AGG-2025

Intelligent Edge Networking

Next Generation Concepts for Ethernet/DSL aggregation and Dynamic Service Selection

Dr. Frank Brockners

Recuerde siempre:

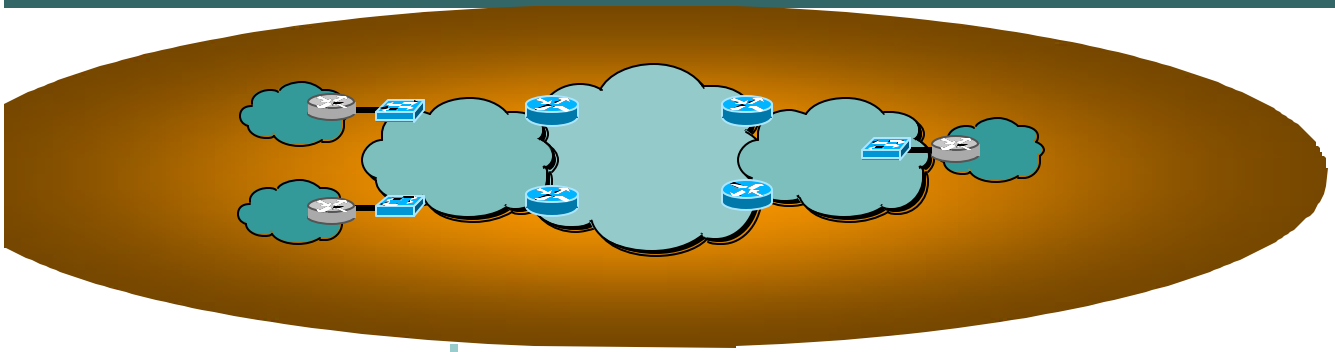
- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.

- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.

- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.

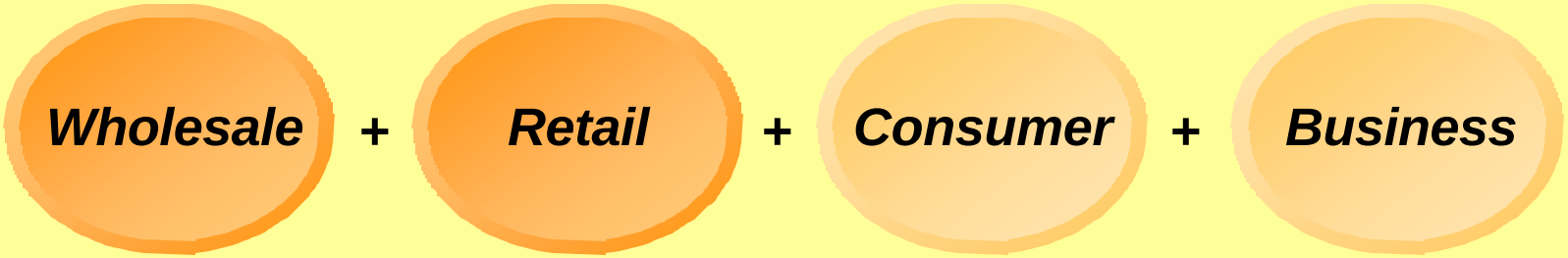
- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

Agenda



- **Integrated Access/Aggregation Architecture**
  - **Towards an Integrated Access/Aggregation Architecture**
  - **Focusing the Key Challenges**
    - **Customer to VLAN mapping**
    - **MAC Scalability**
    - **Scalable Multicast Deployment**
    - **Security**
- **Service Control and Subscriber Management**
  - **Sessions, Identity, Policies**
  - **Case Studies**
  - **Configuration Brief**

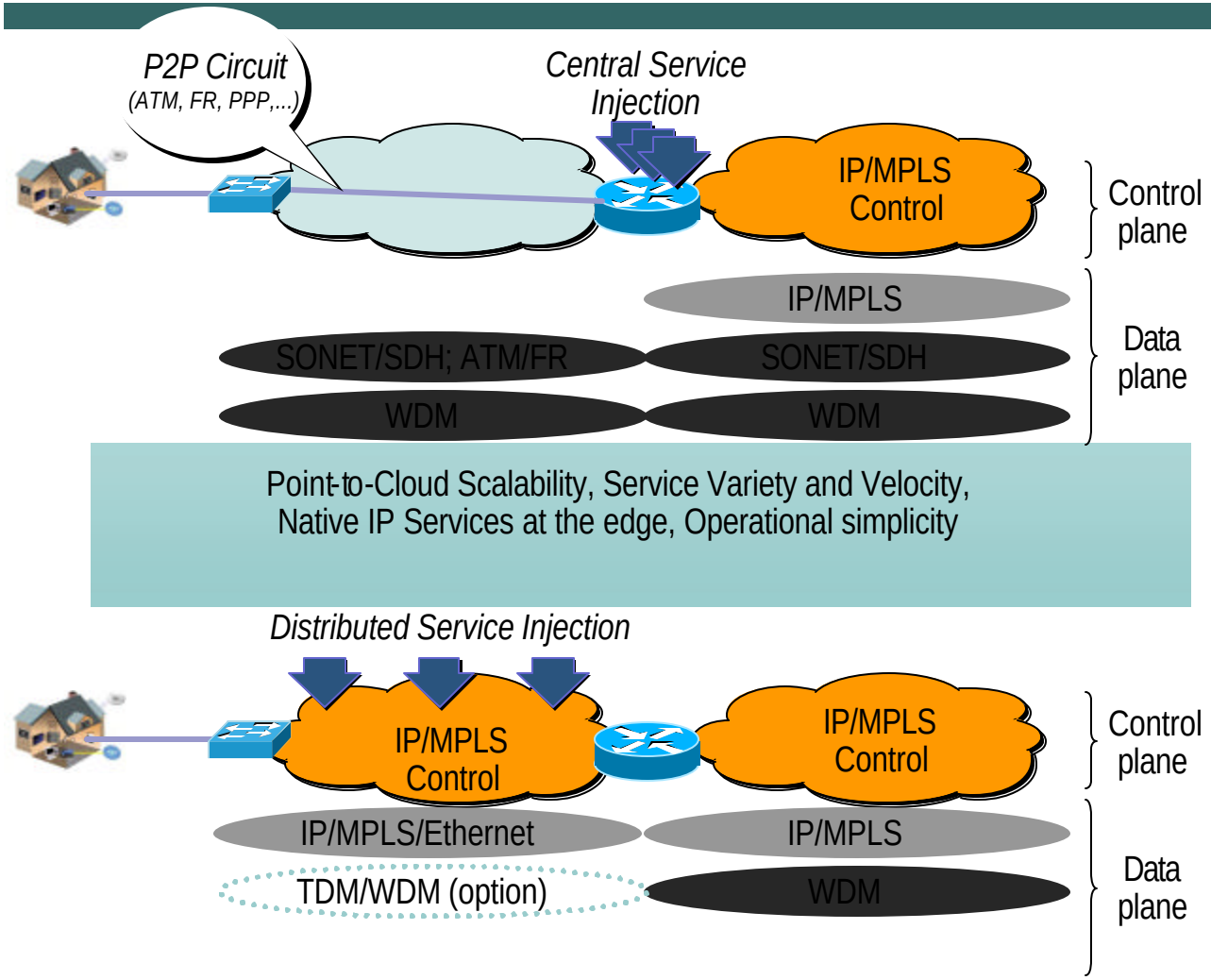
Towards a Scalable Multi-Service Network
Creating One Generic Approach for…



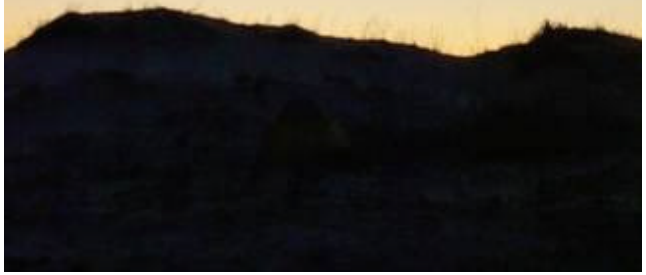
ONE single architectural model
for wholesale, retail, consumer and business services

Enable Mass-Customization and Mass-Scale: ***Policy Networking***	***Leverage proper Layering:*** ***Implement Services & Functions at the appropriate layer***	***Reduce cost; Increase ARPU*** ***Existing & New Services; Bundles***

Towards a *Scaleable* Forwarding plane:
Access/Aggregation Architecture Vision



"Access networks move from Circuits to Packets *and* leverage native IP"



This is also supported by the vision statement of the E2E research group:
"Making the world (of communications) a different place"
http://www.ir.bbn.com/~craig/e2e-vision.pdf

One Network for Residential & Business Services
Why Ethernet?

Cisco.com

- ***Native Ethernet*** **maturing to Carrier Transport**
- **Support "*Point to Cloud*" Model: No circuit provisioning**
- **Packet based – IP Services friendly**
- **Multiple Services Injection Points**
- **Local Switching in Access**

Focus on the User-Perspective: Ethernet Services, UNI, Traffic Engineering, E-LMI, ...

SP-Ethernet: Provider Bridges (802.1ad); EFM (802.3ah); Connectivity Management – OAM: 802.1ag; 802.1ah Backbone Bridges, 802.1ak Multiple Registration Protocol, 802.1aj Media Converters, etc.

L2VPN, PWE3 WG – Building the Network Core: VPWS, VPLS

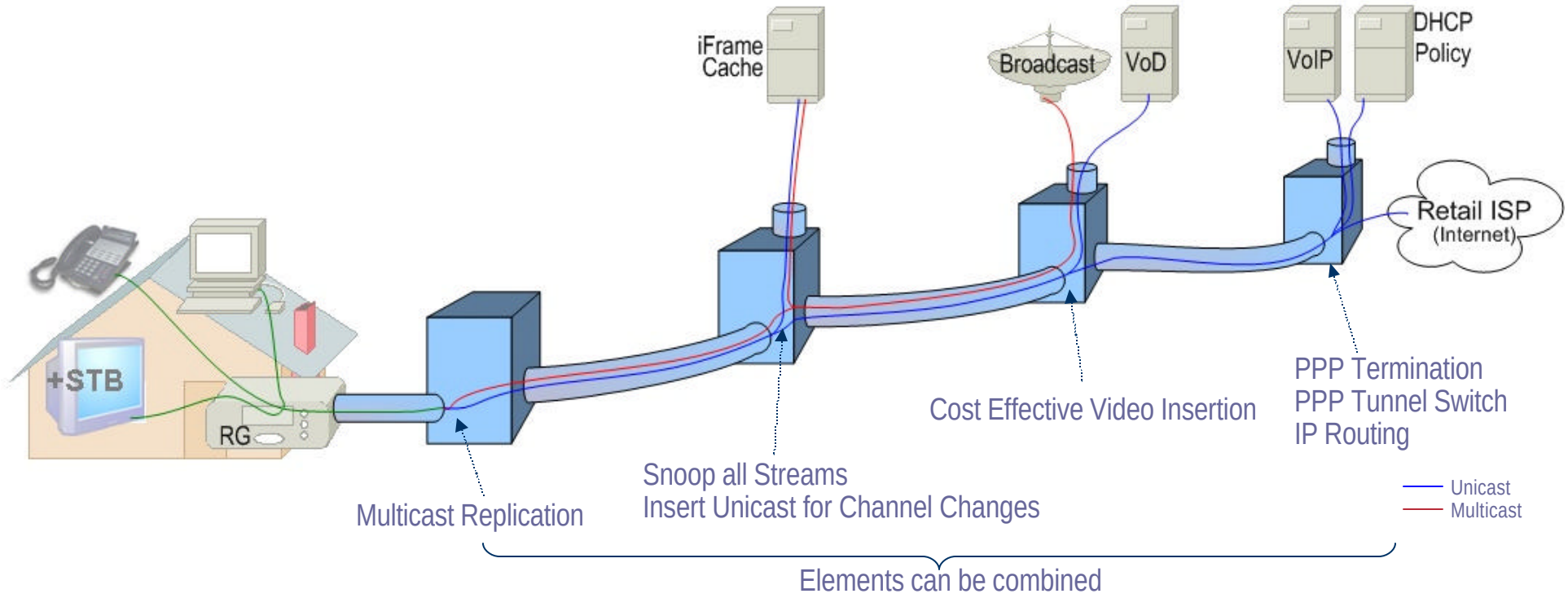
SG15/Q12, SG13/Q3; Architecture of Ethernet Layer Networks, Services etc. – from a Transport perspective. E2E OAM.

Ethernet to Frame-Relay/ATM Service Interworking

DSL related architecture & transport aspects (WT-101): BRAS-requirements, Ethernet Aggregation / TR-59 evolution, subscriber session handling, …

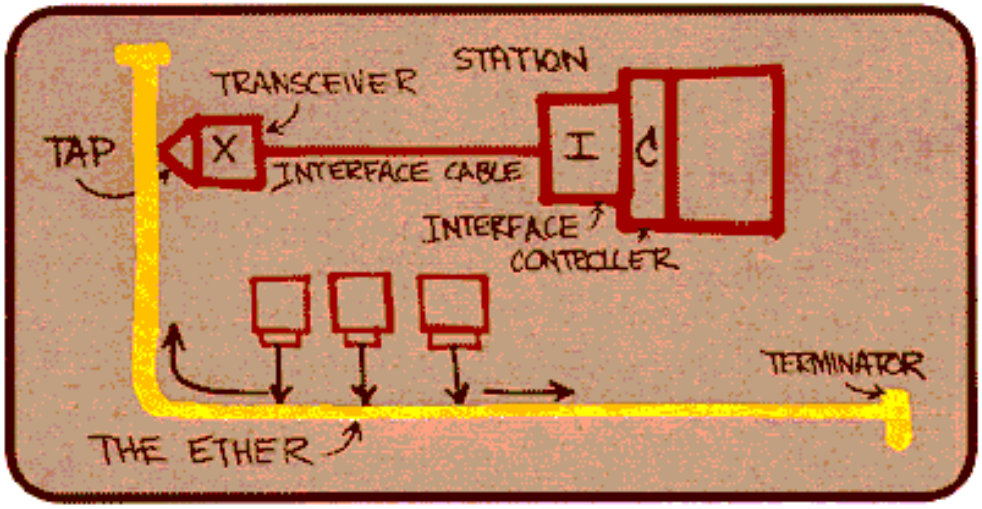
...making sure all 'cooks' are cooking the same soup

Residential Target Architecture(s)
Application Mix Can Require Multipoint at Sequential Hops



- Cost Optimization (OPEX and CAPEX) naturally leads to multiple service insertions
- Application Servers only have *limited* economic ability to move towards or away from RG
- Services don't care if insertion points are L2 or L3 Network Elements
- Multipoint Ethernet switching leveraged
- Optimizing each network hop for L2, L2+, and/or L3 is a complex function

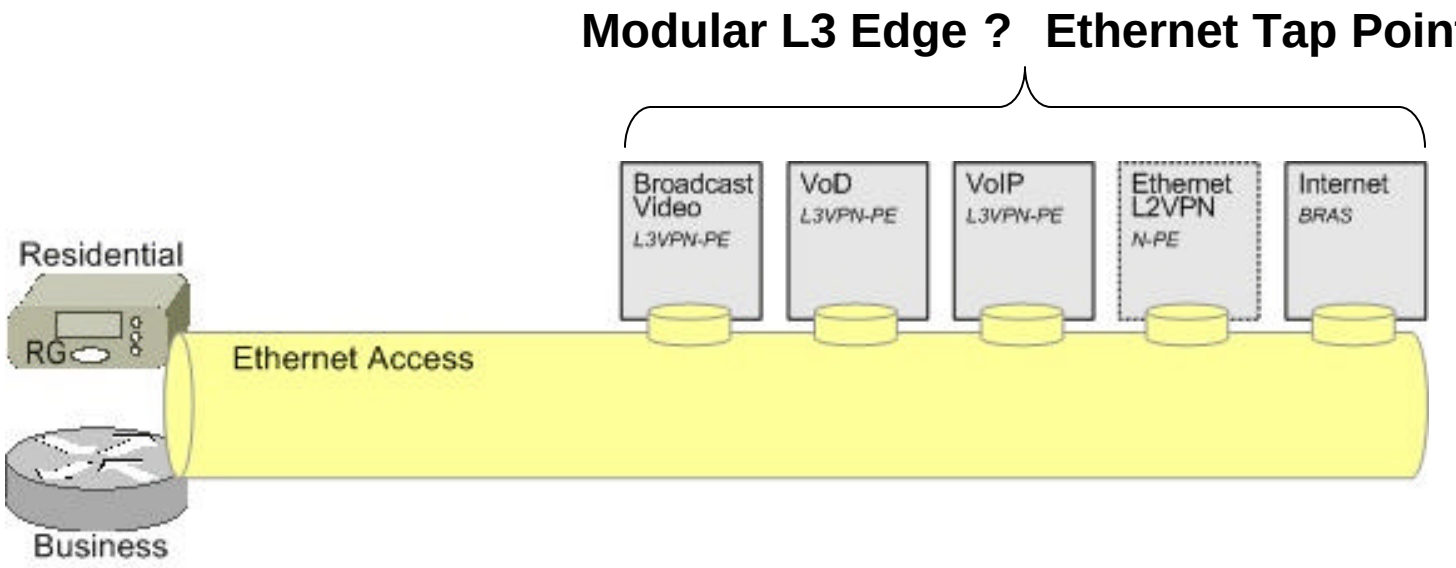
Generalizing SP Ethernet Access
Evolving the Original Idea of the Ethernet Service Bus



Metcalfe's Original Concept of Ethernet (1976)

- **Ethernet began as Shared Media Tap points for workstations & bridges**
- **We need to leverage the multipoint nature of Ethernet in SP access more than we have to date. There is a *lot* of value here…**
  - **Service Insertion Point Economics**

Generalized Architecture Vision
View from CE: Ethernet Tap Points by Application

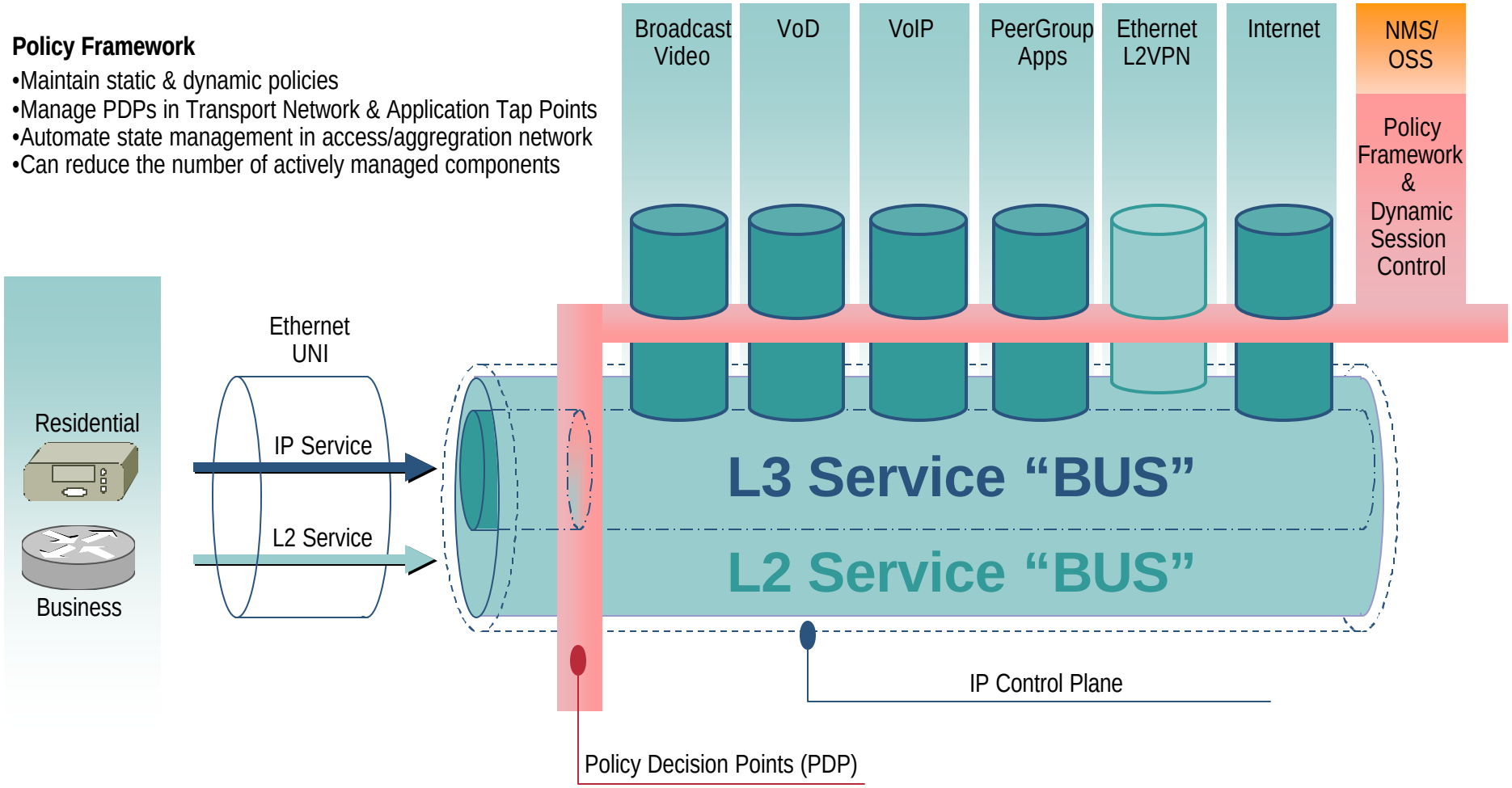


- Different L3 Edge by service, services can be added and managed independently
  - Network becomes design to cost for incremental SLAs
- SP Edge physically could be one L3 box, but likely is many
- Supports to Geographic segmentation of application servers
- Allows services & transport to be reused across a variety of access technologies
- Intermediate tunneling technologies transparent to the CE (QinQ, .1Q, Pseudowire, etc.)
- Collision domain is replaced by per-hop L2/L3 QoS capabilities & Traffic Engineering by SLA

Architecture Vision:
IP Controlled Service Bus Concept

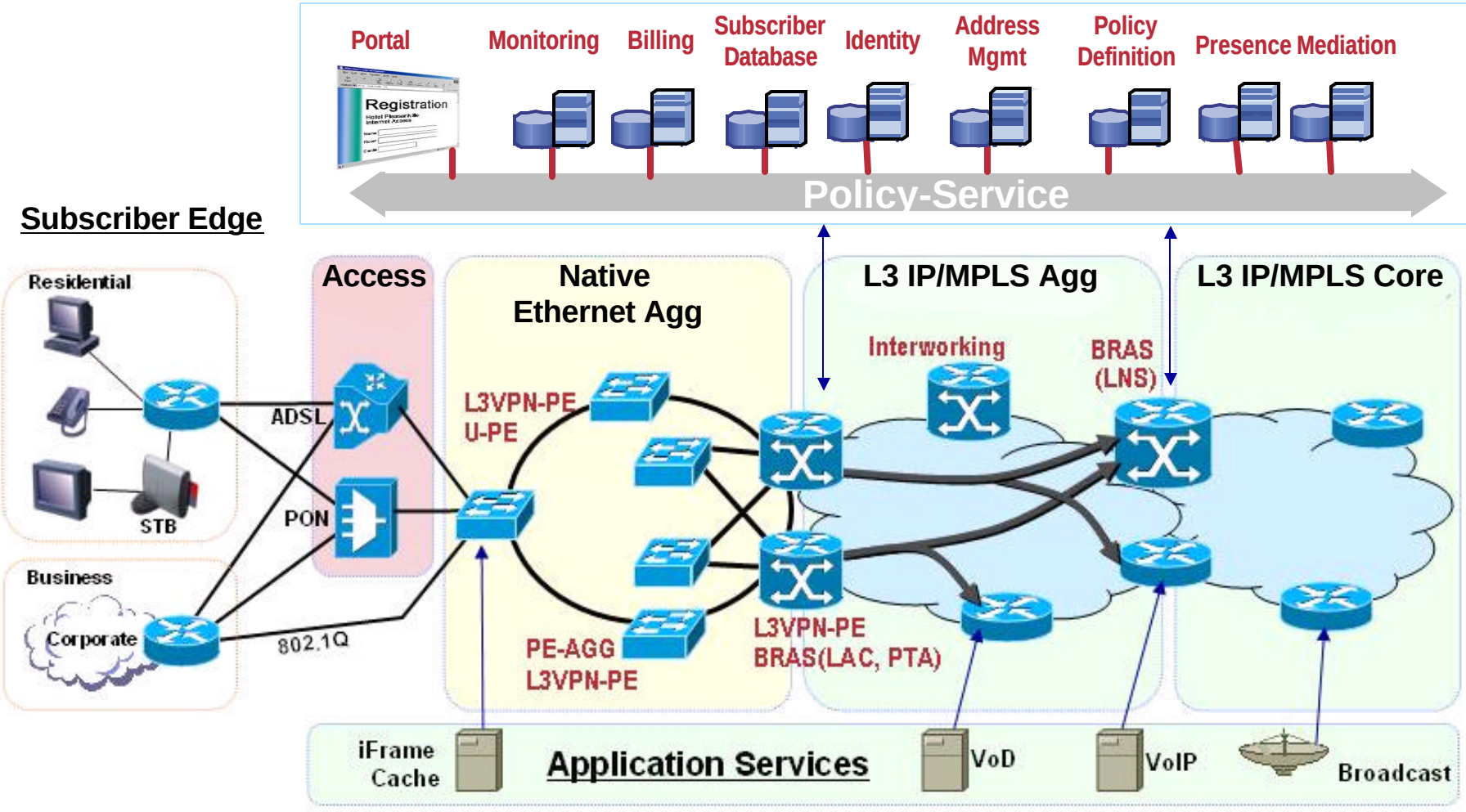
Policy Framework

- Maintain static & dynamic policies
- Manage PDPs in Transport Network & Application Tap Points
- Automate state management in access/aggregation network
- Can reduce the number of actively managed components

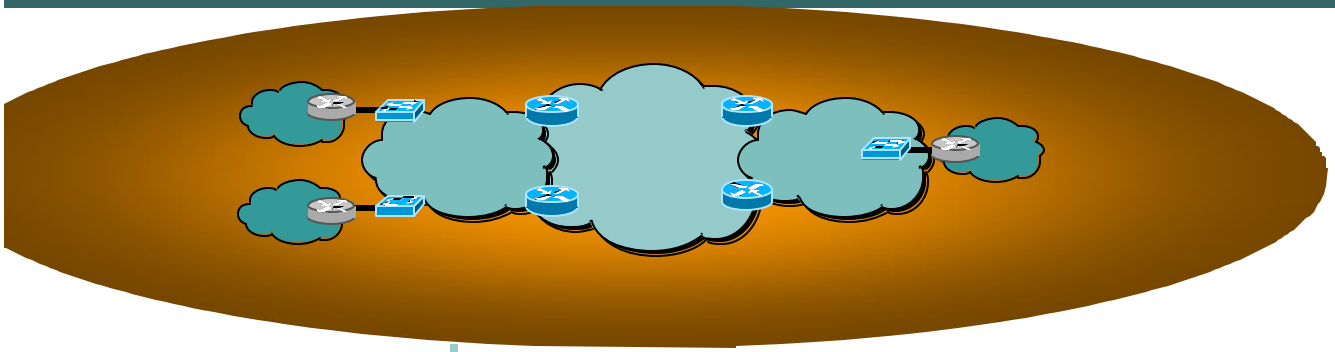


Broadband High Level Target Architecture

Cisco.com

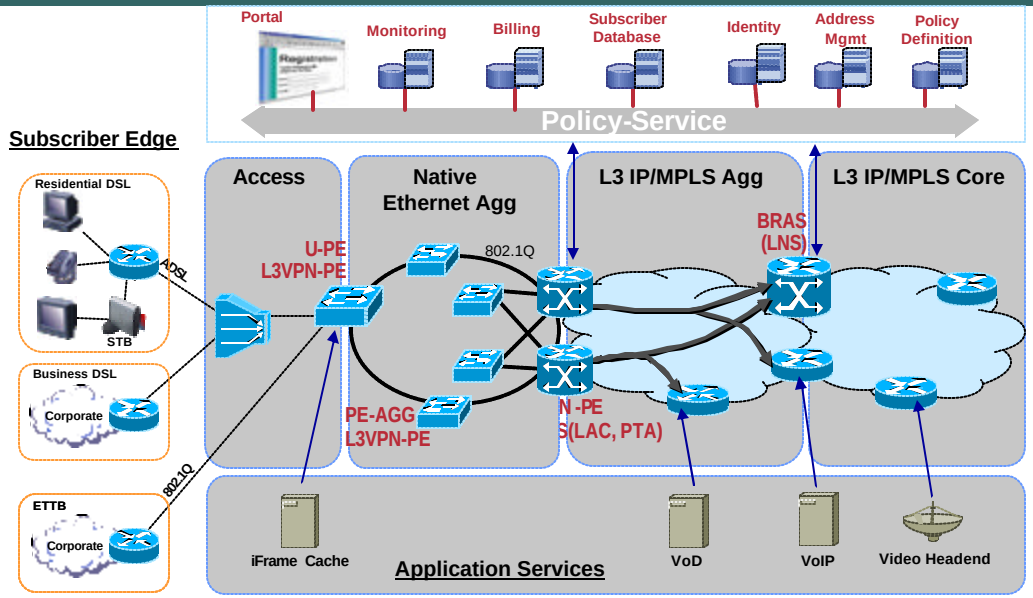


Agenda



- **Integrated Access/Aggregation Architecture**
  - **Towards an Integrated Access/Aggregation Architecture**
  - **Focusing the Key Challenges**
    - **Customer to VLAN mapping**
    - **MAC Scalability**
    - **Scalable Multicast Deployment**
    - **Security**
- **Service Control and Subscriber Management**
  - **Sessions, Identity, Policies**
  - **Case Studies**
  - **Configuration Brief**

Focusing the Key Challenges



- **Providing Business Ethernet Services and Aggregation Residential Customer with Ethernet**
  - **Model for Residential Aggregation:**
    How to "map customers to VLANs/Service Instances"?
  - **Subscriber Isolation**
  - **Vast scalability**
    (1000s of DSLAMs w/ > 1000 users per DSLAM, 1000s of ETTB)
  - **Security, Scalable Multicast**

Focusing the Key Challenges

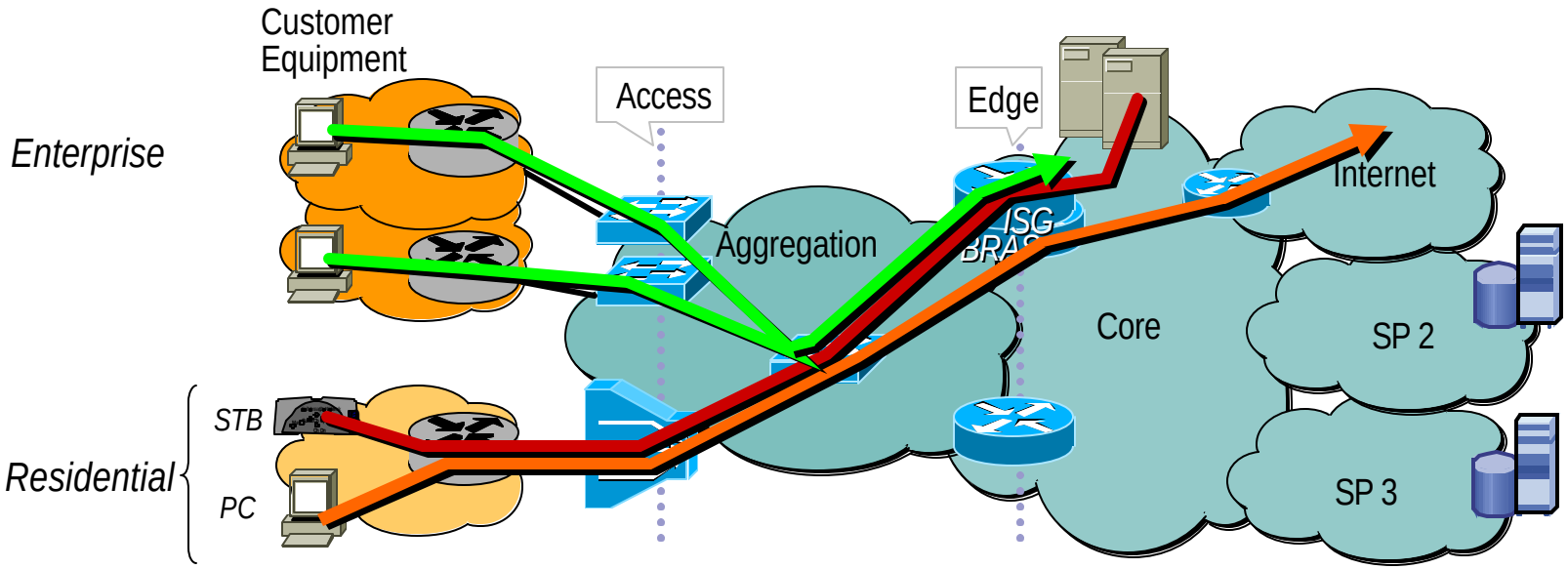
One Integrated Access Network for Business and Residential Services

