Cisco Expo 2009

Policy Control Architecture for Wireline Networks

Intelligent Service Gateway

Ahmad Chehime

Welcome to the Human Network.

Agenda

- Services Evolution Requires:

  Cisco ISG – Intelligent Service Gateway

- "Classic" Policy Control for Broadband Applications
  - Portal Based Self-Services
  - Tiered Services (Time & Volume)
  - Advanced Application Aware Tiered Services

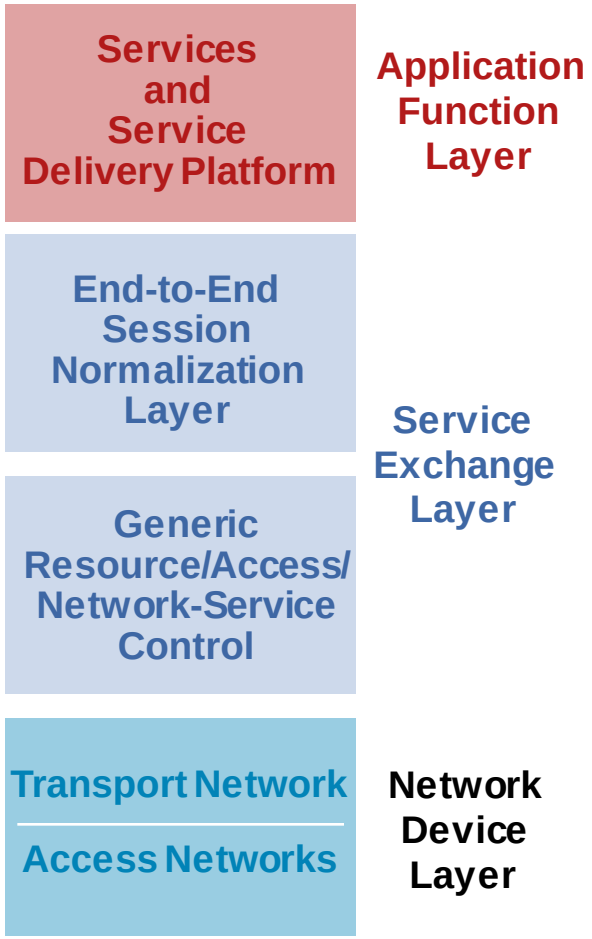
Services Evolution:

Intelligent Service Gateway

Welcome to the Human Network.

Next Generation Network
Overview and Drivers

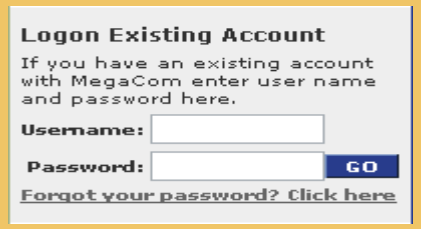
- SPs to offer differentiated services
  - Rapid introduction of new value added services
  - Personalized applications to reduce churn and enhance differentiation
  - Multimedia and Combinational (e.g. Fixed-Mobile) Services
- SPs require close User and Network control
  - Authentication, Charging, Policy Enforcement (QoS, Security, Accounting…)
  - "Walled Garden" Service Concept for a wide variety of Services
- Network Convergence
  - Access independence and mobility
  - Transport convergence over IP
  - Reuse of common resources
  - Aging PSTN Equipment
  - Price pressure of commoditization



The New User Experience
Enabling the Next Wave of Broadband

Add Subscribers

Register



Log in

Add Services

Pay As You Go!	Pay What You Use!	Broadband Light	Broadband Basic	Broadband Premium
Buy credit	Buy	Buy: $19.99	Buy: $29.99	Buy: $39.99

Add Value

Branded VoD ($4.99/movie)

Branded TV ($29.99)

Branded Phone ($15.99 + LD)

The Elements of Customization

Identity

Subscriber identified using multiple dimensions. Identity gathered:

- **From multiple sources and events**
- **Over session lifecycle**

Differentiated Services

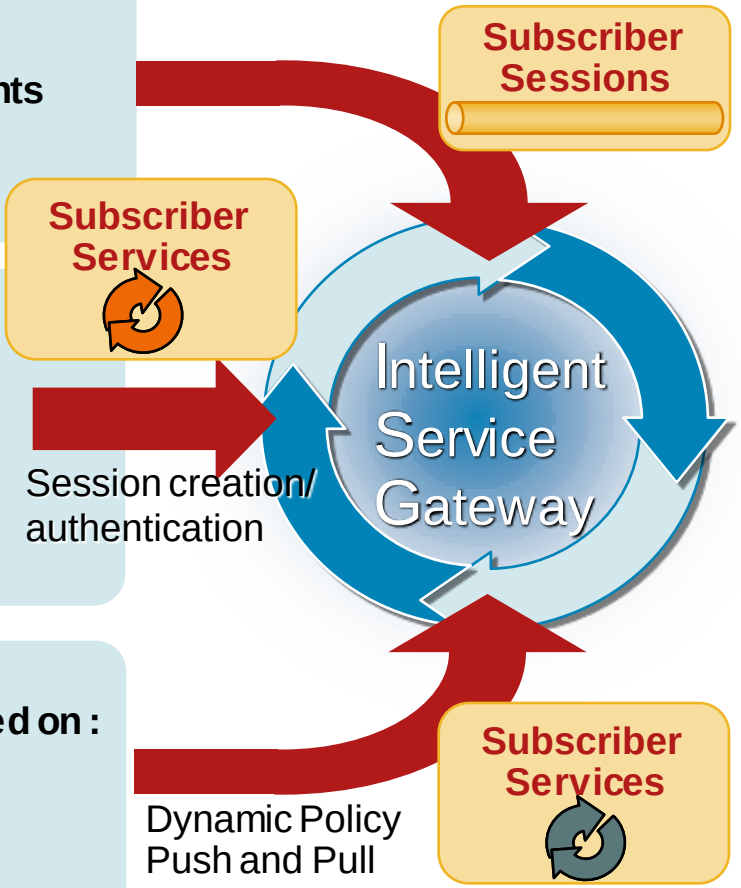
Different Services and Rules applied based on:

- **Who subscriber is**
- **Where he is**
- **What he requires**

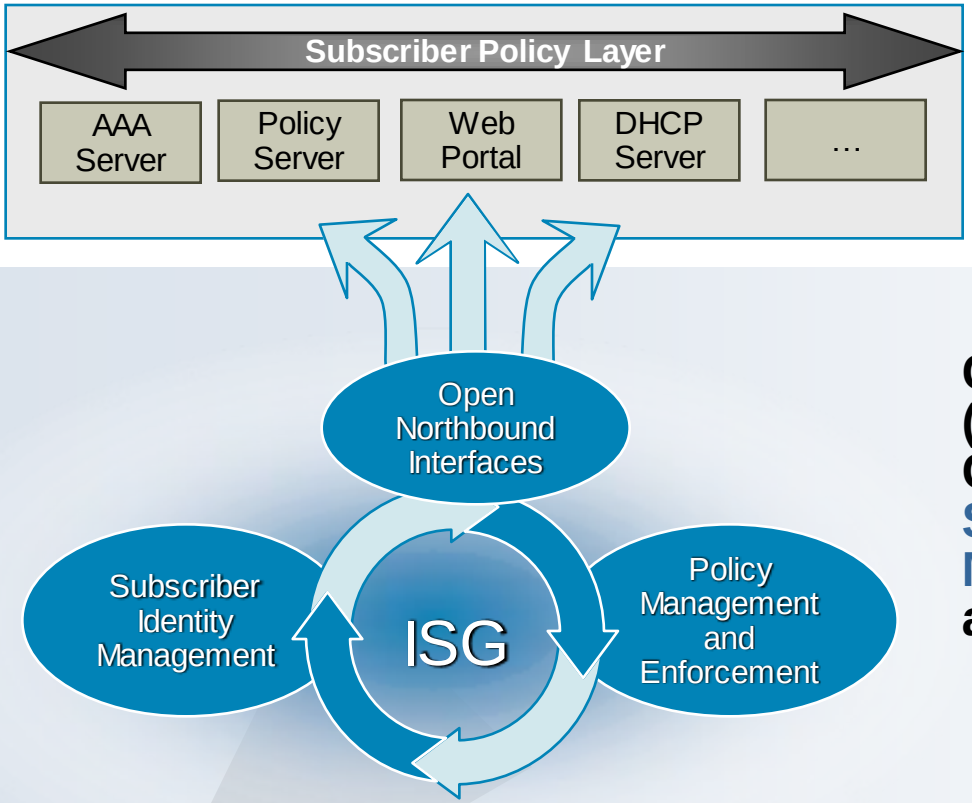
Dynamic Service Management

Services and Rules updated based on :

- **How subscriber behaves**
- **What he requires NOW**



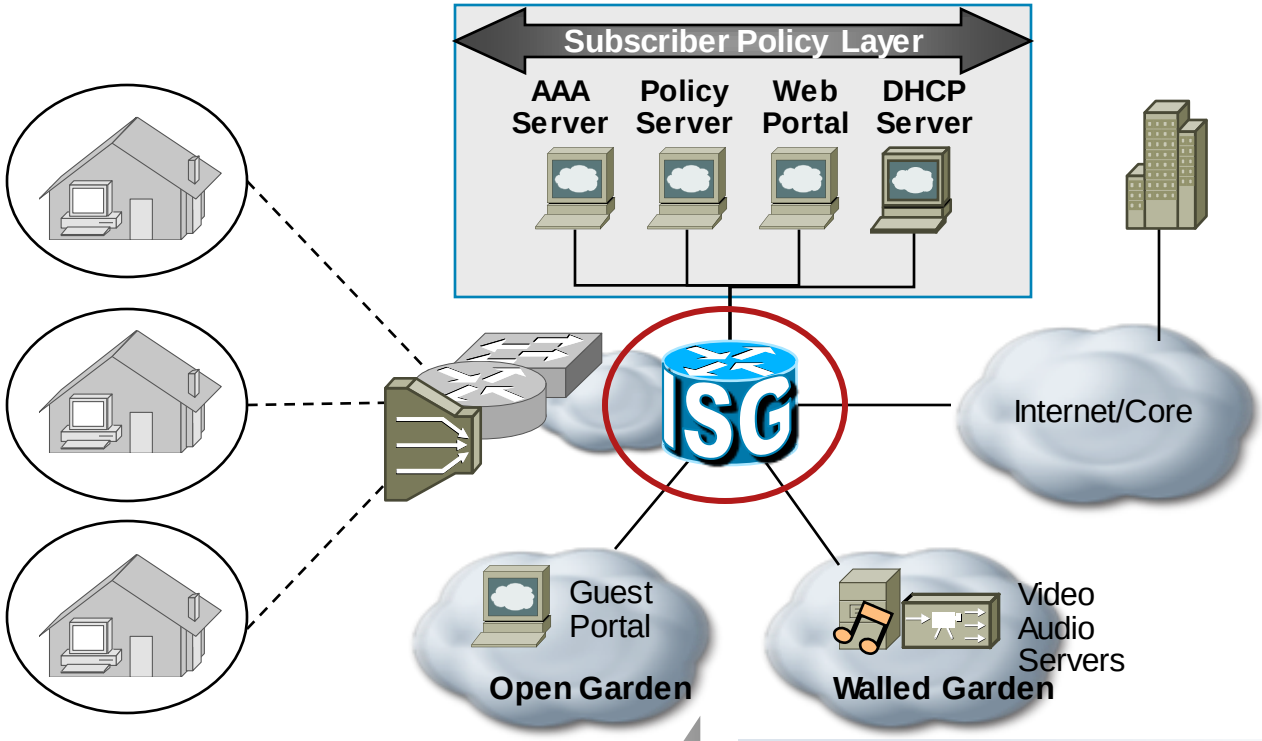
What Is ISG?



Cisco Intelligent Services Gateway (ISG) is a licensed feature set on Cisco Routers that provides Session Management and Policy Management services to a variety of access networks

So focal, that the entire device is often referred as an: Intelligent Service Gateway router or simply "The ISG"

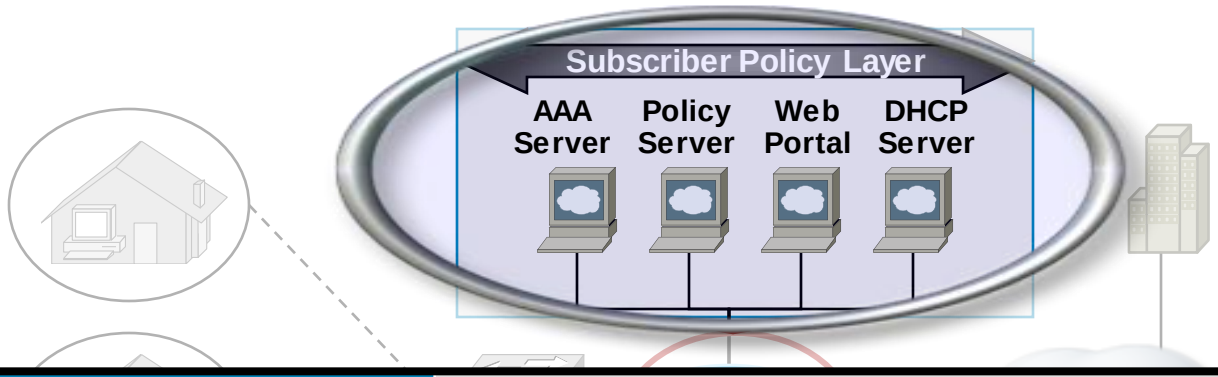
ISG's Place in the Network



- Sits at the edge of the network
- Communicates with other devices to control all aspects of subscriber access in the network
- Single point of contact

- **Subscriber Identification**
- **Subscriber Authentication**
- **Subscriber Services Determination and Enforcement**
- **Dynamic Service update**
- **Per access and per service accounting**

ISG's Subscriber Policy Layer

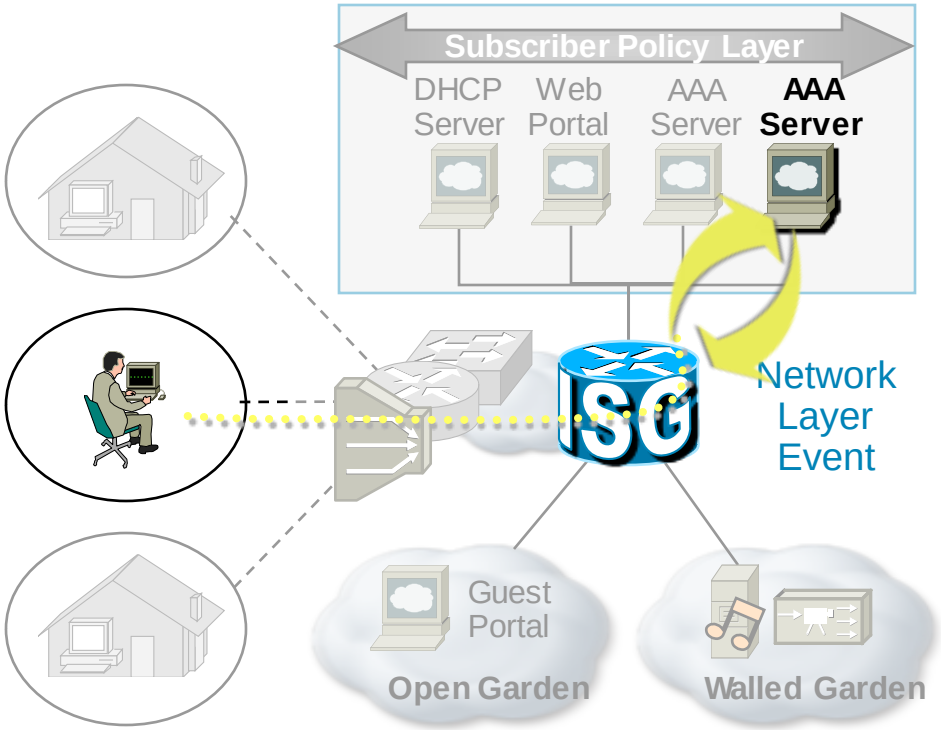


AAA Server	Subscriber Authentication Subscriber Authorization: User and Service Profile Repository Per access and Per Service Accounting Front-end toward billing system
Policy Server	Dynamic Policy Push (Application Level Trigger)
Web Portal	Front end toward the subscriber for: Self Subscription Web Logon Service Selection (Application Level Trigger)
DHCP Server	Hand over of addresses to subscribers Class-based address handover for ISG driven address pool selection

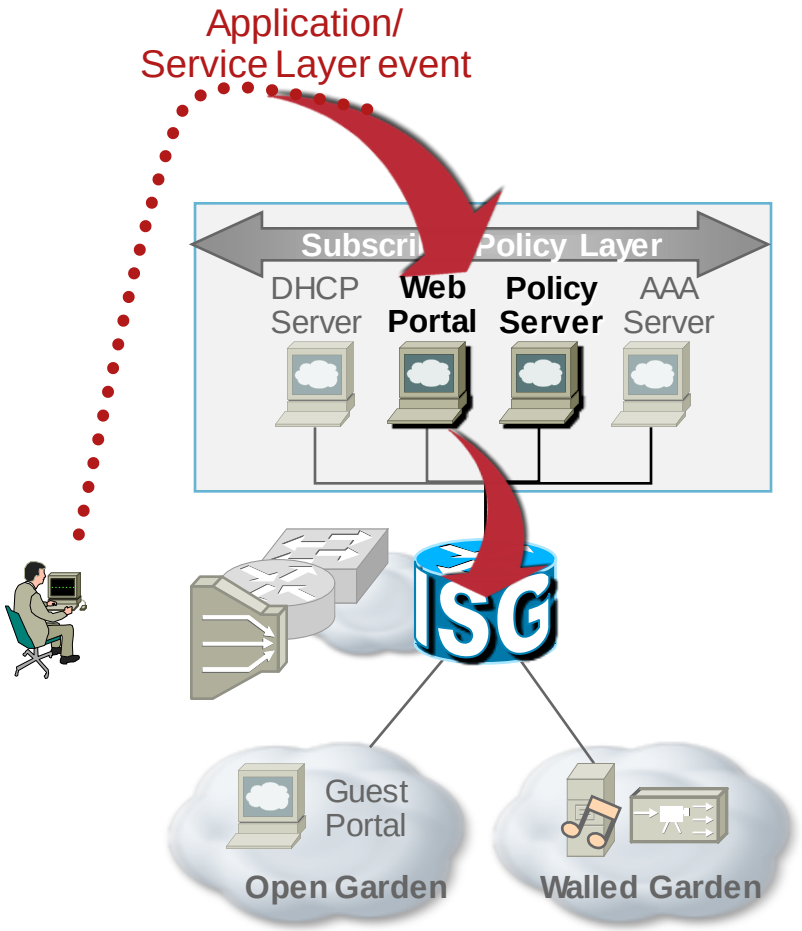
AAA Server, Policy Server, Web Portal can co-reside in the same appliance

