SIMPLY CONNECTED FOR UNIFIED COMMUNICATIONS AND COLLABORATION (UC&C) REFERENCE ARCHITECTURE

A Blueprint for Enabling UC&C Applications on Juniper Networks Infrastructure

Table of Contents

List of Figures

Executive Summary

Today's highly competitive global marketplace requires seamless communication and collaboration among employees, customers, partners, and suppliers. The promise of reduced costs, combined with enhanced collaboration and productivity, has led many companies to adopt Unified Communications and Collaboration (UC&C) solutions that combine the entire set of available information applications under the single but broad umbrella of communications.

UC&C is *not* a single product but rather a solution composed of a variety of communication tools and components. This evolution started with voice and has gradually progressed to conferencing, video, instant messaging (IM), presence, and other collaboration applications.

Enterprise telephony has developed technologically from analog phones, legacy PBXs, and time-division multiplexing (TDM) trunks to today's converged IP networks with diverse IP phones, soft phones, centralized IP PBXs or UC&C servers, and Session Initiation Protocol (SIP) trunks for telecom network Public Switched Telephone Network (PSTN) termination. New and rich services such as presence, video, instant messaging (IM), and file sharing have optimized the way members of an organization collaborate anywhere, anytime. In addition, new market players have entered the traditional enterprise telephony space, now redefined as *Enterprise Unified Communications*.

This reference architecture presents an overview of the network architecture and design considerations that support Juniper's vision of modern UC&C deployments. It can serve as a guide for network designers and administrators who are interested in architecting and building a network infrastructure optimized for UC&C applications.

Introduction

Increasing numbers of enterprises are deploying UC&C applications and services. This is not surprising since IP-based UC&C brings indisputable advantages—enhancing productivity, boosting corporate responsiveness, and reducing overall total cost of ownership (TCO). These important business benefits stem from:

- A single converged IP infrastructure for data, voice, and video
- Rich collaboration features (presence, IM, file sharing)
- Diverse endpoints (IP phones, soft clients on PCs, and smartphones)
- Centralized cloud-based applications that provide service to fixed and mobile endpoints virtually anywhere

IP technology is what powers UC&C, it represents an extremely powerful foundation, but one must pay close attention to a number of key challenges that allow UC&C to live up to its potential. Such challenges include:

- Security—Being open and flexible, IP communications are exposed to security threats.
- Quality of service (QoS)—As IP communications are built around a packet-based architecture, special means must be taken to achieve QoS comparable or superior to that provided by the legacy circuit switch telephony services.
- Reliability—As a business critical service, IP-based UC&C must satisfy stringent reliability requirements.
- Performance—The ability to provide all of the above for high volumes of real-time communications is critical for large-scale deployments.

In an enterprise environment, a solid network infrastructure is required to build a successful UC&C system. UC&C applications place strict requirements on IP packet loss, packet delay, and delay variation (jitter). Therefore, network administrators need to enable most of the QoS mechanisms throughout the network and ensure that the network infrastructure is high performing, resilient and secure, and adheres to open standards.

Juniper Networks has a long tradition of delivering high-performance, secure, and assured products, and when it comes to UC&C, these products play a paramount role. In addition, Juniper strongly believes in standards-based open networks. As such, it is one of the members of the Unified Communications Interoperability Forum (UCIF), ensuring that customers are free to build their UC&C networks using standards-based, interoperable building blocks.

Juniper Networks New Network for Collaboration is an approach that can help enterprises build the best network possible to run their UC&C applications and to connect people and information seamlessly and easily.

Major Trends in UC&C

The major trends in UC&C cover three predominant areas: bandwidth-hungry applications, Bring Your Own Device (BYOD) and mobility, and risk mitigation and compliance. Table 1 lists and defines these major trends associated with UC&C.

Table 1: Major Trends in UC&C

Major Trends	Definition
Bandwidth-hungry UC&C applications	Many new unified communications applications require more bandwidth. Many popular business applications such as Microsoft, Oracle, SAP, PeopleSoft, and video conferencing have introduced communication-enabled versions that require, in some instances, more than 10 times the bandwidth of their previous versions. As a result, this increased bandwidth requirement has seriously impacted performance, reliability, and availability. Other activities such as data backup to local servers can be bandwidth intensive as well. However, these activities can be scheduled to occur during times of low usage to reduce their impact on the network.
BYOD and mobility	Employee-owned consumer devices are making their way into the workplace, creating a new set of security, scalability, and management challenges for IT departments. User productivity increases as network performance and accessibility improve. The campus and branch networks should be leveraged with services such as wireless coverage and remote access to maximize productivity.
Risk mitigation and compliance	Critical UC&C resources should not only be protected from external threats but from internal threats as well. This protection should cover large, multiple LANs and provide high-performance capabilities in unison with LAN/WAN accessibility.

Unified Communications and Collaboration

Businesses have always used various tools to facilitate communication and collaboration between employees. Recently, technological developments in communication networking have permitted enterprises to effectively expand operations globally, while maintaining contact and collaboration using a variety of tools such as voice, e-mail, and video conferencing. The proliferation of additional tools such as IM, Web conferences, and content collaboration has increased productivity for these globally dispersed organizations.

Traditionally, all tools have their own deployment methods and architectures, and these often translate into costly and complex implementations. Ultimately, the result is limited deployment and availability of resources. At the application level, these communication and collaboration tools are integrated in unified platforms, and a variety of endpoints are integrating similar capabilities to simplify access and increase the usability and effectiveness of these tools.

Concurrently, the communication medium is being converged on IP networks, and the development of standardized protocols such as SIP and Real-Time Transport Protocol (RTP) has enabled this convergence. Networks are developing greater capability to support collaboration and communication tool integration into a single communication network to provide a cost-effective way to globally connect the mobile workforce, which improves productivity and increases operational efficiency.

In the following section, we review various communication and collaboration tools that are integrated to support UC&C. We present the infrastructure components that allow us to integrate these tools, and we cover the high-level requirements that allow us to connect this infrastructure, thereby providing an effective communication platform. In addition, we focus on network architecture requirements to support a communication platform that ensures performance, resiliency, reliability, security, and simplicity to connect a global workforce across various locations in today's enterprise.

Architecture

UC&C Solution Framework

Figure 1 depicts Juniper Networks UC&C solution framework, which consists of three layers:

- UC&C application
- UC&C infrastructure
- UC&C network

The network layer needs to be a high-performance, resilient, open, and secure layer that forms a solid foundation for supporting UC&C infrastructure and applications.

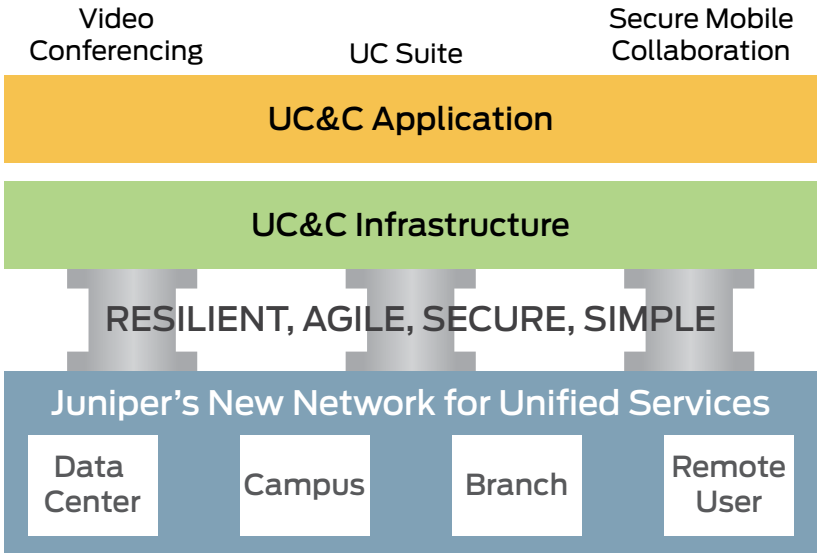

Figure 1: UC&C architecture

Juniper's approach to building networks with this model carefully considers the specific requirements created by UC&C applications and then builds the single best possible network to meet those needs. The network should have the following characteristics:

- High performance—UC&C applications are sensitive to latency and jitter. In some cases, especially with the increased adoption of video, these applications also require more bandwidth.
- Resilient—Business communications equal mission critical traffic and in a converged environment, applications can only be as reliable as the network. Juniper focuses on simplicity in the platforms and in the network architectures to deliver a truly resilient and available network to drive the user experience.
- Open—The network needs to be standards-based to ensure interoperability with any application or protocol that the enterprise chooses to adopt. Having this level of agility is key for enterprises that are looking to accelerate innovation and differentiate themselves competitively.
- Secure—It is imperative to have the ability to secure the UC&C application traffic, much like any other data application, to maintain privacy, security, and to meet regulatory compliance requirements.

With this network, enterprises are free to build various elements of their UC&C infrastructure, as well as adopt any number of UC&C applications to meet their needs. Juniper maintains broad and established relationships with many vendors in this space and has tested and validated configurations to validate and optimize performance and operations. This empowers our enterprise customers with freedom of choice for their UC&C solution, while maintaining confidence that the network can deliver these services and continue to ensure a rich user experience.

In this reference architecture, we refer to several products and technologies that are specific to our strategic partners, Polycom and Microsoft Lync. The concepts and recommendations outlined in this document are valid also with solutions from other vendors.

