CAMPUS LAN DESIGN GUIDE

Design Considerations for the High-Performance Campus LAN

Table of Contents

Table of Figures

Introduction

The corporate LAN has evolved from a passive background business component to a highly active, highly visible core asset that enterprises rely on to support day-to-day operations critical to their market success. Today's network is a strategic instrument that must be accessible any time from anywhere—simultaneously offering fast, secure, reliable services at scale regardless of location. It has also evolved from traditional client/server data flow support to peer-to-peer flow support, and it must also accommodate an increasing number of devices and services. In addition to centralizing applications and data centers, enterprises are consolidating servers and data centers to simplify operations and reduce costs. Existing campus infrastructure solutions cannot meet the requirements needed to provide secure and reliable high-performance access for campus users, nor do they provide the centralized management capabilities critical for reducing costs and streamlining operations.

A new campus LAN design that meets campus security, connectivity, and performance challenges while enabling key IT initiatives is needed. It also must scale, offer operational simplicity, and flexibly accommodate new computing trends without an entire redesign.

Campus Overview

The term campus, when used in this document, refers to a main enterprise location consisting of one or more buildings in close proximity at the same locale. A campus is usually, though not necessarily, the corporate headquarters or a major site. A multi-floor office building housing an enterprise, a corporation with several buildings in an office park complex, and the sprawling facilities making up a university are all examples of a campus. All buildings and floors on the campus are connected to shared resources and services in a data center, which may or may not be part of the campus, via a campus LAN or WAN connection. The campus may also be connected to remote locations such as branch and regional offices via a WAN.

As most business processes are carried out online, any campus LAN downtime or inefficiency has a negative impact on the corporate bottom line. Secure, high-performance, highly available LAN services are crucial to ensure that each campus facility is always online so that business productivity and customer satisfaction are maximized. This document focuses on the challenges and considerations facing today's enterprise so that they may plan and create a LAN meeting those requirements.

The campus LAN is made up of three main layers: the access layer, the aggregation layer, and the core layer. Each layer, covered in more detail further in this document, provides a set of services to the enterprise that require a series of considerations and address a set of challenges.

Services Needed in the Campus LAN

The campus LAN must provide the following high-level services to optimize efficient business operations:

- LAN Connectivity—The campus infrastructure must provide secure wired and wireless LAN connectivity for an increasing number of IP devices such as computers, telephones, PDAs, surveillance cameras, smartphones and more.
- Security—Security is critical to all campus LAN services. Access to networks and applications must be open and pervasive, yet remain secure and controlled. Today's networks not only need to effectively handle unmanaged devices and guest users attempting network access, they also need to address support for unmanageable devices, post admission control, and application access control, visibility, and monitoring. Key security components and policies include:
    - Policies ensuring Quality of Service (QoS)
    - Mitigating denial of service (DoS) and distributed denial of service (DDoS) attacks and threats
    - Ensuring that the organization meets compliance criteria

  All security policies should be centrally managed and remotely deployed.
- Unified Communication—Deployment of VoIP phones using Power over Ethernet (PoE) technology, as well as video conferencing and web-based training through video on demand (VOD) applications, over the same campus LAN infrastructure as data calls for the logical separation of delivery of these services. Implementation of QoS policies is also needed to prioritize and guarantee delivery of latency/jitter, and loss sensitive VoIP and video traffic over data.

- High Performance—LAN-like application performance must be provided at all times throughout the campus. Moderate oversubscription is common in the LAN access layer but line-rate performance is highly desirable in the LAN aggregation and core layers.
- High Availability (HA)—Downtime is not an option in today's campus LAN. It must offer at least five nines or 99.999 percent of reliability with a goal of approaching the level of service provided by the public switched telephone network (PSTN). HA should be addressed throughout the LAN design. Networking equipment and software that is cost-effective, feature-rich, highly reliable, and offers centralized management capabilities is vital to reduce downtime and operational costs. Robust, reliable connectivity is also required. In addition, emerging technologies such as unified communications depend on an optimized and always-on, high-performance network from end to end to function effectively.
- Centralized Management—A key service required in a campus LAN is centralized management of all network switches, firewalls, routers, VPN, and intrusion detection and prevention (IDP) devices. Centralized management solutions reduce the time and expense required to configure and manage network devices. In addition, network traffic can be more easily analyzed with such a system, facilitating network performance optimization.

Each of these areas is addressed in more detail in this document and, when appropriate, additional considerations or challenges for a specific service or feature are presented.

Scope

This design guide proposes practices, technologies, and products that help campus architects and engineers design a modern campus LAN.

It also introduces issues related to changing campus needs and presents practices, technologies, and design considerations for campus architects and engineers. In addition, this guide shows how infrastructure solutions from Juniper Networks allow businesses to advance the economics of networking through a truly innovative, game-changing operating environment that helps them increase revenue and raise productivity today and into the future.

Campus LAN Design Considerations

A new campus LAN design is needed as legacy solutions cannot meet these key requirements, nor reduce costs and streamline operations. The new LAN design must also scale and accommodate emerging computing trends and additional network services without an entire redesign. The following section summarizes some of the trends and technical considerations for designing a modern campus network to address these requirements. These considerations are not necessarily specific to Juniper Networks solutions and may be applied universally to any campus network design, regardless of the vendor.

Enterprise Computing Trends

In addition to the services previously mentioned, the following trends must be considered in a campus LAN design:

- Proliferation of unified communications

  The adoption of unified communications including voice, video, and data services is on the rise. According to Forrester Research (2006), 46 percent of all companies in North America have installed IP telephony systems and 39 percent use VoIP to communicate with their remote users. Such deployments have a direct impact on the high-performance and high availability requirements of a campus LAN. For example, not only must adequate LAN and WAN bandwidth be provisioned, but QoS rules must identify, classify, and prioritize traffic to deliver effective VoIP communication services.
- Bandwidth-hungry applications

  In addition to the increased bandwidth needed for unified communications, many popular business applications such as Oracle, SAP, and PeopleSoft have introduced web-enabled versions that require, in some instances, more than 10 times the bandwidth of their LAN-based counterparts, seriously impacting performance, reliability, and availability. Though it's recommended to schedule data backup to local servers during times of low network usage, it's possible such network services could be bandwidth intensive.

- User productivity

  Since most business processes are now carried out online, the corporate LAN is a critical component of business growth and innovation. Because of that, any LAN downtime or inefficiency negatively impacts the corporate bottom line. Conversely, boosting network performance enhances business productivity, according to Information Week (2007). As such, the network must be leveraged with services such as wireless coverage and remote access to maximize productivity.

- Increasing focus on security

  FBI/CSI statistics show that 72 percent of all companies surveyed reported at least one security incident in 2006. And there continues to be a proliferation of both internal and external attacks. Not surprisingly, a 2006 Forrester Research survey found that 57 percent of all firms consider "upgrading security environment" a top priority. As critical business processes become more distributed and unified communications present new vulnerabilities, the need for robust security is likely to intensify. User access policies are needed.

- Demand for wireless services

  One of the main drivers of better business decisions is access to key information and resources at all times. Employees of modern business go to meetings with their laptops in tow, expecting wireless access to all of their applications, data stores, resources, and services. Not only must wireless service be provided throughout the campus, but it should enable users to seamlessly move across the campus without service disruption, much like roaming cell coverage. Such wireless service enables users to access whatever materials are needed to support a presentation or budget forecast, start a download from a centralized server and have it finished by the time they get to the conference room with their laptop, or talk on a Wi-Fi phone throughout the campus.

  Wireless service and access must always be secure. Different levels of wireless access must be provided for contractors, partners, and other guest users, ensuring not only that the proper level of service is delivered but that access to the appropriate resources is restricted.

- Server centralization and data center consolidation

A 2007 Forrester report states that 51 percent of all firms consider server centralization a key priority. Gartner (2007) also reports that most enterprise servers operate at 20 percent capacity. New technologies like virtualization are needed to better utilize these resources. At the same time, most campuses need local servers that require extra security, bandwidth optimization, and traffic prioritization.

To further reduce costs, simplify operations, and comply with regulatory guidelines, enterprises are also consolidating data centers. According to a 2006 Nemertes Research report, 91 percent of companies interviewed were under compliance constraints and more than 50 percent of the companies had consolidated their dispersed data centers into fewer larger data centers in the last 12 months, with even more planning to consolidate in the next 12 months.

In addition to high availability requirements ensuring nonstop operations, centralization raises new latency and security issues. Centralized management solutions that help reduce the time and resources devoted to keeping campuses online and operational are also needed.

Infrastructure Solutions

The network infrastructure of today's campus is no longer sufficient to satisfy these requirements. Instead of adding additional costly layers of legacy equipment and highly skilled IT resources to support the growing number of devices and services in the campus network, enterprises need a new, more integrated and consolidated campus solution.