ISG's Dynamic Policy Activation

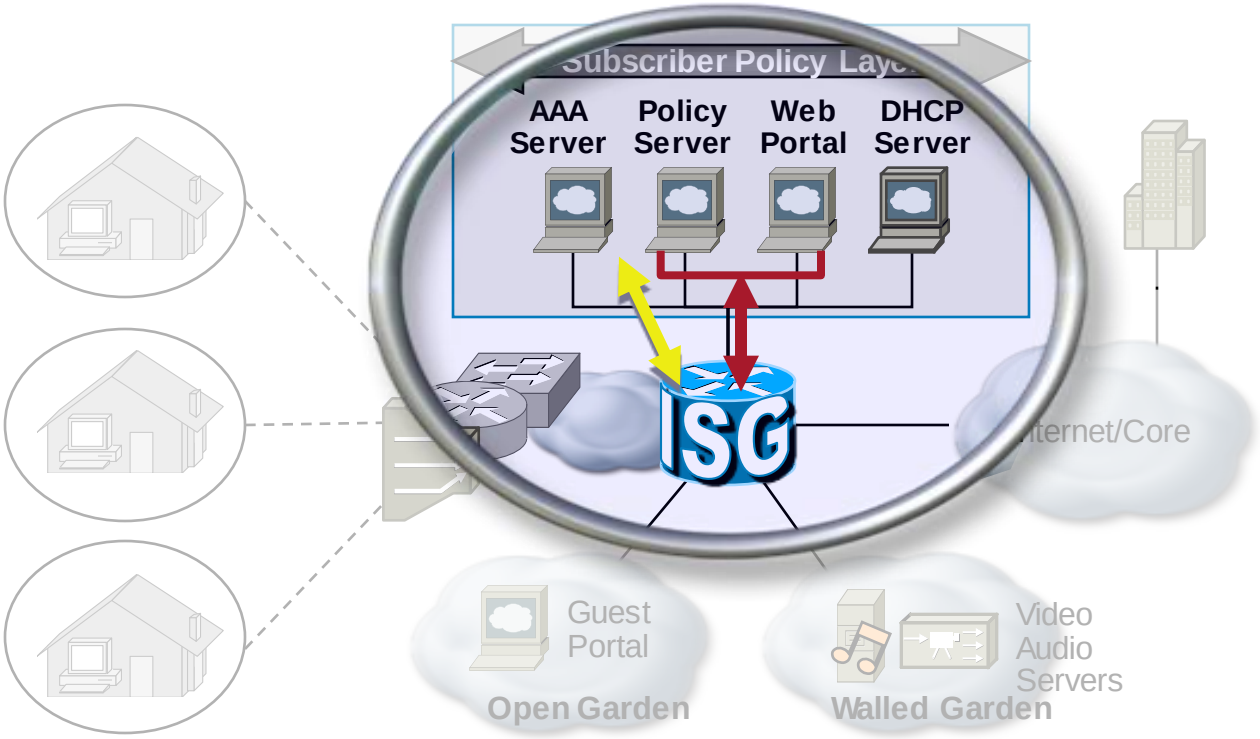
Dynamic Policy pull
(e.g. Automatic Service-Profile Download on Session Establishment)



Dynamic Policy push
(e.g. "Turbo Button")



ISG's Northbound Interfaces



RADIUS Interface, for subscriber AAA functionalities and service download

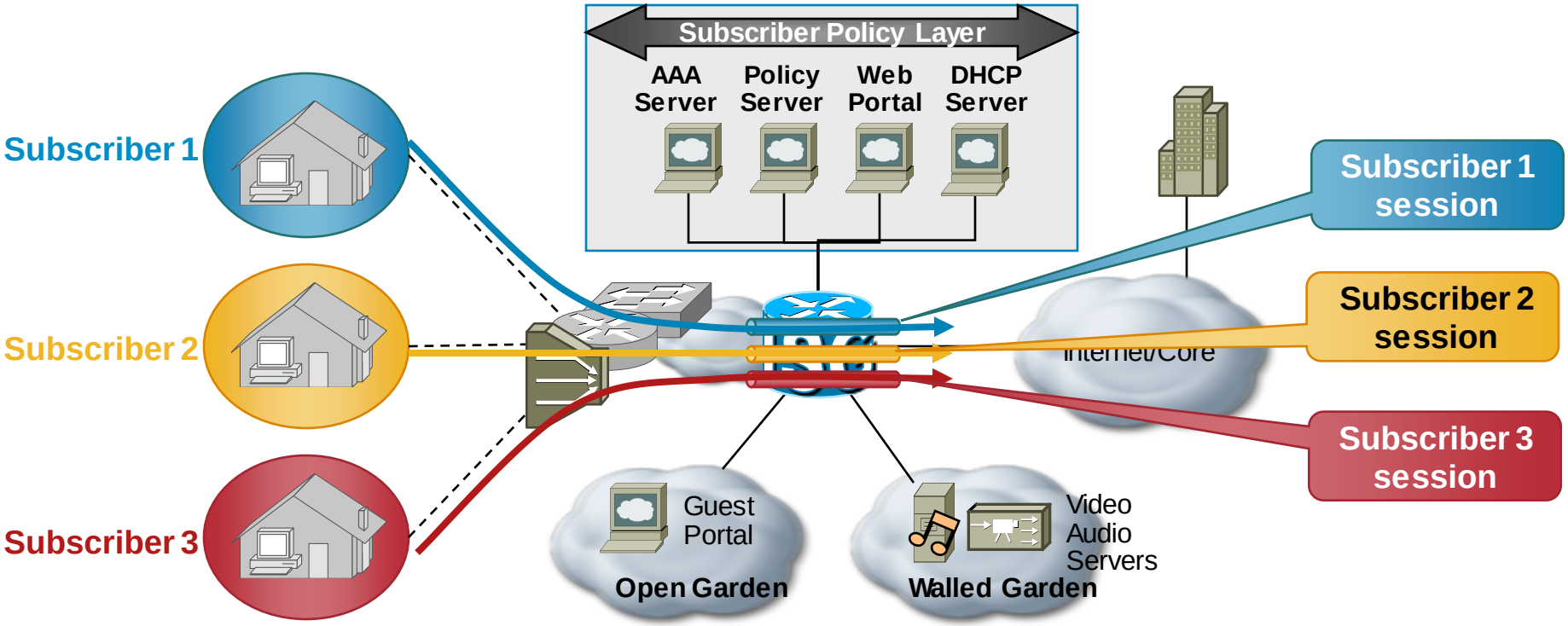
Policy PULL

RADIUS Extensions (**RFC 3576**) and **XML** based (**SGI**(*)) **Open Interfaces**, for dynamic, administrator or subscriber driven, session and service management functions

Policy PUSH

(*) SGI: Service Gateway Interface

The Subscriber Session in ISG

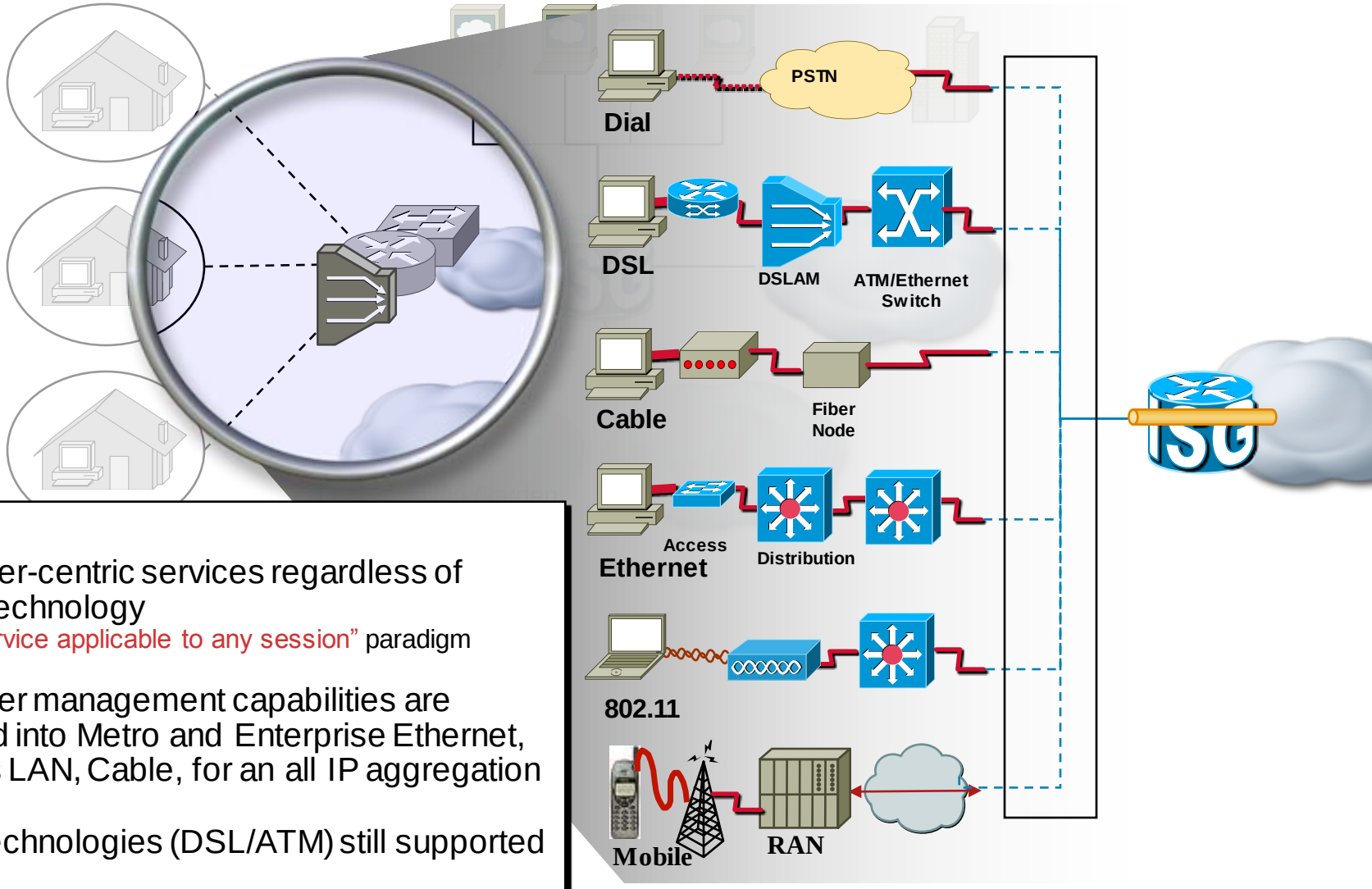


- Construct within Cisco IOS that represents a subscriber

  subscriber: billable entity and/or an entity that should be authenticated/authorize

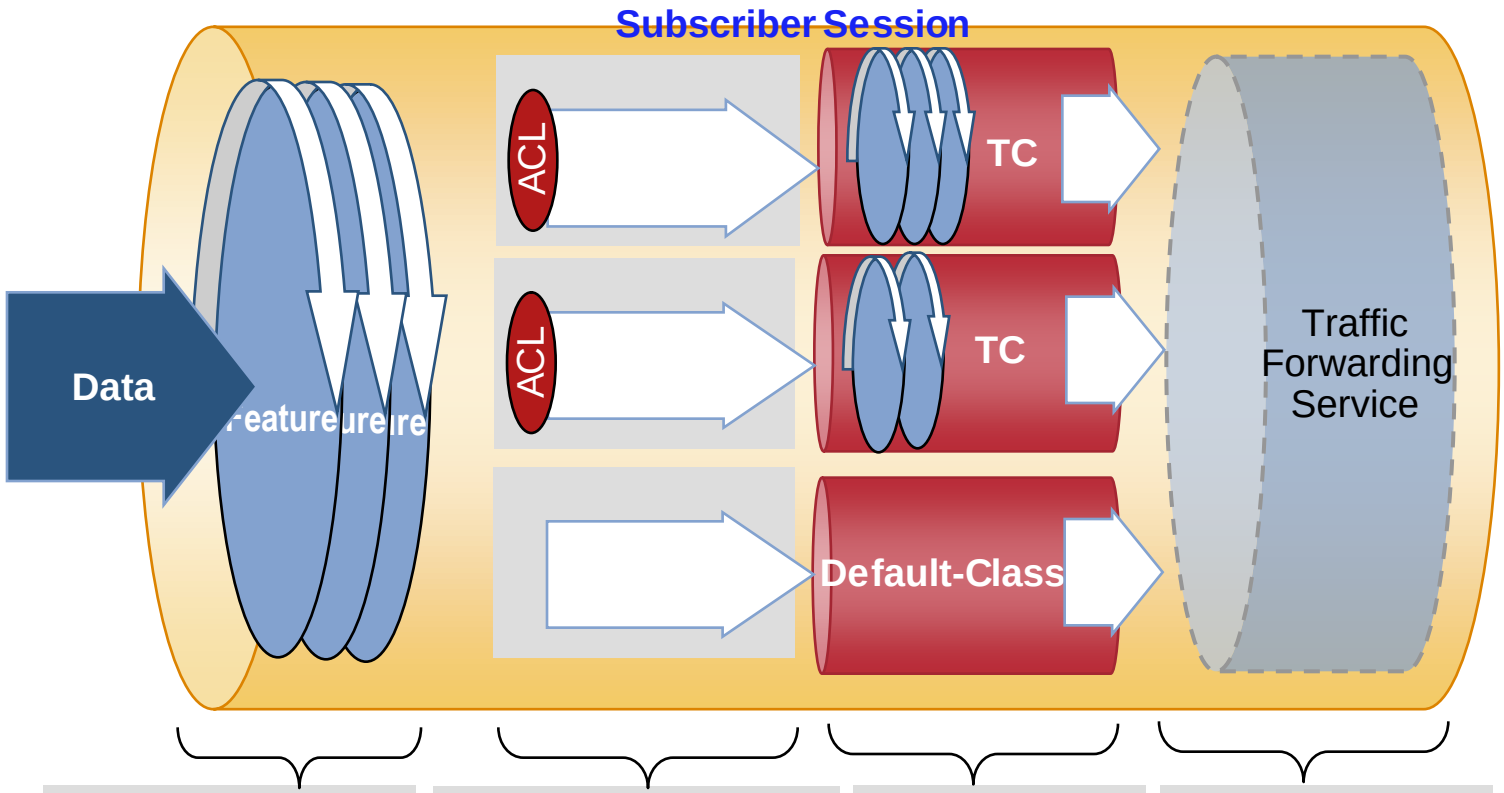
- Common context on which services are activated
- Created at first sign of peer activity (**FSOL** = First Sign Of Life)

ISG's Access Technology Abstraction



- subscriber-centric services regardless of access technology
  "any service applicable to any session" paradigm
- subscriber management capabilities are extended into Metro and Enterprise Ethernet, Wireless LAN, Cable, for an all IP aggregation
- legacy technologies (DSL/ATM) still supported

ISG Subscriber Session Data Plane



Session-Features: Apply to the entire session e.g. per-user-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)

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

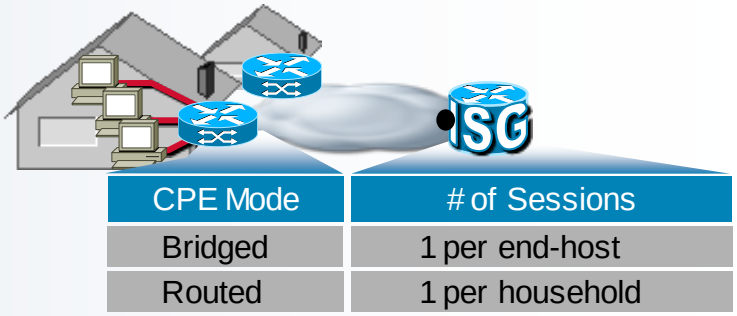
ISG Session Types

- Based on Subscriber Access Protocol not Technology
- Session typologies:

Dynamically Created Sessions:

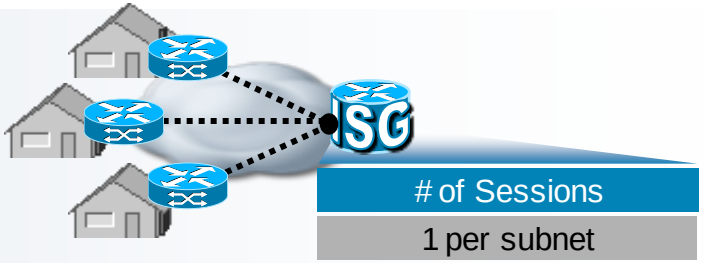
PPP sessions

IP Sessions



IP "Subnet" Sessions

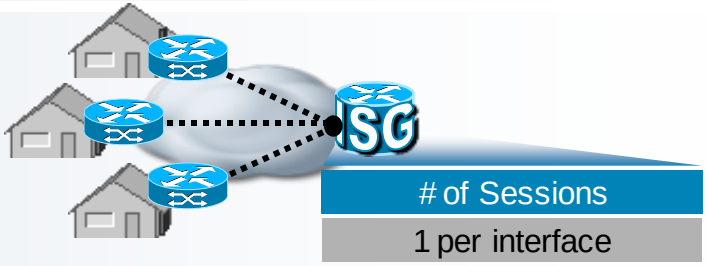
- Subscriber "Subnet" membership determined during authentication
- Authentication mandatory for subnet sessions



Statically Created Sessions:

Interface Sessions–

IP based access only

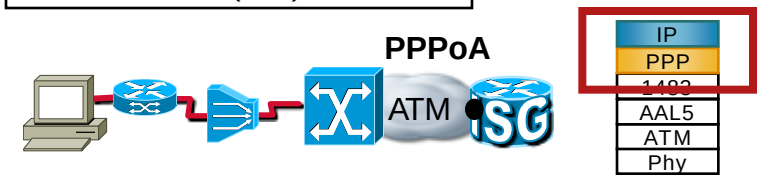


Subscriber Dynamic Sessions

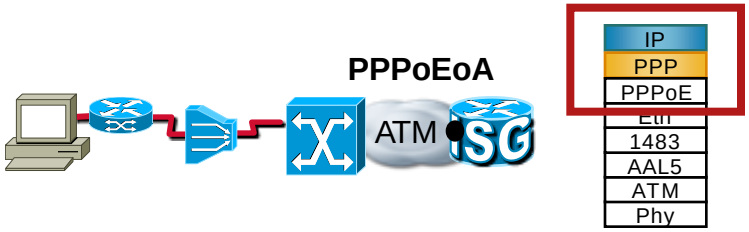
PPP Sessions

Virtual Template w/
Virtual Access (sub)Interfaces

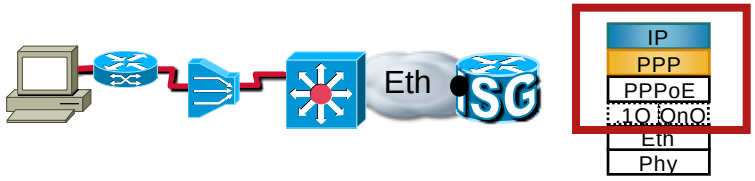
PPPoA



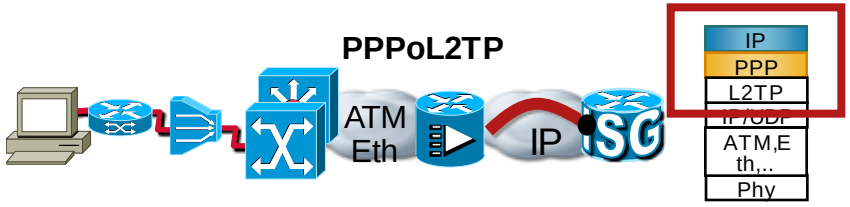
PPPoEoA



PPPoEoE / PPPoEoVLAN/PPPoEoQnQ

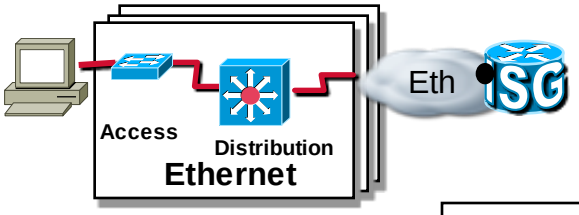


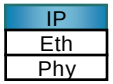
PPPoL2TP



IP Sessions

IP–Layer2 Connected

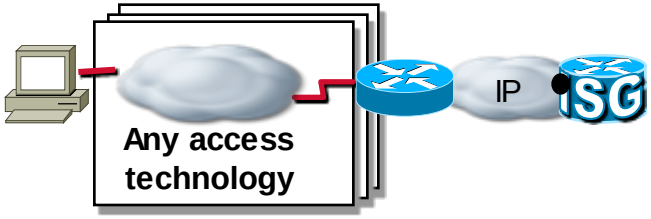


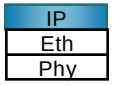


Native IP capable transport technologies
802.11, 802.16

802.3 based main intfes
Subinterfaces: .1q, QnQ

IP–Routed

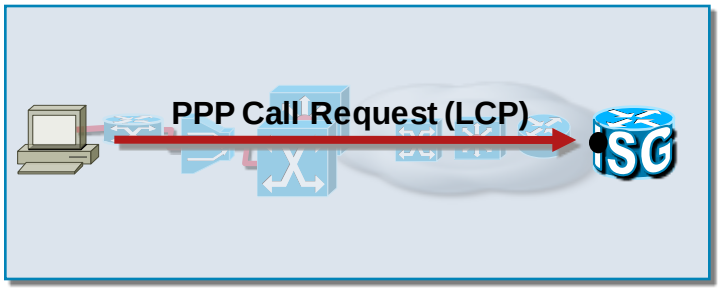




Dynamic Session Initiation

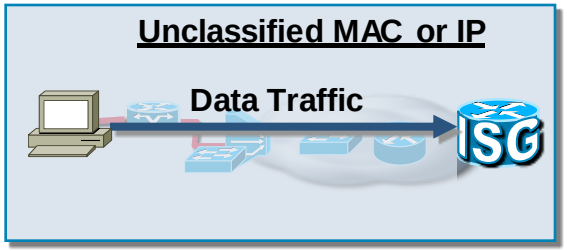
- ISG sessions are initiated at the First Sign of Life (FSOL)
- FSOL depends on the Session Type

PPP Sessions - FSOL

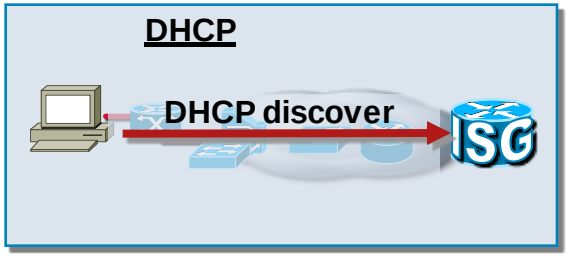


IP Sessions - FSOL

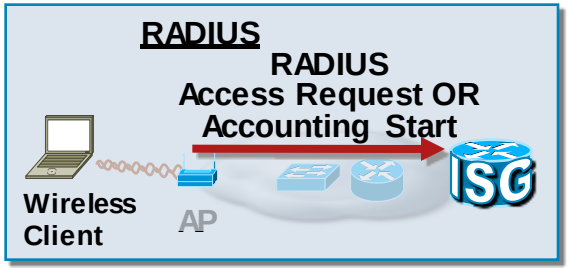
.... there are options .....



