White Paper

The Five Nines IP Network

Contents

Nokia is the first to bring 99.999% (Five Nines) service availability to the IP network's edge. Its ASR 2020™ Aggregation Service Routers allow service providers to build a high availability IP infrastructure and benefit from up to 70% lower cost of network ownership.

Abstract

"Five Nines" availability (99.999% uptime) is a staple in traditional TDM networks. Now that IP-based communications are mission critical, customers are demanding the same level of availability from their service providers' IP networks. Although IP networks run on top of a resilient optical transmission layer, and the IP core can yield high availability with a diversely routed mesh of routers, the IP edge remains a single point of failure.

Nokia ASR 2020 Aggregation Service Router brings Five Nines availability to the IP service edge. It is the industry's first IP routing platform that is capable of delivering services with PSTN-grade availability and SONET-like resiliency.

It not only provides a reliable solution for mission-critical IP traffic, but it also removes a major barrier to the migration of non-IP services to IP/MPLS networks. In addition to enhancing IP services, the ASR 2020's unmatched multiservice capabilities enable service providers to converge TDM private line, Frame Relay, and IP services into their IP infrastructure, further lowering the total cost of network ownership.

This paper looks at the requirements for availability in IP networks, dissects the anatomy of service recovery, and examines the Five Nines IP network's economic and competitive advantages.

The Five Nines IP Network

Five Nines Availability: An IP Network Requirement

The explosive growth of business IP network traffic represents a major revenue opportunity for service providers who can step up to the challenge of delivering mission-critical IP-based services. Unfortunately, today's IP networks lack the resiliency needed to support the high service availability (99.999% uptime) required for these mission-critical IP applications.

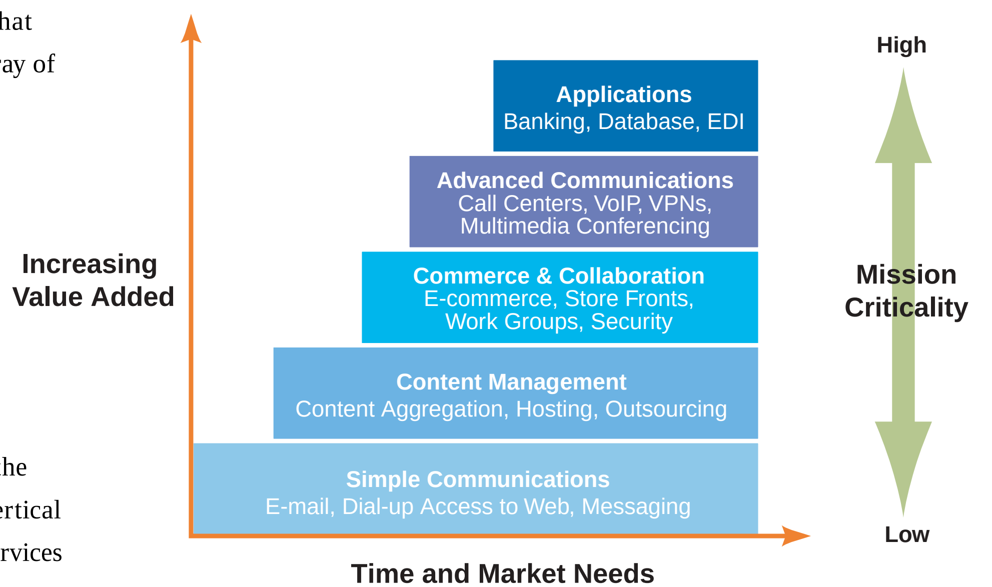
Business IP's tremendous momentum is forcing service providers to take a new look at how these networks are built. The days of using IP networks for just web browsing and e-mail are gone. IP has become a ubiquitous communications protocol that underpins an increasing array of enterprise IT services. The criticality of services running on IP continues to increase (see Figure 1).

