Building the Carrier-Class IP Next-Generation Network

This white paper describes the requirements for IP networks to support an IP Next-Generation Network (NGN) environment. Carrier-class IP will become a fundamental requirement in the development of IP NGN and associated services. Illustrating how this development might occur for a typical traditional service, a scenario is presented in which carrier-class telephony is migrated from traditional circuit switching to IP. Each aspect of carrier-class IP in this migration is discussed to provide for a complete overview.

INTRODUCTION

The approach to building service provider networks is undergoing a basic change. Common themes in this change are convergence of infrastructure and services and integration of service offerings, with IP being the new fundamental technology. Cisco Systems® has developed a framework architecture to help service providers make a successful transition. Called Cisco® IP Next-Generation Network (NGN), this framework spans several Cisco technologies and areas of core expertise.

Most delivery vehicles used by service providers today are subject to change. Some areas of change are fully addressed by taking a different approach at the network edge and core, while being transparent to the customer. Other areas involve radical changes and expansion in how services are delivered, what services can be delivered, and the level of performance and service guarantees associated with a specific service. Some of these changes, all part of the Cisco IP NGN framework, follow:

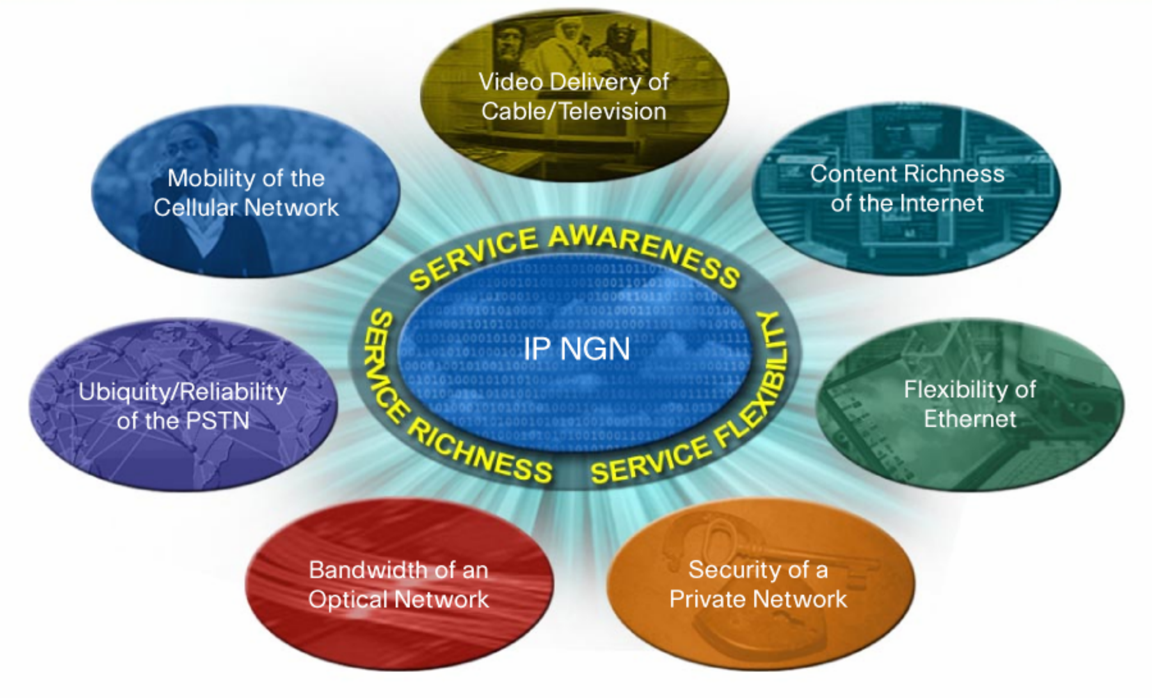
- Video services—In broadband environments it is common to receive television and different kinds of on-demand programming through IP. This transition will continue and will also involve interactive video services.
- Broadband networking—Although broadband deployments are rapidly expanding, the transition from being used as simple access to providing for networked home environments has just started.
- Wireline data services—Most business data services are still being delivered through last-mile Frame Relay or ATM services. The IP infrastructure will offer these plus other services on the same infrastructure, meeting the same customer delivery requirements.
- Telephony services—Traditional carrier telephony has been moving toward packet technology for some time and is now poised for a breakthrough as several traditional circuit-switching vendors are shipping packet-based voice solutions. In addition, the convergence between fixed and mobile voice services is about to begin.
- Wireless and mobile services—As mobile services converge with fixed voice services, the mobile handset is becoming a multimedia window into the converged voice, video, and data world, with real-time video and online gaming ready to take off on this communication device.