UC&C Applications

Today's global enterprise workforce uses various methods for communication such as e-mail, phone and video calls, IM, Web conferences, as well as various collaboration platforms for daily business operations. While many of these applications are enterprise owned and controlled, some of these applications are over-the-top (OTT) or free cloud-based services. The integration of these communication tools and collaboration services simplifies access to various tools and creates an environment that allows rapid collaboration in this fast-paced business world. The tight integration of various capabilities of e-mail, voice, and video communication, combined with IM and Web conferencing, simplifies the deployment model and enables additional functionalities such as endpoint devices to integrate various capabilities in a single platform. The UC&C platform provides access to integrated applications enabling voice, video, and various data communication capabilities. These applications primarily run on application layer protocols such as HTTP, SIP, and RTP that run on top of TCP/IP. In the following section, we review an infrastructure that supports UC&C services.

UC&C Infrastructure

The UC&C infrastructure integrates various applications providing many types of services into one integrated platform. This allows operators to leverage certain core services and information, while increasing efficiency and scale of specialized infrastructure services such as VoIP, video, e-mail, IM, and presence.

Unified services are enabled using the following core services:

- **Registrar and Call Routing Server**—The registrar server is responsible for registration of various endpoints. The registration process can identify the endpoint, provide necessary configuration options, store the location information and associated attributes in the location's database, and maintain the location database for the domain. Typically, a single registrar server manages the location information for the entire domain, and location information can be distributed to various locations for efficient call routing functions. We recommend that the registrar server function be deployed in a resilient architecture and in a central location such as the data center.

  The call routing server is responsible for receiving communication requests from various endpoints and for facilitating the request/response signaling between the communicating endpoints. This function is referred to as a proxy function. The call routing function, through a centrally located infrastructure service, enables efficient call signaling across a globally dispersed organization. This function can be integrated into the infrastructure to provide the call registration function.

  However, to enable scale for large deployment, a pool of call routing servers may be required. This pool of call routing servers also provides sufficient resiliency to efficiently provide call signaling between various endpoints.

  Increasingly, UC&C vendors are offering integrated registrar and call routing server functionality in a single hardware platform. Examples include Cisco Unified Communications Manager (CallManager) and Polycom Distributed Media Application (DMA) 700.

- **Session Border Controller**—The session border controller (SBC) enables communication between the user endpoints managed in a domain by a single registrar pool and by external domains. Session border controllers can be distributed across enterprise locations to efficiently manage call signaling and routing in closer proximity to the endpoints. In addition, they provide functionalities such as security, topology hiding, and QoS enablement, and they can be integrated with various media gateway services to provide media transcoding. Examples include AudioCodes Mediant 3000 E-SBC and Acme Packet SBC.

- **Media Gateway**—The media gateway enables call signaling and routing to existing PSTNs using multiple Foreign Exchange Office (FXO) or Primary Rate Interface (PRI) T1 types of traditional voice networks. The media gateway functionality can be distributed across various enterprise locations to provide efficient call routing. Examples include Avaya G450, G650, and AudioCodes' IPM blades and media resource blades.

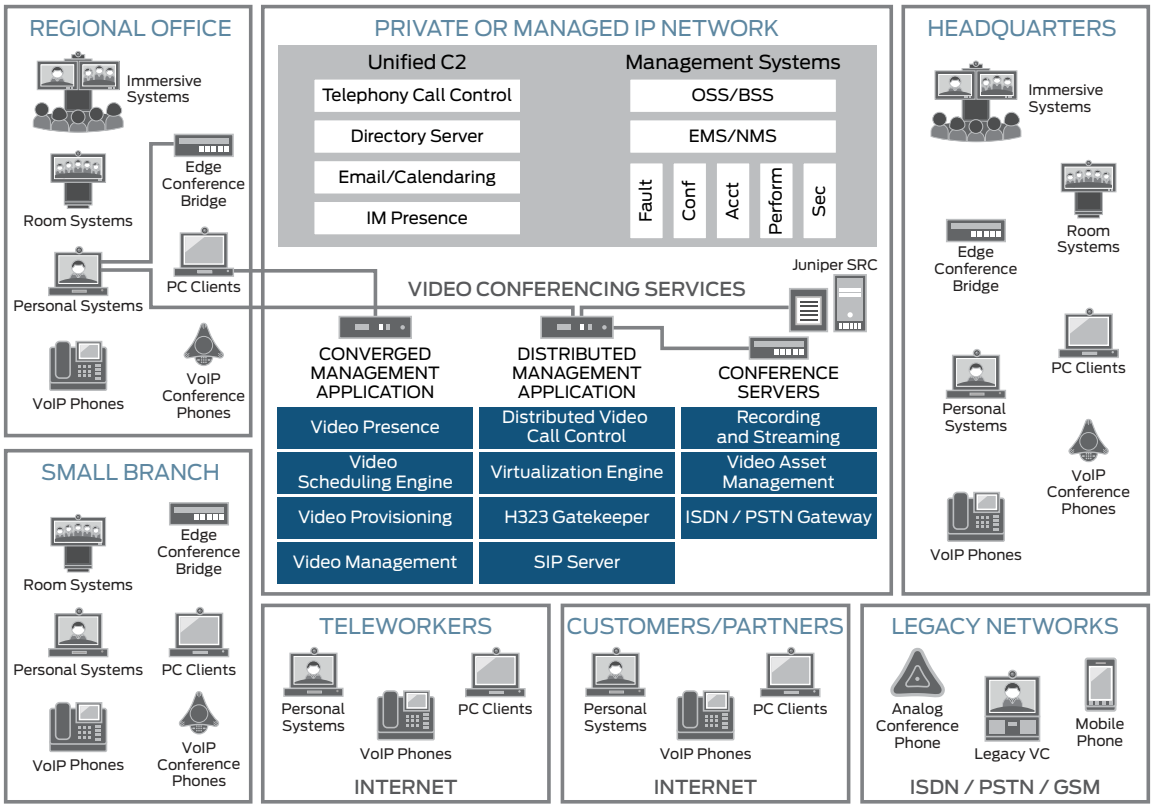

Figure 2: UC&C components and their location in the distributed enterprise

Video services infrastructure integration, combined with other collaboration services such as voice and e-mail, enable new methods of collaboration. The evolving, high-performance IP networks, with service guarantees for various types of services, allow integration of various collaboration services on the converged IP network. The following components primarily enable video infrastructure services:

- **Videoconference bridges**—UC&C video conferencing capabilities demand efficient use of network bandwidth and high-speed transcoding services. Developing and enabling HD video and video conferencing require distributed platforms to efficiently and in real time process voice, video, and content collaboration. Video conferencing bridges are specially designed hardware platforms that increase the processing speeds for this high volume data and maintain real-time communication.
- **Collaboration applications**—Voice and video collaboration services, combined with various data applications such as e-mail, IM, presence, and joint collaboration services like SharePoint and Web conferencing capabilities change the way today's enterprises can collaborate internally, as well as with partners and customers. These data applications have always run on IP networks, and with the convergence of voice and video services in a new collaborative platform such as Microsoft Lync, they open new possibilities for enhanced interaction.

The following identify several infrastructure components for data collaboration applications:

- **IM and Presence**—Rich presence and IM capabilities help workers find and communicate with each other efficiently and effectively. Integration with familiar Microsoft Office productivity tools and Microsoft SharePoint makes IM and presence a natural part of the everyday workflow, enhancing collaboration while making knowledge and expertise inside the organization readily accessible to all users.

  Presence establishes a user's personal availability by using common states such as "available" or "busy." With rich presence information, users can make more effective communication choices. A user's presence is a collection of information that includes availability, willingness to communicate, additional notes (such as location and status), and contact preferences.

  Enabling users to approach colleagues at the most convenient times using the most operative communication modality contributes to a more productive work environment. Contact management options allow users to control what information others can see, such as whether they are working from home, at a client's site, or simply unavailable.

- **Endpoints**—A variety of endpoints can be used in a UC&C deployment. These endpoints range from gateways that support ordinary analog phones in an IP environment to an extensive set of native IP phones offering a wide range of capabilities. When deploying endpoints, network administrators should consider several factors, including configuration, authentication, upgrades, signaling protocol, and QoS. The UC&C system must be designed appropriately to accommodate these factors.

For more information on technology alliance partners in the UC&C space, please refer to **www.juniper.net/us/en/company/partners/technology-alliances/unified-communications/**.

UC&C Network

In today's globally dispersed enterprise environments, the collaboration infrastructure components are hosted in resilient data center networks with a few strategic components distributed across the enterprise network to increase efficiency. The variety of endpoints where services are accessed reside at various enterprise locations in a fixed wired network or in a expanding mobile wireless network. In addition, the growth in users accessing such services remotely has increased with the expectation of consistent user experiences and service availability. The convergence of all these critical services on an IP network forces a high demand on the UC&C network for performance, resiliency, reliability, scalability, and security.

In the following section, we review the network requirements that are important to consider when designing and implementing an enterprise network that will support UC&C applications.

Network Requirements for UC&C Enablement

Connectivity—Ubiquitous Connectivity to Disparate Sets of Resources

As part of the enterprise campus and branch network design, the following critical aspects of network connectivity must be considered:

- The campus and branch LAN hosts a large population of end users that require high speed and highly available network connectivity to the resources residing at the data center and on the Internet. In addition, multiple LAN segments can exist and networks deployed that differ in security levels and other services offered.
- WLAN access is quickly becoming a preferred network access for various endpoints. Today's employees attend meetings with their laptops expecting wireless access to all of their applications, data stores, resources, and services. Not only must wireless service be provided throughout the campus, but it also should enable users to move across the campus seamlessly without service disruption, much like roaming cell coverage.
- WAN connectivity must enable campus users to access the data center, campus network applications, and Internet connectivity.
- Superior speed for campus network backbone connectivity, data replication, business continuity, and use of technologies such as MPLS must be provided.