A major source of current revenue comes from traditional services, like TDM private lines and Frame Relay. According to the industry research groups Vertical Systems and RHK, these services will represent $50 billion in revenue in 2003, increasing the total available revenue by 300% compared to IP revenue alone. The ability to aggregate these services onto IP represents an opportunity to further lower the total cost of ownership (TCO) of IP networks. It provides a way to improve the Return On Investment (ROI) for the estimated $70 billion in core routing and transmission equipment that service providers will purchase by 2003 (RHK estimate).

Supporting mission-critical IP services and migrating non-IP services to IP networks requires service providers to achieve the same 99.999% level of network availability that is supported within the traditional PSTN infrastructure. It is obvious that as IP moves up in the service food chain, achieving the PSTN-level availability will be crucial to meeting customer expectations and to growing IP network revenues.

The Issue is Above the Optical Transmission Layer

Network architects that focus on high availability seek to eliminate single points of failure from their networks. By deploying redundant core elements and utilizing lower layer restoration mechanisms such as SONET Automatic Protection Switching (APS), service providers have achieved Layer 1 facility and network element protection that yields 99.999% network availability. In accomplishing this, service providers have succeeded in



Source: Morgan Stanley Dean Witter

Figure 1. The mission criticality of IP-based communications is increasing rapidly.

eliminating multiple points of failure from their core networks.

Optical Layer resiliency, however, does not translate into fault tolerance at the IP Service Layer. The Service Layer fault tolerance requires that IP edge routers rapidly recover from hardware and software faults while maintaining the continuity for routing protocols and states so that subscriber services and the service provider IP networks are not affected. These capabilities need to be introduced before the declaration of the Five Nines IP network can be made.

Today's IP Edge: A Single Point of Failure

As the business IP traffic grows, service providers continue to deploy high-density edge routers that support greater numbers of subscriber per network element. A single edge aggregation router typically terminates hundreds or thousands of subscribers. It is at this network edge where the customer's mission-critical services are delivered, and where the service providers must assure conformance to the same high-grade Service Level Agreements (SLAs) as exist for private line (TDM) today.

Edge router failures should be avoided if these SLAs are to be achievable. Today's legacy edge routing platforms, however, lack fully redundant implementations that can provide the resiliency to avoid service downtime. As such, they represent a single point of failure in the network (Figure 2).

Legacy Edge Routers Can't Deliver 99.999% Availability

Current legacy routers have what are referred to as "hot standby" controllers. This means that the router has a secondary card that is powered on. However, these secondary cards were not designed to immediately restore services. Also, traditional router Operating Systems (OSs) lack the fault tolerance characteristics that allow the OS, routing protocols, and states to recover seamlessly. As a result, there will be a loss of service if the active controller card fails because the standby routing card has to boot the OS and reconverge the routing protocols, even if it is already powered up. In some cases a significant amount of manual intervention is required.

The typical router experiences at least one system failure (hardware or software) per year. If the router is equipped with "hot standby" controllers, the best-case recovery time in each failure instance is 7-10 minutes. This figure assumes that the system reboot and routing protocol recovery and reconvergence

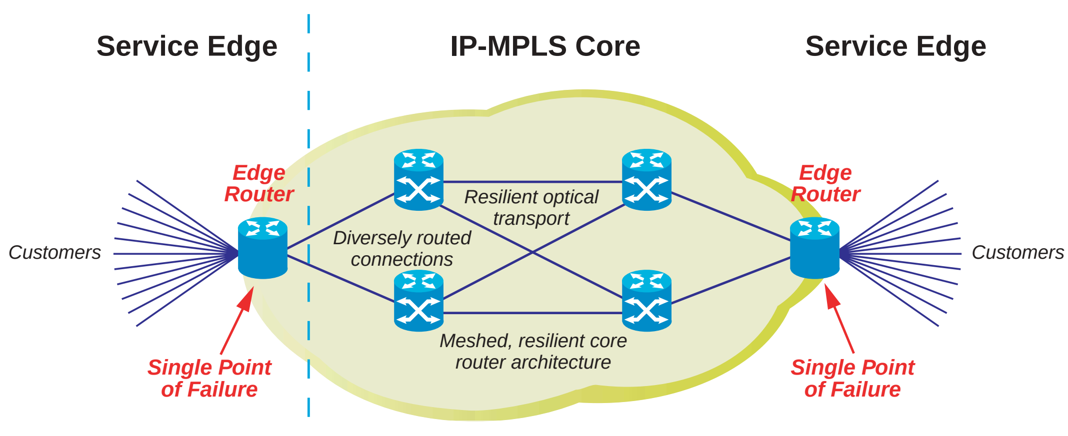


Figure 2. The IP Service Router represents a single point of failure at the edge.

