



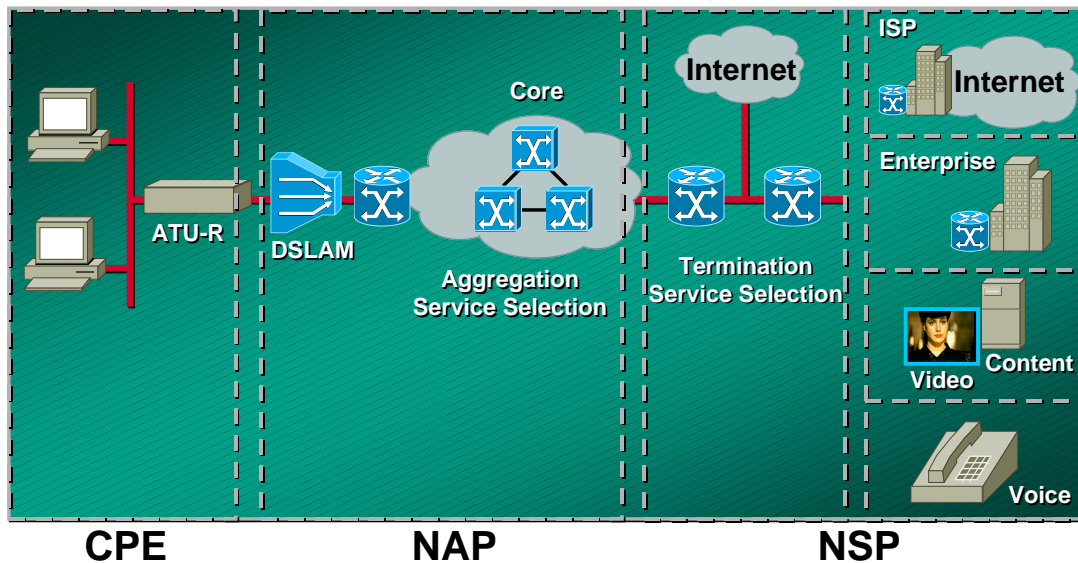
The Challenge

- There is a long list of service architectures in “DSL land”
- Each has its own acronym, difficulties and advantages
- There are some hard and fast rules to know but many design tradeoffs are based on “strongly held opinions” (a.k.a. religious issues)

Agenda

- **Understanding Different Architectures**
- **Design Considerations for Implementing Various Architectures**
- **Applying these Architectures to Real Life Scenarios**

Functional Segments



CPE; Customer Premise Equipment
NAP; Network Access Provider
NSP; Network Service Provider

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

5

Typical Service Offerings (= Business Model)

- **Retail**
- **Wholesale**
- **VPNs/corporate access**
- **Services offered**
 - Value added services (voice, video, portals, etc.)
 - Service selection capabilities for subscribers

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

6

Access Methods (How Subscriber Traffic Reaches NAP)

- **Layer 1**
xDSL (ADSL, SDSL, G.Lite, G.SHDSL...)
- **Layer 2**
ATM
- **Layer 3**
IP traffic delivered via bridging,
PPP or routing

Typical Core (How NAP Delivers Traffic to NSP)

- **ATM (end-to-end PVC)**
- **IP (L2x, GRE)**
- **IP + ATM (MPLS/VPN, L2x)**

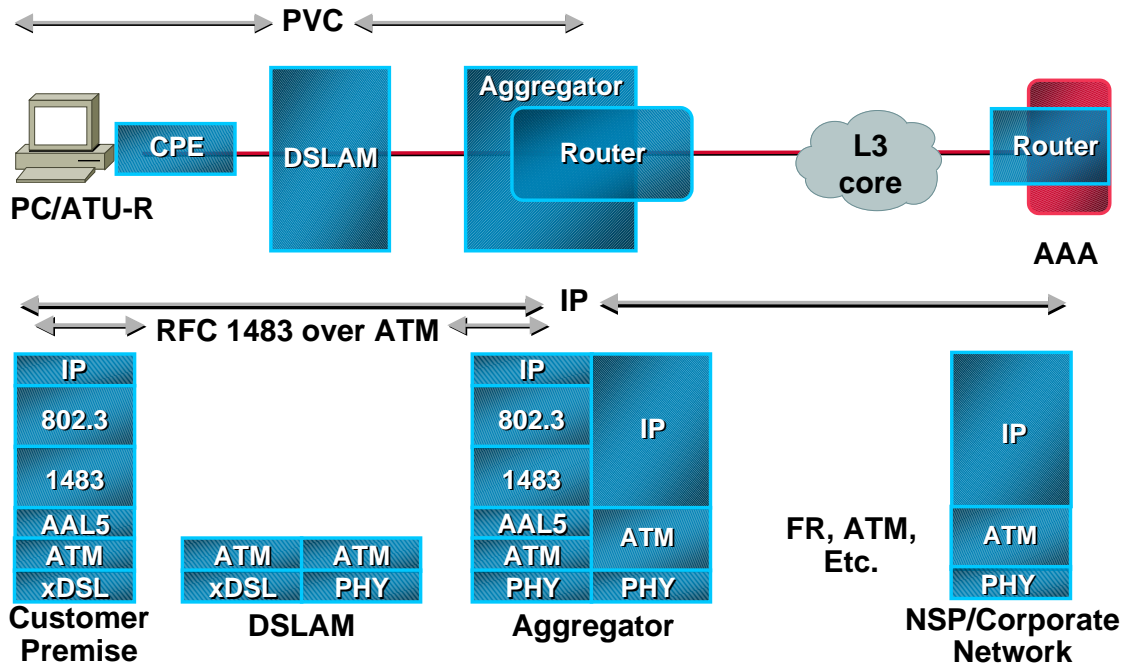
Access Methods

- **Bridging**
- **PPP**
- **Routing**

Bridging Implementation

- **CPE–RFC 1483 (now RFC 2684) bridging**
- **Aggregation/termination**
 - Integrated Routing Bridging (IRB)**
 - Routed Bridge Encapsulation (RBE)**
- **Core**
 - Usually ATM, if no aggregation used**
 - With VC aggregation, typically IP or IP+ATM**

Protocol Stack



2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

11

How Does RBE Work?