Cisco.com

- **Mapping customers to service instances (VLANs)**
  - **Scalability:**
    Number of Service Instances (VLANs)
  - **Subscriber Isolation**
  - **Transparency**
- **Scalability**
  - **Number of MAC-addresses**
  - **Topology**
- **Video Deployment**
  - **Large Scale Multicast Design**
- **Security**

- > 1M users total
  - 10.000s of business services
  - Residential Users: Wholesale and Retail
- 1000s of DSLAMs w/ > 1000 users per DSLAM
- 100s of video channels – broadcast TV and VoD

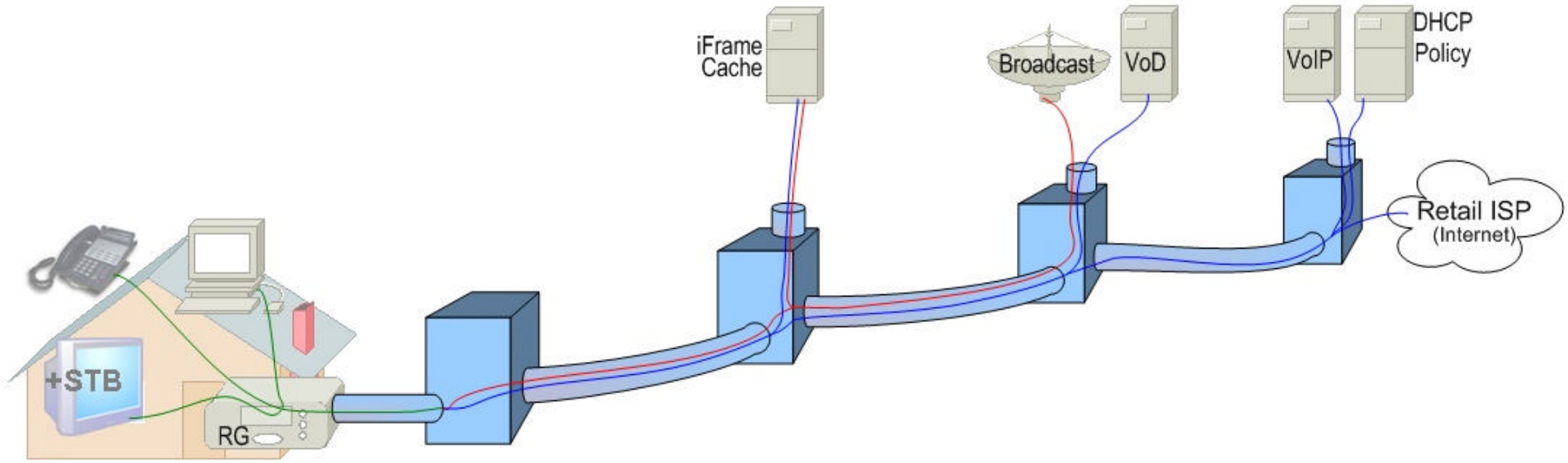
Target: Combined Aggregation Model Business & Residential, Retail & Wholesale



- **Business Customers**
  - **Transparent LAN Services, Access to L3 Services**
- **Residential Customers**
  - **Internet Access**
  - **Access to Value Added Services (Voice, Video, Broadcast)**

Mid-Term Target Architecture(s)
Emerging Categories of Architectures

Cisco.com



Models/Categories

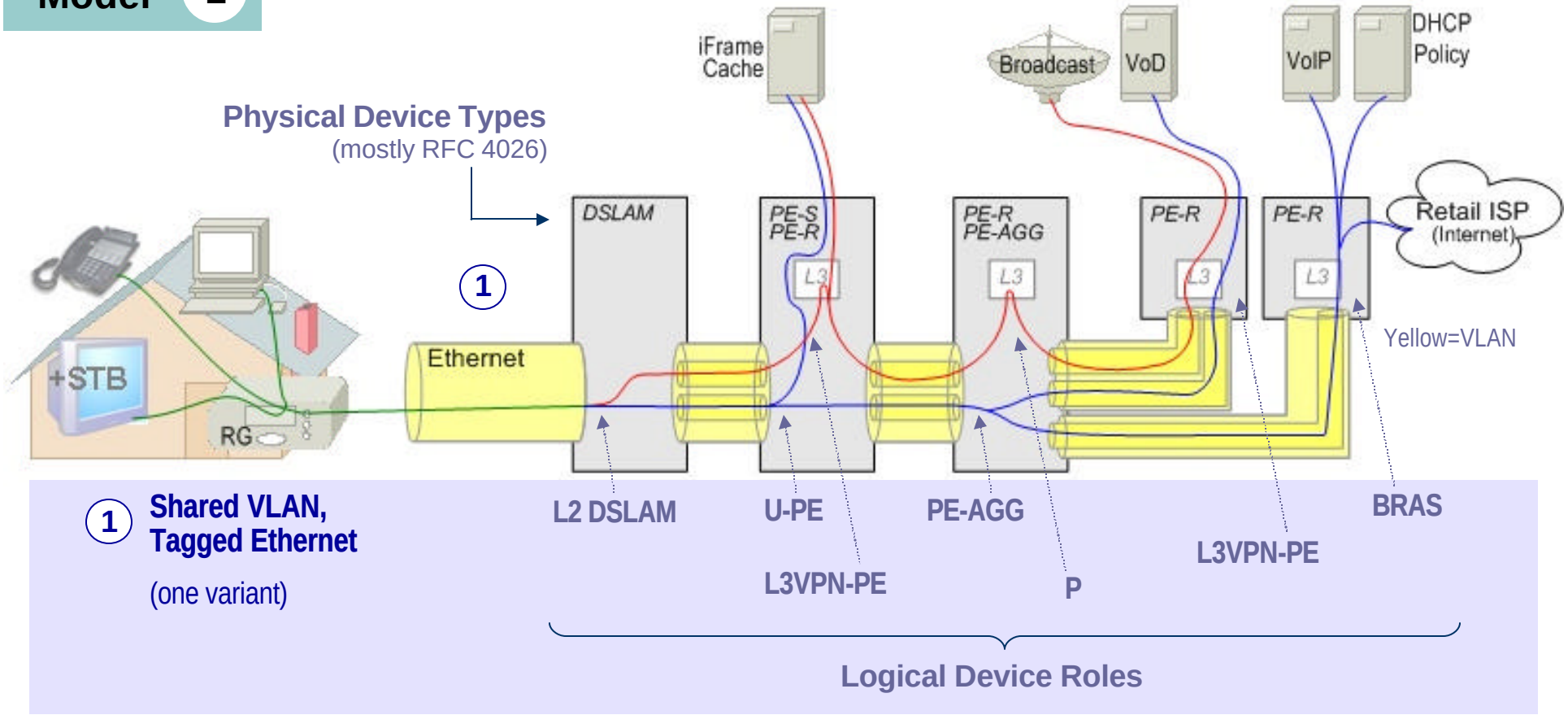
1. **Shared VLAN, Tagged Ethernet**
1b. **Shared VLAN with optional PW-extension, Tagged Ethernet**
2. **Dedicated VLAN, Tagged Ethernet***

* A model 2b, similar to 1b would also be feasible but is not discussed here

Logical Roles per Physical Device Type
Shared VLAN/ISP Access to L3 Services

Cisco.com

Model 1

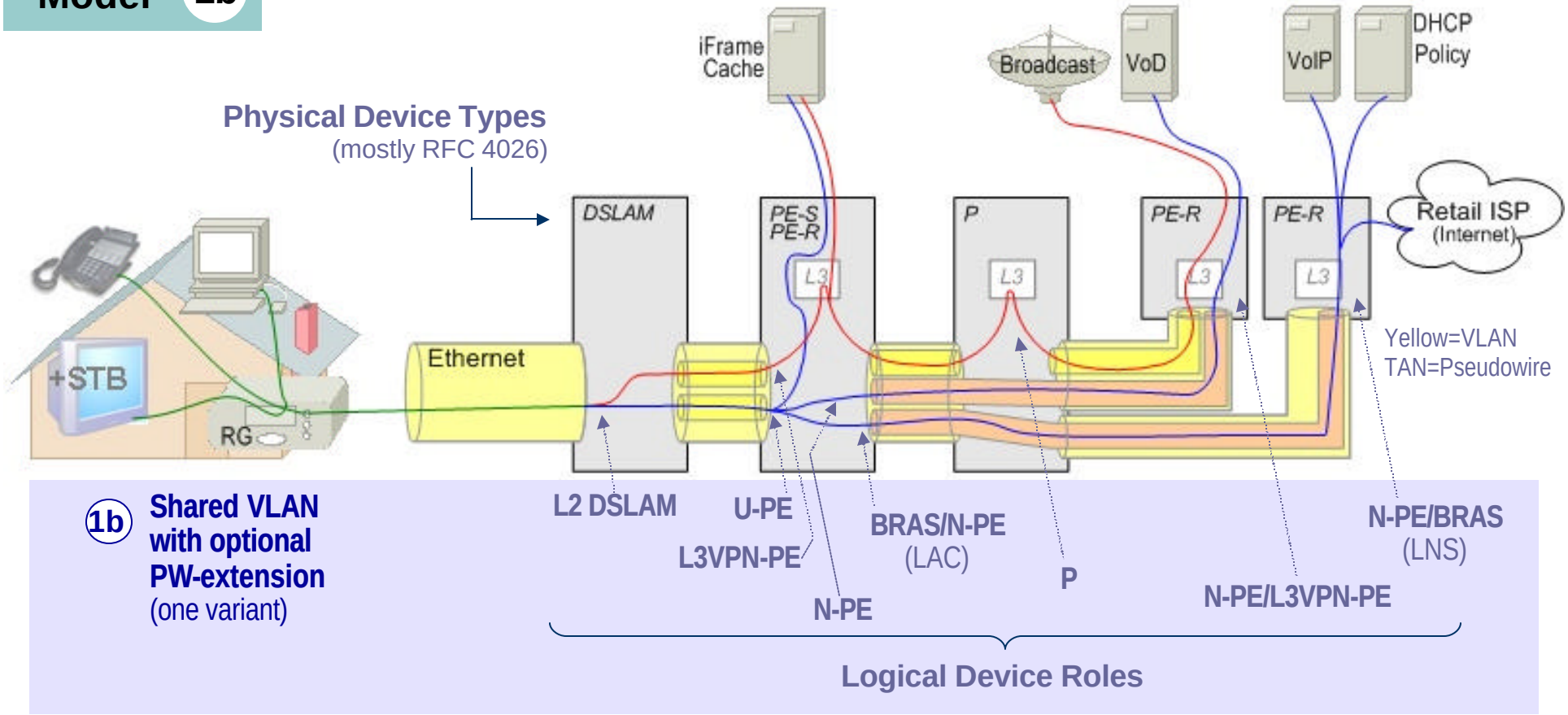


Even for a single UNI, logical device roles can be per VLAN, so one box may fill many roles

Logical Roles per Physical Device Type
Shared/Dedicated Access with Tunneling Option to L3 Services

Cisco.com

Model 1b

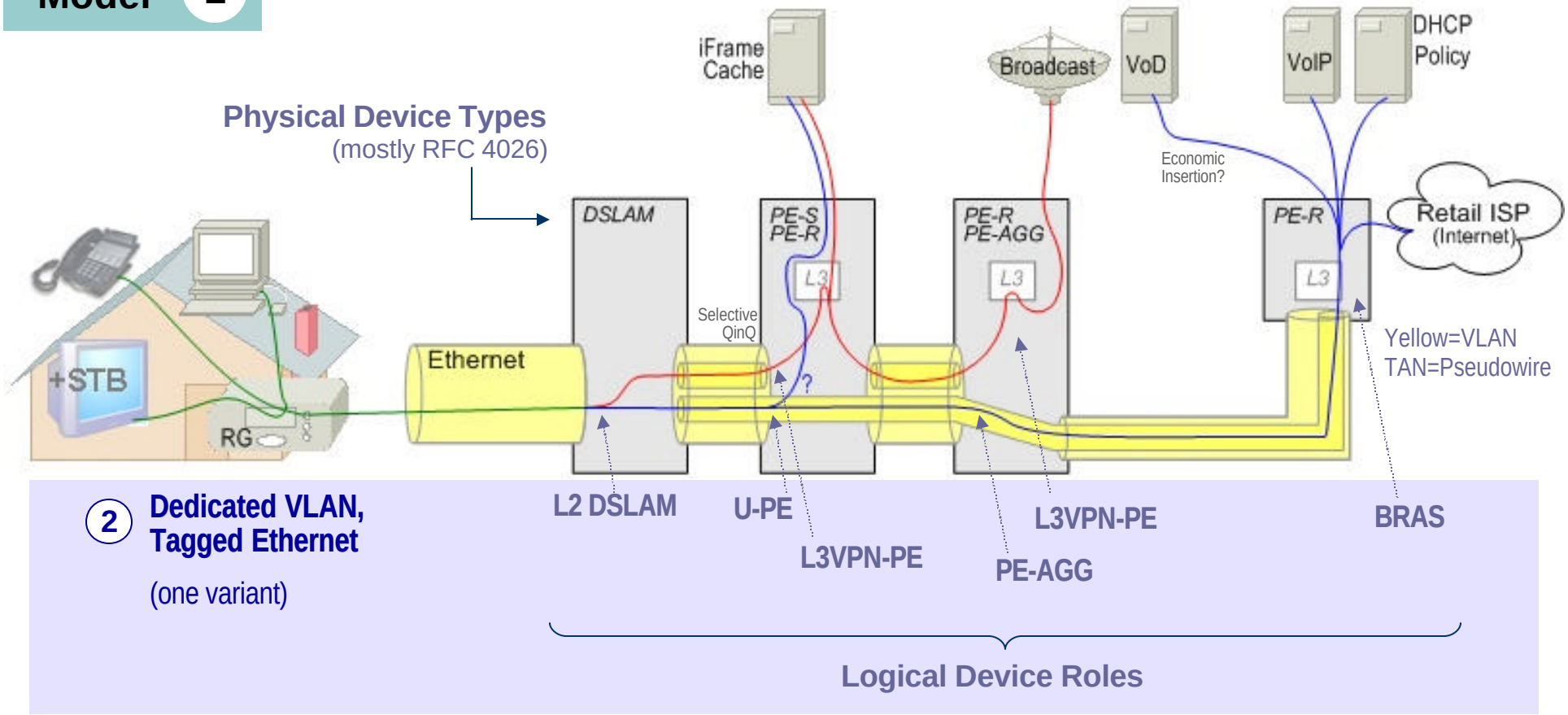


Even for a single UNI, logical device roles can be per VLAN, so one box may fill many roles

Logical Roles per Physical Device Type
Dedicated QinQ/Sub Access to L3 Services

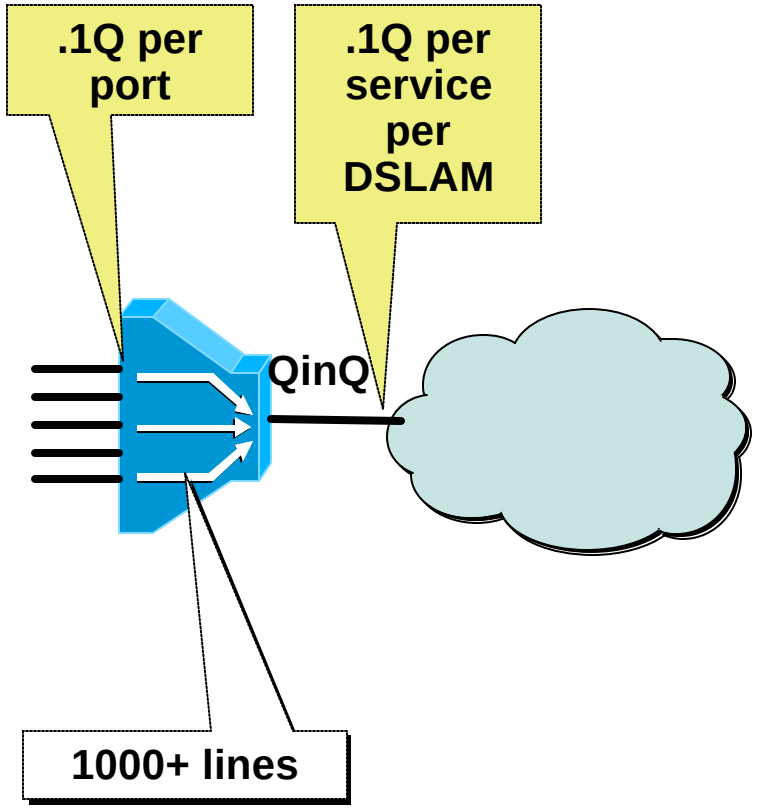
Cisco.com

Model 2



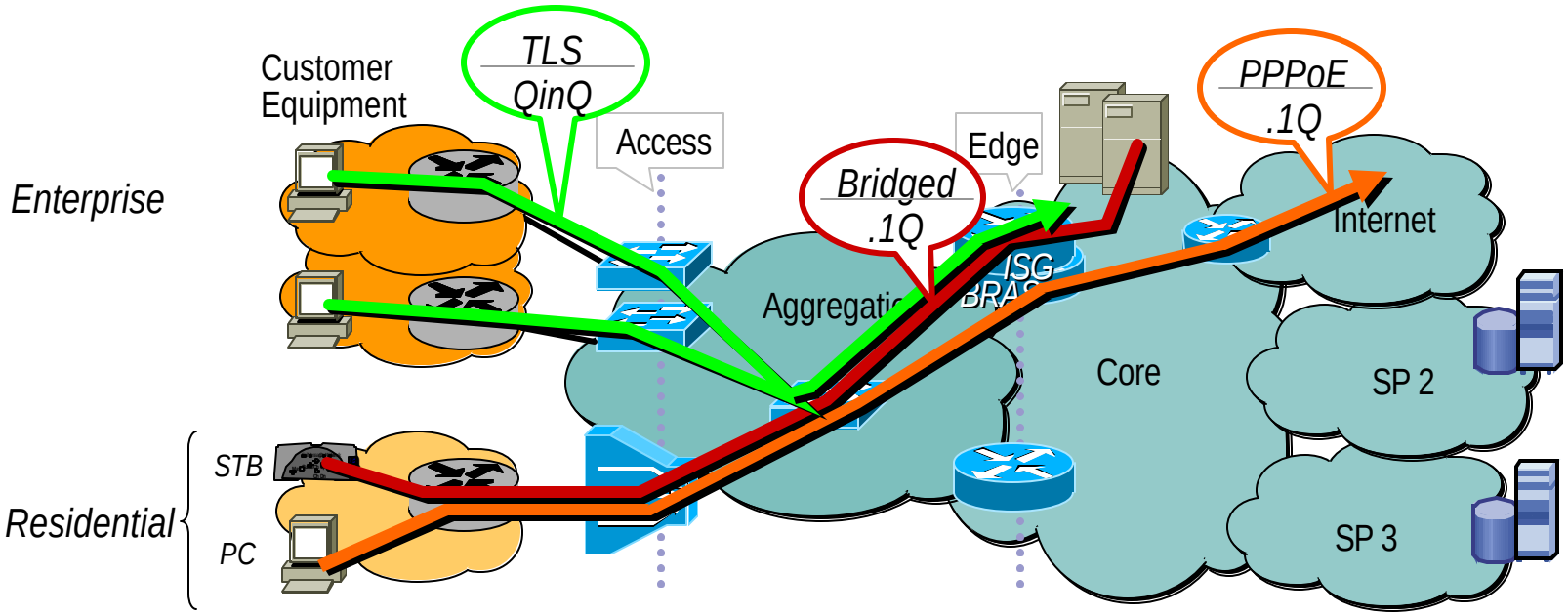
Even for a single UNI, logical device roles can be per VLAN, so one box may fill many roles

Review:
QinQ for DSLAM Aggregation?



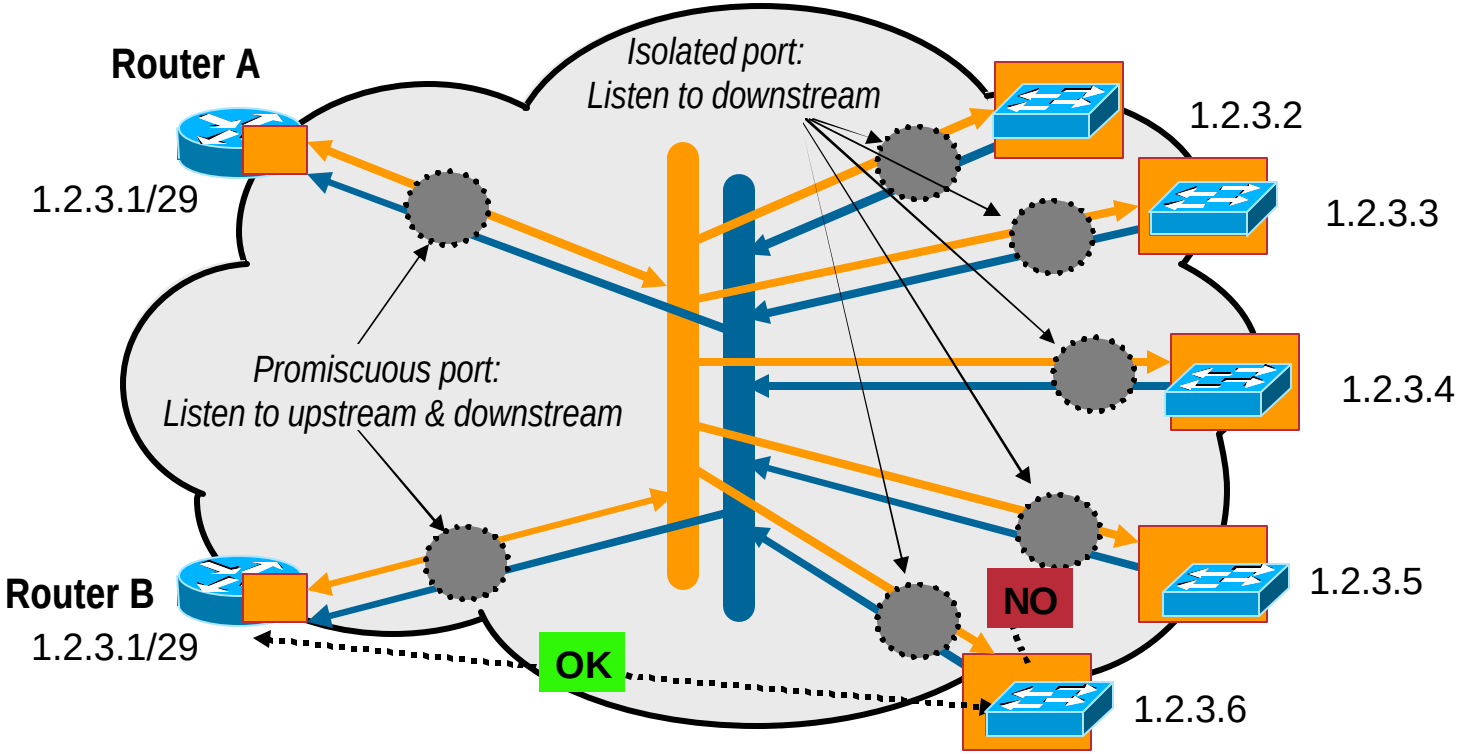
- **Pros**
  - **Model similar to current ATM**
  - **Provides subscriber isolation**
  - **Suitable for Business Services**
- **Cons**
  - **Provisioning Cost similar to current ATM network (circuit per subscriber)**
  - **4k Service Instances limitation not solved**
  - **Multicast replication at N-PE required**

Combined Aggregation Model



- **Business Customers**
  - **One subscriber per 802.1ad / “QinQ”**
- **Residential Customers**
  - **One VLAN per Service -> Scale, no VLAN exhaust**
  - **Combination of natively bridged services (video, voice) as well as PPPoE (current Internet Service)**

How to isolate multiple users on one VLAN? *Private VLANs!*

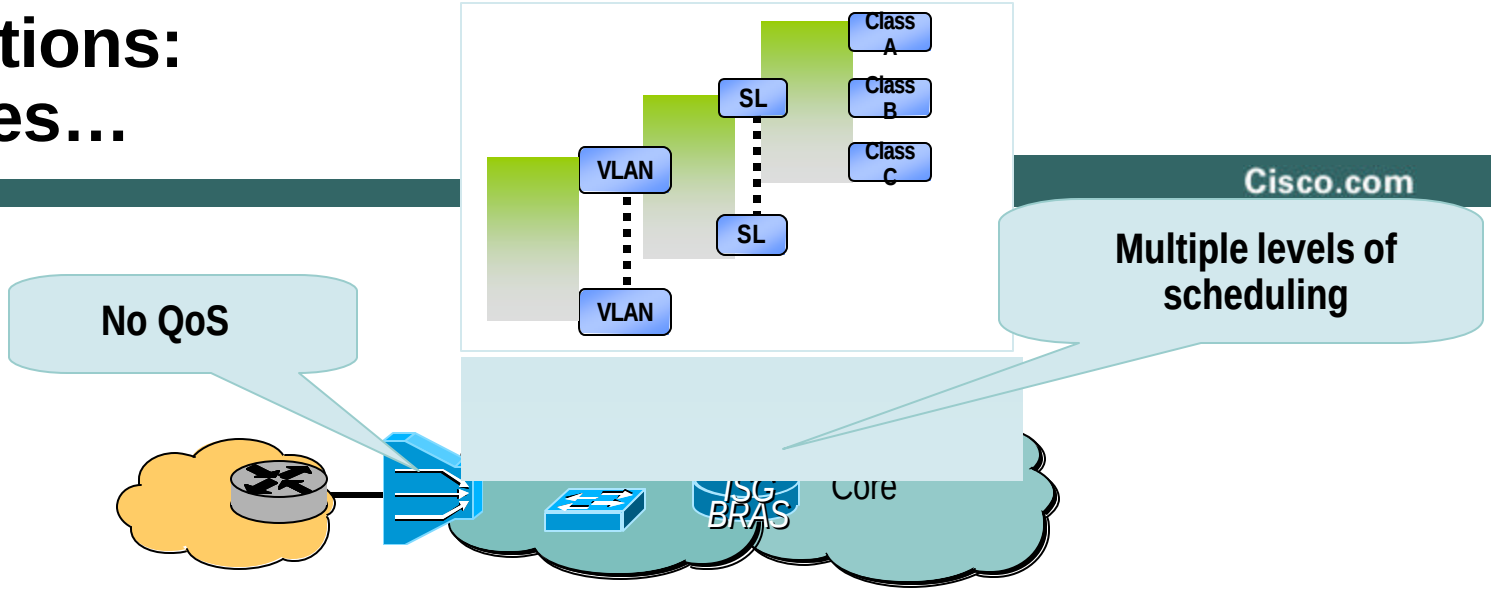


- **A few Routers, many Subscribers – ETTX, DSL-Aggregation…**
- **Two P-VLANs, one "Down", and one "Up" – using "shared VLAN learning" (802.1Q)**
- **Can be shared between switches (e.g. in a ring)**
- **All Hosts are isolated from each other**
- **Very Efficient Multicast replication through IGMP Snooping**

QoS Options: Examples…

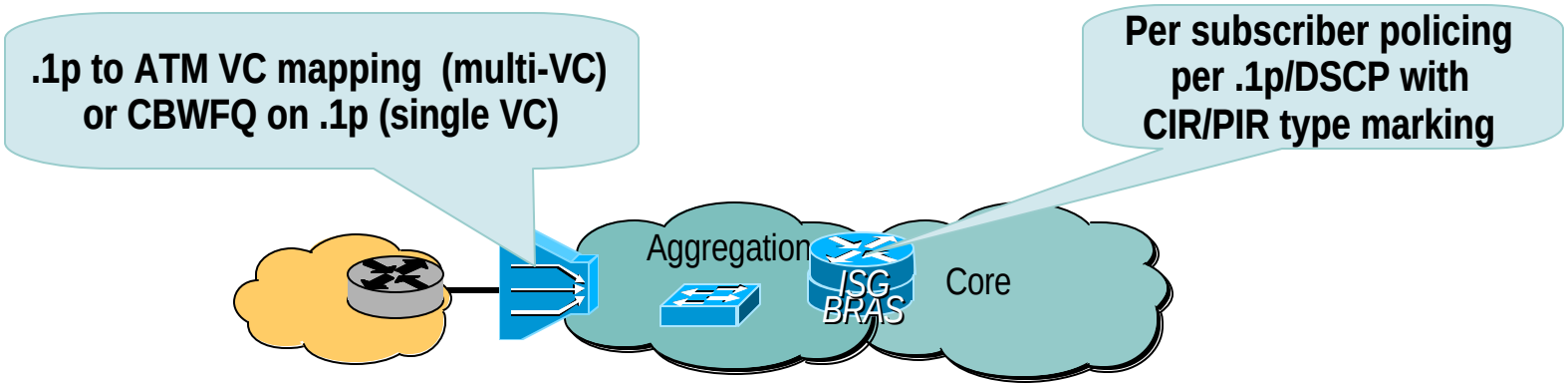
Cisco.com

Centralized QoS Model (TR-59 like)



Q: **How to account for traffic inserted *downstream* from the ISG/BRAS (e.g. VoD)?**
Q: How many levels of Scheduling on the ISG/BRAS?

Distributed QoS Model (Diff-Serv in Aggregation)



Q: Policing vs. Shaping for long-term/short term TCP sessions.
Q: QoS capabilities of DSLAMs?

Note: Many additional QoS Models exist.