Many of the service provider applications and technologies originated in environments where the requirement to be “carrier class” is fundamental at both node and network level. These requirements accompany the existing service when it is converged into a packet network, so the IP infrastructure must be able to meet the same carrier-class requirement at both node and network level.

The IP network not only will replace one specific infrastructure used for a single application or service, but it will also have to do so for several different technologies and services and, on many occasions, in the same node. Concurrently, all service-specific requirements imposed by each individual service must be honored.

To meet these stringent requirements, the IP NGN must possess a broad range of capabilities, some of which can be somewhat contradictory in nature, to deliver a complete suite of services in harmony. The operating environment of an IP NGN infrastructure will be a mix of all the service components and attributes involved (Figure 1).

Figure 1. Cisco IP-Based Next-Generation Networking

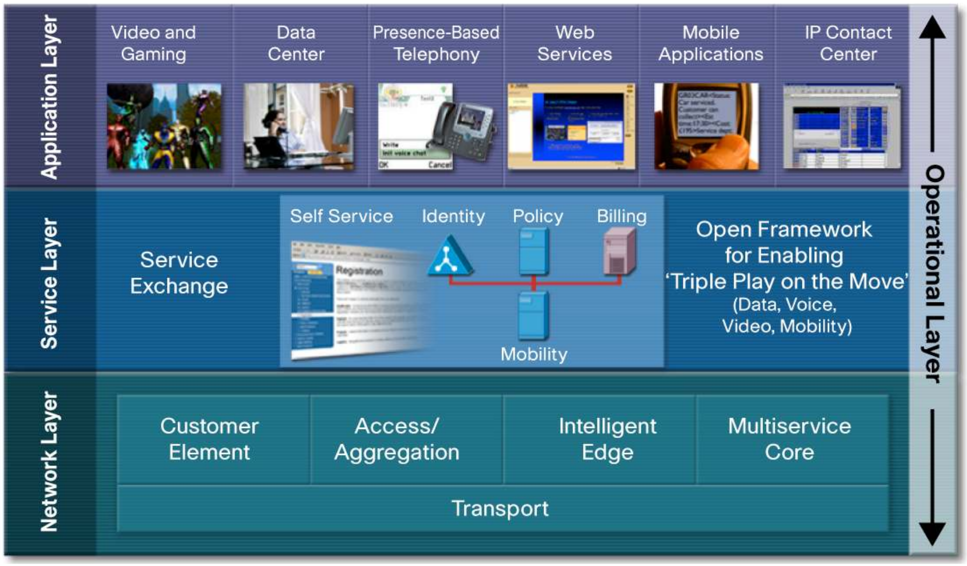

Video Delivery of Cable/Television
Mobility of the Cellular Network
Content Richness of the Internet
SERVICE AWARENESS
SERVICE RICHNESS
SERVICE FLEXIBILITY
IP NGN
Ubiquity/Reliability of the PSTN
Flexibility of Ethernet
Bandwidth of an Optical Network
Security of a Private Network

Clearly a multitude of technologies and platforms must be involved to meet these broad requirements as several previously disparate networks are merged into one. With IP as the common denominator, service-specific and feature-specific platforms will form the multicapable edge, converging around a common IP/optical core. Each different application and technology will place its own unique set of requirements on the IP infrastructure.

As depicted in Figure 2, central to an IP NGN are three fundamental areas of convergence already being enabled by service providers today:

- Application convergence—Carriers can integrate new IP data, voice, and video applications over a single broadband infrastructure for increased profitability. Application convergence opens the doors to “all-media services” such as videoconferencing, which is effectively a new service that is not simply voice, video, or data, but an integration of all three. This and other innovative value-added services can be delivered over any broadband connection. Service providers will have a range of new possibilities for revenue and portfolio differentiation.
- Service convergence—The Cisco IP NGN makes a service available to end users across any access network. For example, a service available in the office can be available over a wireless LAN, a broadband connection, or a cellular network. All these access networks can transfer the service and the state of connection transparently as the user roams, using the most efficient and cost-effective means possible. This kind of “service agility” creates a stronger relationship between the carrier and end user and can help increase customer retention.
- Network convergence—Creating a converged network is a goal that many carriers are already pursuing through their efforts to eliminate multiple service-specific networks or to reduce multiple layers within a network. A “many services, one network” model in which a single network can support all existing and new services will dramatically reduce the total cost of ownership for service providers.