- **Subscriber traffic is carried in a BPDU**
- **The routed-bridge ATM interface treated as a routed interface;**
- **For packets originating from the subscriber end**
Ethernet header is skipped
Packet forwarded based on Layer 3 information
- **For packets destined to the subscriber end**
Destination IP address is checked on the packet
Outbound interface is determined from routing table
ARP table is checked for the destination Mac address,
if none found than ARP request sent out on the destination interface only

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

12

Access Methods

- Bridging
- **PPP**
- Routing

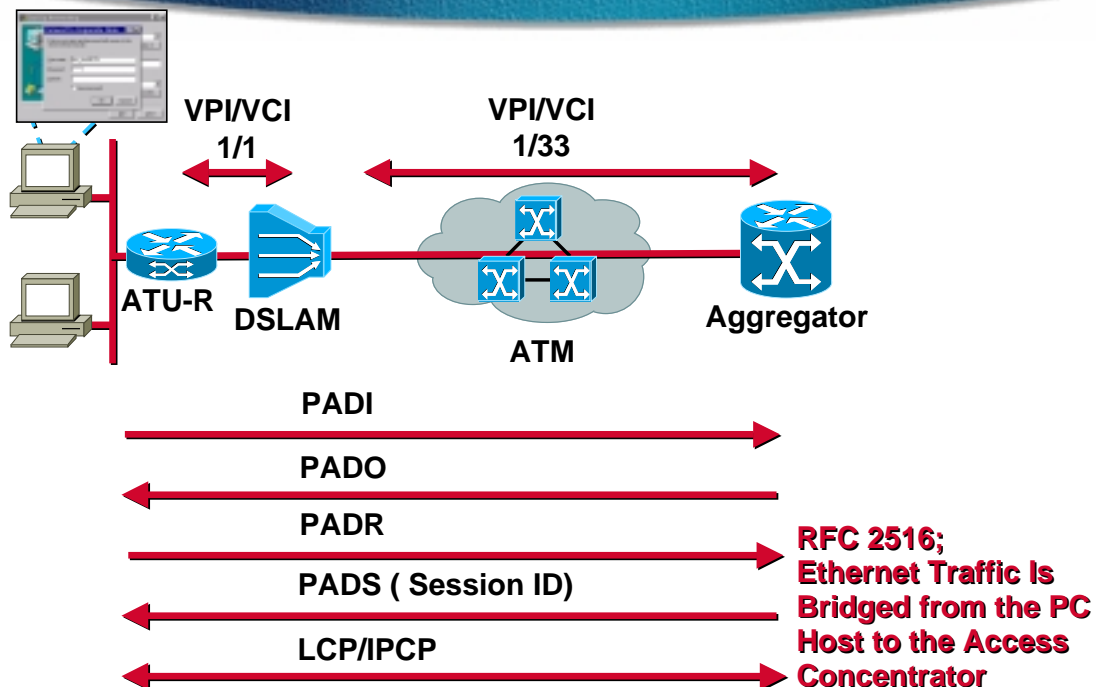
PPP Implementation

- **Three access methods from subscriber**
PPPoA, PPPoE, L2TP client
- **Aggregation**
PPP sessions terminated
PPP sessions tunneled over to NSP
- **Core**
End-to-end ATM PVC, PPP
terminated at NSP IP, ATM or IP+ATM;
(L2TP, L2F, MPLS/VPN)

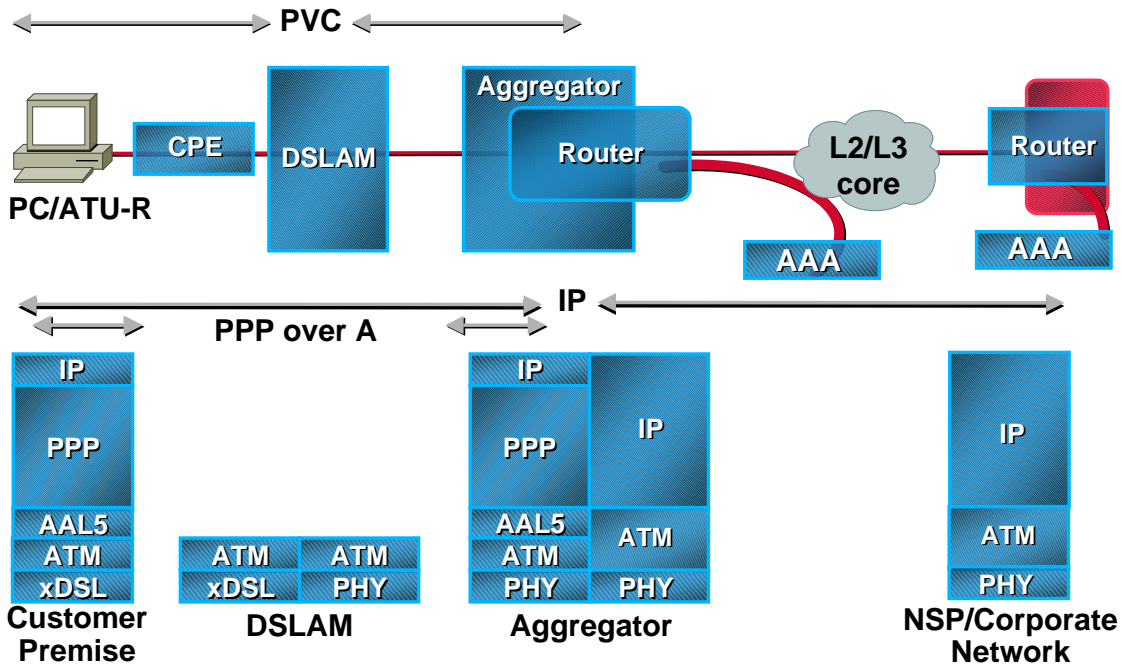
How Does PPPoA Work ?

- Based on RFC 2364 (PPP over AAL5)
VC multiplexed PPP, LLC encapsulated PPP
- CPE and aggregation goes through;
LCP negotiation
Authentication phase
IPCP
- Aggregation configured with virtual template
Brings up the virtual access interface
Assigns IP address to the CPE via local pool, dhcp, local radius or proxy radius
Establishes a 32-bit host route

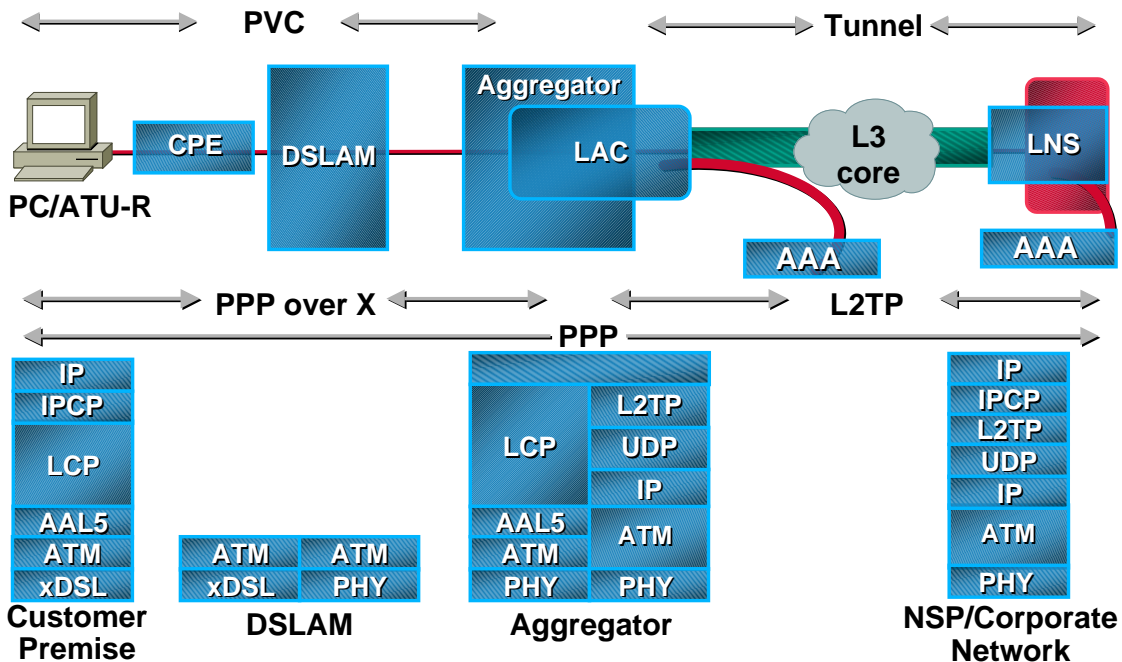
How Does PPPoE Work?



