JUNIPER NETWORKS ENTERPRISE WAN SOLUTION ARCHITECTURE

An Enterprise WAN Solution Focusing on WAN Aggregation of Large Enterprise Regional Remote Sites

Table of Contents

List of Figures

Introduction

The network is a key component in the success of a modern enterprise as it connects 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 this growing challenge. Several trends in the enterprise have had a negative effect on complexity, network performance, and scale.

The first trend is the explosion of Internet-connected devices. Five years 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 has a negative impact on 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 utilize 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 a network architecture that is built so that it can expand to handle the exponential growth in user bandwidth consumption over the next 5 to 10 years.

A second trend in the enterprise is the emergence of application hosting data centers and the distribution of content. In the past, applications, data, and content were largely localized—users needed access to a local e-mail 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 data centers 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.

A third trend in the enterprise is the rapid change experienced as business models evolve. Enterprises often acquire new companies to expand their products and services and need to integrate them quickly to enable faster time to revenue. This means that they need to take over management of the acquisition network and resources. The traditional network model that favored individual uplinks to remote sites becomes complex and unmanageable as acquisitions become more commonplace and there is a need for a more extensible mode.

A final trend affecting enterprises is the view that they should operate like service providers, treating the organization as customers for their services and meeting higher standards for service delivery. This "providerization" of the large enterprise poses great challenges to the traditional WAN designs and architectures as the enterprise seeks to act as its own service provider. Many companies choose to build completely private WAN clouds, and many others look to build hybrid networks that give them control and management of strategic portions of the network instead of relying 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. The 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.

About Juniper Networks Validated Solutions

Juniper Networks validated solutions are complete domain architectures that are expert designed, lab tested, and documented to provide guidance in the deployment of complex solutions. Juniper Networks solution validation labs put all solutions through extensive testing using both simulation and live network elements to ensure comprehensive validation of all published solutions. Customer use cases, common domain examples, and field experience are combined to generate prescriptive configurations and architectures to guide customer and partner implementations of Juniper solutions. This approach enables partners and customers to reduce time to certify and verify new designs by providing tested, prescriptive configurations to use as a baseline.

The enterprise WAN solution is verified by Juniper solution testing, a detailed framework that tests the solution from both a network and application perspective. Testing and measuring applications at scale verifies the integration of the network, compute, storage, and virtualization components. Juniper solution testing provides the peace of mind and confidence that the solution behaves as described in a real-world production environment.

Scope

The Juniper Networks Enterprise WAN solution is designed to meet the needs of an increasingly complex network segment that is a key enabler to current and future business requirements. This document serves as a high-level overview of the Juniper Networks 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. More detailed technical coverage of the solution can be found in the *Enterprise WAN Design and Implementation Guide*.

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

- **Enterprise WAN**—The interconnection of multiple types of enterprise locations includes branch, headquarters, and data center. (There are plans for the complete enterprise WAN scenario to be covered by a future version of the solution.)
- **Internet Edge**—The interconnection of the enterprise WAN to one or more service providers enables user access to the Internet and external access to corporate resources.
- **WAN aggregation**—This is the consolidation of multiple enterprise branch networks onto a single enterprise WAN.
- **Data center interconnectivity**—The interconnectivity between enterprise data centers enables resiliency in the enterprise data center. (This scenario is covered by the Juniper data center interconnect solution.)

