Revitalizing Centrex Services Application Note

Expanding the Opportunities for Centrex Services

Converge voice and data traffic onto a single Centrex system.
Continue existing services while providing a cost-effective, unified architecture to support higher value IP Centrex services.

This application note addresses how to build an IP Centrex service offering that:

- Maximizes the opportunity for Centrex services
- Helps protect existing Centrex revenue by allowing you to gradually migrate to an IP Centrex solution
- Scales Centrex services by supporting multiple customers on each physical IP router
- Enables you to deliver VoIP solutions to customers with overlapping private IP addresses
- Enables your customer to easily access Centrex services without sacrificing security
- Minimizes your operations costs by integrating with your existing OSS system
- Provides the carrier-class reliability required for converged services

Lucent Technologies
Bell Labs Innovations



Table of Contents

1. Introduction 3

2. Maximizing the service opportunity for Centrex solutions 3

Migrating Centrex services to IP 4

Eliminating the geography barrier 4

Providing a consistent set of features to a global set of sites 4

Accelerating service provisioning 5

Providing flexible telephony services to traveling employees 5

3. Deploying the right equipment for the right service 5

Understanding the Lucent IP Centrex solution 6

Staging the migration to IP Centrex to protect existing Centrex revenue 7

Supporting multiple customer circuits on each physical IP router 7

Support overlapping private IP addressing of customer CPE devices 8

Simplifying access to the service while helping to ensure security 9

Integrating with existing OSS systems 9

Providing carrier-class reliability 10

High availability 10

Fast service restoration 10

4. Conclusion 12

1. Introduction

Conceived decades ago by AT&T, Centrex services have been a popular solution to the voice network demands of many corporations. To offer Centrex services, carriers portion off Class 5 switch resources in their Central Office (CO), making them available to their enterprise customers.

During the current telecom downturn, enterprises have been reluctant to invest in PBXs and other equipment. Centrex services can turn this reluctance to the service providers' advantage. Hosted Centrex services enable enterprises to take advantage of state of the art telephony without purchasing and maintaining costly voice network equipment—making them an attractive alternative to PBXs for cost-conscious enterprises.

Today, about 15% of the total US corporate market uses Centrex services—consuming an estimated 18 million lines nationwide. This adoption rate has remained relatively stable over the past several years. However, because enterprises are reluctant to make new capital investments to upgrade their aging telecommunications equipment, hosted Centrex services offer service providers an opportunity to increase revenues and capture market share in a down economy.

This application note examines the factors that have limited the acceptance of traditional Centrex services in the past and describes how migrating to an IP-based Centrex service model can help service providers overcome these concerns, increase market share and create new revenue opportunities from their legacy Class 5 switches.

2. Maximizing the service opportunity for Centrex solutions

In the past, the service opportunity for traditional TDM-based Centrex services has been limited to the geographic region served by the individual Class 5 switch. Although service providers can offer Centrex services to corporations with offices in multiple areas, the precise feature set offered to each customer site depends on the capabilities of the legacy Class 5 switch serving each region. This makes it difficult for service providers to deploy a consistent feature set to businesses that have multiple offices in different geographical locations.

In addition, because TDM-based Centrex services require a dedicated line on each side of the connection, traditional Centrex services are slow to provision and expensive to maintain. Establishing the service requires the provider to send a technician to the customer site to create the physical connections. Accommodating move, add, and change orders requires additional truck rolls to update the physical network configuration at the customer site. TDM-based Centrex also requires a significant footprint at the customer location to house the cross-connect equipment linking these dedicated lines.

Even with these service limitations, traditional Centrex services have proven to be a successful revenue generator for service providers and a dependable service for enterprises. Service providers who can deploy a Centrex service and be free of concerns about geography, feature inconsistency, or difficult service provisioning have a unique opportunity to generate new revenues and take market share using their legacy Class 5 switches.

