Enabling User-Based Service Subscription

Session SPL-205

Agenda

• Data Services
• Service Selection for Broadband Access
• Service Selection User Interface
• User Self Care
• Subscriber Service Center
• Case Studies
• Conclusions
Data Services

What Are Broadband Services?

- Content Screening
- Streaming
- Security
- Entertainment
- Internet Access
- Family Surfing
- Corporate Access
Service Selection for Broadband Access

Service Selection Components

- Directory Service
- RADIUS
- Authentication Service
- Security Policies
- Back Office
- Service Selection
- User Interface
- SSC
- Network Awareness
- Service Access
- Services
Network Gateway(s) Requirements

- Provide user control of services
- Provide user access via:
  - Bridged, Routed, PPP access, L2TP, GPRS, 802.11
- Network layer service access
  - MPLS-VPN, Routed, L2TP, Proxy
- Open, Walled Garden support
- Authorization, authentication, accounting

Core Network Architectures: Service Selection Gateway
SSG Packet Flow

SSG Host-Object

- Host Object—A “Host Object” represents an active user account in the SSG internal database. It is created as soon as the user is authenticated successfully. The Host Object is comprised of the following:
  - Implements User ID concept
  - Subscriber Host IP Address
  - Subscriber User-ID
  - IDB of the Downlink Interface
  - Service Connection List

Cisco IOS# show ssg host
SSG Service Object

- **Service Object**—A “Service Object” contains all the relevant information about a service (destination network). Service Object is created from a “Service Profile” which is obtained from local configuration or from a AAA Server.

  - **Service Name**—Name of the service itself
  - **Domain Name**—A list of domain names associated with this service (used for DNS redirection)
  - **Service Type**—Defines the kind of service (Passthrough, Tunnel or Proxy)
  - **Destination Network**—Every service is identified by allowing/disallowing access to a network segment identified by a combination of IP Address and a Mask
  - **Next Hop Address**—Used to determine next hop for routing upstream traffic
  - **Remote RADIUS Server Info**—For Proxy type service

```cisco
Cisco IOS# show ssg service
```

SSG Connection Object

- **Connection Object**—A “Connection Object” represents an active connection to a service (destination network). It is created when a subscriber logs on to a service and is destroyed when he/she logs off the service.

  - **Connection Object**—Service that this Connection Object refers to

```cisco
Cisco IOS# show ssg connection 10.0.0.1 secure-vault
```
SSG Overlapping IP Addresses

User-ID to VPN Mapping

(User

Service Selection Gateway

USER1-ID

Services1.com

USER2-ID

Services2.com

USER3-ID

Services3.com

(L3) Web Service Selection

Authentication Service

Directory Service

SSC

Service Definition

Security Policies

RADIUS

Enable Service Selection

Service Access

SSG

Passthru

Proxy

Tunnel
L2 Service Selection

Split DNS

When the SSG receives a DNS request, it will perform domain name matching between the domain in the DNS request and the Domain attribute(s) from the user’s currently logged in Services.

If a match is found the request is redirected to the DNS server configured for the matched Service.
Cisco IOS Service Access Methods

Service Selection Gateway

- MPLS -VPN
- IPSEC -VPN
- Content Replication
- Multi-rate
- Security

L2TP
- Bridging
- PPP
- Routed
- GPT

IPSEC Secure Service

Service Selection

- Security Policies
- RADIUS
- Directory Service
- SSC

Virtual Vault

IPSEC

Service Access
Service Selection
User Interface

Service Selection UI Features

“It should Be Web-Based”

• Dynamic User Interface
• HTML and PDA, WAP
• Security (http, https)
• Languages, Icons, Multimedia
• Banners and advertising
• User Self Care

JAVA Server Pages
Service Selection Dashboard

Dynamic User Interface

- Personalized Menu of Services
- Branded Partner Logo and Advertising
- Personalization Options
- Jump Page for Partner Services

JAVA Server Pages

Users Are Different

- User menu
- Error Messages
- Status Messages
- Extensibility is key

Internationalization (i18n, i10l)

User menu
Error Messages
Status Messages
... Extensibility is key

user1
user2
Tailoring to Users Access

Who am I? Where am I? What am I using?