- IP packet with unknown MAC or IP source address
  - Use MAC for L2-connected IP sessions
  - Use IP for routed IP sessions



- DHCP Discover message
- ISG must be DHCP Relay or Server



- RADIUS Access/Accnt Start
- ISG must be a Radius Proxy
- Typically used in PWLAN and WiMAX environments

Session Authentication

Authentication: Allow Access to Network Resources Only to Recognized Users

Authentication models supported:

- **Access Protocol Native Authentication**:

  PPP: CHAP/PAP

  IP: EAP for wireless client

- **Transparent Auto Logon (TAL):**

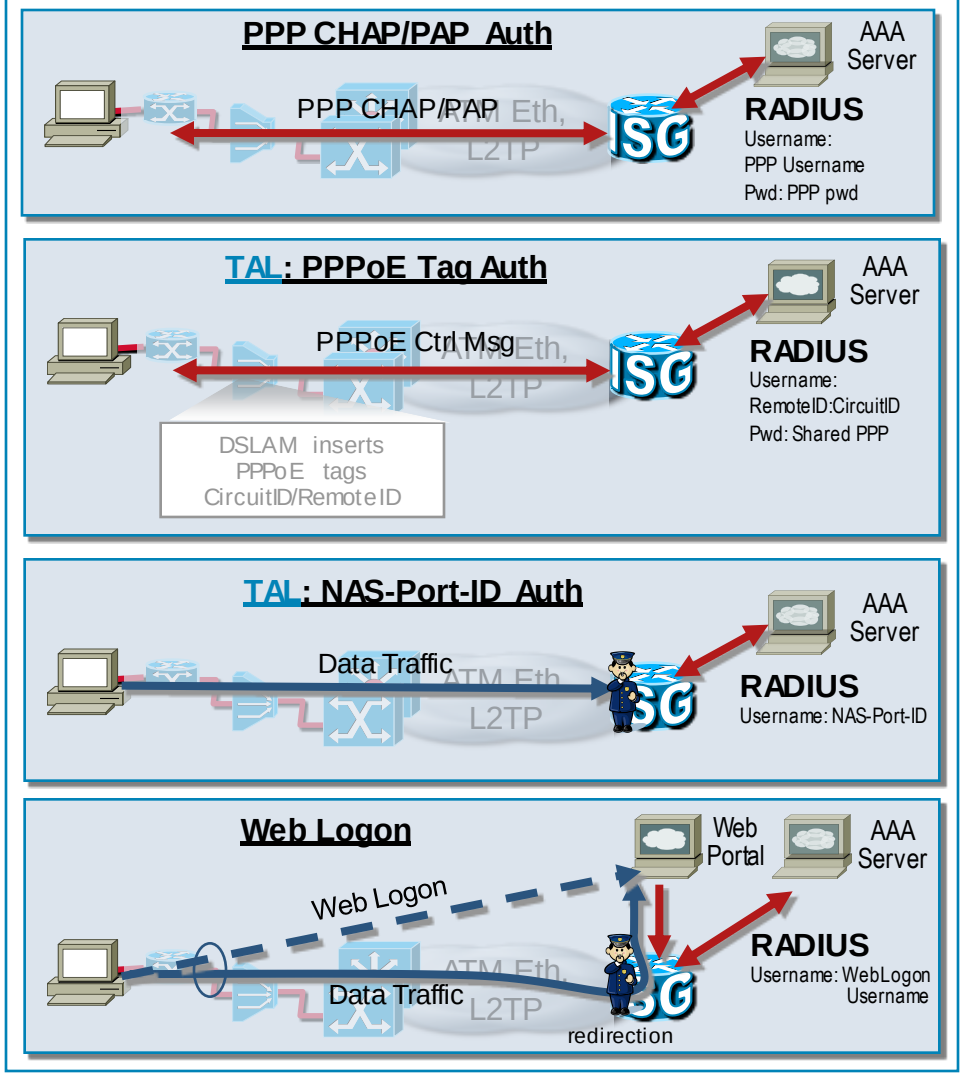
  Authenticates using network identifiers. Typically "subscriber traffic" related identifiers

- **Web Logon**

Authentication is not mandatory on a session, but used in most situations

Session Authentication—PPP

PPP - common scenarios



- Uses legacy PPP authentication protocols
- Applicable to all session types

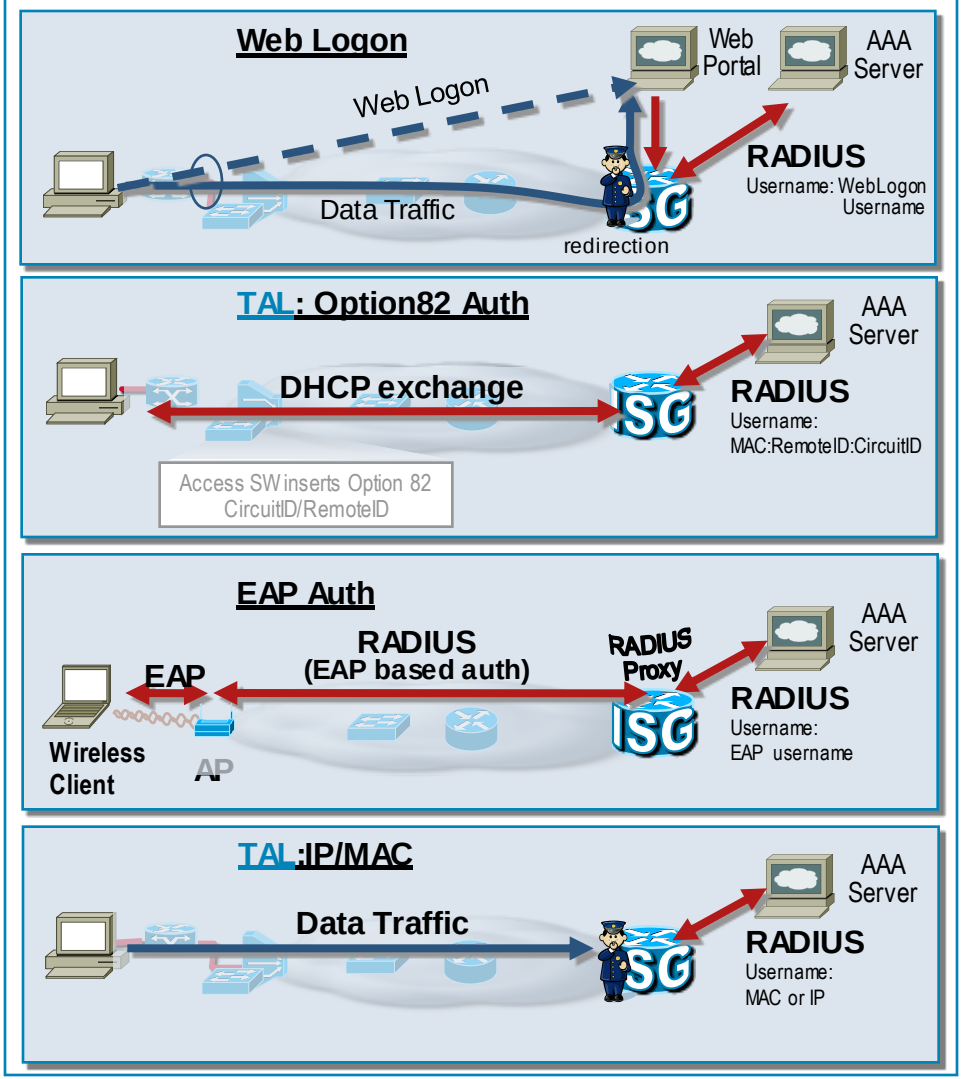
- DSLAM inserts PPPoE tags, typically Circuit and Remote ID
- ISG performs authentication using a combination of Circuit and RemoteID as username
- Only available for PPPoE sessions

- ISG performs authentication using NAS-PortID as username
- Typically used w/ PPPoA and PPPoEoQnQ where a single subscriber is associated to VC/subif

- User traffic redirected to a Web Portal to enter credentials (username and password)
- User Credentials propagated to ISG
- ISG uses credentials to authenticate user with AAA
- Applicable to all session types

Session Authentication—IP

IP – common scenarios



- User traffic redirected to Web Portal to enter credentials
- User Credentials propagated to the ISG
- ISG uses credentials to authenticate user with AAA server
- Applicable to all session types

- Access Switch inserts Option82 Circuit and Remote ID in DHCP Requests
- ISG performs authentication using a combination of Circuit and RemoteID as username
- ISG session must be DHCP initiated

- User starts EAP authentication with Access Point (AP)
- ISG impersonates RADIUS server toward AP and RADIUS client toward real server
- ISG learns session authentication status by proxying RADIUS messages betw/ real RADIUS client and Server
- ISG session must be RADIUS initiated

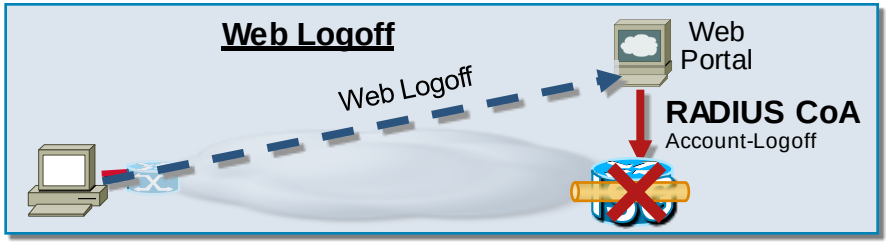
- ISG performs authentication using identifiers from subscriber traffic (source IP/MAC)
- Typically used in IP-L2 connected topologies to support clients w/ static IP address or in IP-routed topologies

Session Termination

IP and PPP Sessions

Idle and Absolute Timeouts/Timer Expiry

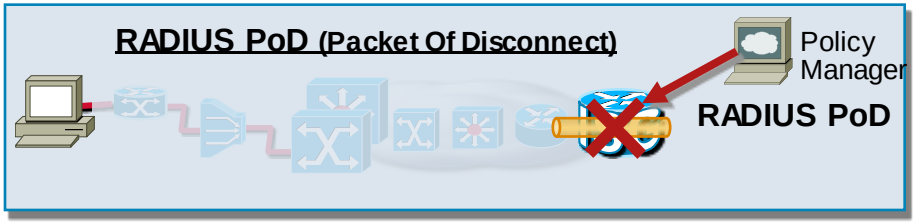
Web Logoff



PPP Sessions Exclusively

PPP and PPPoX protocol events

RADIUS PoD (Packet Of Disconnect)

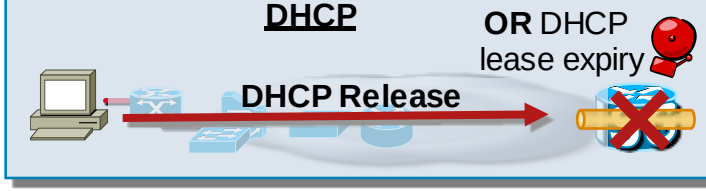


IP Sessions Exclusively

ICMP/ARP keepalive failure

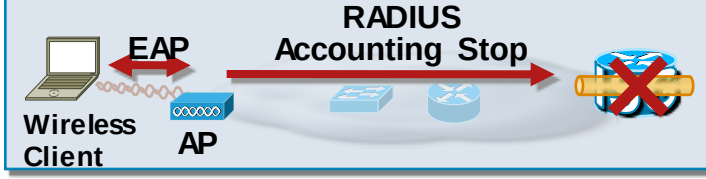
ICMP Keepalives used to terminate routed sessions
ARP keepalives used to terminate l2-connected sessions

DHCP



DHCP initiated sessions only

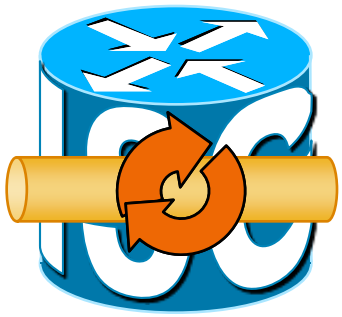
RADIUS



RADIUS initiated sessions only

ISG Services

Service: a collection of features that are applicable on a subscriber session Service = {feat.1, feat.2,...,feat.n}

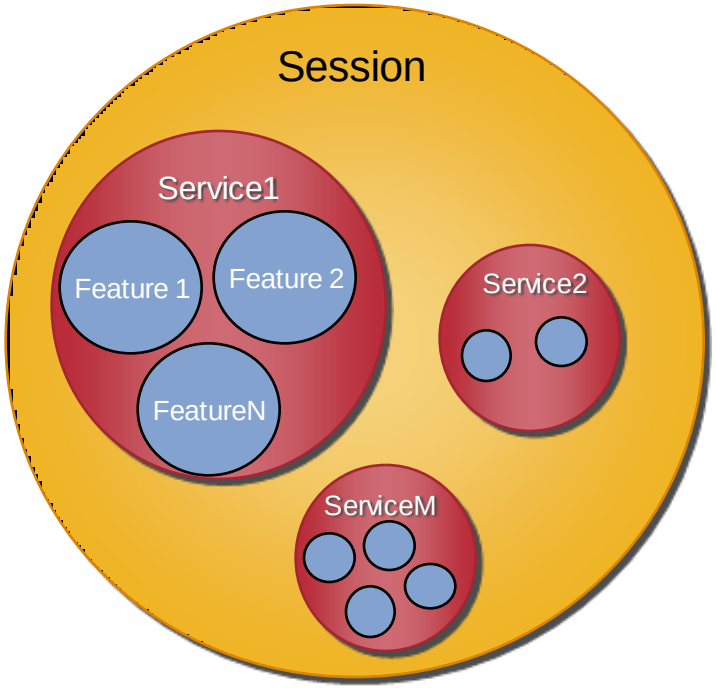


Features		
	Session Administration	Portbundle (PBHK) Keepalives: ICMP and ARP based Timeouts: Idle, Absolute
	Traffic Conditioning	QoS: Policing, MQC Security: Per User ACLs
	Traffic Forwarding Control	Subscriber Address Assignment Control Redirection: Initial, Permanent, Periodic VRF assignment: Initial, Transfer L2TP assignment
	Traffic Accounting	PostPaid Prepaid: Time/Volume based Tariff Switching Interim Broadcast

Associated to **Primary Services**

Primary Service: contains one “traffic forwarding” feature and optionally other features. Only one primary service can be active on a sess.

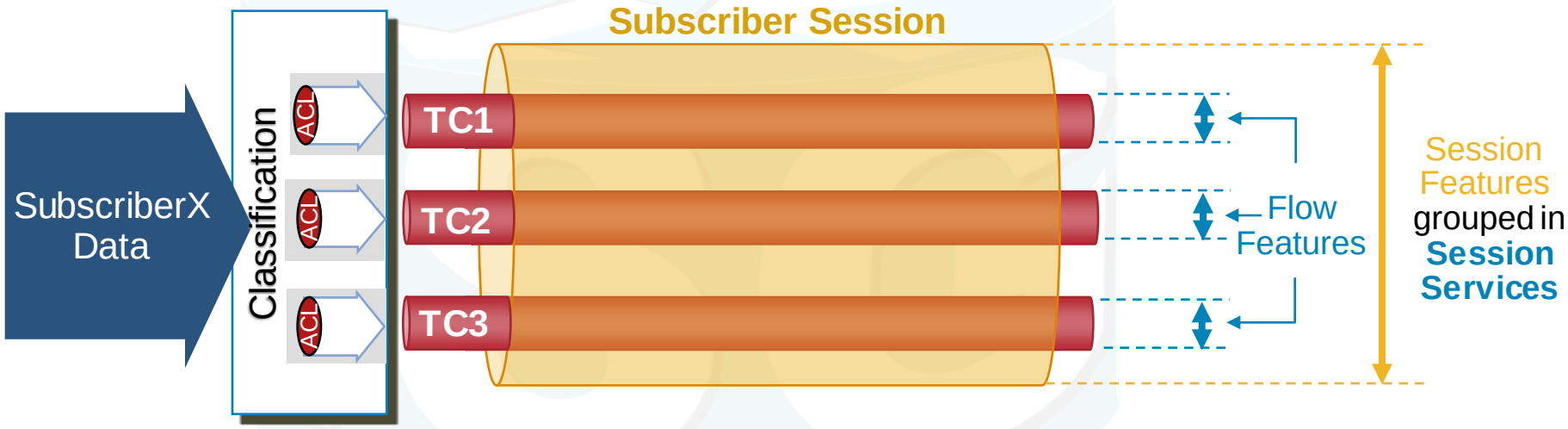
How Many Features in a Service? How Many Services on a Session?