Protocol Encapsulation PPP Termination



Protocol Encapsulation L2TP Tunneling of PPP Sessions



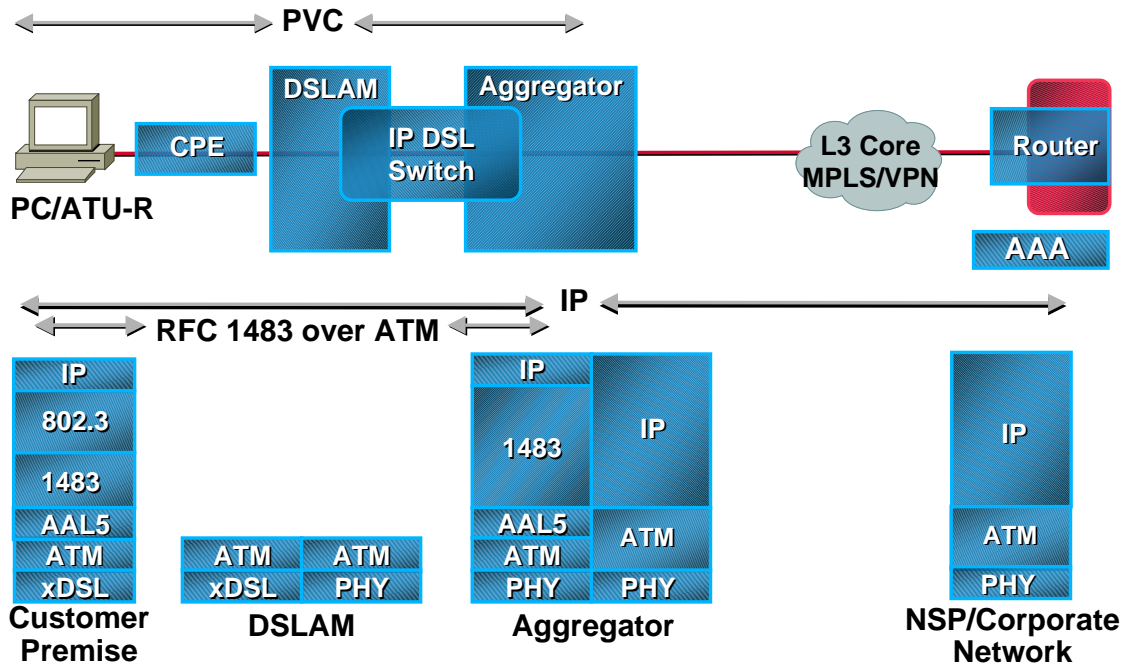
Access Methods

- Bridging
- PPP
- **Routing**

Routing Implementation

- **CPE**
 - CPE in routing mode, single or multiple subnet behind CPE
 - Routing protocol support
- **Aggregation**
 - Learns subscriber routes through routing protocol or static routes
- **Core**
 - Typically, IP+ATM (MPLS/VPN)

Protocol Stack



2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

21

How Does it Work?

- Routed PDUs (Protocol Data Units) encapsulated in AAL5
- Sub-interface on aggregation device configured to route IP
- Packets forwarded based on the destination IP address
- CPE and aggregation can exchange routes using routing protocols or use static routes

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

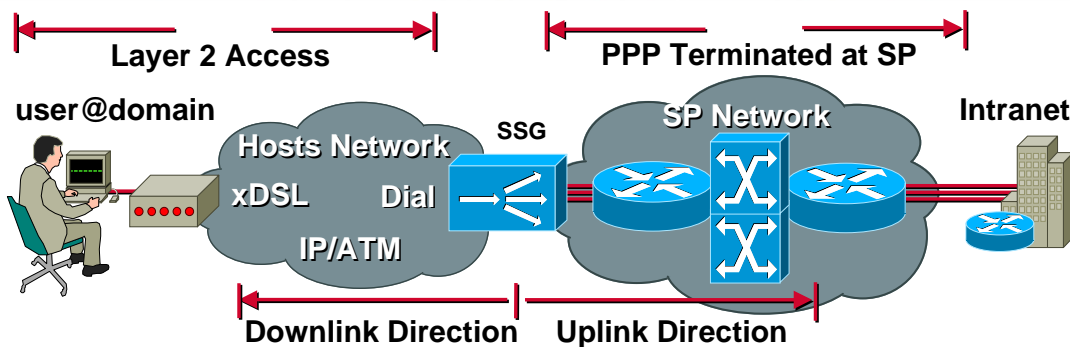
cisco.com

22

Service Selection

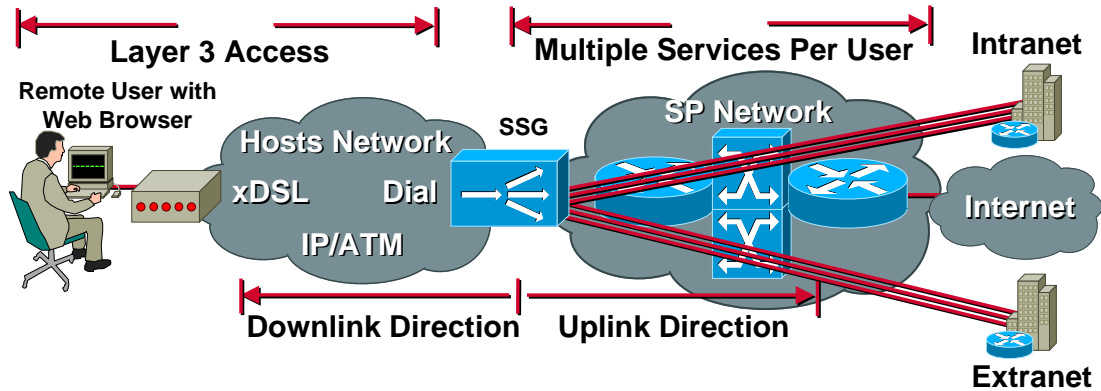
- **Layer 2 service selection with PPP**
PTA–MD, PPPoE
Only single destination per PPP session
- **Layer 3 service selection with PPP, bridging and routing**
Web selection
Multiple destinations simultaneously even with single PPP session