Security

The network security architecture must employ layers of protection from the network edge through the core to the various endpoints for defense in depth. A layered security solution protects critical network resources that reside on the network. If one layer fails, the next layer stops the attack or limits the damages that can occur.

This level of security allows IT departments to apply the appropriate level of resource protection to the various network entry points based upon their different security, performance, and management requirements.

Layers of security that should be deployed in the network include:

- Denial of service (DoS) protection at the edge
- Firewalls to tightly control who and what gets in and out of the network
- VPNs to protect internal site-to-site communications traversing the public Internet
- Intrusion prevention system (IPS) solutions to prevent a more generic set of application layer attacks
- Insider threat protection through network access control
- Secure remote access to enterprise resources from anywhere and from any endpoint on the Internet
- Mobile Device Management (MDM) to maintain control over the diverse range of mobile endpoints

Management—Centralized Network Policy and Control

Unified Communications is dynamic in nature. Endpoints are diverse and may roam from office to home. The service typically is based in centralized data centers or in clouds with dynamic load balancing and geographic redundancy schemes. Managing such a service, including configuration and monitoring, is challenging if not performed with advanced techniques that automate most of the processes.

Policy-based networking is a powerful concept that enables devices in the network to be efficiently managed—especially within virtualized configurations—and used to provide granular network access control. The policy and control capabilities should allow organizations to centralize policy management and distribute enforcement. The centralized network policy and control management solution should ensure secure and reliable networks for applications and users as it provides appropriate levels of access control, policy creation, and network and service management.

Visibility

It is important to have visibility into network traffic and security events to effectively maintain and manage resources. It is also critical to collect IP traffic flow statistics to give enterprises insight into data flows, resource utilization, fault isolation, capacity planning, tuning, and offline security analysis. WAN utilization and user-level visibility can help IT better support application performance by leveraging network services and other resources. Network-wide visibility is crucial to a granular view of security events that helps determine how these events are handled.

Extending this visibility to develop a deeper understanding of application-specific traffic is crucial for optimizing network and application performance and thus ensures a rich end user experience. For example, specific compression and acceleration technologies can be applied at the network layer to accelerate e-mail applications such as Microsoft Exchange. Another example is preventing employee access to services such as YouTube and social networking sites from impacting business applications. Understanding these applications and enforcing policies based on the application ensures that business critical applications meet or exceed performance expectations of end users.

QoS, Latency, and Jitter

Unified Communications is real time in nature and includes voice services that replace traditional telephony. Consumers, and to a greater degree businesses, have stringent requirements for the level of call quality that a communications service must provide. Because UC&C runs over an underlying packet-based IP infrastructure, it may experience packet delay, jitter, or loss if the network is not engineered properly. When this is the case, call quality may degrade to unacceptable levels.

To truly assure UC&C application experience over large networks, QoS is a key requirement. It is critical to assign and manage QoS levels to ensure satisfactory performance of the various software applications, including UC&C applications that are sensitive to jitter, packet loss, and latency. Complex UC&C applications and infinite endpoints make QoS all the more important.

A minimum of three levels of QoS, each of which determines a priority for applications and resources, is as follows:

- Real time
- Business critical
- Best effort

These are especially critical with voice and video application deployments, because QoS can mitigate latency and jitter issues by sending traffic along preferred paths or by enabling a fast reroute to anticipate performance problems or failures. The campus network design should allow flexibility so that administrators can assign multiple QoS levels based on end-to-end assessment, and also allow rapid and efficient management to ensure end-to-end QoS for the enterprise.

High Availability

High availability (HA) disaster recovery is a key requirement for any network-based application in the enterprise network and must be considered not only in terms of what is happening within the LAN, but also by what is happening with connections to critical off-campus resources such as data centers and other branch locations. Network HA should be deployed using a combination of link redundancy (for both external and internal connectivity, and critical device redundancy to ensure uninterrupted network operations and business continuity. Moreover, devices and systems deployed within the confines of the campus network should support component-level HA such as redundant power supplies, fans, and Routing Engines. Another important consideration is the software/firmware running on these devices, which should be based on a modular architecture that provides features such as unified in-service software upgrade (unified ISSU) to prevent software failures/upgrade events from impacting the entire device. Software failures/upgrades should impact only a particular module, thereby ensuring system availability. For further information concerning disaster recovery, please refer to Secure L2 Stretch over L3 Networks Data Center Interconnection Implementation Guide at **www.juniper.net/us/en/solutions/enterprise/data-center/simplify/#literature**.

In the following section, we review how Juniper's new network addresses these requirements and connects all users at various locations to the services hosted in the data center.

Simply Connected for a UC&C Network

Figure 3 illustrates a high-level network diagram of simply connected for UC&C architecture that provides a communication network for converged voice, video, and real-time data applications, combined with other business applications.

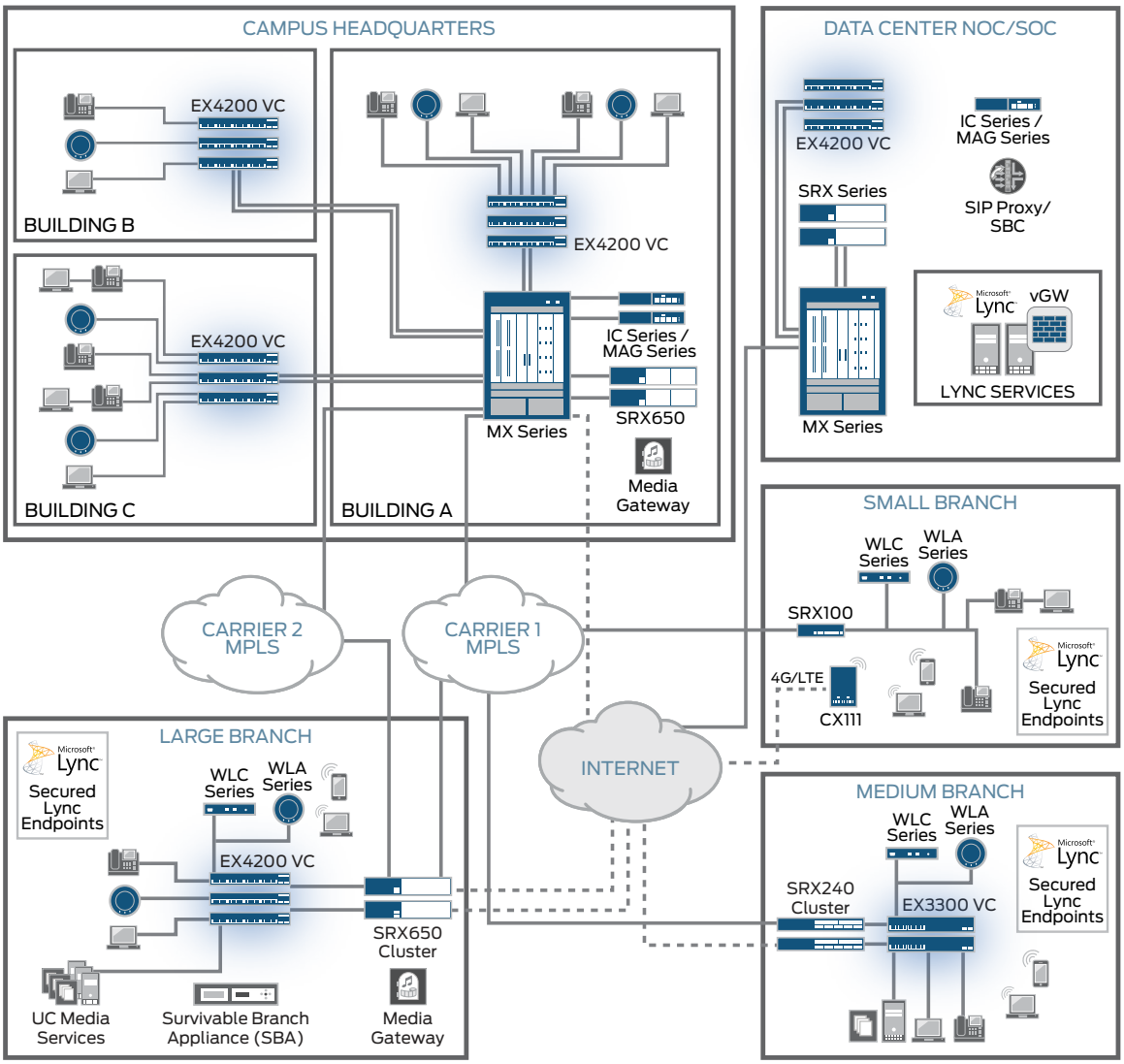

Figure 3: Simply connected network architecture

Campus

From a simply connected for UC&C solution perspective, a majority of users access the UC&C applications and services from their campus location. Thus, the campus network is a strategic location in the distributed enterprise helping to drive productivity, and it needs to be fast, secure, reliable, and scalable. The campus network has evolved from supporting traditional client/server data flows to supporting real-time application traffic such as video conferencing and multicast traffic flows, while accommodating the ever-increasing number of devices, services, and users.

At the same time, enterprise users have experienced a rapid shift in expectations. Today's enterprise users want to connect to the campus network with any device—be it their laptop, smartphone, or tablet. Being able to support more types of mobile devices while providing secure, pervasive connectivity with the mix of wired and wireless access that is right for your business is critical for success.