UI RADIUS Control

User Profiles
- jdoe
  - Password = letmein
  - account = internet
  - account = community
  - account = news
- tihor
  - Password = wombat
  - account = internet
  - account = news
  - account = games
- guest
  - Password = guest
  - account = internet
  - account = community
  - account = games

Service Profiles
- Internet
  - Password = cisco
  - Service-Info = "Internet"
  - Service-Info = "R192.168.4.10;255.255.255.255"
  - Service-Info = "http://www.cisco.com"
- Games
  - Password = cisco
  - Service-Info = "Games"
  - Service-Info = "R192.99.50.10;255.255.255.255"
- News
  - Password = cisco
  - Service-Info = "News"
  - Service-Info = "R192.200.99.1;255.255.255.255"
- Community
  - Password = cisco
  - Service-Info = "Community"
  - Service-Info = "R192.168.5.10;255.255.255.255"
User AAA

- **RADIUS** is a natural choice
  - Well understood wholesale model
  - Widely deployed
  - Works per user session
- But semantics are very limited
  - No relationships
- Directory offers richer semantics
  - Role-Based Access Control (RBAC)
  - Wide-spread adoption of directories
- Solution: RADIUS front-end to LDAP store

UI RBAC Control

Who you are, what you can do, When you can do it...
User Service Control

- Web Servers
  - RPC API
  - SNMP
  - Telnet

- Directory Service
  - LDAP
  - RADIUS

User Boot Sequence

- L2
  User Connection: PPP or some other method.

- L3
  DHCP (for SSD reachability)
  Client configuration: WINS, DNS, Default Router
  Only access to SSD

- SSD
  Browse to the Dashboard and select Services
TCP Redirect

Step 1
Unauthorized subscriber attempts to connect to a service on a tcp port i.e. www.yahoo.com

Step 2
HTTP packet is redirected to the SSC or cluster of SSCs (dest IP address and port rewritten)

Step 3
Subscriber logs into the SSC and is authenticated/authorized

Step 4
Subscriber is then presented with a personalized Home Page, or the Providers Home Page or the original URL (configurable)

TCP Redirect

#ssg http-redirect group portal server 1.1.1.1 9090
#ssg http-redirect group portal server 1.1.1.2 9090
#ssg http-redirect port 9001 group portal

nrp# show ssg http-redirect group portal
HTTP redirect group portal;
Showing all HTTP servers (Address, Port):
  1.1.1.1, 9090
  1.1.1.2, 9090
TCP ports to redirect:
  9001

Cisco IOS CLI
User Logon (Single Sign On) and Service Logon

Step 1
User launches PPP connection and attempts to get authenticated.

Step 2
PPP User gets authenticated against a RADIUS server.

Step 3
Alternatively the PPP could have been authenticated against a Directory.

Step 4
Once authenticated, the user can access the Default Network and hence browse to the SSC.

Step 5
This user has an auto service (Internet) configured and that service is automatically connected.

Step 6
The SSC then presents the user with their homepage—remember this is Single Sign on mode.

Step 7
The user then chooses a service (Corporate Internet) which is a proxy service and gets presented with a service logon page.

Step 8
The user enters the username and password and gets authenticated against the proxy service Radius server and is connected to this service.

Step 9
The Corporate service then appears in a new browser window against the proxy service Radius server and is connected to this service.

Open and Walled Garden(s)

Open Garden—Free Services
Walled Garden—Authenticated Services

OPEN-GARDEN (Free Services)

Walled-GARDEN (Authenticated Services)
The Open Garden Networks

- The open garden is a list of networks open to **unauthenticated** users
- Allows the service provider the ability to provide limited free access to specified services

---

Cisco IOS Open Garden Config

```plaintext
ssg open-garden opengarden-wwwin.com
ssg open-garden opengarden-zapple.com
!
local-profile opengarden-zapple.com
  attribute 26 9 251 "R192.168.52.10;255.255.255.0"
  attribute 26 9 251 "D10.0.0.1"
  attribute 26 9 251 "Ozapple.com"
!
local-profile opengarden-wwwin.com
  attribute 26 9 251 "R192.1.99.10;255.255.255.255"
  attribute 26 9 251 "D192.168.1.1"
  attribute 26 9 251 "Ocisco.com;zap.com"
```
Walled Garden