L2 Service Selection



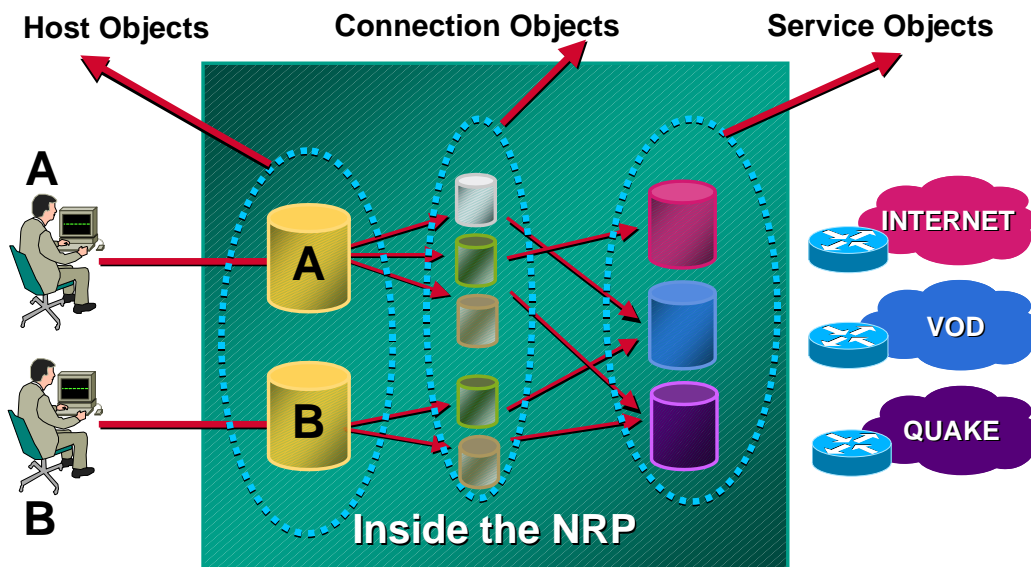
- PPP termination aggregation (PTA–MD) permits the user to access one service at a time
- Each user can determine their own destination and be charged accordingly
- Standard PPP termination as in dial

Layer 3 Service Selection



- Service selection via web browser
- Multiple-simultaneous servers per user
- Each user can determine their own destination and be charged accordingly
- Each host is associated with a host object
- Each connection has a connection object

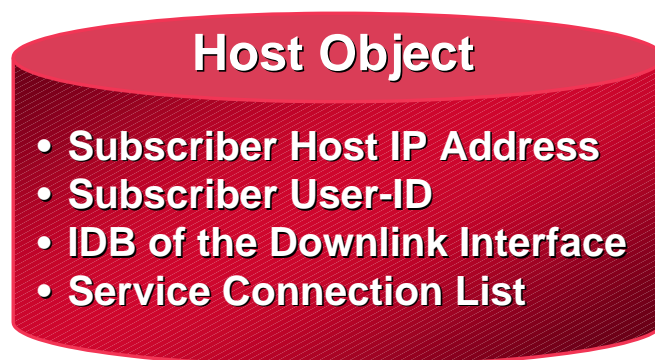
SSG Terminology the Object Model



Example: User A has 3 services defined, User B has 2 services

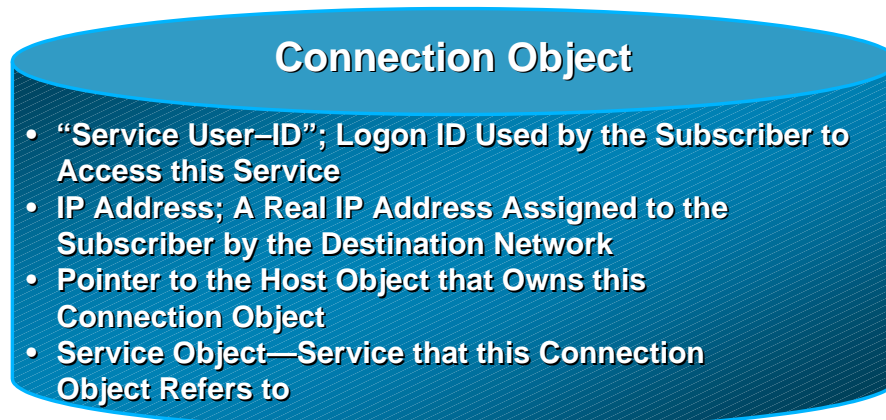
SSG Terminology (Cont.)

- **Host object:** A “Host Object” represents an active user account in the SSG internal database. It’s created as soon as the user is authenticated successfully. The Host Object is comprised of the following:



SSG Terminology (Cont.)

- **Connection Object:** A “Connection Object” represents an active connection to a service (destination network); It’s created when a subscriber logs on to a service and is destroyed when he/she logs off the service
- A Host Object “owns” one or more Connection Objects



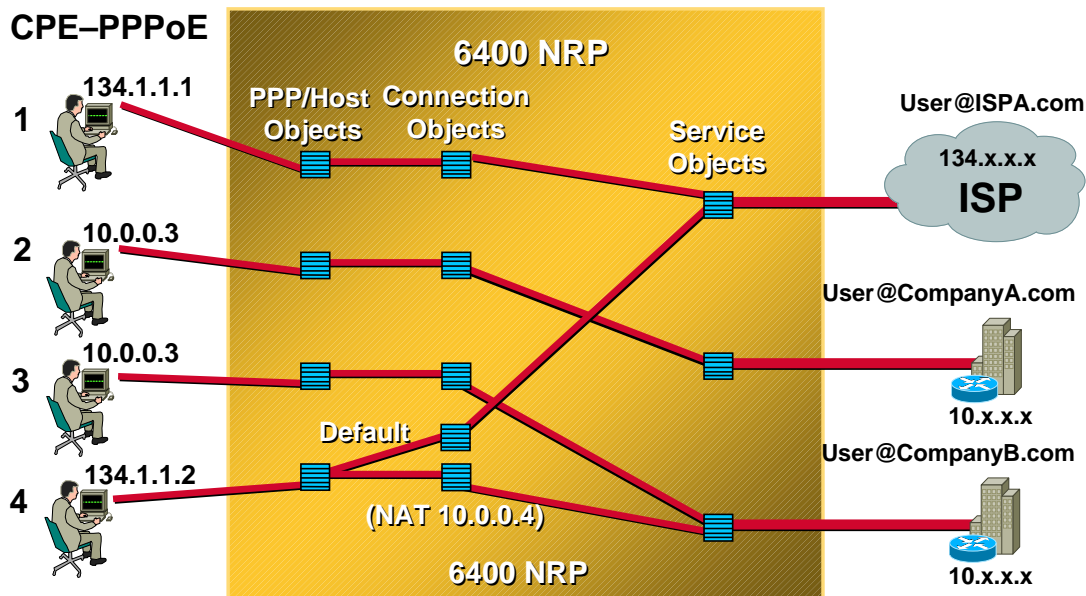
SSG Terminology (Cont.)