To help solve these campus challenges, Juniper provides:

- Mobility—Enterprise users can choose and change their access devices whenever they wish, allowing them to use their personal smartphones and tablets on the corporate network.
- Control—Network and security administrators can manage security by controlling who and what devices can access the corporate network with a simple, single client that works on most devices.
- Simplicity—Network administrators can simplify the wired network to improve performance and reduce complexity, while supporting the evolution to more wireless.
- Virtual Chassis in switching—Operators can reduce the number of physical and managed devices with Juniper Networks Virtual Chassis technology, where multiple switches can be managed as a single logical device.
- Nonstop wireless performance—Users can experience the same high performance on wireless as they do on wired Ethernet.

Figure 4 shows the functional tiers in a typical campus environment: access, aggregation core, security, and WAN edge.

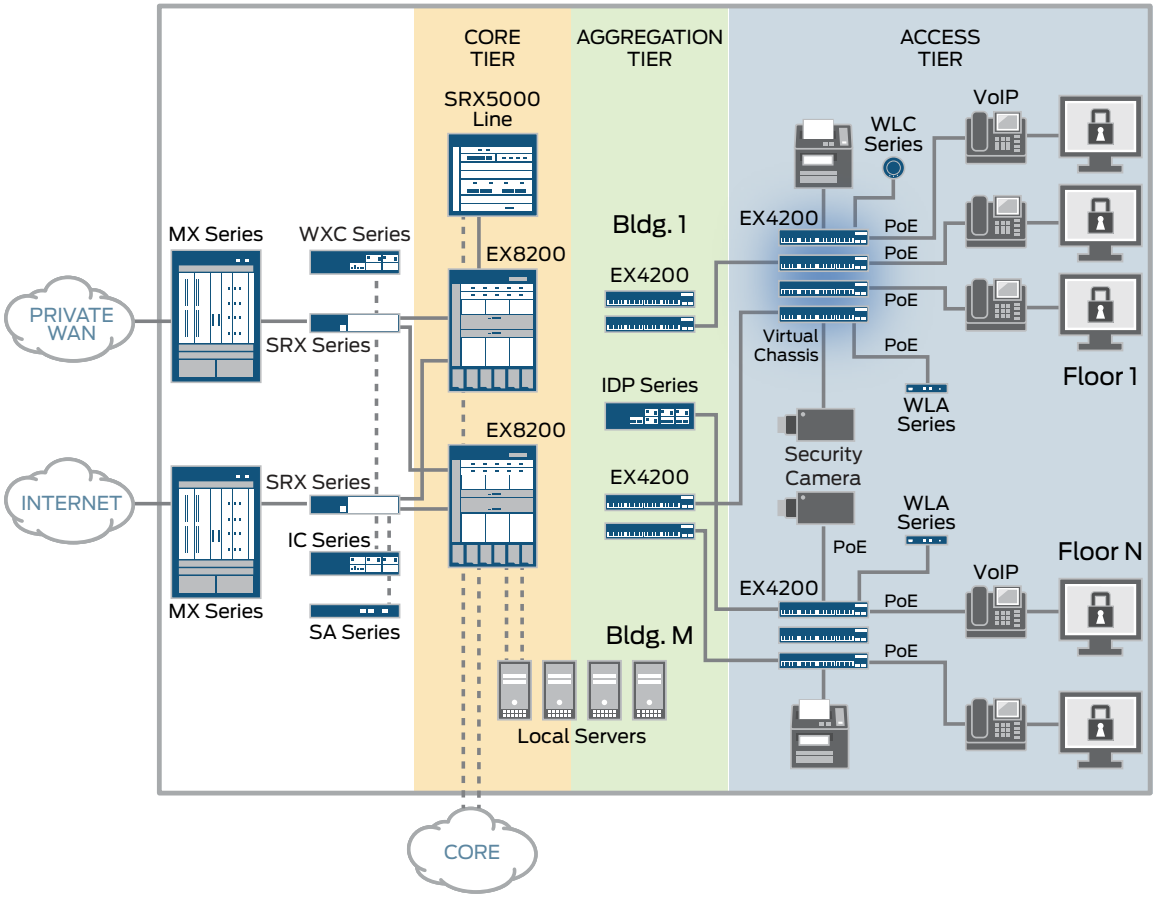

Figure 4: Typical campus network

Access Tier

The access tier consists of Juniper Networks EX Series Ethernet Switches with Virtual Chassis technology, and it provides connectivity to various endpoints such as laptops, desktops, VoIP phones, and video endpoints. A set of distributed wireless access points connects to various access tier devices, and these are managed centrally through a wireless access controller to provide seamless, mobile connectivity to campus users. The access tier devices connect to core tier devices using multiple links through link aggregation technology to provide higher throughput, as well as meet resiliency requirements. The EX Series devices in the access layer for wired access perform local switching, including Power over Ethernet (PoE) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED).

Wireless

Juniper Networks WLA Series Wireless LAN Access Points provide complete access point, mesh, and bridging services. They offer high performance and reliable mobility indoors and outdoors for any Wi-Fi device, enabling scalable deployment of wireless VoIP, video, and location services.

Juniper Networks WLC Series Wireless LAN Controllers enable seamless integration of reliable, scalable, and secure wireless LANs with existing wired infrastructures. A broad range of controllers serves installations of any size, delivering seamless mobility and nonstop wireless availability. Juniper Networks WLM1200 Wireless LAN Management Appliance unifies infrastructure, security, and services management, enabling network administrators to plan, configure, deploy, monitor, and optimize wireless networks of any size and geography from a single console.

Core Tier

The core tier consists of 10GbE EX Series Ethernet Switches (with Virtual Chassis) and provides simplified connectivity to all campus locations such as floors and buildings. The core tier provides the core routing function and integrates with security services and WAN services. The core tier can also be virtualized to meet the campus's segmentation and security requirements and provide required network agility.

Security Tier

The security tier consists of the security services gateway cluster using Juniper Networks SRX Series Services Gateways. The SRX Series devices are deployed in cluster mode to meet the resiliency requirements in the network. The SRX Series cluster provides security services such as stateful firewall and intrusion prevention. Unified access control is a standards-based, scalable network access control solution that is deployed enterprise-wide across all locations with enforcement points such as EX Series and SRX Series devices.

Juniper Networks Junos® Pulse is an integrated, multiservice network client that provides dynamic connectivity, security, and application acceleration through mobile or nonmobile devices, with a user experience that requires little or no user interaction. Junos Pulse provides identity and location awareness and can migrate seamlessly from one access method to another based on device location.

When deployed in conjunction with Juniper Networks SA Series SSL VPN Appliances and Juniper Networks Unified Access Control, Junos Pulse Access Control Service delivers fast, secure, anytime and anywhere network access, and it automatically migrates from one type of access such as remote access, to another or local network access based on the user's location. This functionality enables a rich and seamless end user experience.

The Juniper Networks MAG Series Junos Pulse Gateways deliver secure, remote, and mobile SSL VPN connectivity, network access control, and application acceleration for authorized users through a single converged gateway with a single enabling client.

For more information, please refer to **www.juniper.net/us/en/products-services/security/mag-series/**.

WAN Edge Tier

The core tier connects to a pair of Juniper Networks MX Series 3D Universal Edge Routers, which provide advanced routing services such as MPLS and integrate in a private MPLS WAN backbone. The traffic engineering capabilities of an MPLS network enables end-to-end QoS and can meet service-level agreement (SLA) requirements for real-time applications such as voice and video.

Assured Video Conferencing

From real-time desktop video and telepresence sessions to recorded meetings, application-driven network infrastructure resource controls are enabled by the integration of Polycom's Distributed Media Application (DMA) and Juniper Networks SRC Series Session and Resource Control Modules.

The network responds dynamically to the needs of the video service and makes network policy changes to ensure that every communication session goes through the network with the expected level of quality. This joint solution delivers higher network scalability, service reliability, and reduced day-to-day network administrative requirements for video services.

By dynamically allocating network resources, the SRC Series enables service providers to deliver differentiated products and services. The SRC Series modules provide a feedback loop between applications, users, and the network to connect the service layer to the network layer. Open interfaces allow integration with any network and any service offering, regardless of where the demand is generated.

Unlike competitive solutions that use authentication, authorization, and accounting (AAA) for policy management or deploy static policy enforcement, the SRC Series delivers granular dynamic policy enforcement on a per-service basis. This allows providers to deliver revenue-generating services on top of existing sessions. In addition, the SRC Series modules readily interface with existing subscriber management databases to facilitate the mapping of available network resources to subscriber and service profiles.

When an enterprise places a video call from the employee desktop, conference room, or from an immersive telepresence suite, the call is routed to Polycom's Distributed Media Application (DMA) in the service provider data center. DMA interfaces with the Juniper Networks SRC Series Policy Engine to correctly provision all devices on the service provider network for adequate bandwidth to accept the call and deliver it with assured quality. It then pushes the call parameters onto an available Rich Media Exchange (RMX) bridge located at the customer premises, which provides media processing for the duration of the call and integration of differing endpoint capabilities. Figure 2 shows UC&C components and their location in the distributed enterprise, as well as the Advanced Video Coding (AVC) components.

For more information on Juniper's campus reference architecture and assured video conferencing, please refer to the following:

- *Juniper Networks Horizontal Campus Validated Design Guide* at **www.juniper.net/us/en/local/pdf/design-guides/jnpr-horizontal-campus-validated-design.pdf**
- *Polycom® Solutions for Juniper Networks – Assured Video Conferencing* at **www.polycom.com/solutions/uc_environments/juniper/assured_video_conferencing.html**

Branch Offices

Branch offices are business satellite facilities that are geographically dispersed. Network connectivity is critical to branch business operations. Branch offices contain a relatively small amount of computing resources when compared to central facilities or data centers. Branch facilities generally are located where customer interaction occurs, which means increased demands on applications, network performance, and security.

