Juniper Networks | Engineering Simplicity

Reference Architecture: Enterprise WAN Network Design

Published
2023-10-16

RELEASE

Table of Contents

About This Guide

This document describes how to build cost-efficient and self-driving network solutions for remote offices. It shows how to set up primary WAN and backup LTE connections on SRX Series Services Gateways. You use these connections to provide wired and wireless Internet and Intranet access to employees on-site, as well as wireless Internet access to guest devices.

RELATED DOCUMENTATION

> https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-183-branch-in-a-box.pdf

Introduction

IN THIS SECTION

The network is a key component in the success of a modern Cloud ready and Edge Compute ready enterprise because it connects sensors, devices and users to business applications and services. A fast and reliable WAN service that connects all of an organization's offices is no longer a luxury—it is crucial to business success. The productivity of a workforce can be attributed to and enhanced by the quality of the enterprise WAN network.

As the WAN has grown and become more important, the operational and financial challenges of operating the network have become more of a burden to organizations. The challenges of operating the WAN need to be addressed in a way that enhances not only performance and reliability, but also security, privacy, and compliance. A complete enterprise WAN network architecture can effectively address these growing challenges. Several trends in the enterprise have had an affect on complexity, network performance, and scale. The following sections cover these trends.

Centralized Cloud Data Centers

A first trend is centralized cloud data centers and the distribution of content. In the past, applications, data, and content were largely localized—users needed access to a local email server and database and could, for the most part, perform their duties without impacting the WAN.

Today, many enterprise applications and data are stored in either centralized data centers or in a hybrid cloud and accessed via constrained and often oversubscribed WAN links. This centralization of enterprise applications and data has strained the traditional model of WAN access, which was to provide low bandwidth and oversubscribed links to remote sites. The growth of bandwidth requirements, not only for connected devices but for business-critical applications, has led the enterprise to seek new ways to deal with the WAN and its design and performance.

Edge Compute

The second trend is edge compute driven by the need to lower application response times and the cost associated with sending data round-trip to a centralized cloud for every transaction. With the compute moving closer to the edge and closer to the consumer of data only the essential subset of data is sent to the centralized cloud for latency critical applications. This is not only driving bandwidth growth as traffic travels between the edge and the cloud, but also placing higher demands on WAN performance. This is leading enterprises to reconsider their WAN design.

Explosion of Internet–Connected Devices

The third trend is the explosion of Internet–connected devices. A decade ago, the enterprise needed to deal only with computers and other directly connected devices that were standardized and issued by the IT department. Today, every user has a smartphone, tablet, and laptop—often their own—that require an Internet connection. Each of these devices consumes a great deal of bandwidth and can impact network performance. While some enterprises ignore this traffic impact, the pressure to keep the workforce happy and productive has forced many enterprises to adopt a “bring-your-own-device” (BYOD) policy and use Wi-Fi and security policies to enable network access to all of a worker’s devices. Enterprises must build a network that can not only handle the bandwidth requirements of today’s devices, but also expand to handle the exponential growth in bandwidth consumption over the next 5 to 10 years.

Enterprises Needing to Operate as Service Providers

A final trend is the view that enterprises should operate like service providers, treating the organization as customers for their services and meeting high standards for service delivery. Treating large enterprises as a service provider poses great challenges to the traditional WAN designs and architectures.

Many companies choose to build completely private WAN clouds, while others look to build hybrid networks that give them control and management of strategic portions of the network instead of relying solely on an outside provider. This movement introduces a great deal of complexity, especially for the traditional model of remote site uplinks, and demands a new approach to privatizing the WAN. Enterprises that fit this mold are looking for ways to simplify the transition to a private WAN and need new architectures to support this transition all while increasing network performance and reliability.

Scope

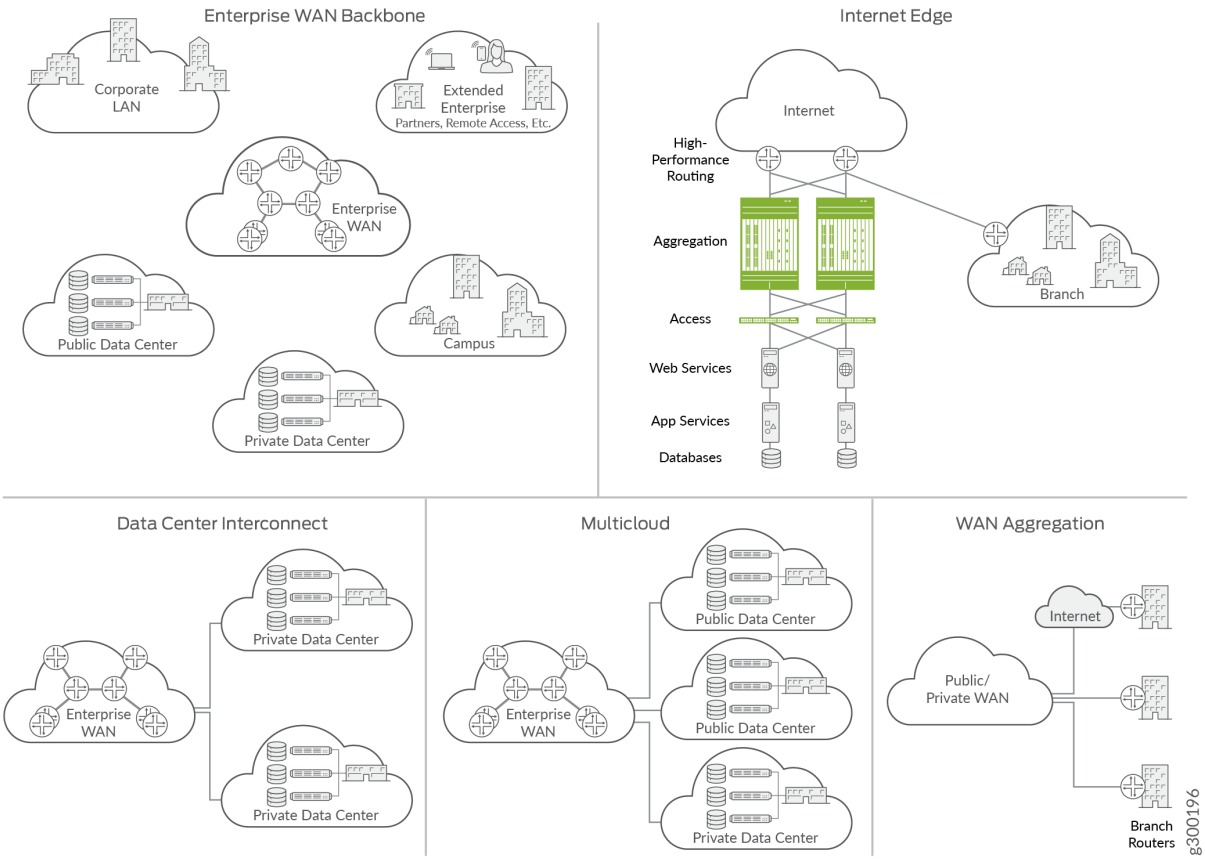
The Juniper Networks Enterprise WAN solution is designed to meet the needs of an increasingly complex network segment that is a key to current and future business requirements. This document serves as a high-level overview of the Enterprise WAN solution and includes an overview of challenges, business drivers, design considerations, and recommendations, as well as a high-level overview of the solution.