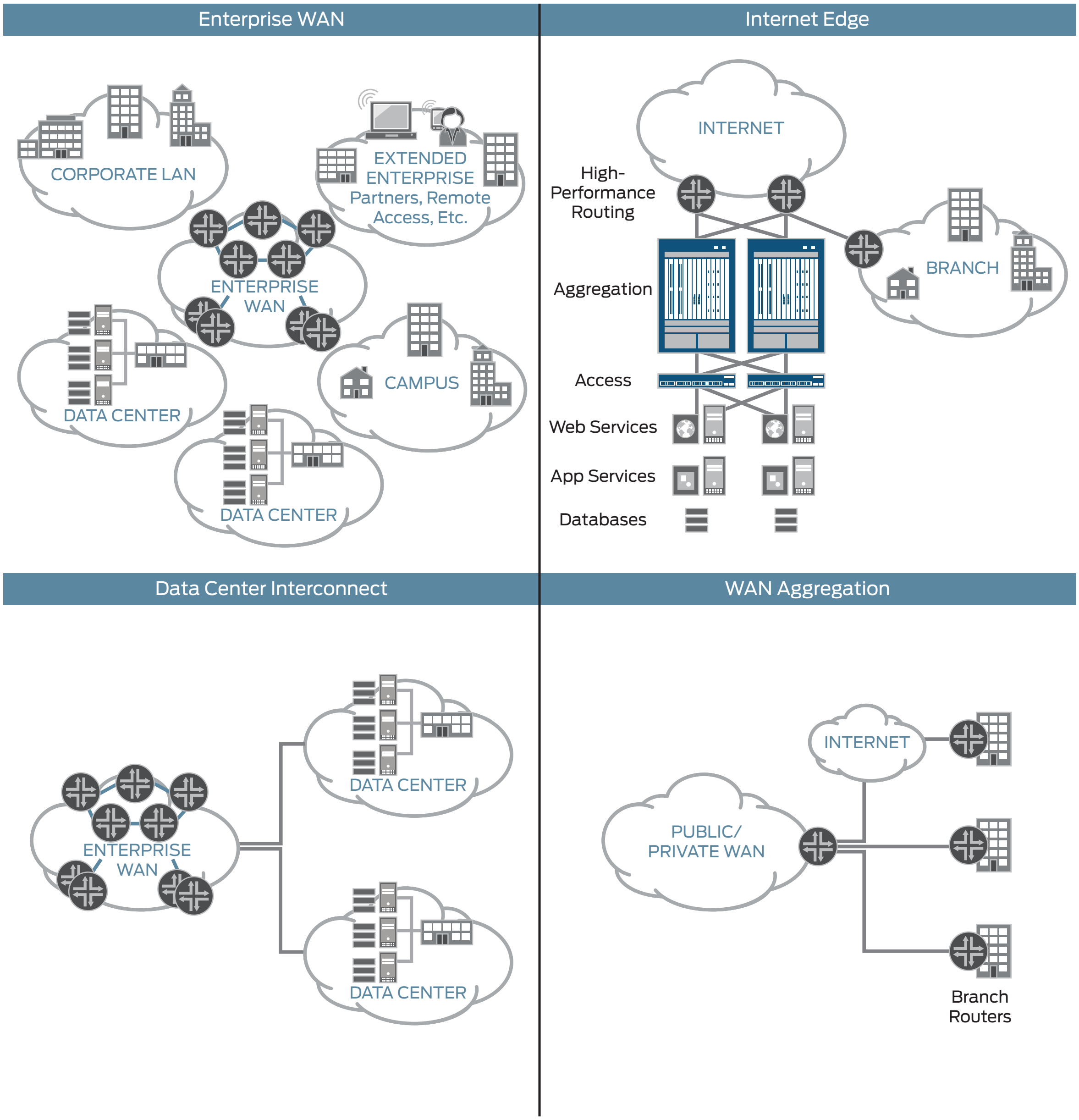


Figure 1: Juniper Networks Enterprise WAN solution scope

Target Audience

The primary audience for this guide includes the following resources:

- **Network Architects**—They are responsible for creating the overall design of the network architecture that supports their company's business objectives.
- **Juniper Partners**—Key resellers and system integrators 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

The enterprise WAN consists of various network segments and configurations that enable the enterprise to generate revenue in today's highly connected, dynamic environment. The enterprise WAN itself consists of various business site types that must be interconnected in order to enable business and revenues. 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). 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 various 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.

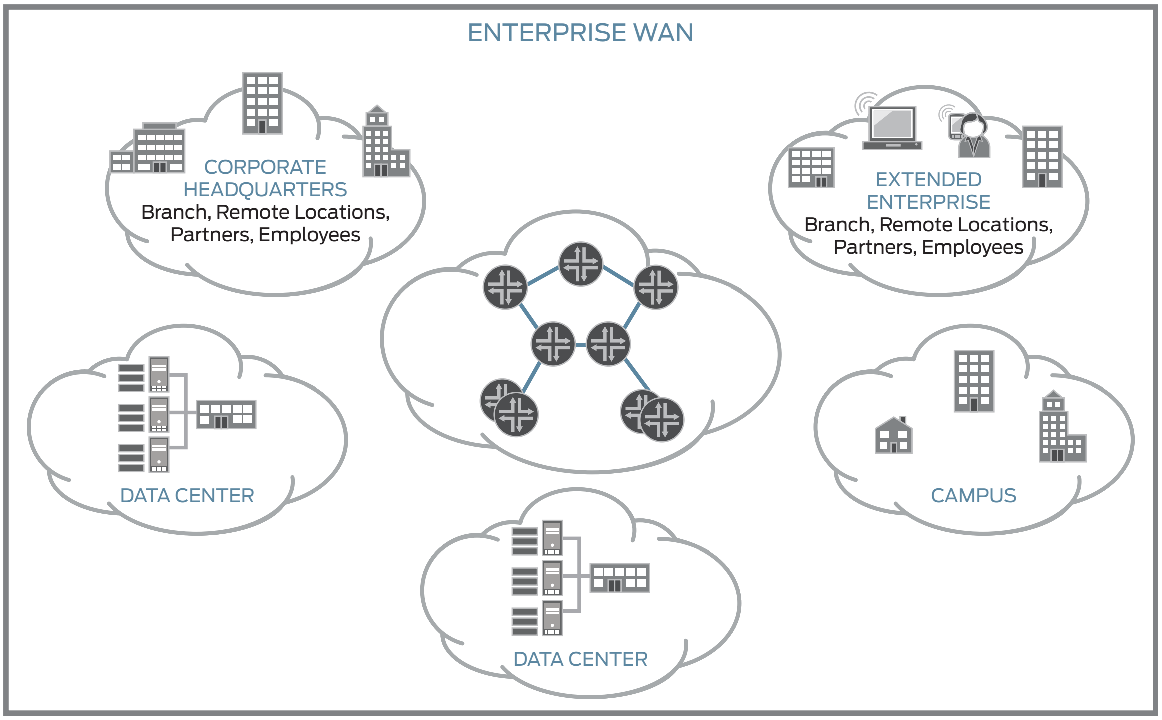

ENTERPRISE WAN
CORPORATE HEADQUARTERS
Branch, Remote Locations, Partners, Employees
EXTENDED ENTERPRISE
Branch, Remote Locations, Partners, Employees
DATA CENTER
CAMPUS
DATA CENTER

Figure 2: The Enterprise WAN

A large enterprise WAN can be built in several ways to accommodate control, security, and performance concerns within the business. The three models of enterprise WAN network are public, hybrid overlay, and private (Figure 3). A public enterprise WAN utilizes 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.