Branch offices typically lack local IT staff, therefore the equipment hosted at these facilities must be cost-effective, feature rich, highly reliable, and offer centralized management capabilities. Because most enterprises employ far more users in branch offices than compared to headquarters, a branch office infrastructure must perform as well as the enterprise's headquarters network.

Most branch offices connect directly to headquarters using a private WAN link, a VPN over the Internet, or a VPN over a private WAN link.

Small Branch

A small branch consolidates routing, switching, and security into a single multifunction business gateway device. Juniper's SRX Series provides WAN routing and connectivity, security, and access control and switching services, including PoE and LLDP-MED to the UC&C endpoints.

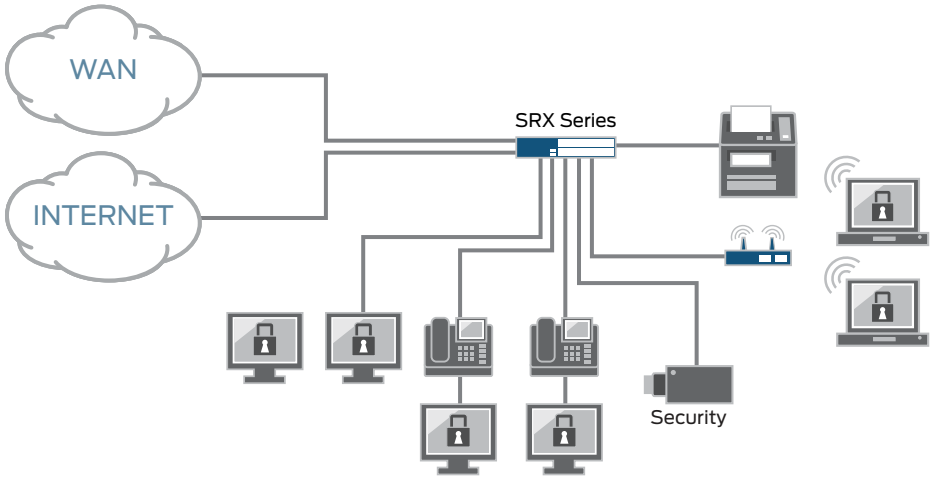

Figure 5: Small branch network architecture

Medium Branch

The optimized branch office includes a high availability pair of SRX Series devices that connect to one or more switches, which are deployed as Layer 2 devices. The SRX Series handles routing and security, while the EX Series performs local switching, including PoE and LLDP-MED. In the event of an SRX Series device failure, the network continues to operate on the backup SRX Series device.

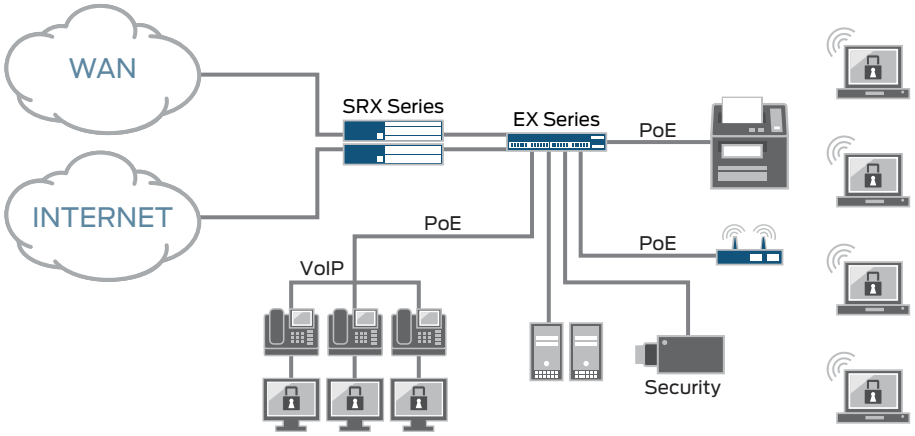

Figure 6: Medium branch network architecture

Large Branch

The critical large branch office includes a pair of high availability SRX Series devices that connect to one or more switches, which are deployed as Layer 3 switches using a Virtual Chassis configuration. The SRX Series handles routing and security, while the EX Series performs local switching, including PoE and LLDP-MED. If the primary SRX Series device fails, the backup SRX Series takes over as the primary, allowing continuous network operation.

For those enterprises that require local survivability, Juniper Networks has partnered with AudioCodes to offer that functionality. SRX Series Services Gateways, working in concert with AudioCodes MediaPack or Mediant Series survivable media gateways, provide highly reliable branch SIP-based VoIP solutions. These solutions combine Juniper's integrated PoE, switching, security, and QoS with AudioCodes' best-in-class media gateways and Enterprise Session Border Controllers (E-SBCs) to offer local survivability, FXS/PSTN, and SIP trunk connectivity. For more information, please refer to *Survivable VOIP Branch Solution with SRX Series and AudioCodes Gateways* at **www.juniper.net/us/en/local/pdf/solutionbriefs/3510411-en.pdf**.

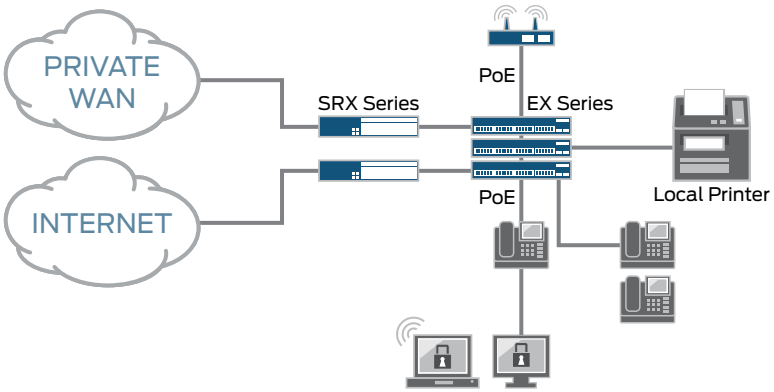

Figure 7: Large branch network architecture

For more information on branch office architectures, refer to Juniper's *Branch Office Connectivity Guide* at **www.juniper.net/us/en/local/pdf/app-notes/3500143-en.pdf**.

Connecting Branch Offices to the Data Center

With UC&C services following the general IT trend towards supporting services from centralized clouds, it is paramount that communications traverse the WAN securely and reliably at all times. This may require redundant or backup WAN connectivity to ensure availability of the IP network.

Traditionally, local backup options like TDM trunks and survivable call servers (SCS) have been used to provide communications in case of WAN connectivity failures. However, once the IP network proves to be trustworthy, these devices can be eliminated and a much simpler, consistent, and cost-effective architecture can be realized.

Redundant WAN Interfaces

Redundant WAN interfaces on the SRX Series, as well as multihoming with more than one service provider, dramatically increase the reliability of the connection between a branch and the centralized locations that provide UC&C service. Adding redundant interfaces allows network administrators to preserve the full UC&C user experience in the event of an outage, without deploying a separate survivable branch service with dedicated and costly PSTN connections at each branch.

Examples of this approach include a managed service provider WAN and Internet access as a backup, or a lower cost broadband connection to the Internet with a wireless WAN (WWAN) 3G or 4G Internet connection for backup.

High-Performance VPNs

WANs are commonly shared networks. This is true for the Internet and also for service provider private MPLS networks. Because most enterprises want to ensure the privacy and integrity of their communications while users traverse the WAN, it is imperative that the branch gateway supports high-performance, secure VPNs on any interface. The branch SRX Series supports hardware accelerated, high-performance IPsec VPNs that enable the secure communications of high volumes of data, voice, and video. Additionally, support for multiple IPsec tunnels and dynamic routing, including equal-cost multipath (ECMP) across the VPN and VPN monitoring services, enables a resilient and flexible VPN design when multiple WAN connections are deployed.

Figure 8 illustrates how the branch office connects to the data center with branch SRX Series Services Gateways using multiple WAN connections and VPN tunnels to support the always-up connectivity demands of UC&C.

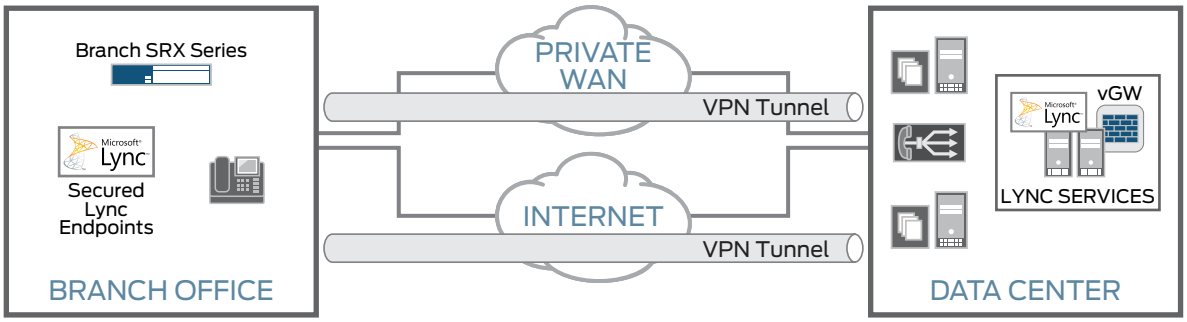

Figure 8: Branch connected to the data center using redundant WAN connections

Data Center

The data center is an essential corporate asset that connects all servers, applications, and storage services. Businesses rely on their data centers to support critical business operations and drive greater efficiency and value. As such, the data center is a key component of any UC&C solution because it hosts all of the UC&C-related servers.