- Offer unique value-added services
  - Internet content filters
  - Parental management tools
  - Online wallet
  - Video content
  - Music content
  - Gaming services
  - Online Meetings
  - Data backup and storage

User Self Care
Self Care

- Change password
- Change home address
- Change subscriptions
- Create new accounts
  Sub accounts: children
  Subscribe sub-accounts to services

Change Home Address

Step 1
User starts a session and arrives at the SSC Homepage

Step 2
User chooses Self Care option and selects the Change address option

Step 3
And gets presented with a change address screen

Step 4
The user enters the new address details and submits the changes

Step 5
The new account information is saved into the Directory and this new address is now set

Account 1234: User Profile
--------------------------------------------
Account Type: Parent
User Name: Ric
Surname: Pruss
Given Name: Richard
Phone Number: 555 123 4567
Fax: 555 123 4567
Email: ric@cisco.com
Address: 84 Acacia Grove, Los Gatos, CA 12345
Role: Self Manage, Subscriber, Parent
Group: Gold
Subscribed Services: Internet, Corporate, Games, Shopping
Auto Services: Internet

Account 1234: User Profile
--------------------------------------------
Account Type: Parent
User Name: Ric
Password: password
Surname: Pruss
Given name: Richard
Phone Number: 555 123 4567
Fax: 555 123 4567
Email: ric@cisco.com
Address: 13 Acacia Grove, East Palo Alto, CA 56789
Role: Self Manage, Subscriber, Parent
Group: Lead
Subscribed Services: Internet, Corporate, Games, Shopping
Auto Services:
Service Subscription

Step 1
User starts a session and arrives at the SSD Homepage

Step 2
User chooses Self Care option and selects the Service Subscription option

Step 3
And gets presented with a list of services to subscribe to or to unsubscribe from

Step 4
The user selects services to subscribe to or unsubscribe from and submits the changes

Step 5
The changes are saved into the Directory and these new details are available to use straightaway

Subscriber

Account 1234: User Profile
Account Type: Parent
User Name: Ric
Password: cisco
Surname: Pruss
Given name: Richard
Phone Number: 555 123 4567
Fax: 555 123 4567
Email: ric@cisco.com
Address: 12 Acacia Grove, Los Gatos, CA 12345
Role: Self Manage, Subscriber, Parent
Group: Gold
Subscribed Services: Internet, Corporate, Games, Shopping
Auto Services: Internet

Create Sub-Account

Step 5
The new account information is saved into the Directory and this account is available to be used straightaway.

Subscriber

Account 1234: User Profile
Account Type: Parent
User Name: Ric
Password: cisco
Surname: Pruss
Given name: Richard
Phone Number: 555 123 4567
Fax: 555 123 4567
Email: ric@cisco.com
Address: 12 Acacia Grove, Los Gatos, CA 12345
Role: Self Manage, Subscriber, Parent
Group: Gold
Subscribed Services: Internet, Corporate, Games, Shopping
Auto Services: Internet

New Account 4321: User Profile
Account Type: Child:Parent=1234
User Name: Josh
Password: barney
Surname: Pruss
Given name: Joshua
Phone Number: 555 123 4567
Fax: Email: josh@cisco.com
Address: 12 Acacia Grove, Los Gatos, CA 12345
Role: Self Manage
Group: Gold
Subscribed Services: Games
Auto Services:
Subscriber Service Center

Service Selection Control

Billing
Self Care
Policies
SSG
User
Admin
LDAP/RADIUS
API
Service Access
Requirements

- User service control
- Support for user authentication, authorization and accounting
- Per user and per service billing
- Operator management tool
- Scalability and fault tolerance

SSC Layered Architecture
Device Control and User/Service Profiles

- **Control Plane**
  - API
  - RADIUS
  - CORBA
  - RPC

- **Data Sources**
  - JDBC
  - LDAP
  - API

**SSC Session**

Authentication, Authorization and Management

- **Authentication**
  - API
  - RADIUS

- **Authorization**
  - RADIUS
  - LDAP
  - AUTH

- **User Interaction**
  - HTTP
  - SNMP
  - JMX

**SSC Session**
Service Publishing Models

- Single Policy
  - Security Policies
  - RADIUS
  - Directory Service
  - Authentication Service
  - Hidden Service
  - Subscribed and Possible to Select
  - Auto-Service on Start; Selected and Available in the Subscription List