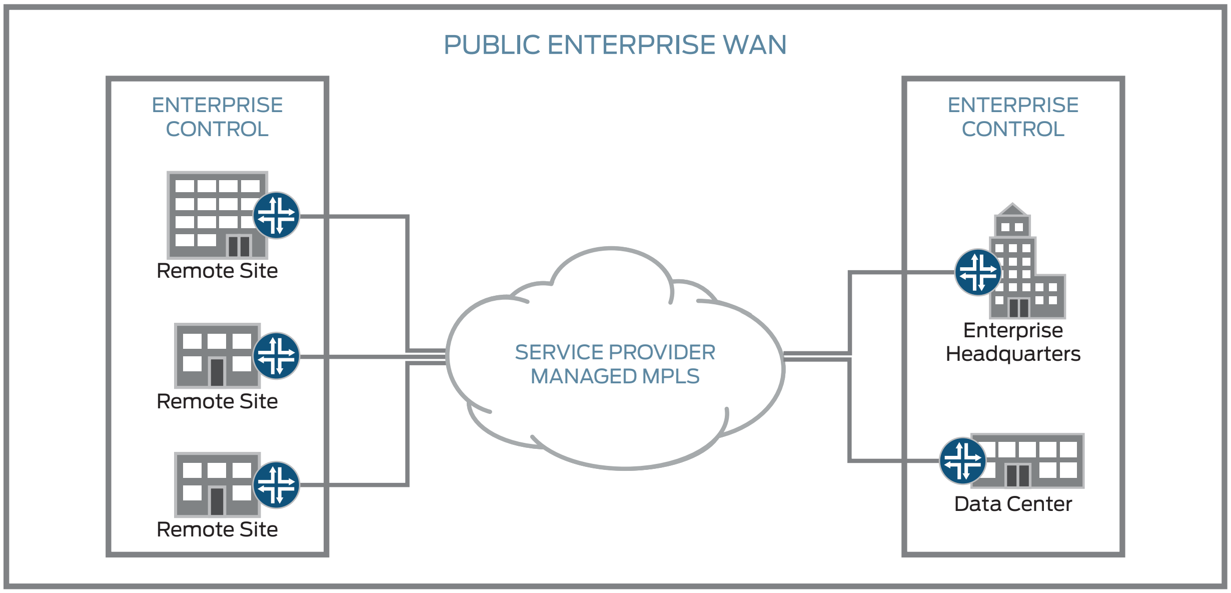


Figure 3: Private enterprise WAN is managed entirely by the service provider

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

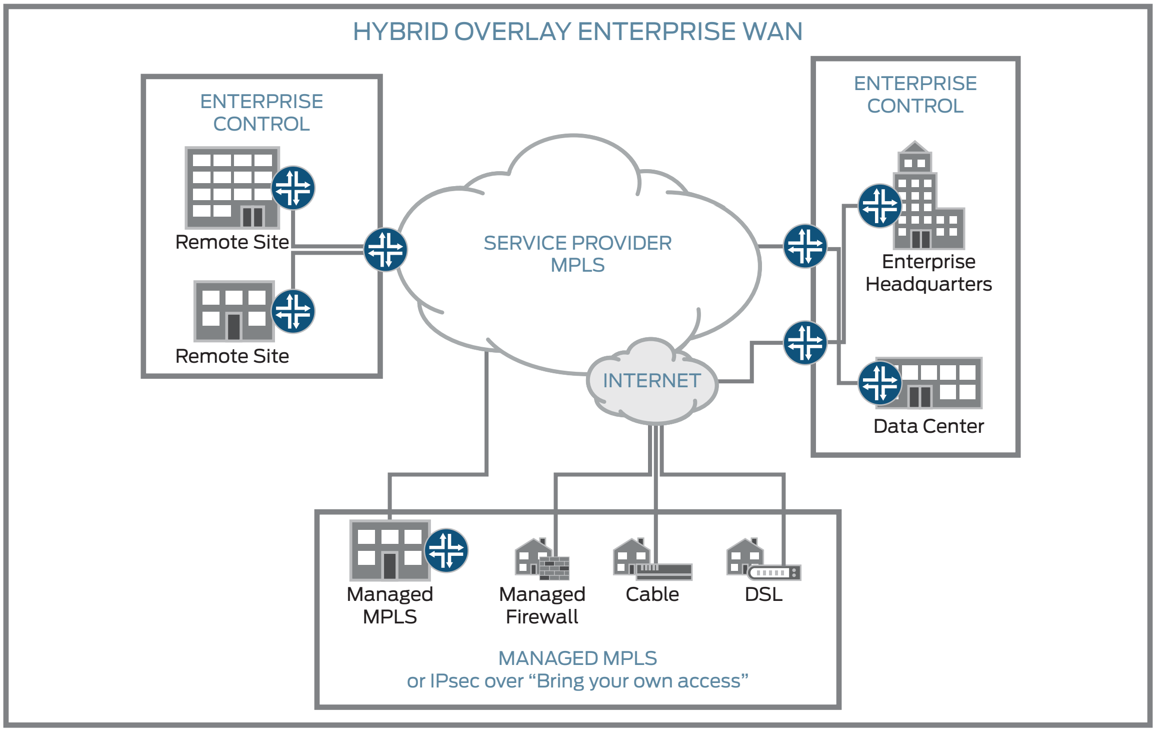


Figure 4: The hybrid overlay enterprise WAN

Often, the hybrid approach is not sufficient. In cases where the enterprise wants to build and manage the entire MPLS network, a private solution is favored (Figure 5). In these solutions, the carrier provides core services to regional aggregation hubs and acts only as logical transport. All MPLS, class of service, and other configurations are performed by the enterprise. This model gives the greatest amount of control to the enterprise but often at great expense.

