DSL Architecture: Reliability Design Plan

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

CONTENTS

CHAPTER 1

Introduction

This brief chapter summarizes the purpose, scope, assumptions, and intended audience of this document. The remainder of the document is split into two parts:

- DSL Network Architectures
- Redundant Physical Network Considerations

Purpose

This document has two chief goals:

- To present various digital subscriber line (DSL) architectures as models for customers as they plan for DSL deployment.
- To illustrate how Cisco redundancy features can be used to support DSL environments and to explain how these features can be used to achieve reliability in a DSL Network.

Scope

This document addresses design and implementation of Cisco DSL technology solutions for remote customer premise equipment (CPE), central office (CO) CPE, and service provider (SP) equipment.

Technologies addressed in the architecture portion of this document include:

- Integrated Routing and Bridging (IRB)/RFC 1483 Bridging
- Routed Bridge Encapsulation (RBE)
- Point-to-Point Protocol over ATM (PPPoA)
- Point-to-Point Protocol over Ethernet (PPPoE)
- Service Selection Gateway (SSG)

Redundancy topics addressed include:

- Customer Premise Equipment (CPE) Considerations
- DSLAM 61xx/62xx Considerations
- Cisco 6400 Universal Access Concentrator (UAC) Considerations
- Chassis Redundancy

Related Documents

Product guides on CCO:

- 6100 (NI-1): http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c6100/index.htm
- 6100 (NI-2): http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c6130ni2/index.htm
- 6400: http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/index.htm

DSL technical marketing engineering (TME) architecture publications:

- http://dsl.cisco.com/architecture/
- *DSL SSG Training Lab* document by Rohit Aggarwal

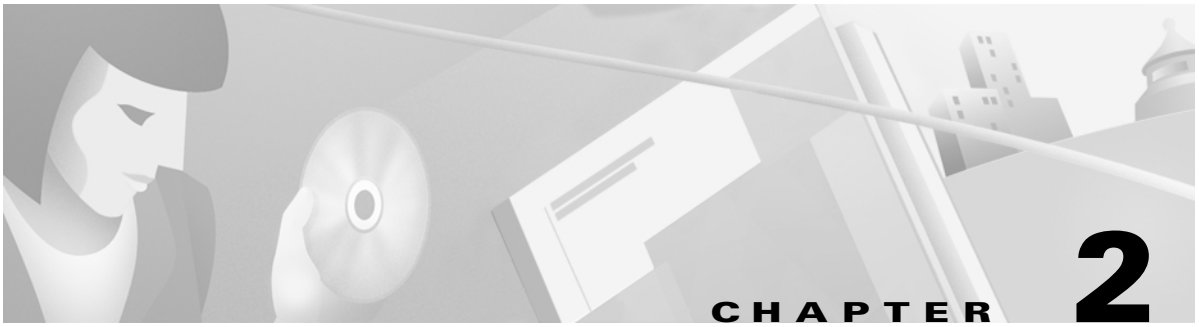
Intended Audience

This document is intended for but not restricted to the following audience

- Professional Services
- NSA consultants
- Training
- TAC
- DSL customers

Document assumes that the reader has

- Advanced xDSL technology knowledge
- Familiarity with xDSL Architecture Components



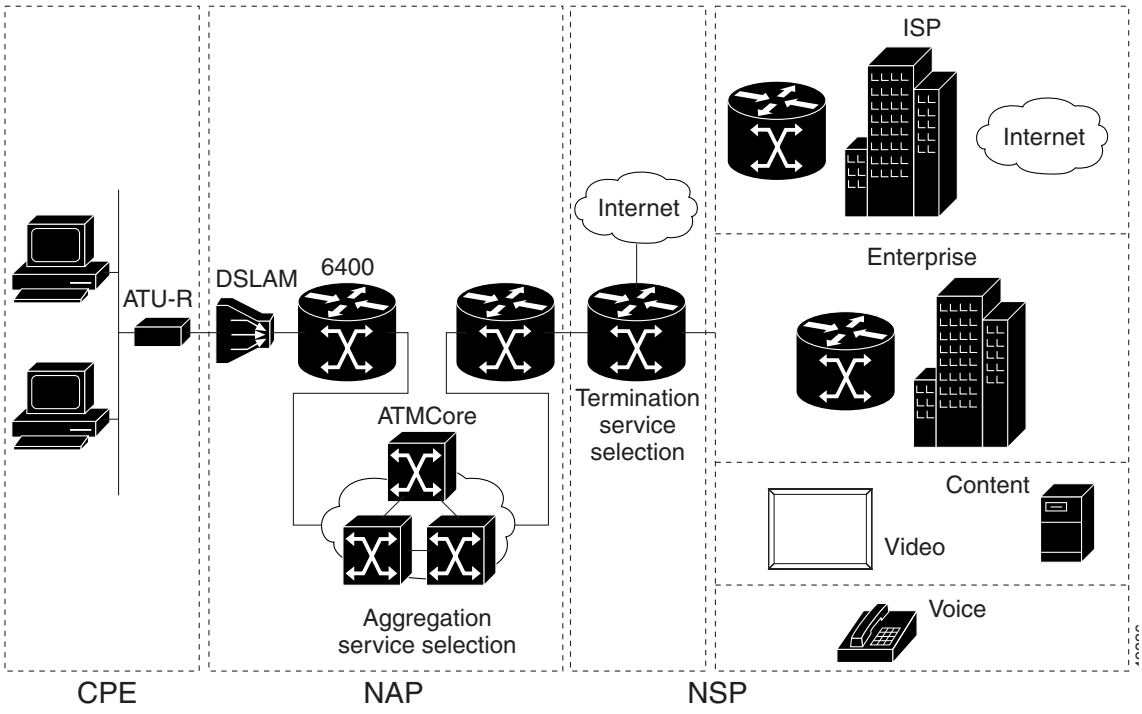
CHAPTER 2

DSL Network Architectures

This chapter provides a brief overview of available asymmetric DSL (ADSL) architecture options. A typical ADSL service architecture is illustrated in Figure 2-1. In the architecture illustrated, the network consists of Customer Premise Equipment (CPE), the Network Access Provider (NAP) and the Network Service Provider (NSP).

CPE refers to an end-user workstations (such as a PC) together with an ADSL modem or ADSL terminating unit router(ATU-R). The NAP provides ADSL line termination by using DSL access multiplexers (DSLAMs). The DSLAM forwards traffic to the local access concentrator, which is used for Point-to-Point Protocol (PPP) tunneling and Layer 3 termination. From the Layer 2 Tunneling Protocol Access Concentrator (LAC), services extend over the ATM core to the NSP.

Figure 2-1 Overview of a DSL network deployment including CPE, NAP and NSP components



Technology Overview

In this section some of the major DSL architectures are briefly addressed. The order of the architectures presented is from the most simplistic (bridging based) to the most robust and scalable (PPP based). Five general design scheme are described:

- Integrated Routing and Bridging (IRB)/RFC 1483 Bridging
- Routed Bridge Encapsulation (RBE)
- Point-to-Point Protocol over ATM (PPPoA)
- Point-to-Point Protocol over Ethernet (PPPoE)
- Service Selection Gateway (SSG)

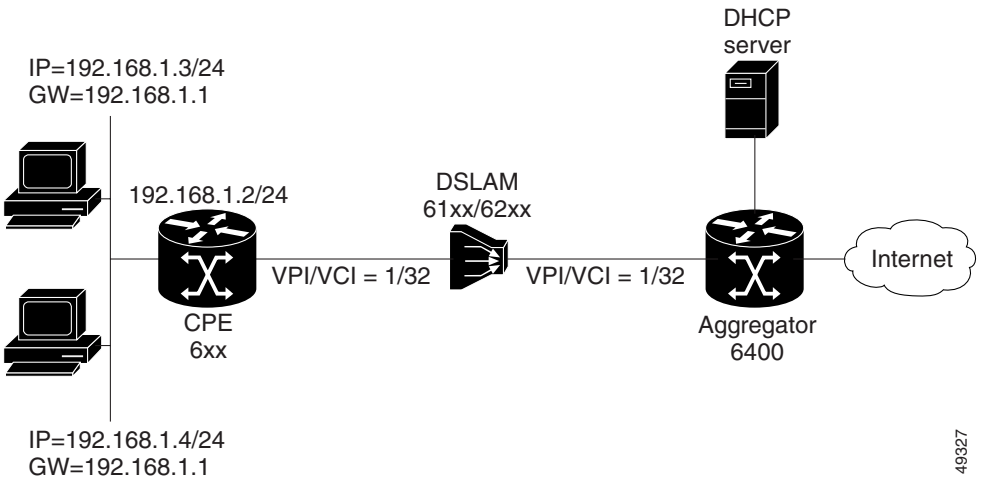
Integrated Routing and Bridging (IRB)/RFC 1483 Bridging

The RFC 1483 bridging architecture is very simple to understand and implement. AnATU-R acts as a bridge between the Ethernet and the wide-area networking (WAN) side. As a result, it requires minimal configuration.