Focusing the Key Challenges

One Integrated Access Network for Business and Residential Services

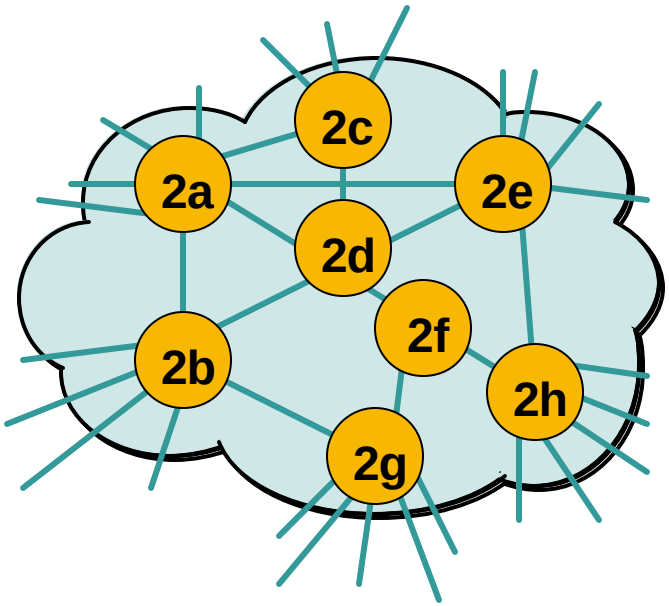
Cisco.com

- **Mapping customers to service instances (VLANs)**
  - **Scalability: Number of Service Instances (VLANs)**
  - **Subscriber Isolation**
  - **Transparency**
- **Scalability**
  - **Number of MAC-addresses**
  - **Topology**
- **Video Deployment**
  - **Large Scale Multicast Design**
- **Security**

- > 1M users total
  - 10.000s of business services
  - Residential Users: Wholesale and Retail
- 1000s of DSLAMs w/ > 1000 users per DSLAM
- 100s of video channels – broadcast TV and VoD

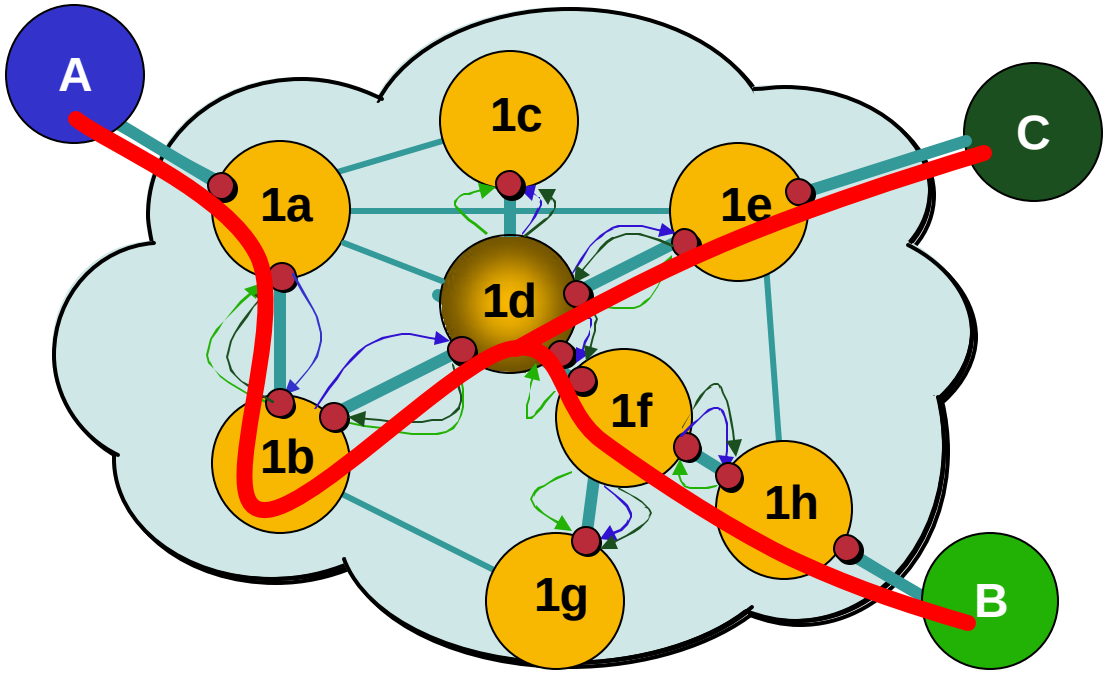
MAC Address Scaling
Too many MAC addresses to learn?

- **Bridges learn MAC addresses to efficiently fwd traffic**
  - **Memory is a limited resource**
  - **Example: 4k VLANs * 1k MAC addresses per VLAN == 4M MAC addresses to learn….**
- **Solution: Don't learn unless you have to...**
  - **Bridges with only 2 <u>active</u> ports in a VLAN do not have to learn for that VLAN.**
  - **Manage the amount of customer MAC addresses (SLA!)**



Scalable learning:
IEEE 802.1ad – clause 16.6 combined with MVRP

1. STP converges
2. MVRP converges
3. Bridges “count” active ports (●) per VLAN and apply scalable learning
4. Only Bridge 1d has to learn for the VLAN shown



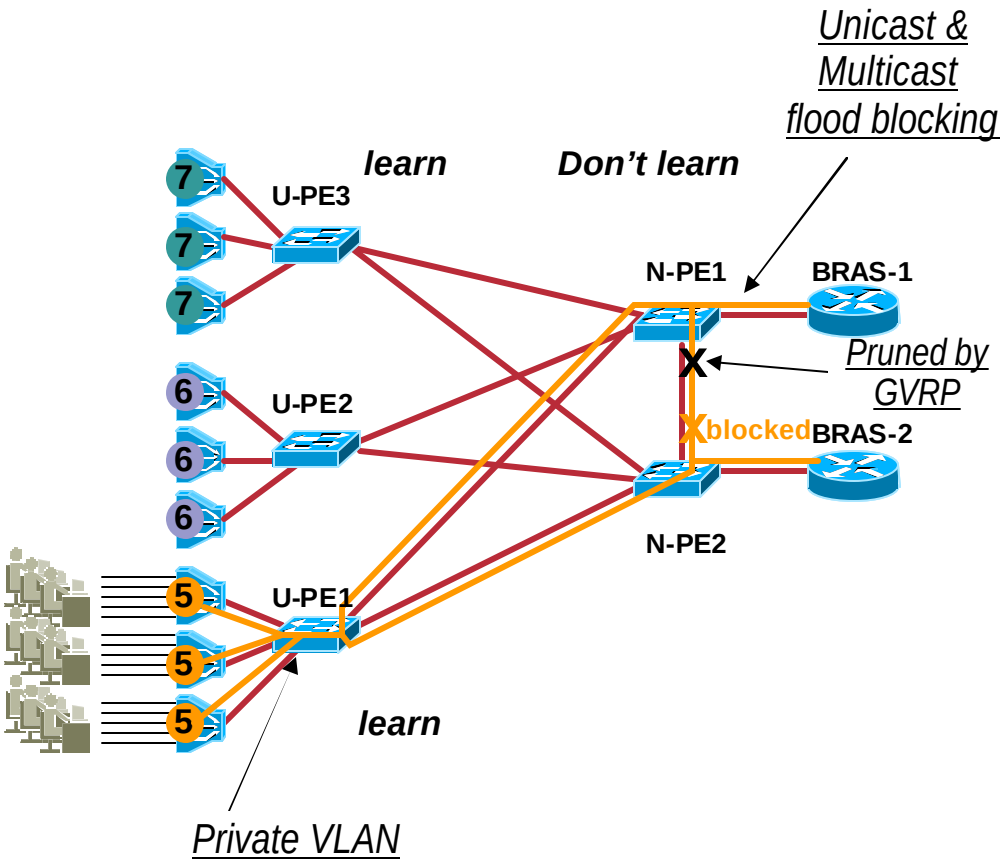
Note: Graphics simplified: Messages towards blocked STP ports not shown

IEEE P802.1ak – Multiple Registration Protocol (MRP) *supporting IEEE P802.1Q*

- **Define and Standardize the Successor the "GARP family" (GVRP, GMRP) for Providers**
  - **P802.1ak will define MVRP (Multiple VLAN Registration Protocol) and MMRP (Multiple Group MAC addresses Registration Protocol)**
- **Focus on scalability and rapid convergence**
  - **GMRP and GVRP were developed with Enterprise requirements in mind – Scalability was not the key focus**
    - **MRP will use an optimized way to encode state – to scale MRP protocols (MMRP, MVRP) to 4k VLANs**
  - **MVRP will provide for "rapid healing of network failures without interrupting services to unaffected VLANs" (from P802.1ak PAR)**
- **PAR approved in Oct/04**

Control the topology to make most efficient use of "Scalable learning"

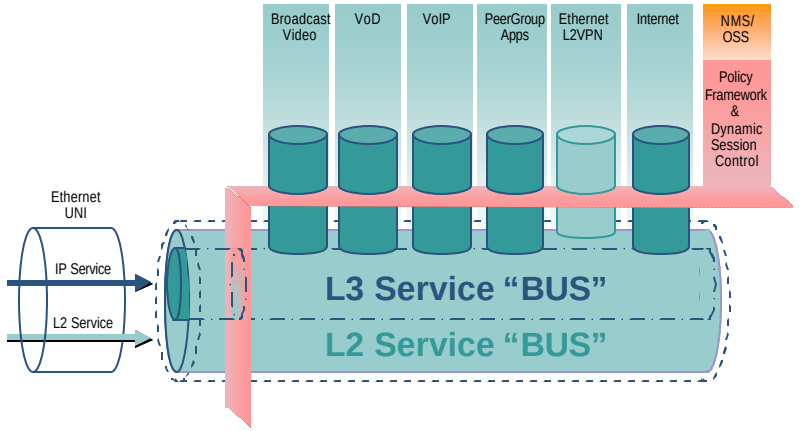
- **Constrain the topology so that core switches do not need to learn**
  - **VLAN per Service and Access Switch (U-PE) (multiple DSLAMs within a single VLAN)**
  - **Leverage Private VLAN**
  - **Access Switches learn**
  - **Core Switches don't learn, but leverage scalable learning (PVL) and GVRP**



Example of a constrained topology to avoid MAC-address learning on N-PEs

MAC-Address Scalability - Summary

- **If you Bridge, don't learn if you don't need to…**
- **Leverage the protocol which is best suited for Service delivery**



Employ the L2/L3 BUS Concept

L3VPN – IP/MPLS in the Access/Aggregation

Broadcast TV – IP multicast in the Access/Aggregation

Residential Internet Access – L2 Access/Aggregation

Focusing the Key Challenges

One Integrated Access Network for Business and Residential Services

Cisco.com

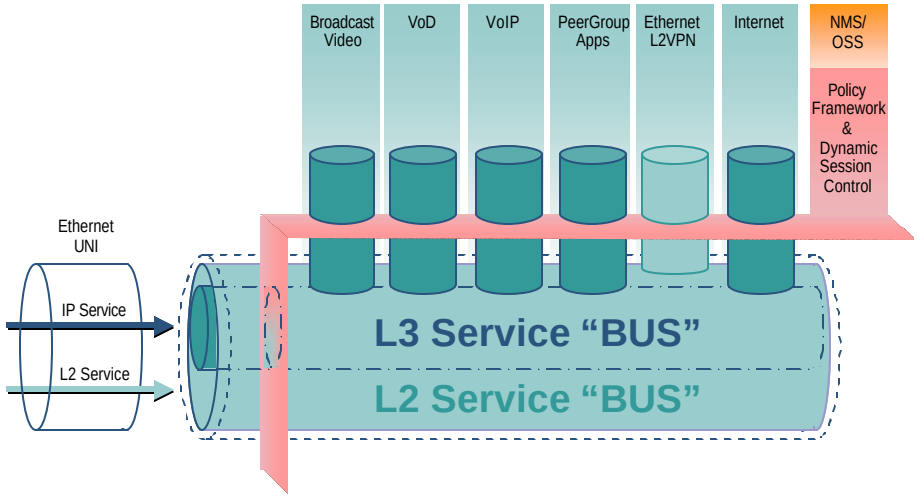
- **Mapping customers to service instances (VLANs)**
  - **Scalability: Number of Service Instances (VLANs)**
  - **Subscriber Isolation**
  - **Transparency**
- **Scalability**
  - **Number of MAC-addresses**
  - **Topology**
- **Video Deployment**
  - **Large Scale Multicast Design**
- **Security**

- > 1M users total
  - 10.000s of business services
  - Residential Users: Wholesale and Retail
- 1000s of DSLAMs w/ > 1000 users per DSLAM
- 100s of video channels – broadcast TV and VoD

Video Architecture Evolution

- **Cover multiple Designs from Video Head End to Set Top**

  Video Broadcast and Video on Demand



- **Architectural Evolution from L2 to L3 for Video**

  Early "ETTX" designs used L2-only access networks (cost driven)

  Apply Service-BUS (multiple service-tap points) concept w/ Service Driven Control Plane

    IP-Multicast to the access/aggregation for Video Delivery: Enhanced Scalability, Resiliency and Flexibilty

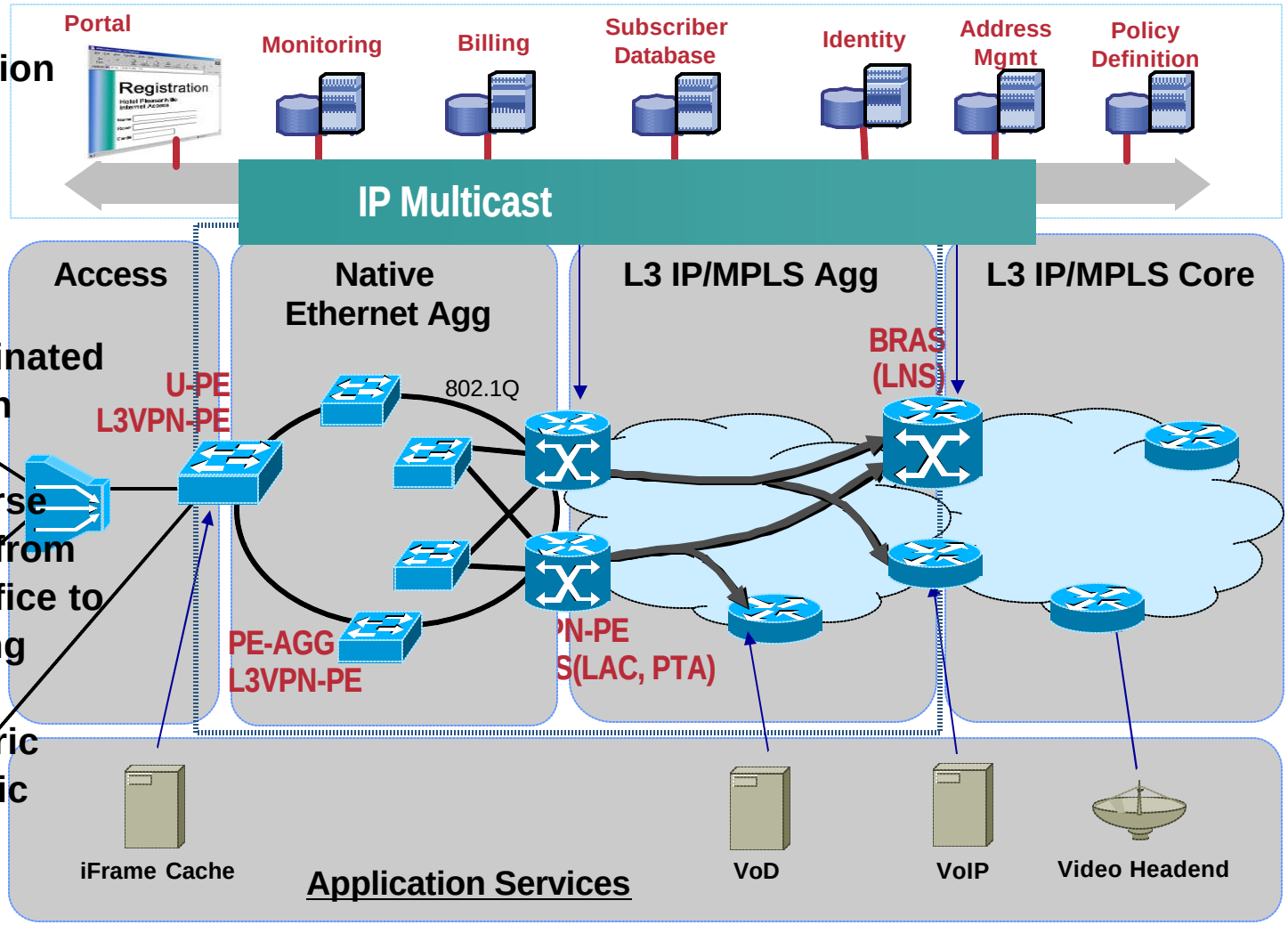
BB DSL High Level Target Architecture
Video Transport

Layer 3 Aggregation for Video in Distribution Network

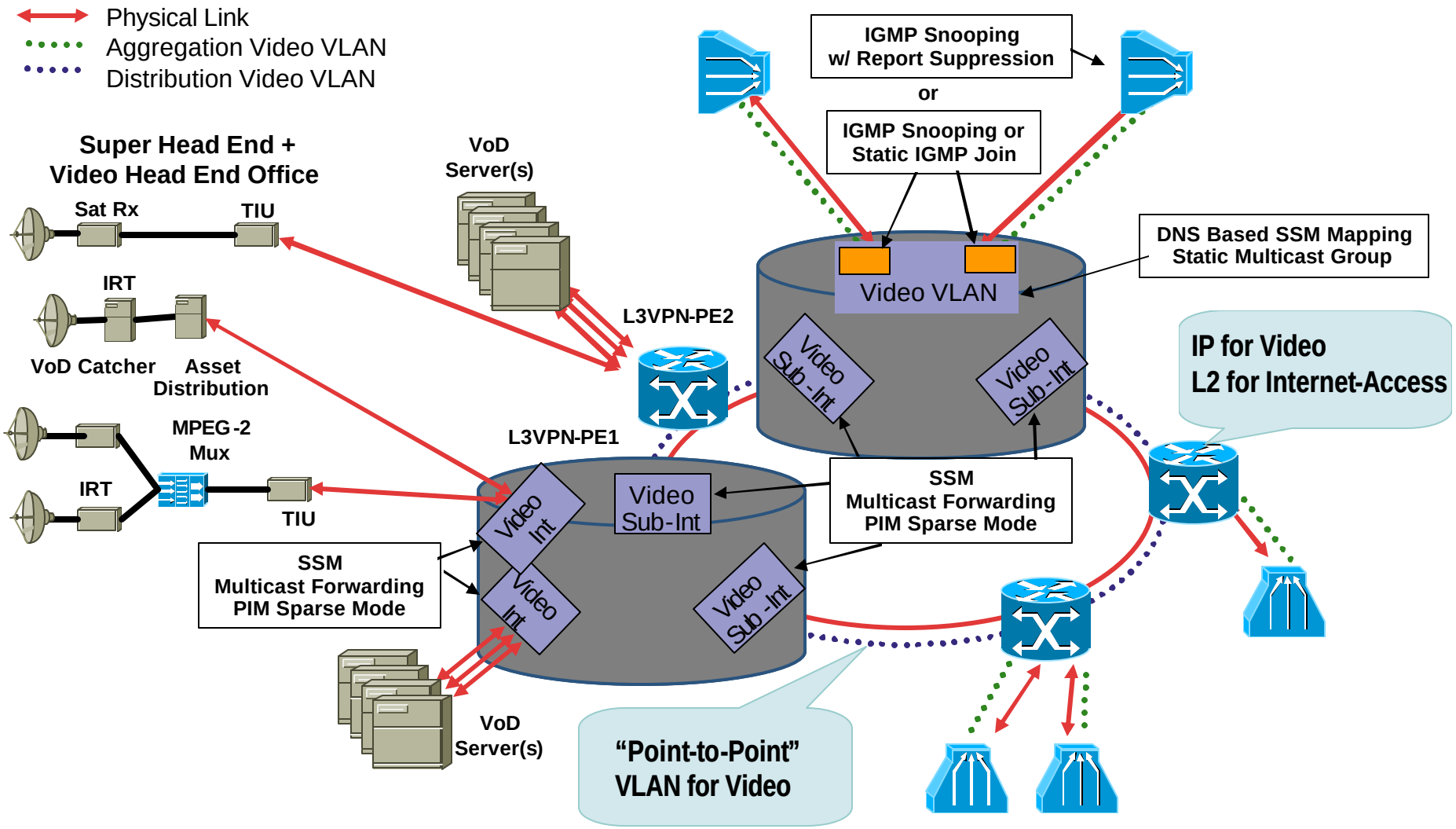
Video VLAN from DSLAMs Terminated on Aggregation Router

Video May Traverse Multiple Hops from Video Head Office to Video Switching Office

Support Symmetric and Asymmetric Transport



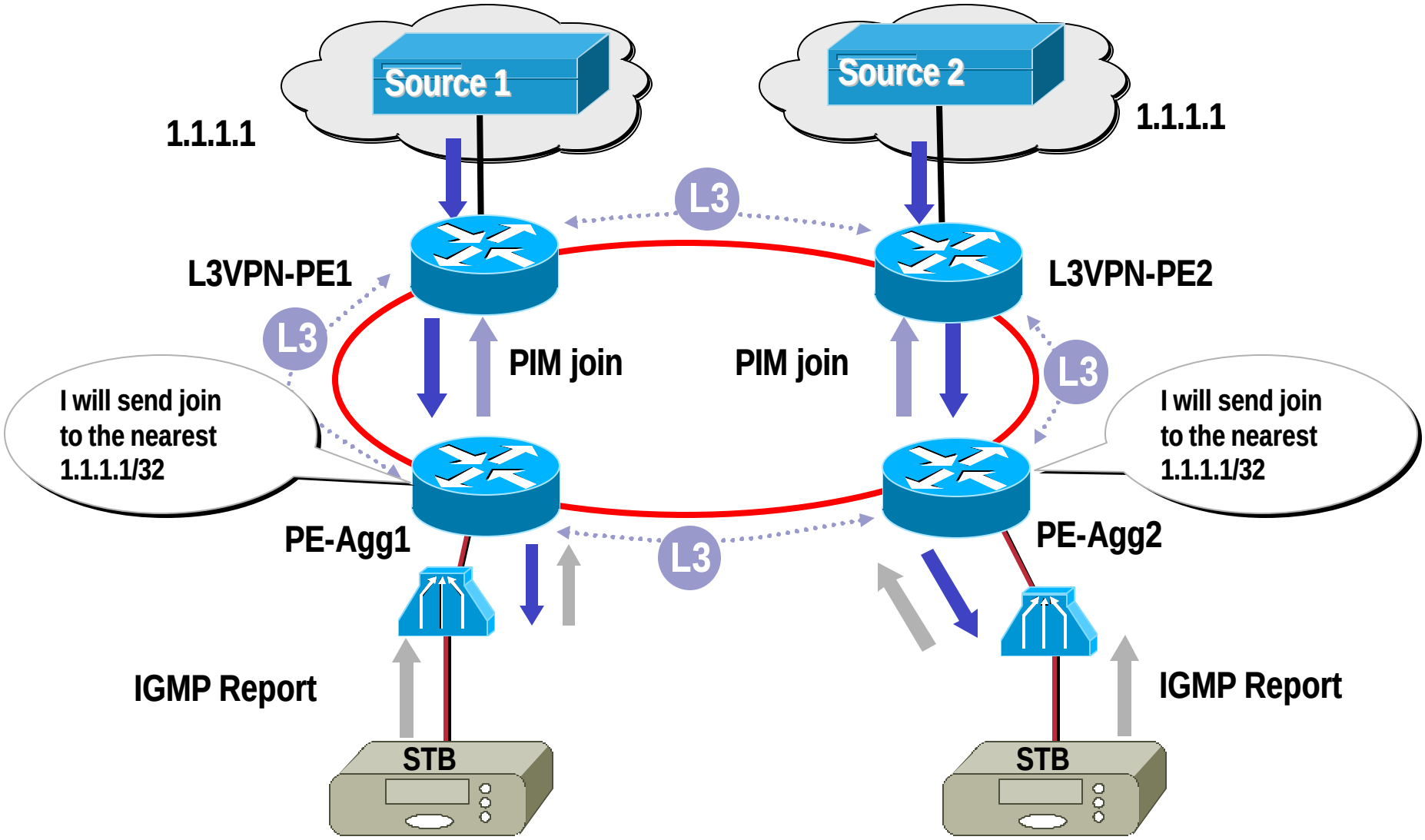
Multicast Forwarding
IP Multicast in the Access/Aggregation



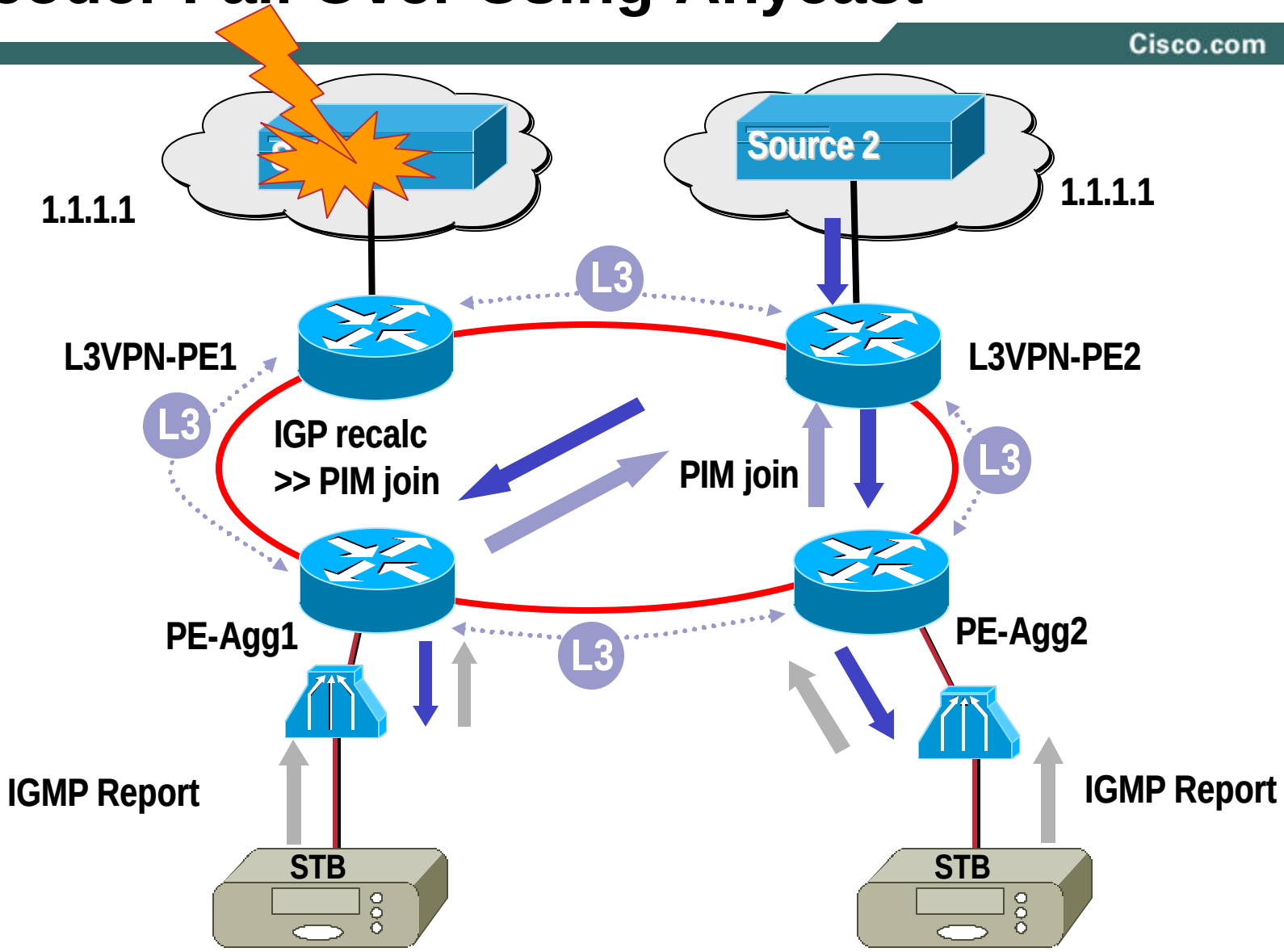
Why Layer 3 for Video in Access/Aggregation Network?