- No limit in the number of features per service, however consider that:
  - A service is smallest atomic configuration unit that can be activated/deactivated on a session
  - Deactivating a service implies deactivating all associated features
- Not all features (and therefore services) are compatible w/ each other
- No limit in the number of services per session, however:
  - Only 1 primary service can be active at any given time on the session
  - Good Practice: Different services should have different set of features

ISG Feature Granularity

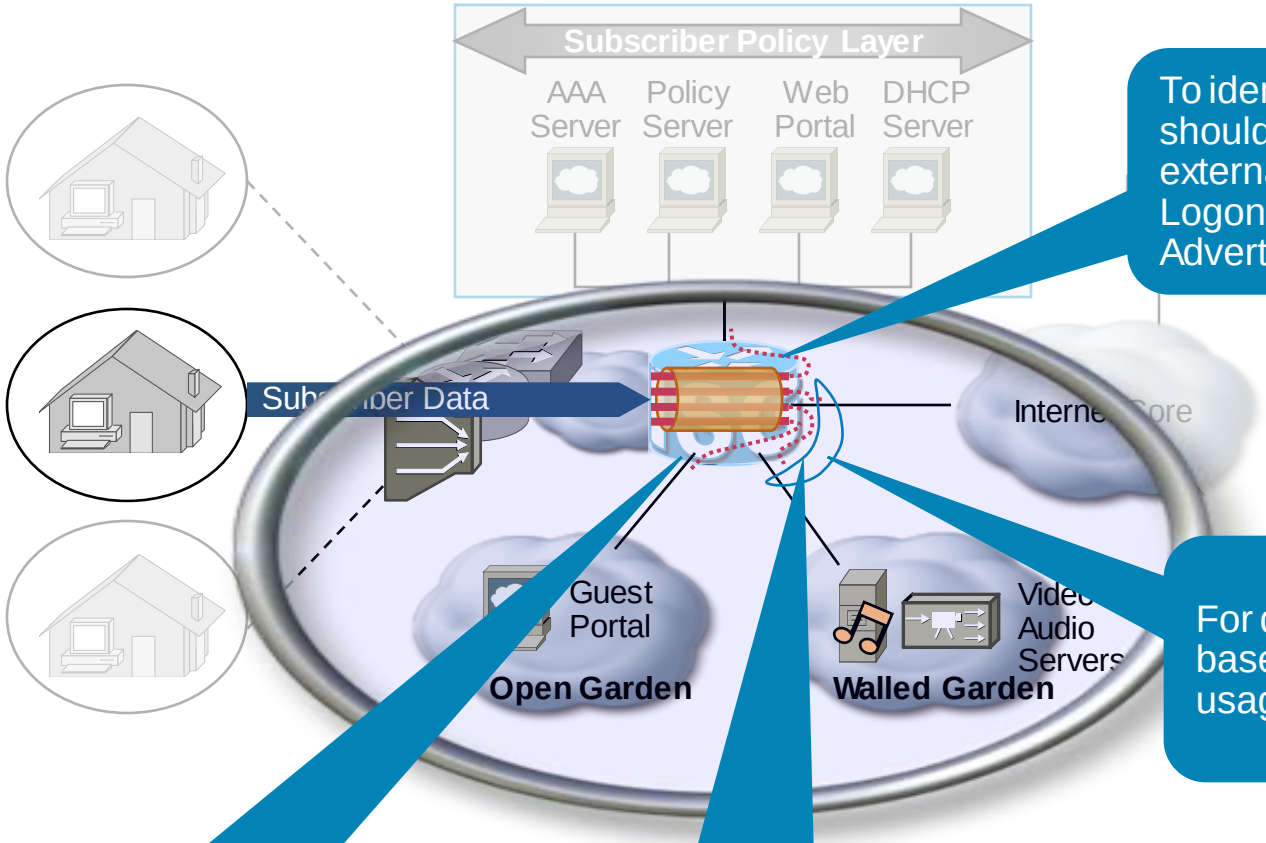
Per Session or Per Traffic Class (TC)?



- ISG Classification resembles Modular QoS CLI (MQC)
- Only traffic that can be identified via an IP ACL (standard or extended) can be classified

- Each Traffic Class can have a different set of features applied
- A Traffic Class and associated features also referred as TC service
- A Default TC can be used to drop traffic that could not be classified

When Should I Use TC Services?



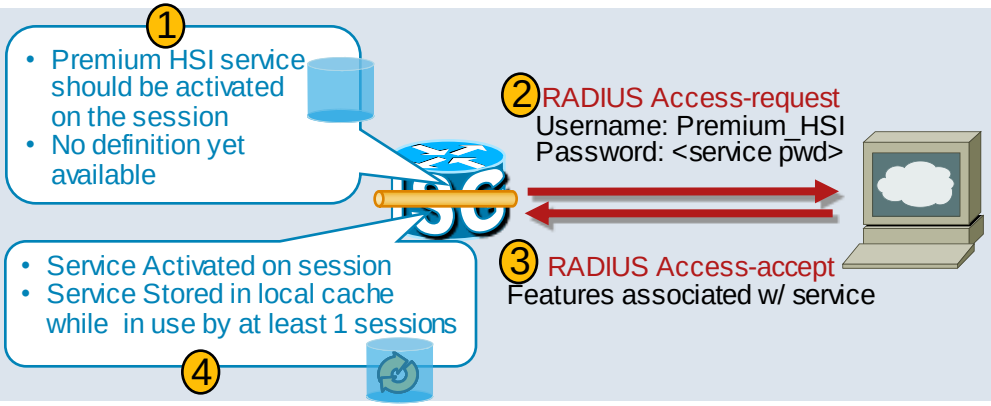
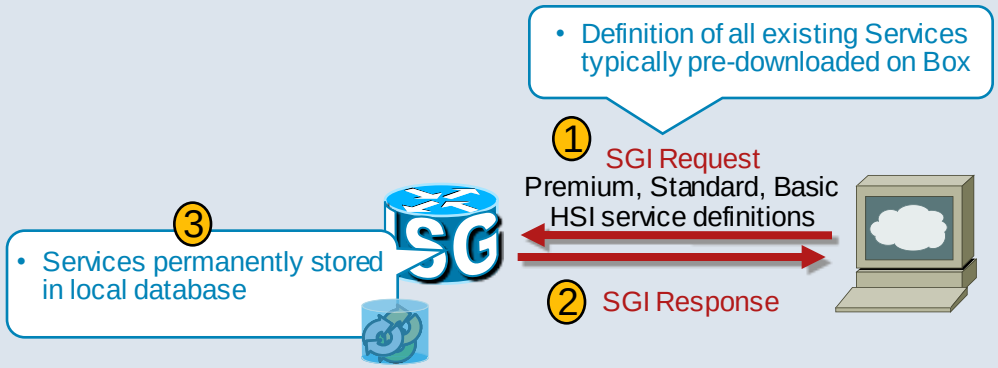
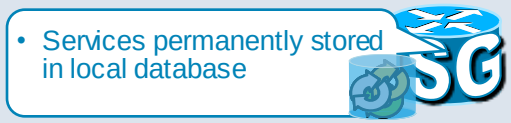
To identify what traffic should be redirected to an external appliance (Web Logon, Periodic Advertisement)

For differentiated billing based on application usage

To permit Open Garden traffic over an unauthenticated session while dropping all other traffic (default drop)

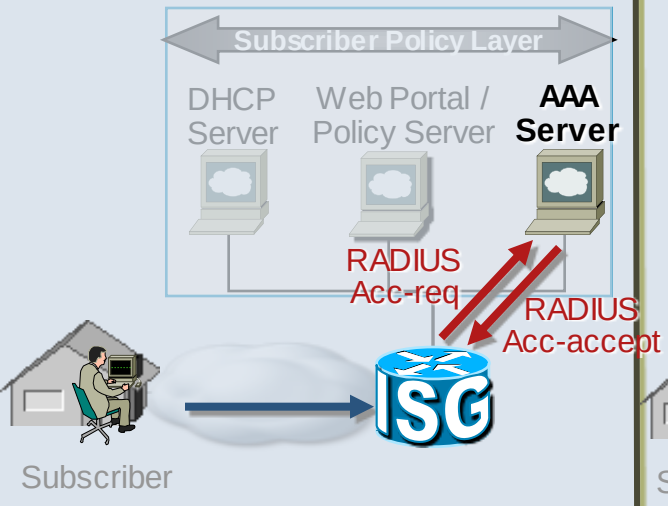
To offer different QoS levels to different flows

Defining Services

	Location	Download
	**AAA Server** • Services defined in **Service Profiles** • Standard and Vendor Specific RADIUS attributes used • On demand download on a need basis	
	**Policy Manager** **(supporting the SGI Interface)** • Services defined in XML • Pre-download of all existing services	
	**ISG** • Services pre-configured using CLI • Services defined on **Service Policies:** policy-map type service <name>	

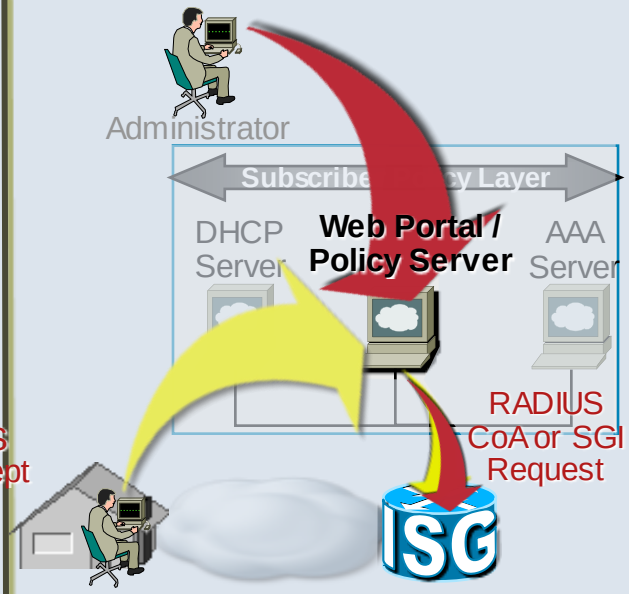
How Services Are Activated on a Session?

During Subscriber Authentication/ Authorization



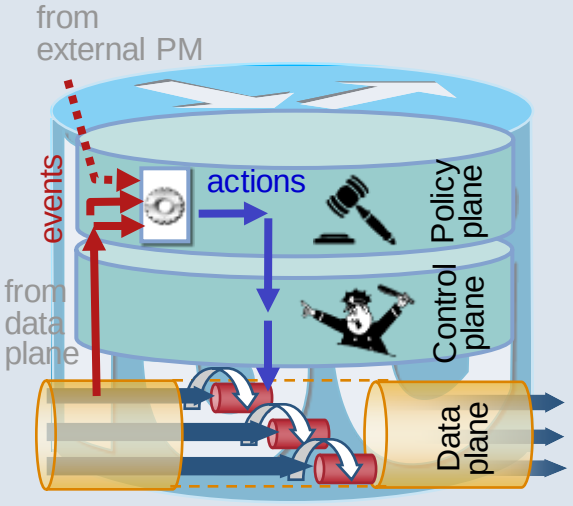
- Subscriber is successfully authenticated
- RADIUS Response includes Services and Features to activate on Session (from UserProfile)

Via an external Policy Server/Web Portal



- Service Activation request sent by External Policy Managers via a RADIUS CoA or a SGI Request message

Via the On-Box Policy Manager

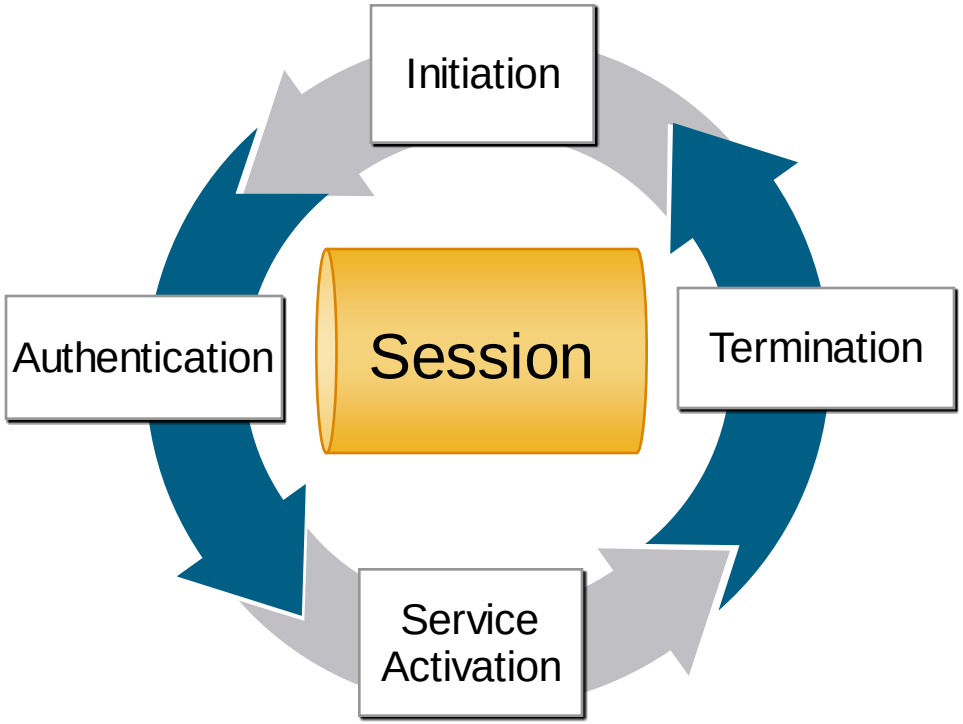


- **Policy Plane** determines what **actions** to take on session based on **events**

  actions *include* applying a service
- **Control Plane** ensures actions are taken –i.e. provisions the data plane
- **Data Plane** enforces traffic conditioning policies to the session

The On-Box Policy Manager (PM)

Handles all aspects of subscriber session lifecycle
not just Service Activation!



Session Life Cycle

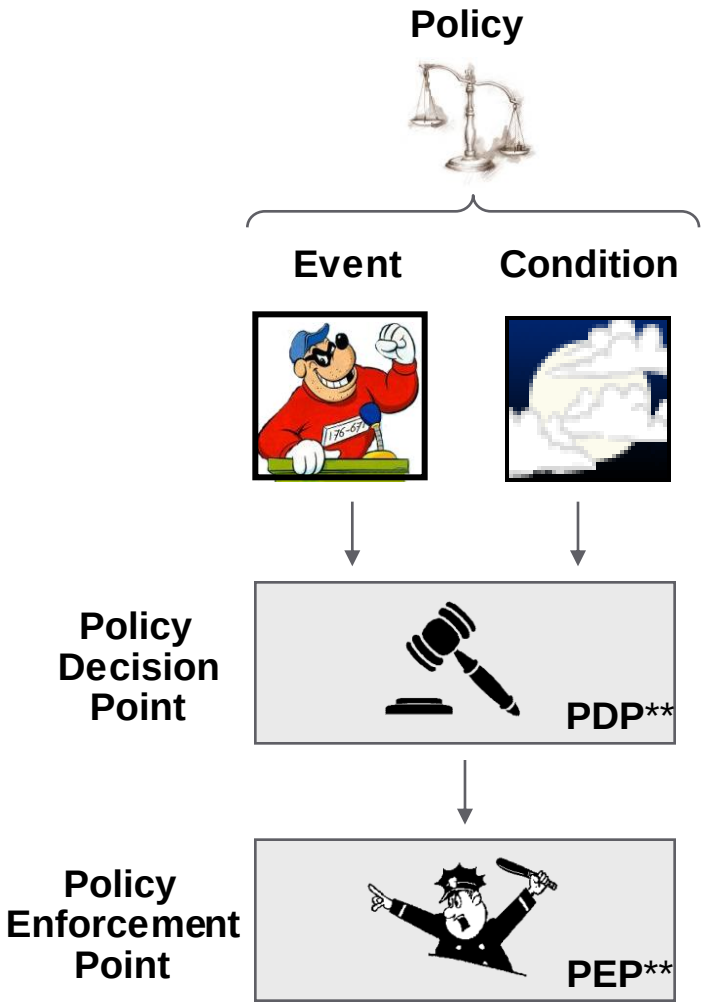
described using

Cisco Policy Language

Through CPL and the On-Box PM
ISG is not only a Policy Enforcement Point (PEP)
it is also a Policy Decision Point (PDP)

Customize and Control: Policy
Definition and Nomenclature

- **Policy**: Set of rules which govern the choices in behavior of a system and that are comprised of conditions and actions, where conditions are evaluated when triggered by an event.*
- **Traffic policies**: Policies for which the execution trigger is the arrival of a data packet, and for which the action(s) constitutes some form of processing of this packet before it is forwarded to another device, are known as traffic policies.*
- **Control policies**: Policies for which the execution trigger is an explicit control-plane event (e.g. a signaling event, a timer expiry event etc.), and for which the action(s) does not entail the processing of a forwarded data packet, are known as control policies.*



*Source: Draft ETSI TS 182 019; **PEP, PDP: See RFC2753

Cisco Policy Language CLI

Control policy-map	Conditional class of events	Actions
policy-map type control *<name>*	event1 class type control *<conditions>* event *<event type>* event2 more events	action1 action2 more actions for event

Typically applied on interface

Defines all aspects of session processing

Events are identified by their event type

Common event types:

- Session-start: New session detected
- Account-logon: Account-Logon msg. received from external source
- Service-start: new service start req. from external source
- Service-stop: Service termination req. from external source
- Timed-policy-expiry: Set Timer expired

Event actions are executed only if <conditions> are met for the event

- Multiple instances of same event w/ unique condition
- Different set of actions for same event type
- Conditions account for other aspects surrounding the event

Actions are in a ordered list

Different set of actions per {event, condition}

Common action types:

- Service: Used to start a new service
- Service Unapply: Used to terminate an active service
- Authenticate: Used to authenticate a session using subscriber's credentials
- Authorize: Used to authenticate a session using one or more network identifiers (TAL)
- Set-Timer: Used to generate an event after a configured amount of time