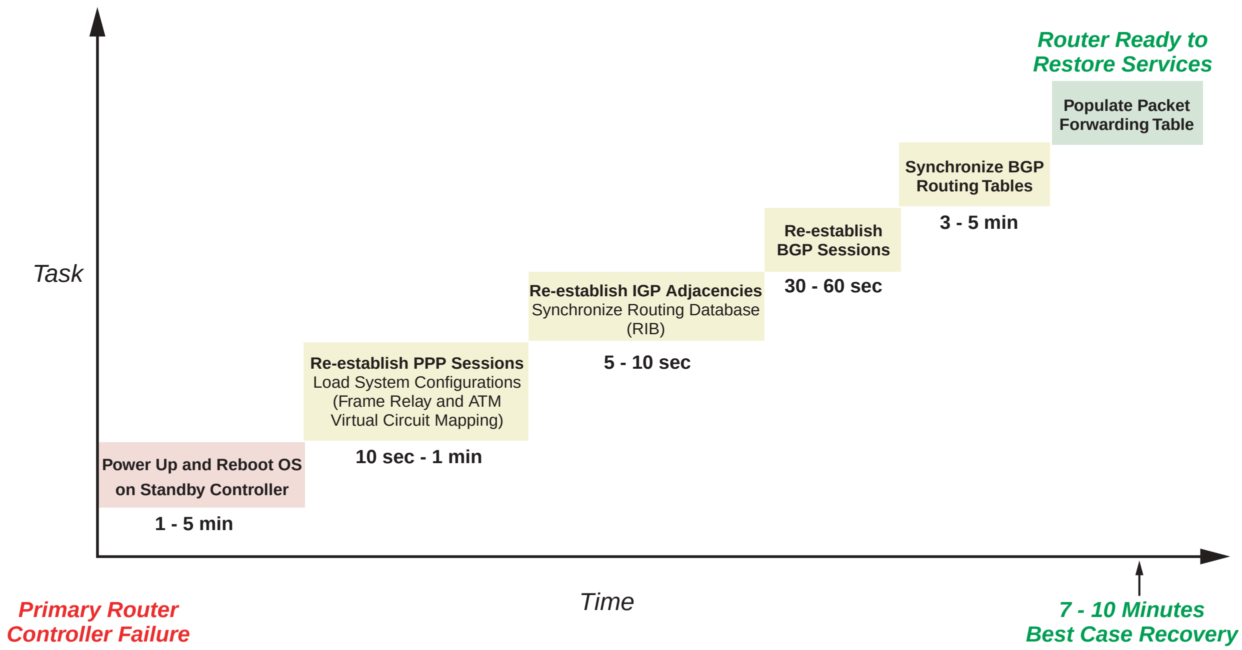


Figure 3. The best-case edge router recovery sequence requires 7 to 10 minutes.

is handled automatically (see Figure 3). But edge routers are also taken out of service on average three times a year for software upgrades, since the in-service software upgrades in these routers are not possible. In total, the legacy edge router is down at least 40 minutes per year. If a routing engineer has to get involved with additional troubleshooting, the outages can balloon into several hours per incident.

A rating of 99.999% network availability translates into approximately 5 minutes of downtime per year. Clearly, with 7-10 minutes of recovery per incident, the legacy routers can't meet this objective. Some service providers are attempting to make the edge more tolerant to faults by deploying two legacy routers in parallel. While substantially more expensive than a single router on the edge, this solution only garners a slight improvement in availability (router outages still typically require at least five minutes of downtime per incident). Neither legacy edge router approach is able to deliver on the Five Nines availability goal for IP networks.