The use cases and scenarios covered by the enterprise WAN solution include:

- Enterprise WAN aggregation and backbone—The interconnection of multiple types of enterprise locations includes branch, headquarters, and data center.
- Internet Edge—The interconnection of the enterprise WAN to one or more service providers allows user access to the Internet and to external corporate resources.
- Data Center Interconnectivity—The interconnection between enterprise data centers enables resiliency.
- Enterprise Multicloud—The interconnection between applications and micro-services across multiple public cloud and/or public and private clouds.

The following figure shows each use case:

Figure 1: Juniper Networks enterprise WAN solution scope



Target Audience

The primary audience for this reference architecture includes:

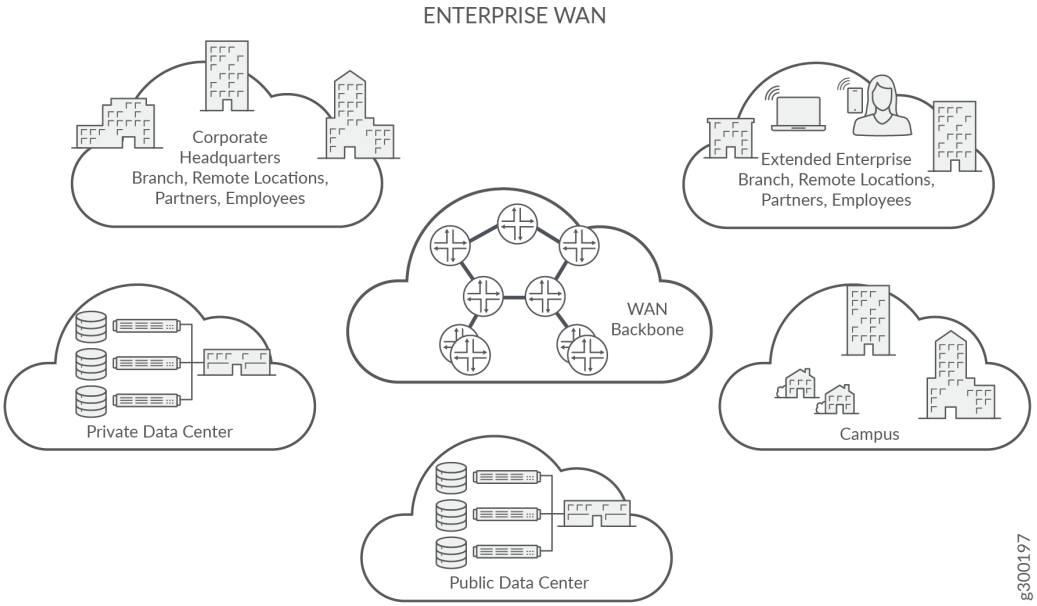
- Network Architects—They are responsible for creating the overall design of the network architecture that supports their company's business objectives.
- Juniper Partners—They are the key resellers and system integrators who seek to design and build enterprise WAN implementations based on Juniper technologies.
- Enterprise Engineers—They are responsible for working with architects, planners, and operations engineers to design and implement the network solution.

Enterprise WAN Overview

IN THIS SECTION

The enterprise WAN consists of network segments and configurations that enable the enterprise to generate revenue in today's highly connected, dynamic environment. The enterprise WAN itself consists of business site types that must be interconnected to enable business and revenue. The corporate LAN and data center are at the core of the enterprise WAN. These sites provide a bulk of the enterprise support, applications, and business enablers.

Figure 2: Enterprise WAN overview



The enterprise WAN is the sum of the configurations and design of the interconnections between the data center and corporate headquarters and the rest of the enterprise. The enterprise remote sites can consist of campus environments as well as small offices, revenue gateways (such as a storefront or branch sales office), and other remote locations.

The enterprise WAN is often designed to provide dedicated interconnection with partners, home-based workers, and other support resources. This is the key to the solution as it provides the backbone over which most enterprise traffic travels. Understanding the enterprise WAN as a whole is key to understanding the subsequent solution components—WAN aggregation and Internet edge.

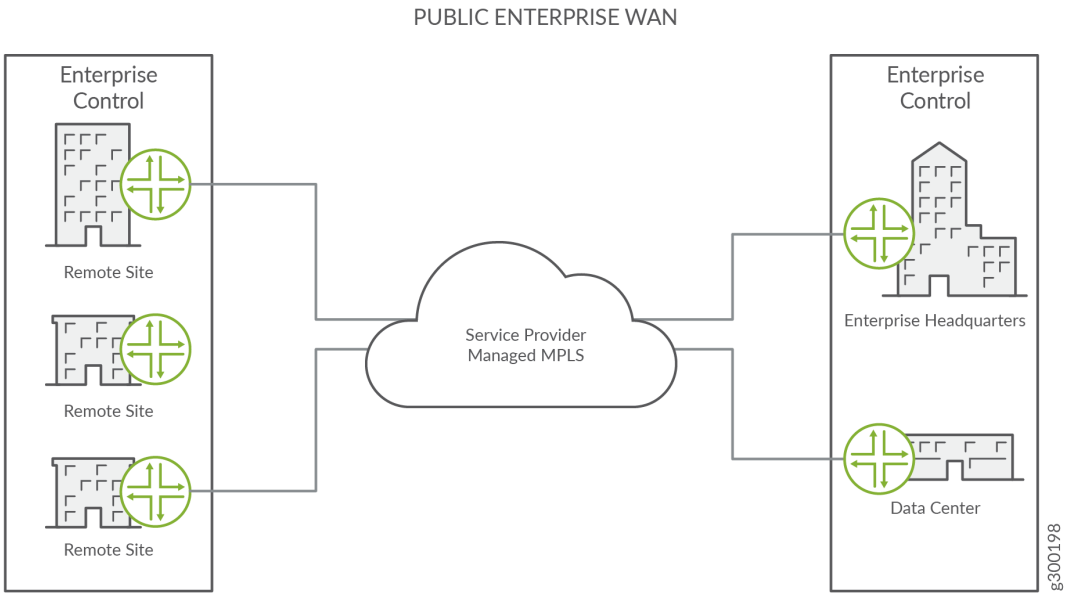
A large enterprise WAN can be built in several ways to accommodate control, security, and performance concerns. The three models of enterprise WAN network are public, hybrid overlay, and private.

