POWERING UNIFIED COMMUNICATIONS WITH BRANCH SRX SERIES SERVICES GATEWAYS

Analysis of the Optimal Branch Network Architecture for Successful Unified Communications in the Enterprise

Table of Contents

Table of Figures

Executive Summary

Unified communications (UC) including voice, video, and data is gaining increased momentum in the enterprise space. This is due to the clear advantages that UC brings to the enterprise—enhancing productivity, boosting corporate responsiveness, and reducing overall total cost of ownership (TCO). However, in order for unified communications to live up to its potential, it is important to understand that UC places different demands on the underlying IP infrastructure than traditional data applications.

This white paper is intended for enterprise management and IT technical staff. It describes the advantages that UC brings to the enterprise, including converged networks, rich collaboration tools, and dynamic endpoints online anytime and anywhere. It also introduces the key challenges that must be addressed in order to build a successful UC service. These include security, reliability, quality of service (QoS), and performance. Finally, it shows how Juniper successfully addresses these challenges by providing a powerful IP infrastructure that lets enterprises revolutionize their communications as they fully embrace UC. Settling for anything less than the best available IP technology results in expensive networks that attempt to compensate for their weaknesses with complicated solutions and provide an inferior user experience.

The focus of this paper is on the branch architecture and the key role played by Juniper Networks® SRX Series Services Gateways in that environment. The branch SRX Series is Juniper's next-generation secure router platform for small- to medium-sized offices, built on Juniper Networks Junos® operating system and industry-leading hardware. The SRX Series offers a combination of best-in-class routing, switching, and security—all in one product family.

In addition to the branch SRX Series, Juniper offers a comprehensive suite of products that provide a full solution for the enterprise. These include products scaled for branch, campus, and data center applications, all powered by the same Junos OS, providing unmatched consistency, better performance with services, and superior infrastructure protection at a lower TCO. For additional information, see relevant documentation for the high-end SRX Series Services Gateways, Juniper Networks EX Series Ethernet Switches, router product lines, and more.

Introduction

Enterprise telephony has come a long way from analog phones, legacy PBXs, and time-division multiplexing (TDM) trunks to converged IP networks with diverse IP phones, soft phones, centralized IP PBXs or UC servers, and Session Initiation Protocol (SIP) trunks for telecom network (PSTN) termination. New and rich services like presence, instant messaging (IM), file sharing, etc. have optimized the way members of an organization collaborate anywhere, anytime. And, new market players have entered the traditional enterprise telephony space now redefined as enterprise unified communications.

Increasing numbers of enterprises are deploying UC applications and services. This is not surprising since IP-based UC brings indisputable advantages to the enterprise, enhancing productivity, boosting corporate responsiveness, and reducing overall TCO. These important business benefits stem from:

- A single converged IP infrastructure for data, voice, and video
- Rich collaboration features (presence, IM, file sharing, etc.)
- 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 unified communications. It represents an extremely powerful foundation, but one must pay close attention to a number of key challenges in order to let UC live up to its potential. These include:

- **Security**—Being open and flexible, IP communications are exposed to security threats.
- **QoS**—As IP communications are built around a packet-based architecture, special means must be taken in order to achieve quality of service comparable or superior to that provided by the legacy circuit switch telephony services.
- **Reliability**—As a business critical service, IP-based unified communications 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.

Juniper has a long tradition of high-performance, secure, and assured products. When it comes to UC, these qualities 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), making sure that customers are free to build their UC networks using standards-based interoperable building blocks.

The branch SRX Series is Juniper's next-generation secure router platform for small- to medium-sized offices, built over Junos OS and industry-leading hardware. The SRX Series product line offers a combination of best-in-class routing, switching, and security all on one platform.

The balance of this paper will demonstrate how SRX Series Services Gateways can be leveraged to deliver enterprise IP networks that power secure, high QoS, reliable, and high-performance unified communications. Settling for anything less than the best IP technology will only result in an expensive network with a mix of complicated solutions and an inferior user experience.