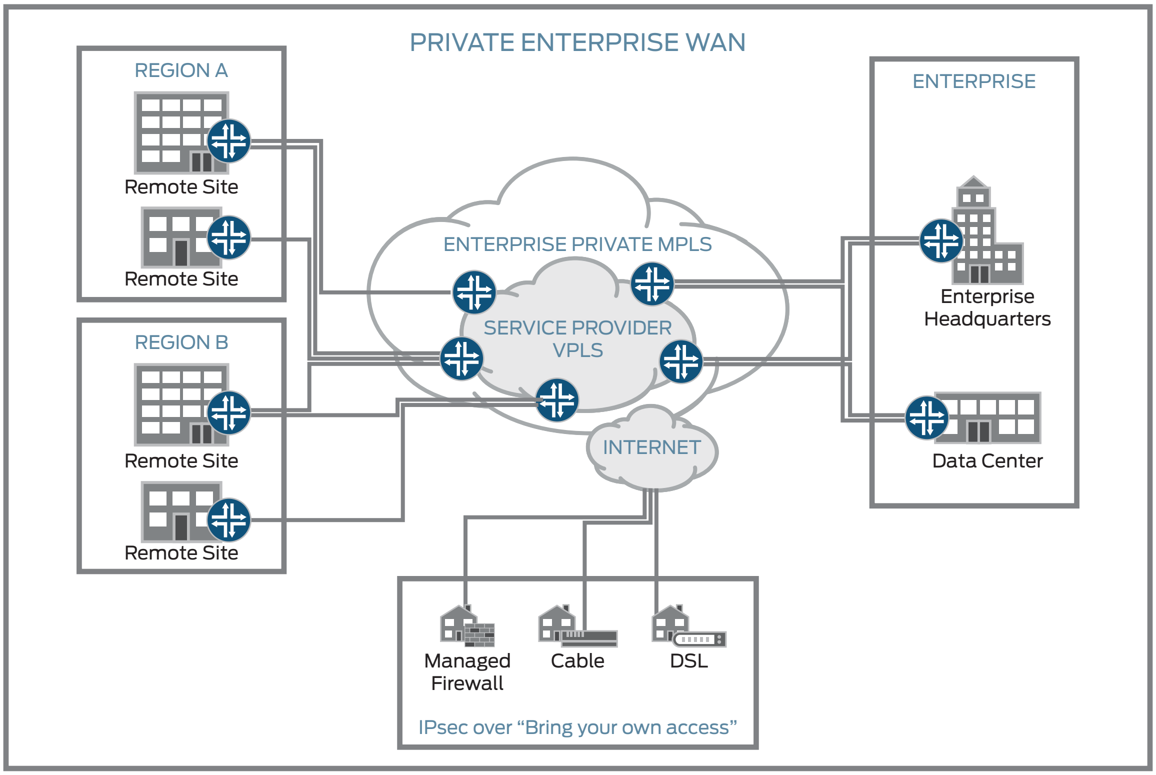


Figure 5: The private enterprise WAN is almost entirely managed by the enterprise. Remote sites and home users are brought into the network using IPsec over public transport.

In hybrid overlay and private enterprise WAN deployments, the key to the solution are the WAN aggregation routers that are often collocated 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 (Figure 6). It is within this enterprise WAN component that the various networks and site types are stitched together to enable seamless communication between the enterprise's various locations. The aggregation model featured most often is that of a single backhaul to a corporate headquarters or data center where all site-to-data center traffic, and site-to-site traffic are sent to be routed within the enterprise. The aggregation of WAN connections can be handled by private leased line, MPLS Layer 3 VPN, Layer 2 VPN, 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.

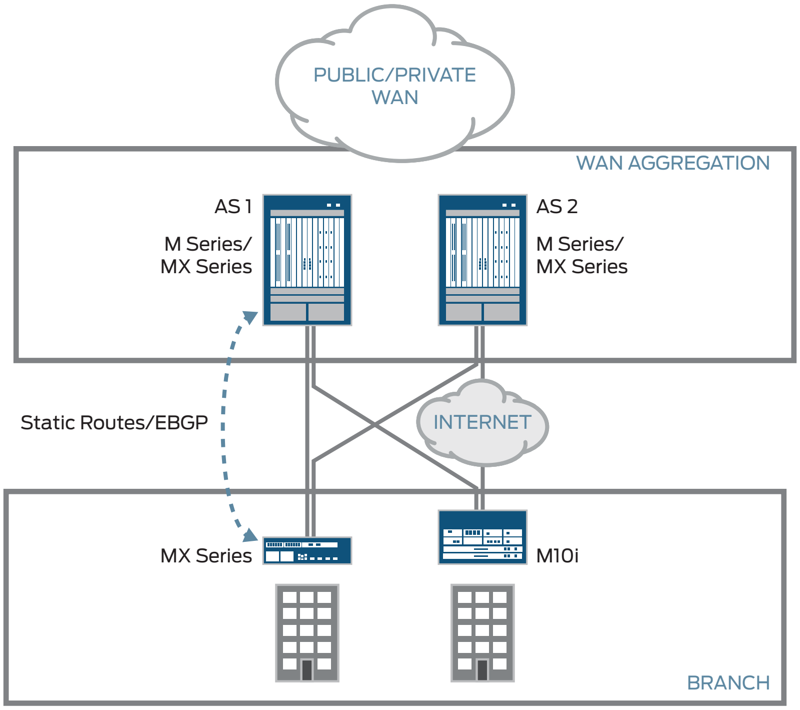
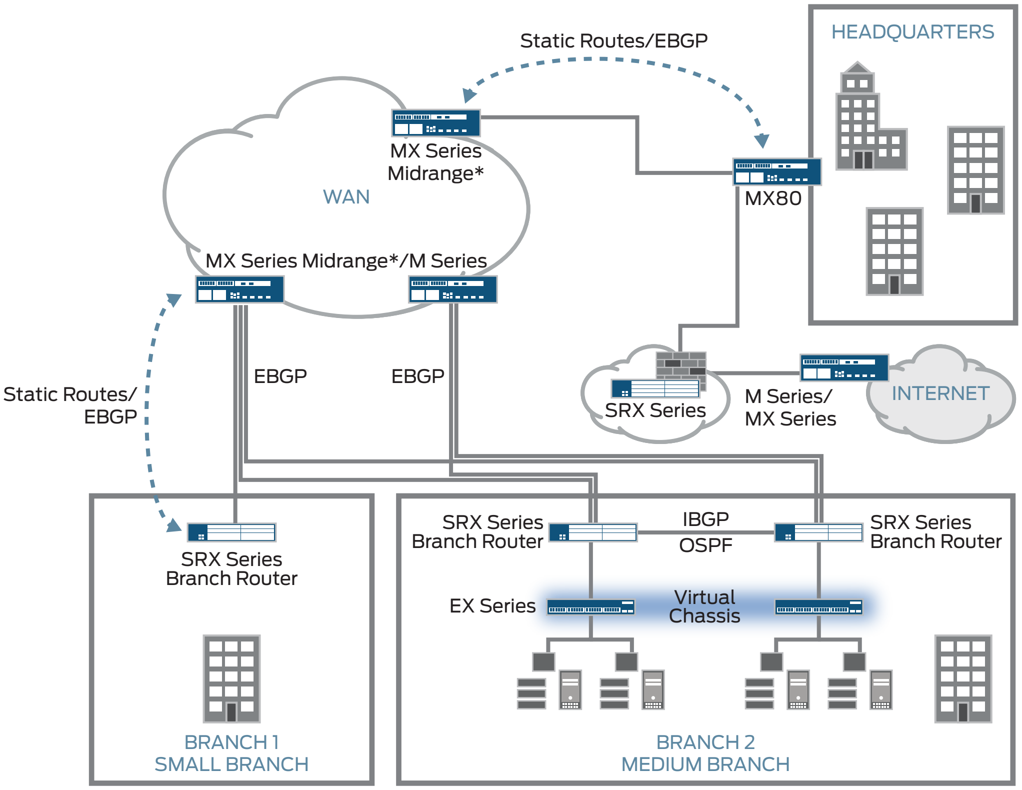