With RFC 1483 bridging, CPE 802.3 Ethernet frames are segmented into asynchronous transfer mode (ATM) cells through ATM adaptation layer 5 (AAL5). The receiving equipment is notified of the type of protocol segmented into to cells because the standard calls appending logical link control/subnetwork access protocol (LLC/SNAP) information to the 802.3 frame before its segmented into the ATM cells. This enables the node route processor (NRP) in the 6400 to determine which protocols are embedded within theATM cells. This also allows for multiprotocol support for the subscriber. Since the bridge is in bridging mode, it does not care what upper layer protocols are being encapsulated.

Figure 2-2 illustrates a typical RFC 1483-based architecture.

Figure 2-2 RFC1483 Bridging (IRB) Architecture Example



Design Considerations

Some of the key points of this architecture that needs to be kept in mind while designing a DSL solution with IRB.

- Simple configuration
- No security for access
- Users in a bridge group (broadcast storms)
- Security by filtering
- Unable to limit devices or a location

Various other implementation aspects to consider include:

- Nature of subscribes, such as residential or small office/home office (SOHO)
- Services offered by NSP
- Type of billing
- Typical data volume, peak load timing variations, etc.

Security is the principal concern with an RFC 1483 architecture because bridging is vulnerable to *IP hijacking*. This security problem can be solved by using separate *bridge groups* per user. This approach is not optimal because the Cisco IOS has a bridge group limitation of 255. A more scalable solution would be to have the users coming to different multipoint subinterfaces and belonging to the same bridge group. Users in the same bridge group would not be able to see each other.

The RFC 1483 bridging model more suitable for smaller Internet service providers (ISPs) and corporate access networks where scalability is not an issue. Due to security and scalability issues bridging-based DSL architectures are losing popularity. NSPs and ISPs are migrating to Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet (PPPoE) which are scalable and secure, but more complex to implement.

Note IRB (RFC 1483-based bridging) strategies are not a recommended architecture and customers using IRB are encouraged to migrate to Routed Bridge Encapsulation (RBE) or one of the PPP-based protocols.

Node Route Processor (NRP) Configuration

The following is an example minimum configuration to bring up RFC 1483 bridging (IRB) on the NRP. The configuration reflects a typical IRB setup where a Bridge Group Virtual Interface (BVI) provides Layer 3 connectivity for a bridge group.

```
!
bridge irb
bridge 1 protocol ieee
 bridge 1 route ip
!
interface ATM0/0/0.132 point-to-point
 description PC6, RFC1483 Bridging
 no ip directed-broadcast
 pvc 1/32
  encapsulation aal5snap
 !
 bridge-group 1
!
interface BVI 1
 ip address 192.168.1.1 255.255.255.0
!
```

Routed Bridge Encapsulation (RBE)

Routed bridge encapsulation (RBE) was designed to address disadvantages of IRB, such as broadcast storms and security, while providing ease of implementation.

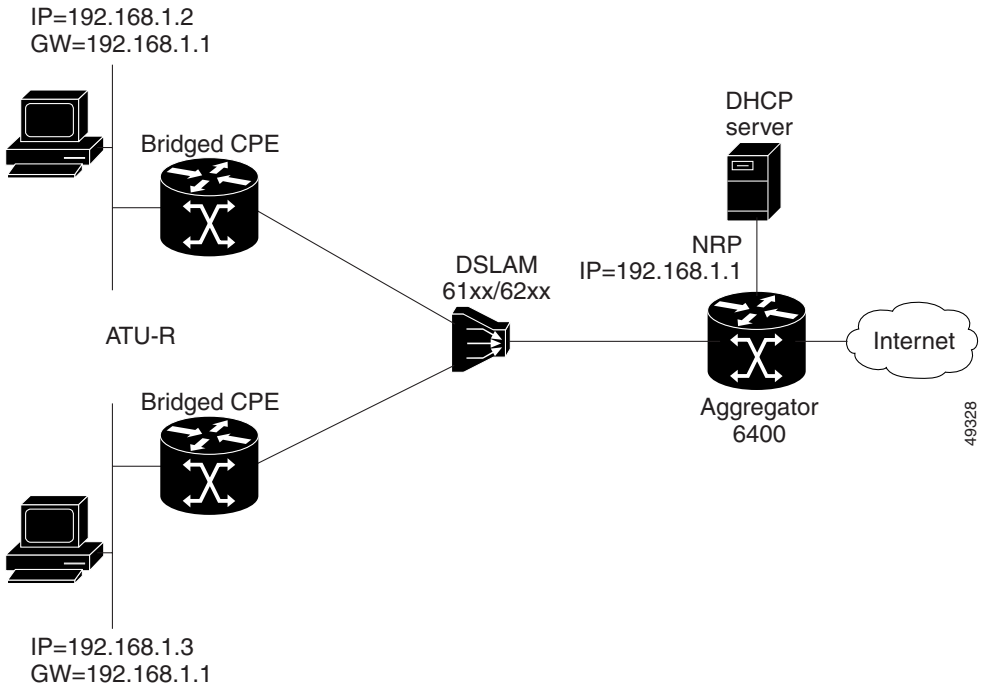
With RBE, when an NRP receives RFC 1483 packets, the packets are not bridged but instead routed based on IP header information. This happens without the need for a bridge virtual interface. For packets coming in from the ISP side to the CPE, the NRP makes routing decision based on the IP destination. If no address resolution protocol (ARP) information is present, the NRP sends out an ARP request to the destination interface.

One of the main advantages of RBE is its ease of migration from IRB. Configuration on the ATU-R is the same.

It also resolves the security issues associated with IRB and RBE does not suffer from the number of bridge group limitation.

Figure 2-3 illustrates a typical RBE network architecture.

Figure 2-3 Route Bridge Encapsulation Architecture Example



Design Considerations

Most of the design/implementation consideration are the same as with the IRB architecture. However security is enhanced and better performance results because each subinterface is treated as a routed port.

With RBE, a single virtual circuit (VC) is assigned a route, a set of routes, or a *cider* block. As a result, the trusted environment is reduced to a single CPE represented by one of these. The NAP/NSP controls the addresses used by the CPE by configuring a IP subnet on the subinterface. This allows the NAP/NSP to control the number of users attached to the ATU-R.

RBE is only supported on point-to-point subinterfaces. The interfaces can be numbered or unnumbered.

In the case of unnumbered interfaces there can be a situation in which multiple subinterfaces use the same numbered interface (such as Ethernet0/0/0 172.10.10.0). In this case all the subscribers behind these subinterfaces will be in the same subnet. In order to create a mapping between the subscriber and the ATM subinterface, you must add static hosts routes. Please see configuration provided in the following NRP Configuration. section

Note New Feature in 12.1(1) DC1: Dynamic Host Configuration Protocol Relay for Unnumbered Interfaces Using ATM RBE

Note Dynamic Host Configuration Protocol (DHCP) Relay now supports unnumbered interfaces using ATM RBE. DHCP Relay automatically adds a static host route specifying the unnumbered interface as the outbound interface.

Note DHCP Relay can also now use the **ip dhcp database** global configuration command. This optional command allows the DHCP Relay to save route information to a TFTP, FTP, or RCP server for recovery after reloads.