Juniper Networks delivers a proven IP infrastructure for the campus that meets these challenges, enabling the performance, scalability, flexibility, security, and intelligence needed to not just meet but increase campus user productivity. Juniper Networks offers flexible configurations and price points that meet the needs of all campuses, while delivering high-performance throughput with services such as firewall, Juniper Networks Adaptive Threat Management Solutions, VPN, MPLS, IPV6, and Connectionless Network Service (CLNS).

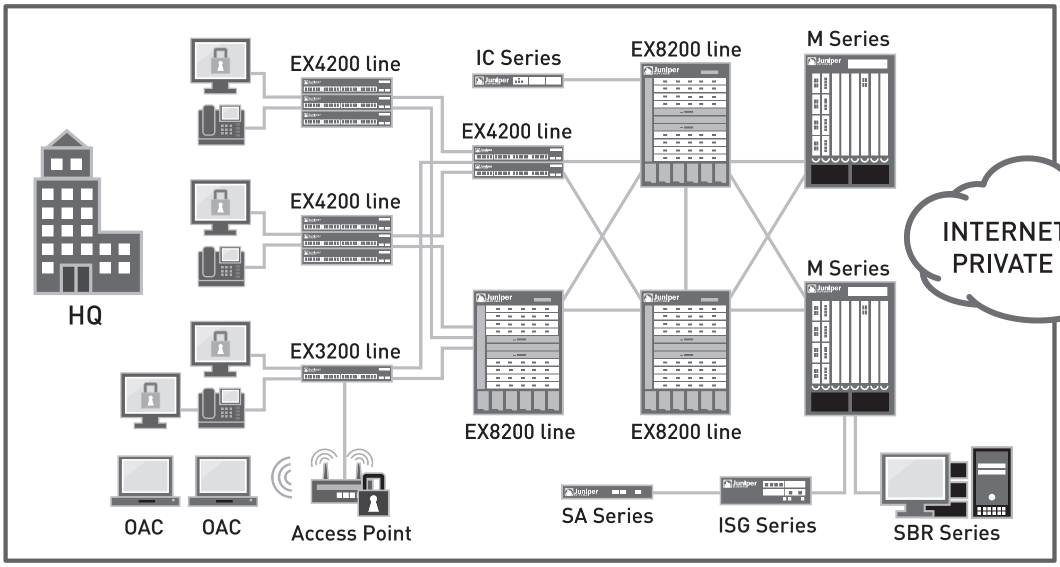


Figure 1: Highly available campus LAN configuration

Campus Architecture Overview

Layered Approach

An enterprise campus LAN architecture may span up to three layers, from desktop devices connected to wiring closet switches at the access layer to the core layer at the center of a large campus LAN. The hierarchical topology segments the network into physical building blocks, simplifying operation and increasing availability. Each layer within the hierarchical infrastructure has a specific role.

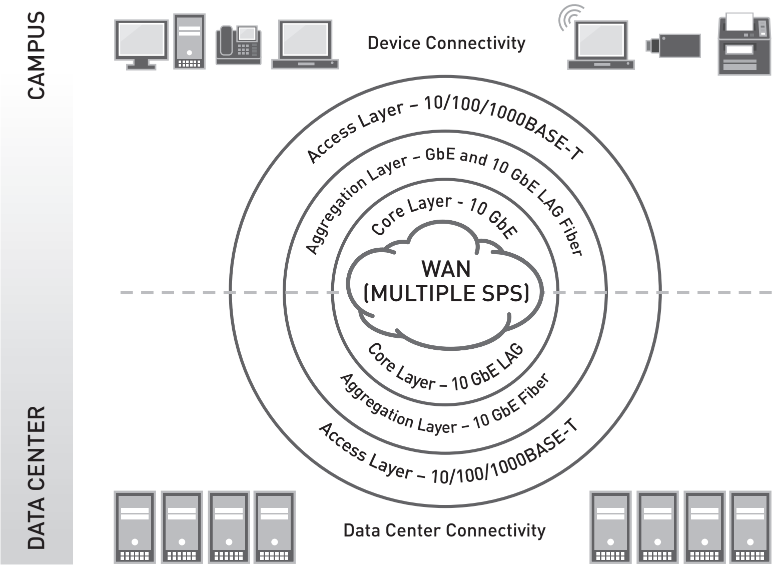

CAMPUS
Device Connectivity
Access Layer – 10/100/1000BASE-T
Aggregation Layer – GbE and 10 GbE LAG Fiber
Core Layer - 10 GbE
WAN
(MULTIPLE SPS)
Core Layer – 10 GbE LAG
Aggregation Layer – 10 GbE Fiber
Access Layer – 10/100/1000BASE-T
DATA CENTER
Data Center Connectivity

Figure 2: The layered approach

- The access layer provides an access control boundary and delivers network connectivity to end users in a campus.
- The aggregation layer aggregates connections and traffic flows from multiple access layer switches providing a core enforcement perimeter as it delivers traffic to core layer switches.
- The core layer provides secure connectivity between aggregation layer switches and the routers connecting to the WAN and the Internet to enable business-to-business collaboration.

This document focuses primarily on how these layers are deployed in the campus network. Areas outside of that scope are presented when relevant to the discussion. For example, certain campus configurations may collapse one or more layers.

Benefits and Challenges to the Layered Approach

A multilayered architecture facilitates network configuration by providing a modular design that can rapidly and economically scale. It also creates a flexible network on which new services can be easily added without redesign. The layered approach also delivers separated traffic, balances load across devices, and simplifies troubleshooting.

This three-layered approach traditionally requires additional hardware and can be costly to configure, deploy, and administer for small campuses. To account for that, small campuses may collapse one or more layers.

Note: This document deals primarily with three-layered LAN designs, though it also introduces a two-layered design with a converged aggregation and core layer. Those supporting extremely small campuses may wish to view the Juniper Branch LAN Design Guide for LAN designs that collapse multiple layers.

Trying to address emerging bandwidth, throughput, and port density requirements, networks in the past have grown bloated with extra layers of inefficient, ill-suited legacy hardware that not only fails to meet these needs, but also adds considerable management complexity, reduces network availability, and drives up capital and operational expenses.

A Network Revolution

A recent entrant into the evolving switching market, Juniper Networks has factored lessons learned and experiences into the development of a new portfolio of Ethernet switch products and network solution designs that address contemporary issues and accommodate future growth. These new products are designed to eliminate unnecessary network layers while providing a platform for delivering higher availability, converged communications, integrated security, and higher operational efficiency. With these solutions, Juniper Networks simultaneously advances the fundamentals and economics of networking by delivering greater value, increasing simplicity, and lowering the total cost of network ownership.

Implementation: Access Layer

The campus access layer provides network connectivity to end users by connecting devices such as PCs, printers, IP phones, and CCTV cameras to the corporate LAN via wired or wireless LAN (WLAN) access points. Access layer switches typically reside in the wiring closets of each floor in each campus facility.

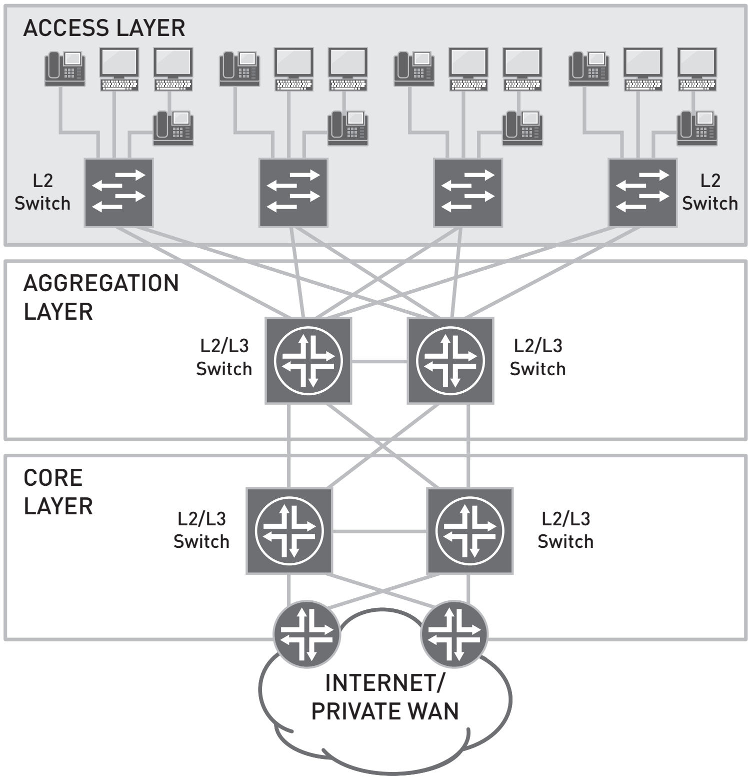


Figure 3: Access layer at a highly available campus LAN

The access layer provides connectivity, Power over Ethernet (PoE), quality of service (QoS), and security with policy services and network access control.

Access Layer Design Considerations

Wired Port Connectivity

Accounting for an adequate number of wired ports for all computers, IP phones, CCTV cameras, WLAN access points, and other IP devices is the first step to addressing port requirements. The logical segmentation required and the number of logically separate networks that should share the same LAN must also be determined. Access layer switches must be scalable and provide HA features in addition to over-provisioned and underutilized Gigabit Ethernet or 10-Gigabit Ethernet uplinks to aggregation layer switches. These considerations help establish what type of hardware configuration is needed.