- Enables IP Multicast Replication in Distribution Network
  - Source Based Replication (SSM) More Secure
- Enables Anycasting for Multicast
  - Fast Failover (IGP fast convergence), Redundant Multicast Sources
- Avoid Multicast Fail Over Issues with L2 Forwarding
- Simpler VLAN topologies
  - Multicast and Unicast (Control-Traffic) in same VLAN
- Aggregation Supports Simultaneous L2 and L3
  - Catalyst Switches Support Different Switching Models on Per VLAN Basis
    - Layer 2, Layer 3, Layer 2 + Layer 3
- Architecture deployed in production networks today

Anycast Based Load Sharing



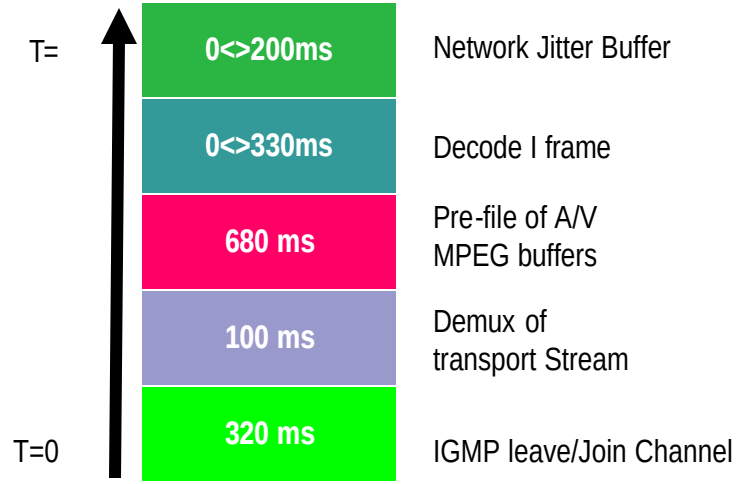
Encoder Fail Over Using Anycast



IP Multicast for Broadband TV Delivery
Channel Changing

Contributors to Channel Change Delay @STB

1. Multicast Leave for old Channel (50 msec)
2. Delay for Multicast Stream to Stop (150 msec w/ Fast Leave)
   - Delays Due to IGMP Queries / Timeouts on Access Link
   - Fast Leave Processing on DSLAM Removes This Delay
3. Multicast Join for New Channel (50 msec – 200 msec)
4. Jitter Buffer Fill (200 msec)
5. I-Frame Delay (500 msec – 1 sec)

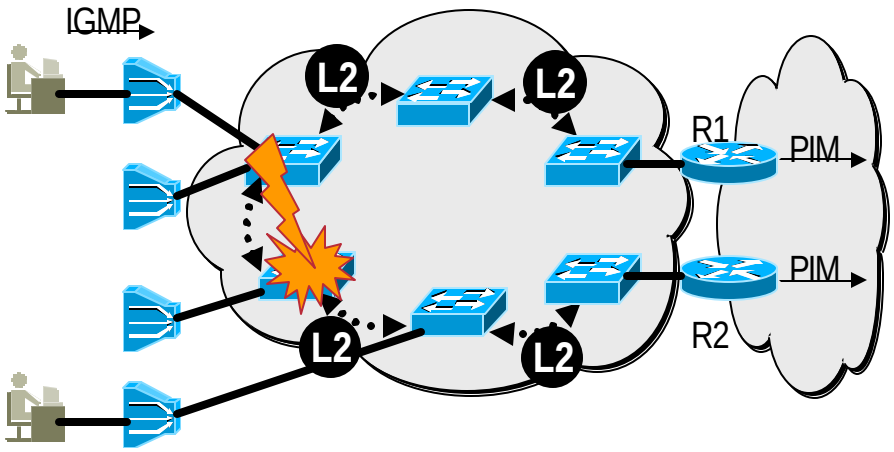


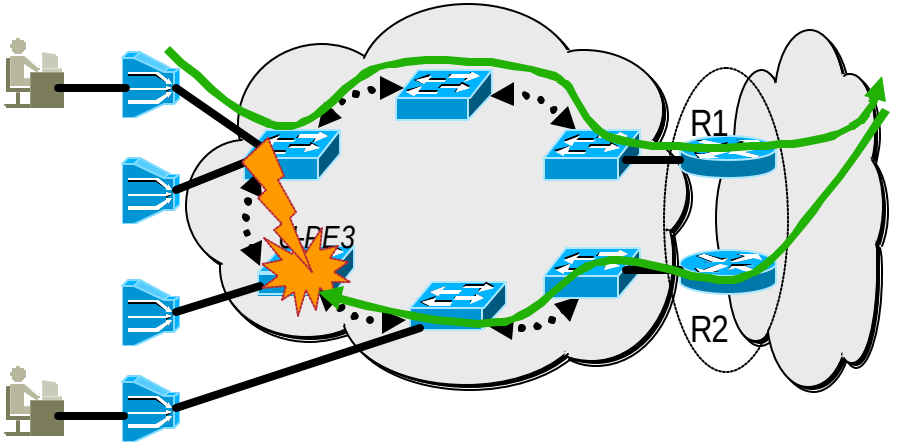
Signaling delay is negligible compared to the delay incurred by the video coding requirements

Forwarding Architecture
Redundancy

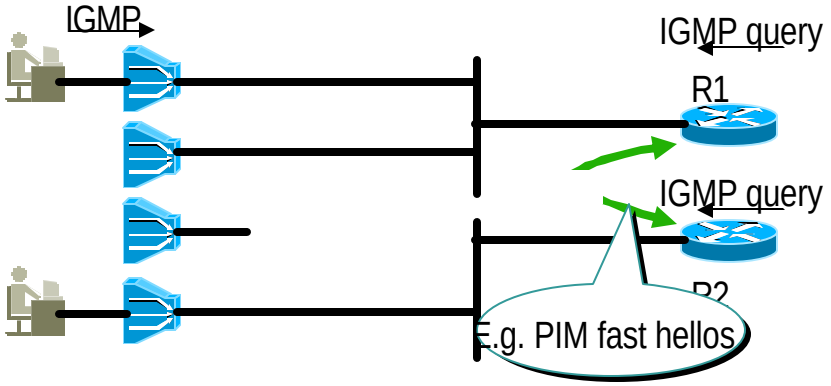
- **Dual L3VPN-PE Routers to Redundant Video Components**
  - **Video Servers**
    - **Load Balancing Achieved at Video Session Layer**
    - **Ensure that VoD Server Can Load Balance Across Pumps**
  - **Real Time Encoders**
    - **Redundant (Primary / Backup) Encoders Attached to L3VPN-PE Routers**
    - **Use Anycast Based Fail Over**
- **Distribution / L3VPN-PE Failures Detected by Routing Layer**
  - **Layer 3 re-convergence in Distribution Network on Failure**
  - **With OSPF tuning < 1 sec IP re-convergence achievable**

Architecture Redundancy Discussion Failover Scenarios (1/2)

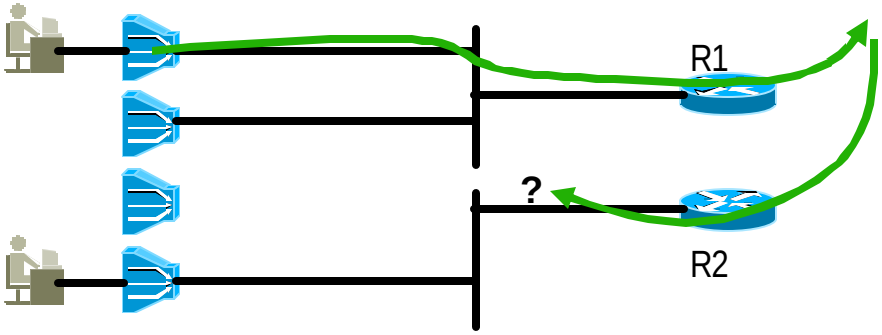




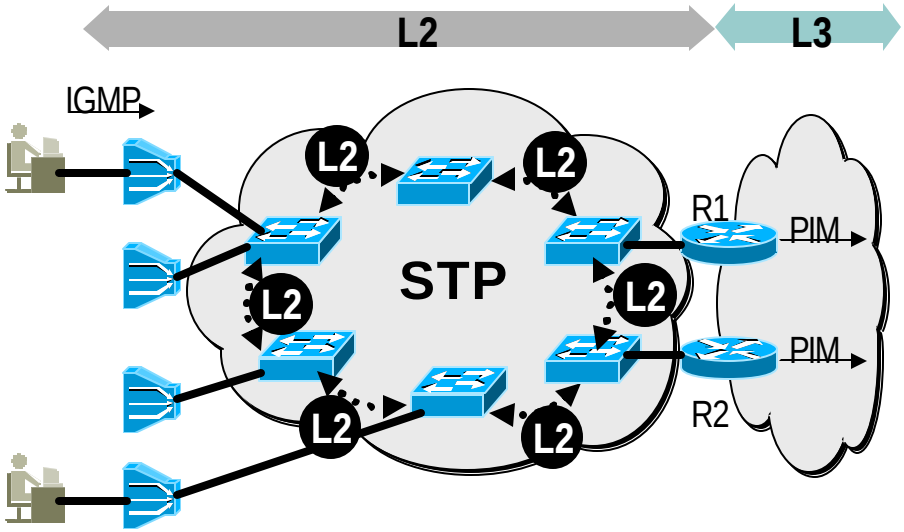
Logical view



Logical view



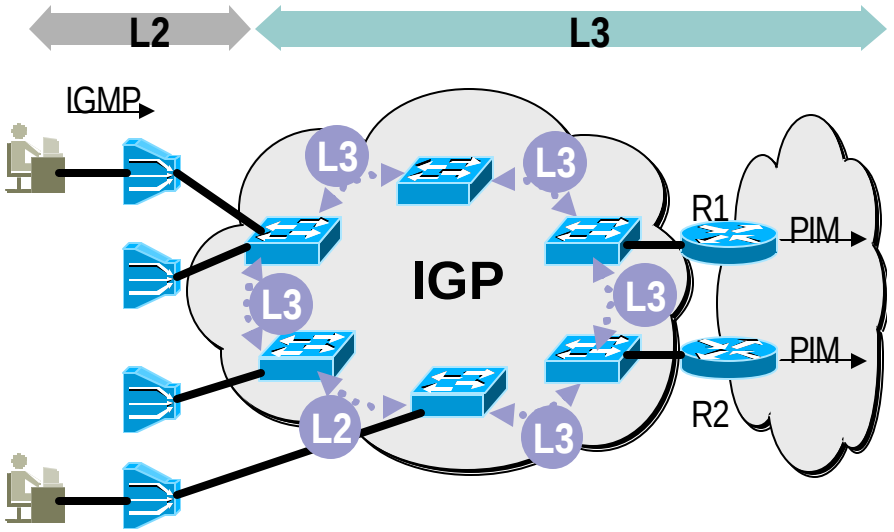
Architecture Redundancy Discussion
Failover Scenarios (2/2): Solution Approaches



- **Both: Video (mcast) and video control (ucast) delivered at L2**

  (traffic sourced into same vlan by STB – if different fwding for L2 and L3 DSLAM/STB/HAG would need separate traffic (and control such as IGMP, DHCP etc.)

- **STP (802.1w/s) in the aggregation network avoids traffic-blackholing**
- **L3-IP-Mcast benefits cannot be leveraged in the agg network**



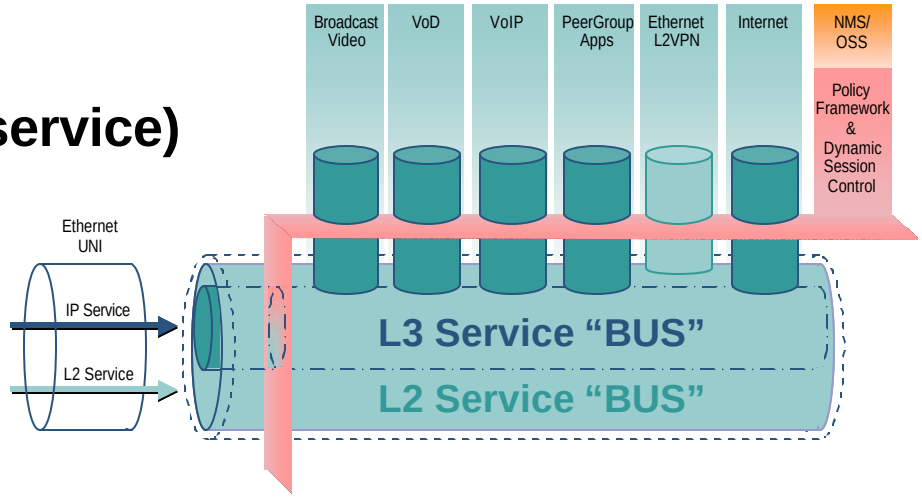
- **Both: Video (mcast) and video control (ucast) delivered at L3**

  Aggregation is L3 only for video (total service separation).

- **L3 IGP (OSPF/ISIS) for protection**
- **Leverage L3-IP-Mcast benefits at the aggregation**

Total Service Separation

- **Apply Service BUS concept (separate address space per service)**
  - **Video = VoD Servers, Middleware, Real Time Encoders**
  - **Voice = Voice Gateways**
  - **Internet Access = BRAS**



- **Individual Forwarding Infrastructures can be different**
  - **Optional separate Physical Media per Service in Residential Network (Unidirectional links)**
    - **Simplifies Service Based Traffic Classification**
    - **Different Services have different profile requirements (BW, QoS,...)**
- **Supports Service Provider Organizational Structure**
  - **Different management teams**

Focusing the Key Challenges

One Integrated Access Network for Business and Residential Services

Cisco.com

- **Mapping customers to service instances (VLANs)**
  - **Scalability: Number of Service Instances (VLANs)**
  - **Subscriber Isolation**
  - **Transparency**
- **Scalability**
  - **Number of MAC-addresses**
  - **Topology**
- **Video Deployment**
  - **Large Scale Multicast Design**
- **Security**

- > 1M users total
  - 10.000s of business services
  - Residential Users: Wholesale and Retail
- 1000s of DSLAMs w/ > 1000 users per DSLAM
- 100s of video channels – broadcast TV and VoD

Ethernet Security

Cisco.com

- **Service-Variety / enhanced Service-Attributes result in possibly new security threads**
  - **Layer2/3 different from simple Layer1**
  - **E.g. Denial of Service attack can impact SLA (availability)**
- **Ethernet-centric attacks**
  - **MAC, ARP, VLAN-Hopping, SPT, CDP, DHCP,…**
  - **Pro-Active and Re-Active Defence required**

Attacks and Defensive Features/Actions

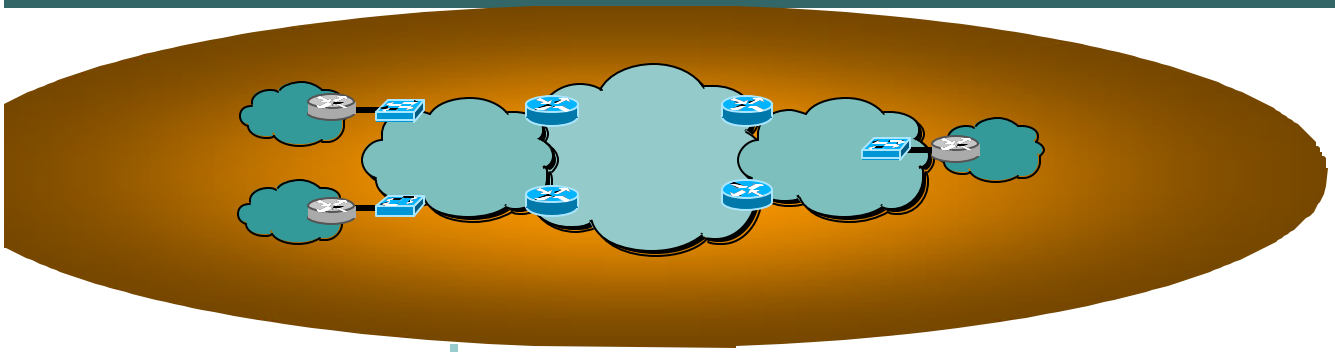
Cisco.com

Attack	Defensive Features/Actions
MAC attacks (CAM table overflow)	Port Security
ARP attacks (Arp spoofing, misuse of gracious ARP)	Private VLANs, wire-speed ACLs, dynamic ARP inspection
VLAN hopping, DTP attacks	Careful configuration (disable auto-trunking, used dedicated VLAN-ID for trunk ports, set user ports to non-trunking, avoid VLAN 1, disable unused ports,…)
Spanning tree attacks	BPDU Guard, Root Guard, MD5 VTP authentication (consider whether you need VTP at all)
DHCP Rogue Server Attack	DHCP snooping (differentiate trusted and untrusted ports)
Hijack Management Access	Secure variants of management access protocols – not telnet etc, but SSH,… as well as out of band management)
Pro-Active Defence	Deploy MAC level port security, wire-speed ACLs, VMPS, URT, 802.1x

Protect the Access.... (Ether-DSLAM or Access-Switch)

- **Security Features – Protect the Edge**
  - **Limit number of MAC addresses per port**
  - **L2 isolation between ports and across multiple switches (PVLAN or equivalent)**
  - **Traffic control (mcast/bcast storm control)**
  - **Support L2 and L3 ACL**
    - **ARP Spoofing, DHCP Attacks, IP-Addr. Spoofing**
  - **DHCP snooping with IP source guard**
  - **IGMPv3**
  - **IGMP filtering**
  - **802.1x**

Agenda



- **Integrated Access/Aggregation Architecture**
  - **Towards an Integrated Access/Aggregation Architecture**
  - **Focusing the Key Challenges**
    - **Customer to VLAN mapping**
    - **MAC Scalability**
    - **Scalable Multicast Deployment**
    - **Security**
- **Service Control and Subscriber Management**
  - **Sessions, Identity, Policies**
  - **Case Studies**
  - **Configuration Brief**

Broadband in a Consumer's World

Consumers express identity – and require customization

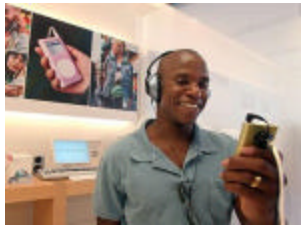
Cisco.com


Online Gaming and Communities

Blogs

Specific Knowledge

Customized Content (ie. podCasting)



"The less control a company has over its marketing message, the better its credibility."

"Brands no longer belong to a company but to the people who use [the company's products]"
The Economist April 2, 2005

Users create their own UNIVERSE

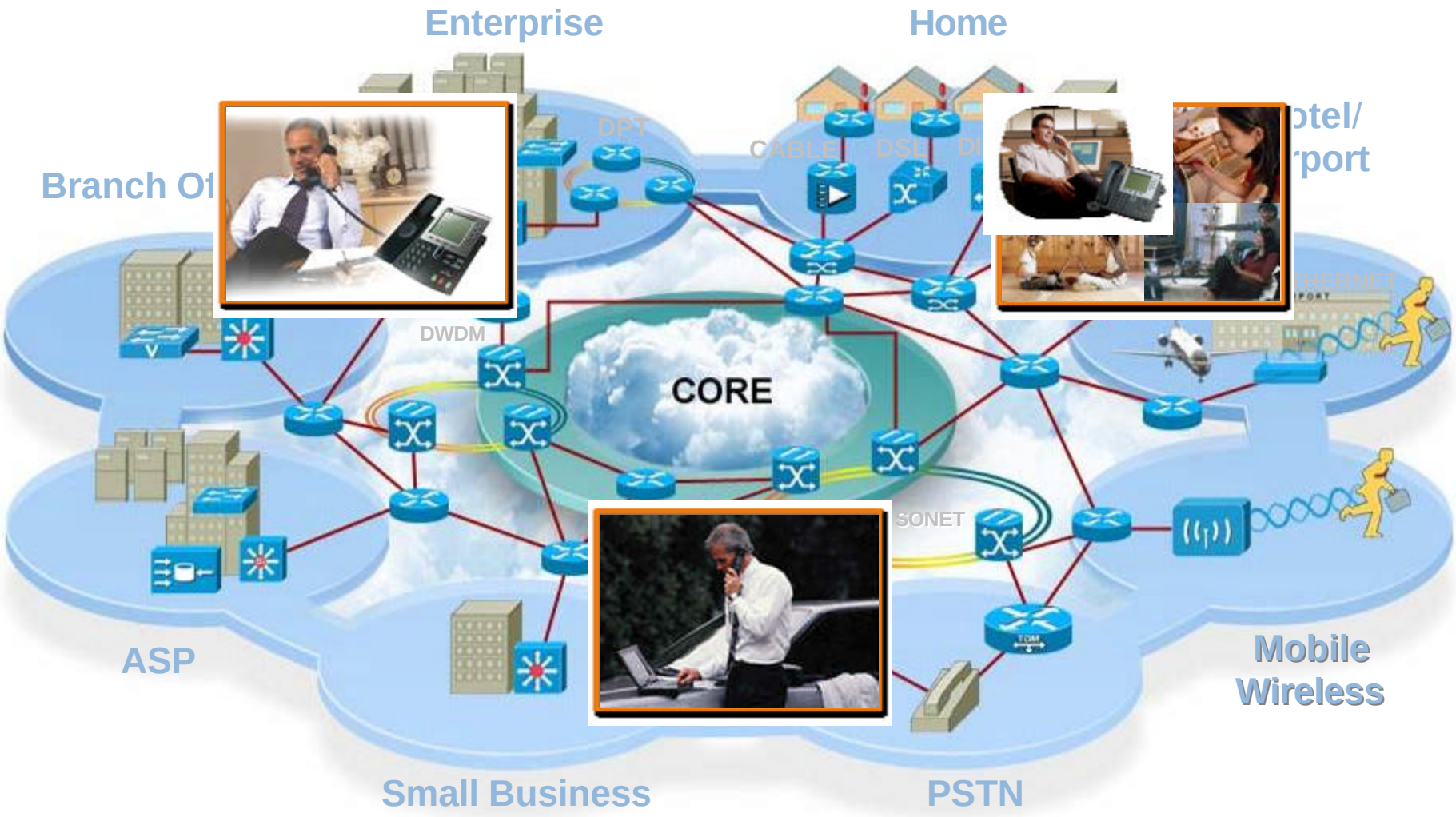
- **Peer Group dependent Identity and Behavior > High Degree of Customization**
- **Ubiquitous Access to Services – different locations, different access methods and media**
- **Wide Service variety, New Services adopted quickly**

The User is King in Broadband – Success or Failure in the Broadband Market depends on how well the SP will be able to create and support the users Universe…

Triple Play on the Move

Service Continuity, Customer Stickiness

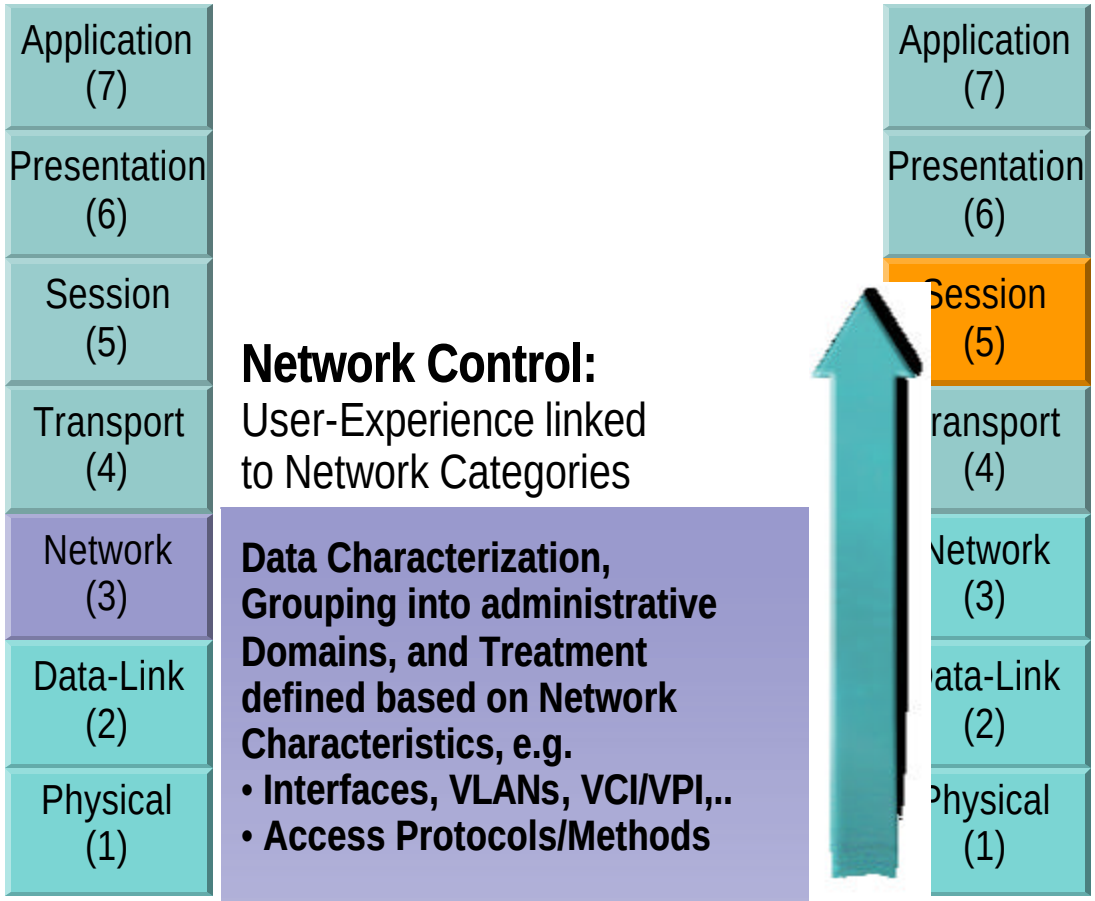
Cisco.com



Building the Users Universe is all about the Session

Identify the User and treat him according to the definition of his Universe

Virtualization of the Network Layer for the User



Network Control:
User-Experience linked to Network Categories

Data Characterization, Grouping into administrative Domains, and Treatment defined based on Network Characteristics, e.g.
- **Interfaces, VLANs, VCI/VPI,..**
- **Access Protocols/Methods**

Session Control:
"User-Aware Network"

Data Characterization, Grouping and Treatment defined independent of Network Characteristics.

Session (formal):
"A set of policy associated with a L2/L3 classifier for a single billing entity"

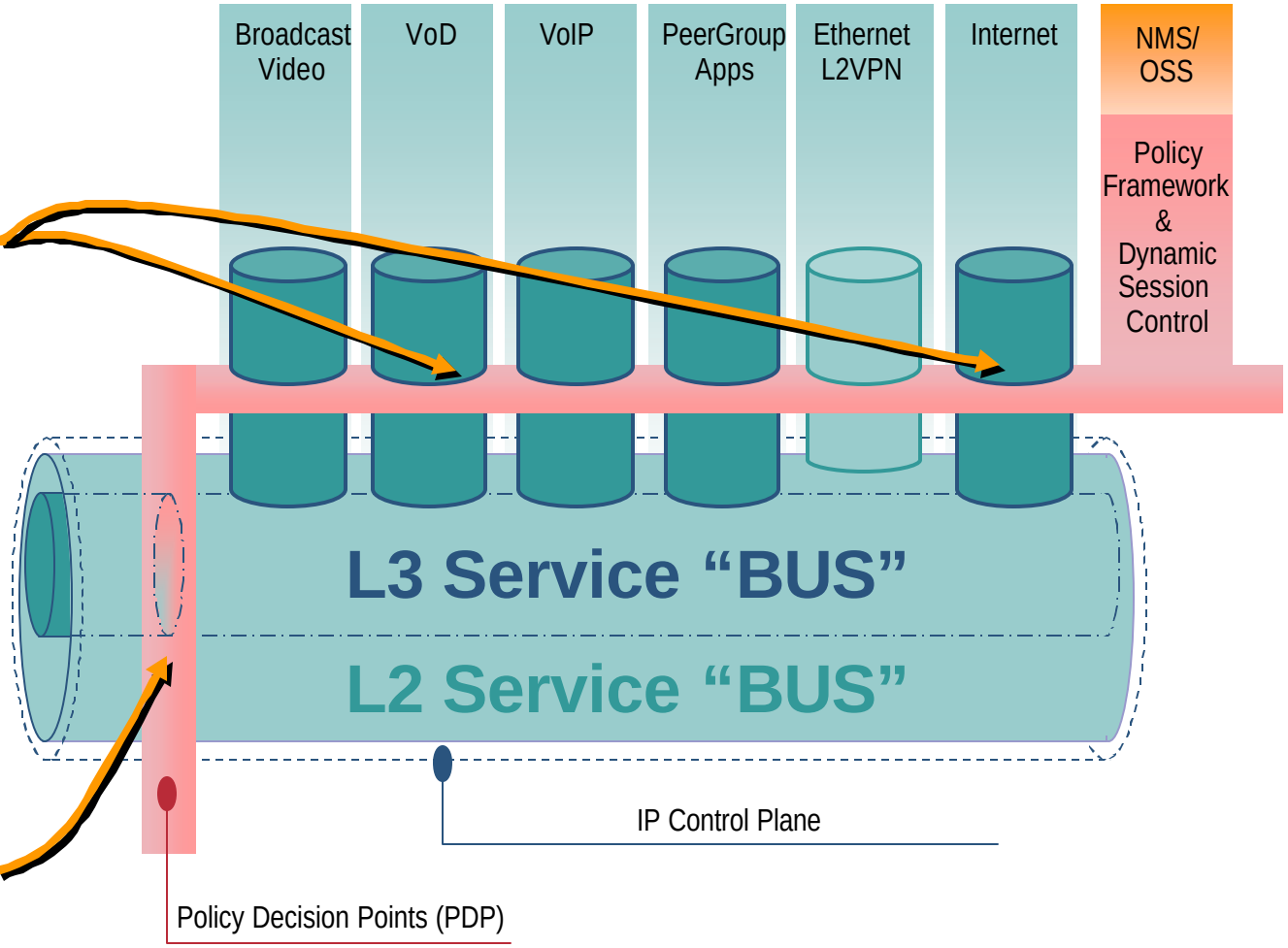
...or: one or multiple data flows which all fall into the same well-defined category (e.g. all flows of one user towards a specific service)

Architecture Vision

Controlling the Service "Tap" Points

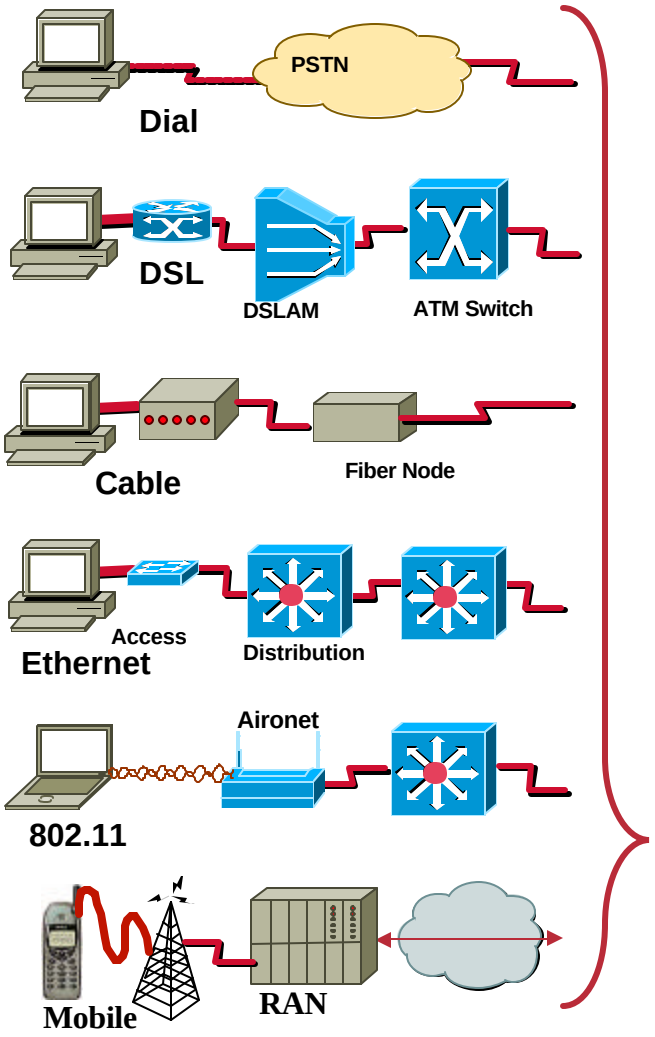
Session recognition and session treatment may be different for different service tap points

Session treatment capabilities (e.g. Policing, shaping, re-direction...) depends on service access (box and interface capabilites)



Includes potential Session Control for Services which do not connect to a Service Tap Point (e.g. Consumer hosted Services)

Generic Session: Common Services, Media Independent



Common Session-Services

Well-known and new Session-Services in IOS:

Examples: Port Bundle Host Key, Prepaid, Layer 4 Redirect, MAC based authorization, VRF Transfer, DHCP Proxy with Policy, Session Dynamic QoS Control,…

Common Generic Session Type

New in IOS

Created at first sign of subscriber activity

Common context on which session-services/policies are activated

Inherent Part of IOS

Dial | DSL | Cable | Ethernet | 802.11 | Mobile | Future..

Different Access Media and Protocols

Stepping Up to Session Control

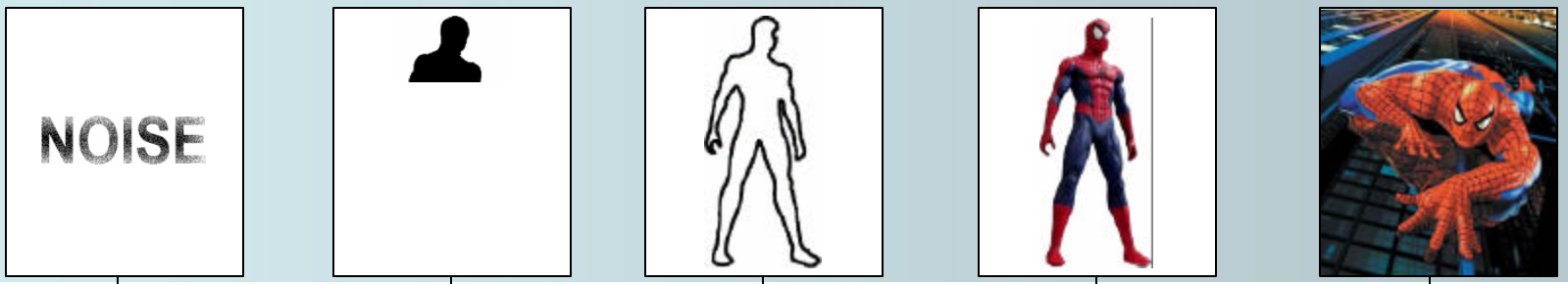
- **Identity**: ***Who*** **is the user?**
  - **Devices, Profile, Location, Presence**
- **Policy**: ***What/Which*** **Services can the user use or access?**
  - **Within what timeframe**
  - **To what extent**
  - **Under what rules**
- **Mobility**: ***Where*** **can the user roam?**
  - **Track/recognize the devices across carriers**
  - **Maintain the session across multiple networks**
  - **Offer all services in all locations**
- **Dynamics**: ***How*** **can I dynamically control resources?**
  - **Interwork and provide rich media control**
  - **Monitor and charge on a per service/per user basis**
  - **Enable application awareness**

Identity: User Identification in a Packet Network
Identity Database filled over time…

Cisco.com

"Real" World Identity Gathering

"Something" + Human Being + Male + SpiderMan + At Work in NewYork



T=0 T=t1 T=t2 T=t3 T=t4

"Packet Data" World Identity Gathering

T=0	T=t1	T=t2	T=t3	T=t4
Active connection to DSLAM port: Provisioned state	DHCP-Discover	User Authenticates himself: Put into VRF of his ISP:	Updated Authentication via Portal	Update from Presence Server
Identity Database	Identity Database: User MAC, Port-ID (Opt. 82)	Identity Database: User MAC, Port-ID (Opt. 82), IP Address/Subnet	Identity Database: User MAC, Port-ID (Opt. 82), IP Address/Subnet, User Service Profile	Identity Database: User MAC, Port-ID (Opt. 82), IP Address/Subnet, User Service Profile, Current User Location

Types of Identity in a Data-World

- ***Primary key***

  A unique identifier which represents a subject, e.g. a user-name

- ***Credential***

  A password or cryptographic signature used to validate a subject's primary key

- ***Alternate key***

  An additional key that is also unique to a subject, e.g. a MAC address

- ***Foreign key***

  A non-unique key that is associated with a subject, e.g. a port ID

Observations: Identity in a Packet Network

- **Identity-Information becomes a function of time**

  Identity Information is part of the Session Information set and gathered over the session lifecycle

- **"Multi-Dimensional" Identity**

  Identity Information gathered from multiple sources and events, not necessarily from a single construct (e.g. like a PPP session)

- **Identity Information gathered in the Packet Data-Path**

  Can be stored on a central repository

  Can be kept on the network element

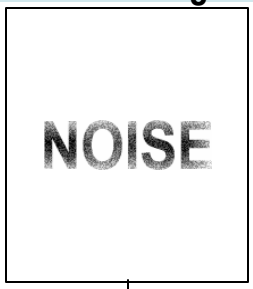
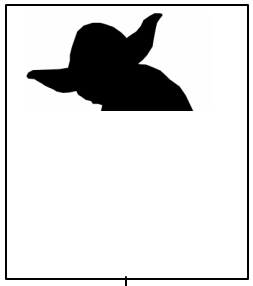
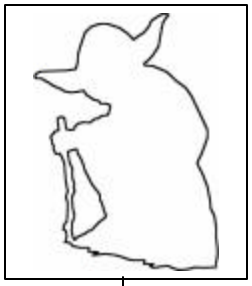
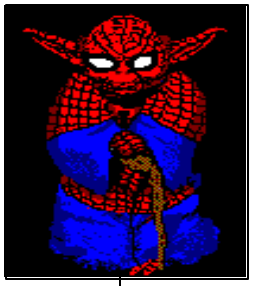
  Both: Keep information locally, replicate to central repository

- **Network Elements (Service Gateways) require knowledge of the Identity (as part of the session context) to apply Session-Services (e.g. policing, shaping, redirection, …)**

  As such, local caching of Identity Information enhances scalability (no always a request to central repository required to access identity information)

Leveraging "Identity in a Data World"
Events, Conditions and Actions

Cisco.com

Identity DB	"Something"	"Creature"	"Humanoid"	Yoda	Yoda ?!?
					