Figure 6: Sample WAN aggregation routers that combine multiple remote branch sites into a single enterprise WAN

The second part of the overall enterprise WAN solution that is covered by this version of the solution is the Internet edge (Figure 7). 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. The Internet edge can also be used to provide backup connectivity to the WAN for branch offices in cases where the primary WAN connectivity fails. The Internet edge also provides transport for remote workers to access the enterprise, either via software-based means (SSL VPN) or via hardware gateways (firewall with IPsec VPN). The Internet edge also provides access to services hosted by the enterprise.



*MX Series midrange consists of the MX5, MX10, MX40, and MX80

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

Enterprise WAN Challenges

The network is critical to the operation and innovation within the enterprise as it enables access to new applications and services by employees, suppliers, and customers. As networks have become faster and more robust to support the current and next generation of business applications, the complexity and expense associated with the network have also grown. The growth in the WAN segment has introduced several key challenges to the enterprise. Deployment ease, flexibility, and scalability are ongoing challenges in this segment. How does the enterprise deploy a WAN easily while ensuring that the components implemented are future proof and able to scale to meet future demands? Another key challenge is in the enabling of cloud services in the enterprise. Companies are increasingly looking to cloud services providers to augment their business, and a WAN that can enable this agility is essential to success. Adding services and more 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 presented in the management of the WAN. The network should be easy to manage once implemented—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 to the network.

The first key challenge of the WAN is in the ease of deployment and in its flexibility and scalability. This ease should extend to the manageability of the network once it has been implemented. The enterprise WAN does not consist of a single branch location, but rather it consists of sites of various size and purpose that are geographically dispersed. This dispersion and difference of purpose can be effectively 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. Unfortunately, deployment of a single WAN architecture is not enough. The technology used to enable the single 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. In addition, having a single operating system throughout the network makes it easier to introduce new services and configurations to the network, as the same configuration is likely to migrate wherever it is needed.

Another key challenge is ensuring that cloud services are easily adopted by the enterprise. The drive to reduce cost in the enterprise 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 often found in the adoption of cloud services in the enterprise. An effective enterprise WAN enables not only intercompany communication, but it enables a robust and high-quality connection to the data center—either through direct interconnection to an enterprise data center or through a direct connection to a cloud data center. Meeting this challenge is critical in controlling cost while enhancing the user experience with the data center.

The final key challenge in the enterprise WAN is 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 in this space 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 services, to name a couple.

Enterprise WAN Design Considerations

This section focuses on high-level design considerations involved in the enterprise WAN use cases included in this document. Each of the solution elements covered should have high-level design goals that inform the choices made during the design of a new or upgraded enterprise WAN. The prime design considerations for the enterprise WAN are:

- **Easy to deploy**—A top goal in any effective network architecture should be ease of deployment. A fantastic solution that features complicated deployment scenarios is likely to encounter more issues than a network that features easy and documented deployment.
- **Flexible and scalable**—New network architecture should be designed to grow with the business and change as business needs dictate. Installing a design that just meets the needs of the 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, as in the case of the enterprise WAN, 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.
- **Easy to manage**—An effective network design features management that is simple and centralized. The ideal scenario has a single operator with a single pane of glass who is able to manage the entire network. Designing ease in the management of the network is just as important as any other factor in the network design.
- **Services ready**—Finally, a network should be able to easily adopt new technologies and services that allow the network to provide enhanced functionality to the business. The ability to introduce value-added services in line with existing network flows is a key design consideration in an enterprise WAN solution. This enables the network administrators to 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 with thousands of remote sites often are spread out among different geographical locations. The locations might have labels like branch office, regional site, or headquarters. WAN aggregation design should inform the building of a network for all these locations, regardless of their label or purpose. This means that the architect and network designers should build 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, resulting in a more common network design. To enhance scalability further, a modular design approach should be used. Designers should begin with a set of standard, global building blocks for the network. From there, a scalable network can be designed to meet business requirements. For instance, in an enterprise network, we might start with a core module—connect an Internet edge module and a WAN module to build the complete enterprise WAN network.