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

Service Object

- **Service Name;** Name of the Service Itself
- **Domain Name;** A List of Domain Names Associated with this Service (Used for DNS Redirection)
- **Service Type;** Defines the Kind of Service (Passthrough, Tunnel or Proxy)
- **Destination Network;** Every Service Is Identified by Allowing/Disallowing Access to a Network Segment Identified by a Combination of IP Address and a Mask
- **Next Hop Address;** Used to Determine Next Hop for Routing upstream Traffic—Discussed Later
- **Remote RADIUS Server Info;** for Proxy Type Service only

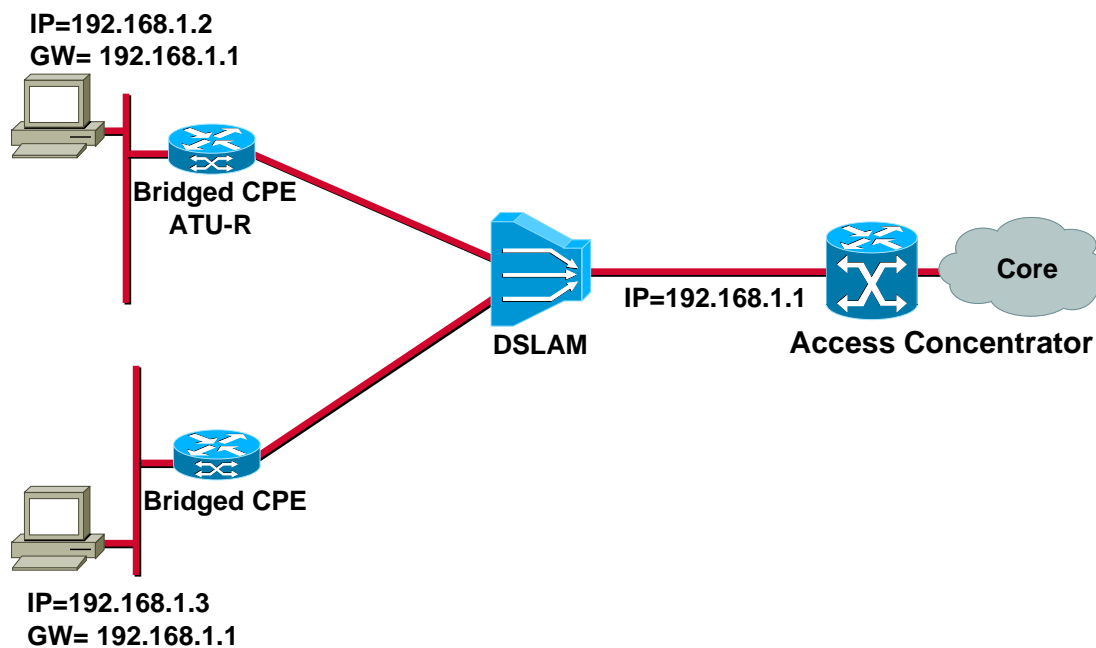
Overlapping IP Address Support



Agenda

- Understanding Different Architectures
- **Design Considerations for Implementing Various Architectures**
- Applying these Architectures to Real Life Scenarios

Typical RBE Architecture



RBE IP Address Management

- **IP addresses provided by DHCP**
Server can be;
 - On NAP network
 - On NSP network
- **If using DHCP relay, the remote server must be reachable and must have a return route**

Pros and Cons

PROS

- **Highly scalable and better performance than IRB**
- **Avoids IP hijacking, ARP spoofing and broadcast storms**
- **Efficient way to control number of hosts behind CPE**
- **Configuration-less CPE**
- **Support existing bridged CPE**
- **Simple implementation/provisioning**
- **L3 SSG/SSD**

CONS

- **Consumes more IP address if used with numbered interfaces**
- **No accounting (unless using L3 SSG) and authentication**
- **In wholesale scenario, NAP needs to provide IP address**

Design and Implementation Key Points for Bridging

- **Very simple implementation and provisioning**
- **Reduce the subscriber maintenance cost tremendously for the network access provider**
- **Security holes for bridging overcome by RBE, no more ARP broadcasts and IP hijacking; Efficient use of the bandwidth**
- **IP addresses assigned to hosts via DHCP server**
- **DHCP server could be located at NAP or NSP**

Design and Implementation Key Points for Bridging Continued

- **IP address conservation with the support of DHCP relay with unnumbered interface (RBE)**
- **Core is mainly IP if subscriber traffic terminated at NAP, otherwise end-to-end PVC (which results in VC depletion issue)**
- **SSG; Web selection can be used to provide accounting**
- **Service selection possible via SSG web selection; service selection at layer 2 (subscriber end) not possible**

Where Can We Use Bridging?

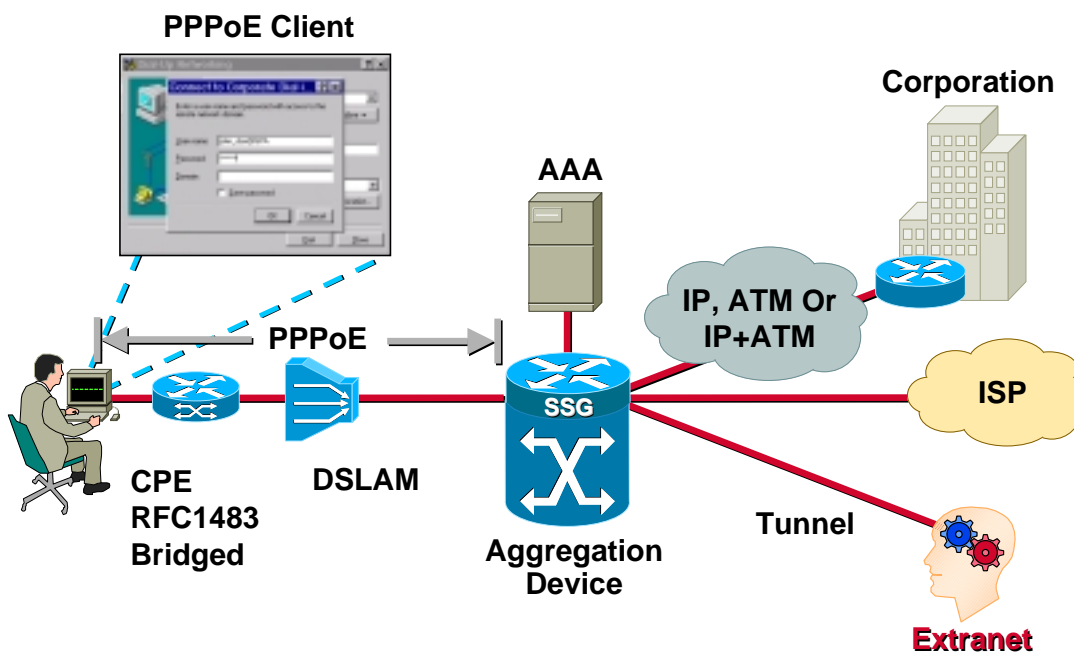
- **If the ATU-R is very simple and can only do RFC1483 (now RFC 2684) bridging**
 - **Early models of all CPE were simple bridge**
- **The NAP/NSP does not want to maintain the client software on hosts**
- **Good for ISP**

Where Can We Use Bridging (Cont.)