WLAN Connectivity

Ideal for employees meeting in conference rooms or areas other than their offices, as well as contractors, partners, and guests, wireless access must be provided across the campus. With the plethora of IP devices available on the market and used in the workforce, especially by unknown guests, a comprehensive security policy must ensure that only trusted devices access the campus network. Further, the appropriate LAN resources must be restricted and made available only to those with the proper credentials. This is especially true for contractors, partners, and other guests. Seamless coverage enabling a user to roam the campus with the same login credentials is also expected.

There are two main designs for flexible and roaming wireless solutions:

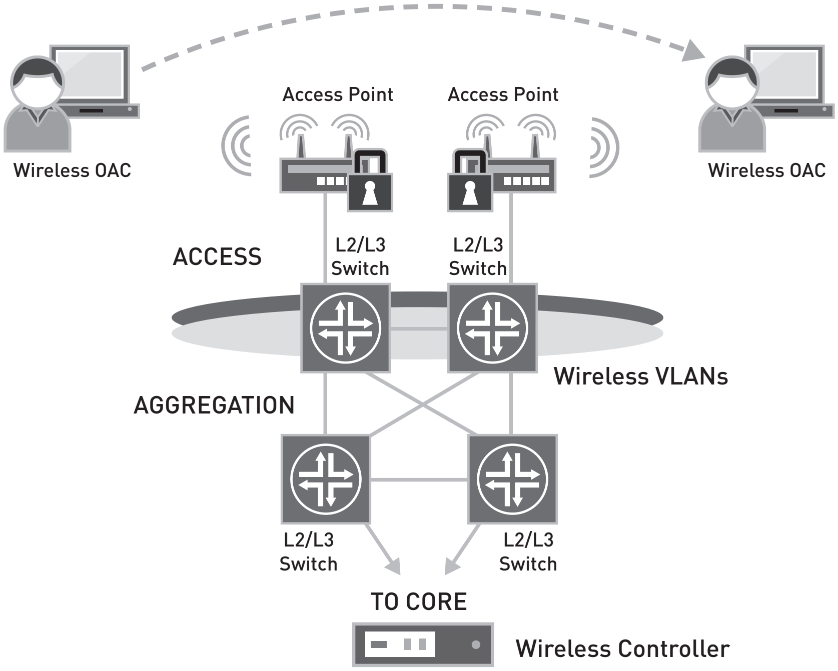


Figure 4: Flexible and roaming wireless access solutions

- Non-controller based wireless access—In this design, an 802.1Q trunk for access point to switch is required. Roaming requires spanning at least two VLANs between access layer switches.
- Controller-based wireless access—This design uses a virtualized, centralized wireless controller. Access point VLANs are placed local to the access switch. Roaming does not require spanning VLANs across the campus network.

PoE

Nearly all campuses have IP phones today, most of which require PoE to function. Campus facilities are likely to also have PoE security cameras and WLAN devices. Accounting for the correct number of PoE ports is vital as the system configuration depends on it. Some access equipment doesn't provide PoE services, so it's important to make sure to use traditional wall powered IP phones, CCTV cameras, and WLAN access points in those installations. In addition to accounting for the number of PoE ports, it is important to determine the level of power needed for the devices connected to each port. Many devices requiring PoE will use up to 15.4 watts, the maximum allowed for class 3 PoE.

However, there are some devices such as security cameras with advanced pan, tilt, and zoom functions and IEEE 802.11n WLAN access points that may need more than 15.4 watts of PoE.

Virtual LAN and Spanning Tree Protocol

Campus LANs use VLANs to logically group sets of users, devices, or data, regardless of location, into logical networks through software configuration instead of physically relocating devices on the LAN. VLANs help address issues such as scalability, security, and network management.

VLANs are in essence Layer 2 broadcast domains that exist only within a defined set of switches. Using the IEEE 802.1Q standard as an encapsulation protocol, packets are marked with a unique VLAN tag. Tagged packets are only forwarded or flooded to stations in the same VLAN. To reach any station not belonging to the same VLAN, tagged packets must be forwarded through a routing device. Any switch or switch port can be dynamically or statically grouped into a VLAN. Alternately, traffic may be grouped into a VLAN and forwarded through specific ports based on the specific data protocol being sent over the LAN. For example, VoIP traffic from a softphone can be segmented from other traffic and put into a VLAN that gets a higher quality of service.

- Spanning Tree Protocol (STP)

  VLANs may create multiple active paths between network nodes, resulting in problematic bridge loops. Since the same media access control (MAC) addresses are seen on multiple ports, the switch forwarding table can fail. Also, broadcast packets may end up being forwarded in an endless loop between switches, consuming all available bandwidth and CPU resources. STP, the IEEE 802.1D standard, ensures a loop-free topology for any bridged LAN. STP is designed to leave a single active path between any two network nodes by first creating a tree within a mesh network of connected LAN switches and then disabling the links which are not part of that tree. STP thus allows a network design to include redundant links to provide automatic backup paths if an active link fails—without the danger of bridge loops or the need for manual enabling/disabling of these backup links. Each VLAN can run a separate STP instance.

- Issues with STP

  Troubleshooting may be challenging with STP due to complicated routing, incorrect configuration, or improper cabling. Since every packet must go through the root bridge of the spanning tree, routing performance with STP can also be suboptimal. STP often creates underutilized links and lacks a load-balancing mechanism as well. In addition, STP has a slow convergence of up to 30 to 50 seconds after a topology change. To combat this, Rapid STP (RSTP) was created, providing sub-second convergence. Multiple STP (MSTP), the 802.1s standard, supports multiple instances of STP but also increases configuration complexity.

Using Layer 2 versus Layer 3 at the Access Layer

Access switches are configured to use Layer 2 or Layer 3.

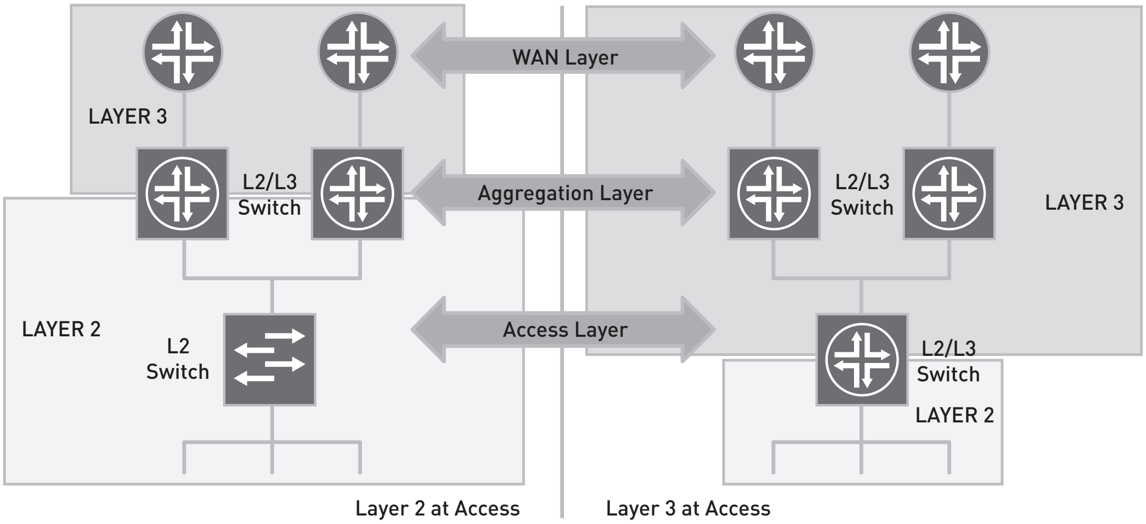


Figure 5: Layer 2 versus Layer 3 at the access layer

- Using Layer 2 at the access layer

  Using Layer 2 at the access layer is the traditional configuration. This provides plug-and-play configuration and makes the deployment in smaller networks easier to implement and manage.

  There are a number of challenges associated with this option. This configuration usually requires STP, resulting in multiple connections, one active and one redundant. The demarcations from L2 and L3 with OSPF add multiple fault isolation domains, which add extra complexity in configuring and managing the network. Troubleshooting can also be more difficult in such configurations. In addition, convergence in case of a switch or link failure often takes too long to ensure a highly-available campus LAN.

- Using Layer 3 at the access layer

  Routing is enabled on the switch when using Layer 3 at the access layer, but it still provides the capability to put users into different VLANs. Layer 3 is more deterministic. No Layer 2 loops are created in this design. Layer 3 should be configured in the uplinks from the access switch to the aggregation layers, with Layer 2 configured at the access switch to the devices. STP can be enabled to prevent inadvertent loops. Or STP can be disabled and bridge protocol data unit (BPDU) protection enabled, making it easier to troubleshoot. When STP is disabled, OSPF or other open-standard protocols can be used to provide sub-second convergence. For larger or more complex networks, this is a low maintenance solution in comparison to using Layer 2 at the access layer. This option is more costly to deploy with legacy network equipment, as Layer 3 usually requires an additional license fee.