Migrating Centrex services to IP

Increasingly, service providers are using IP Centrex to address these challenges. As with traditional Centrex services, IP Centrex gives customers access to a rich set of scalable voice services without the burden of purchasing and housing equipment or developing and maintaining a network with internal, specialized staff. IP Centrex, however, offers a number of advantages for service providers and their enterprise customers that traditional Centrex services cannot match.

Eliminating the geography barrier

With IP Centrex, customer sites are linked through a managed IP network to the Class 5 switch hosting the Centrex services. Because customers connect to their host switch through the managed IP network, a single Class 5 switch in the CO can provide Centrex features to multiple customer sites—regardless of their geographic location.

For service providers, this network architecture means that they are no longer restricted to offering Centrex services to the area served by a particular Class 5 switch. By breaking the geographic restrictions traditionally associated with Centrex services, service providers can extend their market reach and offer a converged voice and data solution to corporations with geographically dispersed offices and workers.

Breaking the regional restrictions also gives service providers the flexibility to manage available Class 5 switch resources more efficiently throughout their network. Because the Class 5 switch hosting the service no longer needs to be physically located in the same region as the customers accessing the service, providers can allocate Class 5 switch resources from any portion of their network to any customer worldwide who needs them. Service providers can use this flexibility either to support all branch offices and mobile workers associated with a particular enterprise from a single Class 5 switch or to supplement Class 5 switch resources in areas with high Centrex service demand with IP Centrex services hosted by a switch in another region.

Enterprises can use hosted IP Centrex services to merge their offices into a global network. This type of seamless integration is simply not possible with PBX or traditional Centrex solutions.

Providing a consistent set of features to a global set of sites

Enterprises can use IP Centrex to extend four-digit dialing and other PBX-like services to all offices and mobile workers associated with a particular enterprise. By merging their corporate facilities into a seamless global network, enterprises can dramatically reduce their long-distance charges for in-house communications, improve in-house efficiency, and use data collection and collaboration applications more effectively. This type of seamless, global integration is simply not possible with IP PBX or traditional Centrex solutions.

Accelerating service provisioning

IP Centrex services are also relatively quick to provision and easy to maintain over time. Enterprises require only IP phones or IP gateway devices to use IP Centrex services. These IP devices connect to the current enterprise LAN and can be routed to the service provider using any standard WAN router—greatly reducing the equipment investments for the enterprise. For the service provider, the limited wiring required to support the service at the customer site results in fewer truck rolls to establish and maintain the service.

With IP Centrex, enterprises can extend advanced voice and data services to every user's desktop through a single Ethernet port shared by the IP phone and the computer. IP Centrex solutions that use Dynamic Host Configuration Protocol (DHCP) to obtain a LAN IP address for individual users significantly reduce move, add, and change (MAC) costs associated with the Centrex services. This approach also means that tradesmen no longer need to continually update and re-map a physical cabled network at the customer site to maintain the service—helping to reduce operations costs for the service provider, while making it easier and more affordable for the enterprise to provide a full Centrex feature set to an ever-changing and increasingly mobile workforce.

Providing flexible telephony services to traveling employees

Enterprises can also use IP Centrex to provide large-office phone features to employees traveling on business. With an IP Centrex solution, employees can access corporate office phone features, including four-digit dialing, caller ID, voice mail, teleconferencing, call transfer and call forwarding, from anywhere in the world using their laptop computer and a soft phone. This virtual office approach increases efficiency by enabling employees to reach customers, co-workers, and other contacts from the road just as if they were in the office. At the same time, the IP Centrex solution helps to reduce communications costs for the enterprise by replacing long distance 800 circuits with low-cost local circuits.

3. Deploying the right equipment for the right service

To provide profitable IP Centrex services, service providers need a solution that can:

- Provide a staged migration to IP Centrex to protect existing Centrex revenue
- Support multiple customer circuits on each physical IP router to improve scalability
- Support overlapping private IP addressing of customer premises equipment (CPE)
- Make the service as simple as possible for the customer to access—without sacrificing security
- Easily integrate with the provider's OSS systems
- Provide the reliability of the PSTN

The remainder of this section describes the Lucent IP Centrex solution and how it delivers each key requirement for profitable IP Centrex services delivery.