Enterprise UC Architecture Overview

Enterprise Telephony Architecture Evolution

Figure 1 illustrates the evolution of the enterprise telephony architecture with the following high-level steps:

1. Analog phones and legacy PBX in the enterprise with a TDM connection to PSTN.
2. IP phones and IP PBX systems replace the legacy telephony equipment in the enterprise, while TDM interfaces are still used to connect to PSTN.
3. Legacy telephony equipment remains in the enterprise, while SIP trunks replace TDM interfaces for optimizing telephony toll.
4. Both enterprise communications and PSTN access are based on voice over IP (VoIP), eventually eliminating analog/TDM equipment altogether.

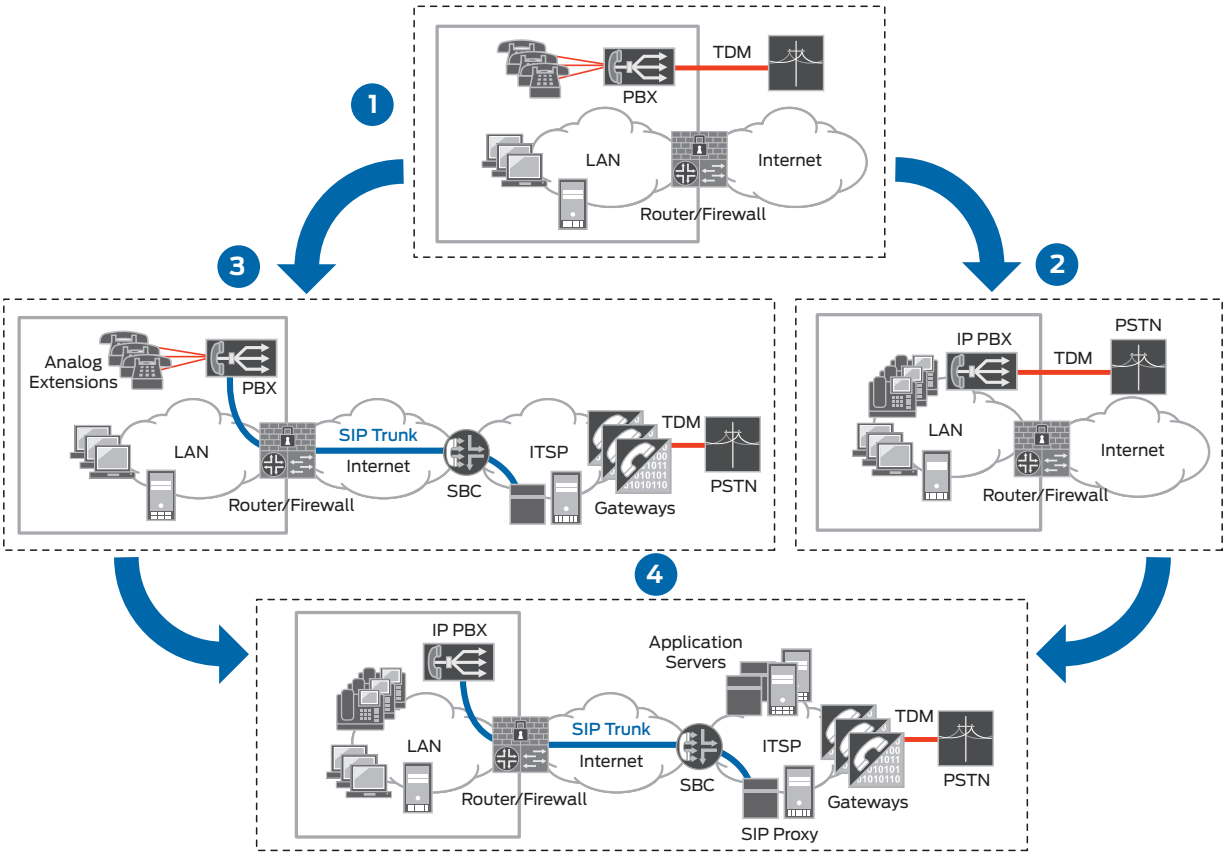

Figure 1: Evolution of enterprise telephony architecture

Modern Enterprise Unified Communications Architecture

The architecture displayed in step 4 of Figure 1 represents the modern enterprise architecture gaining increasing momentum in the market. It is based on the following key elements:

- All communications including data, voice, and video are based on a converged IP infrastructure, both within the enterprise as well as for PSTN termination. The role of TDM is being reduced to backup or emergency PSTN access purposes and will eventually be eliminated altogether.
- Centralized UC services are provided from centralized data centers in one of the following models:
  - Enterprise-owned—the enterprise owns the UC service equipment and is responsible for operating the service.
  - Managed—the UC service equipment is placed at the enterprise's premises but is managed by a UC service provider (the enterprise may or may not own the UC equipment).
  - Hosted—the UC is hosted on the service provider premises and managed by that service provider.
- UC endpoints range from IP desk phones to soft clients running on PCs or smartphones. They can connect to the UC service from almost anywhere, including office locations, home offices, and in travel.
- SIP trunks have become the de facto standard for connecting UC between two separate IP networks such as the enterprise network and the service provider network.

Unified Communications Challenges

Unified communications holds great promise for the enterprise in terms of enhanced productivity and reduced TCO. However, enterprise UC architectures must successfully address a number of key challenges for UC to deliver on its potential.

Security

Unified communications is about connecting anyone, anywhere over standards-based open IP protocols. This means that a UC service may directly interact with diverse endpoints (different brands, soft clients installed on smartphones or PCs) from diverse locations which can include the enterprise LAN, or wireless local area network (WLAN), or an Internet café. The service may also peer with SIP trunk service providers all over the world, and it is very common for the traffic to be carried over shared WANs either owned by a service provider or available over the Internet. In addition, UC is a dynamically growing market where new services pop up every day, and underlying technology and IP-based protocols evolve correspondingly.

The combination of being open, rich, flexible, and dynamic is what makes UC so exciting, but at the same time it exposes UC to security threats such as:

- Denial of service (DoS)—denying or disrupting the UC service using attacks that include flooding UC servers with messages, sending malformed messages, or spoofing messages
- Confidentiality breach—eavesdropping on calls or obtaining related information such as call records
- Fraud—service theft and phishing

Quality of Service

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

Reliability

Unified communications is critical for the success of the business, connecting employees, partners, and customers. Failure of this service may result in significant loss of business for the enterprise; therefore, it is expected to be highly reliable with 99.999% (five nines) being the common expectation for availability.

Performance

High volumes of real-time communications require high-performance networks to carry traffic with no service-level degradation, while still maintaining stringent security.

Management

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

Introducing SRX Series Services Gateways for the Branch

Juniper Networks SRX Series Services Gateways for the branch are secure routers that connect, secure, and manage workforce locations from a few to hundreds of users. By consolidating fast, highly available switching, routing, security, and applications capabilities into a single device, enterprises can economically deliver new services, secure connectivity, and provide a satisfying end user experience. Figure 2 illustrates the SRX Series for the branch product line.

