Network Infrastructure for Ensuring Predictable Business Service Delivery

Abstract

Basic connectivity services are being commoditized rapidly for both business and residential markets. Recognizing this, service providers realize they must add value to remain profitable and use security enhancements and application-aware VPNs to deliver managed VoIP, data, and video services that work in a collaborative, integrated and, most critically, predictable fashion.

The primary requirements to ensure that the network infrastructure is capable of predictable service delivery include high availability, robust QoS, multicast performance, flexible hardware platforms, and integral service capability. These requirements are necessary to support stringent business-class service-level agreements (SLAs) while minimizing capital and operational expenses (CapEx and OpEx).

This paper examines two approaches to service delivery. It compares the use of an appliance-based solution with an integral service delivery model where services such as security (firewall) and session border control are incorporated directly into the router. The appliance-based solution suffers from several weaknesses, including the need to integrate and qualify the hardware prior to service creation, the need to manage and operate multiple hardware platforms and software systems, and the limitation of performance being determined by the weakest link in the service chain. By contrast, integral service delivery can minimize the operational challenges required to create and deliver a new service category. It also provides the best value both in terms of CapEx, by minimizing the number of platforms while enhancing scalability, as well as OpEx, by simplifying network management, sparing, and troubleshooting. Integral services also have the benefit of easily supporting a guaranteed, measurable SLA that is not affected by outside devices.

Introduction

Service providers face the dual challenge of delivering advanced business services while minimizing CapEx and OpEx. As basic data connectivity becomes commoditized, service providers must offer more sophisticated capabilities to their business customers to maintain revenue growth and keep their customer base. The concept of Predictable Business Services builds on the IP Next-Generation Network (IP NGN), which offers a flexible and cost-effective platform for delivering advanced, highly available, differentiated services with guaranteed SLAs. By simplifying the deployment and maintenance of these advanced services, the IP NGN reduces operational expenses that can consume new revenue. The scope of Predictable Business Services is wide, and includes managed VoIP, video (telepresence), managed network-based security, and VPNs (based on both MPLS and IPsec).

This white paper discusses the challenges facing network operators and provides recommendations for building out the infrastructure needed to offer advanced, predictable services.

Operational and Technological Challenges Facing Network Operators

Delivery of Predictable Business Services requires more than just high availability and QoS, although these are certainly both necessary. For services to be predictable they must also be simple to install, provision, maintain, and integrate into an existing network. Anyone familiar with network operations knows that selecting the hardware needed to deliver a new service is only a small part of the challenge. Much more time-consuming and ultimately more critical to the success of a new service are the operational aspects of service delivery. Operational expenses – not capital costs – often hinder profitability.

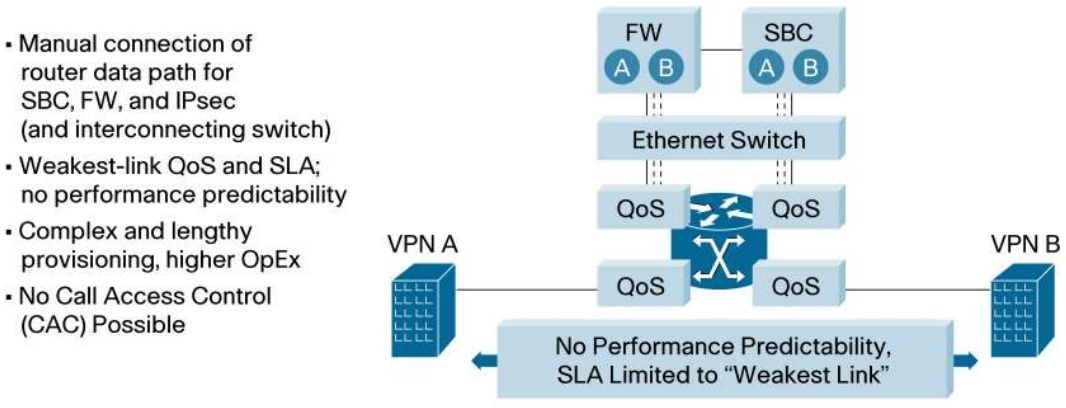
For network operators there are two possible solutions: highly integrated service-delivery platforms that include Layer 3, security, and session border control (SBC) capabilities built into a single, flexible, high-performance platform. The other solution is the "appliance model," which is based on multiple purpose-built platforms that specialize in a given function (Figure 1).