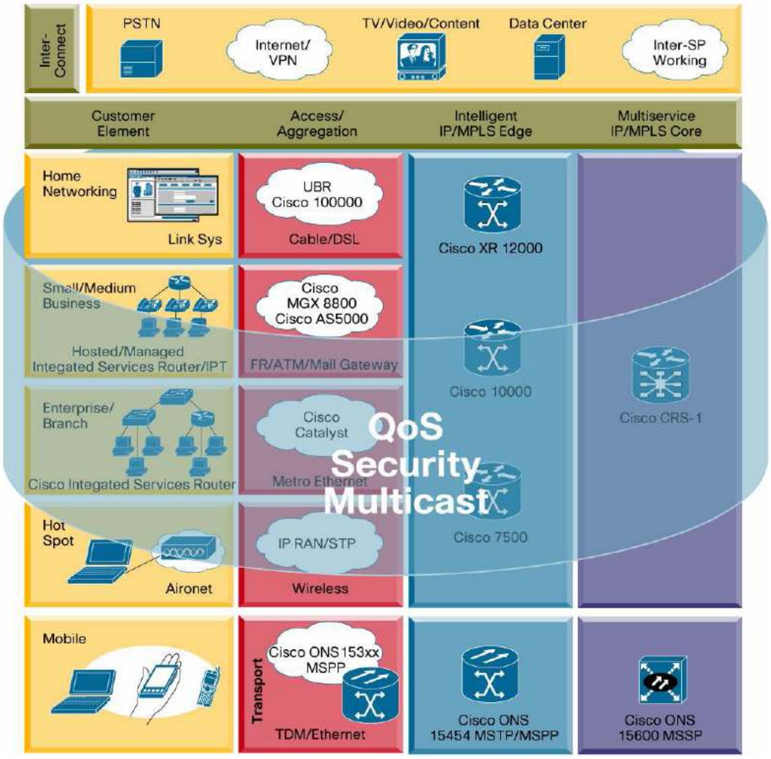
Figure 2. Cisco IP NGN Architectural Overview



At the foundation of an IP NGN is the secure network layer, composed of a customer element, access and aggregation, intelligent IP Multiprotocol Label Switching (MPLS) edge, and multiservice core components with transport and interconnect elements layered below and above.

As seen in Figure 3, the IP/ MPLS core network forms the underpinning of the IP NGN architecture. It is mandatory that the IP/MPLS core meet the carrier-class requirement for this architecture to be viable. The remainder of this paper discusses the transition from a traditional IP/MPLS core to an IP NGN carrier-class IP/MPLS core.

Figure 3. Cisco IP NGN Secure Network Layer



CARRIER-CLASS IP

To deliver the required features and functions outlined in the IP NGN architecture, the first step for many networks will be to assess whether they meet the NGN service requirements. Some traditional services now being migrated to IP are perceived to have nearly spotless service quality, and the networks currently used to deliver them are designed with equipment that qualifies as carrier class in every aspect. The converged IP infrastructure must likewise be carrier-class IP.

As an example of how strict the requirements are when making IP networks truly carrier class, consider the public-switched-telephone-network (PSTN) telephony as the service element being converged to IP. The requirements the IP NGN must meet to take over any service—not just PSTN telephony—fall in five different categories:

- Service requirements—These requirements are put on the infrastructure for transparent delivery of services based on either heritage (as in telephony) or the general requirements for a particular service. These requirements might differ between service providers, and possibly even between different tiers of a similar service.
- Network requirements—These requirements are network-specific and can be tied to specific services or be based on the overall performance goal of the IP NGN infrastructure.
- Security requirements—With a converged network come much more stringent security requirements. Specific requirements for limiting access to services or service nodes should be deliverables as part of a security infrastructure and policy.
- Operational requirements—Services previously offered on time-division multiplexing (TDM) or TDM-like architectures have strict operational requirements for adequate tracking and troubleshooting, health monitoring, and proactive performance monitoring. The IP NGN environment requires different sets of tracking data than does the traditional IP environment.
- Network design—The design of the network significantly affects the ability of the network to meet the requirements of all of the previously listed categories. Most design decisions are made based on a cost-benefit analysis. What is important is that these decisions are made consciously.