Public Enterprise WAN

A public enterprise WAN uses a purely service provider MPLS network to provide pseudo-private enterprise WAN services. The service provider hands off a circuit to the enterprise site and provides all MPLS services transparently to the enterprise. For most enterprises, this architecture provides excellent service with little to no management required by the enterprise.

Many service providers manage the MPLS customer edge (CE) routers at all branches, effectively making the WAN transparent to the enterprise and its users. While this approach is appropriate in most cases, large enterprises often choose to augment or replace the carrier-managed option with their own architecture and design. A hybrid overlay network is often one of these choices.

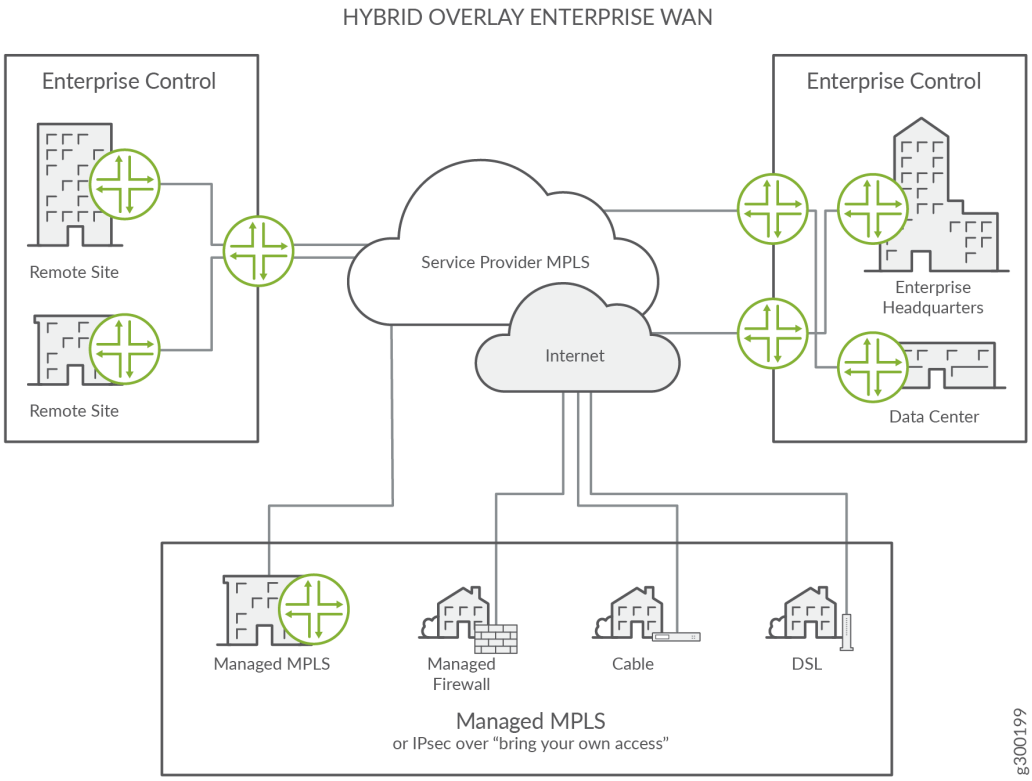
Figure 3: Public enterprise WAN is managed entirely by the service provider



Hybrid Overlay Enterprise WAN

The hybrid overlay network lets the enterprise consolidate and control WAN resources where it makes financial and geographical sense—for example, overlaying private WAN securely over the Internet to augment a carrier-provided private MPLS service. In a hybrid overlay network, regions with a high density of enterprise offices are aggregated onto an aggregation router that the enterprise controls. This aggregation router has a high-speed transport to the rest of the enterprise.

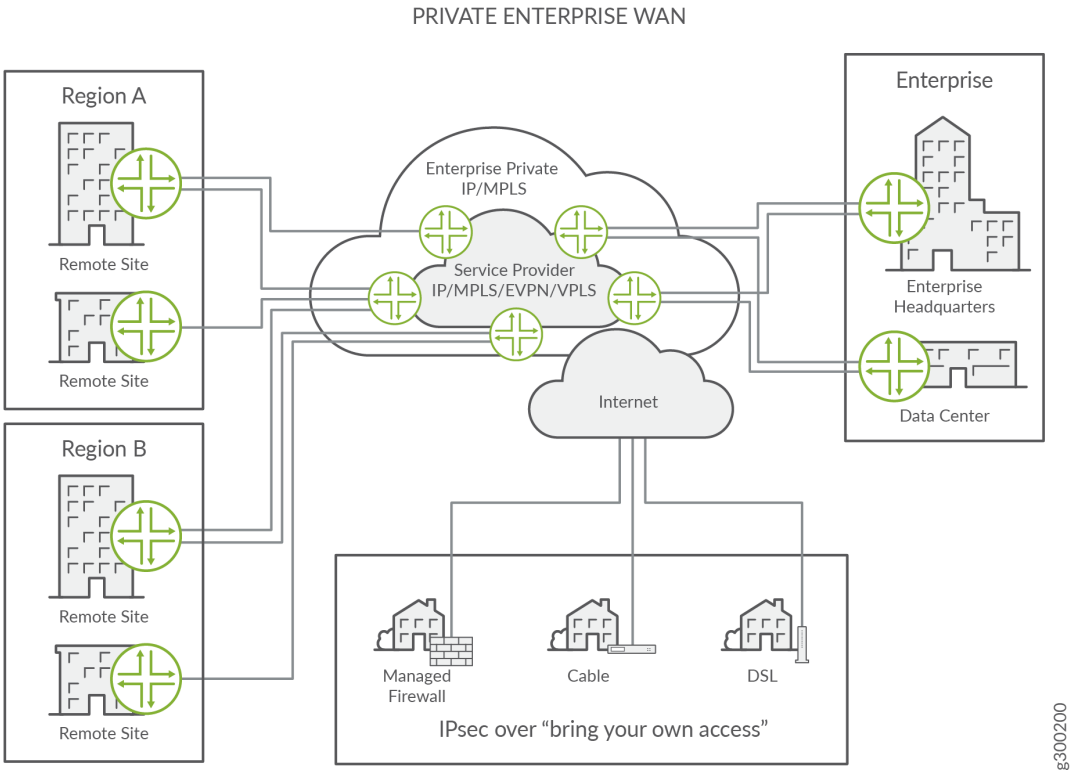
Figure 4: Hybrid overlay enterprise WAN



Private Enterprise WAN

Often, the hybrid approach is not sufficient, and the enterprise wants to build and manage the entire MPLS network. In these solutions, the carrier provides core services to regional aggregation hubs and acts only as logical transport. The enterprise performs all MPLS, class of service, and other configurations. This model gives the greatest control to the enterprise, but often at great expense.