Understanding the Lucent IP Centrex solution

Lucent Technologies provides a robust IP Centrex solution designed to work with the service provider's existing infrastructure. To support IP Centrex services, Lucent provides the iMerge™ Centrex Feature Gateway (CFG), which acts as the gateway between the circuit and packet networks, and the SpringTide® 7000 IP Service Switch Router, which provides edge routing.

Deployed as an access device at the edge of the circuit-switched network, the iMerge™ CFG uses the Telcordia standard GR-303 interface to provide all of the services of a Class 5 central office switch over an IP network. On the ingress side, the iMerge™ CFG interoperates with multiple Class 5 switches, including the Lucent 5ESS® switch, the Nortel DMS, and the AGCS GTD-5®. Because the iMerge™ CFG interoperates with multiple Class 5 switches from multiple vendors in multiple COs, service providers can easily create IP Centrex solutions capable of providing seamless communications to enterprises with geographically dispersed offices and mobile workers—without sacrificing their existing investments in legacy Class 5 switches. Because the iMerge™ CFG open architecture works with CPE from multiple vendors, most enterprise customers can use the equipment already on site to connect to the IP Centrex service.

The Lucent IP Centrex solution interoperates with multiple Class 5 switches in multiple COs, enabling service providers to easily create integrated IP Centrex solutions to link geographically dispersed offices and mobile workers—without sacrificing investments in legacy Class 5 switches.

The Lucent IP Centrex solution uses the SpringTide® 7000 IP Service Switch Router's high-density WAN aggregation capabilities to route traffic between different subnets in customer enterprise LAN IP networks and the iMerge™ CFG. Service providers can use the SpringTide® 7000 switch router to dynamically deliver IP services to their customers, regardless of their customer's location or access method. The SpringTide® 7000 switch router terminates enterprise WAN access at the provider CO on individual, customer-specific virtual routers—using H.323v2-aware network address translation (NAT) to map each CPE endpoint to a unique IP address.

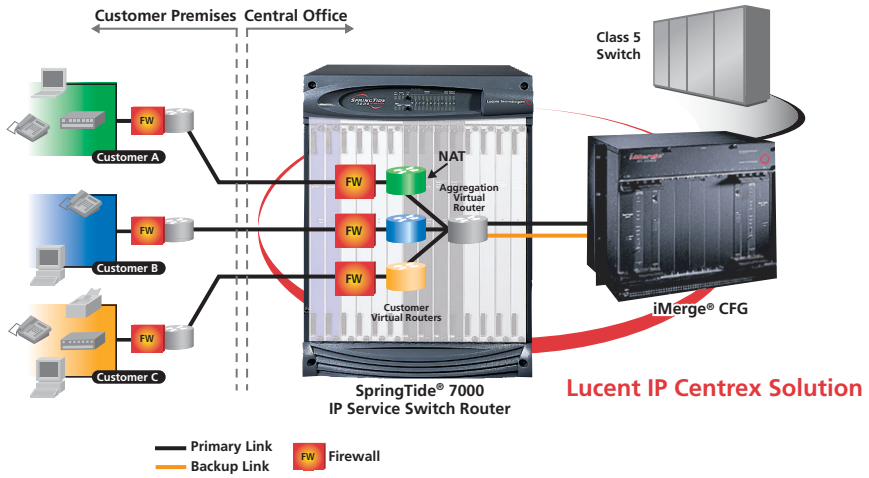

Figure 1—Lucent IP Centrex Solution

Staging the migration to IP Centrex to protect existing Centrex revenue

With the Lucent solution, providers can use the same Class 5 switch to offer both traditional Centrex and IP Centrex services in the same network. This flexibility enables service providers to protect existing Centrex revenues while deploying new IP Centrex services. For example, service providers may choose to leave the traditional Centrex services used by existing customers unchanged, but deploy IP Centrex to all new customers and new customer sites.