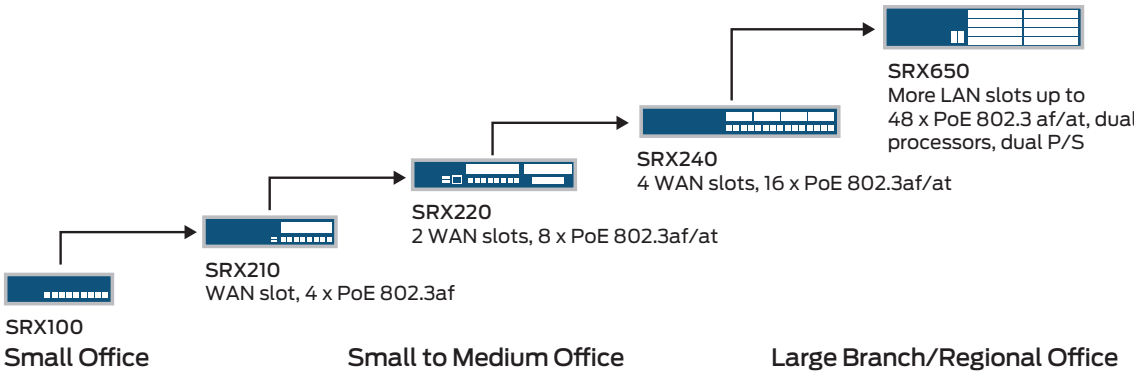

Figure 2: Branch SRX Series

All SRX Series Services Gateways are powered by Junos OS—a proven platform providing unmatched consistency, performance, and superior infrastructure protection at a low total cost of ownership. This is also true for Juniper Networks EX Series Ethernet Switches for the enterprise LAN, J Series Services Routers, M Series Multiservice Edge Routers, and MX Series 3D Universal Edge Routers, including products scaled for branch, campus, and data center applications.

Connecting UC Endpoints to the Enterprise LAN

Connecting UC endpoints to the enterprise LAN should be as straightforward as possible and at the same time provide proper authentication and authorization capabilities. Figure 3 illustrates how UC endpoints connect to the enterprise LAN and WLAN with the branch SRX Series and the Juniper Networks AX411 Wireless LAN Access Point.

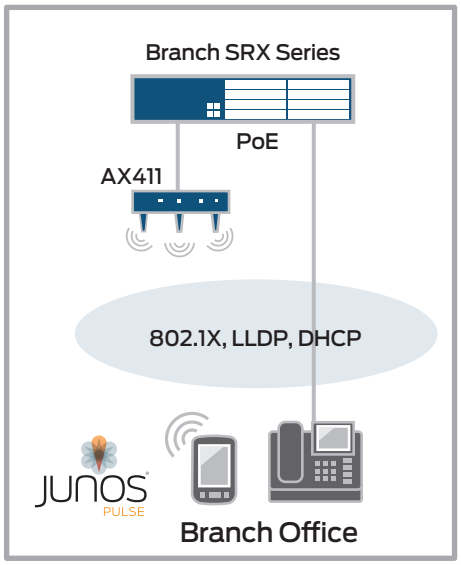

Figure 3: Connecting UC endpoints to the branch SRX Series

Powering UC Endpoints

Power over Ethernet (PoE) ports provide both LAN connectivity and power to UC endpoints such as IP phones, security cameras, etc. All branch SRX Series Services Gateways support PoE—from a few built-in ports in the low-end platforms to modular LAN slots with up to 48 ports in the high-end. For branches that require higher PoE port densities, it is easy to extend these numbers with switches from the EX Series product line.

Securing LAN Access

To protect the converged IP infrastructure from unauthorized users and devices, LAN switches must support network access control based on open standards, including the Institute of Electrical and Electronics Engineers (IEEE) 802.1X and the Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP).

In addition, LAN switches must be capable of participating in policy architecture to ensure that security is consistently applied. For example, edge switches must have the ability to identify and authenticate users and devices such as IP phones, and to enforce the appropriate security and access controls based on policies provisioned by a policy server.

Both EX Series switches and the switched ports of SRX Series platforms support this critical, standards-based LAN access security scheme, and they integrate with policy servers such as Juniper Networks IC Series Unified Access Control Appliances as part of Juniper Networks Unified Access Control framework.

For the client side, Juniper provides the Juniper Networks Junos Pulse soft client. Junos Pulse is an integrated, multiservice network client that provides dynamic connectivity, security, and application acceleration through mobile or non-mobile devices, with a user experience that requires little or no user interaction. It is identity- and location-aware, and seamlessly migrates from one access method to another based on device location.

WLAN Access

UC endpoints often run on wireless devices such as laptops and smartphones. To securely connect these devices to the enterprise's WLAN, Juniper provides the Junos Pulse soft client, as well as the AX411 Wireless LAN Access Point that connects to SRX Series Services Gateways.