Defining a Control Policy

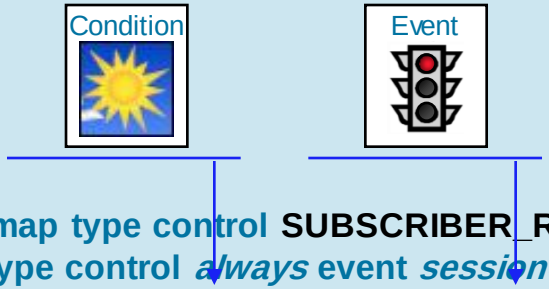
policy-map type control

Control Policy

Associate Events and Conditions to an ordered list of Actions

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 5
 !
 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
!
```

Network Access Services:

User Self-Care

Portal Based Self-Subscription with Re-Direction

Key Ingredient: **Cisco Intelligent Service Gateway - ISG**

User Self-Care
The "Zero-Touch" Network

- User Self Care is
  - Self-Subscription
  - Self-Management
  - Upgrade Services
  - Change Account attributes
  - Cruise Control
  - Sub-Account Creation
  - Parental Control
- User Self Care addresses
  - Streamline Network provisioning and User management
  - Reduce human intervention to Subscriber management to minimum
  - Increase customer loyalty and satisfaction
  - Provide easy and scalable way to up-sell services

User Self Subscription Example

One-Shot Authentication and Transparent Auto Logon

- User Self-Provisions himself at a portal (upon first access to the network)

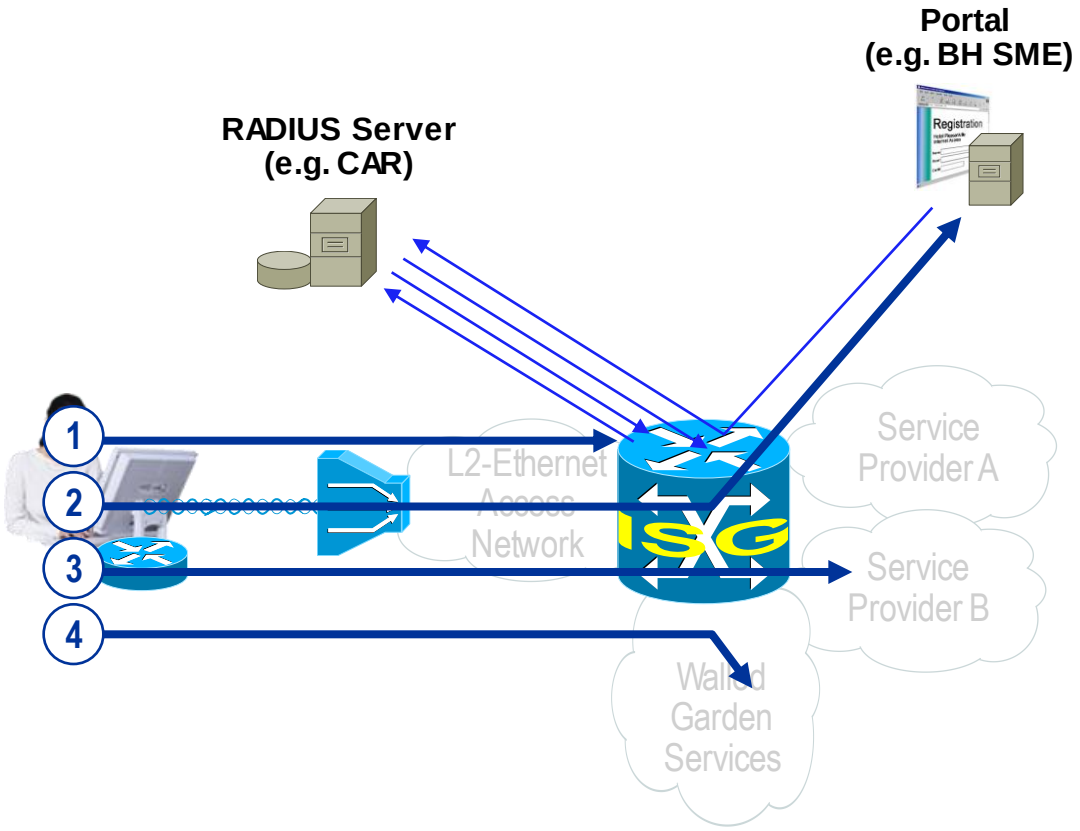
  Choose appropriate Service Provider and Service Portfolio

- Once Provisioned, transparent access to the network is granted without further authentication (Transparent Auto-Logon / Persistent Authentication)

- Can be combined with time or volume based Pre-Paid Services (e.g. only access the Internet for X minutes, or only transfer Y amount of data)

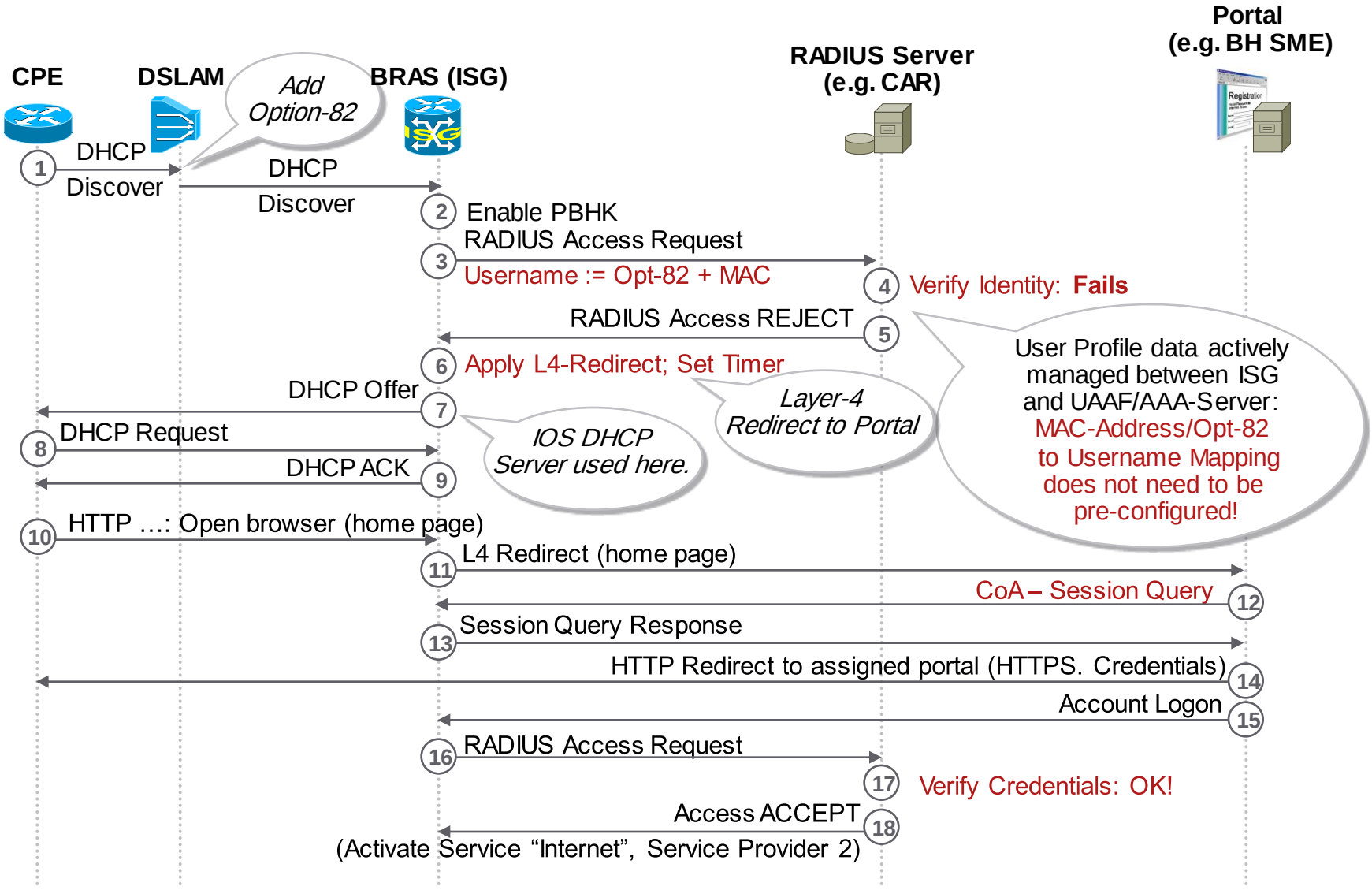
Generic Functional Reference Architecture

One-Shot Authentication and Transparent Auto Logon

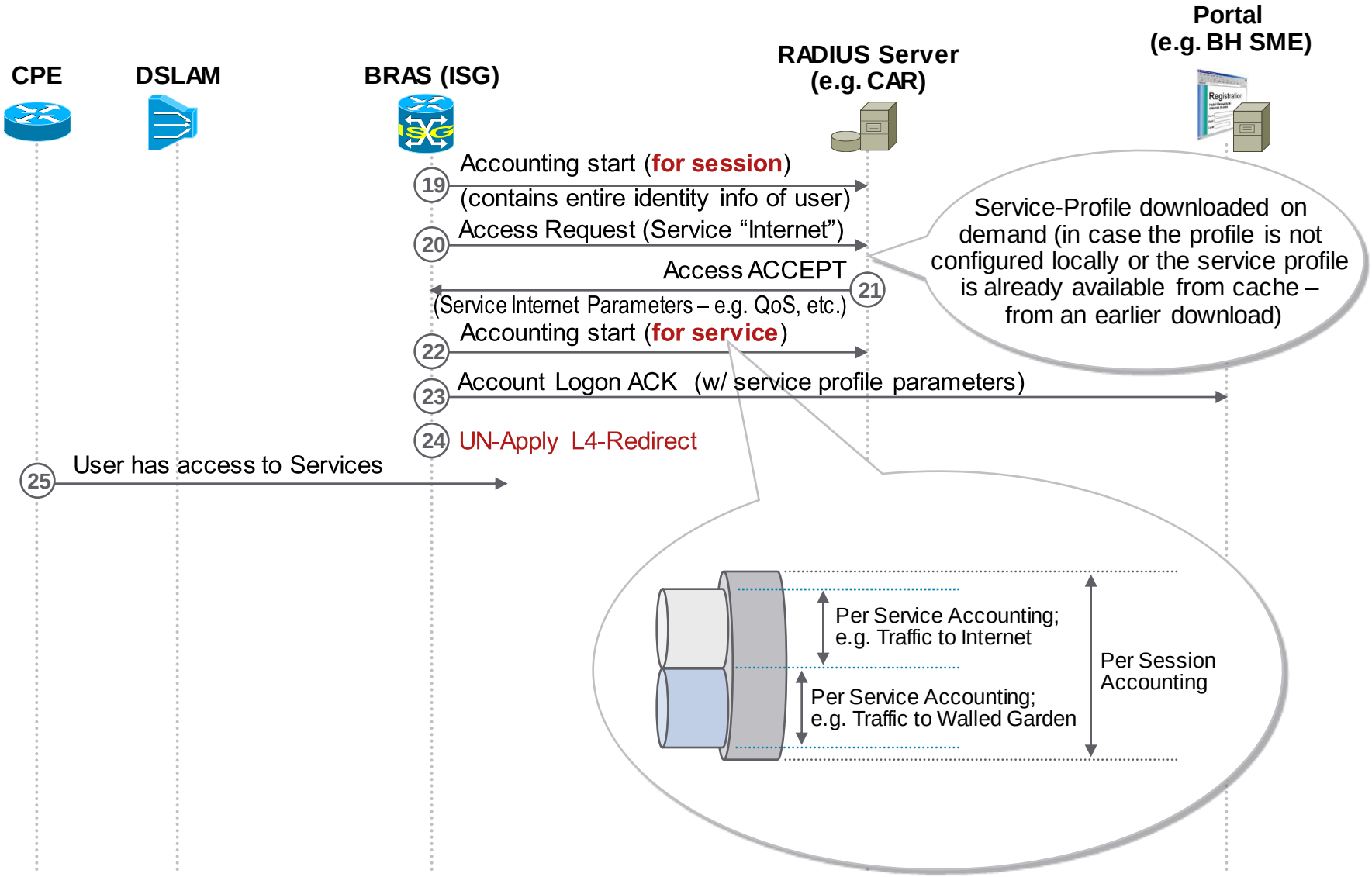


1. User connects to network. ISG identifies User with Line-ID and his MAC-Address. ISG tries to authorize User based on Line-ID and MAC-address, but fails initially (User still un-provisioned)
2. ISG redirects User to Portal. User self provisions himself and inputs his credentials. Portal passes credentials back to ISG and ISG initiates authentication of user via AAA. On success, ISG places User in VRF of SP B and allows full access to network. MAC-Address and Line-ID are saved – to allow for subsequent transparent login
3. User has full access to network. Next time user comes back, ISG will be able to authorize access to the network based on Line-ID and MAC.
4. User has used up quota (time or volume). ISG re-applies default service (e.g. access to Walled Garden only).

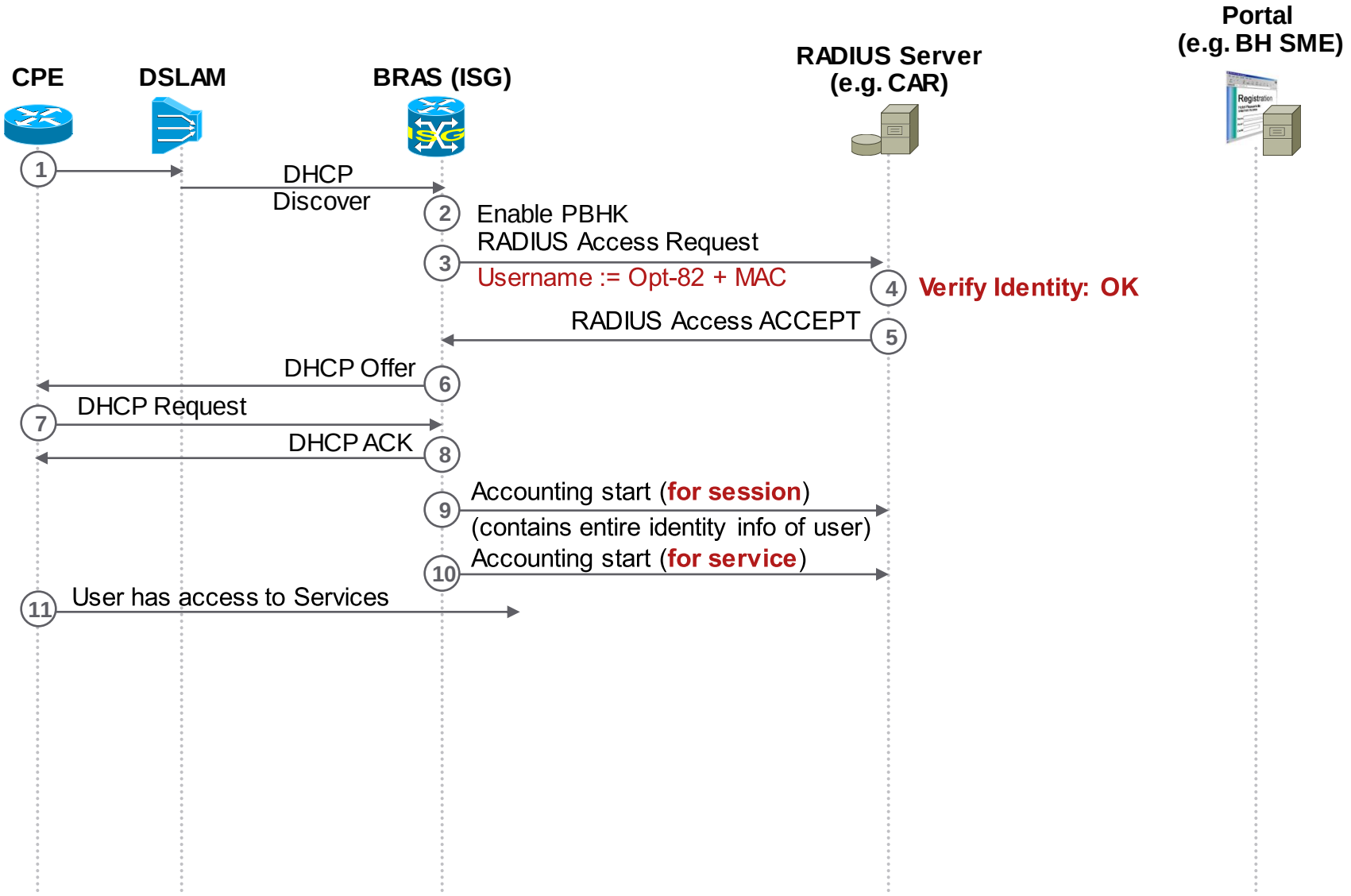
One-Shot Authentication and TAL
First Time Access—Call Flow (1/2)



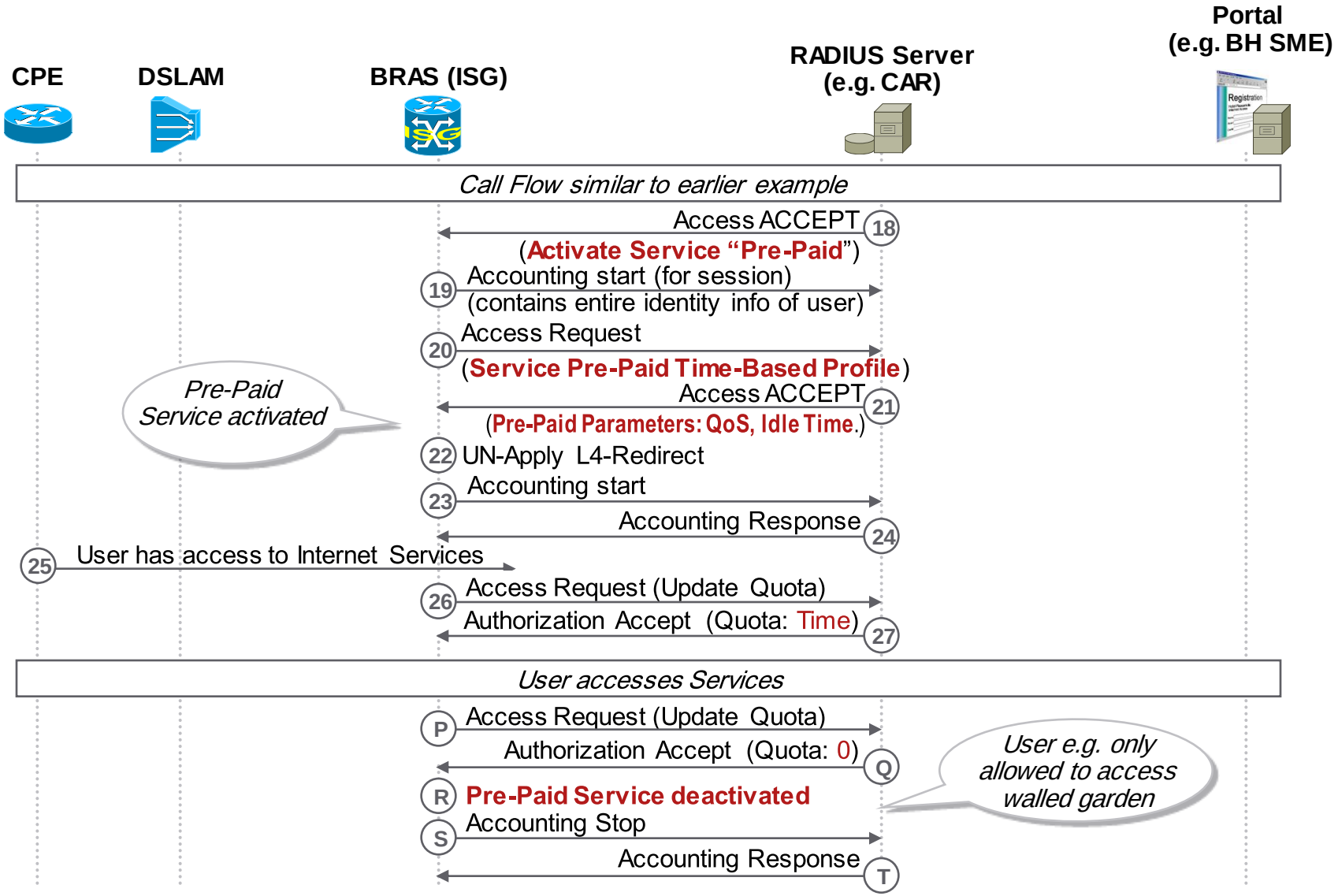
One-Shot Authentication and TAL
First Time Access—Call Flow (2/2)



One-Shot Authentication and TAL
Subsequent Logon—Call Flow



User Self Provisioning
Time-Based Services



Network Access Services:

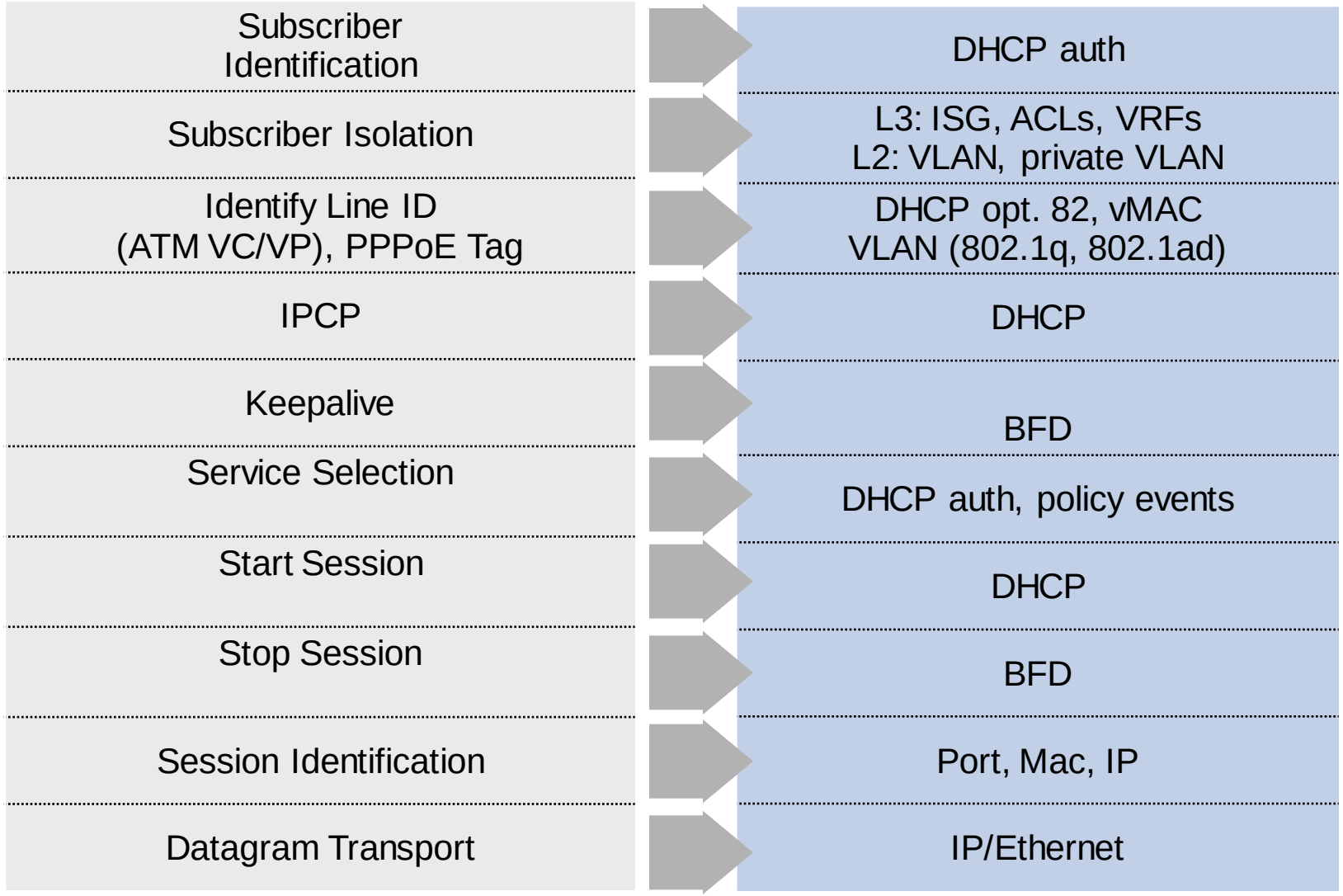
Migration to IP-Sessions

DHCP Authentication

Key Ingredient: **Cisco Intelligent Service Gateway - ISG**

PPP to IP-Sessions/DHCP Migration

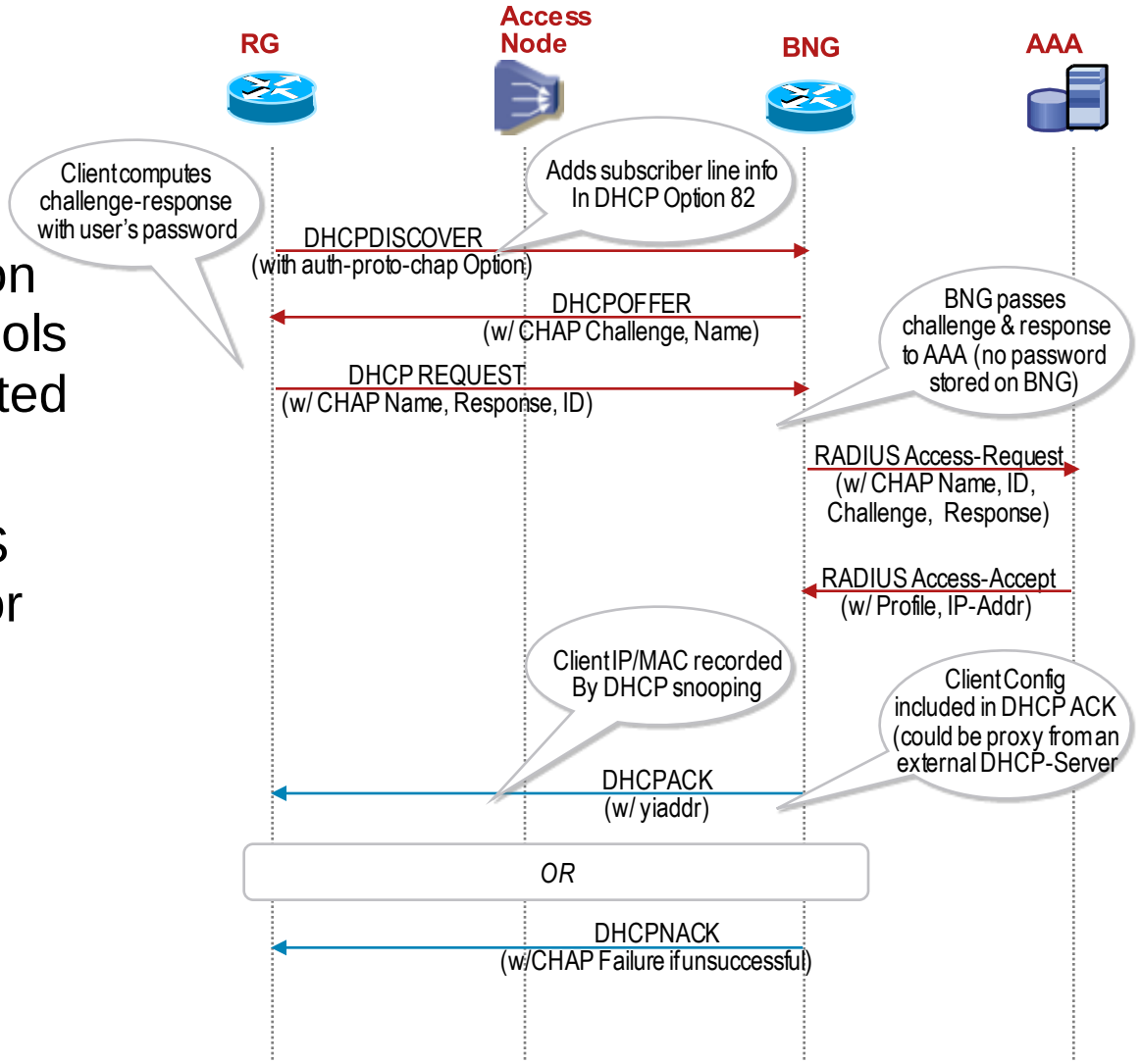