	T=0	T=t1	T=t2	T=t3	T=t4
Event	DHCP-Discover (w/ Option 82, PortID)	Port-ID Auth. failure	User Standard login at Portal	Updated login at Portal: Yoda	ISP security alert: Yoda infected with Spiderman virus
Condition	Always	Always	Successful Authentication	Successful Authentication	Traffic from Yoda-IP-Addr
Control Action	Authenticate PortID or Mac-Addr	Authenticate User via Portal			Re-Authenticate User via Portal
Traffic Action		L4-redirect all traffic to Portal	Allow Internet Access; No access to adult content	Allow access to Jedi community (place into Jedi VRF)	Quarantine infected Yoda (no access anymore)

"Policies"

Session-Services and Policy

- A *session-service* is essentially a collection of policies that are applicable to a *subscriber session*
- *Policies* define all aspects of subscriber session processing
  - Traffic Policies: Define handling of data packets
  - Control Policies: Define handling of System Events
    - Policy Rules + Decision Strategy
      - Event ? Condition ? Action
- Services and policies may be provisioned locally or stored in an external repository or policy server
  - Local Policy Definition – CLI leveraging Cisco Common Classification Policy Language (C3PL)
  - Central Policy Definition – e.g. in RADIUS
- External service definitions may be retrieved on demand or dynamically updated

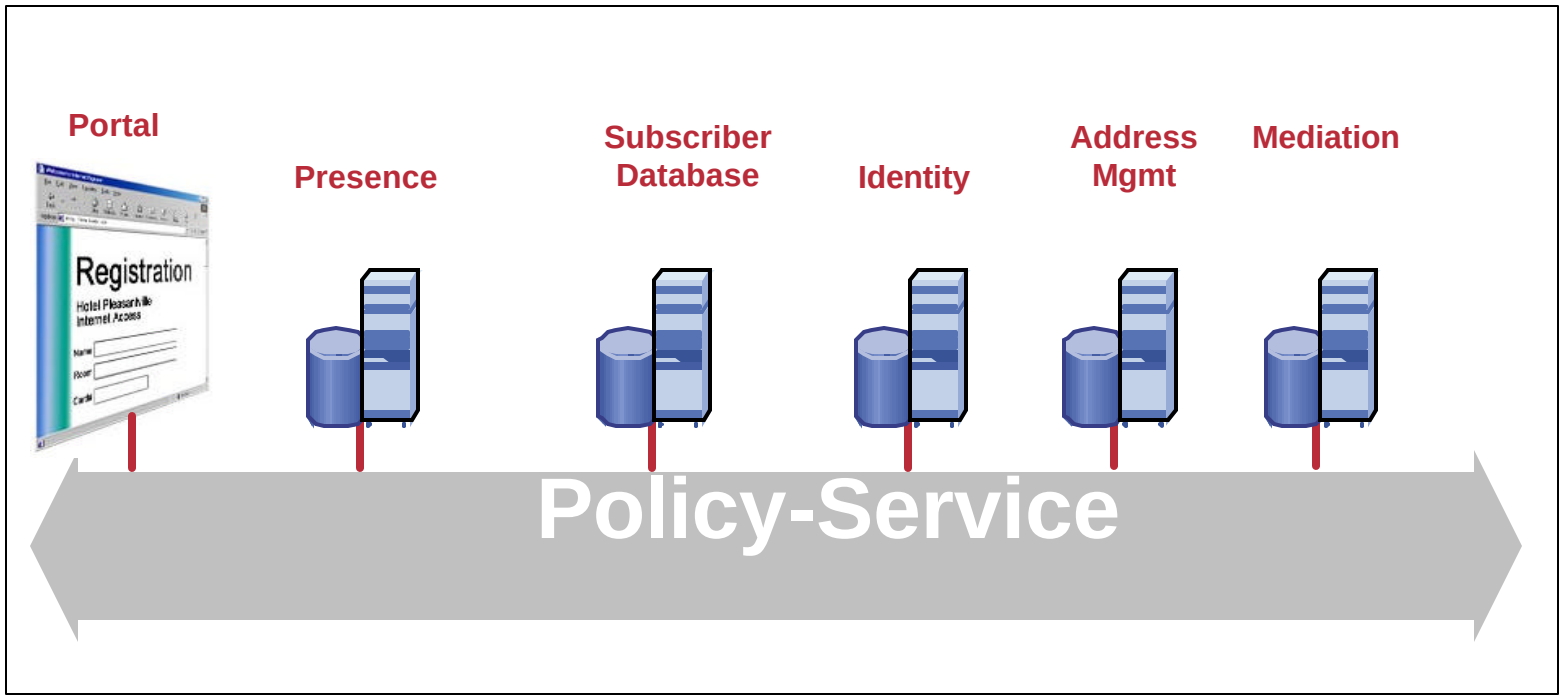
Policy: The legal system of networking

Cisco.com

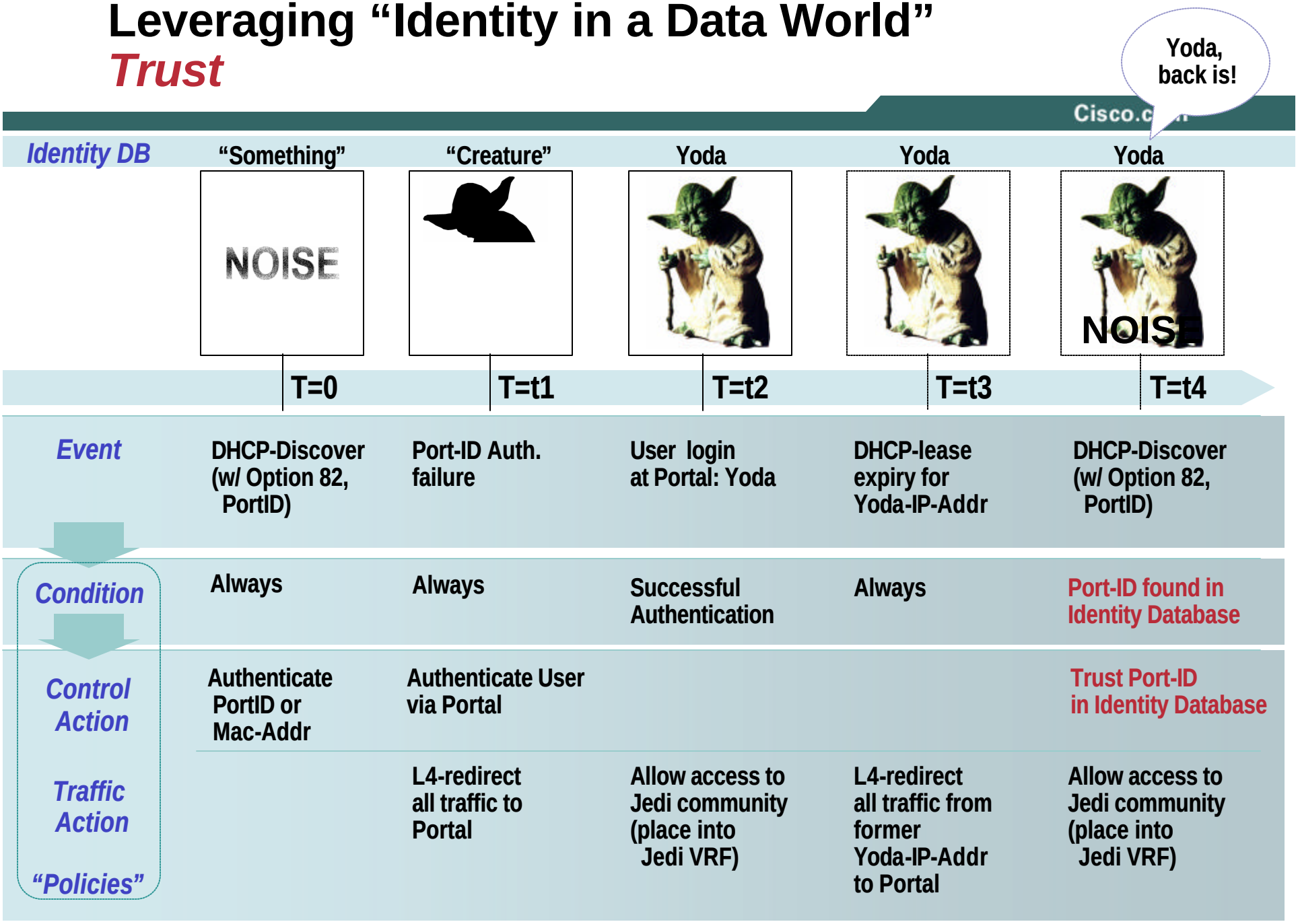
Governance Policy	Networking Policy
Laws – Represents the policy/rules.	Policy Information Model – Represents policy rules.
Courts – Make the decisions based on the laws.	Policy Decision Point (PDP) – Makes decisions based on policy.
Law enforcement services (police) – Enforce the decisions of the Courts.	Policy Enforcement Point (PEP) – Enforces the decisions.

Applications that have a need to set policy

A range of applications want to control the networks policies. If we view the section that interacts with subscribers to control service needs, some commonly seen elements are:



Leveraging "Identity in a Data World"
Trust



Identifying subscribers
Levels of trust

Different *trust* levels give rise to different access models: -

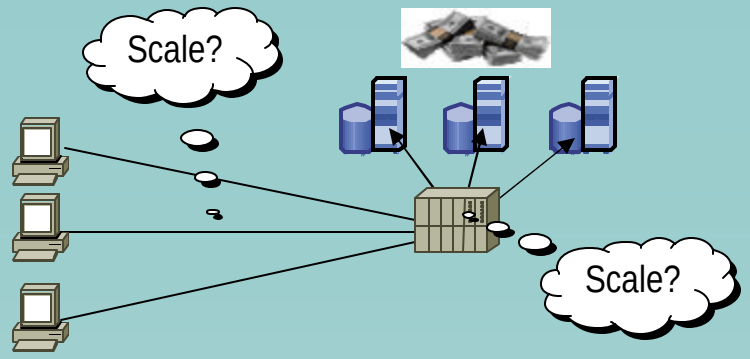
1. **Where fixed identifiers exist, e.g. Line ID, MAC address, *authentication* may be unnecessary. Otherwise…**
2. **Following *authentication*, unique keys may be trusted for session duration (typical operation), or…**
3. **Following *authentication*, session keys may be trusted beyond session duration – reauthentication may follow specific events, or…**
4. **Following *authentication*, secure keys may be exchanged and used to encrypt session packets**

Does Broadband require an Intelligent Network or a Stupid Network?

- **“Fundamentally, it would be a Stupid Network. In the Stupid Network, the data would tell the network where it needs to go. (In contrast, in a circuit network, the network tells the data where to go.) In a Stupid Network, the data on it would be the boss.”**

RISE OF THE STUPID NETWORK, David S. Isenberg, while at AT&T Labs Research, Computer Telephony, August 1997, pg 16-26.

The “Scale AND Bill” Dilemma



IN Model - Point to Point

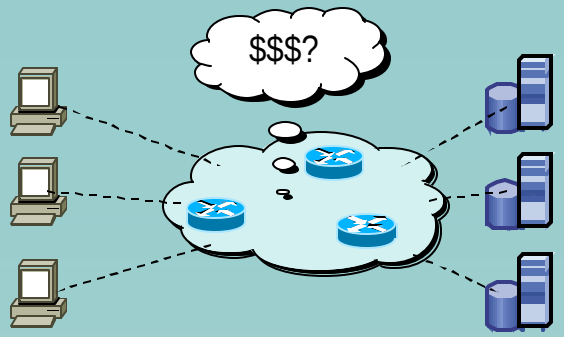
Point to Point Model
> *Centralized* Service Insertion and Control
> Circuit (TDM/VC/PPP) based data plane
> Limited Scaling (scale limted by BW/lines throughput *and* processing of central node

Per *Call* Control
> direct association between client and application service

Per call policy applied to the network
> per call billing etc.

SCALE

$$$$$$



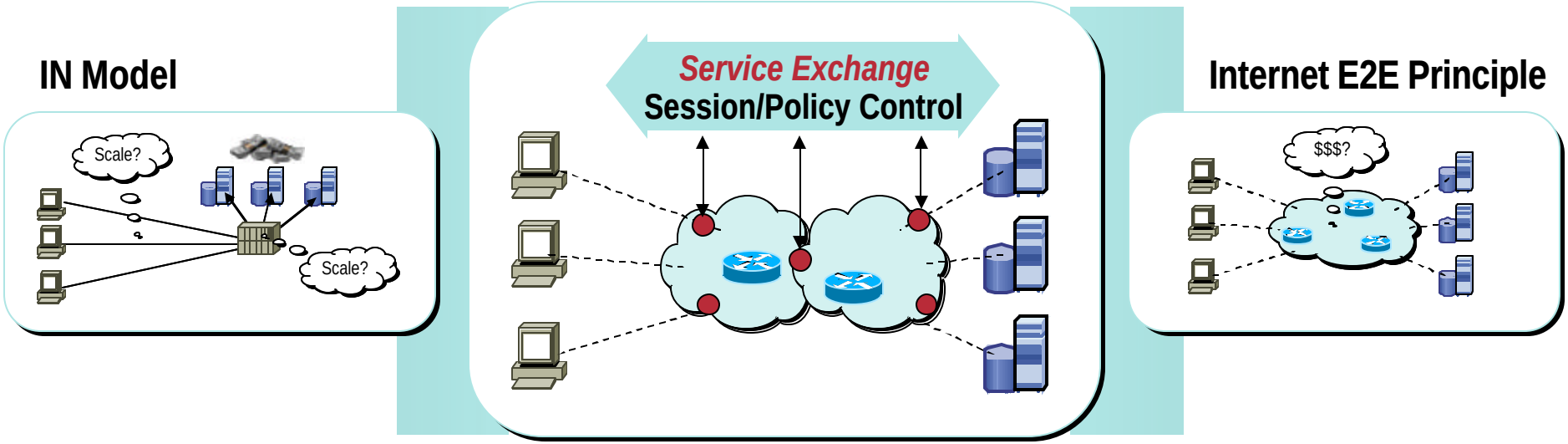
Internet E2E Principle - Point to Cloud

ob-by-Hop/Point to Cloud Model
> Distributed and VERY scalable
> Packet based data plane
> E2E Model leads to full decoupling of network and application control

E2E Principle: **Stateless packet core**
> Lack of application recognition in the network limits the ability to bill for the value of the network

Provisioned Policy only
> volume based billing

Solving the Scale and Bill Dilemma
Meeting in the middle



Scalable and Granular **Billing/Control:**
From Per Call to Per Session Control

Scaleable **Forwarding plane:**
From Circuits (TDM/PPP/...) to Packets

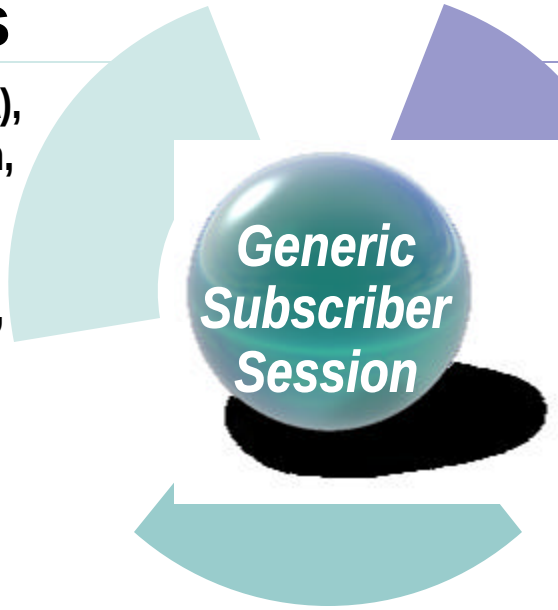
Putting it all together:
Introducing the Intelligent Service Architecture (ISA) in IOS

Access

PPP(PPPoE, PPPoA), Tunnel Termination, Interfaces, Ports, Mobile Wireless, Ethernet, WLAN, IP

Identity

Identification
Authentication
Authorization
Single Sign On



Services

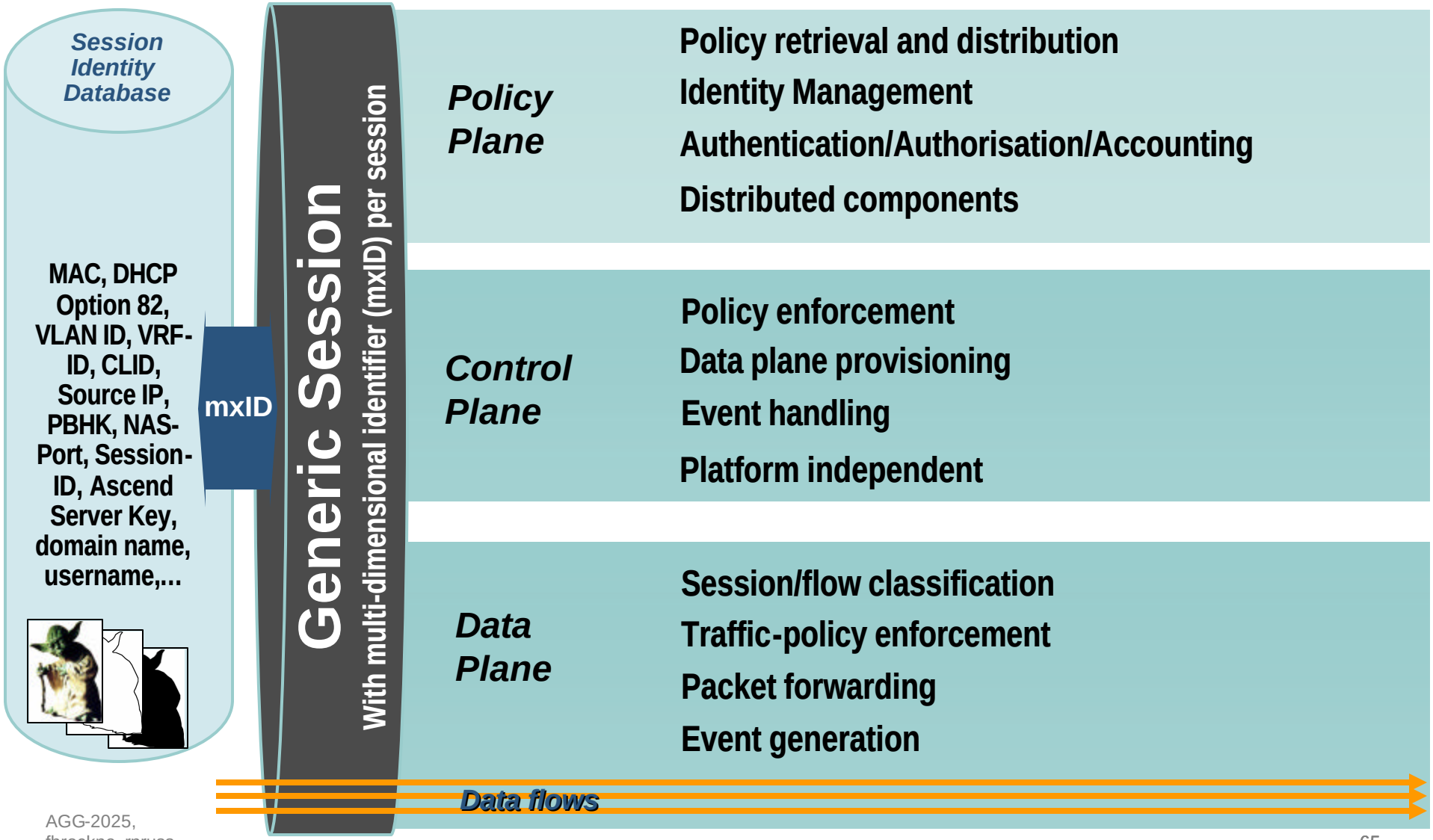
Per-Session Features: Forwarding/Routing, Accounting, Firewalls, QoS

Nomenclature

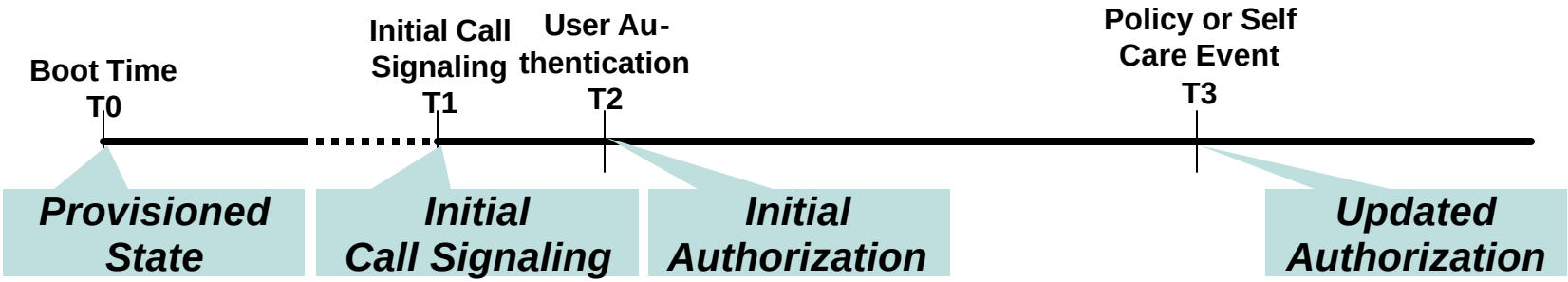
ISA
Intelligent Services Architecture:
Session-Service Architecture, part of IOS

ISG
Intelligent Services Gateway
Device which runs ISA-enabled IOS (e.g. 12.2(27)SBA)

Intelligent Service Architecture (ISA) in IOS (available from IOS 12.2(27)SBA on)



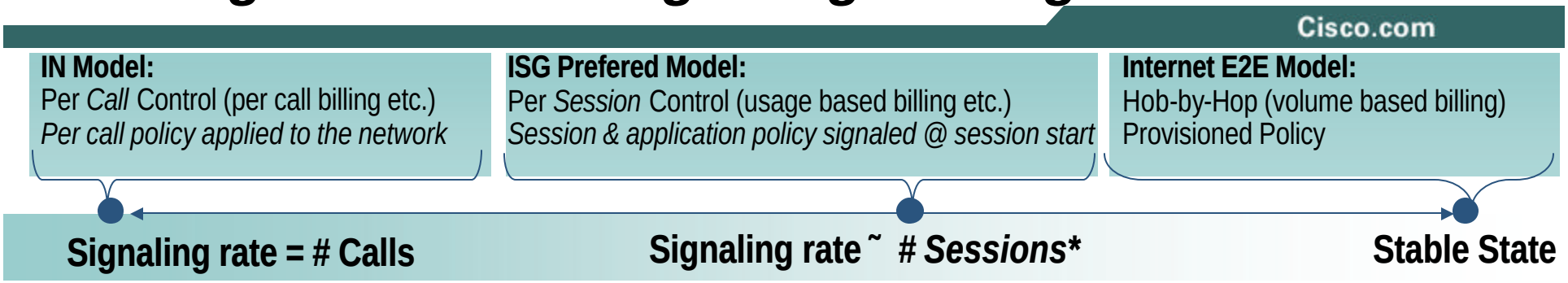
Session Types



Different *classification modes* for different subscriber traffic patterns: -

- ***PPP sessions*** **encompass all traffic received on a PPP connection**
- ***IP sessions*** **encompass all traffic received from a *single IP source address* or *subnet***
- ***Interface sessions*** **encompass all traffic received on a particular physical or virtual interface**
- ***MAC sessions*** **encompass all traffic received from a single MAC address**
- **More to be added…**

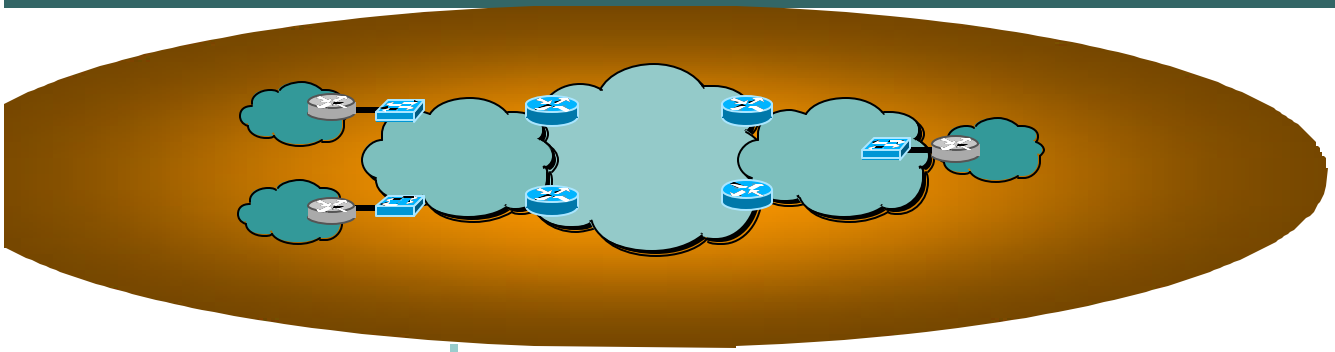
"Sessions" ? "Calls"
Solving the Per-Call Signaling Scaling Problem



- **Session: *"A set of policy associated with a L2/L3 classifier for a single billing entity"***
- **ISG associates a set of signaled policies with the sessions**
  - **ISG-Sessions usually last beyond a single "Call"**
    - **Following scalable design practice, session service policies are long lived and don't change per call**
    - **ISG Session don't assume per call signaling (different from what most "session border controllers" assume), but can support per-call signaling (IN Model)**
  - **Typical target (for Metro/DSL deployments): Session connection static state lifespan of months.**

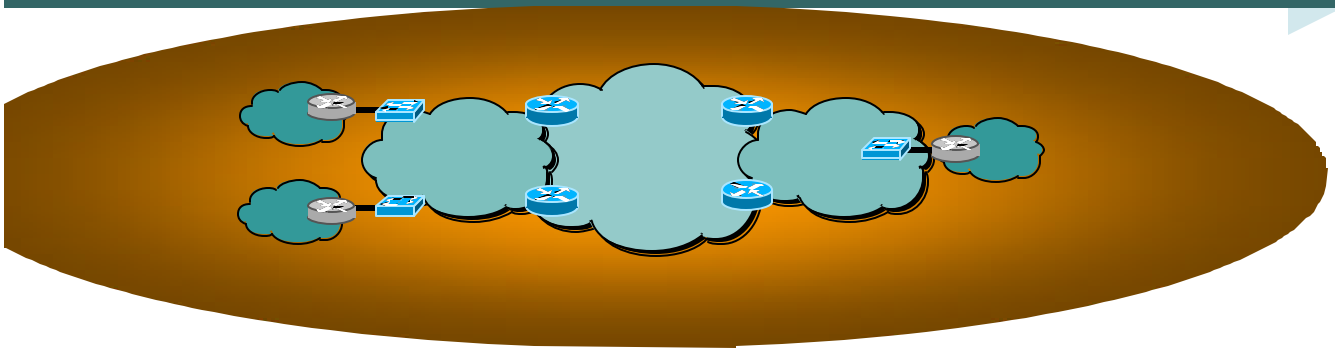
* Subscribers can change application subscription dynamically, thus signalling rate will usuall be 10-15% higher than the # sessions.