By gradually migrating its customers to IP Centrex, service providers can minimize the risks and downtime associated with service changes. This enables service providers to protect valuable revenue while increasing their revenue potential with IP Centrex services that offer greater flexibility and use current network resources more efficiently. This gradual migration is not possible with IP PBX solutions.

Supporting multiple customer circuits on each physical IP router

In IP Centrex solutions built with ordinary IP routers, service providers must dedicate a unique physical router to each customer as shown below.

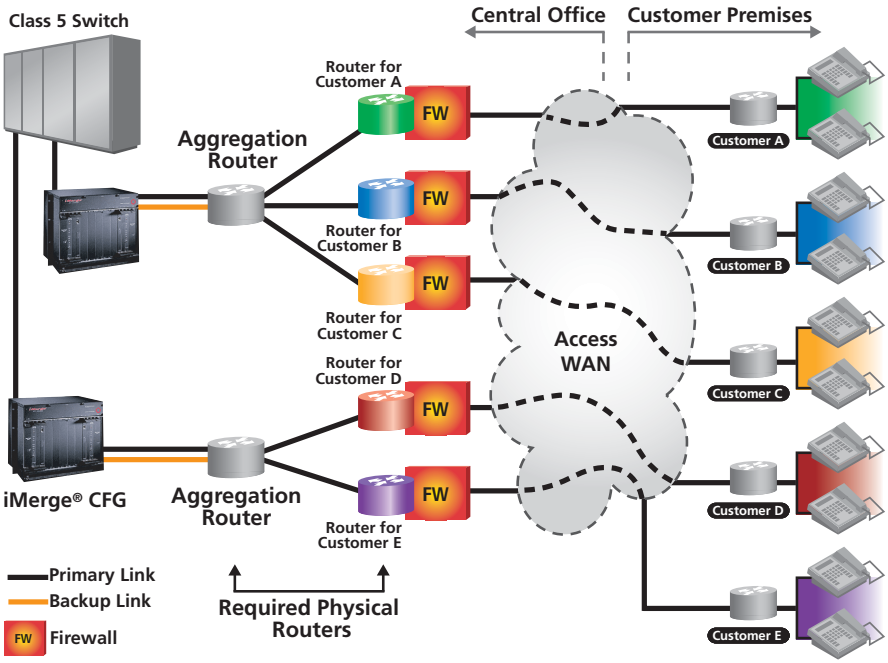

Figure 2—Service providers implementing IP Centrex with the typical IP router must dedicate a separate physical router to each customer. One or more aggregation routers may also be required to interface with the CFG.

The SpringTide® 7000 IP Service Switch Router architecture consists of a collection of virtual routers within a single chassis, enabling the true layer 3 routed network design required to support IP Centrex. Each virtual router acts just like a physical router, with distinct routing tables, dedicated IP interfaces, and network management software. By logically dividing each physical device into multiple virtual routers, each SpringTide® 7000 switch router can support multiple, secure customer circuits—greatly improving the scalability of the IP Centrex service. (See Figure 3.)