- Recommendation

  Unlike competitive products, Juniper Networks solutions provide the ability to deliver either Layer 2 or Layer 3 at the access layer without any added expense, as Layer 3 features are built into the base Juniper Networks® JUNOS® Software license with no extra license fees required. Instead of STP, Juniper solutions also use open-standard protocols such as OSPF with equal-cost multipath (ECMP) for rapid convergence. LAN designs using Juniper Networks EX4200 Ethernet Switch with Virtual Chassis technology also benefit from Redundant Trunk Group (RTG) protocol as a built-in, optimized replacement to STP for sub-second convergence and automatic, high-performance load balancing. And, according to an independent 2007 Lake Partners[1] study, operating expense with Juniper Networks solutions can be up to 29 percent lower than competitive solutions. Juniper switches with Virtual Chassis technology provide simplified device management as well, equating to lower CapEx and OpEx compared to competing solutions.

Considerations for Implementing Unified Communications

Delivering voice, video, and data on a single network infrastructure offers many cost savings and operational simplicity benefits. It lowers communications expense, decreases the overall cost of network ownership, and simplifies network administration and maintenance operations. However, a single network infrastructure also presents a number of network challenges including QoS, security, and port configuration requirements.

Unified communications have real-time requirements that are not necessary for most data applications. VoIP packets, for example, must be efficiently transported throughout the LAN and WAN to ensure high-quality voice communications, even when the network is experiencing high utilization or congestion. Simply adding more LAN or WAN bandwidth doesn't make the network voice-friendly. Latency, jitter, and packet loss are common VoIP challenges that must be accounted for with QoS queuing and scheduling to ensure high-quality VoIP communications. In addition to access-based security measures, addressing port density and PoE requirements for IP phones is fundamental to a successful design.

1. Quality of service

   Access layer devices must be able to identify, classify, and queue traffic across the LAN to ensure optimal performance or QoS. Once identified, traffic is properly assigned and managed to ensure that each application, such as unified communications, delivers satisfactory performance across the entire LAN.

   - Classification and enforcement

   Each type of data flow on the LAN has different QoS requirements. Traditional applications such as Web browsing and email work fine with the best-effort delivery standard on IP networks. However, additional requirements must be met to ensure effective delivery of voice, video conferencing, and other real-time applications. Unlike streaming video, for example, real-time voice data can't be cached or have lost packets retransmitted since both would

[1] How Operating Systems Create Network Efficiency - Lake Partners Strategy Consultants, Inc 2007

add an unacceptable delay and ruin the quality of the communication, resulting in a poor user experience. Voice packets, therefore, must be given top priority when creating QoS policies.

IP phones and other communication devices are likely to be spread throughout the LAN in many different physical locations. VLANs, as discussed earlier, can be used to identify and segment voice, video conferencing, and data traffic, regardless of location, into logical VLANs so that the appropriate QoS parameters can be easily applied to maintain optimal service for each data flow.

To facilitate QoS, data can be classified by a combination of MAC address, IP address, physical port, and protocol. For example, a block of IP phones connected to a specific LAN segment could be placed in a VLAN designated for voice traffic based on the IP phone port numbers. Link Layer Detection Protocol-Media Endpoint Discovery (LLDP-MED) may also be used to discover an IP phone and automatically place it on a VLAN. Or traffic from a softphone can be analyzed at the protocol level, with voice data given top priority regardless of the source port. Once the data is classified with the appropriate Differentiated Services code point (DSCP), it must be queued and scheduled. Most important, the same QoS rules must be enforced consistently throughout the LAN and WAN.

- Built-in QoS

QoS and class of service (CoS) features are built into all Juniper infrastructure, security, and application acceleration solutions. All Juniper Networks switches and routers run JUNOS Software, which comes standard with a full complement of QoS services. Juniper Networks EX Series Ethernet Switches, for example, support eight hardware queues per port and offer a range of policing options from best-effort delivery to enhanced delivery and assured delivery. Since the same JUNOS Software operating system is found across all Juniper router and switch solutions, the same QoS policies can be used throughout the LAN and WAN design for easy and consistent traffic management. In addition, ASICs in all Juniper solutions support QoS by processing prioritized data and minimizing CPU load.

Note: For more information on VoIP QoS, read Juniper pub# 351113-001 August 2005: VoIP on the WAN: It's a Matter of Priorities.

2. Security

Implementing unified communications on the data network increases security exposures that can have serious service impacts. Malicious attacks from outside the network and inadvertent attacks within the network must be prevented. New ways of toll fraud and new security risks like eavesdropping are being discovered at an ever-increasing rate. Additional points of entry are created; a hacked VoIP system now provides a back door to the corporate LAN. Security risks range from viruses, worms, and denial of service (DoS) attacks to unauthorized access. Deployment of VoIP solutions, similar to other network appliances, must account for security of the device itself as well as how it can be used to attack the network as a whole. Juniper Networks IDP Series Intrusion Detection and Prevention Appliances are recommended to thwart VoIP-related attacks as well as typical intrusions. An 802.1X solution should be used to authenticate and manage endpoints via policy-based access. For VoIP phones that do not support an 802.1X client, one can use the MAC-based authentication feature on the EX Series switches to authenticate the phones. Using the protocol-specific application-level gateway (ALG) features on all firewalls is recommended to dynamically open and close ports for each VoIP call.

Threat Containment

It is vital that the access layer include integrated security features to guard against intruders or other external threats such as DDoS attacks. An extra layer of security should be provided by first authenticating users and performing virus checks, then enforcing precise, end-to-end security policies that determine who can access what network resources, as well as QoS policies to ensure delivery of business processes.

Modular Chassis Technology

A campus LAN must be able to quickly and seamlessly accommodate growth and new technologies economically from capital, network overhead, and network operational expense perspectives. This is often addressed at the access layer via modular chassis solutions.

Ideal modular solutions should offer high-density, high-speed ports with optional, cost-effective PoE capabilities. Each modular chassis should also offer high-speed uplink connections and provide the same type of HA features found in traditional chassis-based solutions. The ideal modular chassis solutions should also configure and manage more than one switch as a single Virtual Chassis configuration, dramatically reducing both capital and operating expense while providing additional HA features.

Access Layer Solutions

Scalable Access Solutions with Virtual Chassis Technology

Juniper Networks provides scalable access solutions with true innovation—EX4200 Ethernet Switches with Virtual Chassis technology. This solution advances the economics of networking by delivering the HA and high port densities of a modular chassis in a compact, cost-effective, pay-as-you-grow platform.

1. Features and benefits

   Each compact EX4200 switch offers either 24 100BASE-FX/1000BASE-X ports, 24 10/100/1000BASE-T ports, or 48 10/100/1000BASE-T ports. The 10/100/1000BASE-T platforms offer either full or partial PoE options (partial solutions provide PoE on the first eight ports of the switch; full options provide PoE on all 24 or 48 ports). Each PoE port delivers up to 15.4 watts of power and is compatible with class 0-3 IP phones. The EX4200 switch's built-in LLDEP-MED services help automate and extend the power management of these PoE endpoints as well as assist with inventory management and directories.

   Each EX4200 Ethernet Switch supports optional front panel uplink modules supporting either four Gigabit Ethernet or two 10-Gigabit Ethernet ports for high-speed connections to aggregation or core switches. These uplinks support online insertion and removal.

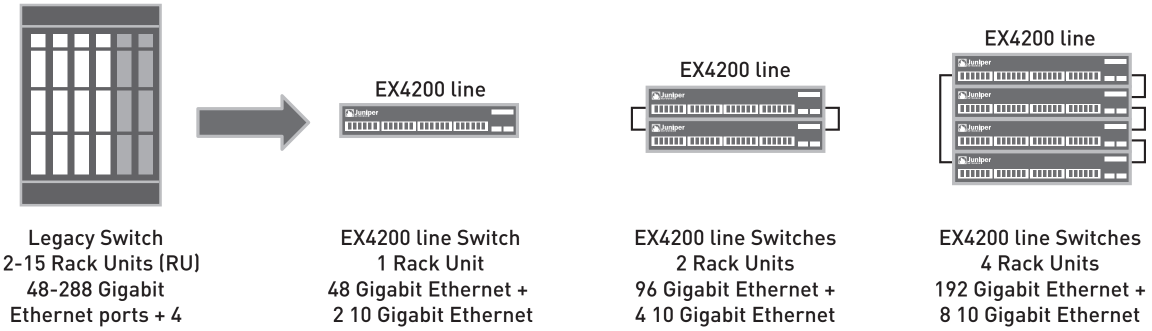


Figure 6: Virtual Chassis technology

2. Pay-as-you-grow scalability

   Juniper Networks Virtual Chassis technology enables a campus to add as many EX4200 switches as needed to meet its connectivity needs. Juniper's unique pay-as-you-grow model allows a campus to start with a single EX4200 switch (1 RU) and incrementally add up to nine more switches to the Virtual Chassis for a total of 10 switches before starting another Virtual Chassis configuration. The switches are interconnected via a 128 Gbps virtual backplane; a Gigabit Ethernet or 10-Gigabit Ethernet uplink module; and a fully loaded Virtual Chassis configuration supporting up to 240 100BASE-FX/1000BASE-X ports, 480 10/100/1000BASE-T ports, or any combination of the two; plus up to 20 10-Gigabit Ethernet uplink ports or 40 Gigabit Ethernet uplink ports, or any combination of the two.