NRP Configuration

The following is an example minimum configuration to bring up RBE on the NRP. The only specific command needed is **atm route-bridged ip** interface on the ATM subinterfaces on which the user VCs are configured. In this example, static routes to the user are implemented. These routes are not required with Cisco IOS Release 12.1(1) DC1 or later which include the new feature *Dynamic Host Configuration Protocol Relay for Unnumbered Interfaces Using ATM RBE.*

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
!
interface ATM0/0/0.132 point-to-point
 ip unnumbered Loopback0
 atm route-bridged ip
 pvc 1/32
  encapsulation aal5snap
 !
!
interface ATM0/0/0.133 point-to-point
 ip unnumbered Loopback0
 atm route-bridged ip
 pvc 1/33
  encapsulation aal5snap
 !
!
!
ip route 192.168.1.2 255.255.255.255 ATM0/0/0.132
ip route 192.168.1.3 255.255.255.255 ATM0/0/0.133
!
```

Point-to-Point Protocol over ATM (PPPoA)

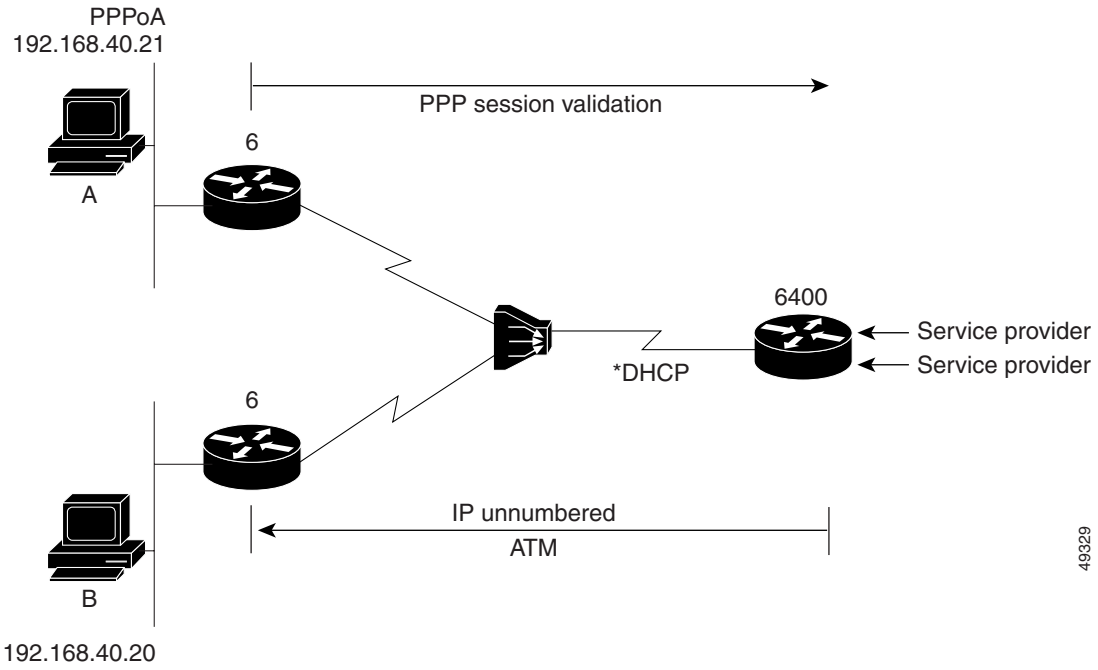
PPPoA was primarily implemented as part of ADSL. It relies on RFC 1483, operating in either LLC/SNAP or VC-Mux mode. The ATU-R encapsulates IP packets into PPP frames and then segments them into ATM cells via AAL5. The PPP link is terminated at the NRP and the originating workstation's IP packet is routed to its final destination through the service provider of choice. The NRP typically uses a *Remote Authentication Dial-in User Service* (RADIUS) server to authenticate and authorize the user, although this can be done within the router. DHCP servers are used to assign the IP address to the user, although this could also be done within the router.

A PPPoA implementation involves configuring the ATU-R with PPP authentication information (login and password). This is the main advantage of this architecture over IRB or RBE implementations, as it provides for per session Authentication, Authorization, and Accounting (AAA).

DHCP with *Network Address Translation* (NAT) can be used at the ATU-R. Implementing DHCP and NAT allows service providers to allocate a single IP address per CPE. This in turn performsNAT or *Protocol Address Translation* (PAT) for the end users. This architecture also offers ease of trouble shooting as the NSP can easily check which subscriber is on/off based on the PPP session.

Figure 2-4 illustrates an example PPPoA network architecture.

Figure 2-4 PPPoA Architecture Example



Design Considerations

Some of the key attributes of this architecture to consider when designing a DSL solution with PPPoA are as follows:

- Security validation per user
- DHCP server capability
- IP address pooling
- Service selection capability

The user login information is configured on the CPE which leads to a single PPP session per VC. Thus the user has access to a single set of services.

Various other implementation aspects that needs to be considered are nature of subscriber (residential or SOHO), services offered by NSP, type of billing, termination point ofPPP,NAT performed at the CPE or the NRP, typical data volume etc.

The number of PPP sessions per NRP is very high which makes PPPoA very scalable.

Following resource restrictions can help in designing the network.

- PPP sessions: 2000 per NRP (or 14000 per Cisco 6400 with 7 NRPs per Cisco 6400)
- Layer 2 Tunneling Protocol (L2TP) tunnels: 300 per NRP

Note These numbers will change with the upcoming releases.

There are various ways to reach a service destination when implementing PPPoA. Examples include:

- L2TP Tunnels
- Terminating PPP sessions at the service provider
- Service Selection Gateway (SSG)

Termination of PPP at the point of aggregation is most common. The NRP authenticates the subscriber using local or RADIUS authentication. The CPE receives the IP address using IP Control Protocol (IPCP). The NRP performs NAT if the IP pool consists of illegal (local) IP addresses.

In L2TP architecture the PPP sessions are not terminated at the aggregation, but rather tunneled to the upstream termination point (SP or corporate net) using L2TP or Layer 2 Forwarding Protocol (L2F). In this model the LAC authentication is based on domain name and the user gets authenticated at the termination end. Thus the user can access one destination at a time and would have to change the domain name on the CPE to change end destinations.

SSG provides *one-to-many* mapping of services as opposed to the *one-to-one* mapping provided in tunneling. With SSG, the subscriber accesses the services using the web-based Service Selection Dashboard (SSD). The user can select one or many services on the fly using the SSD.

In summary PPPoA is becoming the *architecture of choice* because of its scalability, security and SSG support.

NRP Configuration

This PPPoA configurations has four basic tasks:

- ATM PVC (user stream)
- Appropriate atm encapsulation
- Virtual template
- AAA configurations

PPPoA is supported for **aal5mux**, **aal5snap**, **aal5ciscoppp** and **aal5autoppp** encapsulations (**aal5autoppp** is for auto detect PPPoX deployments).

The following is an example minimum configuration to bring up PPPoA on the NRP. The configuration example is for the network shown in Figure 2-4.

```
!
aaa new-model
aaa authentication login default none
aaa authentication ppp default local group radius
aaa authorization network default local group radius none
aaa accounting network default wait-start group radius
!
!
interface ATM0/0/0.1 point-to-point
 pvc 1/31
  encapsulation aal5mux ppp Virtual-Template1
 !
!
interface ATM0/0/0.2 point-to-point
 pvc 1/32
  encapsulation aal5mux ppp Virtual-Template1
!
!
interface Virtual-Template1
 description PPPoATM
 ip unnumbered FastEthernet0/0/0
 peer default ip address pool dsl
 ppp authentication pap
!
ip local pool dsl 192.168.40.20 192.168.40.50
!
!
radius-server host 192.168.2.20 auth-port 1645 acct-port 1646
radius-server key cisco
!
```

Point-to-Point Protocol over Ethernet (PPPoE)

In the PPPoE architecture, an ATU-R acts as an Ethernet-to-WAN bridge and the PPP session is established between the end user's PC and the access concentrator (the NRP). RFC 2516 details the point-to-point session establishment protocol.

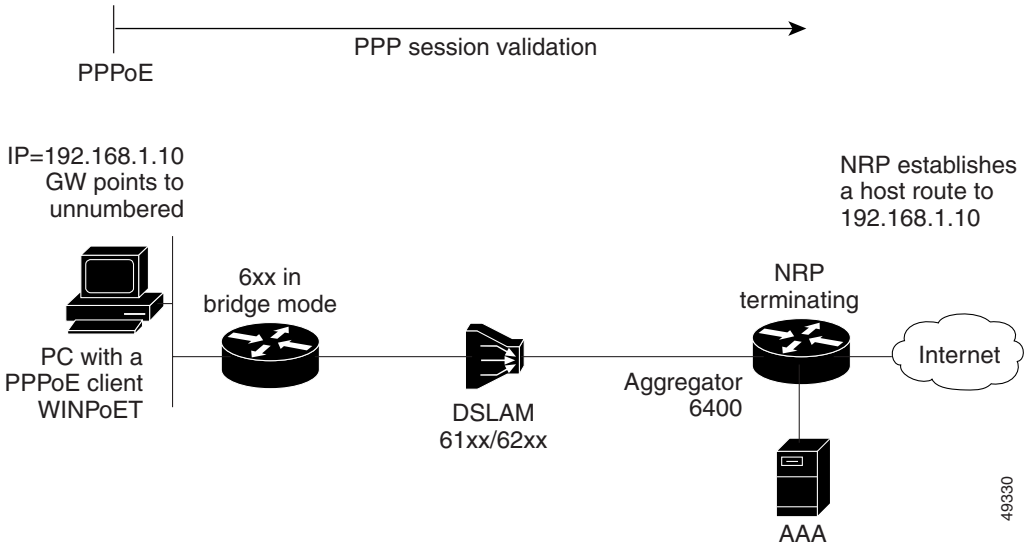
PPPoE requires PPP client software such as Windows PPP over Ethernet Client Software Application (WINPoET) to be installed on each PC on the subscriber side. The client initiates a PPP session by encapsulating PPP frames into a MAC frame and then bridging the frame (overATM/DSL) to the gateway router (NRP). From this point, the PPP sessions can be established, authenticated, addressed, etc. The client receives its IP address using IPCP from the PPP termination point (NRP).

Figure 2-5 illustrates an example PPPoE network architecture.

Note PPPoE is currently only supported with Cisco Express Forwarding (CEF) switching.

Note PPPoE provides all the benefits of PPPoA, for example per session AAA, SSG functionality, security etc.

Figure 2-5 PPPoE Architecture Example



Design Considerations

In general, the design considerations for PPPoA apply to a PPPoE architecture as well. In order to be in compliance with the RFC 2516, IP maximum transmission unit (MTU) must be specified as 1492 in the PPPoE **virtual-template** configuration on the NRP.

In order to control the number of users on the subscriber's side, you can implement the following session limiting global configuration commands:

- **pppoe limit per-mac**— To limit the number of PPP over Ethernet sessions that can originate from a single MAC address.
- **pppoe limit per-vc**—To limit the number of PPPoE sessions that can be established on a VC.

Each of these commands was first introduced with Cisco IOS 12.0(3)DC. For more information, refer to the following feature module:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc3/pppoe.htm

Note Cisco 827 can be used to initiate PPPoE session from the CPE.

NRP Configuration

The following is an example minimum configuration to bring up PPPoE on the NRP. This configuration example is for the network shown inFigure 2-5. PPPoE has all the same configuration tasks as PPPoA, but also includes the configuration of a **vpdn group** with protocol identified as PPPoE. PPPoE is supported for aal5snap and aal5autoppp encapsulations (aal5autoppp is for auto detect PPP over X deployments),

