

## Contents

- [1 Introduction](#)
- [2 Design](#)
- [3 Configuration](#)
  - ◆ [3.1 Control Policy](#)
  - ◆ [3.2 Class Maps](#)
  - ◆ [3.3 AAA](#)
  - ◆ [3.4 Services](#)
- [4 Related Information](#)

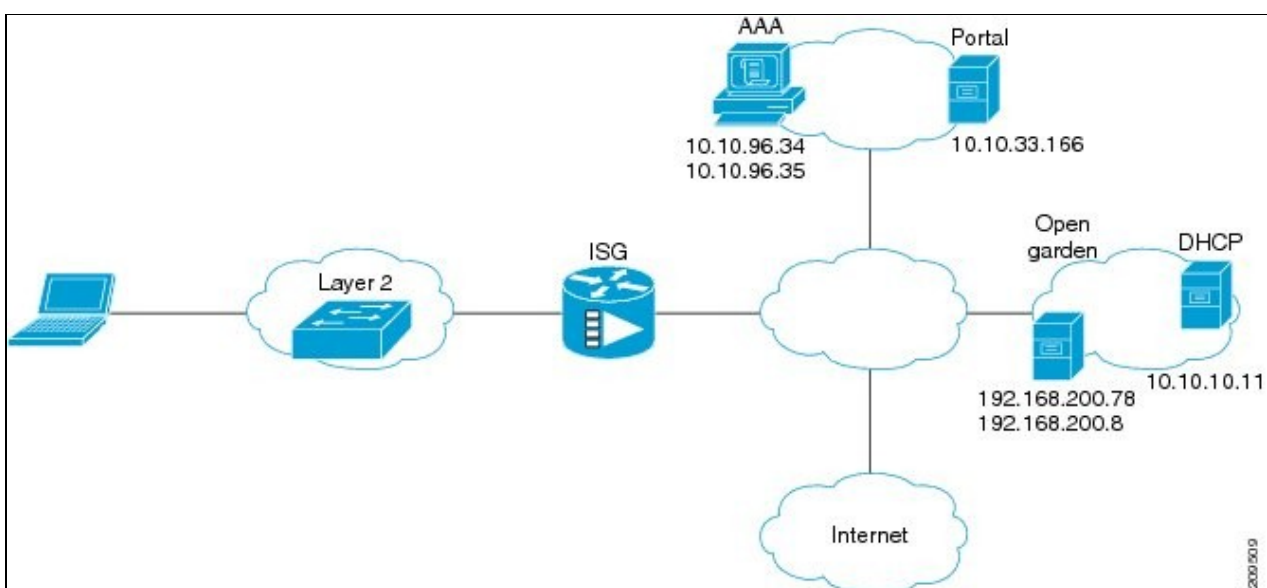
## Introduction

This example provides a sample configuration of Cisco Intelligent Services Gateway (ISG) deployed in a service provider's broadband network with residential subscriber access through DHCP-initiated sessions.

## Design

Service delivery model includes:

- DHCP-initiated sessions with no features
- Transparent auto-logon (TAL) based on DHCP option 82
- Remote ID and web logon fallback through L4 redirect and change of authorization (CoA)
- Downloading of QoS profile from RADIUS server for authenticated users



## Configuration

The following example shows the configuration of a Layer 2 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 DHCP
```

Control policy definition

### Session Start Events

```
class type control always event session-start
  5 authorize aaa list AUTHOR_LIST password EXAMP identifier remote-id
  26 service-policy type service name L4REDIRECT_SERVICE
  27 service-policy type service name OPENGARDEN_SERVICE
  50 set-timer IP_UNAUTH_TIMER 10
!
```

Any FSOL traffic that does not match previous class maps is handled here.

- Authorize
- Apply L4 Redirection service
- Apply Open Garden service
- Set unauthenticated timer

### Account Logon Events

```
class type control always event account-logon
  10 authenticate aaa list default
```

On an account-logon event, authenticate the subscriber.

### 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.

### Session Restart Event