Edge Failures Cause Network Instability, Makes Recovery Non-Deterministic

Compounding the issue is the fact that each edge router outage can cause havoc in the service provider's own network and across peer networks, and the entire Internet (Figure 4).

Inside the service provider's own network, the edge router failure causes adjacent routers to report the loss of communication with the failed router. All of these interior routers must then recompute the shortest path to each of the destinations that were learned via the Interior Gateway Protocol (IGP).

The failed router's BGP neighbors will report that the destinations learned via the failed router are no longer available. These messages propagate across thousands of networks and the tens of thousands of BGP routers that comprise the Internet backbone. When the router recovers, the lengthy notification process must be repeated across the entire Internet backbone.

The outage may also trigger routing advertisement oscillations or "route flaps" which may result in BGP router recomputation, and updates to the routing and forwarding tables throughout the network. In such cases, BGP route flap dampening is used to penalize misbehaving routes by suppressing them for several minutes or even hours, during which time that router's connectivity is lost.

This extended network misbehavior makes the deterministic prediction of recovery time impossible. Clearly, a new better solution is needed.

The Solution: Nokia ASR 2020

Nokia is delivering the world's first fault-tolerant routers for the edge of IP networks. These routers are designed to resolve the issues associated with legacy edge routers and thus enable service providers to achieve 99.999% availability in their IP networks.

Nokia's ASR 2020 Aggregation Service Router represents a new class of service edge products that offer continuous routing capability. Continuous routing capability includes the hardware redundancy specifically architected to run the Nokia AmbOS™, the world's first fault-tolerant routing OS. The ASR 2020 offers a truly "hot" standby processor design in addition to the line card and the selective port-by-port protection. The AmbOS is a breakthrough in the routing OS design. Not only is this operating system's processes fault-tolerant, the stateful redundancy also extends to all routing protocols, such as IS-IS, OSPF, and BGP. This combination is required to achieve the fault tolerance needed to maintain the Five Nines service availability when there is a fault in the edge router.

AmbOS™ dynamically mirrors the routing sessions, information states, and packet forwarding tables among multiple control elements in the ASR 2020. When a fault occurs, this information is not lost and is immediately available to the hot

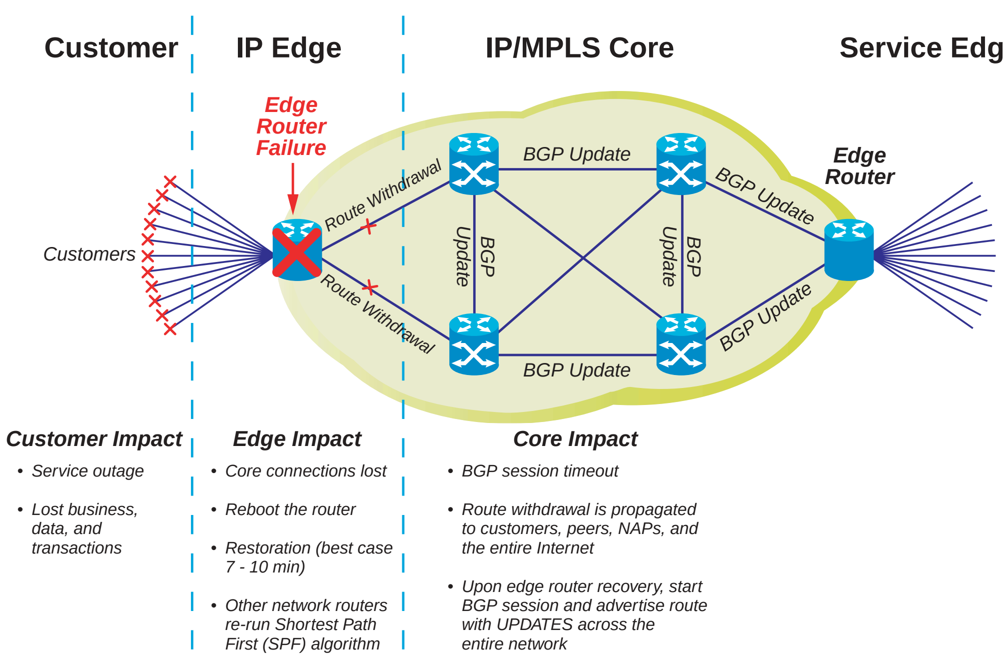


Figure 4. Edge router failure impacts the entire network.