Walled Garden Services

Role Based Access Control

- User → Access → Object
- User → Acquire → Role → Access → Object

Traditional Access Control

Role Based Access Control
Administration Roles and Policies

Step 5
Admin user creates new group and enters the various group parameters

Account 5678: Group Profile
- Group Name: GoldUsers
- Sr: Users: User1, user3, user65, user987
- Jr: Auto-subscribe: Internet
- Pr: Auto-subscribe: Corporate
- St: Auto-subscribe: Games
- Gi: Auto-subscribe: Shopping
- Ni: Auto-subscribe: Community
- Fi: Auto-subscribe: Fashion
- Ti: Auto-subscribe: Travel
- Service type:
- Service URL:
- Subscribed Services: Internet, Corporate, Games, Shopping
- Auto Services: Internet

User Administration: Regional Groups—Zurich

POP 1—Zurich Regional View
1. In very large scale deployments, replications between LDAP directories can be timed so that user changes are immediately available in the area a user is while they propagate slowly to the rest of the network. Allowing the network to scale as if it were a number of small networks, but still allow a user to roam and maintain a coherent view of a user in all areas.

Billing/Accounting

Accounting user based or serviced (connection) based. Accounting record based on elapsed time, or bytes sent/received, packets sent/received.

Interval to send out accounting record for all users different interval for different services.
Fault Tolerance

SLB Device  SSC Servers  RADIUS Servers  Directory Servers

Case Studies
Corporate Network Extension (VPN)

Internet Access

Intranet Access

Operator Internal IP Network

Internet

IP Tunnel

Private and Secured Domain

Game Short Circuit Service

High Speed Direct Connection!!

Variable Latency Internet Connection

LDAP Data Store

Cisco 6400/SSG

IP DSL Switch

Game Server

SSC

Cisco.com
GPRS Solution

- Per User Service Control (Security, Routing, DNS)
- Centralized Provisioning, Distributed Functions
- Contemporary Access to Intranet, Extranet, Internet Networks
- Captive Portal for Consumer Users
- Customizable WEB Service menu for each Corporate
- Common Access for GPRS, GSM Dial-up and 3G data services

Mobile Internet Access
Personalized Service Today

Internet Portal to Set Preferences

User Wishes to Access Emergency Services that a Third Party has Created

User Wants a Tow Truck Emergency Service

Internet Portal Returns a List of Available Emergency Services

Internet Portal Returns a List of the Closest Gas Stations with Tow Trucks

User Hits Send and the Phone Dials the Tow Truck Number

Tow Truck
123 N. Meacham
456 W Algonquin
847-376-3746

User in Use
847-476-3746

Phone Ready
Emergency Forward

Emergency Services
Police Fire Towtruck

Conclusions
Delivering Services

User-Based Service Selection

Layer 2/3 Aggregation

DIAL Point-to-Point

- PVCs, SPVCs, SVCs
- VP/VC Switching
- ILMI/PNNI

Layer 2/3 Aggregation

- L2TP LAC/LNS/TS
- PTA-Multi Domain
- MPLS VPN

- Branded/Captive Portals
- Walled Garden
- Personalization

Profits

Services

Multi-Service Framework

PC

WAP

PDA

Notebook

ADSL

Leased Line

Dial-Up 5300/5400

GGSN

AAA

Directory

Content Gateway

SSG

IP

MPLS

IPSEC

Content Intranet Extranet

WAP
### Subscriber Perspective

- Browser driven
- No host configuration or client software
- Support mobility or multiple access points
- Multiple subscriber access
- Ease of use (of course)
  - Mimic existing internet service selection paradigms

### Service Provider Perspective

- Low cost of operation
- Browser driven
- Subscriber self-care
- Extensible infrastructure to add new applications
  - And target groups of subscribers
- Network and Application services
  - Network aware
- Scale (of course)
- No subscriber training
  - Mimic existing internet service selection paradigms
Reference Web Sites


RBAC: http://csrc.nist.gov/rbac/

JAVA: http://java.sun.com

Enabling User-Based Service Subscription

Session SPL-205
Please Complete Your Evaluation Form

Session SPL-205