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

Resiliency and Security

One of the keys to maintaining a highly available network is building in the appropriate redundancy to guard against failure in the network, whether it is link/circuit, port, card, or chassis failure. This redundancy is carefully balanced, however, with the complexity inherent in redundant systems. Over engineered systems can cause more problems than they prevent, introducing failures caused by overly complex redundancy features. Over engineering a network's resiliency can often result in complete communications failure. All organizations require redundancy in their networks. When building in the necessary redundancy, care and thought must be given to avoid making the redundancy too complex and reliant on too many other modules. The failure of a single component of each service can create 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.

The security of the network is another important factor in designing network architecture. As networks become larger and more complex, entry points into the network and areas where security vulnerabilities exist are more probable. Effective WAN aggregation and enterprise WAN designs ensure a secure network that does not restrict usability to the point where using the network becomes a burden to the end user, hindering the customer experience in the process. Security should be designed to address vulnerability and risk while enhancing the user experience on the network 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, a single pane of glass in the form of a network management application, or a collection of applications, should be used to implement, maintain, and troubleshoot the network as much as possible. The 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 the network 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
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

An architecture that internalizes these management elements in the design process is likely to be easy to manage. Faults are managed 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. Configurations can be managed via third-party tools that manage and execute scripts, or through GUI-based systems that enable the operator to make bulk changes throughout the managed network. Accounting management is essential in environments where multitenancy, or "pay to play" are in use. In an architecture that aggregates multiple business units with discreet billing and service requirements, the ability to tie usage to those accounts is a necessity. Performance management enables the organization to verify the attainment of service-level agreements, either between the enterprise and the service provider, or between the enterprise IT organization and the underlying business units (internal SLAs). Finally, security management is essential to the management of an enterprise WAN 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 to the solution and enhances the management, security, and accountability of the underlying network design.

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 very little change required. A network architecture that is designed and preconfigured 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 supports WCCP is ready to add caching and acceleration services without requiring extensive changes to the network design. Other services that should be considered 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.

A complete enterprise WAN solution that meets these design goals is built to be scalable, flexible, and services ready. Next, we provide a brief overview of the portions of the Juniper Networks enterprise WAN solution.

The Juniper Networks Enterprise WAN Solution

The Juniper Networks enterprise WAN solution is composed of a collection of configuration scenarios that can be combined in modular fashion depending on an organization’s networking and business needs. The solution is built upon the following modular building blocks:

- Aggregation Hub
- Internet Gateway
- Secure Overlay (IPsec VPN)
- Services
- Documentation

The target markets for this solution include any organization that has a wide base of hub sites with a high degree of interconnectivity demands within the enterprise. 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 established by the Juniper Networks enterprise WAN solution. Large enterprises are the mostly 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 the enterprise with 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 is configured to provide 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 component.

Aggregation Hub

There are several modular configuration options for the aggregation hub. 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 Types

Deployment Scenario		Platform	Transport	Head End Router (MX240)
Dual Router Dual Circuit	Large	MX	L3VPN/L2VPN	WAN Aggregation
		M7i	Internet	VPN, WAN Aggregation
Single Router Single Connection	Small	SRX	Internet	
	Medium	MX	Private WAN	WAN Aggregation
		M7i/SRX	Internet	VPN, WAN Aggregation
Single Router Dual Connection	Medium	M7i	Internet	VPN, WAN Aggregation
		MX, M7i	Private WAN	WAN Aggregation
			L3VPN/L2VPN	WAN Aggregation

The aggregation hub configurations provided in the solution design and implementation guide 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 (Figure 8).