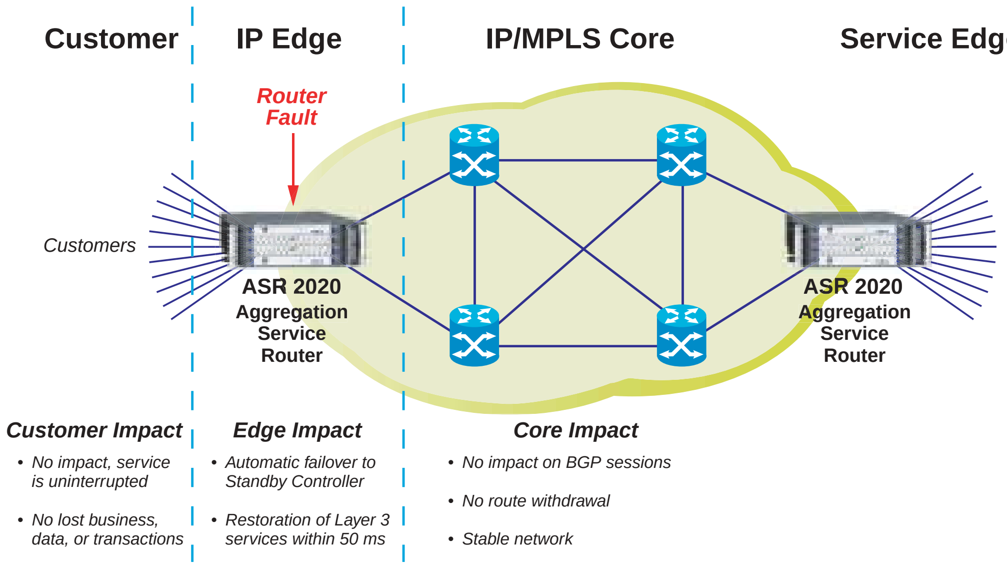


Figure 5. Five Nines IP network solution: The fault-tolerant ASR 2020.

standby controller. This slashes recovery time by orders of magnitude, achieving service restoration in less then 50 milliseconds (Figure 5). The switchover action is thus transparent to both subscriber services and the service provider networks. The result — recovery time is always deterministic and since behavior of the network does not change, the whole network stability is greatly enhanced.

With these capabilities, the ASR 2020 achieves the availability characteristics that only the traditional carrier-grade telephony network elements could claim until now. For the first time, service providers can establish the Five Nines IP network and offer the PSTN-grade SLAs needed for mission-critical IP services and the multiservice convergence.

The ASR 2020 Enables a Better Financial Model

With the ASR 2020, the cost of edge routers alone can be reduced by nearly 70%. In addition to the capital expenditures (CAPEX), the application of the ASR 2020 at the IP edge garners substantial savings in operations costs. The CAPEX includes equipment costs for edge routers, and for ports utilized on core routers, Digital Cross-Connects or SONET Add-Drop Multiplexers (DCS/ADMs). The operations costs include such costs as the initial equipment installation, the recurring costs for office and rack space, and power systems (both primary and back-up).

The ASR 2020 is by far a less expensive alternative to the legacy routers. It avoids the need to deploy complicated and costly redundant routers and redundant network element ports to achieve higher availability. When two legacy edge routers are deployed in parallel, the cost of infrastructure is doubled. Twice as many routers, Digital Cross-Connect ports, and wiring runs must be installed. In the long term, this approach will not scale operationally or financially.