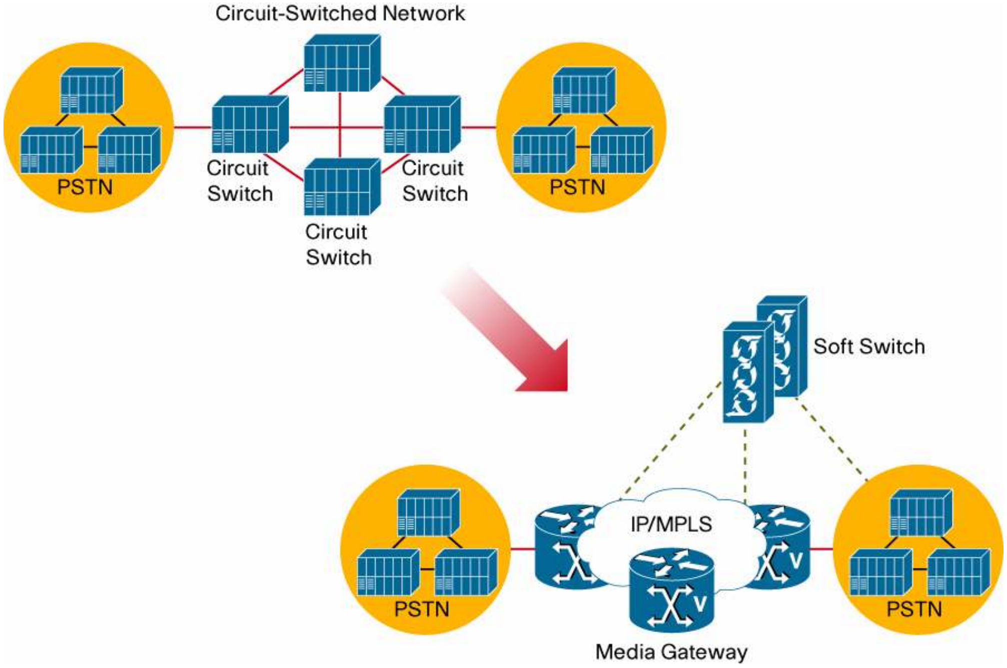
Although these five categories are discussed individually, it is putting all these pieces together that ensures that the network will work as intended. All of them together form the foundation for carrier-class IP.

SERVICE REQUIREMENTS FOR CARRIER-CLASS TELEPHONY OVER IP

The service architecture discussed here and its associated carrier-class requirement is commonly referred to as PSTN modernization or PSTN transformation. In the present scenario, only the core transport is based on IP, as opposed to a complete end-to-end IP architecture. Even so, the network characteristics required to meet the telephony requirements are to a large degree applicable to architectures that are end-to-end IP.

Using IP as the transport vehicle is not the only architectural change of the migration; it also means moving from a centralized circuit-switched telephony architecture to a decomposed soft switch-based architecture (also referred to as split architecture). For many service providers with existing circuit-switched telephony networks, this migration is the first step into a converged environment (Figure 4).

Figure 4. PSTN Transformation



The benefits of PSTN modernization to service providers include:

- Moving from many networks to one
- Higher degree of transport flexibility
- Open and standardized architecture
- Consuming less circuit-switched resources
- Decomposed architecture with centralized call logic, meaning fewer smart network elements needed

All these benefits contribute to better asset use and lower cost of ownership for the service provider.