   Not only does Virtual Chassis technology lower capital expenses when compared to traditional chassis systems, it also dramatically reduces operating expenses by enabling any group of interconnected switches to appear on the network and be remotely managed as a single unit. Coupled with the incremental, pay-as-you-grow model, the compact form factor of the Virtual Chassis configuration enables the campus to save not only on upfront and recurring rack space usage but also on costly power and cooling fees. Small campuses on a budget may consider the Juniper Networks EX3200 Ethernet Switch, which provides most of the same robust features as the EX4200 with the exception of Virtual Chassis technology.

3. Carrier-class reliability

   The EX4200 switch with Virtual Chassis technology also provides the same high availability features as modular chassis-based systems. Each switch supports redundant, load sharing, hot-swappable AC or DC power supplies, as well as a field replaceable, hot-swappable fan tray with redundant blowers, any of which can fail without affecting operations.

Virtual Chassis technology provides unparalleled device and link HA using the virtual backplane protocol and JUNOS Software. Each set of interconnected switches with Virtual Chassis technology automatically takes full advantage of the multiple Routing Engines present to deliver graceful Route Engine switchover (GRES) and nonstop forwarding to ensure uninterrupted operation in the rare event that any individual switch fails. For added device and link HA, a Virtual Chassis can be configured to address any requirements. For example, a single Virtual Chassis configuration of 10 switches can be configured instead as two five-switch Virtual Chassis configurations, or in any other desired combination.

4. Location independence

Another key feature of Virtual Chassis technology is that the virtual backplane protocol can also be extended across the optional Gigabit Ethernet or 10-Gigabit Ethernet uplink ports to interconnect switches that are more than a few meters apart, creating a single virtual switch that spans multiple wiring closets, floors, server racks, or buildings. Even when separated by long distances, interconnected switches with Virtual Chassis technology can be managed, monitored, upgraded, and otherwise treated as a single resilient switch, dramatically reducing recurring management and maintenance costs.

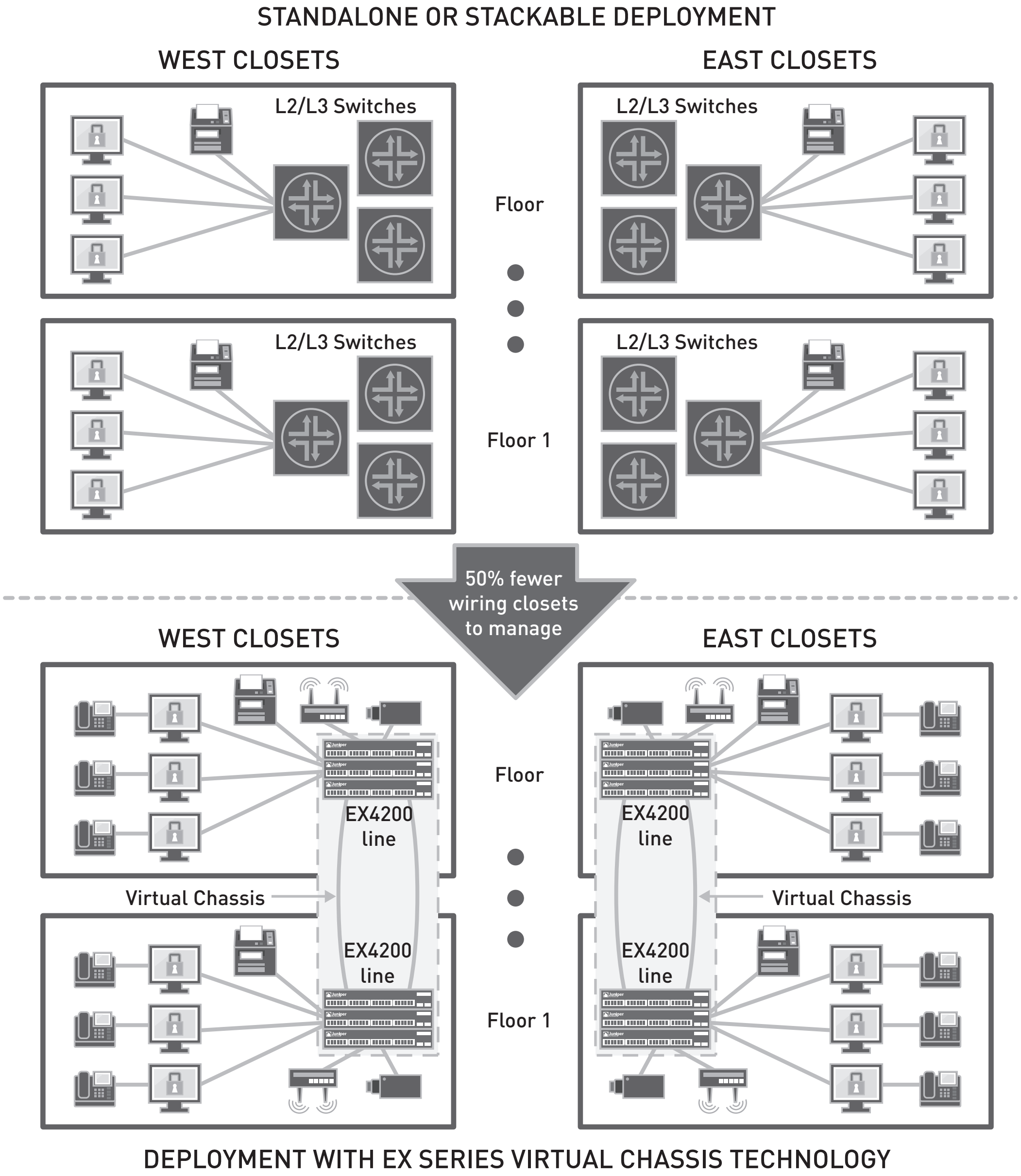


Figure 7: Reducing CapEx and OpEx with Virtual Chassis technology

5. Reducing CapEx and OpEx

   At one-sixth the footprint and less than one-third the cost of the most commonly purchased chassis-based switch offering 48 fiber Gigabit Ethernet ports and four 10-Gigabit Ethernet wire-speed ports, the EX4200 with Virtual Chassis technology represents the new generation of switching.

   Juniper Networks EX4200 Ethernet Switch comes standard with features that are costly add-ons in competitive solutions. For example, the EX4200 includes L3 in the base platform, offers built-in 10-Gigabit Ethernet uplink capability, delivers partial or full PoE, provides built-in redundant power supplies and more in a single cost-optimized platform. OpEx savings include the unified JUNOS feature set and remote mirroring capability for full troubleshooting from a central network operations center (NOC), eliminating the need to send IT staff onsite for maintenance, upgrades, and debugging.

   Not only does Juniper Networks lower CapEx and OpEx by collapsing layers and therefore reducing the number of devices in the network, but Virtual Chassis technology saves on valuable rack space, as well as recurring power and cooling costs. Virtual Chassis technology also frees up precious IT budget dollars that can be invested in new technologies that improve business productivity.

Note: For a full set of features, benefits, and specifications, please view the Juniper Networks EX4200 Ethernet Switches data sheet.

Wireless Solutions

Secure WLAN solutions from Juniper Networks partners Aruba Networks, Trapeze Networks, and Meru Networks are recommended for campuses that wish to provide wireless service. Each solution integrates seamlessly with Juniper Networks Odyssey Access Client (OAC), an enterprise-class 802.1X software access client. Working with an 802.1X-compatible RADIUS server such as Juniper Networks Odyssey Access Client server or Juniper Networks SBR Series Steel-Belted Radius Servers, OAC secures the authentication and connection of WLAN users, ensuring that only authorized users can connect, that login credentials will not be compromised, and that data privacy will be maintained over the wireless link. A specialized version of OAC includes a cryptographic module that has been FIPS 140-2 Level 1 Validated to meet security requirements of government agencies. OAC is also an ideal client for enterprises that are deploying identity-based (wired 802.1X) networking—saving time and effort by permitting one time deployment of wireless and wired 802.1X access while also simplifying the user experience and reducing training costs.

Aggregation Layer

The aggregation layer, sometimes referred to as the distribution layer, aggregates connections and traffic flows from multiple access layer switches to provide high-density connectivity to the LAN core.