Existing solutions based on multiple, single-purpose platforms or appliances typically require the service provider to perform the system integration necessary for service delivery. Also, there is often a lack of flexibility in a network that is created through the use of purpose-built platforms. A more flexible approach that can easily incorporate new services allows the service provider to deploy a single network infrastructure that will not become obsolete a few years after installation.

An example of the multiple platforms needed to deploy services such as voice, telepresence, managed security, etc. include:

- A router to provide Layer 3 protocol support and capabilities, including Layer 3 VPNs and MPLS traffic engineering
- Security appliance (firewall) for IPsec and firewall capabilities
- Session border control appliance for call control, etc.
- An Ethernet switch to tie each of these components together

Figure 1. Appliance Model for Service Delivery



This model presents multiple challenges for service delivery, including:

- **Test and integration**: The network operator first has to verify that all of the components – often from multiple vendors – can interoperate and meet the requirements of the operator. This can be quite challenging because of the many test cases needed, and the difficulty of testing many performance characteristics, including loading, failover, etc. Prior to evaluating the performance of individual platforms that make up the service, a lot of time, money, and effort must be spent.
- **Maintenance**: Each hardware platform must also be maintained for spares, occupies valuable POP rack space, and consumes electrical power.
- **Software**: In addition to the multiple hardware platforms, there is also a need to maintain multiple operation systems or software loads, and to maintain a test lab that ensures that new software updates don't "break" the overall service-delivery chain.
- **SLA performance**: Performance of the overall solution and hence the service is limited by the "weakest link" in the service chain.
- **High availability**: Redundancy can also be challenging. In addition to possibly having to double the number of platforms, unless the appliances can natively support dynamic routing protocols there is no easy way to ensure that a backup route is taken to maintain the SLA.
- **Provisioning**: The need to provision each platform can complicate operations. For service providers that separate voice (managing the SBC) and data (managing the router) there could be other problems where one can interfere with the other.

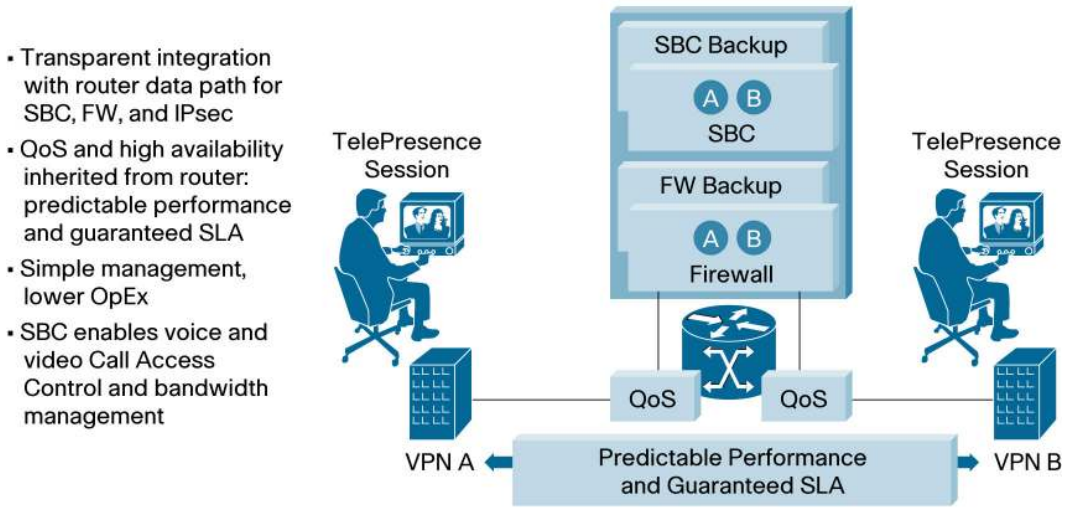
In summary, a more elegant, manageable, and scalable solution would integrate multiple features into a single platform for service delivery.