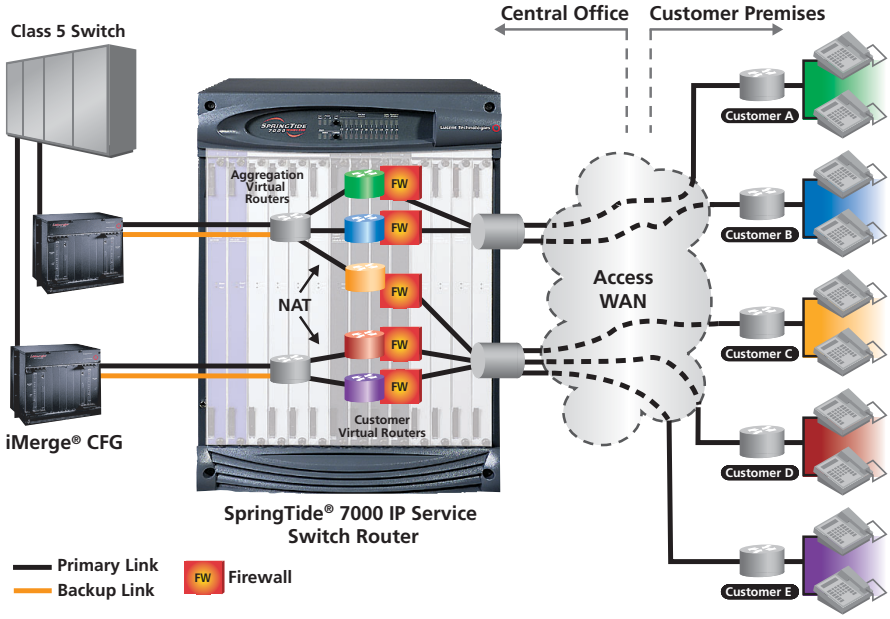

Figure 3—The SpringTide® 7000 IP Service Switch Router uses virtual routers to support multiple customers on each physical device.

By logically dividing each physical device into multiple virtual routers, each SpringTide® 7000 switch router can support multiple, secure customer circuits—greatly improving the scalability of the IP Centrex service.

The virtual router architecture eliminates the need for dedicating a physical router in the CO to each enterprise customer. Instead, service providers can use a single physical device to support multiple customers. This translates to a lower CO footprint and potentially significant cost savings in reduced rack space and power requirements. It also allows providers to easily move customers from one iMerge™ CFG to another by simply reconfiguring the cross-connects between the customer's virtual router and the appropriate aggregation virtual router. In a physical router implementation, service providers would be forced to re-wire the network to complete the migration.

In addition, because the Lucent SpringTide® 7000 IP Service Switch Router provides integrated virtual firewall functionality, service providers do not need to deploy multiple firewall appliances to secure the IP Centrex services provided by each virtual router.

Support overlapping private IP addressing of customer CPE devices

As with any IP telephony application, the iMerge™ CFG requires each IP phone to be mapped to a unique IP address. Since most enterprises use private IP addressing, service providers typically use NAT devices to map the customer addresses to globally unique addresses. NAT devices check the IP header information of packets as they enter or exit an interface. If the source address (egress NAT) or the destination address (ingress NAT) match the configured NAT address range, that address is translated and updated in the header before the packet is sent on. This approach does not work for VoIP, because the IP source and destination addresses for VoIP traffic are embedded in the payload.

To properly translate IP packets containing H.323v2 information in the payload, the SpringTide® 7000 IP Service Switch Router has implemented an H.323v2-aware application layer gateway. The gateway monitors packets in real-time to determine whether the packets are carrying H.323v2 or related protocol messages. If so, the gateway determines the IP addresses involved and translates the header and the payload information. This approach enables customers to use overlapping IP addresses in their private networks without impacting VoIP service delivery in the service provider network.

Simplifying access to the service while helping to ensure security

In the Lucent IP Centrex solution, the SpringTide® 7000 IP Service Switch Router terminates enterprise WAN circuits on a dedicated virtual router. Customers can access the service using any of a variety of WAN access technologies, including ATM PVCs, DS1s, multi-link PPP (MLPPP) trunks, and Gigabit Ethernet VLANs. Because the SpringTide® 7000 IP switch router terminates each circuit on a virtual router dedicated to the customer, carriers can use the same device to deliver services to multiple customers with overlapping IP addresses.

Because the SpringTide® 7000 IP switch router terminates each customer's network connection on a dedicated virtual router, carriers can use one physical device to securely deliver services to multiple customers with overlapping IP addresses.

The SpringTide® 7000 IP Service Switch Router terminates the network connection for each customer on a different virtual router—protecting services against denial of service attacks and from crossover network traffic. Because each virtual router has its own dedicated resources, a denial of service attack on the CO router only affects the customer serviced by that particular virtual router. Service providers using traditional IP routers would have to dedicate an entire physical router to each customer to provide a similar level of protection.