The AX411 is a high-performance, 802.11a/b/g/n wireless LAN (WLAN) access point. It is a dual band, dual radio solution that supports data rates up to 300 Mbps. The AX411 is fully managed by branch SRX Series Services Gateways.

Auto Sensing and Provisioning of UC Endpoints

Link Layer Discovery Protocol (LLDP) is a standards-based protocol that lets network devices in the LAN advertise their identity and properties. LLDP Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that includes support for auto sensing UC endpoints and the application of QoS policies, assigning VLANs and DiffServ code point (DSCP) settings accordingly in order to guarantee high quality communications. PoE power management and E911 device location are also supported as part of LLDP-MED. Both SRX Series and EX Series platforms support LLDP and LLDP-MED.

Dynamic Host Configuration Protocol (DHCP) is commonly used to automatically provision network devices. SRX Series Services Gateways support both standards-based and vendor-specific DHCP options for automatically configuring IP phones.

Connecting the Branch to the WAN

With UC 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. Once the IP network proves to be trustworthy, local backup options like TDM trunks and survivable call servers can be eliminated and a much simpler, consistent, and cost effective architecture can be realized. Figure 4 illustrates how the branch office can be connected to the WAN with branch SRX Series Services Gateways. The following sections explain this in more detail.

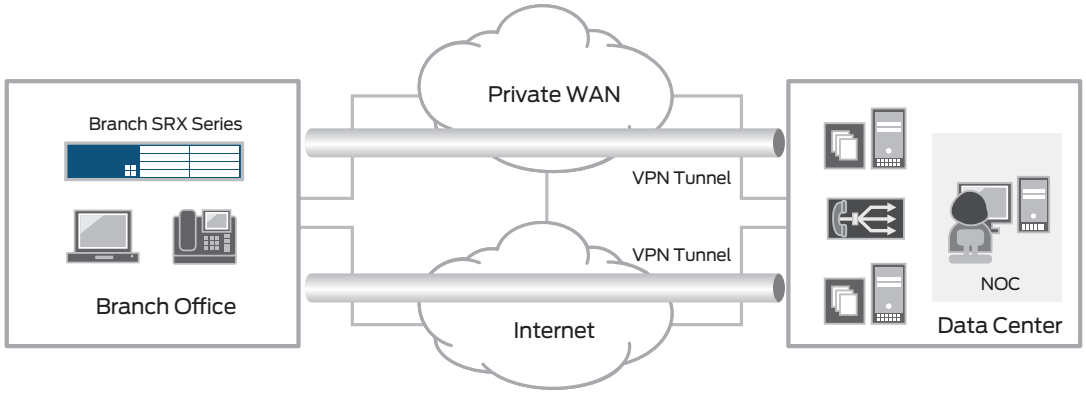

Figure 4: Connecting the branch to the WAN

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 from which the UC service is provided.

Examples for this approach include a managed service provider WAN with Internet access as a backup, or a DSL broadband connection to the Internet with a third-generation (3G) link for failover.

High-Performance VPNs

WANs are commonly shared networks. This is true for the Internet and also for service provider private MPLS networks. Since most enterprises wish to ensure the privacy and integrity of their communications while traversing the WAN, it is imperative that the branch gateway supports high-performance, secure VPNs. The branch SRX Series supports hardware-accelerated, high-performance, IPsec VPNs that enable the secure communications of high volumes of data, voice, and video.

Connecting Remote Workers

In today's dynamic workplaces, many workers work from home or telecommute while travelling across the globe. In order to facilitate this, the enterprise must provide the means for these workers to remotely connect to the enterprise network in a secure manner.

Juniper customers can leverage dynamic IPsec VPNs running between a UAC device or Junos Pulse soft clients and an enterprise gateway. That gateway can be a high-end SRX Series gateway or secure appliance at headquarters, but can also be a branch SRX Series gateway. This gives the worker the flexibility to connect to the closest gateway and optimize network paths to achieve the best results, especially for real-time UC. Figure 5 illustrates this architecture.