```
class type control always event session-restart
  5 authorize aaa list AUTHOR_LIST password 7300test identifier remote-id
  20 service-policy type service name OPENGARDEN_SERVICE
  30 service-policy type service name L4REDIRECT_SERVICE
  50 set-timer IP_UNAUTH_TIMER 10
```

Upon a service-restart event, apply 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-expiry event, if the class-map UNAUTHEN\_COND is true, disconnect the session.

### 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 traffic match-any ISG_OPENGARDEN
  match access-group output name ACL_OUT_OPENGARDEN
  match access-group input name ACL_IN_OPENGARDEN
```

Class-map for the Open Garden Access Control List (ACL)

```
class-map type control match-all IP_UNAUTH_COND
  match timer IP_UNAUTH_TIMER
  match authen-status unauthenticated
```

Class-map for unauthenticated user timeout

### AAA

AAA is a key part of ISG and ISG cannot operate without a minimum AAA configuration.

```
aaa new-model
!
aaa group server radius ISG_TEST
  server 10.10.96.34 auth-port 1812 acct-port 1813
  server 10.10.96.35 auth-port 1812 acct-port 1813
  ip radius source-interface GigabitEthernet1/0/4.1020
  attribute nas-port format d
```

This command is required.

Typical server group definition

### ISG Authentication and Accounting

```
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

aaa authorization network AUTHOR_LIST group ISG_TEST
aaa authorization subscriber-service default local group ISG_TEST
aaa accounting network default start-stop group ISG_TEST
aaa accounting network IP_SESSION start-stop group ISG_TEST group ISG_TEST1
```

- ISG authentication configuration
- ISG authorization configuration
- ISG subscriber services configuration
- Periodic accounting updates
- ISG accounting configuration

## 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-server attribute nas-port format d
radius-server attribute 31 send nas-port-detail mac-only
```

RADIUS  
extensions

## RADIUS Server

```
radius-server host 10.10.96.34 auth-port 1812 acct-port 1813 key 7 <Removed>
radius-server host 10.10.96.35 auth-port 1812 acct-port 1813 key 7 <Removed>
radius-server dead-criteria tries 3
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 15
radius-server directed-request
radius-server domain-stripping
radius-server key 7 <Removed>
radius-server vsa send accounting
radius-server vsa send authentication
```

RADIUS  
server

## CoA Portal

```
aaa server radius dynamic-author
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

## Intelligent\_Services\_Gateway\_(ISG)\_--\_Residential\_Access\_Using\_DHCP\_Sessions\_Configuration\_Example

that are necessary to get the subscriber to a level where they can authenticate themselves. Examples of the service configuration are shown below.

Define hosts reachable by subscribers.

```
ip access-list extended ACL_IN_OPENGARDEN
?
permit ip any host 10.10.33.166
?
ip access-list extended ACL_OUT_OPENGARDEN
?
permit ip host 10.10.33.166 any
?
```

Define return path for client traffic.

```
class-map type traffic match-any ISG_OPENGARDEN
match access-group output name ACL_OUT_OPENGARDEN
match access-group input name ACL_IN_OPENGARDEN
```

Create class map based on the host ACLs.

```
policy-map type service OPENGARDEN_SERVICE
20 class type traffic ISG_OPENGARDEN
!
```

Define the Open Garden service

- Match the traffic class
- Action upon matching the class

### 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_IN_L4REDIRECT
?
deny tcp any host 10.10.33.166
permit tcp any any eq www
permit tcp any any eq 443

class-map type traffic match-any L4REDIRECT
match access-group input name ACL_IN_L4REDIRECT
!

policy-map type service L4REDIRECT_SERVICE
10 class type traffic L4REDIRECT
redirect to group ISG_GROUP
accounting aaa list IP_SESSION
!
class type traffic default input
drop

redirect server-group ISG_GROUP
server ip 10.10.33.166 port 80
```

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

Default action upon traffic not matching

Define the redirect group

- Define the destination address and port

## **Related Information**

### Technical Support & Documentation - Cisco Systems

- [Intelligent Services Gateway \(ISG\) -- WiMAX Service Provider Network Configuration Example](#)
- [Intelligent Services Gateway Configuration Guide, Cisco IOS Release 15.1S](#)
- [Intelligent Services Gateway Configuration Guide, Cisco IOS XE Release 3S](#)