Experience should be similar to former PPP



DHCP-AUTH as "drop-in" for PPPoE

draft-pruss-dhcp-auth-dsl-01.txt* (Alternative 1)

- Use existing DHCP message set
- Reverse Authentication and other Auth Protocols (e.g. EAP) not supported
- All Attributes are mapped from RADIUS including IP address or Pool

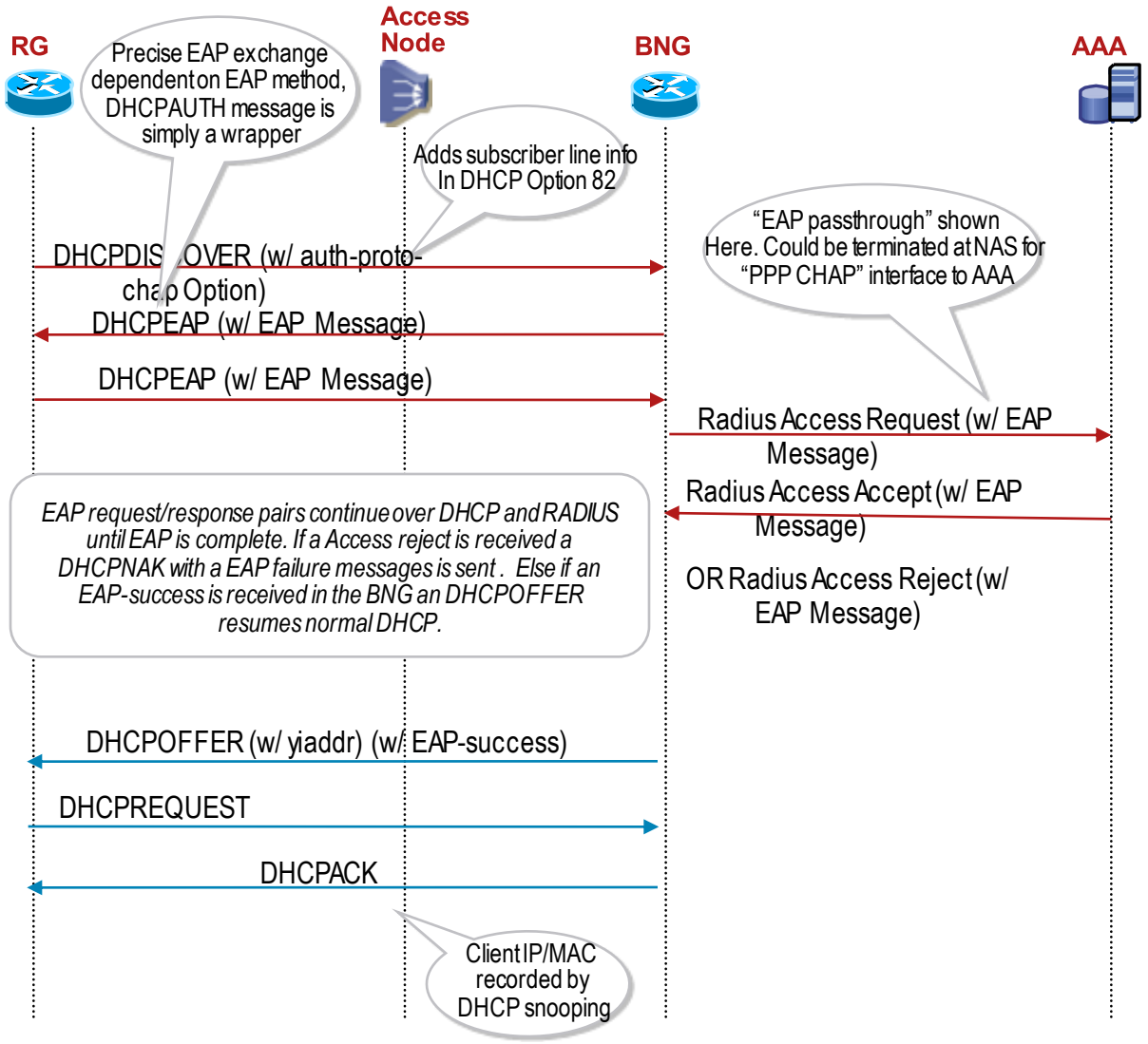


*See: http://www.ietf.org/internet-drafts/draft-pruss-dhcp-auth-dsl-01.txt
http://www3.ietf.org/proceedings/07mar/slides/dhc-2.pdf

Enhanced DHCP-Auth – For EAP, CHAP server auth etc.

draft-pruss-dhcp-auth-dsl-01.txt (Alternative 2)

- Expands capabilities of "Alternative 1" :
  - supports CHAP server authentication
  - supports EAP and with that more advance methods for authentication
- Requires:
  - A new message
  - DHCP message size >= 1604 for use with EAP message option (RFC 2132 – max DHCP message size option)



Network Access Services:

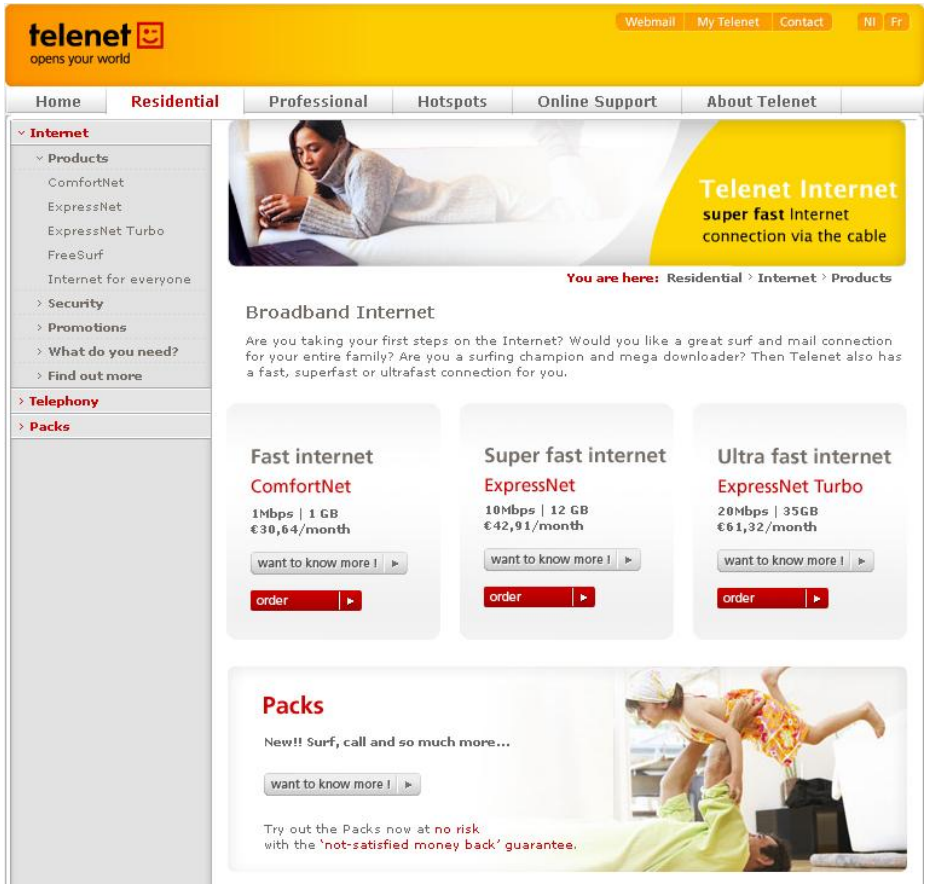
Tiered Services

Tiered Services

Key Ingredient: **Cisco Intelligent Service Gateway - ISG**

One Quota Level per Speed Level
Telenet: Cable Company in Belgium

- Quota complements Speed as a tiering parameter
- When a User reaches Quota, his Internet service is reduced to dial-up speed
- The User then has the option to upgrade his Quota Level or continue at reduced speed till the end of the month
- 15% of the Customers upgrade their Quota every month*
- Belgacom, the Incumbent deployed similar Quota system on xDSL



Source: *http://www.billingworld.com/rev2/main/featureArticle.cfm?featureID=7799

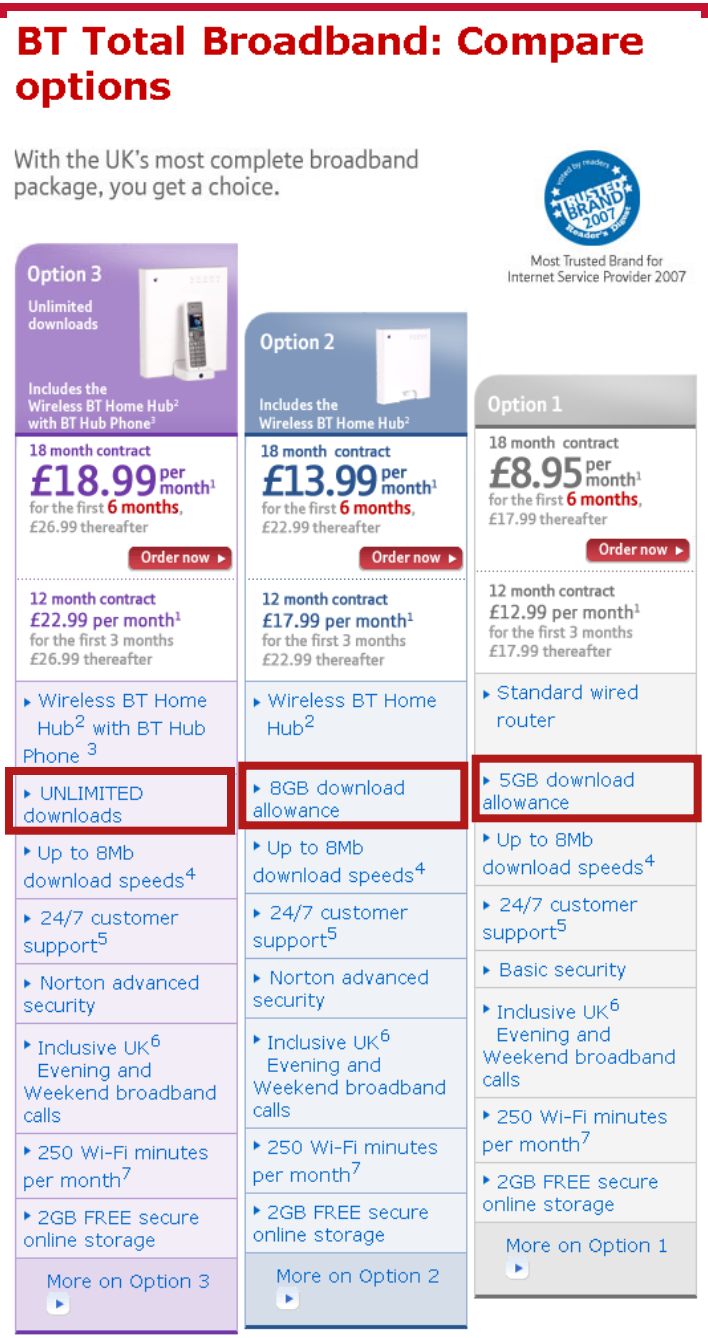
BT Total Broadband

- BT Total Broadband Options

  Option 1 – Basic Internet with wired home router, 5GB download allowance, Basic Security

  Option 2 – Internet with wireless home router, 8 GB download allowance, Advanced Security Package

  Option 3 – Internet with wireless home router and Phone, unlimited downloads, Advanced Security Package

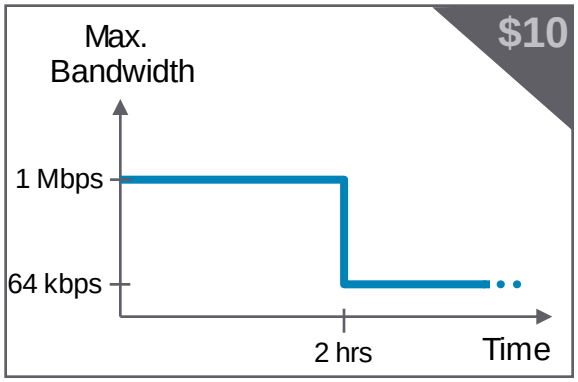


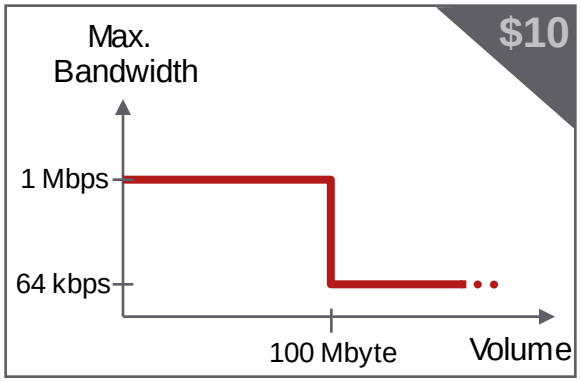
Source: http://www.productsandservices.bt.com/consumerProducts/displayTopic.do?topicId=15744

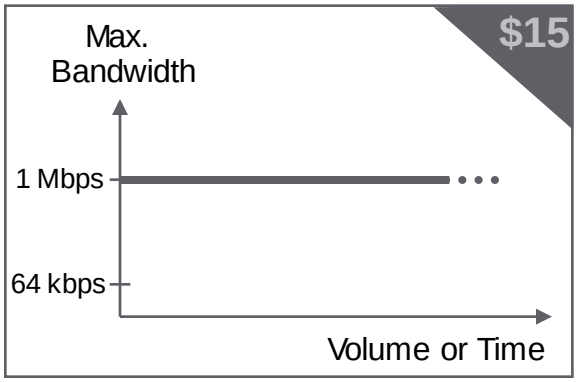
Tiered Services
Example Use Case for Dial Migration

- Many Service Providers have Internet use still on Dial-up connections
- Maintaining Dial Access Server Shelves is costly and in some cases infrastructure support comes to the end of the lifecycle
- Natural Choice is to migrate Subscribers and target shut-down of Dial infrastructure
- New Service Offerings need to be low-cost in order to facilitate migration
- Upgrade to higher profile packages should be automated and self-managed by subscriber

Use Case for Dial Migration
Migration Offerings

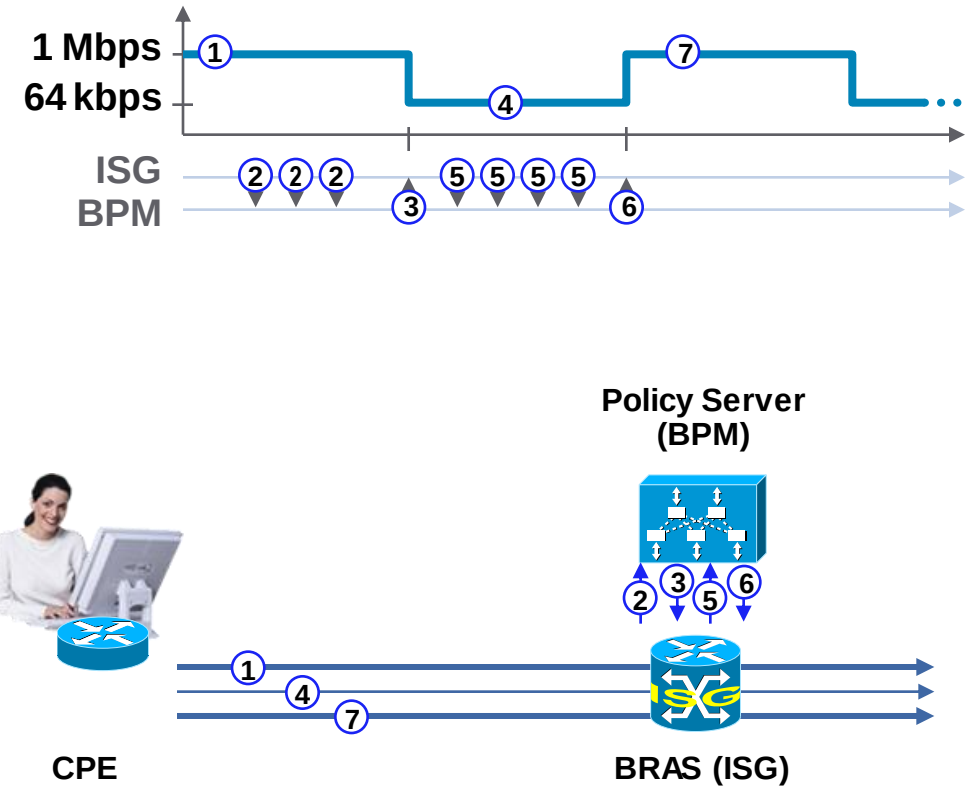






- Time-based, x amount of hour/minute at high-speed per month, then back to dial-bit rate
- Volume-based, x amount of M byte free at high-speed-bit rate per month, then flat-rate dial-bit rate