The maintenance associated with downtime due to router failures and software upgrades can also represent a significant cost element. However, because the length of the legacy router recovery from faults is not deterministic (from 5 minutes to hours per instance), these costs are highly variable. The deterministic behavior of the fault-tolerant edge router leads to reduced administration and management costs and the simplification of capacity planning and traffic engineering.

The Five Nines IP Network Delivers Big Cost Savings

In the Present Mode of Operations (PMO) shown at the top of Figure 6, service providers deploy two edge routers to maximize the network availability. The Future Mode of Operations (FMO) shown at the bottom of Figure 6 is based on a single ASR 2020 fault-tolerant router.

Let's examine one deployment scenario where in both cases we will need to support 12 DS3 circuits carrying subscriber traffic. The PMO case requires twice as many Digital Cross-Connect ports, a total of 24, to connect the primary and back-up routers to the subscriber lines. It also doubles the number of connections to the core, requiring twice as many ports on the core routers.

In the deployment model based on fault-tolerant edge routers, in the first year of operations the ASR 2020-based FMO reduces CAPEX attributed to edge routers and core router/DCS ports by 68% and 50% respectively, and the annualized operating expenses are reduced by 92%. Combined, this yields a 63% reduction in Total Cost of Ownership (see Figure 7).

Not only does the deployment of fault-tolerant routers result in huge savings, it also delivers a plethora of competitive and operational benefits, including:

- Improved performance
- Improved reliability due to the reduction in network elements, cabling and related infrastructure
- Access to the larger pool of revenue-generating services (IP, TDM, Frame Relay)
- Improved customer satisfaction and retention

Because each service provider's network deployment model is unique, Nokia offers customized network cost analysis.

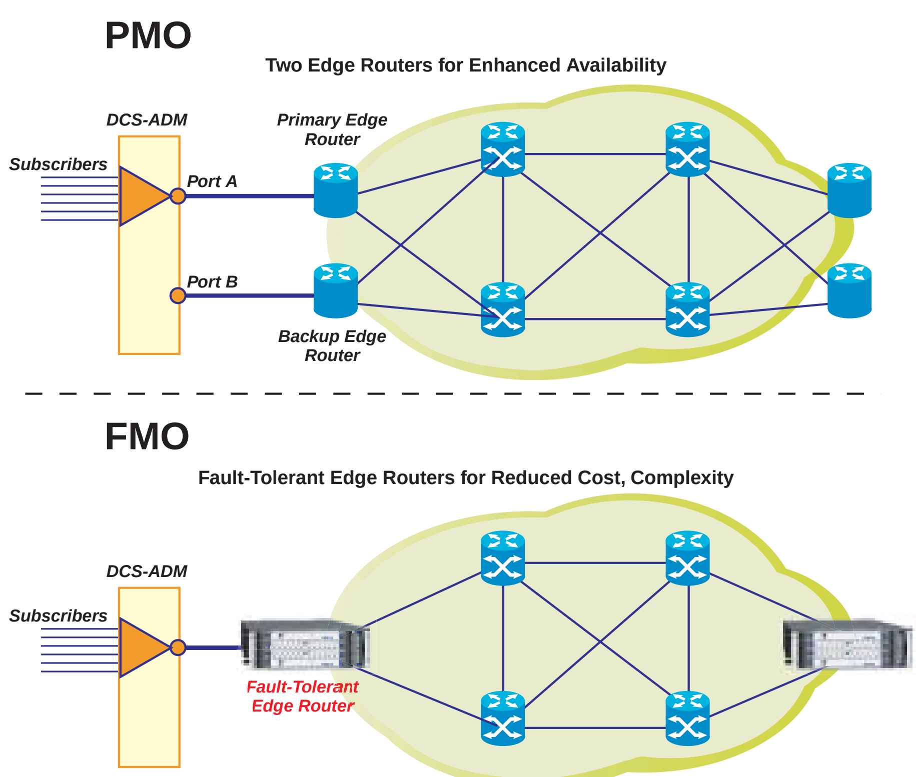


Figure 6. Deployment scenarios: conventional edge router approach vs. the ASR 2020 fault-tolerant edge router.