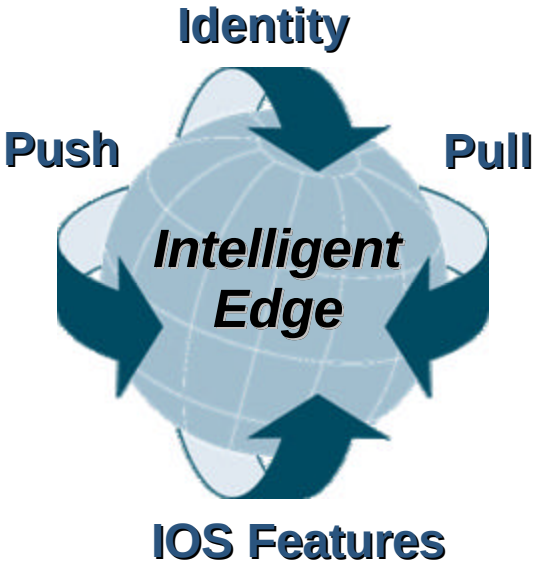
Agenda



- **Integrated Access/Aggregation Architecture**
  - **Towards an Integrated Access/Aggregation Architecture**
  - **Focusing the Key Challenges**
    - **Customer to VLAN mapping**
    - **MAC Scalability**
    - **Scalable Multicast Deployment**
    - **Security**
- **Service Control and Subscriber Management**
  - **Sessions, Identity, Policies**
  - **Case Studies**
  - **Configuration Brief**

ISA Case Studies





Case 1

DHCP event driven login with portal based subscription

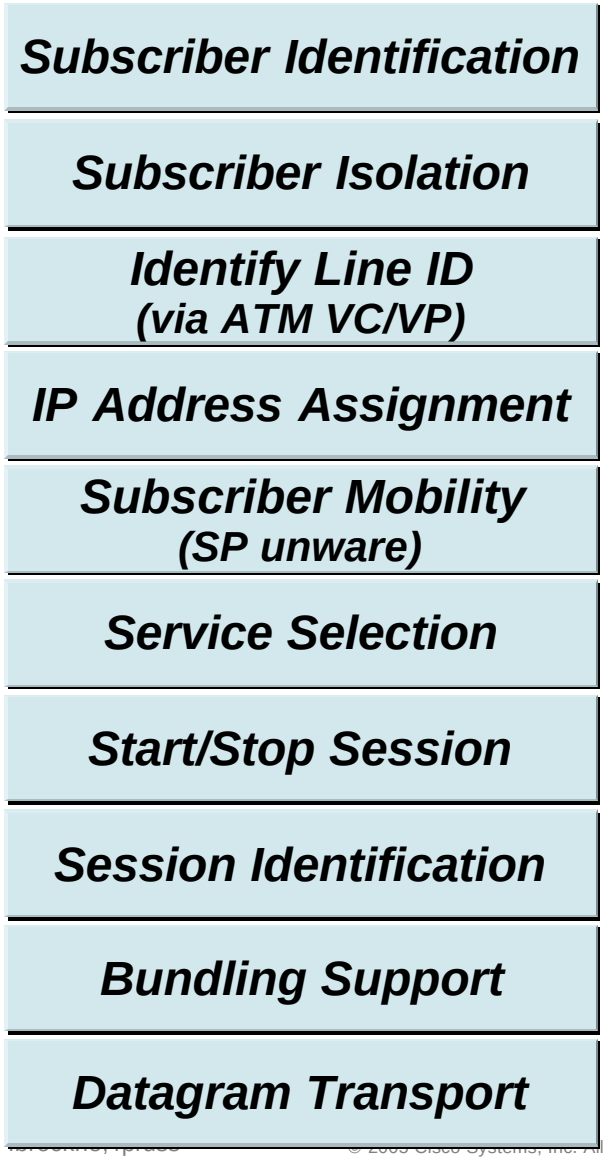
Case 2

Month Volume Cap Policy

Self Subscription

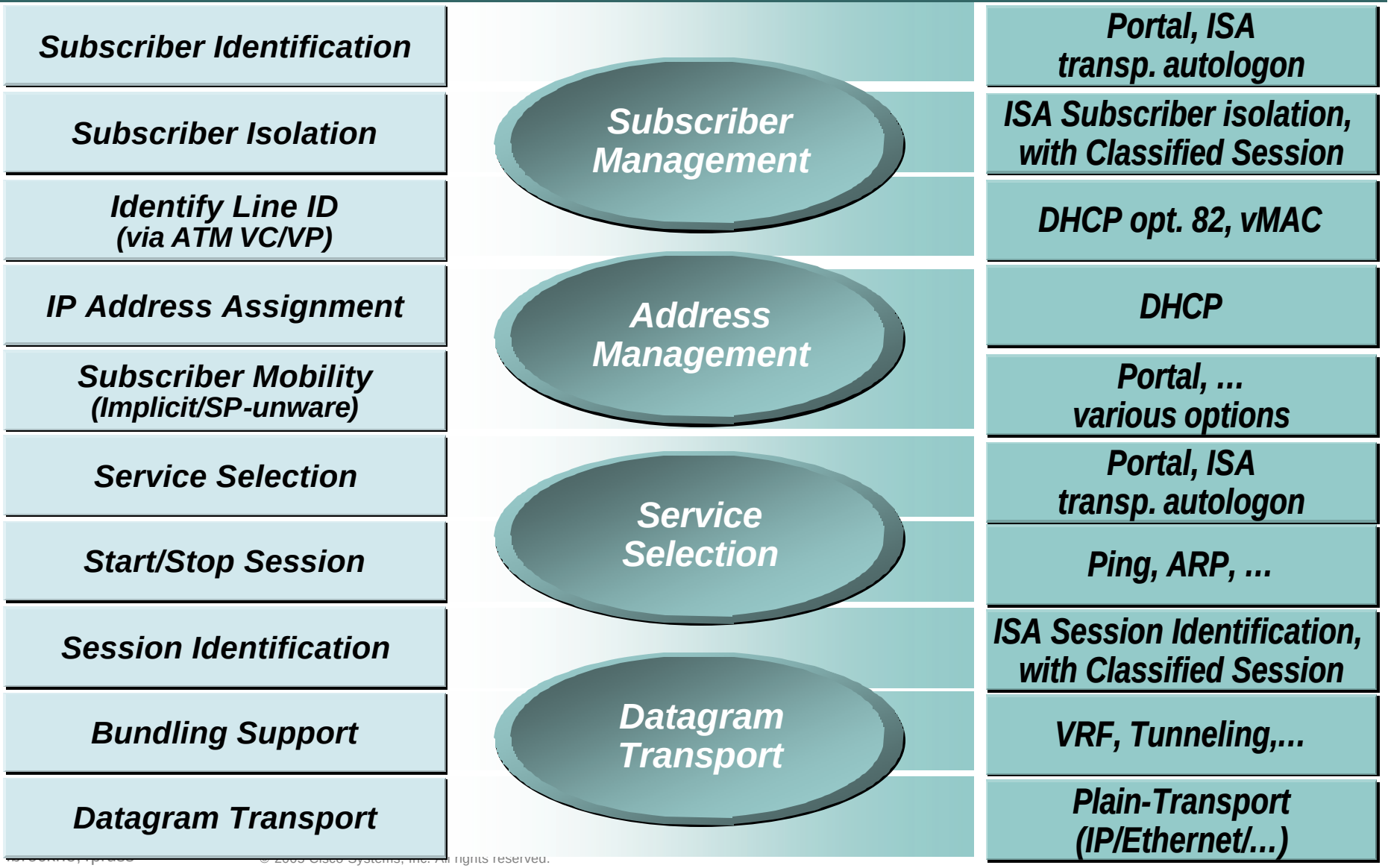
- **Consumer buys an off the shelf CPE, goes home, connects, self registers, gets customized service**
  - **Different CPEs might connect to different Service Providers**
- **Service provider provides pre-provisioned infrastructure and gives access to a differentiated service portfolio without call center based order process**
- **Evolve from current PPP approach**

Evolve PPP-Model (with ATM access)
Decompose & Introduce Layering



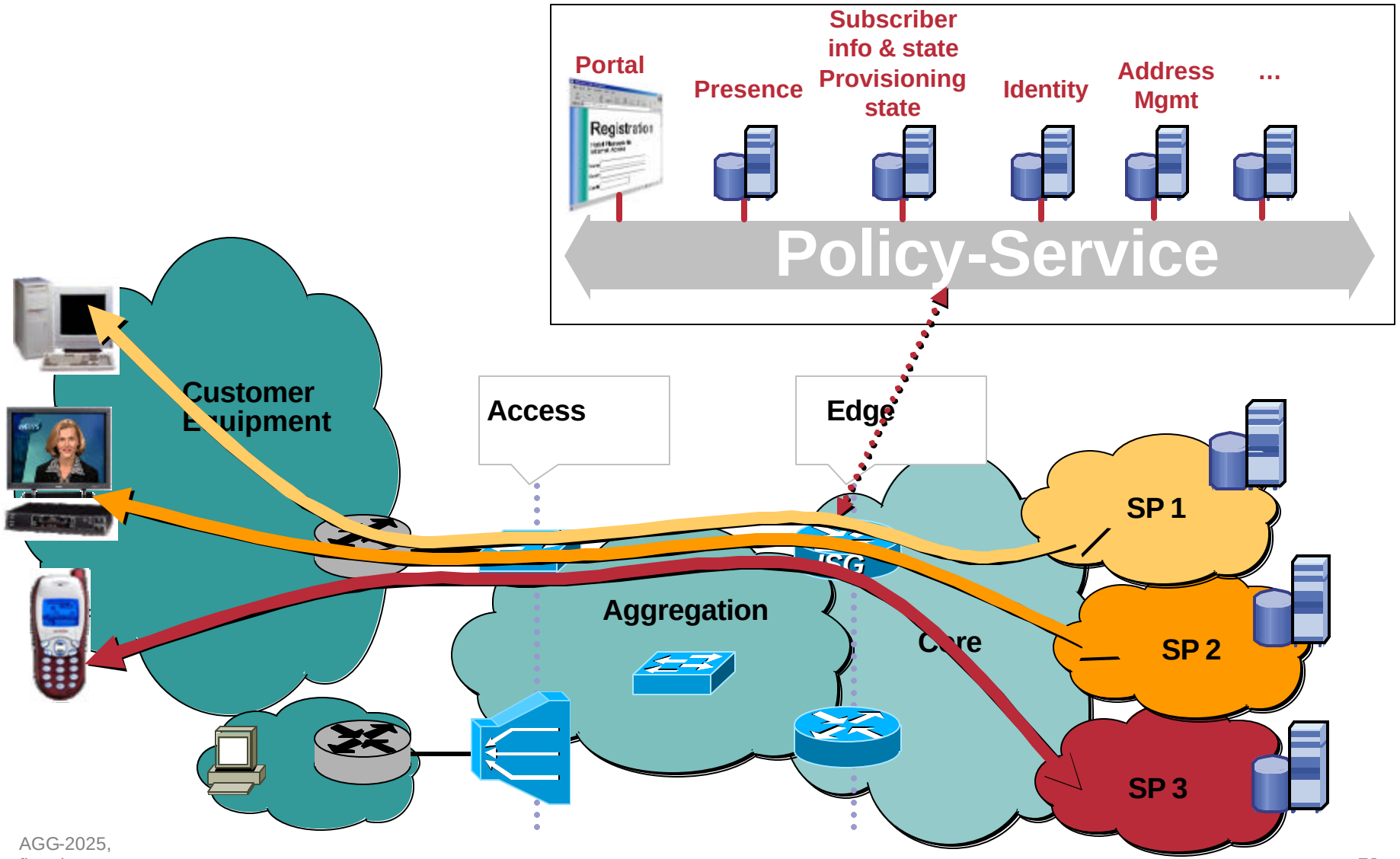
- **Current model tightly links different logical functions, different layers**
- **Evolution should decompose the linkage and increase flexibility**
- **Issues with current PPP approach**
  - **Client trouble-shooting**
    - Represents the majority of help-desk calls
    - Any network fault in the access layer causes calls
  - **Needs to be pre-provisioned in the network and then configured on either the subscribers CPE device or on the PC directly**
  - **For wholesale deployments, PPP termination at the ISP limits access provider's ability to enable IP services at the edge**
    - Network access commoditized

Evolve PPP-Model (with ATM access) – *Don't only mimic - Decompose & Introduce Layering*

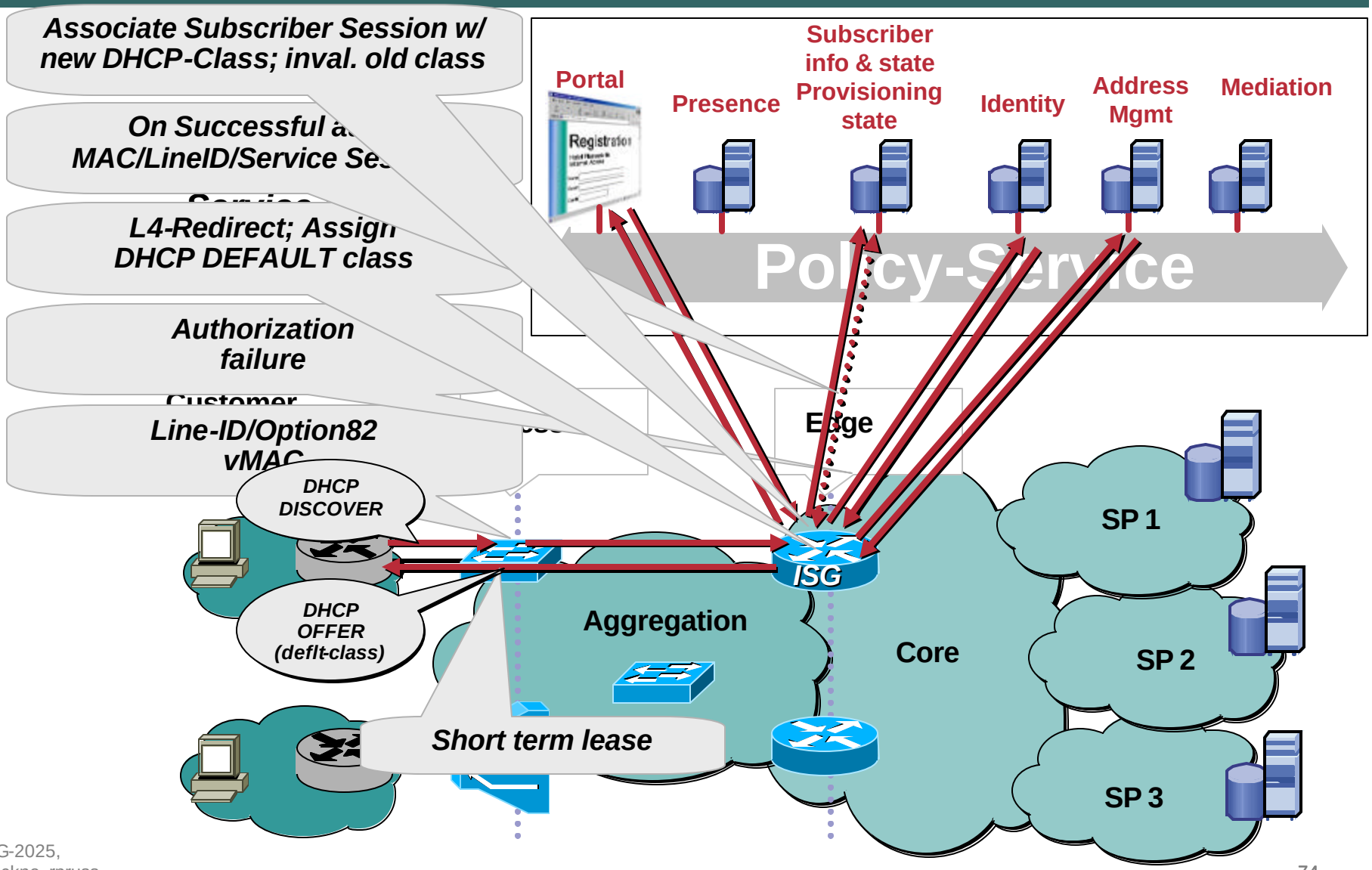


Subscriber Management

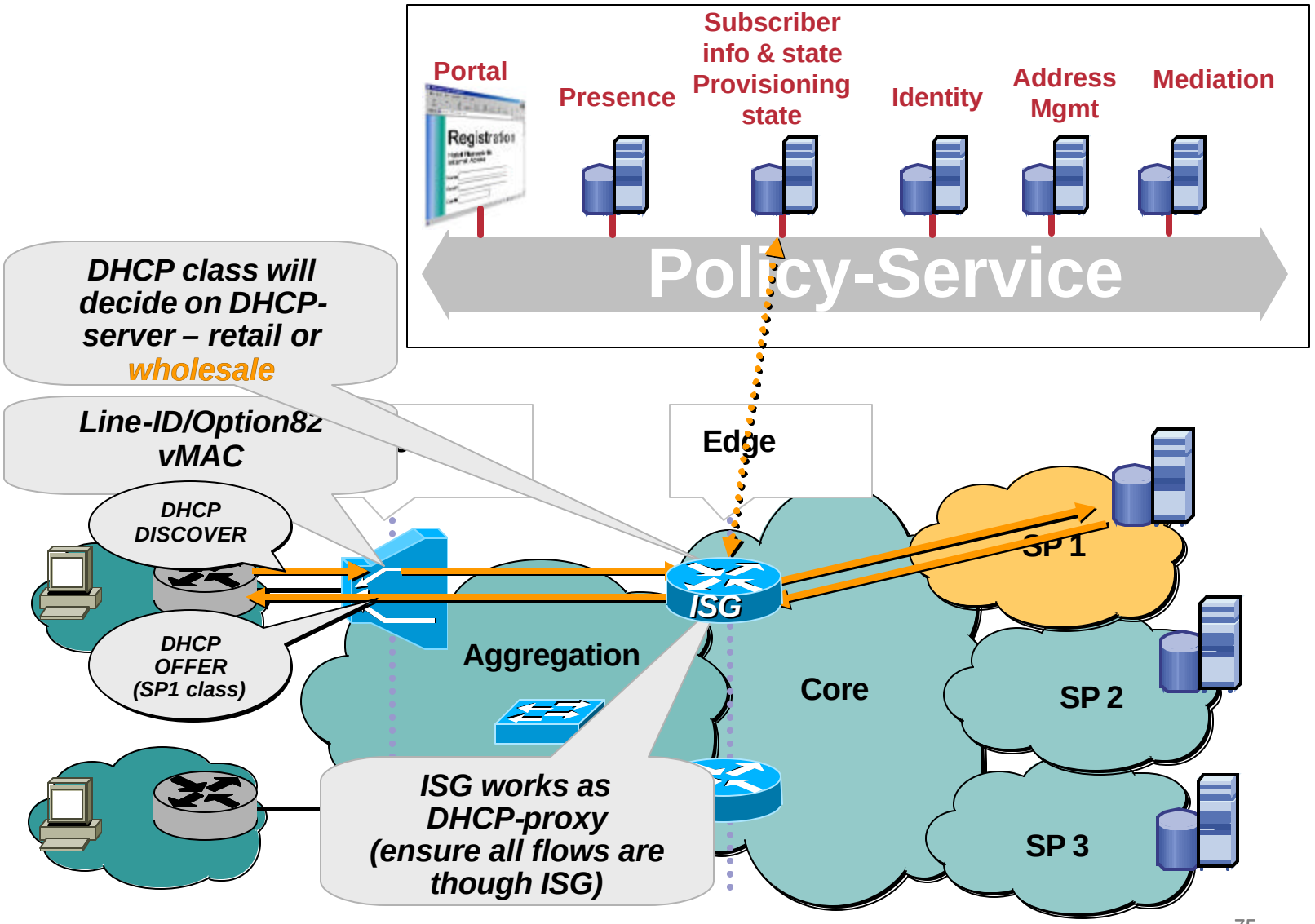
Concurrent Access to multiple (Application-)Providers
Combine Wholesale and Retail



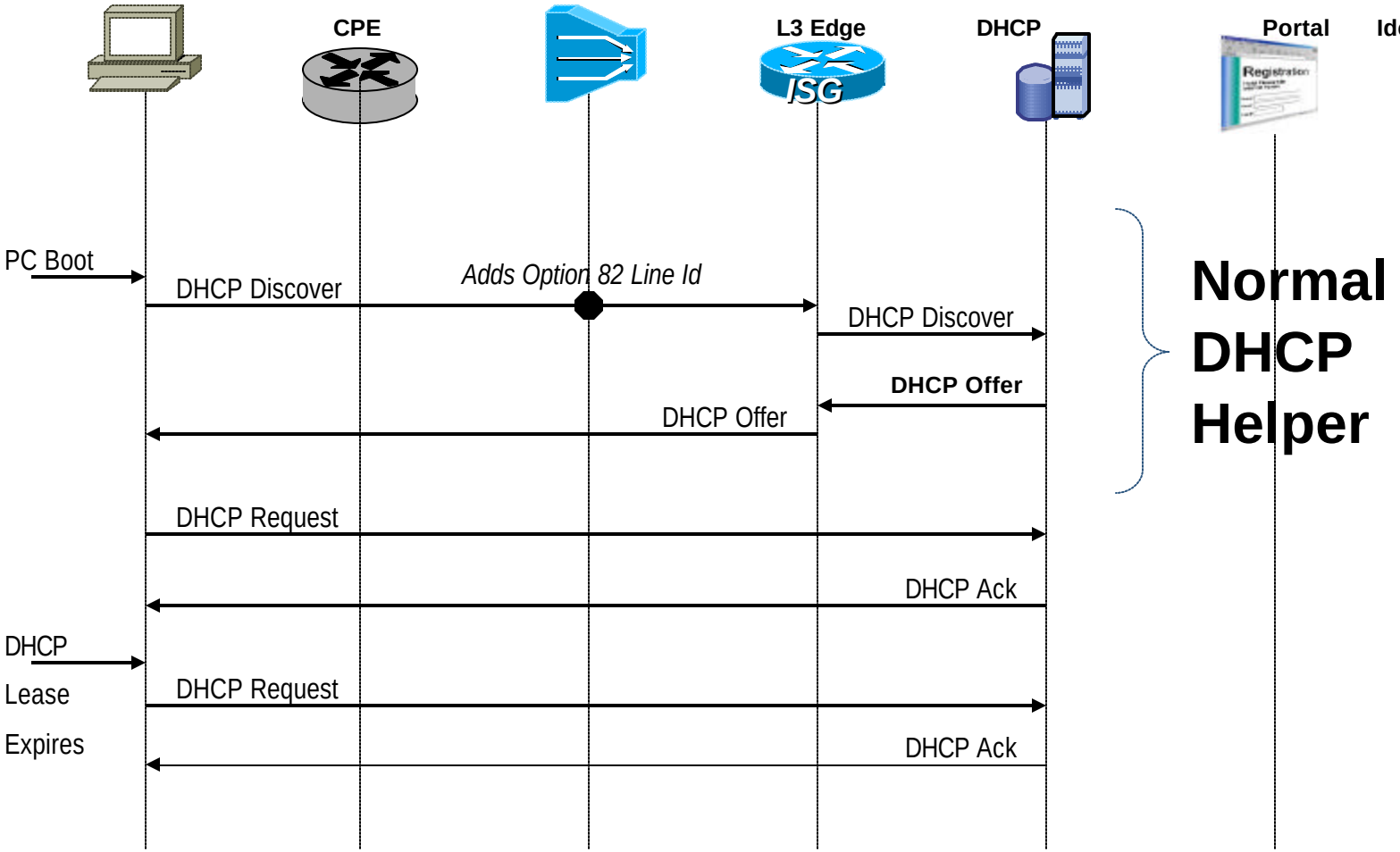
New subscription



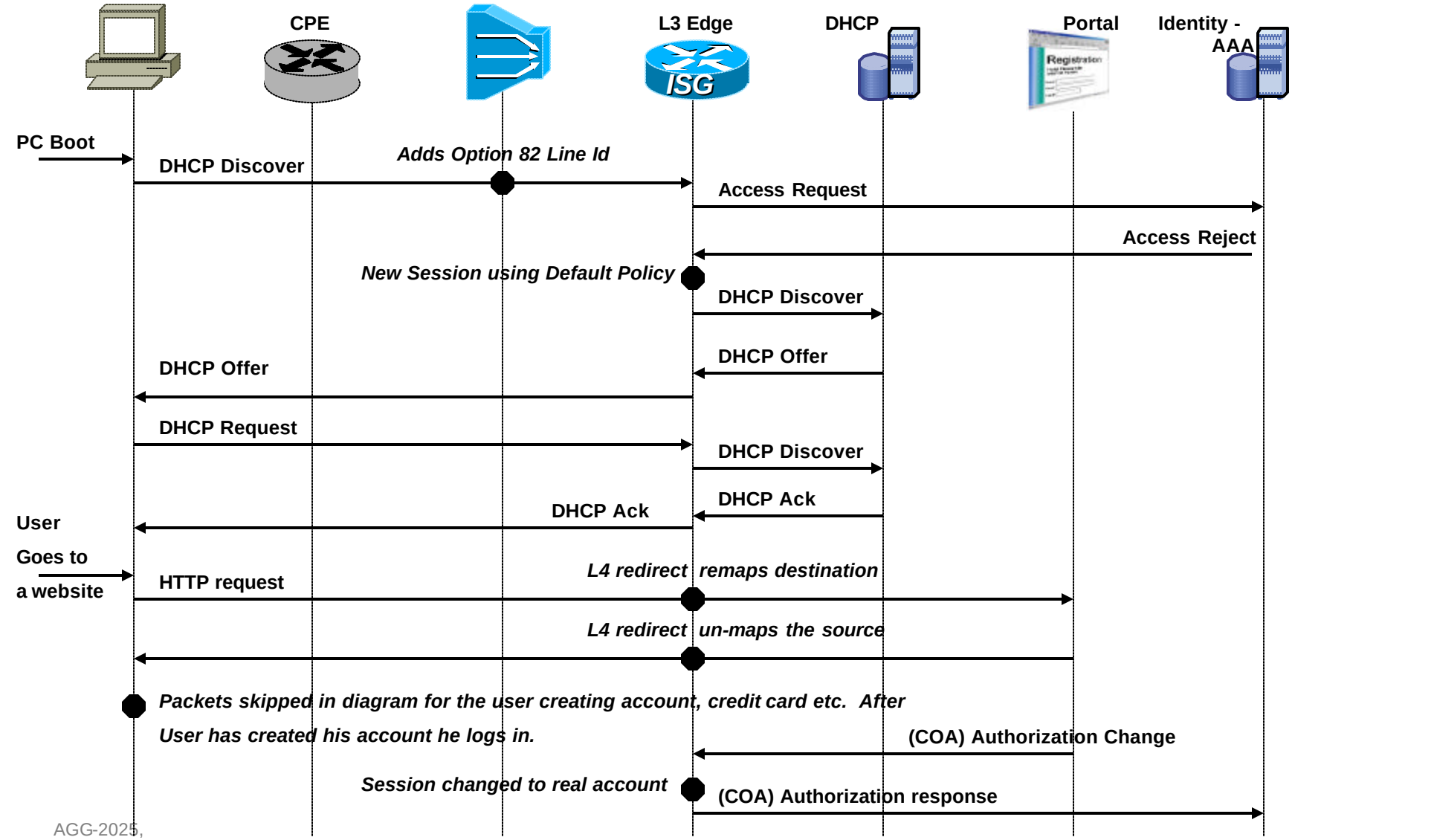
Post subscription operation



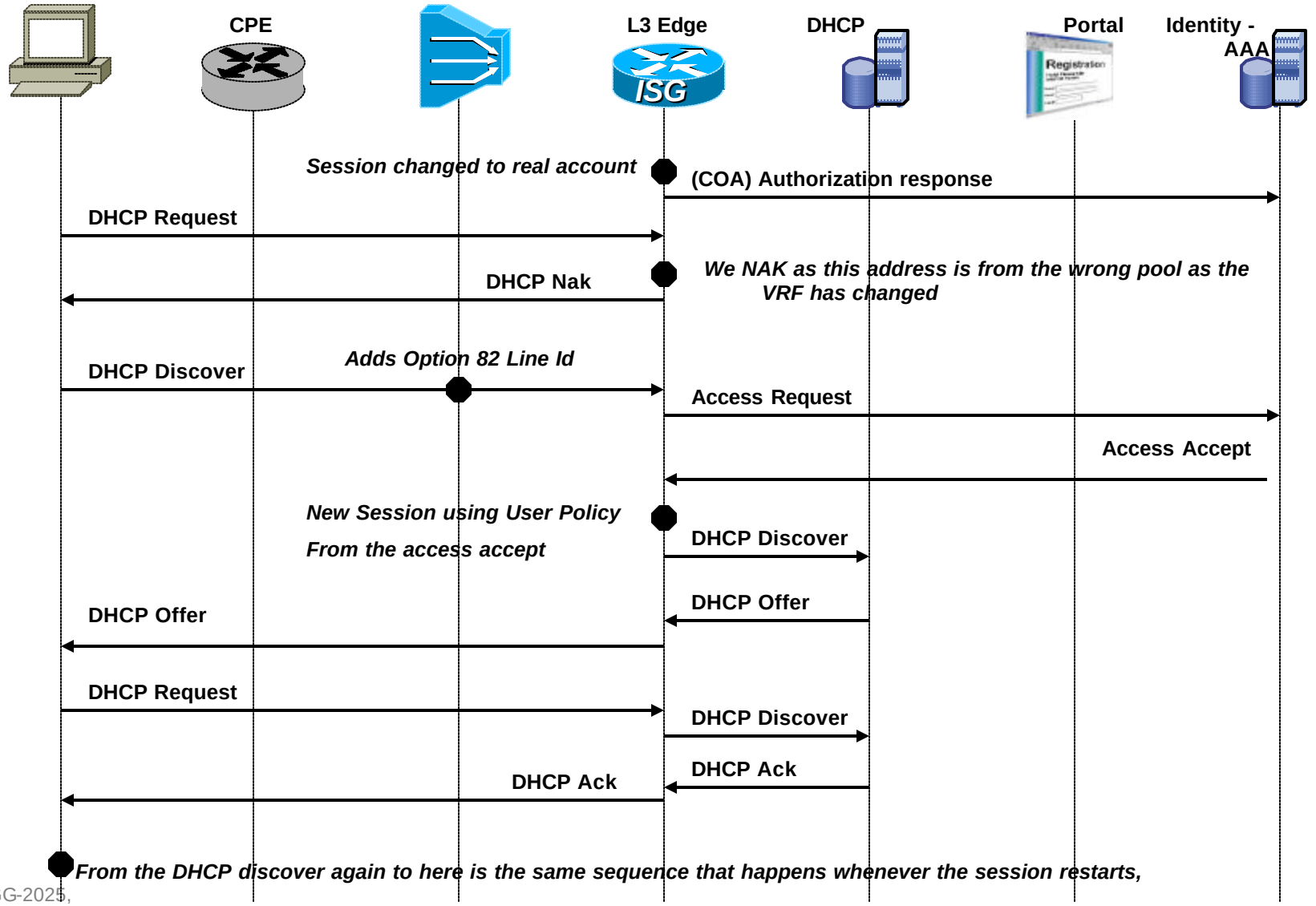
IP Sessions – Leveraging DHCP
Quick refresher on DHCP Helper



IP Sessions – Leveraging DHCP
DHCP Relay Flow diagram (1/2)



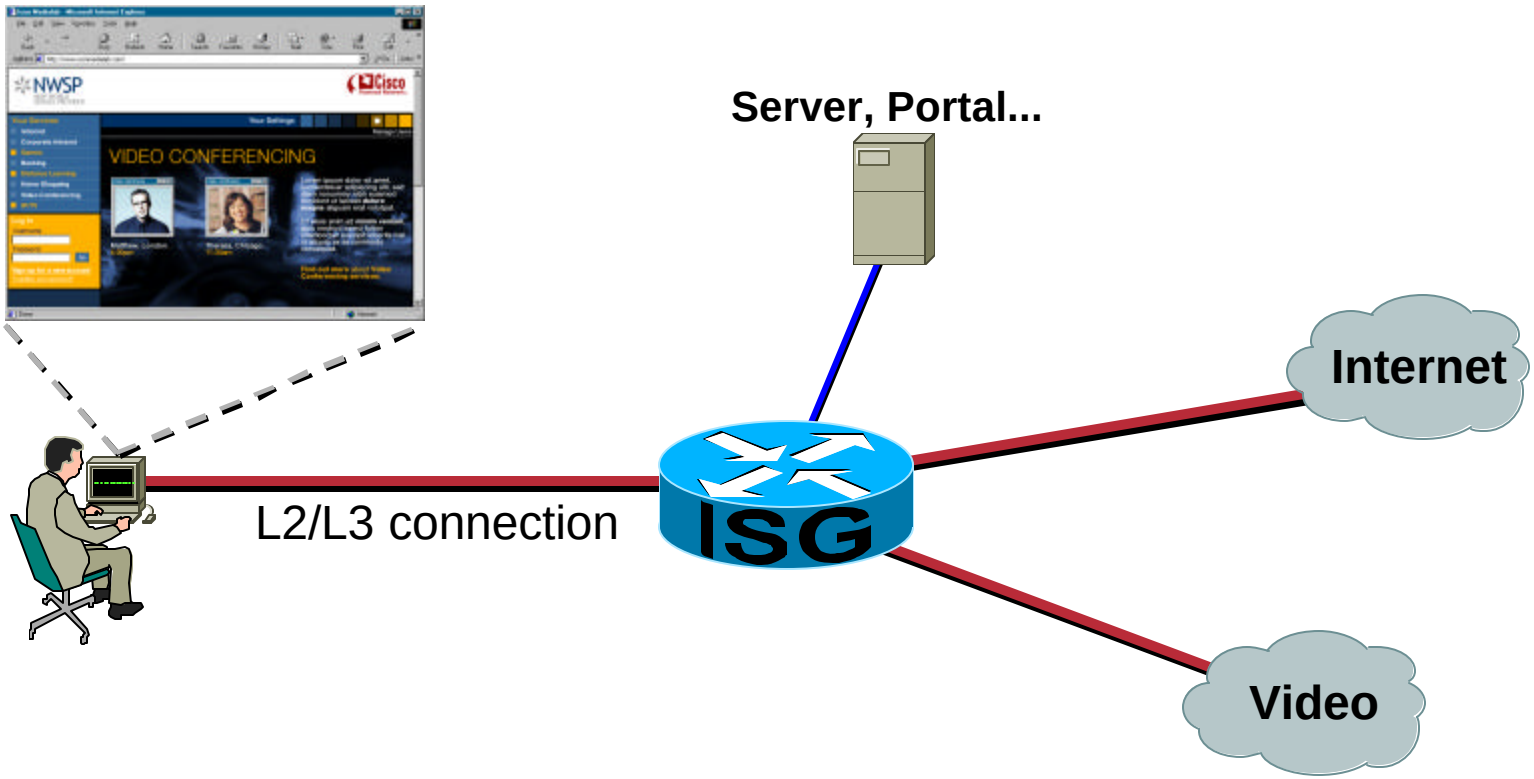
IP Sessions – Leveraging DHCP
DHCP Relay Flow diagram (2/2)



How to redirect subscribers' TCP/UDP traffic to a server (for control & enhanced user experience)?