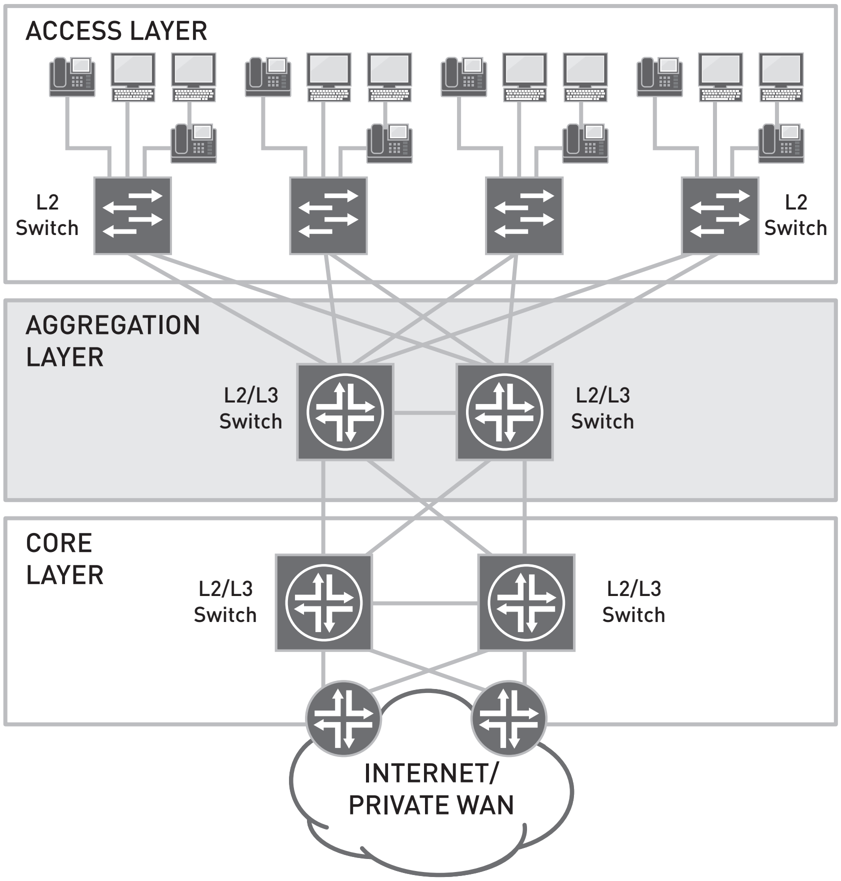


Figure 8: Aggregation layer in a highly available campus LAN

Due to their location in the network, aggregation layer switches must provide scalability, high density, wire-rate ports, and high availability hardware and software features that deliver carrier-class reliability and robustness. Multiple Gigabit Ethernet downlinks from the access wiring closet are needed for redundancy. In addition, multiple 10-Gigabit Ethernet uplinks to the core are required.

Multiple aggregation layer switches delivering wire-rate performance for deterministic operation are used for redundancy. They should run Layer 3 for route summarization, fast convergence, load sharing, and redundant paths.

Aggregation Layer Design Considerations

Segmentation/Virtualization

Aggregation switches should also support generic routing encapsulation (GRE) tunneling for sending mirrored traffic from remote locations to monitoring devices in the NOC for centralized troubleshooting and analysis, or to build segregated overlay networks without the challenges associated with STP.

Distributed Switching

New, emerging technologies are causing a shift in how networks are designed. Administrators are always looking for ways to eliminate STP without the need to push Layer 3 to the access layer. One concept that is garnering a fair amount of attention is distributed switching in the core/aggregation layer. Redundant devices are being transformed into single, logical devices (see Figure 9).

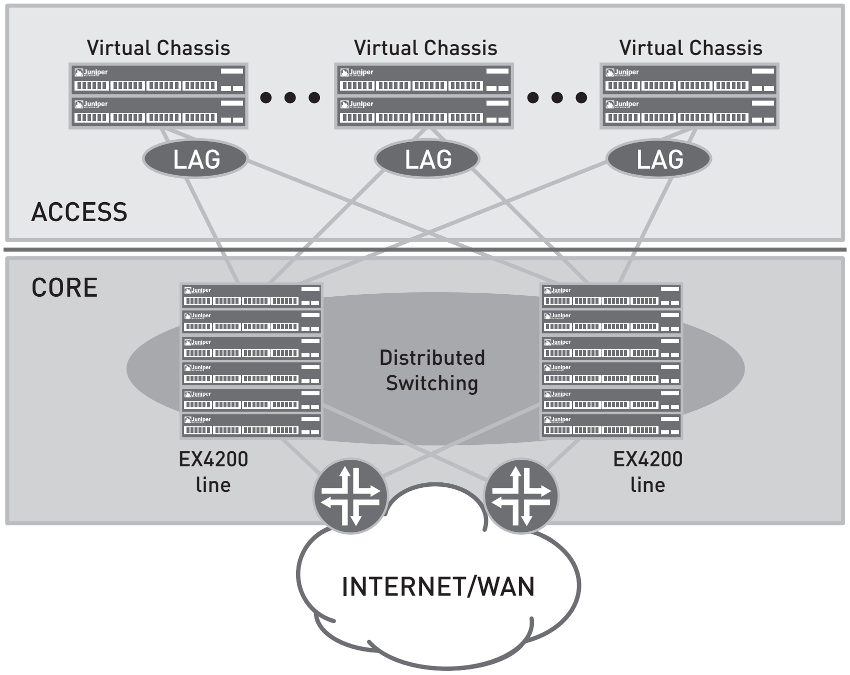


Figure 9: Distributed switching at the core/aggregation layer

By distributing switching at the aggregation or core layers, the following benefits can be realized:

- No STP (configure link aggregation groups to eliminate STP without L3 to the access)
- Layer 2, active/active topology
- Single management

The following should be taken into consideration when deploying distributed switching at the core/aggregation layers:

- Lack of spatial redundancy
- Software management—what is the upgrade process?
- High availability within the chassis—if the Routing Engine fails, do you lose half of your virtual switch?
- Switch capacity when part of the system fails—if half of the virtual system fails, can the other half manage twice the load capacity?
- Split brain—what happens when the system is split into two?

Aggregation Layer Solutions

Scalable Aggregation Layer Solutions

Due to the performance requirements of a highly available campus, HA features and scalability are increased with a LAN design that includes an aggregation layer. The EX4200 or the Juniper Networks EX8200 line of Ethernet Switches can provide the performance and services needed at the aggregation layer.

1. High availability

   In terms of hardware component redundancy, both the EX4200 and the EX8200 line provide redundant Routing Engines, switch fabric, and redundant power and fans that are essential to a network aggregation device. In addition, both platforms run highly modular and resilient JUNOS Software, providing software HA features such as GRES as well as routing protocol graceful restart and Bidirectional Forwarding Detection protocol (BFD). This preserves forwarding operation and minimizes downtime in the event of a device or link failure. The EX Series platforms are also capable of supporting JUNOS nonstop routing and bridging as well as unified in-service software upgrade (ISSU), as the software roadmap allows.

2. Scalable performance

   To meet the aggregation demands of even the largest campus, the EX8200 line of modular switches delivers a powerful, high-density, high-performance 10-Gigabit Ethernet and Gigabit Ethernet solution. Capable of up to 3.2 Tbps throughput, the EX8200 line of Ethernet switches offers up to 64 (eight-slot chassis) or 128 (16-slot chassis) wire-speed 10-Gigabit Ethernet ports.

   The EX4200-24F 24-port SFP+ 2-port 10-Gigabit Ethernet SKU is ideal for low-to-medium density Gigabit Ethernet aggregation needs. Its advanced Virtual Chassis technology enables seamless scaling by allowing up to 10 EX4200 switches to be interconnected via a 128 Gbps backplane or via optional Gigabit Ethernet or 10-Gigabit Ethernet uplink modules. Virtual Chassis technology simplifies administration as these devices can be managed as one unit. In addition, multiple 10-Gigabit Ethernet uplinks from any of the switches that are members of the same Virtual Chassis configuration (up to 10 EX 4200 switches), regardless of physical location, can be link-aggregated for higher bandwidth connections to other aggregation or core switches.

3. CapEx and OpEx savings

   Typically more than two layers of legacy Layer 3 switches are required to achieve the wire-speed port densities demanded by today's high-performance campus. The Juniper Networks EX4200 Ethernet Switch, however, meets these needs and also enables the collapse of the LAN core and aggregation layers, creating a direct positive impact on the economics of networking. Virtual Chassis technology also simplifies network operations and lowers operating expense on all fronts, from JUNOS Software upgrades and moves, adds and changes, to troubleshooting and problem resolution.

   Previously, only expensive chassis-based switches could provide the combination of high 1000BASE-X fiber port densities and the HA features required to satisfy aggregation layer requirements. While certainly scalable and highly available, these modular chassis-based switches are not a very cost-effective solution for such applications. First, they require a considerable up-front investment for the chassis and common equipment, even if not fully populated. Second, because of their size, modular chassis require more space in already crowded racks, taking up valuable real estate. Third, modular chassis require more power and cooling—recurring costs that increase operational expenses and contribute to the production of greenhouse gasses that threaten the environment.