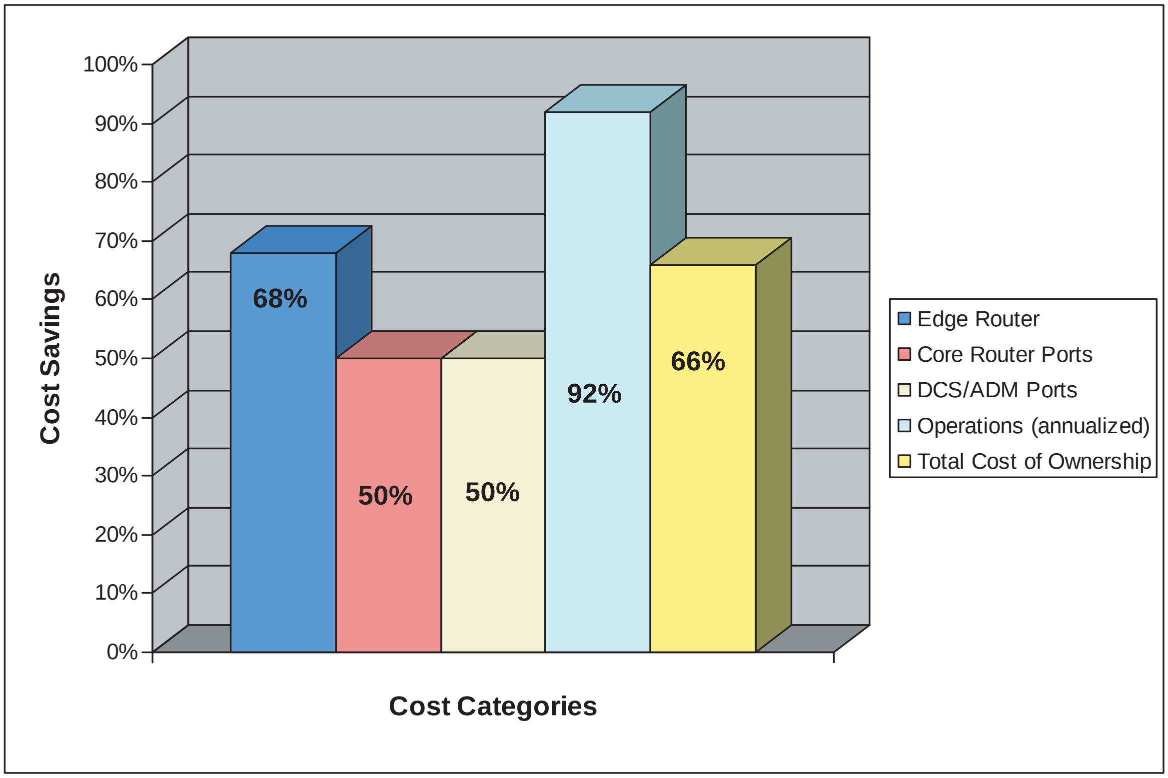


Figure 7. Fault-tolerant edge routers deliver big network savings (source: Nokia Marketing).

Summary

Achieving Five Nines capabilities in IP networks is both a financial and a competitive necessity. Armed with the Nokia ASR 2020 Aggregation Service Routers, service providers can achieve this PSTN-grade availability in their IP networks. It prepares the network for mission-critical IP services, and brings multiservice capabilities that let service providers take advantage of revenues from non-IP services, including TDM private lines and Frame Relay. Five Nines IP network is a model that garners substantially lower Total Cost of Ownership (TCO) and a 300% increase in total available revenue.

Adding this exceptional level of availability to their portfolio, service providers can maintain the value of their IP services by offering premium services with enhanced SLAs suitable for mission-critical applications. The result is significant competitive differentiation, improved customer satisfaction, and increased profit margins.

Nokia Networks
Broadband Systems
1310 Redwood Way
Petaluma, CA 94954
www.nokia.com

NOKIA
CONNECTING PEOPLE