscriber-service default local group AAA_GROUP
```

```
aaa accounting update periodic 30
aaa accounting network ACCNT_LIST start-stop group AAA_GROUP
```

- ISG
aut
con
- ISG
aut
con
- ISG
sub
ser
con
- Per
acc
upd
- ISG
acc
con

ISG RADIUS Server

```
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
radius-server attribute 25 access-request include
```

RADIUS extensions

RADIUS Server

```
radius-server host 10.10.7.14 auth-port 1812 acct-port 1813 retransmit 3 key 7 <removed>
radius-server retransmit 2
radius-server timeout 3
radius-server vsa send accounting
radius-server vsa send authentication
```

RADIUS server

Change of Authorization (CoA) Portal

```
aaa server radius dynamic-author
 client 10.10.80.130
 client 10.10.33.166
 server-key 7 <removed>
 auth-type any
 ignore session-key
 ignore server-key
```

Class of service (CoS) server

Services

Open Garden Service

The Open Garden service is a traffic class that is defined to only allow limited services prior to authentication. These services are typically Domain Name System (DNS), web portal, and any other services that are necessary to get the subscriber to a level where they can authenticate themselves. Examples of the service configuration are shown below.

```
ip access-list extended ACL_IN_OPENGARDEN
 permit ip any host 192.168.200.78
 permit ip any host 192.168.200.8
 permit ip any host 192.168.200.19
?
```

Define hosts reachable by subscribers.

```
ip access-list extended ACL_IN_OPENGARDEN
 permit ip any host 192.168.200.78
 permit ip any host 192.168.200.8
 permit ip any host 192.168.200.19
?
class-map type traffic match-any TC_OPENGARDEN
 match access-group input name ACL_IN_OPENGARDEN
 match access-group output name ACL_OUT_OPENGARDEN

policy-map type service OPENGARDEN_SERVICE
 10 class type traffic TC_OPENGARDEN
 !
 class type traffic default in-out
  drop
```

Define return path for client traffic.

Create class map based on the host ACLs.

Define the Open Garden service

- Match the traffic class
- Action upon matching the class
- Default action upon traffic not matching

Layer 4 Redirect Service

The L4 Redirect service is typically used to force subscribers to a web portal for authentication purposes.

```
ip access-list extended ACL_REDIRECT
 deny   tcp any host 10.10.6.16 eq www
 deny   tcp any host 10.10.6.16 eq 8080
 permit tcp any any eq www
 permit tcp any any eq 8080

class-map type traffic match-any TC_L4_REDIRECT
 match access-group input name ACL_REDIRECT

policy-map type service L4_REDIRECT_SERVICE
 20 class type traffic TC_L4_REDIRECT
  redirect to group REDIRECT_GROUP

redirect server-group REDIRECT_GROUP
 server ip 10.16.6.16 port 8090
```

Define traffic to be diverted

- Do not divert traffic going to the portal
- Divert all other web traffic

Create a class map for the diverted traffic.

Create L4 Redirect service

- Traffic that matches the class-map is sent to the redirect group

Define the redirect group

- Define the destination address and port

PBHK Service

```
access-list 110 permit ip any host 10.10.6.16
access-list 110 permit ip any host 10.10.6.28

ip portbundle
```

Apply PBHK to traffic to web portals.

```
 match access-list 110
 source Loopback100
 source Loopback101

interface GigabitEthernet1/0/0.123
  encapsulation dot1Q 123
 <snip>
 ip portbundle outside

policy-map type service PBHK_SERVICE
 ip portbundle
```

Define port bundle

- ACL defining which traffic requires PBHK
- Interface for PBHK addressing
- Additional interface for PBHK addressing

Outgoing interface towards web portal.

Apply port bundle

Related Information

Technical Support & Documentation - Cisco Systems

- Intelligent Services Gateway (ISG) -- Residential Access Using DHCP Sessions Configuration Example
- Intelligent Services Gateway Configuration Guide, Cisco IOS Release 15.1S
- Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S