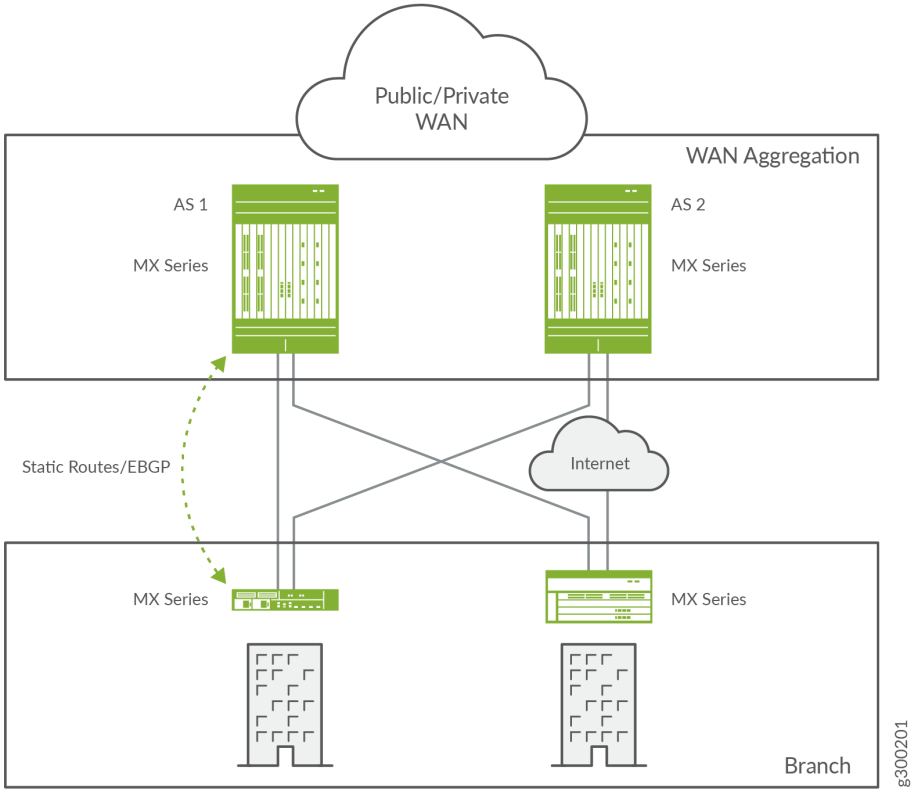
Figure 5: Private enterprise WAN is almost entirely managed by the enterprise. Remote sites and home users are brought into the network using IPsec over public transport



WAN Aggregation

In hybrid overlay and private enterprise WAN deployments, the key to the solution are the WAN aggregation routers that are often co-located at the carrier office. As such, the WAN aggregation routers are a key focus of the overall enterprise WAN solution. WAN aggregation is a network architecture that consolidates multiple networks, such as the campus, branch, and data center networks, onto the enterprise WAN network. WAN aggregation stitches together networks and site types to enable seamless communication between the enterprise’s locations.

Figure 6: Sample WAN aggregation routers that combine multiple remote branch sites into a single enterprise WAN



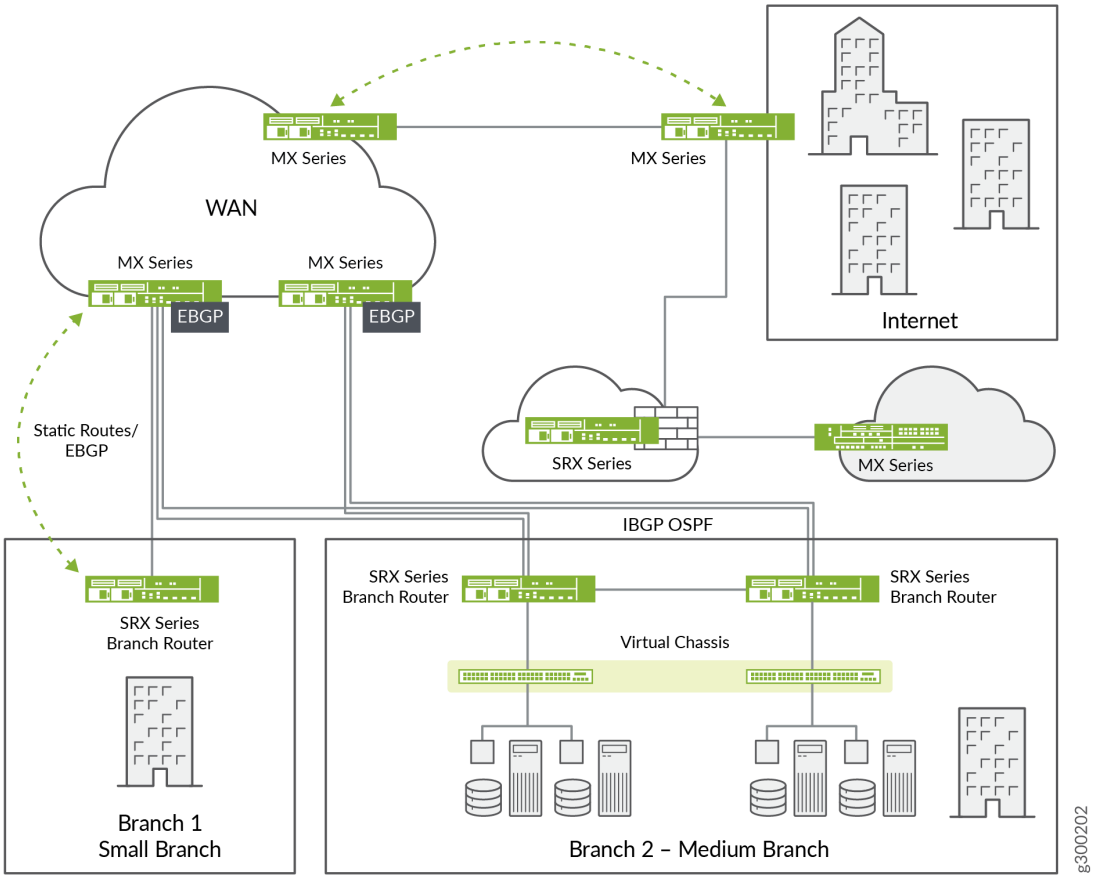
The most common aggregation model is a single backhaul to a corporate headquarters or data center where all site-to-data center traffic and site-to-site traffic are routed within the enterprise.