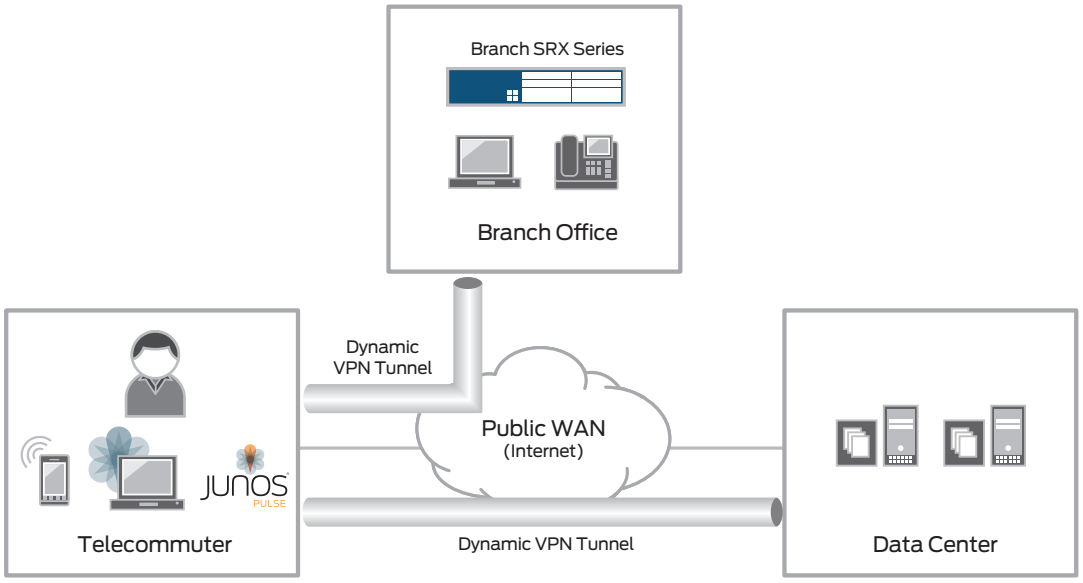

Figure 5: Connecting remote workforce to the enterprise

Optimizing Security

As already mentioned previously in this paper, security is imperative in order for enterprises to be able to leverage open unified communications. This section highlights the comprehensive security that is integrated into the SRX Series for the branch.

High-Performance Firewall

SRX Series Services Gateways have been built with best-in-class routing and firewall in one product. As such, they support advanced firewall capabilities that include zone segmentation, access lists, protocol stateful inspection, and more. These capabilities ensure that access to UC endpoints and any other gateway or server in the branch is protected and restricted according to administrator policies. For example, a "guest" zone used for "untrusted" Wi-Fi endpoints in the branch's WLAN, or an "untrusted" zone used for Internet traffic will usually have restricted access to other devices on the enterprise network.

Intrusion Prevention System

The branch SRX Series offers the latest capabilities in inline network intrusion prevention system (IPS) functionality to protect the network from a wide range of attacks. IPS includes UC-specific attack signatures (such as SIP signatures) that can be updated on a daily basis as part of the IPS signature database with industry-leading response times for maximum protection of network resources.

Application-Level Gateways

Application-level gateways (ALGs) are available on the branch SRX Series for various UC-related protocols such as SIP. ALGs inspect the UC signaling and dynamically control firewall pinholes to allow only authorized media flows through the firewall. ALGs can also perform Network Address Translation (NAT) to the signaling protocols such that the network resources behind the ALG are completely hidden (topology hiding).

Optimizing Quality of Service

Users of UC services expect excellent voice and video quality while simultaneously accessing applications and data. To meet user expectations and deliver full value to the enterprise, UC-based services and applications must have consistent and predictable performance. Achieving this requires that a common set of robust QoS mechanisms be supported end-to-end across the LAN and WAN.

All SRX Series Services Gateways provide eight hardware-based class-of-service (CoS) queues on every port, as well as a common set of queuing, traffic shaping, and congestion management algorithms. With these mechanisms, enterprises can accommodate numerous classes of traffic and define very granular QoS policies.