```
aaa new-model
aaa authentication login default none
aaa authentication ppp default local group radius
aaa authorization network default local group radius none
aaa accounting network default wait-start group radius
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface ATM0/0/0.132 point-to-point
 pvc 1/32
  encapsulation aal5snap
  protocol pppoe
 !
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0/0
 no ip route-cache cef
 peer default ip address pool pppoe-pool
 ppp authentication pap
!
ip local pool pppoe-pool 192.168.1.10 192.168.1.50
!
radius-server host 192.168.2.20 auth-port 1645 acct-port 1646
radius-server key cisco
!
```

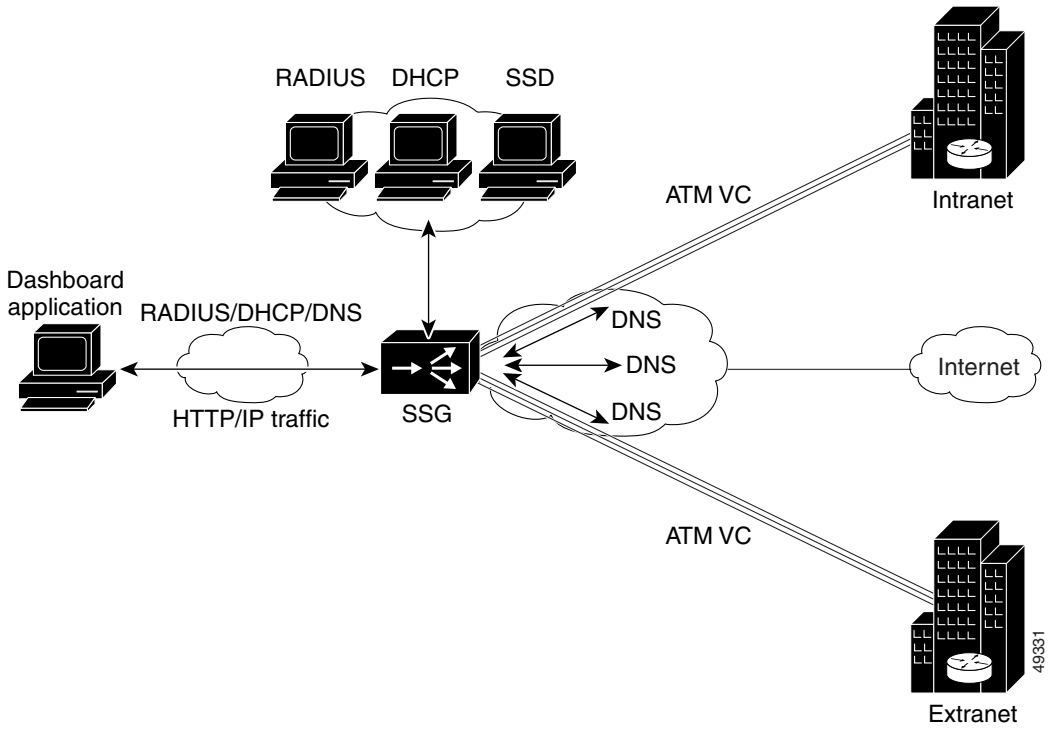
Service Selection Gateway (SSG)

SSG is a Layer 2 and Layer 3 solution for DSL that provides RADIUS authentication and accounting for user interactive policy routing to different IP destinations (services). Using the Service Selection Dashboard (SSD), a user selects from a predetermined list of services for which they are authorized access.

Note The Cisco SSD functionality discussed throughout this document is available only with the NRP-SSG with Web Selection product.

Figure 2-6 illustrates an example SSD-based SSG network environment.

Figure 2-6 Service Selection Gateway



SSD/SSG operates as follows:

1. The user opens an HTML browser and accesses the URL of the Cisco SSD, a web server application. The Cisco SSD forwards user login information to the NRP-SSG, which forwards the information to the AAA server.
2. If the user is not valid, the AAA server sends an Access-Reject message.
3. If the user is valid, the AAA server sends an Access-Accept message with information specific to the user's profile about which services the user is authorized to use. The NRP-SSG logs the user in, creates a host object in memory, and sends the response to the Cisco SSD.
4. Based on the contents of the Access-Accept response, the Cisco SSD presents a dashboard menu of services that the user is authorized to use, and the user selects one or more of the services. The NRP-SSG then creates an appropriate connection for the user and starts RADIUS accounting for the connection.

Note When a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged networking environment, disconnects from a service without logging off, the connection remains open and the user will be able to access the service again without going through the logon procedure. This is because no direct connection (PPP) exists between the subscribers and the NRP-SSG. To prevent non-PPP users from being logged on to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.

Design Considerations

NRP-SSG supports the following capabilities:

- Pass through
- Proxy
- Transparent pass through
- Multicast
- PPP termination aggregation packet forwarding services

Details are available at:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc3/ssgfm.htm#xtocid113302

The next hop gateway attribute is used to specify the next hop key for a service. Each NRP-SSG uses its own next hop gateway table that associates this key with an actual IP address.

Note This attribute overrides the IP routing table for packets destined to a service.

When using a PPPoE client, then the user SSD login name must be same as the PPPoE user login name. A host object with username and password is created when a PPPoE session is terminated at the NRP. The same attributes are used by SSG to log the user into SSD.

If the CPE is configured with PPPoA and PAT, then the user SSD login name must be same as the PPP user login name configured on the CPE. With PAT configured on the CPE, only one user should be using the SSD because with NAT/PAT the NRP/SSG sees only one source IP coming in from the CPE

With a transparent pass through filter configure, as soon as a user logs into the SSD, the user will be cut off from the services configured in the transparent pass through filter. One way to get around this is to configure Auto login services that are same as those supported by the transparent pass through filter.

NRP Configuration

In the following example SSD and RADIUS are running on the same system

```
!
aaa new-model
aaa authentication login default local group radius
aaa authentication login console local
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
enable password cisco
!
ssg enable
ssg default-network 192.168.1.85 255.255.255.255
ssg service-password cisco
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key cisco
!
radius-server host 192.168.1.85 auth-port 1645 acct-port 1646
radius-server timeout 60
radius-server deadtime 2
radius-server key cisco
!
```

SSD Configuration

The following is a sample SSD configuration fragment:

```
AUTHENTICATE_GUEST_TUNNEL=off
AUTHENTICATE_GUEST_PROXY=off
GUEST_USERNAME=guest
REAUTHENTICATE=on
GUEST_PASSWORD=password
GUEST_LOGONS=on

[ADMIN]
LOGIN_NAME=root
PASSWORD*=admin
[MESSAGING_SERVICE]
PORT=9902
DEBUG_MESSAGE_SERVER=1
MAX_MESSAGE_TIME_TO_LIVE=120
MAX_OUTSTANDING_MESSAGES_PER_USER=10
IPADDRESS=192.168.11.10 <<<<< IP address of SSD Server
MAX_OUTSTANDING_MESSAGES=10000