Cisco.com

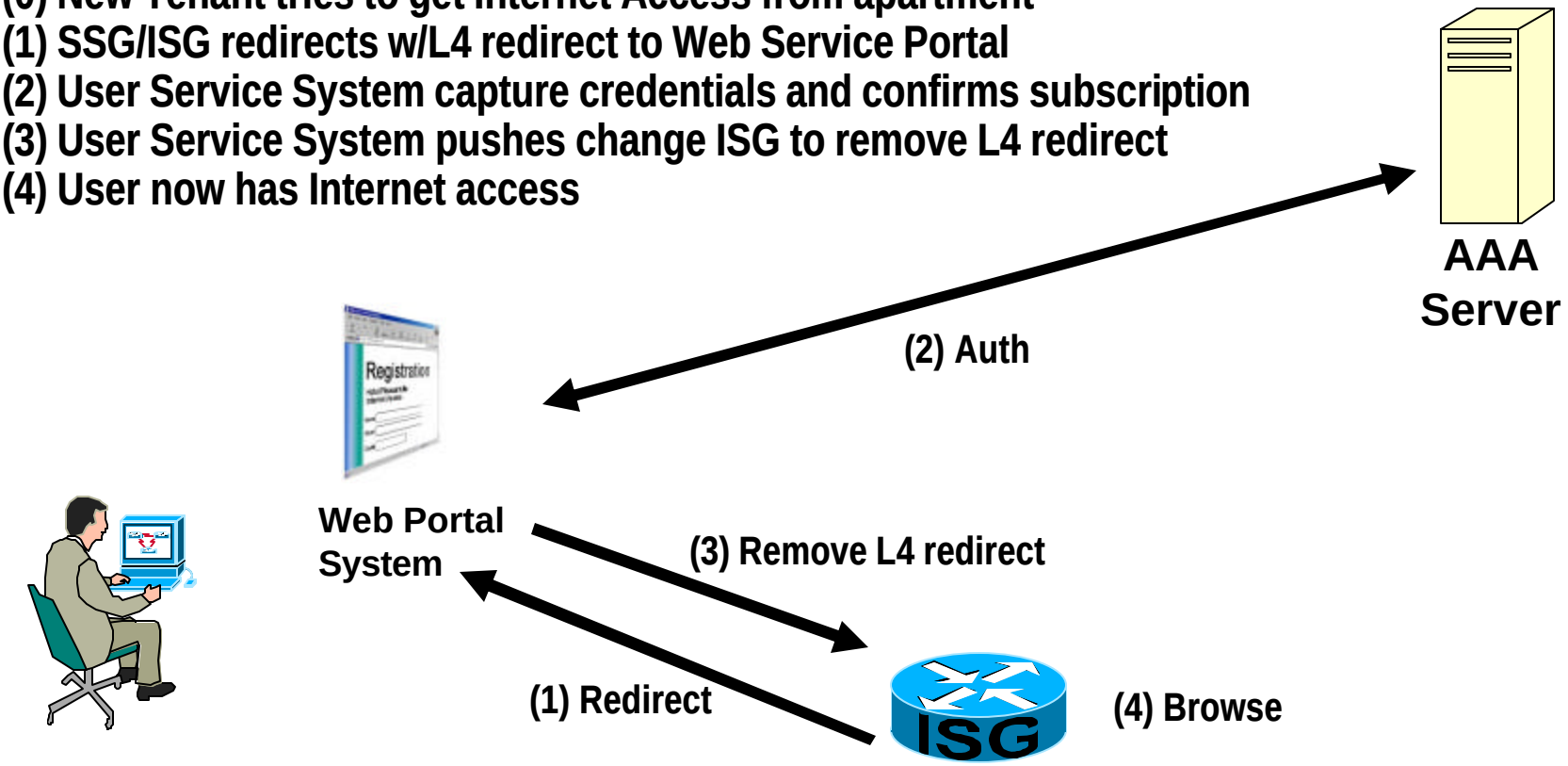
ISA L4-Redirect



How to authenticate a formerly unknown User?

ISA Captive Portal

(0) New Tenant tries to get Internet Access from apartment
(1) SSG/ISG redirects w/L4 redirect to Web Service Portal
(2) User Service System capture credentials and confirms subscription
(3) User Service System pushes change ISG to remove L4 redirect
(4) User now has Internet access

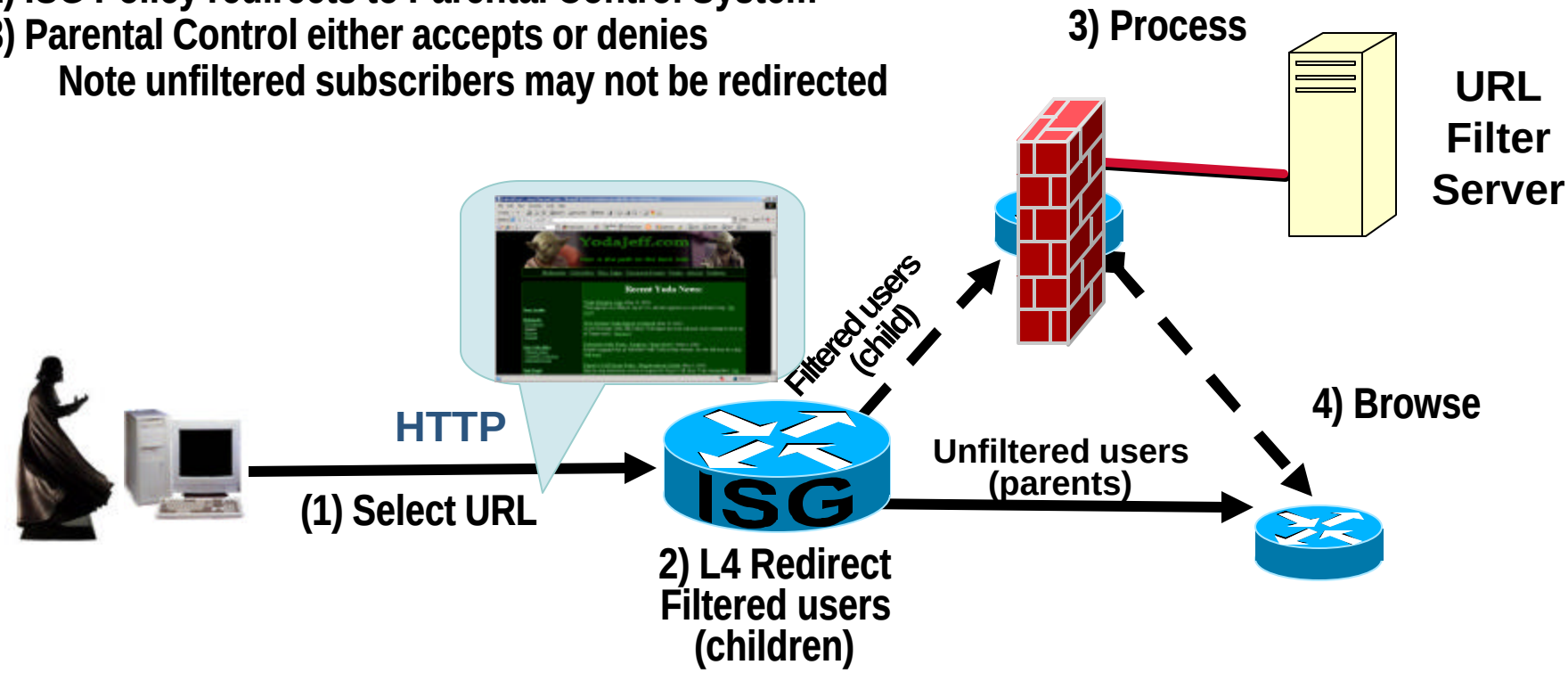


How to restrict certain users from accessing certain services?

Cisco.com

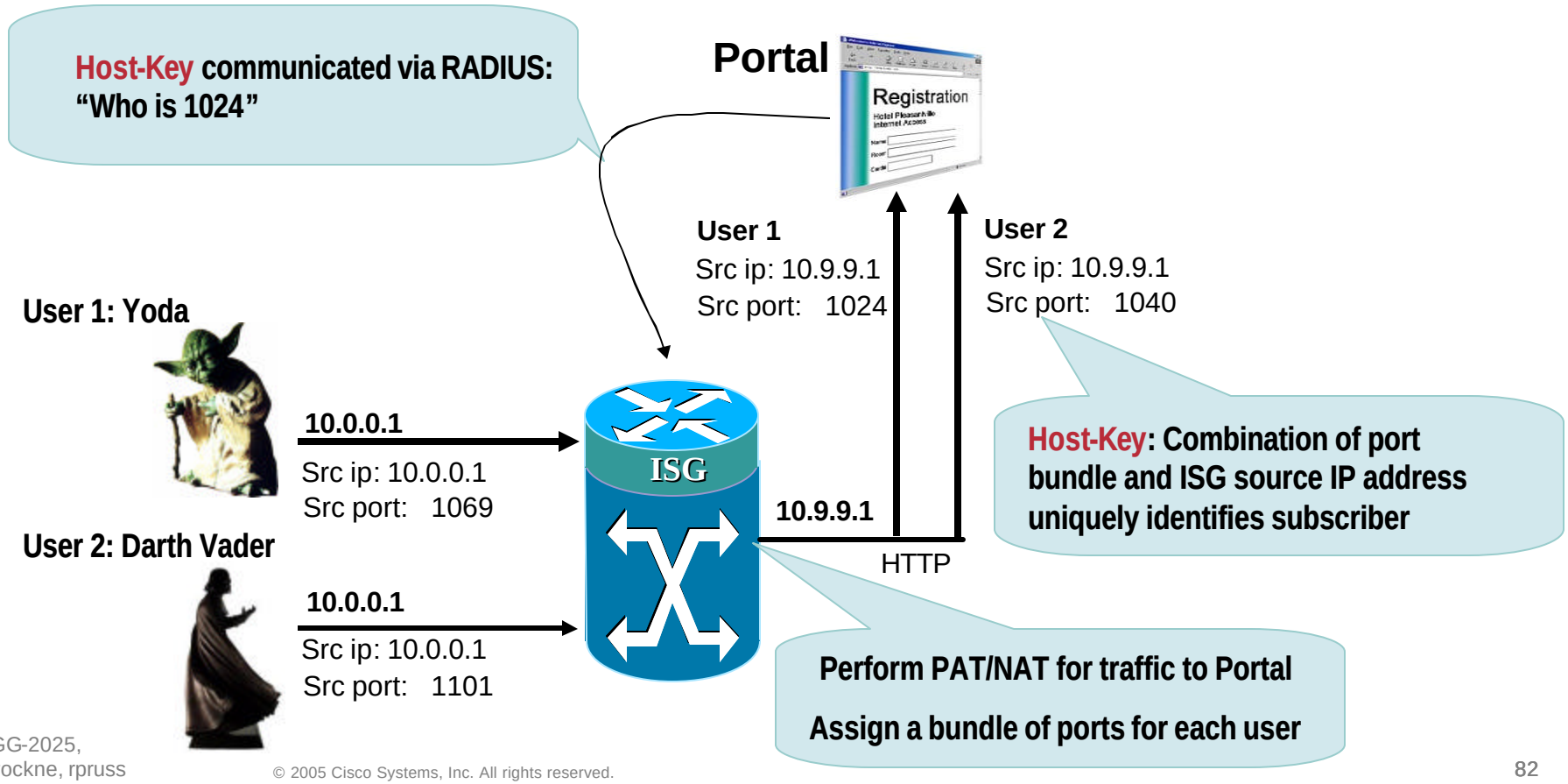
ISA Parental Control (Conditional L4 redirect)

(1) Child Tries to Access URL
(2) ISG Policy redirects to Parental Control System
(3) Parental Control either accepts or denies
Note unfiltered subscribers may not be redirected



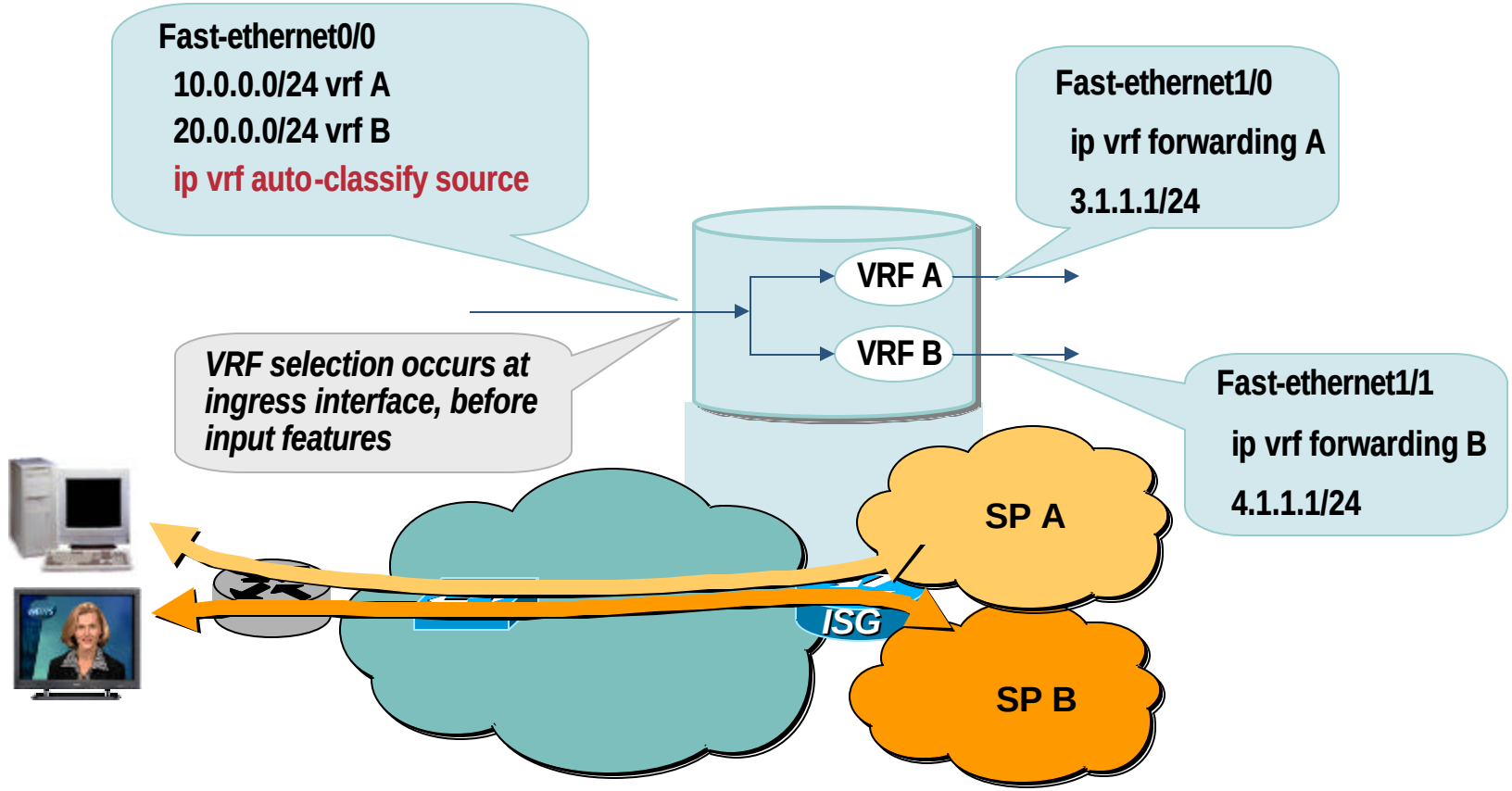
How to support overlapping Host-IP Addresses?

ISA Single Sign on for Port Bundle Host Key



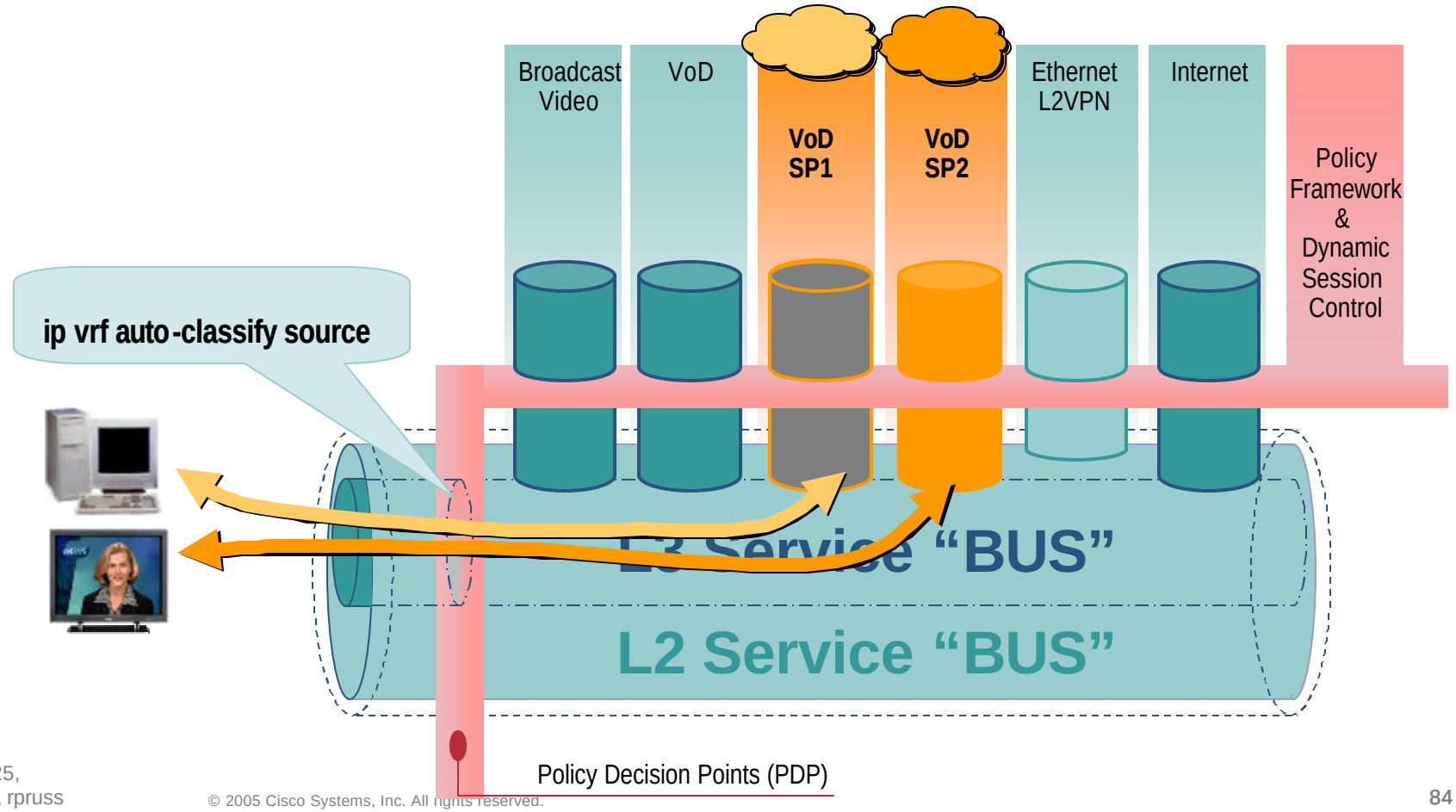
Once the appropriate Source-IP is assigned, how to transfer the subscriber into the appropriate VRF?

ISA VRF transfer, Autoclassify Source



Automatically Selecting Services based on assigned IP-Address - Example

ISA Autoclassify Source



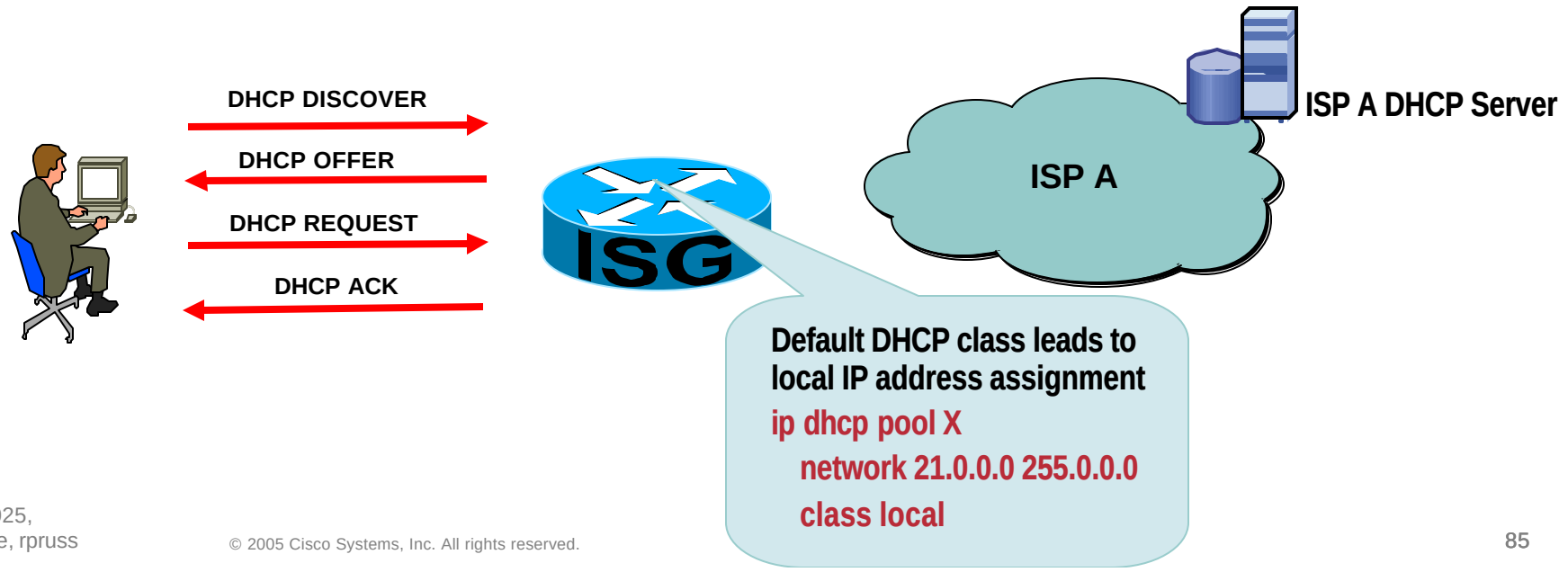
Address-Assignment: How to facilitate flexible selection of the DHCP server based on service domain?

Cisco.com

ISA DHCP Proxy with Policy

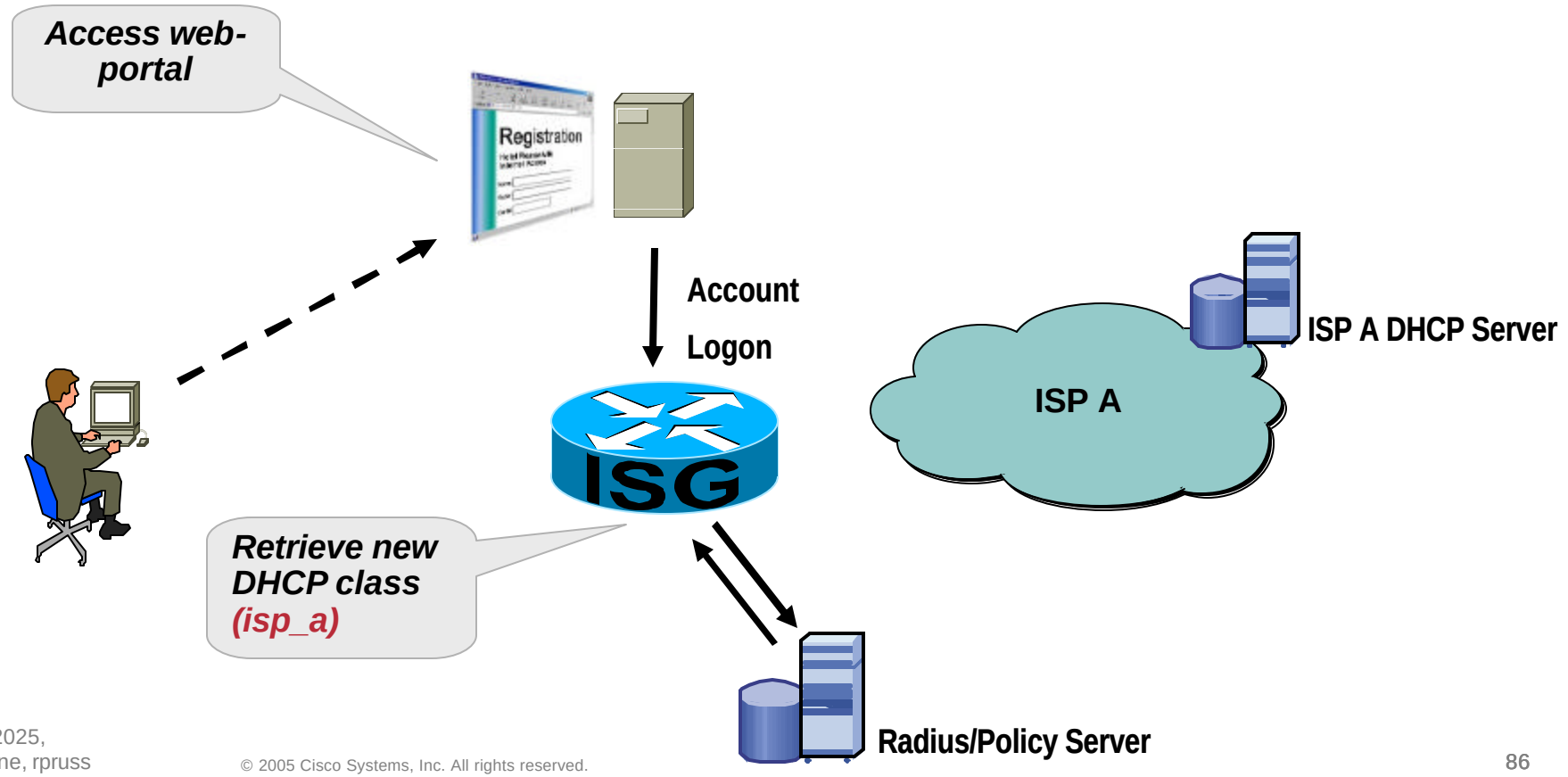
- Influence the IP address pool and the DHCP server that are used to assign subscriber IP addresses
- Associate a DHCP address pool class with an address domain

> Extended DHCP relay function (DHCP proxy – ISG needs to be in the return path!)



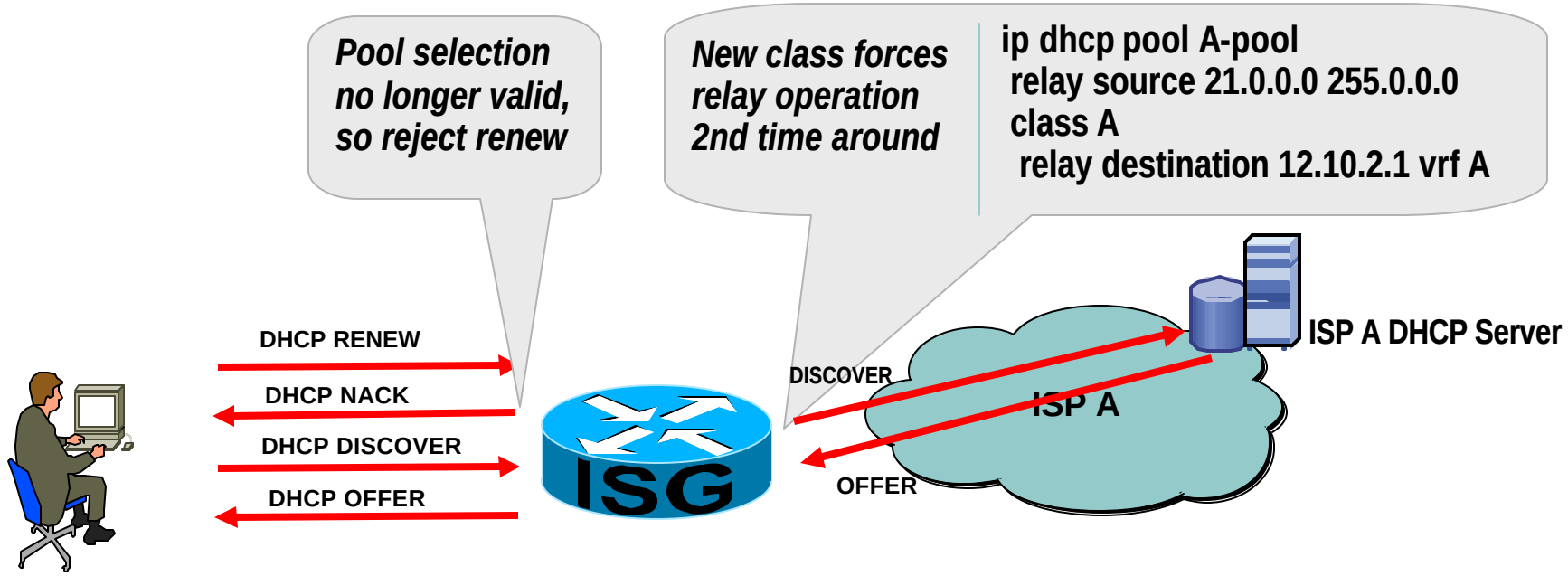
Address-Assignment: How to facilitate flexible selection of the DHCP server based on service domain?

ISA DHCP Proxy with Policy (contd.)



Address-Assignment: How to facilitate flexible selection of the DHCP server based on service domain?