Integral Model for Delivering Predictable Business Services

Cisco® offers an alternative to the appliance-based model: an integral service model that allows providers to easily scale services and capacity (Figure 2). Using intelligent routing platforms such as the Cisco XR 12000 Series Routers, service providers can cost-effectively meet the following requirements:

- Continuous system operation: Business customers demand that their service remain in operation at all times.
- Multiservice QoS and scalability: QoS is critical to ensure that low-latency traffic such as voice and telepresence is prioritized and that one customer cannot interfere with another. The network must also be capable of easy scalability as traffic growth increases.
- Virtual output queues (VoQs) to avoid head-of-line blocking (HoLB): These help ensure that one customer cannot interfere with another customer simply by making extensive use of their bandwidth.
- Efficient multicast performance: Business video traffic, especially distance learning, often makes extensive use of multicast protocols.
- Secure virtualization: For greater efficiency, routing platforms should be capable of being segmented into multiple "sub-routers" – in effect multiple routers sharing a single hardware chassis but having their own operating system, route processor, etc.
- Integral service capability: Advanced services such as Session Border Control and firewall are ideally built directly into the router.

Figure 2. Cisco Integral Service Model



Continuous System Operation

Dropping customer traffic will quickly result in lost accounts and expensive penalties. However, Cisco IOS® XR Software uses a microkernel-based operating system to provide granular process independence, fault containment, and isolation. With these unique capabilities, the Cisco XR 12000 Series can be maintained, upgraded, enhanced, and scaled without service interruptions. Combined with the distributed architecture and redundant components of the Cisco XR 12000 Series, Cisco IOS XR Software helps enable a carrier-class infrastructure that supports “always-on” operations. Primary High Availability features include:

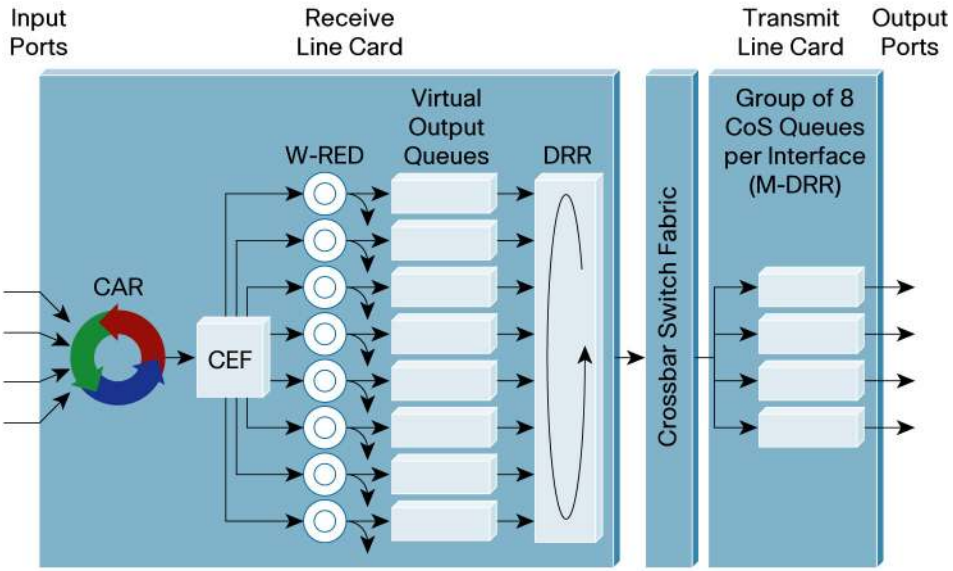
- Redundant power supplies, fans, controllers, and processing elements
- Distributed architecture with separation of data, control, and management planes
- Process management through redundancy, failure detection, isolation, tolerance, and recovery
- In Service Software Upgrade (ISSU), which supports nonstop forwarding (NSF) and graceful-restart extensions of routing and signaling protocols
- Hot-swappable hardware support with online-insertion-and-removal (OIR) functions
- Hardware memory fault detection and correction through parity or error-correction-code (ECC) memory