The data center hosts the core infrastructure to provide a simplified central point of control for UC&C services. Typically, an enterprise data center is deployed across two physical locations to provide resiliency for core infrastructure services. The data center network is designed to provide high performance, reliability, resiliency, security, and agility.

The data center hosts UC&C core services with various types of redundancies built into the application and network layer. This includes all UC&C servers, video conferencing servers, and recording and streaming servers in the enterprise data center. UC&C core services require a high-performance, deterministic latency and failure resilient network to minimize the convergence time so that it is transparent to the end users.

Data centers must be planned and managed carefully to meet the growing performance demands of users and applications. Agility and scalability are key requirements to meet future capacity increases that ever-growing businesses demand. Data centers connect through a private WAN using MPLS technology. The MPLS WAN provides the necessary infrastructure to deploy UC&C core services in a resilient manner across multiple data centers, such as a Layer 2 extension across data centers using virtual private LAN service (VPLS) for call server cluster deployment and SQL replication. The traffic engineering capabilities of an MPLS network enable end-to-end QoS to help ensure bandwidth and latency requirements of such services.

Figure 9 summarizes the architecture for data center deployment. For detailed design considerations, design options, and implementation steps for the data center network architecture, please refer to the *Cloud-Ready Data Center Reference Architecture* at **www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf**.

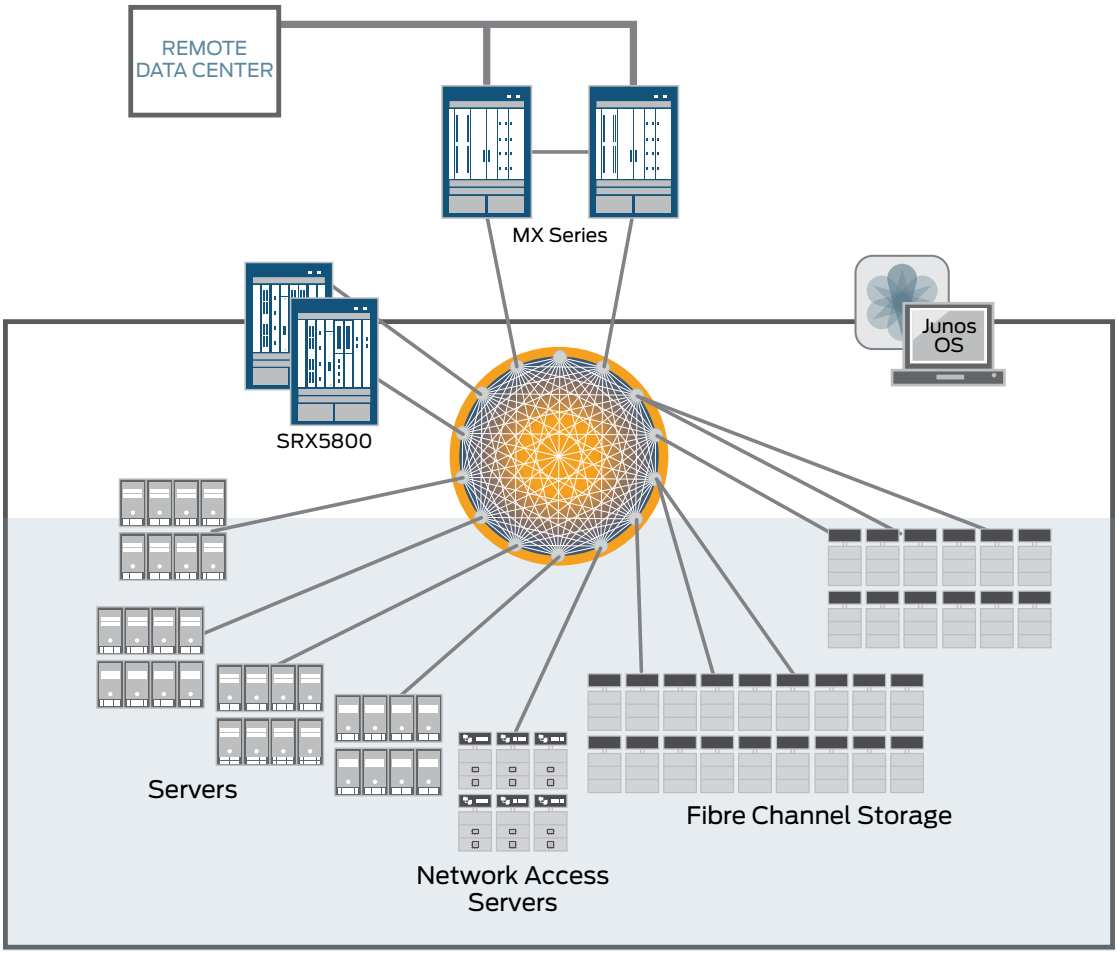

Figure 9: Data center reference architecture

Providing End-to-End QoS Using Junos OS QoS

As discussed earlier in the network requirements section for UC&C, QoS is critical for UC&C applications because these are real-time applications that are extremely sensitive to latency, jitter, and packet loss. From an UC&C end user perspective, QoS is experienced on the end-to-end (usually round trip) flow of traffic. However, it is implemented as a set of behaviors at each hop. This is an important distinction that is absolutely fundamental to QoS, and it is critical that readers thoroughly understand this point.

In effect, this means that a single hop with no configured QoS can destroy the end-to-end experience, and subsequent nodes are completely ineffective in recovering the end-to-end quality of the user experience. This does not mean that QoS must be configured at every hop. However, it is critical to understand that a single congested hop can be the undoing of the most intricate QoS design. Class of service (CoS) is a configuration construct used within the Juniper Networks Junos operating system to configure an individual node to implement certain behaviors at that node, such that the end-to-end QoS is consistent with the desired end-to-end user experience or application behavior.

To satisfy UC&C requirements, end-to-end QoS is required. Junos OS offers standards-based IETF Differentiated Services (DiffServ), which not only work well within their realm but also interoperate with other vendors' QoS implementations and Microsoft Lync. Junos OS provides a common language across Juniper's routing, switching, and security devices, which simplifies the QoS configuration and deployment for UC&C applications. For more information on QoS, please refer to *Day One: Deploying Basic QoS* at **www.juniper.net/us/en/community/junos/training-certification/day-one/fundamentals-series/deploying-basic-qos/**.

Network Security

Juniper Networks offers end-to-end security solutions that can protect all the critical elements of a UC&C deployment (network infrastructure, call control platforms, IP endpoints, and UC&C applications). Juniper's security solutions extend to various enterprise locations such as the data center, campus, and branch, and at the end user device level, thus providing multilayered security. The following highlights the functionality that Juniper's security solution provides:

- Dynamic and granular access control to prevent unauthorized access to UC&C services
- Threat protection for the UC&C infrastructure, such as protection against DoS or protocol fuzzing attacks
- Network security policy enforcement to administer effective UC&C policies for applications and users, such as general whitelists, blacklists, or specific SIP application-level gateways (ALGs) for dynamic firewalling
- Service protection to help ensure maximum uptime for UC&C applications
- Network-level encryption services that enable customers to encrypt signaling and media to prevent eavesdropping while maintaining security policies across distributed enterprise locations

Enterprise security issues are intensified by the increased mobility of network users, the BYOD phenomenon, the growing utilization of contractors, the colocation of partners on site, visiting guests, the proliferation of UC&C, and the demand for wireless access. IT must protect valuable enterprise resources from internal and external threats across large or multiple LANs with secure and ubiquitous LAN and WLAN access.

Increased security threats and risks force campus and branch LANs to remain secured and controlled on all fronts while providing open and pervasive access to maintain and increase productivity. The most effective security architecture to ensure maximum protection from network and application layer threats is based on multilayered protection that is appropriate for each location on the network. Holistic solutions that offer comprehensive security features, proven reliability, and exceptional performance are needed. IEEE 802.1X and network access control should be used to effectively handle unmanaged devices and guest users attempting network access, as well as to support unmanageable devices, post admission control, application access control, visibility, and monitoring. Firewalls and intrusion prevention systems also are needed to help ensure security across the LAN. In addition, QoS can be used as a security tool to identify, classify, and queue traffic. For example, QoS policies can protect access to departmental resources or ensure that high priority data flows are not impacted by malicious traffic. Figure 10 shows how external and internal threats can be stopped using IPS, ALG, and core security.