The aggregation of WAN connections can be private leased line, MPLS Layer 3 VPN, Layer 3 tunneling, any of the Layer 2 VPN technologies, or by an Internet VPN. It is common to find a mix of these connection methods in the WAN aggregation as the enterprise often selects transport based on business need and criticality.

Internet Edge

The second part of the overall enterprise WAN solution is the Internet edge. The Internet edge acts as a centralized gateway for the enterprise, providing connectivity to the Internet for branch offices as well as enabling connection of remote workers and partners to enterprise resources.

Figure 7: Sample Internet edge network with remote branch traffic backhauled to headquarters for Internet access



You can also use the Internet edge to provide:

- Backup connectivity to the WAN for branch offices when the primary WAN connectivity fails.
- Transport for remote workers to access the enterprise, either using software (SSL VPN) or hardware gateways (firewall with IPsec VPN).
- Access to services the enterprise hosts.

Enterprise WAN Challenges

The network is critical to the operation and innovation in the enterprise because it lets employees, suppliers, and customers access new applications and services. As networks have become faster and

more robust to support the current and next generation business applications, complexity and cost have also grown.

Growth in the WAN segment has introduced key challenges to the enterprise, including deployment ease, flexibility, and scalability. How does the enterprise deploy and operate a WAN easily while ensuring that the components implemented are future proof and can scale to meet future demands? Other challenges lie in not only enabling cloud services, but also the recent technological advancements in multi-cloud and edge compute.

Companies are increasingly looking to cloud service providers to augment their business, and a WAN that can enable this agility is essential to success. Adding services and devices to meet this challenge increases the total cost of ownership of the WAN and can have an effect on the bottom line.

Once installed, a new challenge is management of the WAN. The network should be easy to manage—addressing this challenge is particularly problematic as the complexity of the network increases. Finally, the WAN should be services ready. A WAN implementation must support technologies that enable future growth and the addition of value-added services.

The key challenges of WAN deployments are:

- Ease of deployment and management along with flexibility and scalability. The enterprise WAN consists of geographically dispersed sites of various size and purpose. This dispersion and difference of purpose can be addressed by introducing a common network that excels at carrying traffic of varying importance between sites as well as between partners and third-party support organizations.

  Deployment of a single WAN architecture is not enough. The technology used to enable the WAN network should also have common factors. Equipment that shares the same operating system can be more easily migrated to more robust platforms as needs dictate. Having a single operating system throughout the network also makes it easier to introduce new services and configurations, as the same configuration can migrate wherever it is needed.

- Ensuring that cloud services are easily adopted. The drive to reduce costs combined with the need to provide a high-quality user experience often collide and cause business needs to come second to the need to control expense.

  An answer to this conflict is found in the adoption of cloud services. An effective enterprise WAN enables a robust and high-quality connection to the data center through a direct connection to a cloud data center. Meeting this challenge is critical in controlling cost while enhancing user experience.

- Ensuring that the network is services ready. The network should be designed to be flexible, scalable, resilient, and secure as these characteristics are all requirements of any service-ready network. An effective architecture is modular in nature, allowing the addition of new services to the enterprise WAN such as VPN, Network Address Translation (NAT), and stateful firewall services. In addition, the enterprise WAN should support implementation of value-added services such as WAN acceleration and content caching.

Enterprise WAN Design Considerations

IN THIS SECTION

This section focuses on high-level design considerations of enterprise WAN use cases. Each of the considerations should have high-level design goals that inform the choices made during the design of a new or upgraded enterprise WAN. The prime design consideration are:

- Easy to deploy—A top goal in any network architecture should be ease of deployment. A fantastic solution that features complicated deployment scenarios can encounter more issues than a network that features an easy and documented deployment.
- Easy to manage—An effective design features simple and centralized management. The ideal scenario has a single operator with a single pane of glass who is able to manage the entire network. Designing ease into the management of the network is as important as any other factor in the network design.
- Easy to operate—Availability of automation tools means greater visibility, actionable insights, and the ability to self heal and self drive the networks through AI. Automation reduces errors and outages while lowering operational costs.
- Flexible and scalable—New network architectures should be designed to grow and change as business needs dictate. Installing a design that just meets the needs of business today is a recipe for increasing expenses and complexity as the network is upgraded piecemeal.
- Resiliency and security—Architecture that is vital to business success should be designed with the expectation that failure and security breaches are not only possible but also probable. Rather than designing around unplanned outages and attacks, design in a way that expects outages and attacks on the network and its protected resources.
- Services ready—A network should be able to easily adopt new services. The ability to introduce services in line with existing network flows is a key design consideration. This lets you add services like WAN acceleration, content caching, elevated security (antivirus, intrusion detection and prevention), to name a few, to the network (often without the addition of new hardware).

Ease of Deployment/Designed for Flexibility and Scalability

Organizations can have thousands of remote sites spread out among geographical locations that have labels like branch office, regional site, or headquarters. WAN aggregation design should inform the building of a network for all locations, regardless of their label or purpose. This means building a network that scales. Standardization is one way to design for scalability. By introducing and adopting a small number of standard designs for common portions of the network, the options for network deployment are limited and simplified.

To enhance scalability further, use a modular design approach. Begin with a set of standard, global building blocks. From there, design a scalable network that meets business requirements. For instance, in an enterprise network, we might start with a core module and then connect an Internet edge module and a WAN module to build the complete network.

Many of these modules are the same for service design. This provides consistency and ease of scalability in that you can use the same modules in multiple areas of the network to maintain the network. These modules follow standard layered network design models and use separation to ensure that interfaces between the modules are well defined.

Resiliency and Security

A key to maintaining a highly available network is building in the appropriate redundancy to guard against failure, whether it is link or circuit, port, card, or chassis failure. This redundancy is carefully balanced, however, with the complexity inherent in redundant systems.

Overly complex redundancy features can cause more problems than they prevent by introducing failures. Over engineering a network's resiliency can result in communications failure. While all organizations require redundancy, you need to avoid making the redundancy too complex and reliant on too many other modules. The failure of a single component can cause a network failure.

With the addition of a significant amount of delay-sensitive and drop-sensitive traffic such as voice and videoconferencing, we also place a strong emphasis on resiliency in the form of convergence and recovery timing. Choosing a design that features failure detection while reducing recovery time is important to ensuring the network stays available in the face of even a minor component failure.