- **Only one PVC from the subscriber CPE to NAP; No requirement for doing routing on multiple PVCs**
- **Suitable for residential users**
- **Early ADSL providers used bridging both for subscriber traffic and also to reach service providers**

This results in a serious problem of VC depletion, the NAP delivers a PVC for each subscriber to the NSP

Typical PPPoE Architecture



2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

39

PPPoE IP Address Management

- **Same as PPP in dial mode**
 - Address can be assigned to host by NAP if session terminated, or by NSP if tunneled
- **IP addresses assigned by RADIUS**
 - Local or proxy
- **IP address assigned from pool**
 - Local or from radius
- **The Ethernet NIC on PC does not need an IP address to start the PPPoE session**

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

40

Pros and Cons

PROS

- Configuration-less CPE
- Support existing bridged CPE
- Multiple sessions per VC
- Per subscriber authentication and accounting
- NAP can offer VPN services using PTA-MD or L2TP tunneling
- Service selection possible at subscriber CPE and also support for web selection

CONS

- Requires client software on the hosts, increases maintenance
- PPPoE client support for non-windows-based operating system

Design and Implementation; Key Points for PPPoE

- Identification of PPPoE client and its compliance to RFC 2516, client software to be installed on all hosts behind bridged CPE
- MRU not to exceed 1492 (PPPoE header=6 Octet, PPP PID=2 Octet), total MRU for Ethernet 1500
Configure on virtual-template
- PPPoE based on dial model, requires subscriber to enter username and password every time they want to connect to a service
- 1 vpdn-group and virtual-template for all PPPoE traffic
Put per user configuration in radius profile

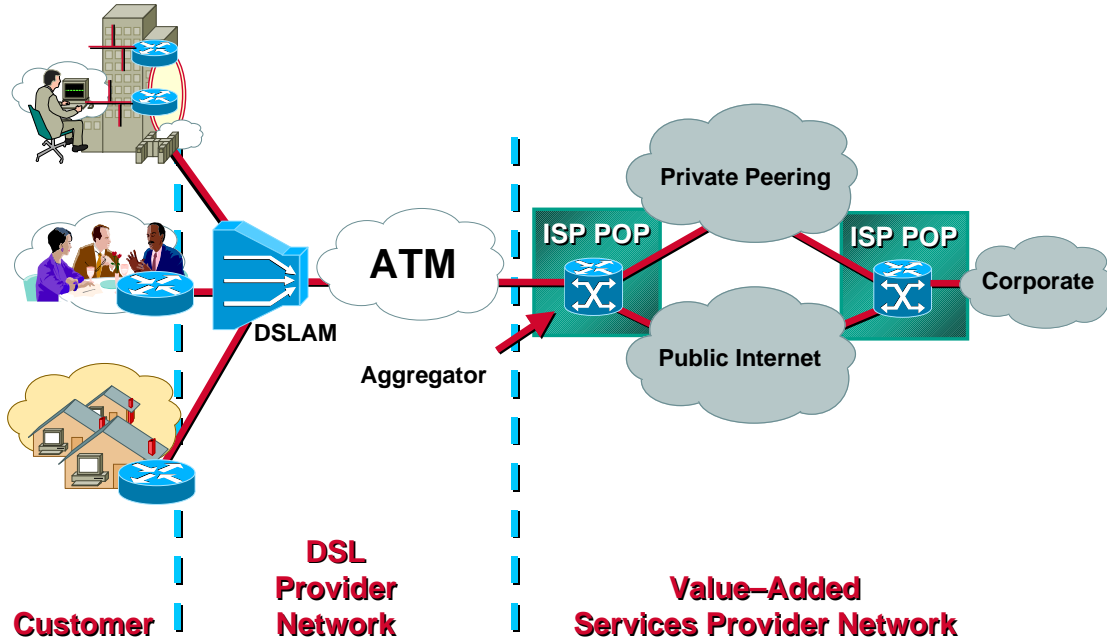
Design and Implementation Key Points for PPPoE (Cont.)

- **Multiple PPP sessions per PVC, allows per subscriber accounting**
- **PPPoE is CEF switched**
- **Cloning virtual access Interfaces is CPU intensive and should be pre-cloned**
- **To avoid Denial of Service attacks, by default only 100 sessions per VC is configured, this can be changed**

When to Use PPPoE

- **Service provider is willing to maintain host software at subscriber end**
- **Dynamic L2 service selection**
- **Low cost CPE, bridged**
- **Offer VPN services using L2X**
- **No routing required on the CPE between multiple PVCs**

Typical PPPoA Architecture



PPPoA IP Address Management

- **CPE is smarter and more complex**
 - CPE can do PAT/DHCP, to conserve IP address
 - IP address gets assigned to CPE
 - IP subnet feature, prevents NAT
- **PPPoA sessions can be terminated on NAP or tunneled out using L2x**
 - If terminated IP address provided by NAP
 - If tunneled by the LNS
- **IP address allocation same as PPPoE**

Pros and Cons

PROS

- VPI/VCI authentication
- Manageable CPE
- Per session accounting and authentication
- IP address conservation if CPE configured for NAT/PAT
- Secured VPN access by using L2x at NAP
- L3 SSG/SSD
- Can use more than one PVC per CPE

CONS

- Single session per VC
- Can not work with PTA-MD if NAT is being implemented at CPE, because SSG requires IP address per host objects
- Per subscriber accounting not possible

Design and Implementation; Key Points for PPPoA

- Feature-rich CPE
 - CPE configuration can be complex and increase install time
 - No host configuration
 - Allows IP address conversation
- NAT
- IPCP subnet negotiation to avoid NAT