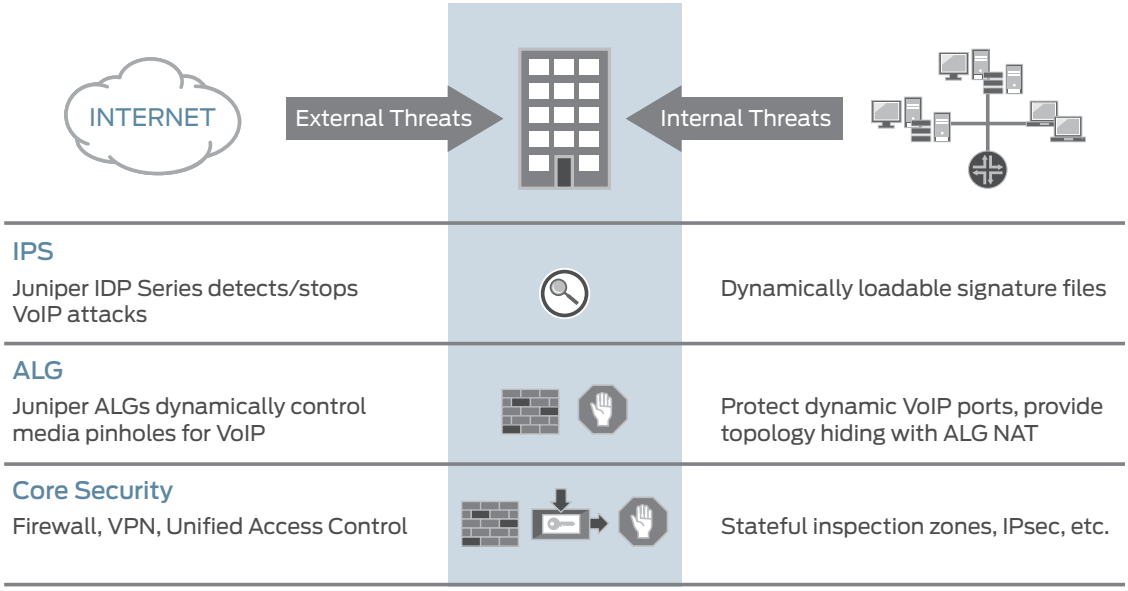

Figure 10: UC&C threat landscape

Multilayered security architecture facilitates network configuration by providing a modular design that can rapidly and economically scale based on the number of users in an enterprise environment. It also creates a flexible network where new security services can be added easily without a total redesign.

The basic idea behind multilayered security architecture is to protect the "crown jewel" (data center resources) with multiple layers of defense; if one device fails, another provides crucial protection. Another important thing to remember is that not every device can be defended, so our layered defense approach should be asset-centric rather than perimeter- or technology-centric. While focusing on an asset-centric layered defense approach is clearly important, we must not forget to protect users who access those assets as well. Therefore, we must protect the end user from not only external threats but also internal ones. This means that the endpoints must be secure at all times.

Access Control and Segmentation

The most vulnerable and most desired targets for attack in a UC&C environment are the endpoints themselves. Therefore, an initial line of defense is required to monitor who (and what) is coming in and out of the wired/wireless network. Authentication and access control should be in place to discourage opportunistic attacks from outsiders.

Authentication and authorization answers two very important questions—"who" is entering the network and "what" service is being delivered, respectively. Once the user and service is verified, the experience delivered for the application/service can be varied per user based on user subscription and profile. Device health and location data is then determined in order to deliver granular access control. Figure 11 shows basic segmentation in an enterprise campus.

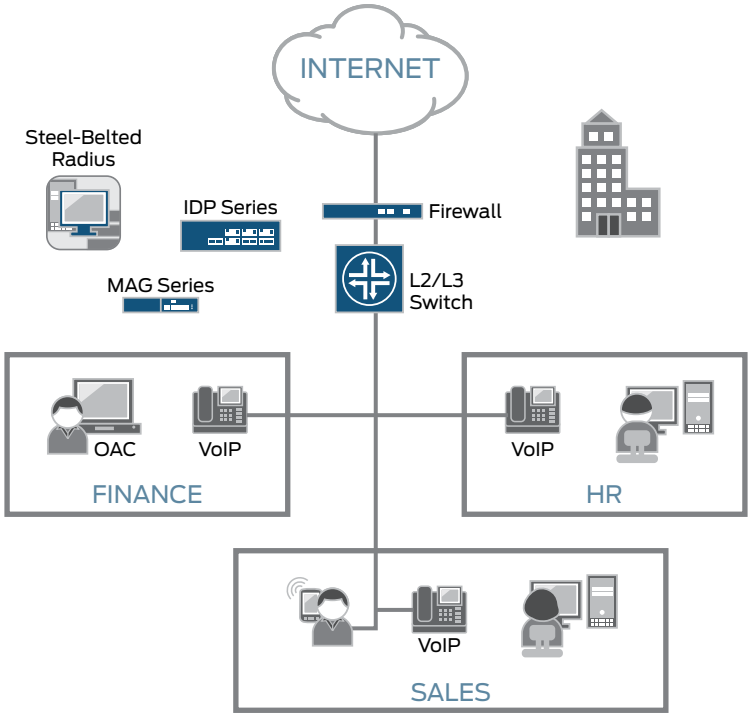

Figure 11: Security architecture in a campus environment

Holistic network access control should be deployed with support for all access technologies (wired, wireless, or remote access) so that only authorized users and applications from devices that adhere to your network security policies are permitted through the first layer. Endpoints (hosts) should be authenticated when they initially connect to a LAN. Authenticating endpoints before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server prevents unauthorized endpoints from acquiring access to the LAN. Network access control should provide both standards-based 802.1X port-level access and Layer 2 through Layer 4 policy enforcement based on user identity.

To achieve differentiated role-based access from internal networks, enterprises should segment the network. Also, the logical control points should be defined to control access to critical data, as well as contain any threat within the smallest segment of the network as possible. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and media access control (MAC) limiting should be leveraged to harden the access layer.

The network access control solution should combine user identity, device security state, and network location information for session-specific access policy by user and for leveraging the existing network infrastructure. The network access control should deliver comprehensive control, visibility, and monitoring, as well as be standards-based, reduce threat exposure, and decrease access control deployment costs and complexity. It should also be adaptable and scalable to meet the network access control requirements for campuses and branches of any size.

Enterprise campuses typically have a number of visiting guests and contractors accessing the network from outside on a daily basis. Because of this, the network access control solution should address the common problem of how to provide appropriate access to temporary guests by using a Web interface. Guests can be granted customizable, limited time access privileges on the network during the duration of their stay. Figure 12 shows an example of how network administrators can enforce endpoint health policies for all types of users.

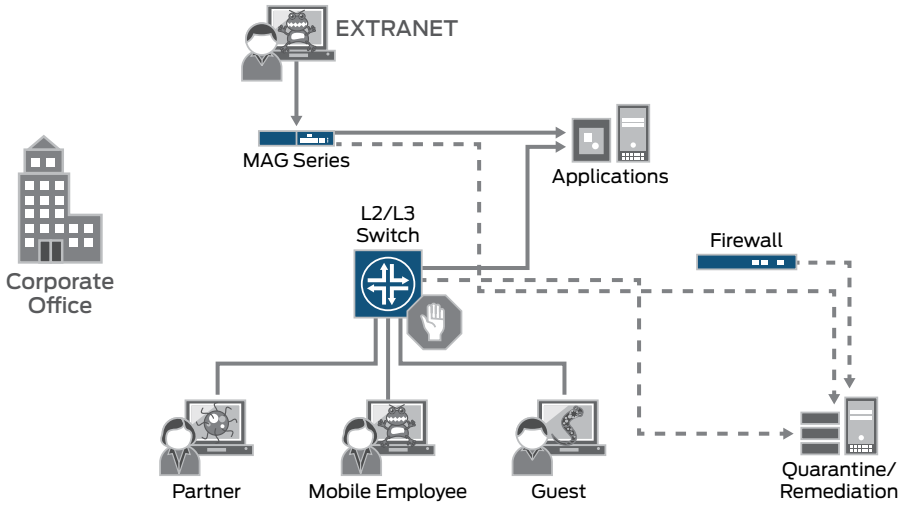

Figure 12: Enforcing endpoint health policy for all user types

The network and security infrastructure (switches, routers, wireless access points, firewalls) should integrate with inventory management and existing AAA systems, as well as network management and monitoring frameworks to gain unprecedented real-time visibility into the campus security environment.

For more information concerning Juniper's unified access control, please refer to **www.juniper.net/us/en/products-services/security/uac/**.

Stateful Firewalls and Router-Based Security

In this ever-changing threat landscape, smarter and more sophisticated attacks have the ability to penetrate the previously mentioned lines of defense. Thus, as an added layer, a sturdy firewall with stateful inspection is necessary.

These firewalls provide stateful inspection of traffic traversing different network segments. In addition, they should be able to create VPNs using IPsec for authenticating and encrypting IP packets to provide critical protection against DoS, distributed denial of service (DDoS), and other types of attacks deployed at the perimeter.

Firewalls must be scalable to handle increasing volumes of traffic when deployed at the network perimeter or at the core, so the network's performance is not negatively impacted during spikes.

Firewall security consists of several distinct features:

- Scalable performance—Leverages new services with appropriate processing capabilities without sacrificing overall system performance
- System and network resiliency—Provides carrier-class reliability
- Interface flexibility—Supports highly flexible I/O configuration and independent I/O scalability
- Network segmentation—Offers security zones, VLANs, and virtual routers, which allow administrators to tailor security and networking policies for various internal, external, and demilitarized zone (DMZ) subgroups
- Robust routing engines—Provides physical and logical separation of data and control planes to allow deployment of consolidated routing and security devices and to ensure security of routing infrastructures
- Comprehensive threat protection—Provides integrated security features and services that include a multi-gigabit firewall, IPS, DoS/DDoS detection and mitigation, Network Address Translation (NAT), and QoS.

In both wireless and wired campus networks, intelligent routers should be deployed to prevent IP spoofing. On the data plane, routers should perform anti-spoofing by implementing access control lists (ACLs) and IP fragment filtering to drop all inbound traffic with suspicious source IP addresses or IP address ranges.

Juniper Networks SRX Series Services Gateways are designed to meet the network and security requirements for

campus LAN consolidation, rapid services deployment, and aggregation of security services. For more information about the SRX Series, please refer to **www.juniper.net/us/en/products-services/security/srx-series**.