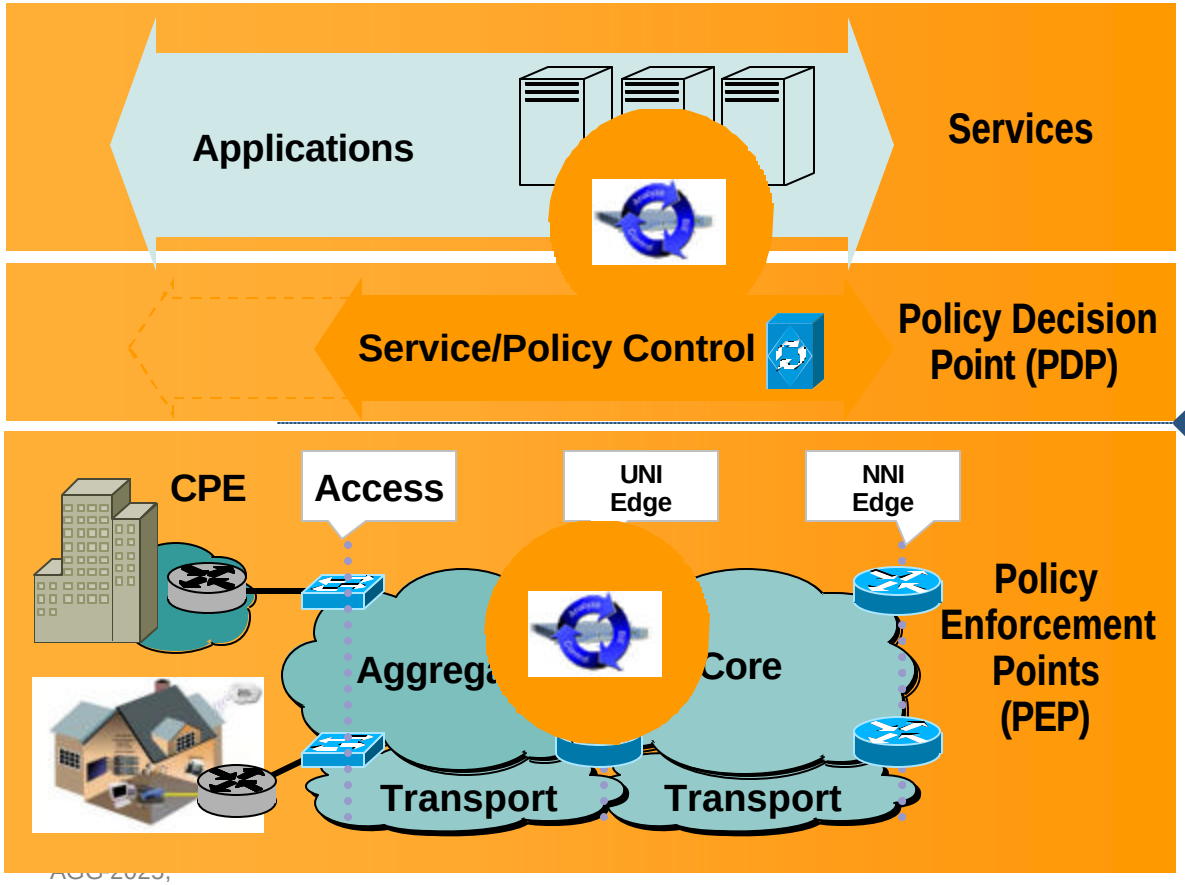
ISA DHCP Proxy with Policy (contd.)



How to Change Sessions Dynamically? (Update Policies etc.)

Cisco.com

ISG Dynamic Interface for Session Control
RADIUS CoA, …

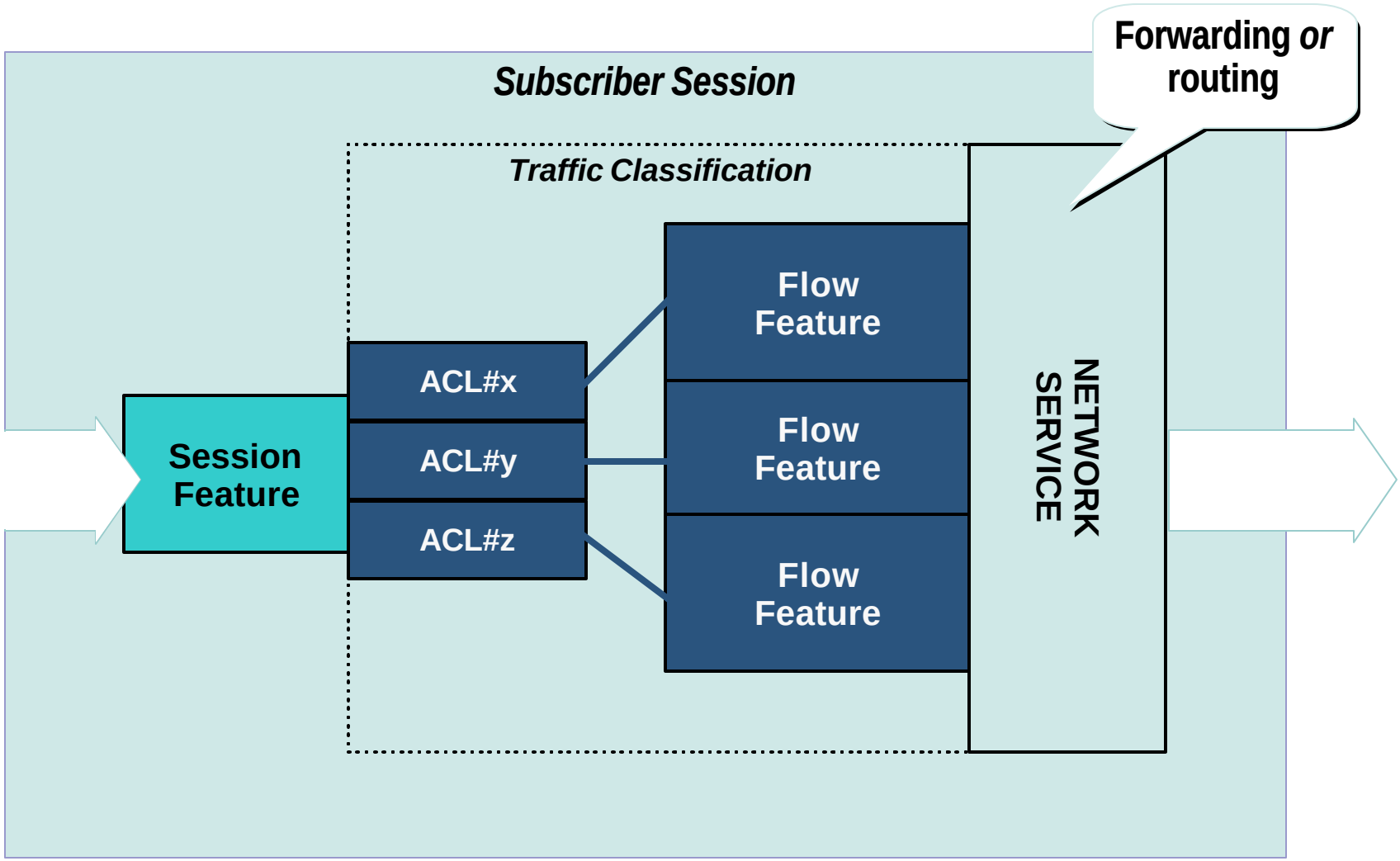


Dynamic Session Interface
- Session logon/logoff
- View Service List
- Service logon/logoff
- View Session status
- View System messages
- Feature Change

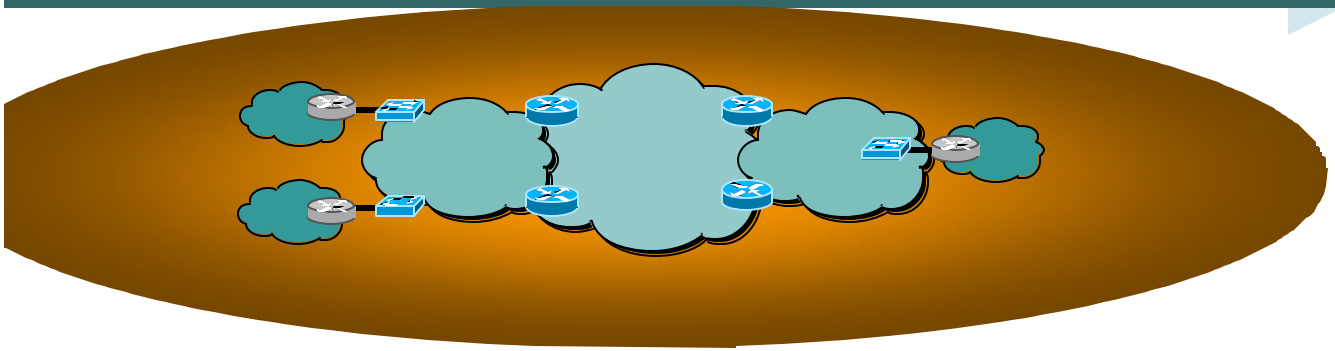
ISG features controllable by RADIUS

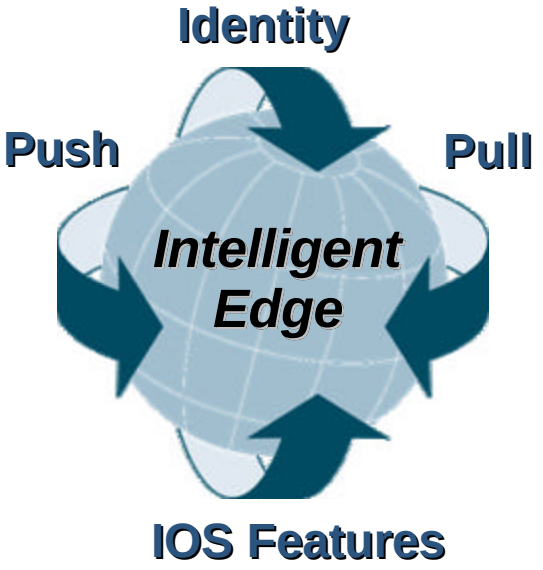
Service polices including traffic policies, L4 redirect, Subscriber ACL, Idle Timer, Session Timer, QoS, Session/Service Accounting, Pre-paid

ISA Subscriber Data Plane



ISA Case Studies





Case 1

DHCP event driven login with portal based subscription

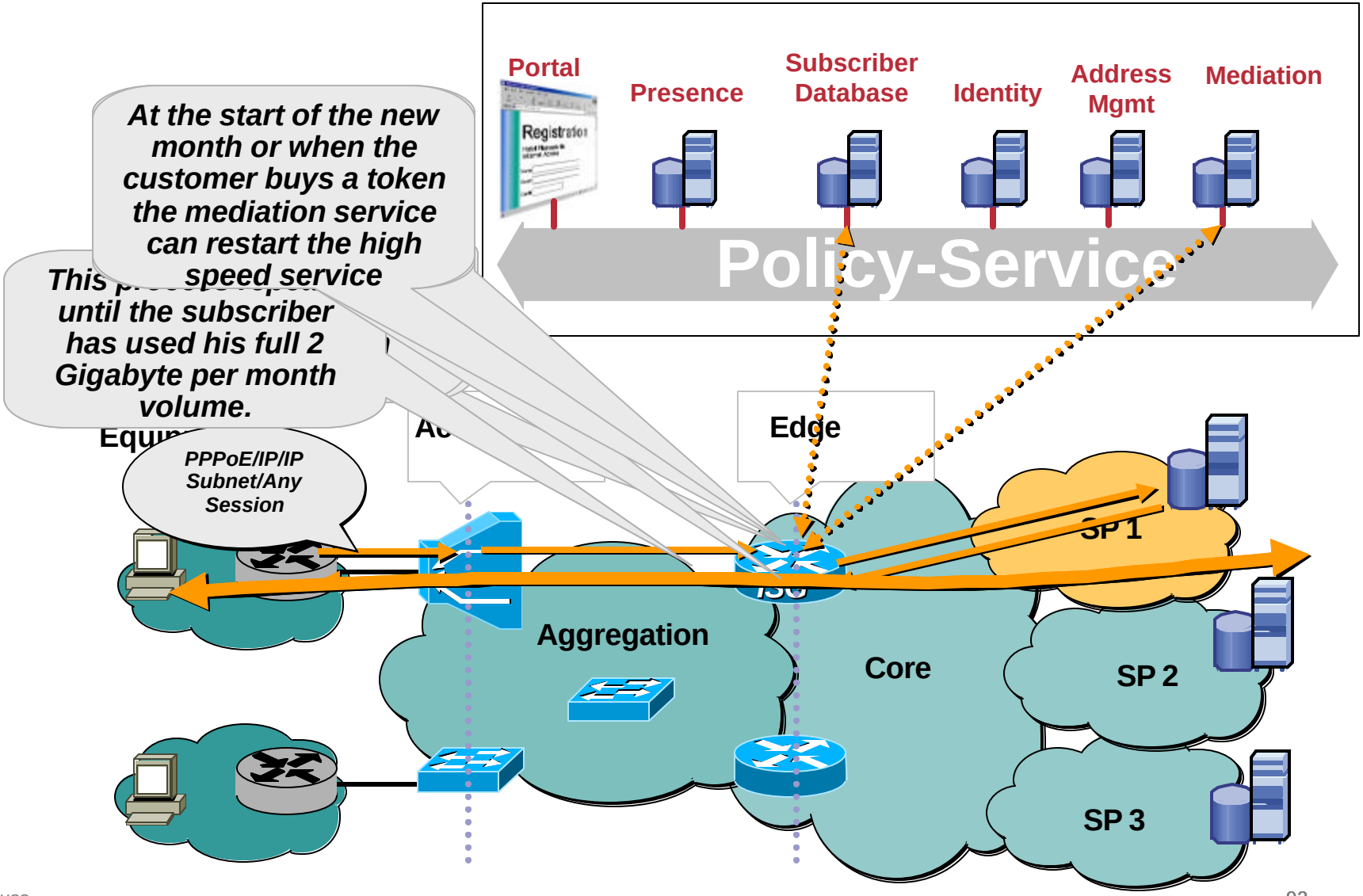
Case 2

Month Volume Cap Policy

You get what you paid for…

- Most consumers do a little web surfing and email. They want a high speed offering.
- Problem is the small percentage that run repositories, file sharing, etc
- Service provider sells a service that runs at 3 meg downstream & 128Kbit up for 2 Gigabytes of traffic per month and dynamic changes per subscriber to 128 kbit bidirectional after 2 Gigabytes .
- Now the Service Provider can provide an additional revenue service of either unlimited traffic volume for the rest of the month or additional volume in increments

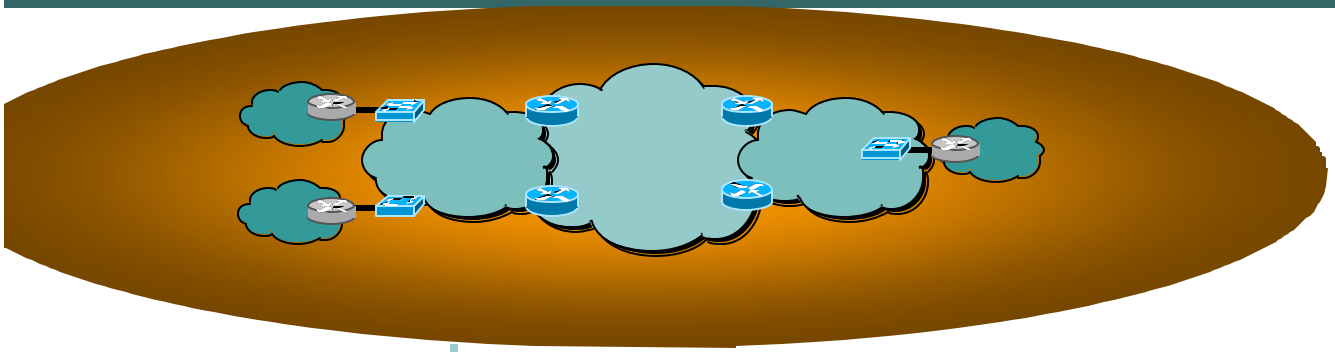
Behaviour changing on Volume



Prepaid Concepts not in example

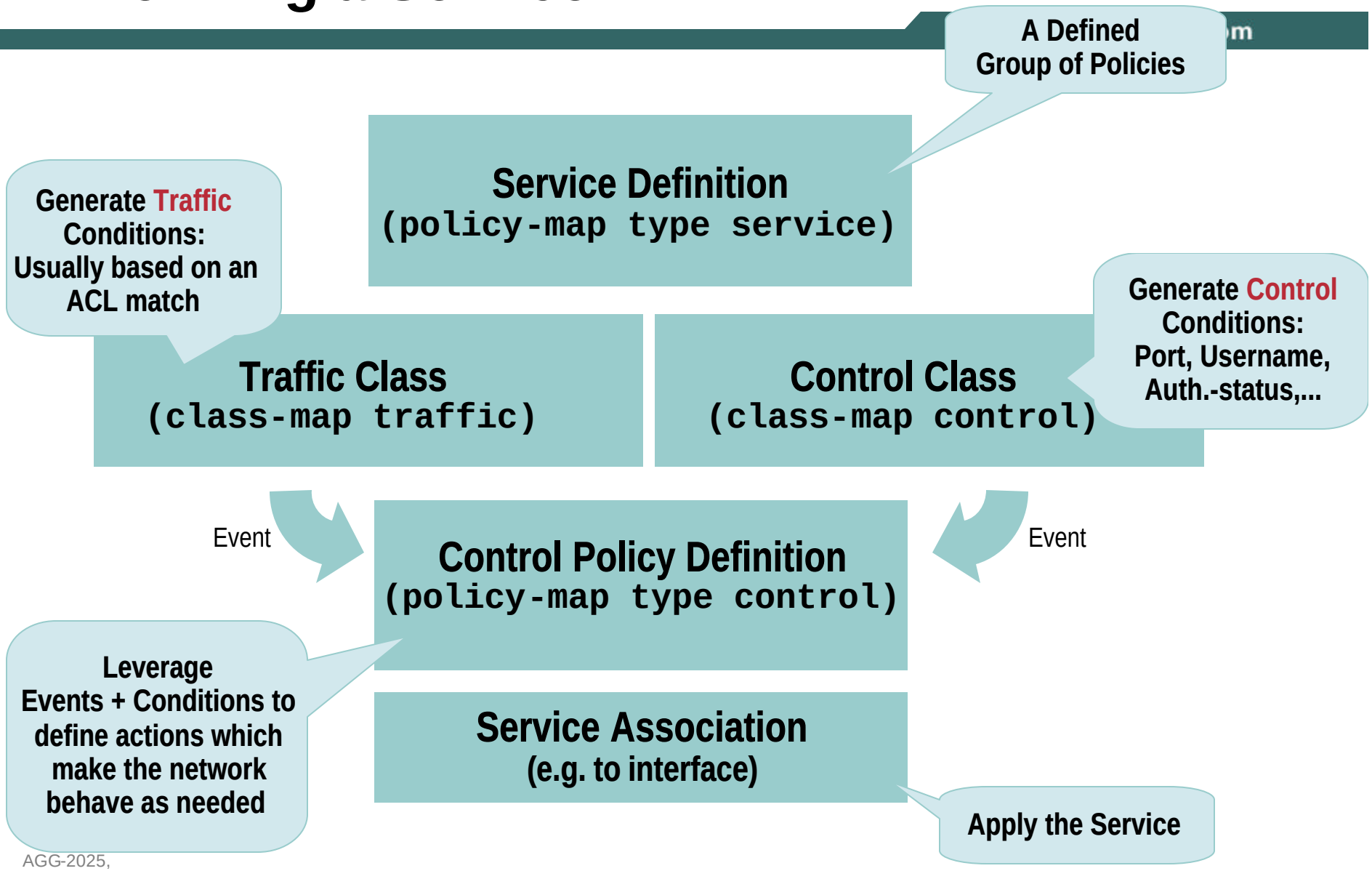
- **Quota allocated in one of two types**
  - **Duration**
  - **Volume**
- **Quota depletion and events just before quota depletion**

Agenda



- **Integrated Access/Aggregation Architecture**
  - **Towards an Integrated Access/Aggregation Architecture**
  - **Focusing the Key Challenges**
    - **Customer to VLAN mapping**
    - **MAC Scalability**
    - **Scalable Multicast Deployment**
    - **Security**
- **Service Control and Subscriber Management**
  - **Sessions, Identity, Policies**
  - **Case Studies**
  - **Configuration Brief**

Defining a Service



Service Definition
`policy-map type service`

- **Groups of Policy Activated Collectively on a Session**
- **Local (CLI – using C3PL) or Remote (RADIUS) Definition**
- **Example:**

```
class-map traffic CLASS_103
    match acl 103
```

Traffic Class Defintion

Matching Criteria for this class to create and event

```
Policy-map type service L4_REDIRECT_SERVICE
  class traffic CLASS_103
        redirect to group SESM
```

Feature (also called Traffic-Action) – here: L4-redirect triggered by traffic class CLASS_103

Control Policy: Events ? Condition ? Action `policy-map type service`

- A given a set of predefined events, operands, operators and actions are used in combination to define network behavior as needed..

  I.e.: If an event E is raised, under condition C1 or C2, do action ‘A’. Condition default, do action ‘B’

- Example:

```
policy-map type control IP_RULE3
  class control always event session-start
   1 service-policy service name PBHK_SERVICE
   2 authorize aaa password lab identifier mac-address
   3 service-policy service name L4_REDIRECT_SERVICE
   4 service-policy service name DEFAULT_NETWORK_SERVICE
   5 set-timer IP-UNAUTH-timer 5
```

Actions

Always == no Condition

Event (predefined)

Implicit action stop if it works

Service Reference (Name)

Creates a timer that will generate an event 5 minutes later.

Applying Control Policies

- **Association**

  A policy can be referred under a global scope, interface scope, atm PVC etc…

- **Example**

```
interface eth3/0
     service-policy control my-pppoe-rule
```

Local or Remote Feature Definiton: Example: Port Bundle Host Key

Cisco.com

- **Features can be configure local (using CLI) or remote (RADIUS)**
- **Feature Examples: Port Bundle Host Key, L4 redirect, Subscriber ACL, Idle Timer, QoS, Session/Service Accounting, VRF, …**

```
interface .... (SESM facing interface)
 ip portbundle outside

policy-map control rule-map
 class control always event session-start
  2 service-policy service ip-portbundle

policy-map service ip-portbundle
 ip portbundle

ip portbundle
 source Loopback0
```

```
Username = ip-portbundle
Password = <subscriber service
password>

VSA cisco av-pair [26,9,1]:
“ip:portbundle=enable”
```

- **Note:**
  - **The PBHK feature is a feature which works on the entire session (No Traffic Class)**
  - **Keeping PBHK a separate service, is advised. You could configure L4 redirection under the same policy-map but what if you would like to unapply the service…**

Conditional Debugging for ISA

- Thousands of sessions
- Requires: Conditional debugging / Debug Filtering

  `debug condition …`

  Applicable to AAA/Radius, VPDN, PPPoE, PPPoA, PPP, Session Manager, Local ID Manager, Feature Modules, ATM Components, Policy Manager

- Example

  Step1: At the router exec prompt, enable conditional debugging:

  ```
  Router1# debug condition username foo@cisco.com
  ```

  Step2: Enable the required debugs

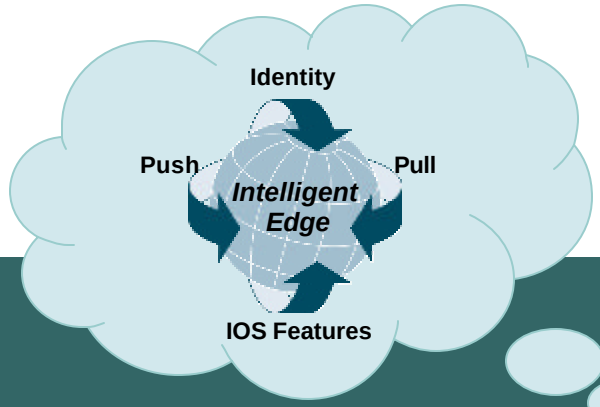
  ```
  Router1# debug ppp negotiation
  Router1# debug vpdn l2x-event
  Router1# debug pppoe event
  Router1# debug subscriber event
  ```

One Final Note: Doesn't ISA resemble SSG?

- **ISA implements a new Session Architecture in IOS**
- **The externally observable behavior of ISA resembles in several components SSG**
- **ISA Highlights beyond SSG**

MPLS integration	Reduced CAPEX and OPEX with integrated edge for MPLS and Broadband Aggregation with Service Selection
Multidimensional Identity	Facilitates policy enforcement based on multiple criteria
In-VRF service selection	Subscriber authentication, service selection based on VRF
Conditional debugging	Debugging based on any subscriber, service or any other identifier
Policy based rules	Association of actions based on events
Dynamic Policy Push	Policies for session bandwidth, security, accounting can be pushed dynamically in real time while session is still active
IP Sessions	Extended support including subnet and IP interface control

Summary & Closing Thoughts



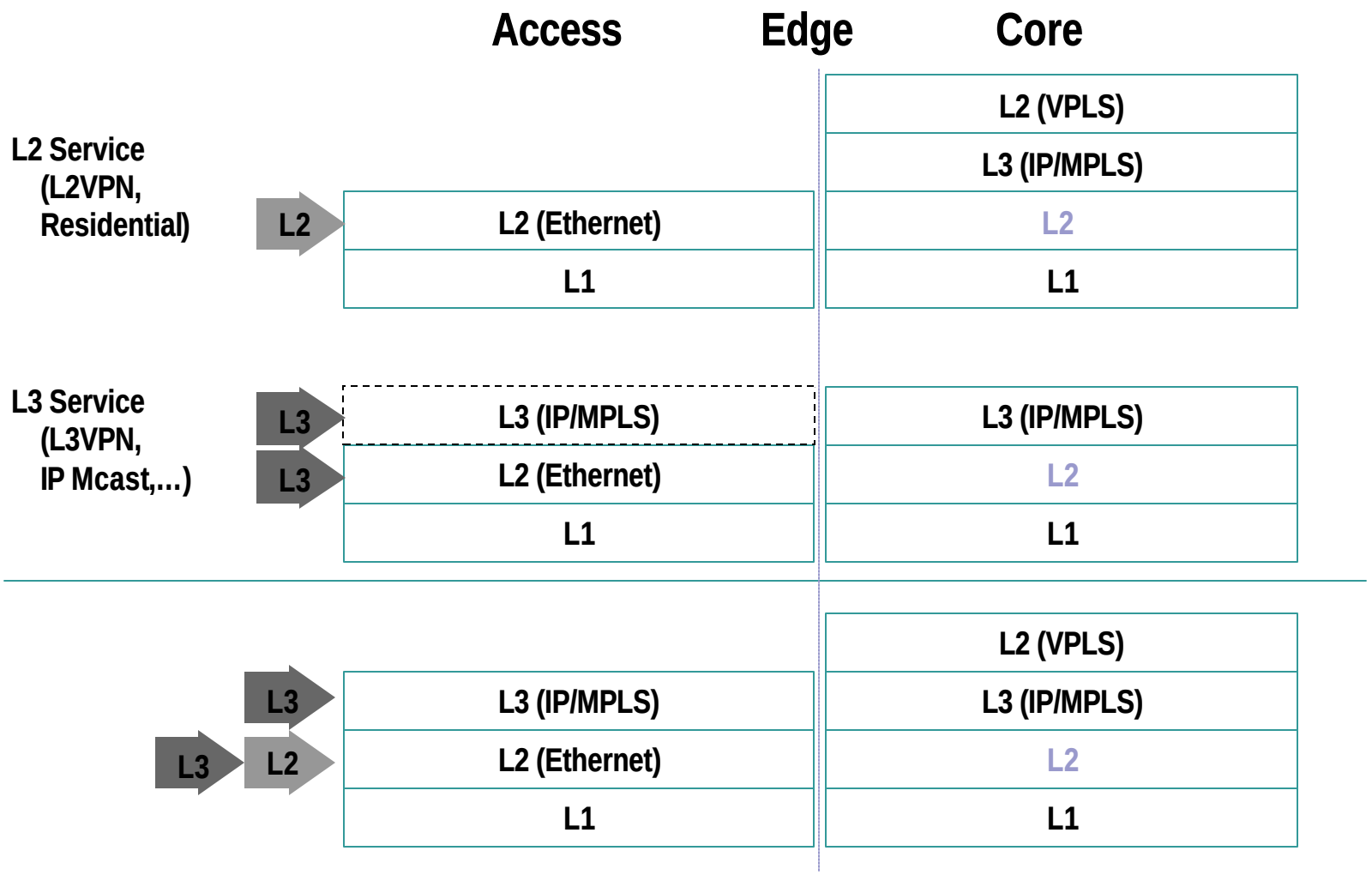
ISA: Thoughts on the future

- SGI
- P-Cube
- Evolution of shared network and application identity
- Growing set of applications
- Revenue for the service providers!
- Better services for end users!!

Service driven Reference Architecture:

"L2 Service with L2 edge, L3 Services with L3 edge (or L2 as backhaul)"

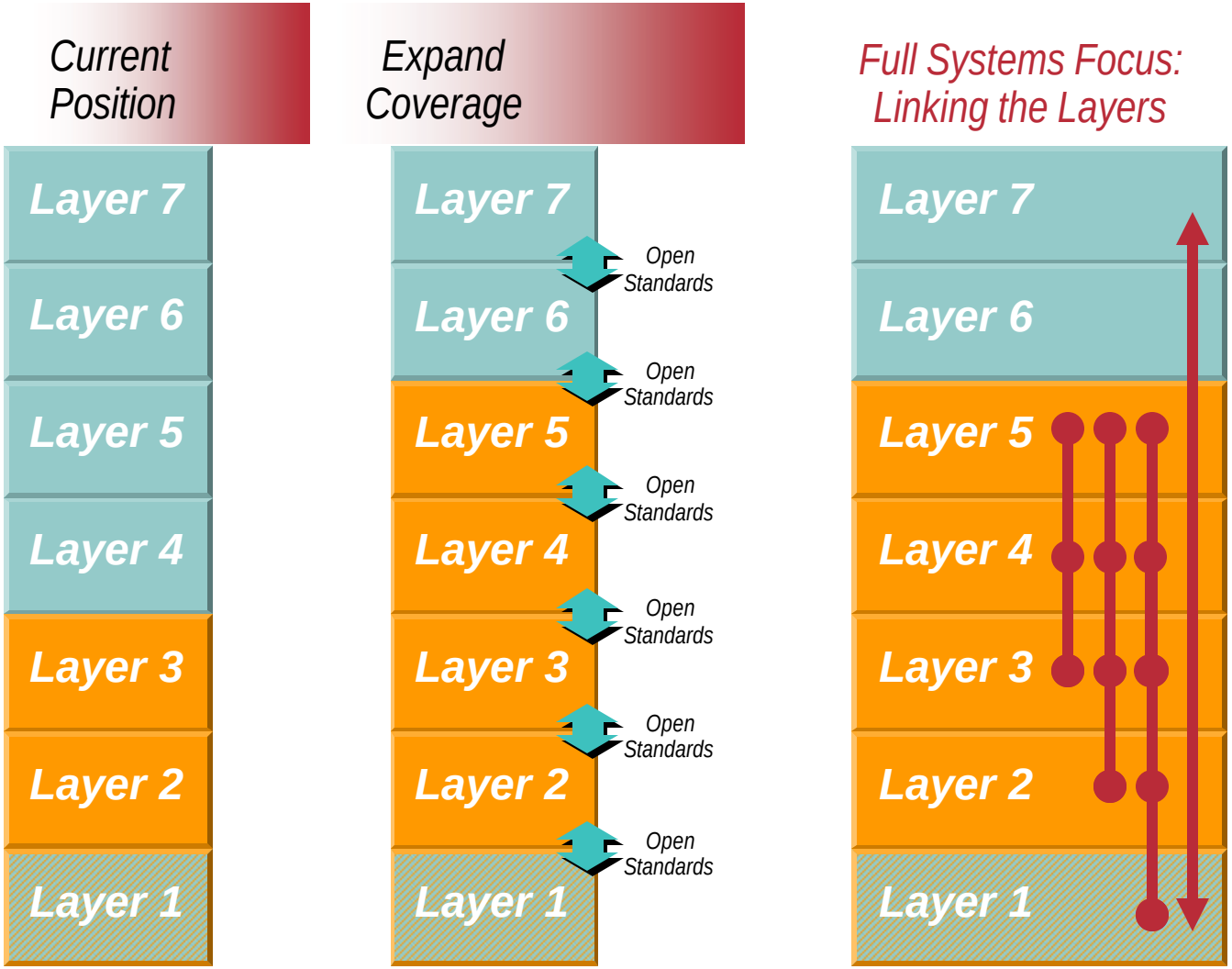
Cisco.com



Summary: Convergence & Expanding to Layer 5 Session Control

Introduce New Profitable Services

Increase CAPEX & OPEX Efficency



Reference Materials

- **The Stupid Network Article - http://www.isen.com/stupid.html**
- **Cisco Vision on Network Evolution – http://newsroom.cisco.com/dlls/tln/content/Cisco_Tech_Vision_frame.html**

Complete Your Online Session Evaluation!

Cisco.com

Muchas Gracias por asistir a esta sesión.

Por favor, complete el formulario de evaluación.

¡Muchas gracias!

Session ID: AGG-2025

"Intelligent Edge Networking:
Next Generation Concepts for Ethernet/DSL aggregation and Dynamic Service Selection"