Multiservice QoS and Scalability

With distributed processing intelligence, robust QoS, and multicast mechanisms, the Cisco XR 12000 Series allows providers to scale both services and customers and maintain predictable performance using IP Service Engine (ISE) line cards (Figure 3). Key features of the ISE line cards include:

- Cisco IOS XR Software distributes processing intelligence to each ISE line card (that is, OS infrastructure and applications, Layer 3 forwarding, line card-specific control functions, and packet manipulation) and to additional route processors installed in the system (for example, Border Gateway Protocol [BGP], Intermediate System-to-Intermediate System [IS-IS], etc.). Distributed processing intelligence removes software limitations to system scale and allows network operators to take full advantage of the aggregate capacity of installed hardware in the system.
- ISE line cards take advantage of the industry's most sophisticated 2.5- and 10-Gbps application-specific integrated circuits (ASICs), which are fully programmable to support the diverse and continually changing Layer 3 feature set required by multiservice IP Next-Generation Networks.
- Dedicated queuing ASICs on each ISE line card provides unparalleled per-customer QoS that protects against jitter and delay of video and time-sensitive data and voice applications without impacting scale or performance.
- Cisco IOS XR Software service separation architecture between data, control, and management planes helps enable deployment of new features without service disruption. Its modular software architecture accelerates service delivery with individual packaging of feature sets, and allows components to be installed, updated, or deleted individually.