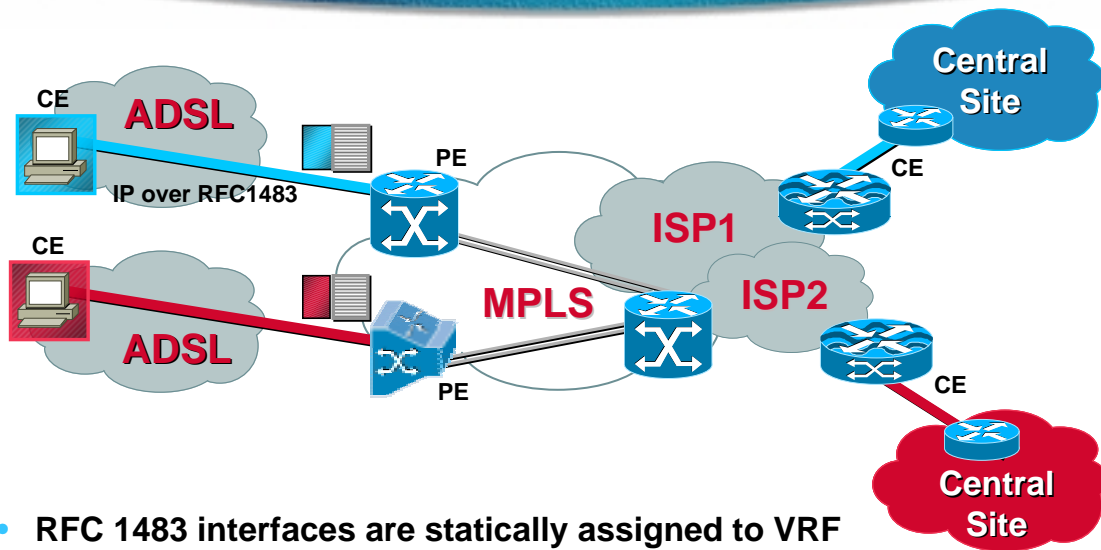
Design and Implementation; Key Points for PPPoA

- **VPI/VCI-based authentication**
- **NAT can break L3 service selection**
Only one IP address seen by SSG
- **Number of subscribers limited by number of VCS supported**
One session per VC

When to Use PPPoA

- **No host-based software**
- **Authentication and accounting**
- **Need to conserve IP addresses**
- **Intelligent CPE**
Access-lists
- **Use of Multiple PVCs on CPE for different services**
- **If require closed user group**
VPI/VCI authentication

RFC 1483 Routing



- RFC 1483 interfaces are statically assigned to VRF
- Can run RIP, BGP across upstream interfaces
- ADSL provider cannot offer service selection

IP Address Management

- Exactly the same issues and solutions as RBE

Address assignment

DHCP configuration

Routing

When to Use

- **Routing implemented mainly for enterprise customers**
- **If access provider wants to offer VPN services to enterprise, or different ISPs**

Pros and Cons

PROS

- **Best approach to provide enterprise VPNs**
- **Manageable CPE**
- **Accounting possible through NetFlow**
- **IP address conservation if CPE configured for NAT**
- **Firewall feature set, to avoid DoS attacks**
- **Can have more than one subnet behind the CPE**
- **L3 SSG/SSD**

CONS

- **CPE to be configured for routing, requires routing understanding, and increases maintenance and provision costs for service provider**
- **No authentication unless used with web selection**

Design and Implementation; Key Points for RFC 1483 Routing

- Same as any routed network
- CPE to do 1483 routing and support routing protocol(s)
- Dynamic routing reduces provisioning efforts
- IP address assigned through DHCP server
- Number of interfaces on aggregation depends on IDB limits

Summarizing Access and Core Architectures

Access	IP	L2TP	PTA-MD	MPLS-VLN
RBE	✓	✓ SSG	✗	✗
PPPoE	✓	✓	✓	✓
PPPoA	✓	✓	✓	✓
1483R	✓	✓ SSG	✗	✓

**IP Address Management Varies Depending on
Access and Core Architecture Selected**

Things to Consider

- **Identify the business model**
Wholesale vs. retail, corporate access/VPN vs. residential
- **Who is providing the IP addresses?**
Is it NAP or NSP or enterprise?
Tunneling is an easy way to support last 2 options
- **Do addresses overlap?**
They nearly always do in residential scenarios
- **How is NSP reached from NAP?**
L2 core makes PTA easier
L3 core requires either tunnels or IP-VPN
- **Is NAT tolerated?**
If not, no L3 service selection
- **Is host based–software acceptable?**
If not, no PPPoE/L2TP

Things to Consider

- **Network management, provisioning/billing**
- **Traffic engineering for bandwidth allocation and QoS, SLA**
- **Geographical distribution of PoPs and aggregating them**
- **NSP's hardware requirements for terminating tunnels and PPP sessions**
Includes interface type
- **Oversubscription**
Within NAP cloud
NSP interface speed; subscriber interface speeds

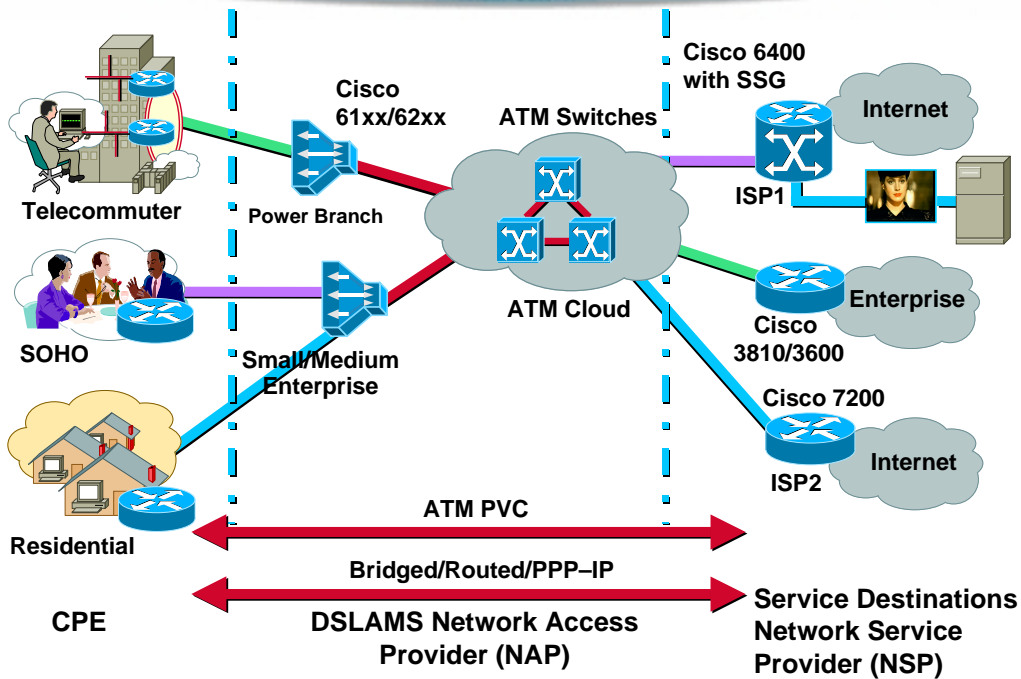
Agenda

- **Understanding Different Architectures**
- **Design Considerations for Implementing Various Architectures**
- **Applying these Architectures to Real-Life Scenarios**

Scenario 1: Requirements

- **Customer is a NAP, acting as NTP**
- **NAP does not want to handle any IP address management**
- **NAP does not offer any local services**

Scenario 1: End-to-End ATM



2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

cisco.com

61

Scenario 1: Design Considerations

- VC depletion
- ISP to terminate high number of ATM PVCs
- NAP does not manage any IP addressing, ISP can opt to provide public or private address
- CPE could implement any encapsulation method, defined by ISP; Provisioning done by ISP
- NAP can not offer per subscriber accounting
- Suitable for low volume of subscribers per ISP

2900
1173_05_2000_c2 © 2000, Cisco Systems, Inc.