   The EX4200 with Virtual Chassis technology represents the new generation of aggregation switching. It delivers greater value while reducing capital and operating expenses, freeing up valuable IT resources to invest in new technologies to improve business productivity.

Note: For a full set of features, benefits, and specifications, please view the Juniper Networks EX4200 Ethernet Switches data sheet.

Core Layer

The core layer provides a fabric for high-speed packet switching between multiple aggregation devices or the access layer in a collapsed network. It serves as the gateway where all other modules meet, such as the WAN edge.

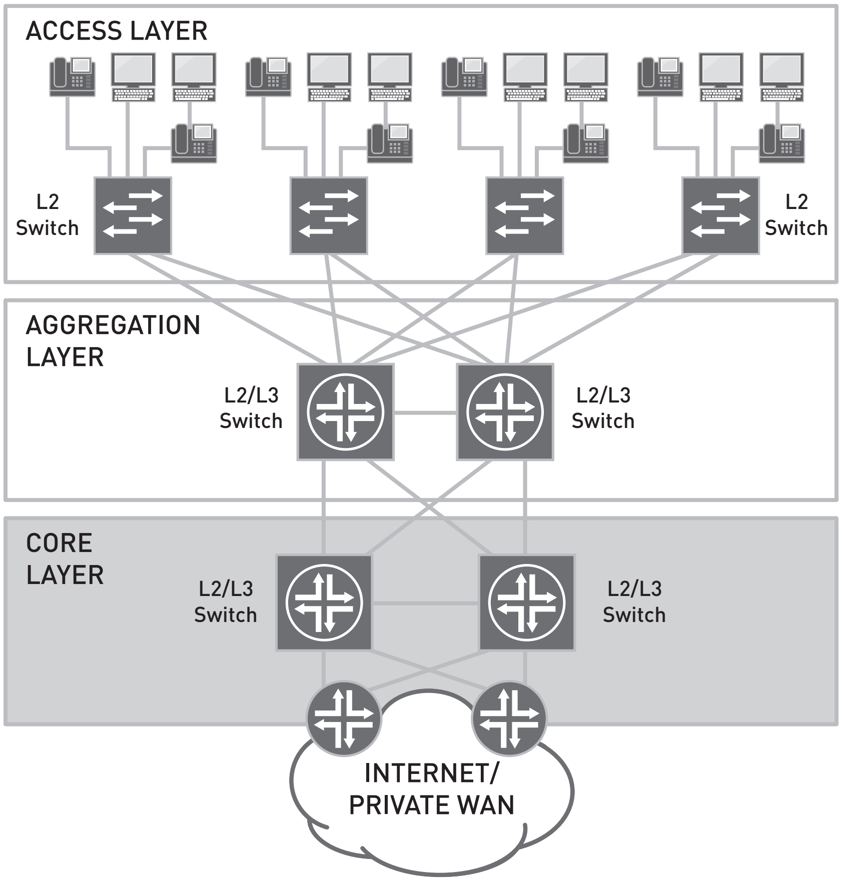


Figure 10: Core layer in a highly available campus LAN

Core Layer Considerations

High-density throughput and HA features are the main core layer considerations. The core typically requires a 10-Gigabit Ethernet interface for high throughput, and wire-rate performance. Core layer switches should also offer redundant control plane, power and cooling components for device redundancy. The design should include multiple core layer switches as system redundancy for network redundancy and optimal convergence.

Core Layer Solutions

High Performance Core Layer Solutions

Due to its HA and high-performance features, the Juniper EX8200 line is recommended as a core layer switch solution.

1. High availability

   The EX8200 line of Ethernet switches offers a fail-safe core layer solution. Redundant links to each core layer device are provided in the event of a device or link failure. Redundant Routing Engines and switch fabrics as well as redundant power supplies and fans are offered. All equipment runs JUNOS, providing software HA features such as QoS and GRES, preserving forwarding and routing operations during device events with nonstop forwarding and automatic load balancing.

2. Scalable performance

   The EX8200 line of modular switches delivers a powerful, high-density, high-performance solution. Capable of up to 3.2 Tbps throughput, the EX8200 line of Ethernet switches offers up to 64 (eight-slot chassis) or 128 (16-slot chassis) wire-speed 10-Gigabit Ethernet ports. The EX8200 line today delivers up to 80 Gbps of switching capacity per slot. By providing capacity now, the EX8200 line allows users to easily migrate to higher speed connections when they are ready—without requiring any changes to the switch fabric, Routing Engines, power supplies, or cooling system. The EX8200 line also offers a redundant control plane and runs Juniper's operating system—JUNOS Software—for maximum software HA.

3. CapEx and OpEx savings

Typically more than two layers of legacy Layer 3 switches are required at the core to achieve the wire-speed port densities demanded by today's high-performance campus. Enabling the collapse of the number of core layers, the high-density, high-performance Juniper Networks EX8200 line of Ethernet switches creates a direct positive impact on the economics of networking. The solution also lowers operating expense and simplifies all network operations via JUNOS Software.

Delivering greater value while reducing capital and operating expenses, the EX8200 line frees up valuable IT resources that may be invested in new technologies to improve business productivity and further streamline operations.

Note: For a full set of features, benefits, and specifications, please view the various Juniper Networks EX Series Ethernet Switch data sheets.

Is the Core Layer Essential?

As it's possible to mesh the aggregation layer in a two-layer network, not all feel the core layer is essential in a campus LAN.

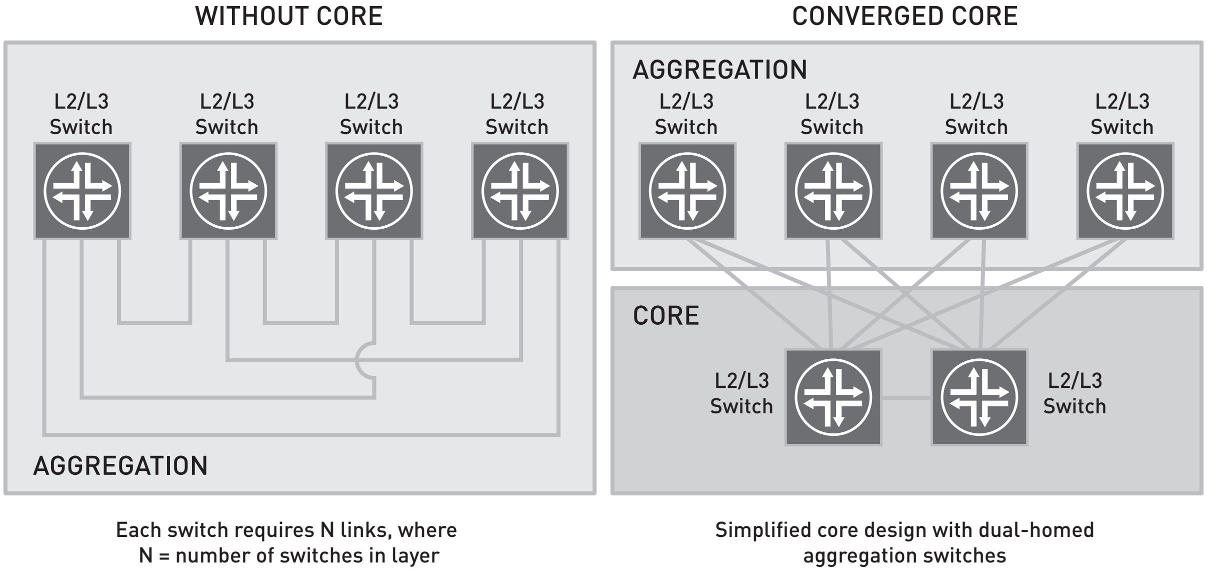


Figure 11: Benefits of the core layer

Challenges and Benefits

Typically, more than two layers of legacy Layer 3 switches are required to achieve the wire-speed port densities demanded by today's high-performance enterprises. While meshing aggregation switches is possible, each aggregation switch requires N-1 meshed links, where N equals the number of aggregation groups. This design is hard to manage and scales poorly, wasting valuable ports in each group when additional aggregation switches are added. Previously, only expensive chassis-based switches could provide the combination of high 1000BASE-X fiber port densities and the HA features required to satisfy aggregation requirements. While certainly scalable and highly available, these modular chassis-based switches are not a very cost-effective solution for such applications. First, they require a considerable up-front investment for the chassis and common equipment, even if not fully populated. Second, because of their size, modular chassis require more space in already crowded server racks, taking up valuable real estate. Third, modular chassis require more power and cooling—recurring costs that increase operational expenses and contribute to the production of greenhouse gasses that threaten the environment.

A dedicated core layer offers dual-homed aggregation to the core, simplifying scaling and providing OSPF ECMP for load-sharing, redundant links.

Consolidating the Core and Aggregation Layers

Most core switches, designed for an earlier time when Gigabit Ethernet was the newest and fastest technology, deliver a limited number of 10-Gigabit Ethernet ports to support high-performance, high-speed uplinks from aggregation switches deployed throughout the campus. While the limited port densities offered on these devices may have been sufficient at some point, constant network expansion means that they have long outgrown their efficacy.