- Virtual Network Operator (VNO) sponsored periodic advertising with redirect to VNO Ad homepage

Generic Functional Reference Architecture
Dial Migration—Components



Precondition: User provisioned for migration service. Initial Authentication and Authorization completed. User's service profile available on BPM.

1. User accesses the network. Active Profile is "High-BW-Service".
2. ISG sends frequently sends interim accounting records to BPM.
3. BPM tracks quota. If quota expired, BPM sends CoA to ISG, changing the service profile to "Low-BW-Service".
4. User accesses the network. Active Profile is "Low-BW-Service".
5. ISG continues to frequently send interim accounting records
6. Start of New Months: BPM sends CoA to ISG, changing the service profile to "High-BW-Service" and toping up the quota for High-BW-Service.

Tiered Services

Key Ingredient: **Cisco Intelligent Service Gateway - ISG**

Welcome to the Human Network.

Advanced Tiered Services:

Leveraging Application Awareness

Key Ingredient: **ISG, SCE (Service Control Engine)**

Personalized Subscriber Management
Operational Services Examples

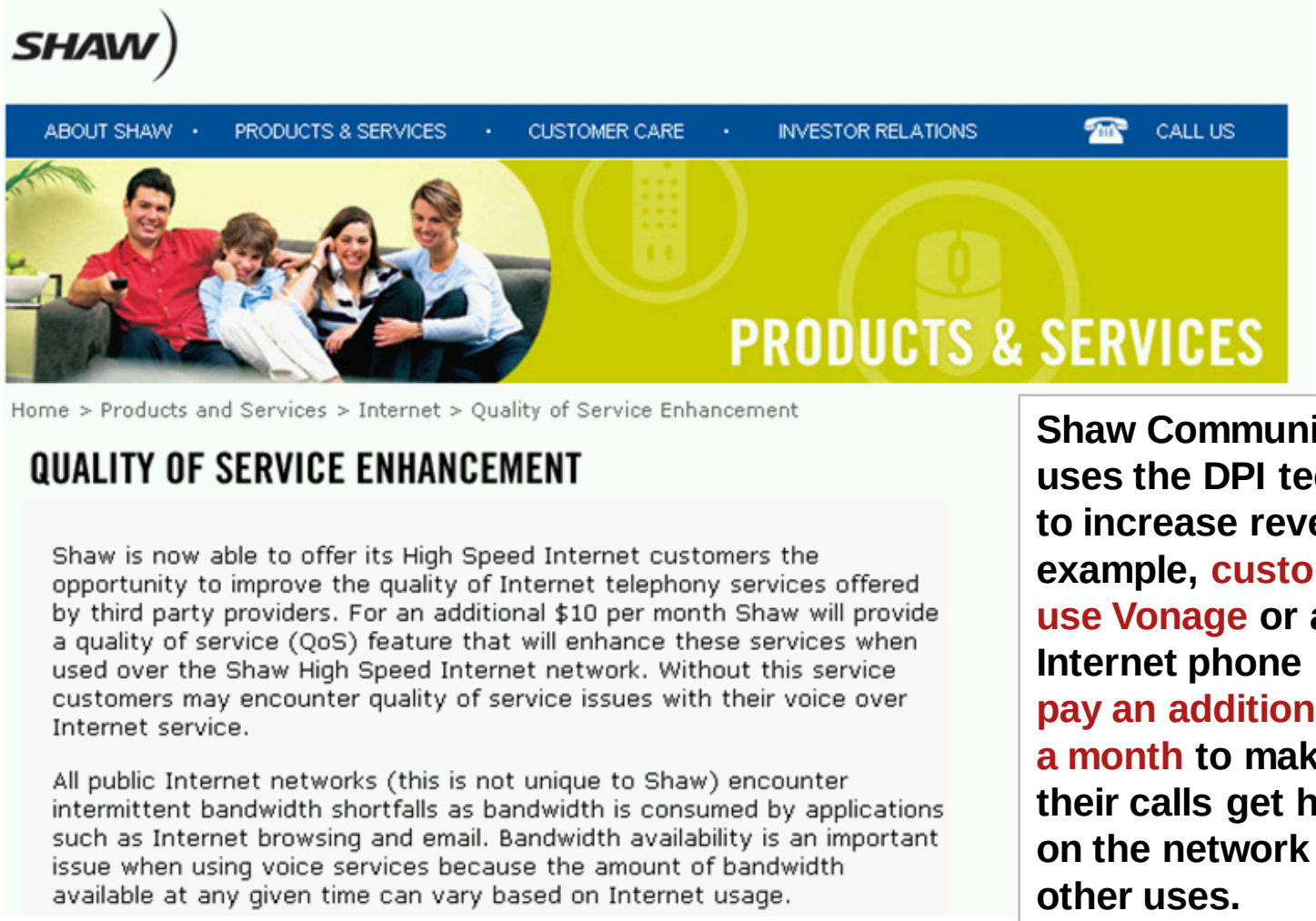
- Content Filtering
  - Subscriber-managed parental control
  - Basic website blacklisting provided free of charge
  - Comprehensive filtering & security for a small monthly subscription

- Implement Fair Use Policy
  - Eliminates bandwidth bottlenecks
  - Enhanced user experience for the average user

Usage	Less Than 2.8GB	Less Than 4.2GB	Less Than 5.6GB	Over 5.6GB
E-mail + WWW	No Limit	No Limit	256 kbps	256 kbps
Audio/Video Streaming	No Limit	128 kbps	64 kbps	48 kbps
P2P	48 kbps	28 kbps	28 kbps	16 kbps

User Quota Based on 7-Day Timeframe

Improve Over-the-Top-VoIP towards User
Shaw Communications (Canada)



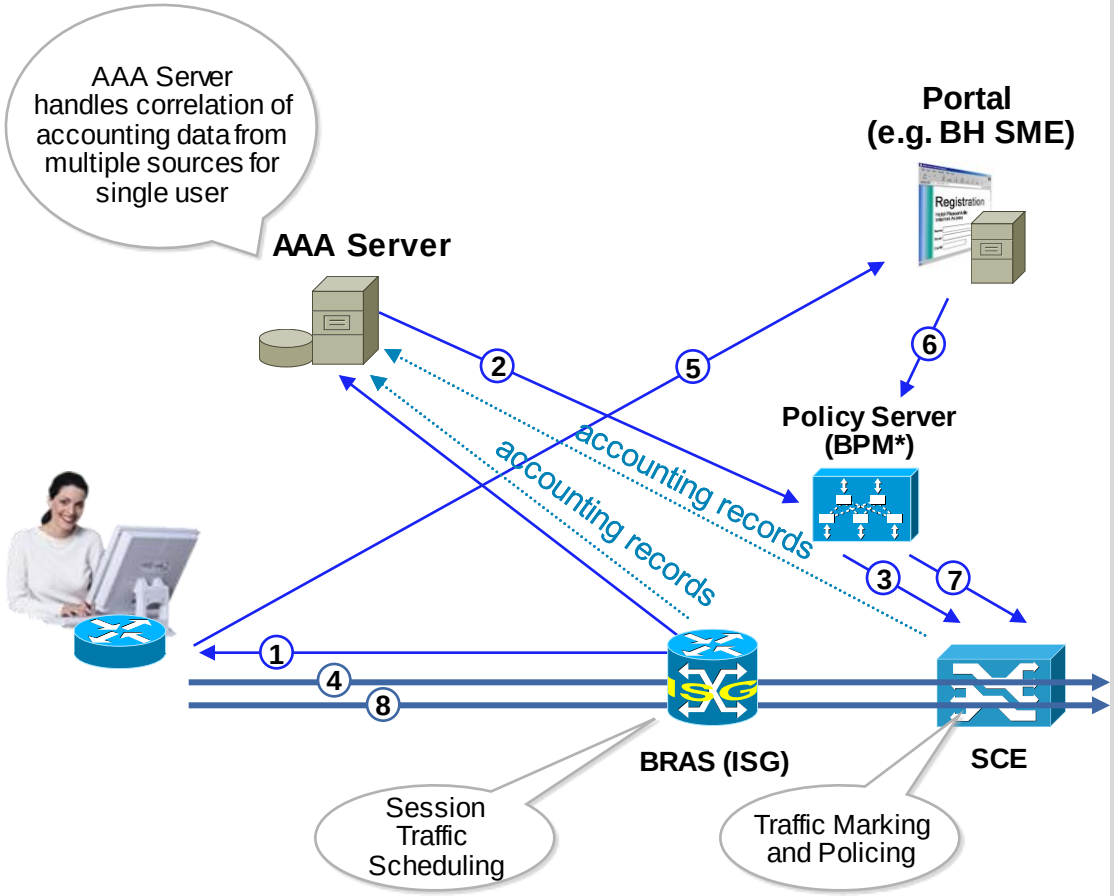
Shaw Communications also uses the DPI technology to increase revenue. For example, customers who use Vonage or another Internet phone service can pay an additional CAD $9.95 a month to make sure that their calls get higher priority on the network than some other uses.

Source: http://www.shaw.ca/en-ca/ProductsServices/Internet/ServiceEnhancement.htm

Application Aware Data Services
Example: Improve Over-the-Top-VoIP

- User has an existing subscription for Internet Access and is leveraging “Over-the-Top Voice over IP” Applications (e.g. Skype), though voice quality is not always acceptable
- SP offers User to prioritize “Over-the-Top Voice over IP” for an additional $9.95 a month
- User can order an self-provision the service through a portal (“Per-Application Turbo Button”)

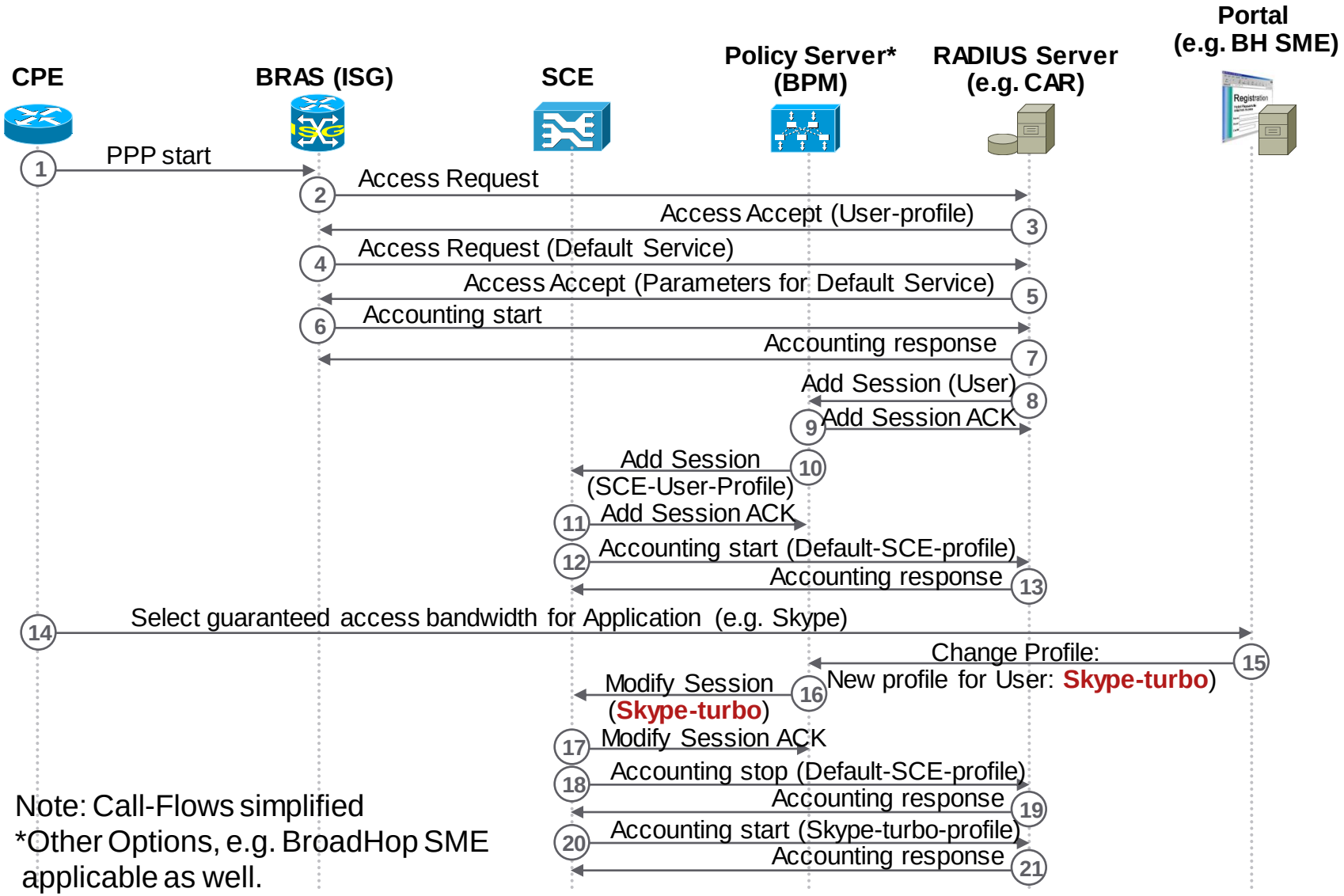
Application Aware Data Services
Example: Improve Over-the-Top-VoIP



1. PPP session setup. User default access profile downloaded to ISG.
2. AAA-Server notifies BPM of new access session and forwards user-profile of BPM.
3. BPM creates user-session on SCE and enables default profile
4. User accesses the network with default profile active.