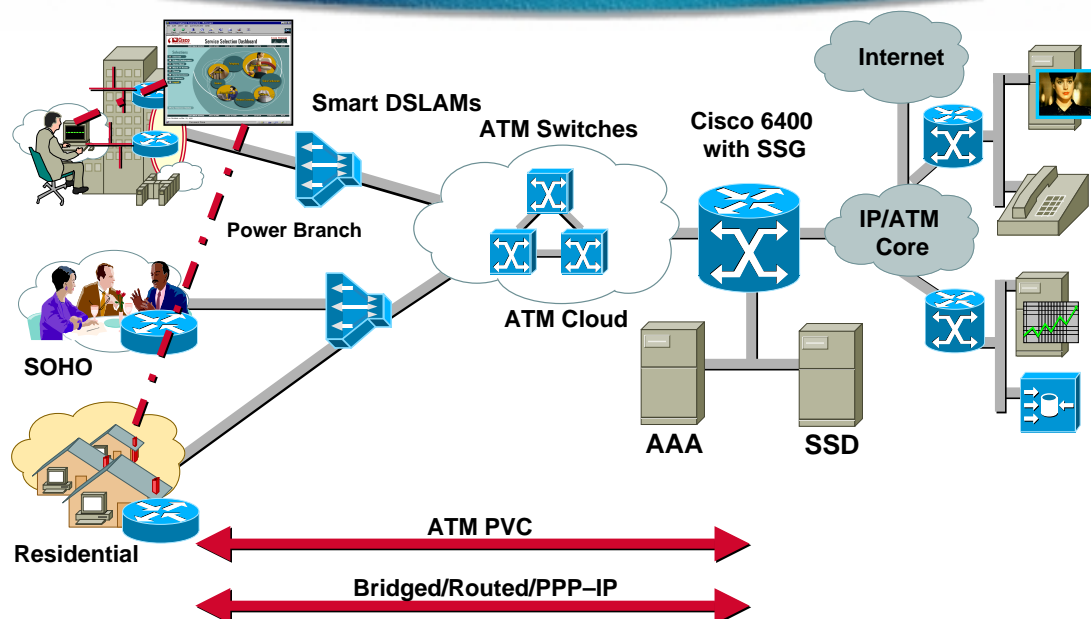
cisco.com

62

Scenario 2: Requirements

- **NAP is also an ISP**
- **Wants to offer contents and portals**

Scenario 2: Retail



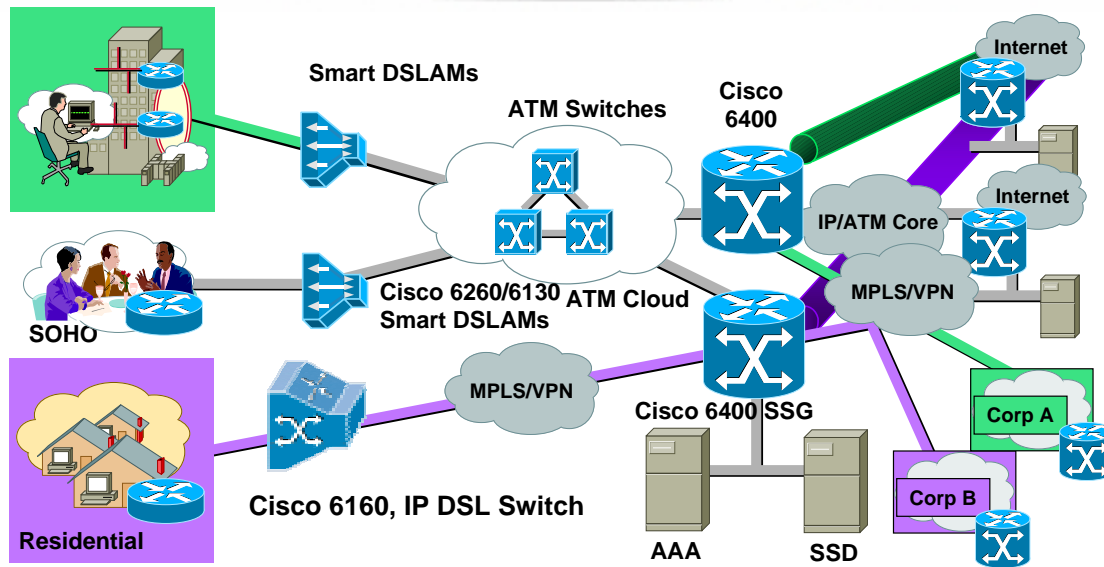
Scenario 2: Design Considerations

- **NAP needs to terminate subscriber PVCs**
- **Access is best suitable using RBE; Although, option for PPPoA, PPPoE is available**
- **NAP to provide IP address to the subscriber, using DHCP**
- **NAP to offer web-based service selection**
- **Subscriber can still access their corporate via Internet using IPSec or L2TP tunnel initiation**
- **Accounting using SSG and AAA**
- **Services reached via IP core of NAP**
- **If NAP opts to offer access to other ISPs, NAP may need to implement NAT**

Scenario 3: Requirements

- **NAP wants to offer wholesale services to other ISPs**
- **Wants to offer VPN services to corporate**

Scenario 3: Wholesale



Scenario 3: Design Considerations

- NAP can either reach ISPs using L2TP or PTA–MD
- Tunnel grooming, delivering IP, managed LNS
- Provide VPNs to corporate using MPLS/VPN
- For enterprise, 1483 routed access and for resident/SOHO PPPoE
- Layer 2 service selection possible using PPPoE for Residential/SOHO subscribers
- NAP can still have accounting records
- IP address managed by the ISP

Summary

- **Understanding different architectures**
- **Design considerations for implementing various architectures**
- **Applying these architectures to real life scenarios**

Relevant Sessions

- **2905–Troubleshooting DSL-Based Networks**
- **2906–DSL Product Update**



Design Principles for DSL-Based Access Solutions

Session 2900



Please Complete Your Evaluation Form

Session 2900

CISCO SYSTEMS



EMPOWERING THE INTERNET GENERATIONSM