 [AAA_PRIMARY]
PORT=1645
SHAREDSECRET=cisco
SERVICE_GROUP_PASSWORD=cisco
TIMEOUTINSECONDS=10
IPADDRESS=192.168.11.10 <<<<<< IP address of Merit Radius Server
PACKETRETRY=5

[AAA_SECONDARY]
PORT=1645
SHAREDSECRET=cisco
SERVICE_GROUP_PASSWORD=cisco
TIMEOUTINSECONDS=10
IPADDRESS=192.168.11.10 <<<<<< IP address of Merit Radius Server
PACKETRETRY=5

[SSG]
PORT=1645
SHAREDSECRET=cisco
TIMEOUTINSECONDS=10
IPADDRESS=192.168.11.3 <<<<<< IP address of 6400 NRP E0
PACKETRETRY=5
```

RADIUS Configuration

```
###### SSG user profiles

user1   Password = "cisco"
        Service-Type = Framed-User,
  Account-Info = "Nvideo-city",
        Account-Info = "Nnapster-mp3",

###### SSG service profiles

# SSG Video-City Service profile.
video-city Password = "cisco", Service-Type = Outbound
         Service-Info = "IVideo-City",
         Service-Info = "R192.168.5.0;255.255.255.0",
         Service-Info = "MC",
         Service-Info = "TP"


# SSG Napster-MP3 Service profile.
napster-mp3 Password = "cisco", Service-Type = Outbound
         Service-Info = "INapster-MP3",
         Service-Info = "R192.168.6.0;255.255.255.0",
         Service-Info = "MC",
         Service-Info = "TP"
```

Refer to the following document for more configuration details:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120dc/120dc3/ssgfm.htm

Redundancy Design Considerations

Reduced downtime and increased availability are the chief concerns in DSL network design. The network should be designed such that subscribers see the benefits of this “always on” service. Table 2-1 maps potential failure points to the kinds of considerations (if any) to weigh in building redundancy into a DSL network.

Table 2-1 DSL Network Redundancy Considerations

Potential Point of Failure	Redundancy Considerations
Customer Premise Equipment (CPE)	A Cisco 6xx is a CPE router, which is either routing or bridging traffic between the Ethernet and the WAN link. There is not much redundancy support present or needed at the CPE since it provides connectivity to a single subscriber. For SOHO implementations, redundancy can be provided by using two DSL lines.
CPE to Central Office (CO) link	The link between the end stations (such as a home) to CO is assumed to be secure and reliable and is maintained by the Telco.

Table 2-1 DSL Network Redundancy Considerations

Potential Point of Failure	Redundancy Considerations
DSL Access Multiplexer (DSLAM)	Cisco 61xx and Cisco 62xx nodes are key components as they aggregate hundreds (thousand if subtending is used) of subscribers. Chassis/system redundancy is not available at this point. The *backup chassis* approach can be used to achieve minimum downtime and high availability. Refer to the "Chassis Redundancy" section on page 3-7 for implementation details. Some issues to consider when assessing such a solution include the following: **ATU-C Issues** • ATU-C modem card redundancy is needed. • Software support is not available. The document will be updated with the IOS release version when that information is available. **Network Interface Issues** • Physical support for a backup network interface slot is available. • Software support is not available. The document will be updated with the IOS release version when that information is available.
Cisco 6400	Chassis/system redundancy is not available at this point. The *backup chassis* approach can be used to achieve minimum downtime and high availability. Refer to the "Chassis Redundancy" section on page 3-7 for implementation details. Some issues to consider when assessing such a solution include the following.: • **NSP**—See the "Node Switch Processor (NSP)" section on pa ge3-5 for implementation details. • **NRP**—See the "Node Route Processor (NRP)" section on pag e3-5 for implementation details. • **Node Line Card (NLC)**—See the "Node Line Card (NLC)" section on page3-6 for implementation details.

Redundancy Design Constraints

Deployment of a high-availability solutions involves a number of constraints to consider when assessing any redundancy-base implementation. Three key considerations include:

- Human intervention is required for redundant chassis approach as explained in Chassis Redundancy, page 3-7.
- The access path from CPE to the DSLAM (single pair of twisted copper) is not covered in a redundancy solution.
- The NSP path downstream form the aggregation switch is not covered by a redundancy solution.

CHAPTER 3

Redundant Physical Network Considerations

This chapter summarizes hardware options for implementing redundant DSL network environments. The following sections are included:

- Customer Premise Equipment (CPE) Considerations
- DSLAM 61xx/62xx Considerations
- Cisco 6400 Universal Access Concentrator (UAC) Considerations
- Chassis Redundancy
- Example Network Redundancy Solutions

Customer Premise Equipment (CPE) Considerations

Cisco Customer Premise Equipment (CPE) associated with DSL deployments are summarized as follows:

- Cisco 67x series products, including the Cisco 675, Cisco 675e, Cisco 677, the Cisco 678 and Cisco 673, are Ethernet to DSL bridge/routers.
- Cisco 627 is anATM-25 to ADSL modem for single user connections as well as for data service unit (DSU) connectivity to business-class routers,
- Cisco 633 is a serial symmetric DSL (SDSL) data service unit (DSU) for business router connectivity.
- Cisco 827 is an Ethernet to ADSL fixed configuration, Cisco IOS-based router that includes a 10BaseT interface and an ADSL interface. The Cisco 827-4V version includes four analog telephone Foreign Exchange Station (FXS) ports.
- Cisco 1417 is a business class ADSL router that provides firewall and QoS features included with Cisco IOS.

Table 3-1 outlines relevant attributes and briefly describes the application of each of these devices.

Table 3-1 Details of Various Cisco ATU-R Devices

	Modulation	OS	Description
Cisco 627	Discrete Multi-Tone (DMT)-2 and G.Lite	CBOS	ATM-25 to ADSL modem
Cisco 633	2B1Q[1] (encode)	CBOS	SOHO/telecommuter SDSL router (1168 Kbps)
Cisco 673	Cisco 673	CBOS	SOHO/telecommuter SDSL router (1168 Kbps)
Cisco 675	Carrierless Amplitude Phase (CAP)	CBOS	SOHO/telecommuter ADSL router
Cisco 675e	CAP and G.Lite	CBOS	SOHO/telecommuter ADSL router
Cisco 677	DMT-2 and G.Lite	CBOS	SOHO/telecommuter ADSL router
Cisco 678	DMT-2, CAP, and G.Lite	CBOS	SOHO/telecommuter ADSL router
Cisco 827	DMT-2	Cisco IOS	SOHO/telecommuter ADSL router
Cisco 827-4V	DMT-2	Cisco IOS	SOHO/telecommuter ADSL Router (4 analog FXS[2] ports)
Cisco 1417	DMT-2	Cisco IOS	ADSL Router (small/medium businesses and branch offices)

1. 2 Binary 1 Quaternary. An amplitude modulation technique used for ISDN and High bit rate Digital Subscriber Loop (HDSL) service in the United States. This is defined in the 1988 ANSI specification T1.601. 2B1Q has four levels of amplitude (voltage) to encode 2 bits. Each voltage level is called a quaternary. Because of the four voltage levels, each level translates to 2 b/Hz.
2. Foreign Exchange Station interface This interface is an RJ-11 connector that allows connection for basic telephone equipment, keysets, and PBXs. It supplies ring, voltage, and dial tone.

Supported data rates for CPE:

- DMT: 8 Mbps downstream; 0.8 Mbps upstream
- CAP: 7 Mbps downstream; 1.0 Mbps upstream
- G.Lite: 1.5 Mbps downstream; 0.512 Mbps upstream

Reliable twisted-pair lines from the customer premise xDSL router (such as a 6xx) to the central office (CO) are terminated at plain old telephone system (POTS) splitters. No redundancy is available in this path and lines are maintained by the local Telco provider.

For SOHO redundancy can be implemented here by using two DSL lines, using one to backup the other.

DSLAM 61xx/62xx Considerations

The Cisco 61xx/62xx Series products provide end-to-end service, carrying data between a DSL subscriber's home or office, a telephone central office (CO), and various networks. The Cisco 6100 Series with the NI-1 system sends and receives subscriber data over existing copper telephone lines, concentrating all traffic onto a single high-speed trunk for transport to the Internet or a corporate intranet. A Cisco 6130 it can be subtended to seven (12 using NI-2) systems while in 6260 it can be subtended to 12 systems.

Network Interface 1 (NI-1)

Network Interface 1 (NI-1) consists of three modules:

- DS3 Subtend Host Module (STM)
- Network Interface
- System Controller Module

DS3 Subtend Host Module (STM)

The DS3 STM host module manages subscribers that are sent from a subtended Cisco 6100/6130 chassis and installed in slot 9 of a subtending host chassis.

Network Interface

The NI-1 module provides a high-speed connection for aggregated data traffic from the xTU-C modules

System Controller Module

The system controller module is the central processing and control system for the main access Cisco 6100/6130. The system controller module contains all software required to perform the provisioning, monitoring, control, status, management, alarm reporting, etc.

Physical Slots

Table 3-2 summarizes physical system slot allocation for NI-1.

Table 3-2 DSLAM NI-1 Slot Usage

	Primary	Backup
DS3 Subtend Module	9	29
Network Interface Module	10	11
System Controller Module	12	30

Note The secondary slots are not supported at this time.

Network Interface 2 (NI-2)

Network Interface 2 (NI-2) consists of the Network Interface module.

Network Interface

The NI-2 module provides a high-speed connection for aggregated data traffic from the xTU-C modules

Physical Slots

Table 3-3 summarizes physical system slot allocation for NI-1.

Table 3-3 DSLAM NI-2 Slot Usage

	Primary	Backup
Network Interface Module	10	11

Cisco 6400 Universal Access Concentrator (UAC) Considerations

The Cisco 6400 UAC uses an eight-slot, modular chassis supporting half-height and full-height cards, slot redundancy, and dual, fault-tolerant, load-sharing AC or DC power supplies. This section summarizes the functions of the following Cisco 6400 modules:

- Node Switch Processor (NSP)
- Node Route Processor (NRP)
- Node Line Card (NLC)

The central slots (slot 0A and 0B) in the Cisco 6400 are dedicated to redundant, field-replaceable node switch processor (NSP) modules that support both the 5-Gbps shared memory and the fully nonblocking switch fabric.

The NSP also supports the feature card and high performance Reduced Instruction Set (RISC) processor that provides the central intelligence for the device. The NSP supports a wide variety of desktop, backbone, and wide-area interfaces.

The remaining slots support up to eight hot-swappable carrier modules for node router processors (NRPs) or half-height node line cards (NLCs). NRPs and NLCs can be configured for redundant operation. As a result, you can have up to four redundant pairs of NRPs or any combination of NRPs and NLCs. The NRPs are fully functional router modules capable of terminating PPP sessions uploaded from your OC-12, OC-3, or DS3 node line cards.

Table 3-4 summarized slot assignment for Cisco 6400 NSP, NRP, and NLC modules.

Table 3-4 Cisco 6400 Slot Usage

	Slot 1	Slot 2	Slot 3	Slot 4	Slot 0A	Slot 0B	Slot 5	Slot 6	Slot 7	Slot 8
NSP					*	*				
NRP	*	*	*	*			*	*	*	*
NLC	*	*	*	*			*	*	*	*

Details regarding Cisco 6400 software and hardware implementation are available at the following location:

- http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/index.htm

Node Switch Processor (NSP)

The Cisco 6400 node switch processor (NSP) provides ATM switching functionality. The NSP uses permanent virtual circuits (PVCs) or permanent virtual paths (PVPs) to directATM cells between the NRP and ATM interface. The NSP also controls and monitors the Cisco 6400 system, including component NLCs and NRPs.

Redundancy need not be explicitly specified between NSPs using the slot identification, because only NSPs can be installed in slot 0. If two NSPs are installed in the Cisco 6400, they automatically act as a redundant pair. Use the **main-cpu submode** command to specify synchronization between the NSPs.

It is possible to force a switch-over of NSP from the active NSP to the secondary NSP. This may be needed if the current running NSP requires removal.

The synchronization between dual NSP's is enabled automatically by default. Use the **main-cpu submode** command to customize that behavior.

Node Route Processor (NRP)

The NRP receives traffic from NLC interface ports via the NSP ATM switch. The NRP reassembles the ATM cells into packets, processes (routes, bridges, etc.) the packets, segments the packets, and sends them back to the NSP for transmission out of another NLC interface. The Cisco 6400 can contain multiple NRP modules, configured to operate independently or as redundant pairs (1+1).

NRP redundancy is achieved by *redundant slot configuration in the NSP*. The following configuration example illustrates creating a redundant NRP:

```
NSP# config term
NSP(config)# redundancy
NSP(config-r)# associate slot 7 8
```

To ensure that the configuration is consistent between redundant NSPs or NRPs, you can configure automatic synchronization between the two devices. Possible options include: synchronizing just the startup configuration, synchronizing the boot variables, synchronizing the configuration register, or synchronizing all three configurations.

A secondary NSP/NRP is suspended during initialization and monitors primary for failure. Primary and secondary NSPs communicate via shared backplane signals for synchronization. On failure, the secondary resumes its suspended boot sequence and takes over as master.

Node Line Card (NLC)

Node line cards (NLCs) provideATM interfaces for the Cisco 6400 system. There are three types of NLC available for the Cisco 6400, each offering a different interface type (OC-12, OC-3). NLC interfaces are controlled by the NSP.

NLC redundancy can be configured between two half-height line cards in adjacent subslots. When subslot redundancy is configured, all ports on the two subslot cards are redundant. The following configuration example illustrates creating a redundant NLC:

```
NSP# config term
NSP(config)# redundancy
NSP(config-r)# associate subslot 3/0 4/0
```

The Cisco 6400 supports 1+1, linear, unidirectional, non-reverting SONET APS (automatic protection switching) operation on its redundant NLC ports. In this 1+1 architecture, there is one working interface (circuit) and one protect interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use. The line overhead (LOH) bytes (K1 and K2) in the SONET frame indicate both status and action.

The protect interface provides communication between the process controlling the working interface and the process controlling the protect interface. With this protocol, interfaces can be switched to the protection channel because of a signal failure, loss of signal, loss of frame, automatically initiated switchover, or manual intervention. In unidirectional mode, the transmit and receive channels are switched independently.

Note Currently, DS3 line card redundancy is not supported on the chassis. 1+1 linear, non-reverting, unidirectional APS is specific to optical interfaces (OC-3/OC-12 in the Cisco 6400). Cisco's APS is based upon the GR-253-Core Specification.

Power Supply

Cisco 6400 supports dual, fault-tolerant, load-sharing AC or DC power supplies.

Software

The latest Cisco IOS software release supporting the redundancy features for the Cisco 6400 can be found at CCO at the following link:

- http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?majorRel=12.1

Note This web location requires CCO registered user login access.

Table 3-5 summarizes Cisco 6400 software support of redundancy.

Table 3-5 Cisco 6400 Available Images

Router Module	Minimum Software Support Requirement
Cisco 6400 - NRP	12.1.1-DC1
Cisco 6400 - NSP	12.1.1-DB1

Component Limitations and Constraints

Important points that must be considered before implementing redundancy in 6400:

- When configuring redundancy between two NRPs or two NSPs, the two cards must have identical hardware configurations. DRAM size, Flash memory size has to be the same.
- Redundancy can be configured only between adjacent (odd and even) slot or subslot pairs.
- In the Cisco 6400 environment, the lower slot or subslot number is for the working device and the higher slot or subslot is for the protection device.

Chassis Redundancy

A redundant chassis solution is useful in the NAP or NSP where multiple Cisco 6400s are used to aggregate traffic. This approach is useful in the absence of software and hardware supported mechanism that would otherwise provide box level redundancy. The Cisco 6400 uses an eight-slot, modular chassis featuring the option of half-height and full-height card and slot redundancy (NSP, NRP, and NLC redundancy), along with dual, fault-tolerant, load-sharing AC or DC power supplies. The approach described in this section can be used to provide box-level high availability.

The redundant Cisco 6400 should be ready to act as backup for any of the active 6400, in terms of both software and hardware configuration. The backup aggregation switch will have noATM or DS3 links coming to the DSLAMs. As a result, the switch will be functionally ready except there will be no incoming user calls.