Network security is another important factor in designing the architecture. As networks become larger and more complex, there are more entry points and areas where security vulnerabilities exist. Effective WAN aggregation and enterprise WAN designs ensure a secure network that does not restrict usability for the end user, hindering the customer experience in the process. The security design should address vulnerability and risk while enhancing the user experience as much as possible.

Ease of Management

An effective WAN aggregation and enterprise WAN architecture should be designed to be easily managed and operated. Ideally, you would use a single pane of glass in the form of a network management application, or a collection of applications, to implement, maintain, and troubleshoot the network.

Old methods of using CLI and truck rolls to manage the network become more of a burden as the complexity of the network grows and as it becomes more vital to the user experience. An architecture that focuses on making the network easy to manage includes all of the elements found in FCAPS, an ISO model and framework for network management.

FCAPS includes the following network management elements:

- Fault management by a central system that polls network elements via SNMP to verify status while network events are sent to the network management system via SNMP traps.
- Configuration management via third-party tools that manage and execute scripts, or through GUI-based systems that allow bulk changes throughout the network.
- Accounting management is essential when multitenancy, or “pay to play” are in use. When you have multiple business units with discreet billing and service requirements, you need to tie usage to those accounts.
- Performance management lets the organization verify that service-level agreements are met, either between the enterprise and the service provider, or between the enterprise IT organization and the business units (internal SLAs).
- Security management is essential to the network. The ability to coordinate security throughout the enterprise and at the service points where security policy is applied is crucial to securing the network. Beyond the configuration of security, the management system should support the reporting of security events so policies can be evaluated and changed to meet evolving security threats.

An effective management system provides a complete FCAPS functionality and enhances the management, security, and accountability of the underlying network design.

Ease of Operation

As enterprise bandwidth grows so does the WAN size and complexity. However, the complexity associated with managing such infrastructure does not have to increase proportionally thanks in part to automation tools. Automation of network operations is less error prone and therefore avoids outages while reducing the CAPEX.

A future-proofed network is designed to stream telemetry, not just provide visibility. It can also extend analytics to provide actionable insights with further extensibility to self-driving networks by self-discovery, self-monitoring, self-configuring and self-healing. The success of any self–driving network depends on algorithms that can predict the state of the network and the necessary action with a high-level of accuracy. The performance of predictive algorithms depends on the data models (correlation engines), and the fidelity of such data models is directly proportional to the amount of data collected (telemetry) over time.

Services Ready

Flexibility, scalability, resiliency, and security all are characteristics of a services-ready network. An architecture featuring a modular design enables technologies and services to be added when the organization is ready to deploy. In a services-ready architecture, new platforms and extensive network changes are not required to enable service adoption—the network is modular and built to accept these new services with little change required.

A network architecture that is designed and configured with class of service (CoS), for instance, is ready to support high-quality voice and video. A network that is designed and configured with multicast is ready to support efficient voice and video delivery. A network with customer edge (CE) platforms that support WCCP is ready to add caching and acceleration services without requiring extensive changes. Other services that you should consider are VPN services, NAT, and stateful firewall services. A network that is designed and built to support these services from day one can be considered services ready.

The Juniper Networks Enterprise WAN Solution

IN THIS SECTION

The Juniper Networks enterprise WAN solution is built on the following modular building blocks:

- WAN Aggregation and backbone
- Internet gateway
- Secure overlay (IPsec VPN)
- Services

The target markets for this solution include any organization that has a wide base of hub sites with a high degree of interconnectivity demands. Large enterprises that operate as pseudo-carriers are the key target of the use cases provided in this solution. Government agencies, universities, financial and health care organizations, and large technology companies are most likely to benefit from the deployment scenarios in the enterprise WAN solution.

Large enterprises are the most likely to establish private aggregation points of presence, enabling them to consolidate WAN connections prior to backhaul to the headquarters or data center sites. This approach provides a central point of control for regional hub sites, enabling cost savings on backhaul—a single aggregation router is connected via high-speed backhaul to the carrier or private MPLS cloud as well as to the Internet edge—and management. In the aggregation model, a single point of presence provides all enterprise transport services to the regional hubs. This minimizes configuration points and enables more robust resiliency and performance to those hub sites.

The next section covers each of the modular components of the WAN aggregation solution.

WAN Aggregation and Backbone

There are several modular configuration options for the WAN backbone. Using the WAN aggregation model (Table 1), the solution features configurations for three deployment scenarios—dual router with dual circuit, single router with single connection, and single router with dual connection.

Table 1: Enterprise WAN Remote Site Type

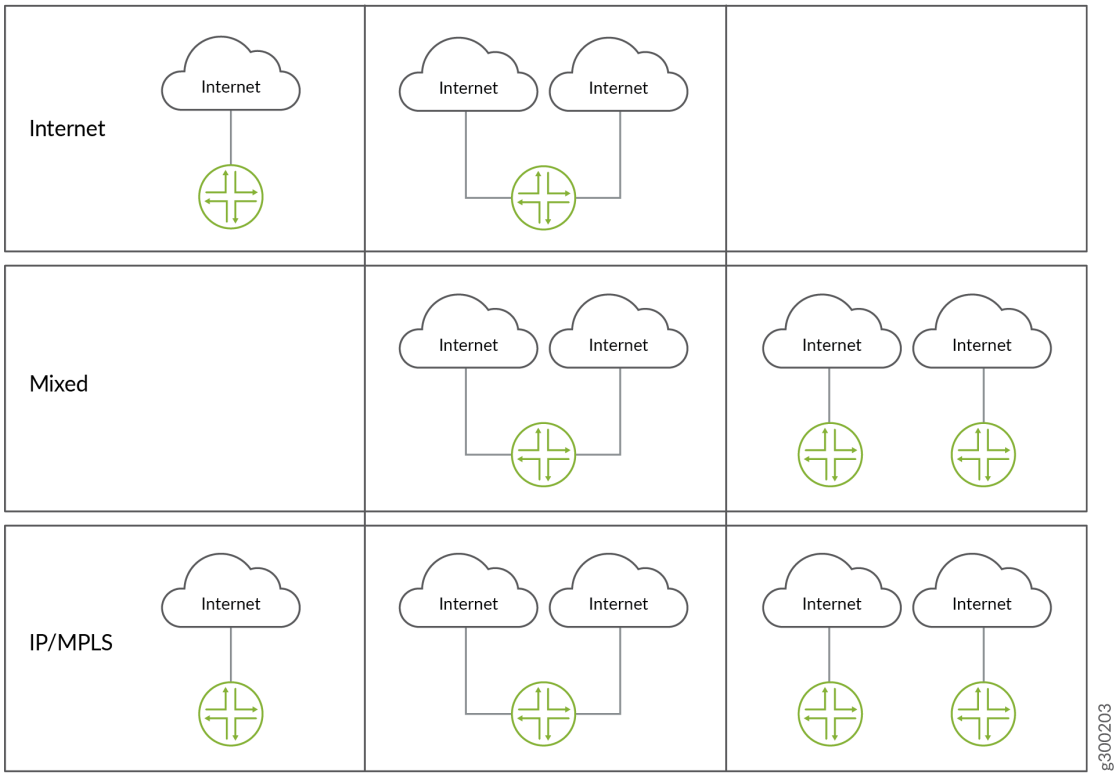
Deployment Scenario	Size	Platform	Transport	Head End Router
Dual Router Dual Circuit	Large	MX	L3VPN/L2VPN/IP Tunnels	WAN backbone
			Internet	VPN, WAN backbone