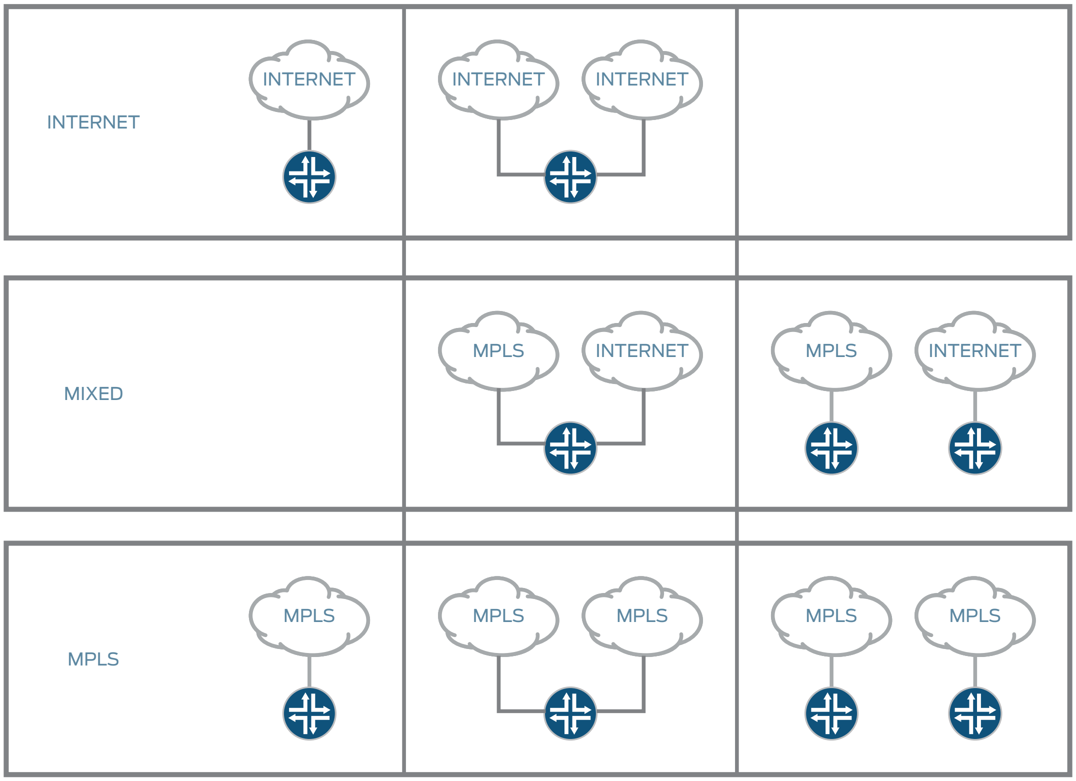


Figure 8: Enterprise WAN deployment scenarios

The Juniper Networks enterprise WAN solution provides configurations for each deployment scenario, design recommendations and troubleshooting information to assist in deploying a new WAN aggregation hub as well as configurations for the remote sites connecting into the aggregation hub. The configurations are tested in Juniper solutions labs and are tested against scalability targets, resiliency and convergence targets, and performance targets. Details on the specific configurations can be found in the *Enterprise WAN Design and Implementation Guide*.

Internet Gateway

The Internet gateway deployment scenario is a foundation of the WAN aggregation deployment scenario. The Internet and mixed aggregation scenarios require working Internet gateway functionality in order to properly provision WAN aggregation. The Internet gateway is used to provide Internet access to hub site users, or more commonly, to provide a public transit for IPsec VPN connection back to the headquarters or data center (Figure 9). In many cases, the hub Internet traffic is provided via backhaul 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 design scenario.

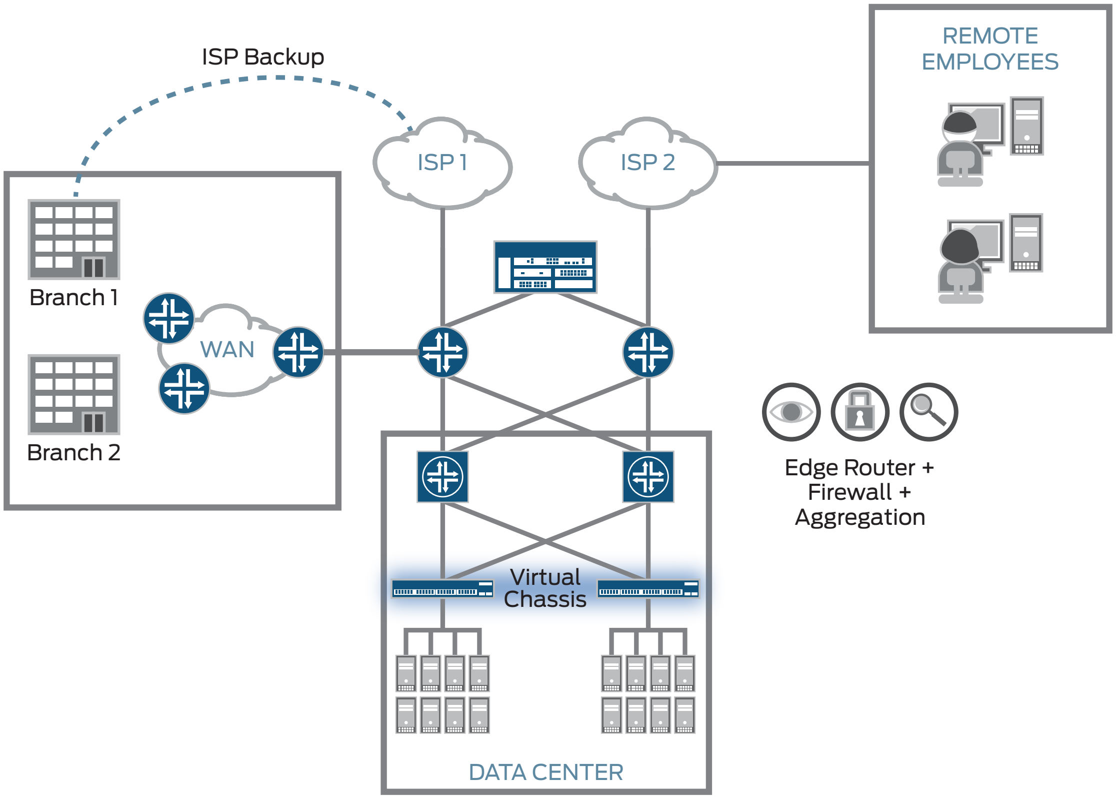


Figure 9: The Internet gateway

The Internet edge module of the larger WAN aggregation solution component provides carrier-class routing and security to regional enterprise sites that have a requirement for localized Internet access. The local access either provides direct Internet connection to the enterprise remotes, or it provides a transit network to enable 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 posture of the enterprise remotes. Services such as dynamic NAT, access lists to whitelist or blacklist-specific destinations, stateful firewall and intrusion detection and prevention services, and active/active load balancing to multiple ISPs are all key components of the solution.

Secure Overlay

Secure overlay is a component of the Enterprise WAN solution that enables branches with limited provider MPLS options to gain access to the enterprise. In these instances, a branch office or home user obtains Internet access from whatever local provider is available (via DSL, cable, or even satellite). The enterprise then provides a managed, pre-configured device to provide IPsec services to the home user. An alternative access method is via a secure client on the home user's computer that allows software-encrypted access to the enterprise. In any event, 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 at a point closer to the Internet edge.