Because every customer uses a different virtual router with a unique set of dedicated resources, including a dedicated virtual firewall, traffic from one customer network cannot cross into another customer network. The SpringTide® 7000 IP Service Switch Router also provides granular separation of configuration privileges to eliminate the potential for any virtual router to gain control of the entire physical device.

Integrating with existing OSS systems

Today's large telephony providers' equipment is provisioned, monitored, and maintained using Telcordia OSS systems. To avoid increasing costs for service providers through inefficient business practices and maintenance procedures, new equipment installations must also comply with these stringent standards.

The Operations Systems Modification of Intelligent Network Elements (OSMINE) process uses the systematic Telcordia method of analyzing, monitoring, and modifying Telcordia software to support system interoperation in a multi-vendor environment. The industry-recognized method for attaining interoperability of network elements and OSSs, OSMINE maximizes the value of network products, ensuring integration with embedded OSSs while meeting flow-through requirements—enhancing network value and minimizing manual intervention.

Because providers cannot easily change their business practices as they evolve their telephony networks, all SpringTide® 7000 IP Service Switch Router components fully comply with TIRKS Stage 2 System Release 19.6, NMA System Release 11.1. The Lucent iMerge™ CFG also uses the existing stable and secure Class 5 infrastructure for billing, OAM&P, signaling (SS7), trunk interface, and CALEA-compliance—enabling service providers to continue using their current Telcordia OSS-based business practices as they evolve their telephony network.

Providing carrier-class reliability

The SpringTide® 7000 IP Service Switch Router used in the Lucent solution has been designed to provide the high-availability and fast service restoration required to provide carrier-class reliability for IP Centrex services.

High availability

The SpringTide® 7000 IP Service Switch Router was designed to meet the high-availability requirements of today's tier 1 carriers. All components are hot swappable and 1:1 or 1:N redundant. The internal control bus can detect the failure of any component in the device and move functionality to the backup component in hundredths of a second. All interfaces can be protected. In most cases, external devices connected to the SpringTide® 7000 switch router will not even detect a failure. The SpringTide® 7000 switch router's high-availability architecture helps carriers provide the level of reliability today's enterprise customer expects.

With the Lucent IP Centrex solution, service providers can continue using their current Telcorida OSS-based business practices as they evolve their telephony network.

Fast service restoration

In IP networks implemented with traditional physical routers, each router chooses between redundant data paths using routing protocols. When a link is lost, routing updates cause the network to reconverge. During this process, each device updates its own forwarding information base before allowing traffic to flow over the backup links. This process can take anywhere from 10-30 seconds. Although this fail over rate is adequate for most data traffic, it is not fast enough to preserve active calls.

In the Lucent IP Centrex solution, operators can configure protection on every SpringTide® 7000 IP Service Switch Router's interface module and port. Operators can protect ATM interfaces using standards-based SONET Automatic Protection Switching (APS). Operators can use Multi-Link PPP (MLPPP) to protect circuits provisioned over channelized interfaces.

To protect Ethernet ports, operators can use standby ports of the same type. In this configuration, the standby Ethernet port carries the traffic if the active port fails due to signal loss, frame loss, interface line card failure, or line card removal. Depending on the number of affected connections, the network experiences data loss for approximately 200–400ms during fail over. This much faster service restoration is essential for supporting voice.

To set up the redundancy, operators configure redundant ATM DS3 or Ethernet lines between the SpringTide® 7000 IP Service Switch Router and any attached devices. In the following diagram, the operator has configured a redundant pair of Ethernet links between a SpringTide® 7000 switch router and an iMerge™ CFG shelf.