In the case of a chassis failure the backup 6400 can be used to handle the calls of the failed chassis until it recovers. Human intervention is required to move the ATM or DS3 link from the failed chassis to the backup 6400. The Fast Ethernet orATM uplinks to the ISP/Internet must also be moved.

This method can be used to provide physical backup for the 6400s.

Considerations

Choosing to deploy a redundant chassis implementation requires planning and resource commitment. Before committing to a redundant chassis solution, be sure to assess factors that might influence the success and supportability of your solutions. Examples of assessment criterion include the following considerations:

- **Real estate for the extra Cisco 6400—**Does your wiring closet have sufficient ventilation for additional Cisco 6400 systems? Can you physically fit additional chassis into your system racks? Do you have sufficient power to support additional Cisco 6400 requirements?

- **Cost of the extra Cisco 6400**—Is the trade-off between downtime and backup hardware worth the capital outlay? Are there mission critical applications running over this connection? Will users accept the downtime associated with failures when no backup exists?
- **Human Intervention Requirement**—Is there a sufficiently knowledgeable staff on hand to handle changes mandated by a redundant chassis swap? Will additional contractors be required to handle remote location swaps?

Advantages

Two important advantages can be attributed to a redundant chassis solutions:

- **Reduced Maintenance Downtime**—The redundant 6400 can be used to reduce downtime to few minutes in case of 6400 software upgrades. Usually the scheduled downtime needed to upgrade a complex system like 6400 can go from half an hour to few hours. Using the backup system approach reduces the downtime to few minutes.
- **Extended Time for Troubleshooting**—In the event of a system problem (crash, memory leak, et.c) the backup Cisco 6400 can be used to handle user calls while support staff (TAC/NSA, Consultant/developer) works to reinstate the failed system and to recover information needed to isolate and diagnose the problem.

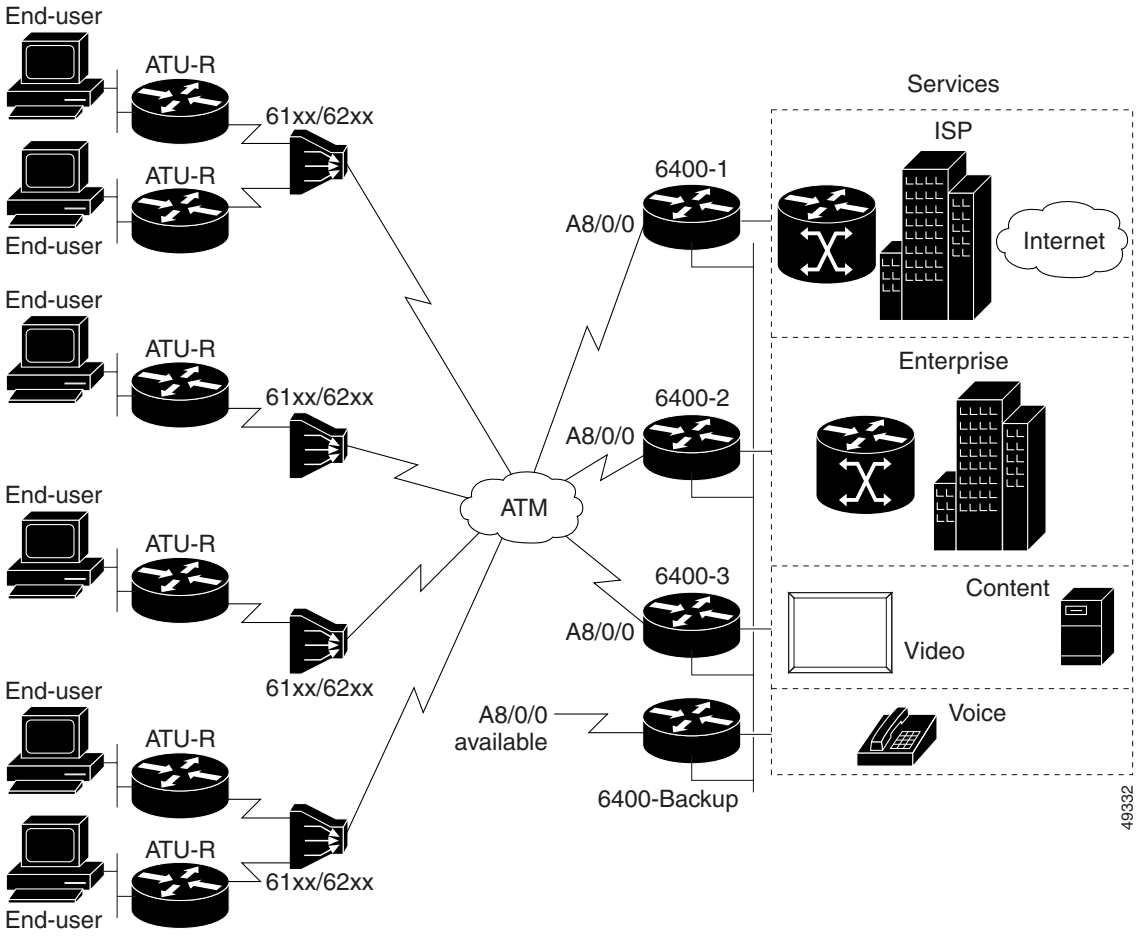
Note In the absence of a backup system the failed 6400 would have been immediately rebooted to establish network connectivity.

Example Network Redundancy Solutions

Figure 3-1 illustrates an example redundant chassis network topology. Optional design solutions are summarized in the sections that follow this illustration:

- Design I: Redundant Chassis Solution
- Design II: Software Configuration Redundancy Solution

Figure 3-1 DSL Network with Redundant Chassis Implementation



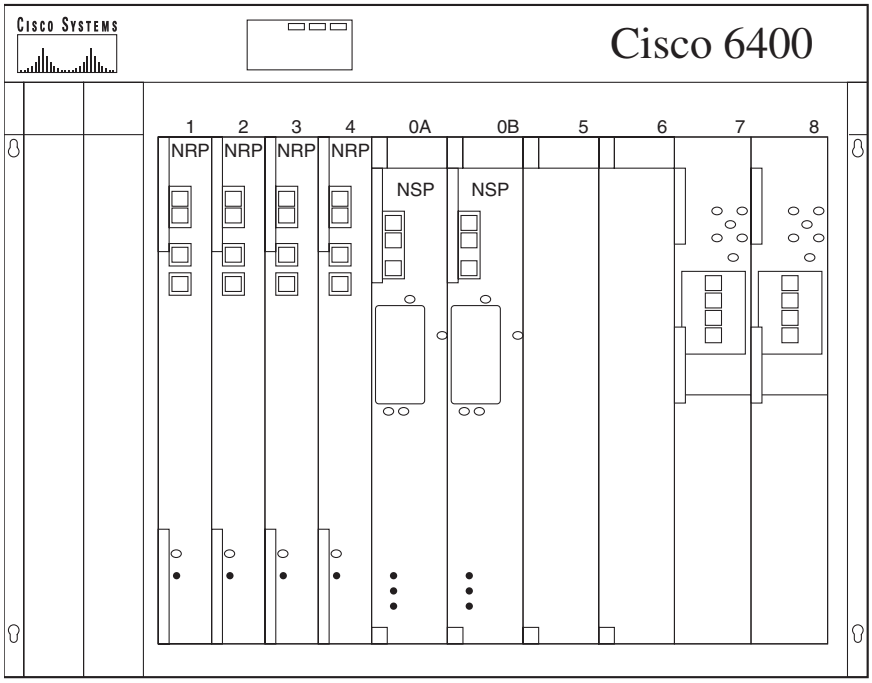
Design I: Redundant Chassis Solution

Given the network topology as illustrated in Figure 3-1, this discussion of a redundant chassis approach focuses on how the chassis redundancy can be used to backup a Cisco 6400. The Cisco 6400 currently handles up to 14,000 simultaneous user calls. The approach can be applied to achieve higher availability for the DSLAM (61xx/62xx).

NRP/NSP/NLC Redundancy Notes

Before the redundant chassis is considered make sure the NRP and NSP within the box are redundant and configured for fail-over. Figure 3-2 illustrates a sample hardware configuration for a Cisco 6400 utilizing NRP/NSP/NLC redundancy features.

Figure 3-2 Example of 6400 with fully redundant NSP, NRP and NLC



To further define the approach adopted for Design I supporting the network illustrated in Figur e3-1, consider the following slot pairings (active/backup) for the Cisco 6400 listed as 6400-1:

- NRP slot 1 and NRP slot 2 are associated; NRP slot 2 is the backup
- NRP slot 3 and NRP slot 4 are associated; NRP slot 4 is the backup
- NSP slot 0B is the backup for NSP slot 0A.

The associated NRPs and NSPs have the same hardware and software configurations including the same size flash and DRAM. Configurations between the two adjacent components will *auto-sync* unless explicitly specified by the **no auto-sync** command. Subslot redundancy association is between subslot 7/0 and subslot 8/0.

One can accomplish the associations suggested here with the following configurations on the NSP:

```
!
redundancy
  main-cpu
    auto-sync standard
!
redundancy
  associate slot 1 2
redundancy
  associate slot 3 4
redundancy
  associate subslot 7/0 8/0
!
```

The other Cisco 6400s in Figure 3-1 (6400-2 and 6400-3) are similarly configured such that NSP, NRP, and NLC are supported with redundant backups.

Design I Backup Chassis Setup Considerations

In the example illustrated in Figure 3-1, The redundant chassis can provide a backup solution for all the three Cisco 6400s (6400-1, 6400-2, and 6400-3). As a result, the backup Cisco 6400 system must have the physical configurations associated with each of the operational Cisco 6400s. Table 3-6 how the configuration mapping should be done.

Table 3-6 Redundancy Design I Configuration Management Chart

Calls (VPI/VCI)[1]	Active Module	Backup Module (6400-Backup)
1/10 – 1/1010	6400-1 NRP-SLOT-1	NRP-SLOT-1
2/10 – 2/1010	6400-1 NRP-SLOT-3	NRP-SLOT-2
1/10 – 1/1010	6400-1 NSP-SLOT-0A	NSP-SLOT-0A
2/10 – 2/1010	1/10 – 1/1010 outgoing interface ATM1/0/0	1/10 – 1/1010 outgoing interface ATM1/0/0
	2/10 – 2/1010 outgoing interface ATM3/0/0	2/10 – 2/1010 outgoing interface ATM2/0/0
3/10 – 3/1010	6400-2 NRP-SLOT-1	NRP-SLOT-3
4/10 – 4/1010	6400-2 NRP-SLOT-3	NRP-SLOT-4
3/10 – 3/1010	6400-2 NSP-SLOT-0A	NSP-SLOT-0A
4/10 – 4/1010	3/10 – 3/1010 outgoing interface ATM1/0/0	3/10 – 3/1010 outgoing interface ATM3/0/0
	4/10 – 4/1010 outgoing interface ATM3/0/0	4/10 – 4/1010 outgoing interface ATM4/0/0
5/10 – 5/1010	6400-3 NRP-SLOT-1	NRP-SLOT-5
6/10 – 6/1010	6400-3 NRP-SLOT-3	NRP-SLOT-6
5/10 – 5/1010	6400-3 NSP-SLOT-0A	NSP-SLOT-0A
6/10 – 6/1010	5/10 – 5/1010 outgoing interface ATM1/0/0	5/10 – 5/1010 outgoing interface ATM5/0/0
	6/10 – 6/1010 outgoing interface ATM3/0/0	6/10 – 6/1010 outgoing interface ATM6/0/0

1. The virtual path identifiers/virtual channel identifiers (VPIs/VCIs) used are unique across all three 6400s (6400-1, 6400-2, 6400-3).

As illustrated in Figure 3-1, the incoming interface (the link from the DSLAM) is A8/0/0 in each of the Cisco 6400s. Each of the Cisco 6400s, including the backup system, has a link to the local management LAN. The local management LAN includes the AAA server, SSG Server and the DHCP Server (if DHCP services on the NRP are not used).

Because each system has a link to the ISPs/Internet, the backup system will have the current routing/forwarding tables.

Design I Backup Cisco IOS Configurations

In this design, no changes are required in the NRP configurations. For example, the Cisco IOS configuration from 6400-1 NRP-SLOT-3 is copied to 6400-Backup NRP-SLOT-2.

However, the NSP in the Cisco 6400-Backup system must be configured so that it combines the configurations of the NSPs of each active Cisco 6400.

The following NSP configurations on the active Cisco 6400s and the backup Cisco 6400 illustrate how this redundant chassis design is implemented:

1. Relevant Cisco IOS configuration fragment for 6400-1 NSP-0A:

```
interface ATM8/0/0
 no ip address
 atm pvp 1 interface ATM1/0/0 1
 atm pvp 2 interface ATM3/0/0 2
!
```

2. Relevant Cisco IOS configuration fragment for 6400-2 NSP-0A:

```
interface ATM8/0/0
 no ip address
 atm pvp 3 interface ATM1/0/0 3
 atm pvp 4 interface ATM3/0/0 4
!
```

3. Relevant Cisco IOS configuration fragment for 6400-3 NSP-0A:

```
interface ATM8/0/0
 no ip address
 atm pvp 5 interface ATM1/0/0 5
 atm pvp 6 interface ATM3/0/0 6
!
```

4. Relevant Cisco IOS configuration fragment for 6400-Backup NSP-0A:

```
interface ATM8/0/0
 no ip address
 atm pvp 1 interface ATM1/0/0 1
 atm pvp 2 interface ATM2/0/0 2
!
interface ATM8/0/1
 no ip address
 atm pvp 3 interface ATM3/0/0 3
 atm pvp 4 interface ATM4/0/0 4
!
interface ATM8/1/0
 no ip address
 atm pvp 5 interface ATM5/0/0 5
 atm pvp 6 interface ATM6/0/0 6
!
```

Failure Example Notes

Having the setup complete as discussed in “Design I Backup Chassis Setup Considerations”, assume a failure occurs. The following notes summarize actions and considerations associated with recovering from a failure of one of the active Cisco 6400 UACs in the example network presented in Figure3-1:

- If, for example, 6400-1 fails (not a module failure, as that is redundant, but a chassis failure), then the link from ATM 8/0/0 of 6400-1 needs to be moved to ATM 8/0/0 of 6400-Backup and the user traffic will be reinstated.

- This approach is not only applicable for a chassis failure, it can be used to decrease scheduled maintenance downtime. The backup chassis is available to take the place of any of the active Cisco 6400s incase one of them needs to be taken out of service.
- The configuration on the NSP (on 6400-Backup) can be modified so that ATM 8/0/1 is used and it can act as active backup for multiple chassis.

Design II: Software Configuration Redundancy Solution

Keeping the same logical topology as illustrated in Figure 3-1, a second possible design approach is to have the software configurations of the active chassis stored in the backup Cisco 6400.

This is useful when all the active chassis are fully loaded without NRP redundancy.

The running configurations from the active Cisco 6400s must be copied to the backup system and saved in flash as defined in Table 3-7.

In this way the backup system can be used to replace any of the active 6400 by just switching to that system's configurations.

Table 3-7 Redundancy Design II Configuration Management Chart

Backup Module (6400-Backup)
NRP-SLOT-1
6400-1-NRP-SLOT-1.CFG
6400-2-NRP-SLOT-1.CFG
6400-3-NRP-SLOT-1.CFG
NRP-SLOT-2
6400-1-NRP-SLOT-2.CFG
6400-2-NRP-SLOT-2.CFG
6400-3-NRP-SLOT-2.CFG
NRP-SLOT-3
6400-1-NRP-SLOT-3.CFG
6400-2-NRP-SLOT-3.CFG
6400-3-NRP-SLOT-3.CFG
NRP-SLOT-4
6400-1-NRP-SLOT-4.CFG
6400-2-NRP-SLOT-4.CFG
6400-3-NRP-SLOT-4.CFG
NRP-SLOT-5
6400-1-NRP-SLOT-5.CFG
6400-2-NRP-SLOT-5.CFG
6400-3-NRP-SLOT-5.CFG

Table 3-7 Redundancy Design II Configuration Management Chart

Backup Module (6400-Backup)
NRP-SLOT-6
6400-1-NRP-SLOT-6.CFG
6400-2-NRP-SLOT-6.CFG
6400-3-NRP-SLOT-6.CFG
NRP-SLOT-7
6400-1-NRP-SLOT-7.CFG
6400-2-NRP-SLOT-7.CFG
6400-3-NRP-SLOT-7.CFG
NSP-SLOT-0A
6400-1-NSP-SLOT-0A.CFG
6400-2-NSP-SLOT-0A.CFG
6400-3-NSP-SLOT-0A.CFG

Design I and Design II Comparison

While these two design approaches both provide redundancy solutions for the hypothetical network arrangement illustrated in Figure 3-1, each makes certain assumptions about the active UACs. These assumptions influence the way the redundancy solutions are implemented.

Design I assumes that half the NRP, NSP, and NLC slots (as illustrated in Figure 3-2) of each active Cisco 6400 systems are used as backup slots. As a result, each active Cisco 6400 includes four NRPs, two NSPs, and two NLCs.

In contrast, Design II assumes that all the NRP slots in each of the active Cisco 6400s is operational with two redundant NSPs and NLCs. The only NRP backup modules in Design II reside in the backup Cisco 6400 system (6400-Backup).

In both designs, the redundant chassis (6400-Backup) includes six NRPs, oneNSP, and one NLC.

In Design I, each active module is backed up by two specific modules:

- One module on the same active Cisco 6400
- One module on the backup Cisco 6400

In Design II, the backup environment differs, as follows:

- No backup NRP modules on the active Cisco 6400s
- One backup module supports three active modules (one from each active Cisco 6400)

From an operational perspective, the chief result is that Design I provides a higher level of inherent redundancy, while Design II provides for more total concurrent access connections.

Note Assuming two additional incoming ATM lines are added to the backup Cisco 6400 in Figure 3-1, Design I can be made to accommodate up to three concurrent Cisco 6400 UAC failures. Design II can only accommodate one complete UAC failure at a time.