Application Layer Security

The most sophisticated network attacks require another logical layer of defense, namely an IPS. The IPS detects unusual or suspicious behavior on the application layer by using customizable signatures based on stateful protocol inspection, attack patterns, and behavioral learning. This capability is vital for enterprises seeking to protect their networks against penetration and proliferation of worms and other malware including trojans, spyware, keyloggers, and adware.

These systems should be designed to detect the presence of attacks within permitted traffic flow to the network by using stateful signatures that scan for attacks based on known patterns. Stateful signatures should be easily customizable in order to fit into different provider requirements and specific concerns.

Juniper Networks AppSecure™ is a suite of next-generation security capabilities for the SRX Series Services Gateways that uses advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network. Working in conjunction with the other security services of the SRX Series, AppSecure provides a deep understanding of application behaviors and weaknesses to prevent application borne threats that are difficult to detect and stop. As an integrated service, AppSecure provides the scalability to meet the requirements of the most demanding environments.

For more information on the standalone Juniper Networks IDP Series Intrusion Detection and Protection Appliances, please refer to **www.juniper.net/us/en/products-services/security/idp-series**.

For more information on the SRX Series AppSecure suite, please refer to **www.juniper.net/us/en/products-services/security/srx-series**.

Mobile Device Security

Today's enterprises are challenged with deploying mobile security and granular access control for a growing number of diverse mobile platforms, including Apple iOS, Google Android, Nokia Symbian, Microsoft Windows Mobile, and BlackBerry. With increasing choices of smartphones and other types of mobile devices, employees often bring their personal devices into the enterprise and use them to access corporate resources. When these devices are lost or stolen, enterprises risk losing sensitive corporate data such as e-mail and confidential documents.

The Juniper Networks Junos Pulse Mobile Security Suite creates a comprehensive solution comprising mobile device security and secure mobile access control. With this solution, enterprises can overcome the challenges of a heterogeneous mobile environment, as well as secure mobile devices from malicious attacks.

For more information, please refer to Junos Pulse Mobile Security Suite at **www.juniper.net/us/en/dm/mobilesecurity/**.

One Goal—Comprehensive Protection

In today's environment of constantly evolving threats, providers require solutions that can protect against unknown and known attacks. Many of the most significant threats involve "zero-day" attacks or unknown pattern attacks that leverage vulnerabilities where there is no signature or software patch.

Furthermore, while external threats such as trojans, viruses, worms, buffer overflows, and SQL injections are the most publicized, internal threats are often overlooked and may be more common than external threats. Implementing multilayered security helps to protect against both external and internal threats.

If one of the components of a comprehensive, multilayer security approach is missing, enterprise campus networks are easily vulnerable to a loss of network integrity, revenue, and even corporate reputation.

Juniper Networks end-to-end security solutions, supported by its integrated products, provide this high level of comprehensive protection to enterprise campus networks. For more information, refer to Juniper's enhanced security and compliance at **www.juniper.net/us/en/solutions/enterprise/security-compliance/**.

Network Management

Network management usually consists of a wide variety of tools, applications, and products to assist network system administrators, who face many challenges when provisioning, configuring, maintaining, and monitoring an enterprise network that consists of routers, switches, and firewalls. Network management systems help network administrators with various device management tasks, including fault-management, configuration, accounting, performance, and security (FCAPS) management, and they also provide programmable interfaces that developers can leverage to automate repeated tasks.

Automate—Ease of Management

To simplify network provisioning, monitoring, and maintenance, Juniper recommends several management tools to reduce network downtime, minimize human error, and accelerate service deployment:

- Junos Space Ethernet Design—Provides best practice service definition such as port security, QoS, and spanning tree to plan, simulate, model, and diagnose issues in the network.
- Junos Space Network Activate—Provides best practice service definition for enterprise-wide LAN services to quickly, accurately, and easily provision VPNs.
- Junos Space Route Insight—Provides a tool to easily plan, simulate, model, and diagnose issues in the MPLS network.
- Junos Space Security Design—Provides a tool to simplify deployment of firewalls and allows administrators to plan, simulate, model, and diagnose security issues in the network.
- Juniper Networks RingMaster software—Provides scalability and flexibility in WLAN deployment and has an easy-to-use interface. RingMaster covers the full lifecycle of a WLAN from planning, configuration, monitoring, and reporting with extensive troubleshooting, audit trail, and access control capabilities. RingMaster Global is a manager of managers, managing multiple RingMaster servers for a full deployment view. With this multiple RingMaster functionality, servers can manage regional sites with RingMaster Global providing a deployment-wide view for a maximum of 20 RingMaster servers (5000x20 = 100,000 access points).

Figure 13 shows an example of Juniper's key management automation tools.

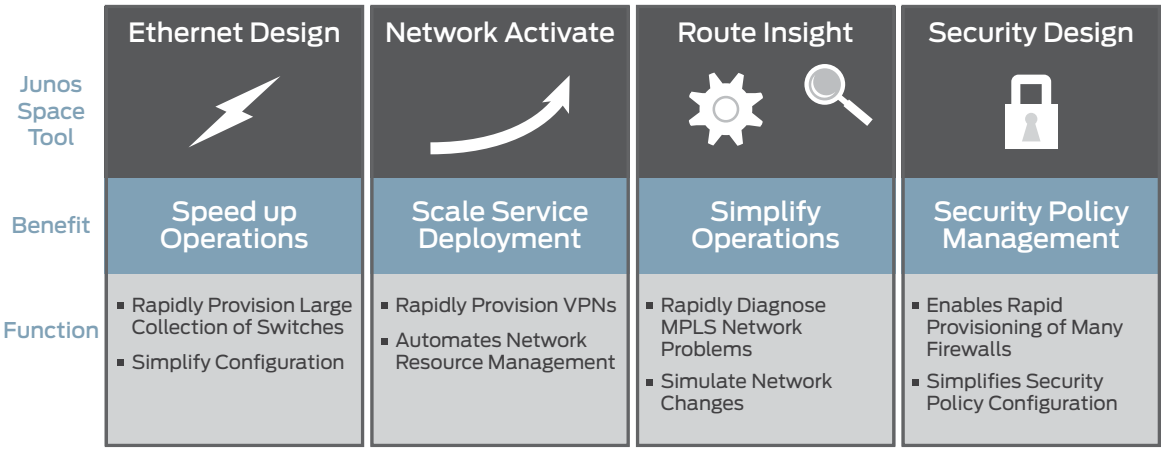

Figure 13: Junos Space Ethernet Design, Network Activate, Security Design, and Route Insight

In addition to network management tools, network architects can benefit from using powerful Junos OS scripts that can help network engineers simplify and automate tasks. The following script types include:

- Configuration scripts—Organizations that frequently change QoS policies that need to be propagated to many routers can use Junos OS configuration scripts. These scripts also ensure adherence to corporate network guidelines.
- Operation scripts—Organizations that want to simplify a series of iterative commands can benefit from creating a custom command using a Junos OS operations script. Enterprises also can create commands customized for specific solutions. These scripts reduce the risk of misconfiguration and improve productivity.
- Event scripts—Organizations can automate configuration changes to specific events with Junos OS event scripts. For example, security can be enhanced by controlling access to user accounts based on an employee's shift time.

Microsoft Lync and Polycom Partnership

Juniper Networks has validated this reference architecture with Microsoft Lync UC&C platform and Polycom endpoints. For further details concerning implementation, see the *Juniper Simply Connected for Unified Communications Services with Microsoft Lync and Polycom* at **www.juniper.net/us/en/local/pdf/implementation-guides/8010087-en.pdf**, and *The New Network for Collaboration—Optimizing UC&C Deployment with Microsoft Lync and Polycom* at **www.juniper.net/us/en/local/pdf/solutionbriefs/3510449-en.pdf**.

Conclusion

With today's ever increasing demands on global communications and collaboration, combined with a myriad of communication tools and end user types and devices, enterprises must deploy a suite of services that enable these communications tools to operate seamlessly over an IP-based network with high performance and a good user experience that is still cost-effective. Major trends in simply connected for UC&C such as unified communications, bandwidth-hungry applications, BYOD, and WAN/LAN security are forcing enterprises to consider a solution that addresses all of these challenges. To meet these challenges and deliver a secure IP network, Juniper offers a new end-to-end UC&C solution that provides a simply connected network for enabling UC&C applications (data center, campus, WAN edge, branch, remote user). This solution offers high performance, resiliency, and security with simplicity in deployment, management, and maintenance.

As a blueprint, this reference architecture illustrates how network administrators and architects can position and integrate Juniper's devices that support the infrastructure, offer services, provide policy and management, and integrate routing and switching in the data center at the most critical points on the campus network. These critical points include the access, aggregation core, security, WAN edge tiers, and most importantly, branch offices where security is critically important, as is the network administrator's ability to maintain high performance and an enhanced user experience. See Appendix A for details about these devices.

Appendix A: Enterprise Network Product Reference List

Table A-1: Juniper Networks Enterprise Products Reference List

Infrastructure		Services			Policy and Management	Integrated Routing and Switching
Routing	**Switching**	**Security/VPN**	**Access Control**	**WAN Optimization**	**Policy and Management**	**Integrated Routing and Switching**
M Series Multiservice Edge Routers MX Series	EX Series	SRX Series ISG Series Integrated Security Gateways NetScreen Series Security Systems IDP Series vGW Virtual Gateway	SA Series UAC Junos Pulse MAG Series	Riverbed (Technology Partners)	IC Series Unified Access Control Appliances Network and Security Manager NSMXpress Odyssey Access Client SBR Enterprise Series Steel-Belted Radius Servers STRM Series Security Threat Response Managers Junos Space SRC Series	SRX Series

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

8030010-001-EN Oct 2012 Printed on recycled paper