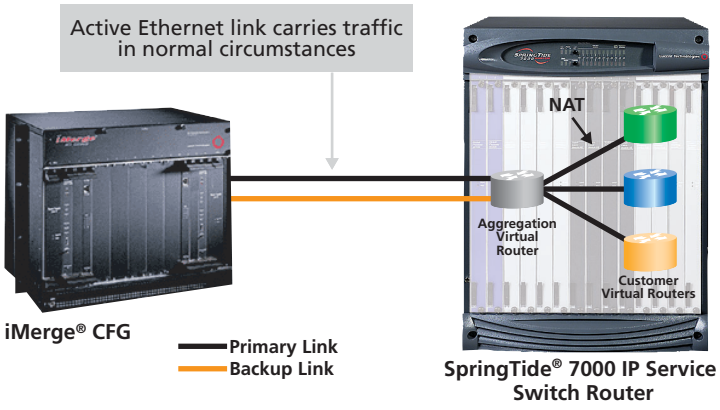

Figure 4—Establishing a redundant Ethernet connection between the SpringTide® 7000 IP Service Switch Router and the iMerge™ CFG

If any component on the active Ethernet link fails, the SpringTide® 7000 switch router detects the failure and switches traffic to the standby link. The iMerge™ CFG shelf also switches over to the standby link. The entire solution recovers within seconds—maintaining all in-process calls. (See Figure 5.)

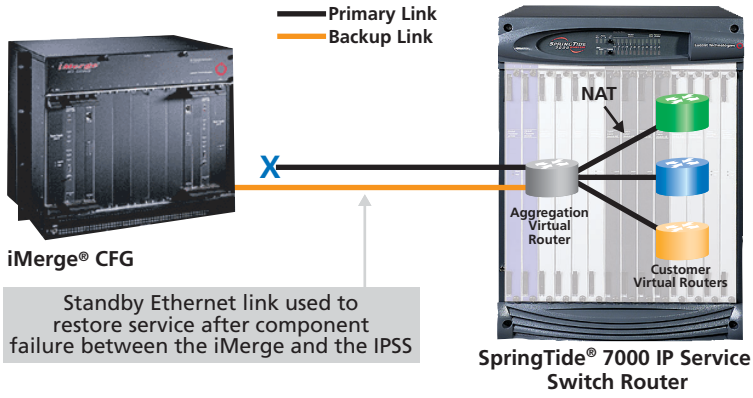

Figure 5—Recovering from component failure

4. Conclusion

IP Centrex services built with the Lucent iMerge™ CFG and SpringTide® 7000 IP Service Switch Router give service providers a unique opportunity to effectively compete with IP PBX vendors and reclaim market share in a down economy.

Service providers can use judicious IP Centrex deployments to gradually introduce their current customers to new IP Centrex services. Lucent IP Centrex enables service providers to implement a carefully staged migration to IP Centrex. Service providers can use the same Class 5 switch to offer both traditional Centrex and new IP Centrex services—helping eliminate the risks and downtime normally associated with service migrations. This enables providers to preserve existing Centrex revenue while creating the opportunity to increase revenue with an IP Centrex offering that provides greater service flexibility and uses available network resources more efficiently.

At the same time, by adding the SpringTide® 7000 IP Service Switch Router to the edge of their existing voice network, service providers are adding the infrastructure to support other valuable IP-based services, such as IP VPNs and IP network management, in the future. With the SpringTide® 7000 switch router, service providers also gain the ability to offer users self-provisioning tools. Service providers use these tools to simplify network management and enable enterprise IT managers to monitor the corporate network, associated charges, and SLA agreements.

For providers with large Class 5 investments, IP Centrex services can be the first step toward the end-to-end packet voice world of tomorrow.

To learn more about our comprehensive portfolio, please contact your Lucent Technologies Sales Representative, Lucent BusinessPartner or, visit our web site at www.lucent.com or www.lucent.com/products/multiserviceswitching

SpringTide® IP Service Switch Router and iMerge™ CFG are trademarks or registered trademarks of Lucent Technologies Inc.

Copyright © 2002
Lucent Technologies Inc.
All rights reserved

MSS v1 09/02

Lucent Technologies
Bell Labs Innovations