5. User reaches out to service selection portal and chooses acceleration for a specific application (e.g. Skype)
6. Portal notifies the BPM of the new service request
7. BPM activates a new service profile which prioritizes Skype (e.g. mark Skype traffic so that it is put into the priority queue on ISG)
8. User accesses the network. Skype traffic is now handled with priority.

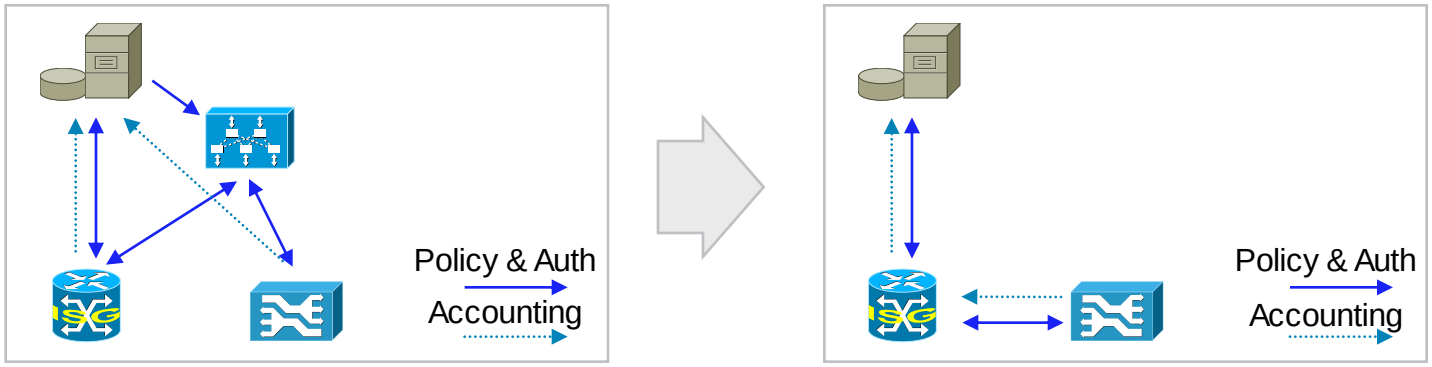
*Other Options, e.g. BroadHop SME applicable as well.

Application Aware Data Services
Example: Improve Over-the-Top-VoIP



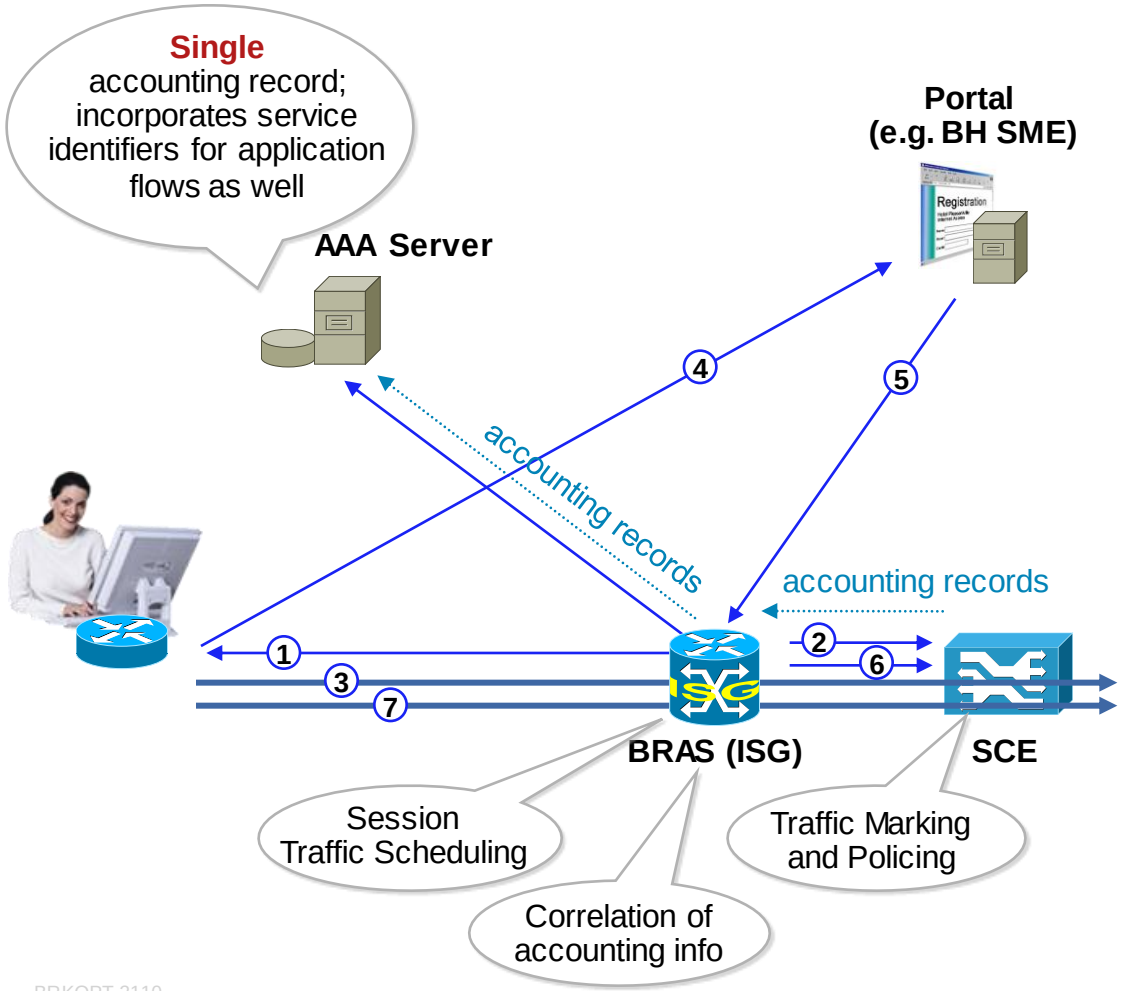
Note: Call-Flows simplified
*Other Options, e.g. BroadHop SME applicable as well.

Alternative Deployment Approach
Leverage ISG-SCE Control Bus



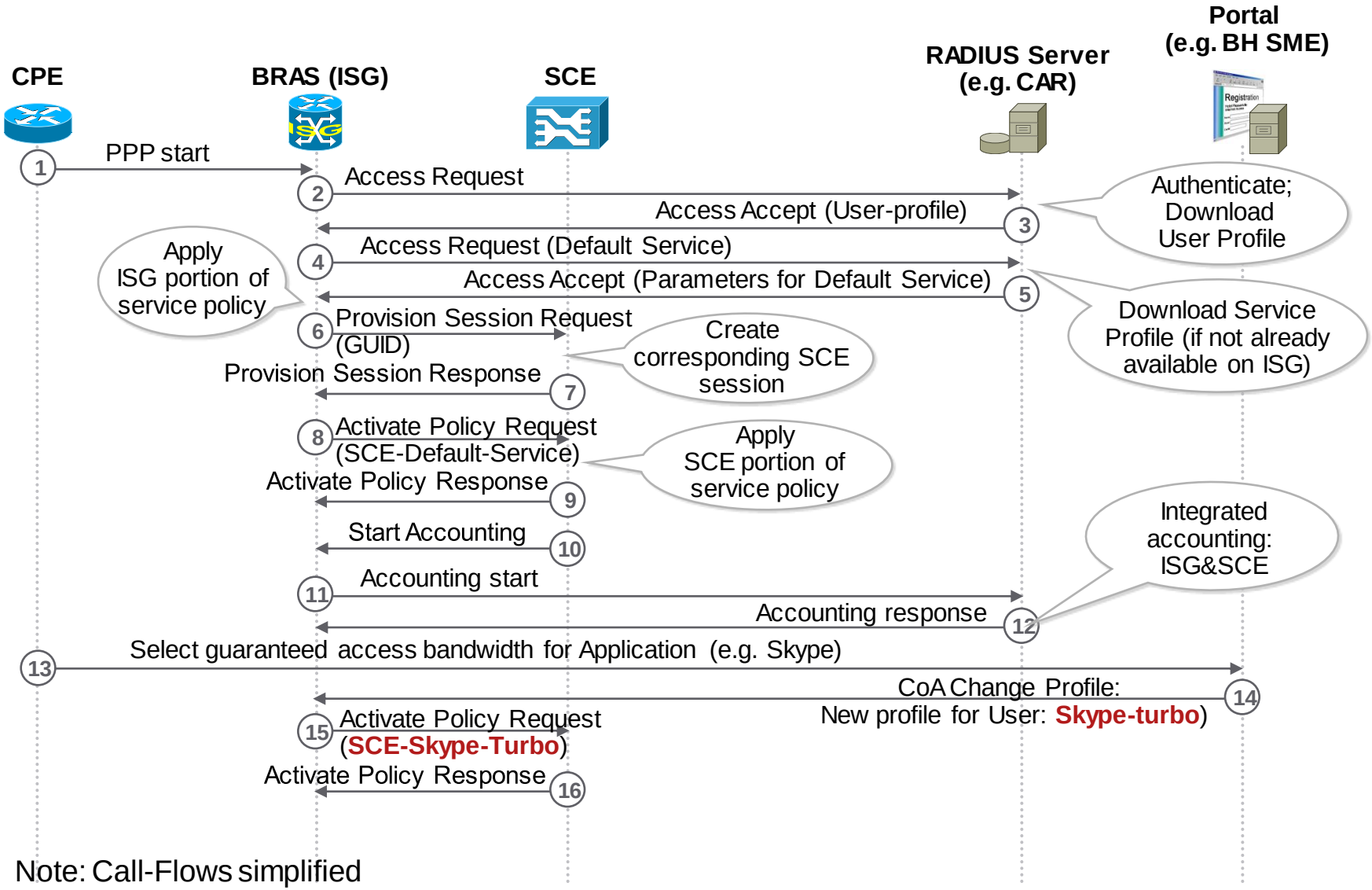
- Leverage upcoming ISG-SCE Control Bus
  - ISG takes the role of PDP and PEP
- Benefits
  - Single northbound interface from ISG (BRAS) platform
  - Single Unified subscriber database
  - CAPEX/OPEX optimized deployment
    - Only need to integrate with one platform (ISG)
    - Reduced resource requirements on AAA/policy layer (RADIUS and policy infrastructure)
  - Increased Scale and Reliability

Example: Improve Over-the-Top-VoIP
Leveraging ISG-SCE Control Bus



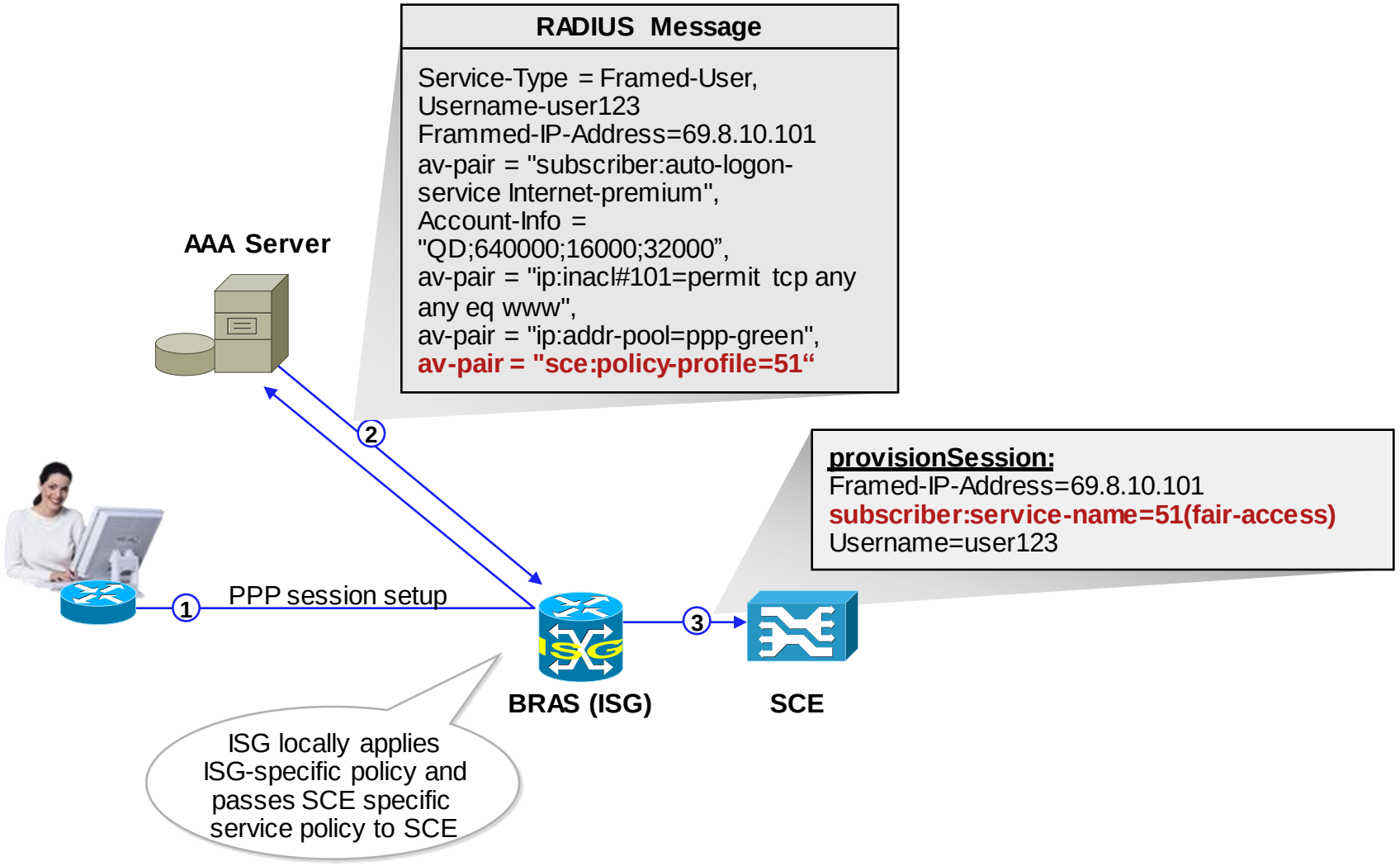
1. PPP session setup. User default access profile downloaded to ISG.
2. ISG establishes session on SCE and passes the portion of the profile relevant to SCE over to SCE.
3. User accesses the network with default profile active.
4. User reaches out to service selection portal and chooses acceleration for a specific application (e.g. Skype)
5. Portal CoA to ISG to enable a new service for the user ("prioritize Skype": e.g. mark Skype traffic so that it is put into the priority queue on ISG.
6. ISG receives the request, determines it is for SCE – and forwards the request to SCE, where the new service policy is activated.
7. User accesses the network. Skype traffic is now handled with priority.

Application Aware Data Services
Example: Improve Over-the-Top-VoIP

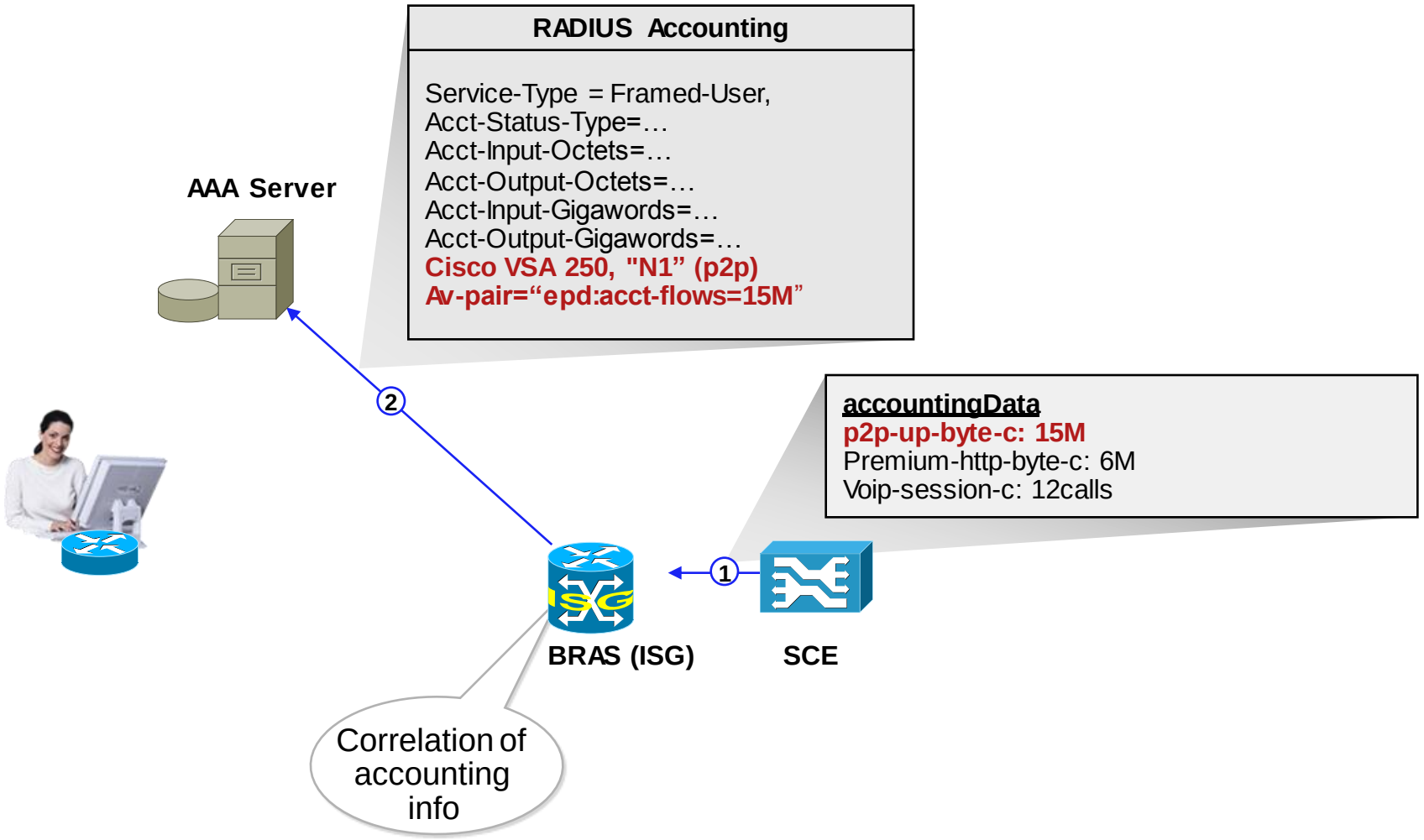


Note: Call-Flows simplified

Enhancements Through ISG-SCE Bus
Delegated Policies



Enhancements Through ISG-SCE Bus
Single Accounting Stream

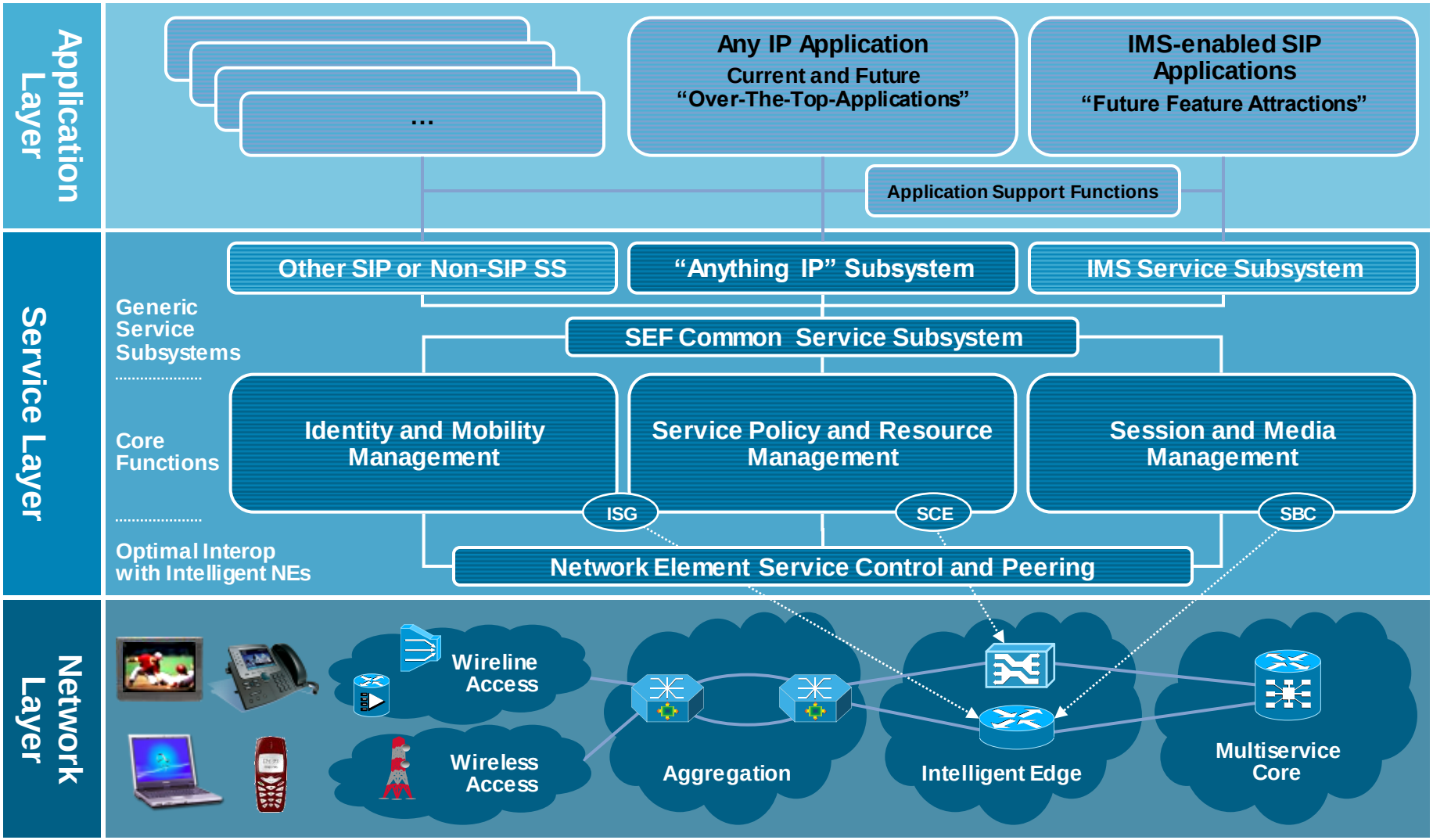


Summary

Welcome to the Human Network.

Cisco IP NGN: Universal NGN Architecture

Enabling all Emerging Network Architecture Standards



Key Takeaways

- **ISG handles the key aspects of dynamic service delivery in BB aggregation networks:**
  - Subscriber identification
  - Service and policy determination
  - (*Including AAA & Dynamic Service Updates e.g. RADIUS CoA, SGI/XML*)
  - Session policy enforcement
  - Session life-cycle management
  - Accounting for access and service usage
- **ISG adds Policy Management Capabilities to the Network Element**
  - Complements stand-alone Policy-Servers
  - Towards a network policy plane: ISG-SCE Bus
  - A key component of SEF
- **Platform Support**
  - ASR 1000, 7600 (SIP-400, ES40), ESR 10000, 7200, 7301

Q and A