Table 1: Enterprise WAN Remote Site Type *(Continued)*

Deployment Scenario	Size	Platform	Transport	Head End Router
Single Router Single Connection	Small	SRX	Internet	
	Medium	MX	Private WAN	WAN backbone
		MX/SRX	Internet	VPN, WAN backbone
Single Router Dual Connection	Medium	MX	Internet	VPN, WAN backbone
			Private WAN	WAN backbone
			L3VPN/L2VPN/ IPTunnels	WAN backbone

The WAN backbone configurations include uplinks directly to the Internet, mixed connection profiles with both MPLS and Internet connections from a hub site, and a complete MPLS connection model with the sites connected into MPLS for all three deployment scenarios as shown in the following figure.

Figure 8: Enterprise WAN deployment scenarios

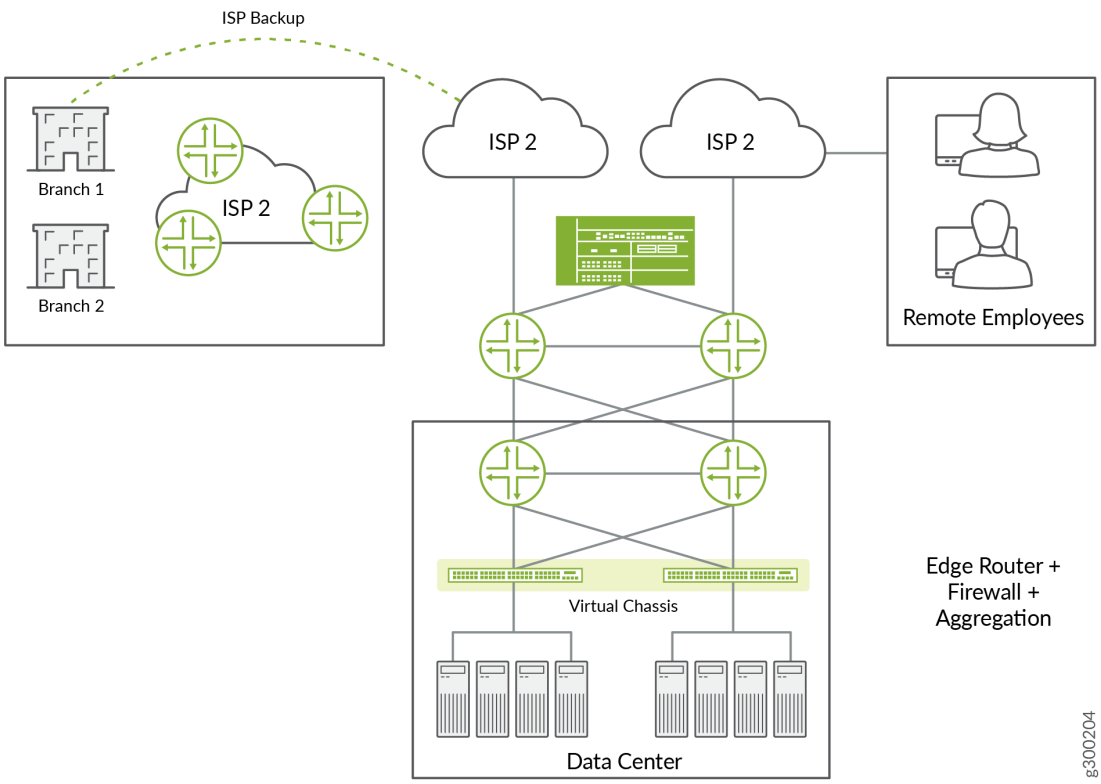


Internet Gateway

The Internet gateway is a foundation of the WAN aggregation deployment scenario. The Internet and mixed aggregation scenarios require Internet gateway functionality to properly provision WAN aggregation. The Internet gateway provides Internet access to hub site users, or more commonly, provides a public transit for IPsec VPN connection back to the headquarters or data center.

In many cases, hub Internet traffic is backhauled to the company headquarters to enable security services such as URL filtering, antispam and antivirus, and intrusion detection and prevention (IDP). By backhauling traffic to a headquarters site, the enterprise can manage and maintain security between its users and the Internet in a central location. By sacrificing some speed and performance, the enterprise can ensure the security of its user base in this scenario.

Figure 9: The Internet gateway



The Internet edge module of the larger WAN aggregation solution provides cloud-grade routing and security to regional enterprise sites that require local Internet access. The local access either provides direct Internet connection to the remote sites, or it provides a transit network to allow intra-enterprise IPsec VPN connectivity.

The aggregation hub providing Internet edge services is services ready and can be easily configured with services that enhance the security of the enterprise remote sites. Services such as dynamic NAT, access lists to whitelist or blacklist-specific destinations, stateful firewall and IDP services, and active/active load balancing to multiple ISPs are all key components of the solution.

Secure Overlay

Secure overlay lets home users or branches with limited MPLS provider options to access the enterprise. The branch office or home user obtains Internet access from whatever local provider is available (via cable, fiber, or satellite). The enterprise then provides a managed, configured device with IPsec services to the branch or home user. Another access method is a secure client on the home user's computer that allows software-encrypted access to the enterprise. This access can be built within the data center using

a VPN gateway or software VPN termination device, or it can be hosted in the cloud closer to the Internet edge.

Services

The enterprise WAN solution is services ready, but what services might an enterprise want to bring into the network? The solution supports Web Cache Communication Protocol (WCCP) to enable WAN acceleration devices to enhance the user experience. Inline, network-driven security services, such as stateful firewalls and deep packet inspection, are also supported.

When the enterprise hosts sensitive data or is likely to be the target of intrusion or attack, control plane protection and denial-of-service protection (DoS and DDoS) are integrated into the solution architecture.