Services

The Juniper Networks enterprise WAN solution is services ready, but what services might an enterprise want to bring into the network? The Juniper solution supports Web Cache Communication Protocol (WCCP) to enable WAN acceleration devices to enhance the user experience where required. Other services that can be supported as inline, network-driven security services are stateful firewalling and deep packet inspection. In cases where the enterprise is hosting 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. Finally, for enterprises that utilize real-time or recorded video content (such as financial streams to banking centers or video lectures within the education sector), the enterprise WAN solution supports the inclusion of 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 Juniper Networks enterprise WAN is able to add these services in line with little to no disruption of the user experience.

Documentation

The Juniper Networks enterprise WAN solution solves the challenges of cost and complexity in the WAN aggregation operation of large enterprises. The solution is verified by Juniper solution testing, a detailed framework that tests the solution for scale, stability, and performance. Juniper solution testing provides the peace of mind and confidence that the solution behaves as described in a production environment.

The *Enterprise WAN Design and Implementation Guide* is a solution document written for architects and engineers. The DIG starts with a high-level overview of the challenges and then drills down into the details and options that make up the enterprise WAN solution. The DIG is a key point of reference for building an enterprise WAN and WAN aggregation network using Juniper Networks platforms. The key areas of the DIG are:

- **Business requirements and segment overview**—This provides a foundation for understanding the challenges that must be overcome to implement a mobile backhaul solution.
- **Design recommendations and considerations**—These weigh the possible configuration choices and provide guidance on the recommended design of a mobile backhaul network.
- **Solution implementation and configuration**—This illustrates how to implement the solution in a production environment.

Enterprise WAN Solution Benefits

The Juniper Networks enterprise WAN solution offers the following benefits to the large enterprise seeking to utilize private MPLS or hybrid overlay network design in combination with WAN aggregation:

- Improved operational efficiency
- Reduced operational expense
- Flexibility and value for investment
- Security
- Carrier-class reliability

Improved Operational Efficiency

The large enterprise can simplify the network by adding regional WAN aggregation routers to a private MPLS or hybrid overlay network. Using Juniper Networks MX Series 3D Universal Edge Routers, the WAN aggregation architectures in the enterprise WAN solution support various link speeds including 10 Mbps all the way through 100 Gbps interfaces. For non-Ethernet interfaces, the MX Series supports DS3 through OC192. The aggregation of multiple low-speed connections to hub sites into a regional aggregation tier that supports high-speed backhaul, the enterprise enables a single point of regional management and improves the potential performance of all connected hub sites by providing high-speed services from the region to the headquarters. The design also uses a single operating system (Juniper Networks Junos® operating system) on all routers, from the aggregation hubs to the small CPE devices used at remote sites (or by home users). This enables operational simplicity by standardizing the operating system within a region, saving network operational time in provisioning and troubleshooting within the WAN aggregation tier.

Reduced Operational Expense

Regional aggregation of enterprise remotes enables the enterprise to provide lower-speed local uplinks to the sites in region. The aggregation hub then provides a higher-speed backhaul transit to the headquarters. The enterprise can control the configuration from the hub to aggregation and across the backhaul to headquarters. This level of control enables a better user experience as the class of service and security services are configured and maintained by the enterprise. The WAN aggregation model enables the enterprise to provide high-speed services to regional remotes at potentially lower cost, utilizing the low-speed links to aggregate remotes to a higher-speed transport.

Improved Flexibility and Value for Investment

The MX Series of routers supports a wide array of upgradeability 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 the enterprise remotes. The MX Series also supports a wide array of interface types, enabling an enterprise remote to upgrade from legacy circuits to high-speed Ethernet easily, as the uplink is performed only between the remote and the aggregation hub. Finally, the network is built for elasticity and performance. Combining a robust class-of-service implementation with backhaul features such as MPLS traffic engineering (TE) and virtual private LAN service (VPLS), the enterprise can more effectively guarantee application performance to the remotes, 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 by the solution. This logical separation enables the enterprise to control not only whom on the outside each operating group can communicate with, but it controls communication and leaks between operating groups within the same enterprise.

Carrier-Class Reliability

The ability to keep the enterprise running is another key benefit of the Juniper Networks enterprise WAN solution. The MX Series routing platform is a carrier-grade component designed with full resiliency at its core. The hardware is designed for resiliency, utilizing redundant control plane and switching plane hardware as well as redundant power and cooling. In a design model where the enterprise is acting 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 large enterprise is under constant pressure to reduce cost, improve performance, and simplify network operations. The Juniper Networks enterprise WAN solution addresses these challenges by providing enterprise-class WAN aggregation and a mix of public and private transports and configurations that suit most any large enterprise seeking to aggregate its regional remote sites.

Additional Reading

Implementing VPLS for Data Center Interconnectivity:
www.juniper.net/us/en/local/pdf/implementation-guides/8010050-en.pdf

Branch SRX Series and J Series Selective Packet Services:
www.juniper.net/us/en/local/pdf/app-notes/3500192-en.pdf

Junos Enterprise Routing by Doug Marschke and Harry Reynolds. O’ Reilly Media.

Enterprise Internet Edge:
www.juniper.net/us/en/local/pdf/solutionbriefs/3510393-en.pdf

Enterprise WAN Aggregation:
www.juniper.net/us/en/local/pdf/solutionbriefs/3510398-en.pdf

Enterprise Data Center Interconnectivity:
www.juniper.net/us/en/local/pdf/solutionbriefs/3510392-en.pdf

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 +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

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

8030013-001-EN Jan 2014 ♲ Printed on recycled paper