Telephony Requirements

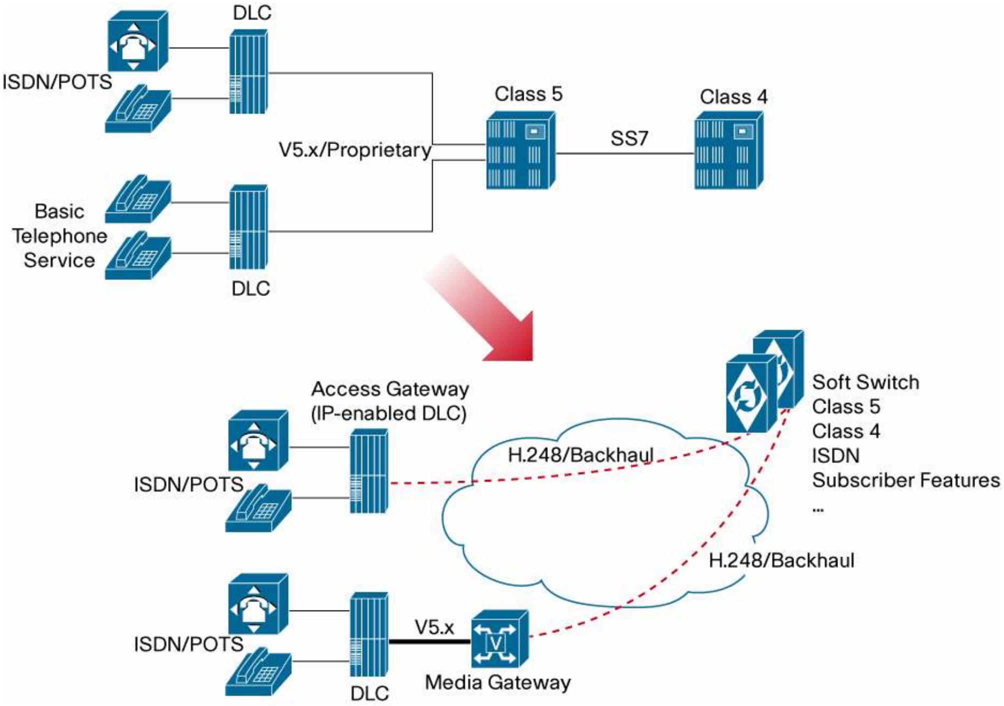
When telephone calls are billed by the second, there is zero tolerance for bad user experiences. If the voice circuit is breaking up, customers will notice and react to echo, noise, or other problems. Failure of any kind can mean that a phone call that would have generated revenue of $0.50 instead costs the service provider $20 in a call to its customer care center. Many service providers therefore view voice quality as a competitive advantage in that it reduces turnover by keeping customers happy. It is also viewed as a means for profitability because it keeps expensive customer complaint calls to a minimum.

The carrier-class telephony requirements are imposed by the signaling used to set up and tear down telephony calls and the actual media (speech, fax, and modem) used in telephony communication. Although there are differences in the detailed requirements between signaling protocols and media streams, it is safe to say that both traffic types place their own stringent requirements on the IP network.

Telephony Signaling Requirements

The signaling requirements are imposed by the protocols used between various entities in the telephony architecture. These entities include the soft switch, media gateway, and copper concentration units (Figure 5).

Figure 5. Telephony Architecture Evolution



Different signaling methods have different requirements. Many of the more recent signaling protocols have been designed for use in an IP environment and as such are more adjustable to and forgiving of latency and packet loss. However, most networks still employ some older and proprietary protocols. Many of these protocols are proprietary predecessors to V.5.x that have been designed to operate across point-to-point TDM circuits and, in the worst case, are directly integrated with SONET/SDH. Obviously the requirements for delay, jitter, and so forth are very stringent. Certain models of TDM-based equipment do not tolerate a loss of signaling connectivity beyond 200 ms, which then results in a signaling timeout and subsequently a stranded data-link-control (DLC) node with service outages for the connected subscribers.

Telephony Media Requirements

The ability of the IP network to meet the media (speech, fax, and modem) requirements is what determines the user experience during an established session. If the IP network cannot meet the media requirements, the result is deterioration of voice quality and the failure of fax and modem calls.

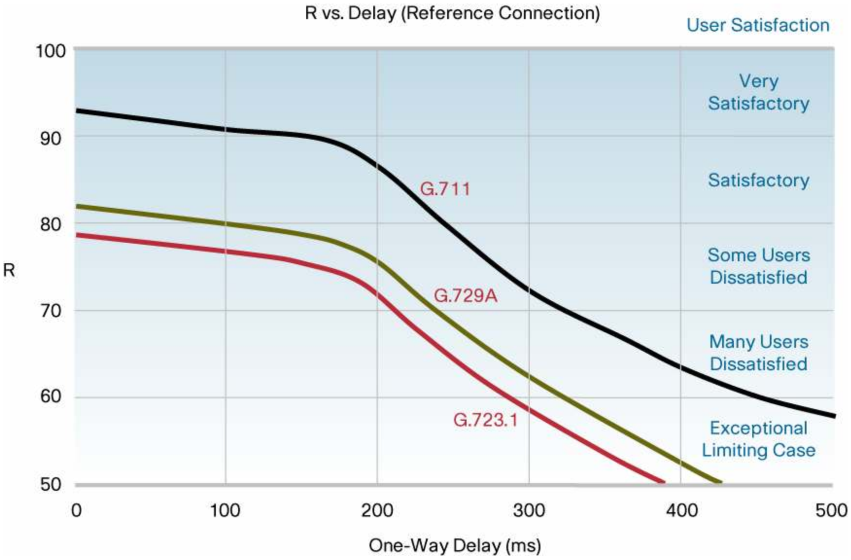
Voice quality is measured using either a manual, subjective measurement methodology called mean opinion score (MOS) or a mathematical method according to ITU-T G.107 (R-value). Many service providers state that voice quality should score higher than MOS 4 (or R-value 80) to be deemed carrier class. In most circuit-switched telephony networks the MOS scores are well above 4. Some countries even require service providers to report poor quality to the authorities.