For enterprises that use real-time or recorded video content (such as financial streams to banking centers or video lectures in the education sector), the solution supports content caching. This service is adopted through enhancements to the network's handling of multicast traffic and by the routing hardware ability to redirect specific flows to secondary devices or virtual appliances that locally cache and serve content to remote sites. The enterprise WAN can add these services in line with little to no disruption of the user experience.

Modernize Your Mission Critical Enterprise WAN Infrastructure

Juniper enterprise WAN solution empowers customers to transition smoothly to a modernized architecture that is flexible, automated, secure, and resilient.

- A Flexible WAN - Juniper provides the agility to adapt to the unknown with flexible chipsets, consistent Junos operating system across the entire portfolio, modular platforms that are backward compatible, future-proof protocols (IPv6, segment routing, MPLS), and a flexible consumption model supporting pay-as-you grow or software subscriptions for features and services.
- An Automated WAN - Juniper offers closed-loop automation that translates business intent into service performance, assuring customers receive a differentiated service experience. Open and standard APIs, customizable DIY tools and visual workflows for visibility, AI, and real-time telemetry streaming allow automation of the entire network operations lifecycle that improves operational efficiency while reducing complexity.
- A Secure WAN – To defend your WAN, Juniper Connected Security extends threat intelligence to Juniper MX Series routing infrastructure. You can block command and control (C&C) traffic discovered by Juniper Advanced Threat Prevention, Juniper Threat Labs, and custom blacklists at the

network hardware level. Juniper Connected Security turns your WAN connectivity layers into automated defense layers.

- A Resilient WAN - For maximized uptime and mission critical Quality of Experiences (QoE), Juniper delivers multi-layer resiliency to ensure uptime, reliability, business continuality, and user satisfaction. At the product and OS level Juniper offers redundant hardware and resilient software features that support graceful RE switchover (GRES), nonstop active routing (NSR), and unified in-service software upgrade (unified ISSU). Juniper offers high-availability architecture features, including multi-homing capabilities, IPVPN, L2VPNs, EVPN, multicast, segment routing with TI-LFA, and others. Additionally, with software-defined management and control, you gain the network visibility to monitor, manage, and diagnose with the latest AI and ML techniques and integrate them into your network operations.

Enterprise WAN Solution Benefits

IN THIS SECTION

The enterprise WAN solution offers the following benefits to large enterprises seeking to use private MPLS or hybrid overlay network design with WAN aggregation:

- Improved operational efficiency
- Reduced operational expense
- Flexibility and value for investment
- Security
- Cloud-grade reliability

Improved Operational Efficiency

Large enterprises can simplify the network by adding regional WAN aggregation routers to a private MPLS or hybrid overlay network. Aggregating low-speed connections to hub sites into a regional aggregation tier that supports high-speed backhaul, enables a single point of regional management and improves the performance of hub sites by providing high-speed services from the region to the headquarters.

This solution includes automation to simplify network operations, lower cost and minimize operational errors. The automation suite is comprised of network visibility enabled by the JUNOS Telemetry (JTI), network health analytics via the Paragon Insights, and operational automation using Paragon Pathfinder. Further, these automation tools are provided as programmable frameworks, wherein applications such as custom route computations can be built with the goal of influencing routing decisions. This enables operational simplicity by standardizing the operating system within a region and leveraging the automation tools, saving network operational time in provisioning and troubleshooting the WAN aggregation tier.

Using Juniper Networks MX Series 5G Universal Routing platforms, the WAN aggregation architectures in the enterprise WAN solution support link speeds from 10 Mbps all the way through 100 Gbps. For non-Ethernet interfaces, the MX Series supports DS3 through OC192.

The design also uses a single operating system (Juniper Networks Junos® operating system) on all routers, from the aggregation hubs to small CPE devices used at remote sites (or by home users).

Reduced Operational Expense

Regional aggregation of enterprise remote sites lets the enterprise provide lower-speed local uplinks to the sites in a region. The WAN backbone then provides a higher-speed backhaul transit to the headquarters. The enterprise can control the configuration from the hub to the backbone and across the backhaul to headquarters. The WAN backbone model enables the enterprise to provide high-speed services to regional remote sites at potentially lower cost, using the low-speed links to aggregate sites to a higher-speed transport.

Improved Flexibility and Value for Investment

The MX Series routers support a wide array of upgrade options. Software licenses and Modular Interface Cards (MICs) can be added to increase the functionality or capacity of an aggregation hub. Within a range of MX Series (low-end or high-end) routers, software licenses can be activated to enable higher speeds on the same platform, supporting expansion in region or the addition of new services to remote

sites. The MX Series also supports a wide array of interface types, enabling a remote site to upgrade from legacy circuits to high-speed Ethernet easily, as the uplink is performed only between the remote site and the aggregation hub.

Finally, the network is built for elasticity and performance. Combining a robust class-of-service implementation with flexible backhaul features such as MPLS traffic engineering (TE), IP tunneling such as GRE and IPSec, Ethernet private VPN (EVPN), SPRING, virtual private LAN service (VPLS), the enterprise can more effectively guarantee application performance to the remote sites, ultimately improving the user experience and, by extension, the bottom line.

Security

The enterprise WAN solution and WAN aggregation deployment scenarios are built from the ground up with security as a key component. Logical separation of remote traffic or even the separation of different operating units within the remote sites is provided. This logical separation lets the enterprise control not only whom on the outside each operating group can communicate with, but it controls communication and leaks between groups within the same enterprise.

Cloud-Grade Reliability

The ability to keep the enterprise running is another key benefit of the enterprise WAN solution. The MX Series routing platform is a cloud-grade component designed with full resiliency at its core, using redundant control plane and switching plane hardware as well as redundant power and cooling.

In a design model where the enterprise acts as a private service provider to its remote sites, the ability to keep the WAN aggregation routers available and performing is critical to the success of the solution. At the routing and software layer, MPLS resiliency mechanisms such as MPLS fast reroute (FRR) and on-demand paths are supported to enable fast recovery from core issues that affect backhaul routing to the headquarters.

In a multiple chassis deployment, where hardware redundancy is supported by uplinks to multiple regional aggregation points of presence, the MX Series supports multichassis link aggregation group (LAG) and Virtual Chassis, enabling a single site to redundantly connect to multiple aggregation points while allowing that uplink to appear as a single logical uplink.

Conclusion

The Juniper Networks enterprise WAN solution meets modern business requirements and digital transformation strategies, while easily supporting business continuity by delivering a flexible, automated, secure, and resilient WAN solution, and offers these benefits:

- Lower costs due to efficiency, scalability, and performance of carrier-grade WAN devices.
- Less complexity thanks to automation and visibility tools that enable simpler configuration and operation.

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.