The way an individual traffic flow is handled depends on its markings and associated QoS policies. SRX Series Services Gateways can apply standard IEEE 802.1p markings at Layer 2 and IETF DSCP or IP precedence markings at Layer 3. An SRX Series gateway will identify incoming traffic, match it against a QoS policy list, and mark it for appropriate handling by subsequent network devices. Beyond these standard marking techniques, Juniper gives enterprises the flexibility to classify and mark traffic based on its ingress port, IP or media access control (MAC) address, VLAN tag, TCP/UDP port number, or any combination of these attributes. QoS policies can be dynamically applied to ports based on information coming from LLDP or 802.1X protocols.

Conclusion

Unified communications including voice, video, and data brings clear advantages to the enterprise, enhancing productivity, boosting corporate responsiveness, and reducing overall TCO. However, in order for UC to live up to its full potential, it is important to understand that UC places different demands on the underlying IP infrastructure than traditional data applications. A successful UC service must be built over a powerful IP network foundation with high performance, security, reliability, and consistent end-to-end QoS.

Furthermore, with UC following the IT trend of centralized cloud-based services, distributed enterprises must pay special attention to their branch architecture. The architecture must be such that there is a consistent and high-quality experience available to workers anywhere, anytime. This needs to be addressed by fortifying the IP infrastructure to securely and reliably connect all workers wherever they are located. Settling for anything less than the best IP technology inevitably results in expensive networks that attempt to compensate for their weaknesses with complicated solutions, and often provide an inferior user experience. Figure 6 illustrates this architecture choice.

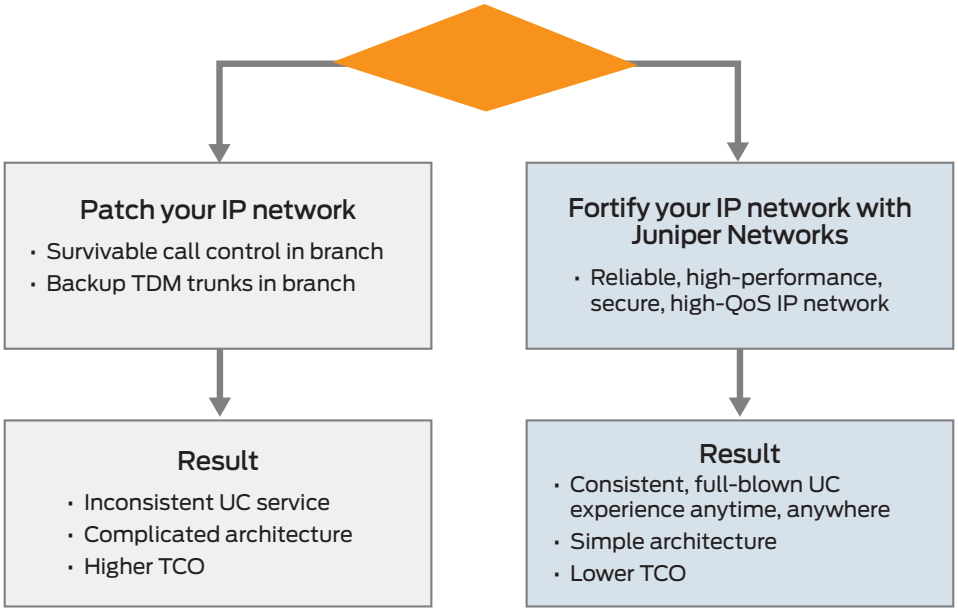

Figure 6: Alternative paths to enable UC over the enterprise network

The branch SRX Series offers a combination of best-in-class routing, switching, and security all in one platform. Addressing all aspects of UC enablement, it is the ideal platform to power unified communications in small- to medium-sized enterprise branch offices.

The SRX Series is part of Juniper's full product portfolio for the enterprise, including switches, high-end edge routers, and more. All are based on the same Junos OS—the proven operating system that provides unmatched consistency, better performance with services, and superior infrastructure protection at a lower TCO.

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.

2000373-002-EN Mar 2012 Printed on recycled paper