When the telephony traffic is migrated from a mission-specific telephony network to a shared IP network, the voice quality must remain unaffected. Collectively, the most critical requirements of good voice quality in an IP environment include:

- Delay—End-to-end (mouth-to-ear) delay must not exceed 150 ms.
- Delay variation (jitter)—Jitter must not add delay beyond what is left in the delay budget.
- Packet loss—This factor depends on codec, sample size, how traffic gets dropped, and whether or not packet-loss concealment is used. Packet loss for telephony should never exceed 0.1 percent.

Depending on the compression method being used, delay, jitter, and packet loss have variable effects on voice quality. As a general rule, higher compression ratio (resulting in lower per-call bandwidth use) means greater impact on voice quality, if any of the basic requirements are not met. Figure 6 illustrates how delay and packet loss affect voice quality.

Figure 6. Effect on Voice Quality of Delay and Packet Loss (loss data from G.113)



Packet Loss %	G.711 Without PLC* (R-Value)	G.711 with PLC Random Loss* (R-Value)	G.711 with PLC Sequential Loss* (R-Value)	G.711 Without PLC (MOS)	G.729* (R-Value)
0	0	0	0	4.42	11
1	25	5	5	3.55	15
2	35	7	7	1.38	19
3	45	10	10	–	23
5	55	15	30	–	–

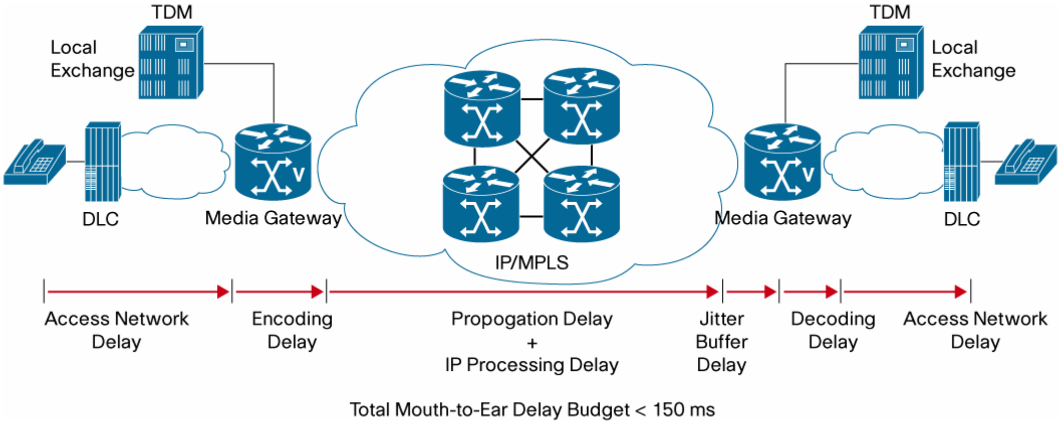
* from G.113

Another important aspect of transport quality is that in addition to speech, fax and modem traffic also uses the transport services of the network, and the associated applications of these services (such as credit card transactions) are very sensitive to interruption.

Although packet loss is mostly due to the provisioning of the network—including capacity planning, quality-of-service (QoS) implementation (network-related), and QoS capability (node-related)—delay has some components that can be influenced and others that cannot. Therefore, the delay characteristics of the network must be reviewed. Without this review, achieving good voice quality will be random at best, with very challenging conditions for troubleshooting.

To begin this exercise, it is imperative to understand where delay is introduced and how much gets introduced. The documentation of that information across the network is called a delay budget. Figure 7 illustrates possible places where delay can be introduced. Some of the delay is fixed and nonconfigurable, some is fixed and configurable, and some is variable—hence the need for a budget.

Figure 7. Delay Reference Model



When the delay budget is established, IP network design decisions can be made.

Network Requirements

To meet these telephony requirements, the IP network must have certain attributes that are not necessarily in place in current IP networks. The network-level requirements can be divided into three categories:

- Network availability—This variable can also be thought of as service availability, ensuring that network service is available to provide a certain subscriber service under changing conditions.
- QoS—The network elements or nodes must be able to provide a reliable QoS to assure an adequate level for the applications that are transported across the network infrastructure.
- Predictable performance—While providing the features necessary for a new service, the performance of existing services and subscribers must not be affected. Without predictable performance, it will be impossible for a service provider to plan and implement a service on a networkwide basis.