Figure 3. Multiservice QoS Capabilities in the Cisco ISE Line Cards

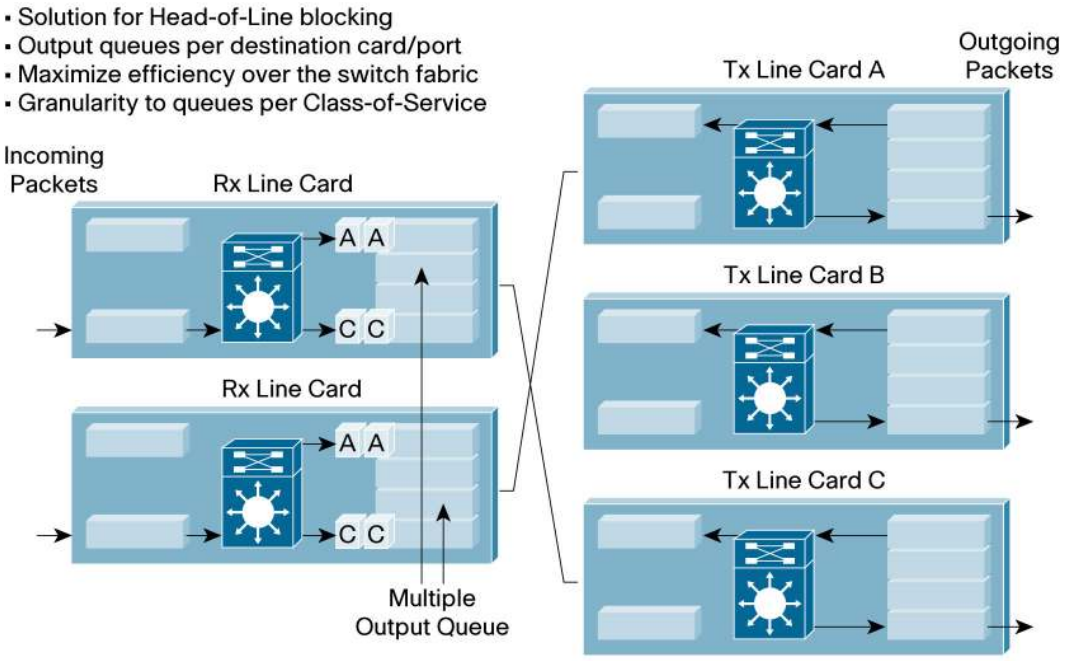


Virtual Output Queues

Head-of-line blocking (HoLB) is a problem that can occur in any system where congestion exists at an output port. It occurs when multiple packets destined for multiple destinations all share one queue. Packets destined for a specific location have to wait until all packets ahead of it are processed before being passed through the switch fabric. An example would be when several multiple-lane highways are merged into a one-lane highway. The best way to solve this is to have several multilane highways merge into one multilane highway.

The Cisco XR 12000 Series uses a unique, multiqueue implementation to eliminate HoLB. As packets arrive into the Cisco 12000 Series line card, they are arranged into one of multiple virtual output queues (VOQs) categorized by slot, port, and service priority as determined by the forwarding information contained in the forwarding table on each line card. Even if a series of packets is being sent from multiple sources to one line card, the other packets in the different VOQ that are destined for other output interfaces can be sent across the switching fabric, avoiding the usual HoLB problem. Figure 4 shows an example where packets to line cards A and B can be sent independently of packets destined to line card C.

Figure 4. Use of Virtual Output Queues to Prevent HoLB



Efficient Multicast Performance

The switching fabric must also be designed for IP Next-Generation Networks and services that require IP Multicast. The switching fabric overcomes the traditional problems associated with IP Multicast by:

- Using special hardware that performs intensive replication of IP packets on a distributed basis (in the fabric and line card)
- Dedicating separate queues (VOQs) for multicast traffic, so that other unicast traffic is not impacted
- Allowing for the creation of partial multicast segments

The Cisco XR 12000 Series supports efficient multicast traffic and does not exclusively burden the line cards to support multicast protocols.

Secure Virtualization

The Cisco Service Separation Architecture (SSA) allows service providers to consolidate multiple networks and services onto a single, “virtualized” platform while keeping each network and service instance separate and secure. This consolidation helps ensure that network anomalies experienced in one service (for example, the public Internet) do not affect another (for example, a private VPN). Services and customers are isolated from each other for maximum security. Additional benefits of consolidation through secure virtualization include feature transparency, optimal point-of-presence (POP) design, and OpEx and CapEx efficiencies as a result of a reduced number of network elements. Primary features of Cisco SSA include:

- Complete physical separation of network and system resources between each logical routing instance on the Cisco XR 12000 Series
- Isolation of traffic flows and management- and control-plane functions per routing instance

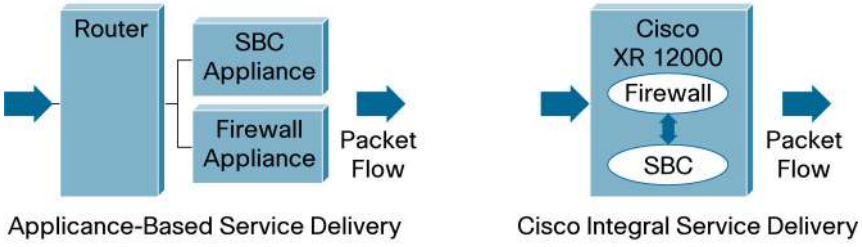
Integral Service Delivery

Cisco Integral Service Delivery enables the characteristics of the router to be inherited by service blades, including QoS, dynamic router protocol awareness, and stateful failover. Management and provisioning are simplified because only a single command line is needed to add a service for a specific customer. Performance is predictable and reliable across the platform, and only a single operating system is required. Service delivery is enhanced because bandwidth-aware Call Admission Control (CAC) can ensure that sufficient resources are available before attempting to set up voice or telepresence sessions. By contrast, the use of external appliances for service delivery requires separate provisioning steps and integration of multiple operating systems, and service performance is limited to that of the least capable platform. The lack of CAC means that services could be enabled without sufficient bandwidth to ensure customer quality of experience. Key benefits of Cisco Integral Service Delivery include:

- QoS and high-availability features for predictable performance inherited from router
- Transparent integration with router data path for Cisco IOS XR Session Border Controller (SBC) and virtual firewall services (Figure 5)
- Simplified management and operations, and lower total cost of ownership

In the Cisco XR 12000 Series, services such as firewall and session border control are virtualized and supported through the use of a multiservice blade.

Figure 5. Appliance-Based Service Delivery Versus Cisco Integral Service Delivery



The Cisco model provides many operational benefits for network operators:

- **Test and integration**: The integral solution is well characterized and easy to deploy. No additional integration or testing is necessary.
- **Maintenance**: One platform supports all necessary service capabilities, minimizing rack space, power consumption, and spares.
- **Software**: Only one version of software must be maintained. Upgrades can be performed in-service with ISSU.
- **SLA performance**: Performance is well characterized and can be measured using tools such as IP SLA.
- **High availability**: The solution is fully redundant and service blades support stateful failover.
- **Provisioning**: By combining multiple capabilities into a single platform, operations and provisioning are greatly simplified. Adding virtual firewall or session border control to a packet flow requires just a single command line. Furthermore, all QoS and ACLs are inherited by the service, eliminating the need to configure multiple static routes, QoS, and ACLs for each appliance.

Table 1 provides a more detailed comparison between the two competing solutions, showing how the Cisco Integral Service model has many advantages.

Table 1. Comparison between Integral Model and Appliance Model

Feature	Cisco Integral Model	Appliance Model
Platform and Implementation	• Single multiservice platform • Session border control and virtual firewall using multiservice blade integrated into Cisco XR 12000 Series • VRF-aware (service instance learns VRF routes) • Stateful failover • IPsec using shared port adapter with full QoS support	• Requires router, external security appliance, external session border control appliance, and switch to interconnect
Simple Operations: Lower OpEx	• One platform in one location with a single management scheme • Firewall or session border control services can be added with one command line, and all QoS and ACLs are automatically inherited	• Multiple platforms for each service with multiple management schemes • Need to connect to appliances using GE or 10 GE; requires an external switch • Must configure VLAN per customer in router, firewall application, and SBC application • Need to configure services and QoS in each appliance
Scalability and Capacity	• Simple and superior scalability by adding additional multiservice blades, not platforms	• Must add external appliances; additional space, power, required
Service Delivery: Predictable SLAs	• QoS and scalability are well characterized and consistent across all services, including IPsec • Bandwidth-aware SBC helps ensure that only calls with sufficient resources will be completed • Provides stateful failover of all sessions	• Different QoS and scale capabilities in each appliance; SLA is based on “weakest link” • Appliances are not easily made VRF-aware • Limited QoS support for IPsec • No CAC
Service Virtualization	• Flexible partitioning of services provides efficient use of router	• Requires dedicated appliance for single application

Conclusion

Service providers recognize that they must provide their end users with advanced, higher-margin services to grow revenue and maintain their customer base. Existing networks built with many platforms are capable of delivering such services only at high operational cost due to the complexity of the implementation and difficulty in characterizing the overall performance of the solution. By contrast, Cisco Integral Service Delivery offers providers the ability to deliver new services with predictable performance and SLA guarantees while simplifying network operations.

For More Information

For more information contact your Cisco sales team or go to http://www.cisco.com/go/pbservices.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-397769-00 03/07