The expectation of a PSTN telephony service is that it is always there and always works. Although the IP network is different by nature, this expectation and the implied service requirements still apply.

Many IP networks are designed with redundancy and they present excellent network availability numbers, but that does not necessarily mean they are well-suited for—or even capable of—delivering toll-quality telephony. The key is that they should meet the delay, jitter, and packet loss requirements during any network condition, including times of load, stress, and failure. For that, all existing network elements, the network topology, and the protection and restoration scheme must meet carrier-class telephony requirements.

Subsecond service restoration is often considered a fundamental criterion for carrier-class telephony, but as discussed previously there are signaling schemes that require sub-200-millisecond restoration—a fact that must be considered when selecting IP equipment, designing the network, and deciding on a protection and restoration strategy.

In a circuit-switched telephony environment, a resource conflict results in calls not being established, so if the appropriate resources cannot be reserved from end to end the call is rejected. Resource conflicts in an IP environment are handled differently, and the consequences can affect not only the call about to be established but also established calls.

In a multiservice environment it is critical to ensure that telephony traffic is treated with priority so as to ensure quality. Although the telephony traffic does not itself generate bursts, it should not suffer from the congestion caused by other traffic types, which can degrade its service level. Consistent and strict QoS and low-latency treatment, through every network element across the network, is therefore a must for predictable service performance.

It is common for traditional network elements providing IP services to degrade in performance as more features are enabled. Certain platforms also degrade in performance when traffic from additional sources is sent to a higher number of destinations or when more line cards in the system contend for centrally shared resources. This situation can lead to troublesome situations for a service provider, where the service might work smoothly one day and the next day have serious problems due to the added load of a few more subscribers or a new line card. Because an inadequate platform would break any carrier-class functions, platform selection is important. A platform that uses hardware-based forwarding and separated control and forwarding planes is a fundamental requirement.

In summary, the network must always be available and must always be capable of delivering carrier-class telephony service—or any other service in the IP NGN environment.

Security

Security is a fundamental consideration in ensuring stable operation of a telephony service. Threats such as worms, viruses, denial-of-service (DoS) attacks, and other malicious activities must not degrade the network or service stability. To ensure stability in the network, strategies that cover several different areas need to be in place:

- Network element security—Providing strong security starts at the node level. Every network element must provide sufficient protection of its own resources and services.
- Network and IP spoofing protection—Providing infrastructure security includes blocking access to internally used subnets, IP spoofing protection and blocking, DoS protection and tracking, and more. IP spoofing—using both registered and unregistered address space—is the most common transport vehicle for malicious activities.
- Control-plane protection—Protected control-plane operation is imperative to ensure stable operation of the entire network. This protection includes both internal and external protection policies, because attacks originate from both ends.
- Service protection—Enabling service-specific security policies can be an effective threat mitigation strategy. If access to nodes or segments that are service-specific can be controlled from the rest of the network, a high degree of protection is immediately achieved.

Security becomes a completely different concern when an IP-based infrastructure is used to provide services traditionally provided on separate networks. TDM networks were not immune to attacks; the difference is that malicious knowledge of attacking IP-based networks and hosts is much more widespread. However, awareness of security is also much higher in the IP industry compared to many of the traditional vendors of earlier-generation equipment.

Awareness needs to be raised with service providers as well, regarding both risks and solutions for the problems. A network that would otherwise be considered carrier class could easily be degraded to something less if security is compromised.

Operations

Most IP networks and traditional telephony networks have some fundamental management differences. Telephony networks are micromanaged down to the phone call level, and records of every call are stored. Because resources in the IP network are not assigned to a specific call this way, a different approach has to be taken to provide for low-level troubleshooting and similar functions.

The telephony networks often have comprehensive operations support systems (OSSs) that provide much information about the current and historical status of the system. Therefore, service providers often want some level of interaction between the IP network and the OSS. This interaction is also required from the IP infrastructure to provide a level of information similar to that previously provided from its circuit-switching counterpart. The required integration between the IP network and the telephony network must cover the following areas:

- Proactive health monitoring—The IP network needs to provide current network responsiveness and health information to the telephony OSS, allowing the telephony control plane to ensure that good routes are chosen for new calls and to reroute established calls when needed. This monitoring should also provide information about any conditions related to voice quality, such as delay, jitter, and packet loss.

- Data and statistics collection—When network problems occur, statistics related to volume, QoS-class performance, and so forth must be available for a proper understanding of the situation and any potential effect.
- System integration—The telephony OSS is typically providing the umbrella OSS function, but it must be able to manage data flows and other information from the IP network. It is therefore imperative to integrate element-management-system (EMS) systems, mediation platforms, and other potentially needed functions to ensure that the telephony OSS remains fully functional in relation to the IP network.

By providing this function in a PSTN transformation architecture, the telephony OSS can continue to be the prime source of information as well as a provisioning tool for the telephony service. Proper monitoring and statistics-gathering functions in the IP-network equipment should be ensured, because otherwise the telephony OSS will have a gap in its monitoring capability that impairs its ability to troubleshoot and plan for the IP component of the infrastructure.

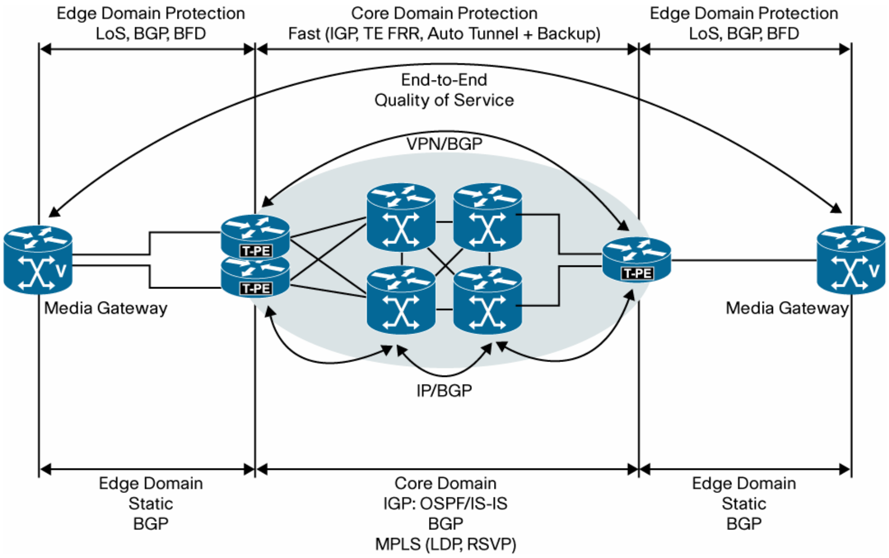
Network Design

Network design is the cornerstone of the ability of an IP network to meet carrier-class requirements. The design phase must take input from the entire scope of requirements discussed previously (service, network, security, and operations) and transparently weave together all elements.

The fundamental design goal for a carrier-class IP network is to enable deterministic network behavior during any operating conditions. What that means in the case of telephony has been discussed in this paper, although the details will always be unique to each individual organization. In building IP NGN, this means defining the same set of requirements for all services that will be supported on the network to ensure that the NGN can meet all the requirements set by all services. If the strictest requirements can be met, then so can any lesser requirements as the network scales to connect more services and customers.

As an example of the different choices to be made, Figure 8 depicts the typical network domains used for a telephony service, with the various technologies used for achieving different functions on a per-domain basis. Though a simplified picture, it still illustrates some of the complexities in the design decisions to be made.

Figure 8. IP Telephony Network Design



As an example, an IP network should be able to detect and work around potential problems and outages without affecting the service availability. Ideally the network should be capable of correcting a problem before the application even notices that an outage has occurred. The approach to accomplish this varies in an IP versus an IP/MPLS network. In addition, different performance parameters apply to these two types of networks, depending on the services supported.

The choices made during the network design phase determine whether the IP network can meet carrier-class requirements. It is therefore critical to gather all the facts first and approach the design in such a way that any future changes can be made with minimal disruption. Services to be supported on a node also guide the selection of network elements.

SUMMARY

IP NGN will fundamentally change how service provider infrastructures and IP networks are built. Services must provide design guidance more than ever before, and service-level requirements inherited from previous services and networks must be honored. Building a carrier-class IP NGN is fundamentally different from how IP networks have traditionally been built.

Carrier-class performance must be a requirement from the beginning in the design of these next-generation infrastructures that are built on packet technology. It has to dictate every design decision—from platform choice to OSS integration—to ensure the proper delivery of a next-generation infrastructure.

CISCO SYSTEMS

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

C11-331938-00 02/06