In order to scale efficiently and provide the necessary 10-Gigabit Ethernet port densities in today's LAN core, these legacy switches must be deployed in multiple layers within the core. While ultimately effective, this approach requires an extra layer of core switches. Not only does it add tremendously to capital expenses by consuming a large chunk of the IT budget, it also complicates operations, adding an additional maintenance and management burden, increasing network latency, and creating unwanted oversubscription ratios that reduce overall application performance.

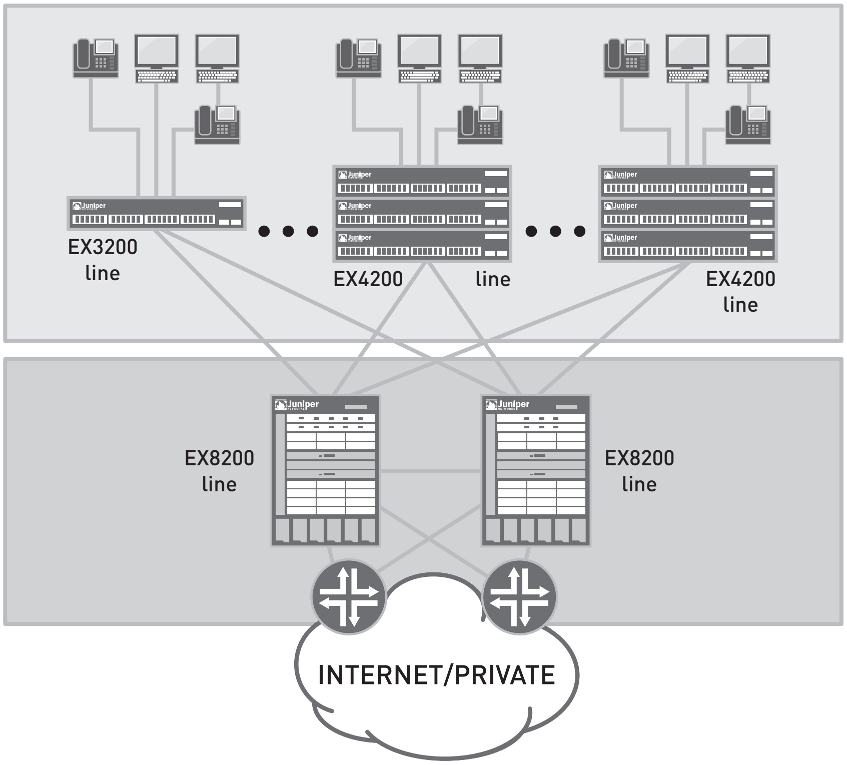


Figure 12: Core layer collapsed into the aggregation layer

Juniper Networks EX8200 line of modular Ethernet switches advance the economics of networking in two ways. First, the EX8200 line delivers the needed 10-Gigabit Ethernet wire-rate port density in the core, eliminating the need to deploy multiple layers of switches that add complexity, cost, oversubscription, and latency. Second, the 10-Gigabit Ethernet port density is sufficient to eliminate the aggregation layer entirely for medium-sized enterprise networks, enabling the access switches to connect directly to the core over wire-speed 10-Gigabit Ethernet links. Eliminating a full layer of aggregation switches dramatically reduces CapEx and simplifies network operations—everything from OS upgrades and moves, adds and changes, to troubleshooting and problem resolution.

For large enterprise networks that require an aggregation layer, Juniper Networks extends those CapEx reductions to the aggregation layer. Aggregation switches, which consolidate distributed wiring closets on a single platform and connect them to core switches, require high-density fiber interfaces to support potentially long runs between floors or even buildings. Due to their critical role of providing connectivity between distributed users and centralized servers in the corporate network, aggregation switches also require HA features to ensure continuous delivery of applications and business processes.

High Availability in the Campus Network

As stressed throughout this document, the campus network should operate with the same reliability and uptime as the PSTN or telecom network, or as close as possible. Downtime is not an option to remain competitive in any industry in today's marketplace. HA may be implemented at many levels—from network protocols, to device-level HA links, to network software.

Device-Level High Availability

Most device failures are due to power supply failures or mechanical cooling problems. It is important to always support business processes with high-quality, carrier-class network devices such as the EX Series Ethernet Switches and Juniper Networks MX Series Ethernet Services Routers. Purchasing equipment with dual power supplies and redundant fans or blowers to minimize equipment failure is always recommended, and raises the mean time to repair (MTTR). Additional device-level HA can be provided by doubling up on key devices to ensure that there is a backup device in the event of a failed device. If neither budget nor configuration supports a full set of backup devices, purchasing extra key device components, such as a backup set of field-serviceable or hot-swappable power supplies or fans, helps mitigate the impact of a device failure.

Link-Level High Availability

Ensuring that business processes maintain vital data flow through internal and external resources is provided through link-level HA. At the campus, link-level HA requires that two links operate in an active/backup configuration so that if one link fails, the other can take over or reinstate the forwarding of traffic that had been previously forwarded over the failed link.

Redundant Links: Square versus Triangle

A square or triangle link configuration can be used to provide redundant paths between devices.

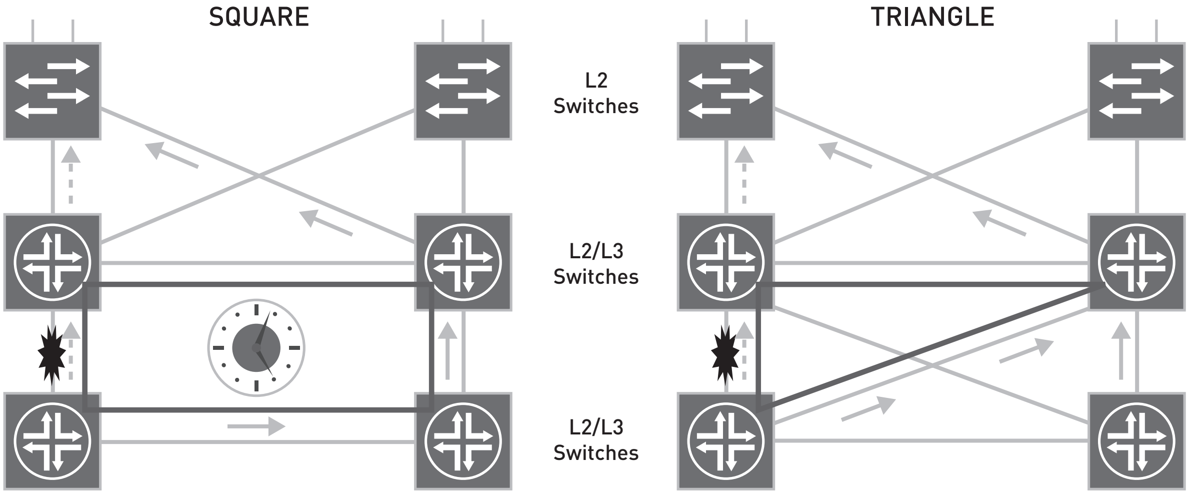


Figure 13: Homing: square versus triangle

1. Peering square configuration

   In this design, a Layer 3 peering square is configured between the aggregation and core layers. Route peering provides a redundant path. Link failure requires Layer 3 protocol convergence, which may vary since the route is non-deterministic. The result of this deployment is dropped sessions and/or lost packets, delivering suboptimal performance.

2. Dual-homed triangle configuration

   In this design, a Layer 3 dual-homed triangle is configured between the aggregation and core layers. ECMP provides a redundant, load sharing path. Any link failure results in a fast failover time since the route is deterministic. The result is optimal performance with minimal packet loss.

Virtual Chassis Technology

Up to 10 Juniper EX4200 switches can be configured as one logical switch using Virtual Chassis technology. Each Virtual Chassis enables fail-safe operations, as each unit is capable of passing data from one to another in the event of a failure. Redundant links to each WAN edge device are also provided in the event of a device or link failure. In addition to the device HA features standard in the EX4200 switches, all equipment runs JUNOS Software, providing software HA features such as QoS and GRES, preserving forwarding and routing operations during device events with nonstop forwarding and automatic load balancing.

Link Aggregation Groups

For high performance link and port level redundancy, a link aggregation group (LAG) is recommended between device layers.

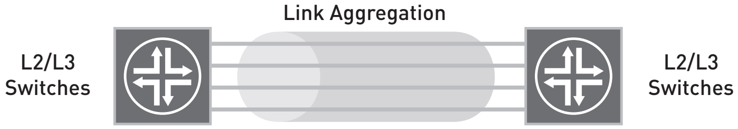


Figure 14: Link aggregation group (LAG)

A LAG requires multiple physical interfaces to be configured as a single logical trunk group. This increases bandwidth between devices. Traffic is distributed across active group ports and links, providing built-in load balancing as well as link and port level redundancy. Link or port failure results in fast failover times with LAG.

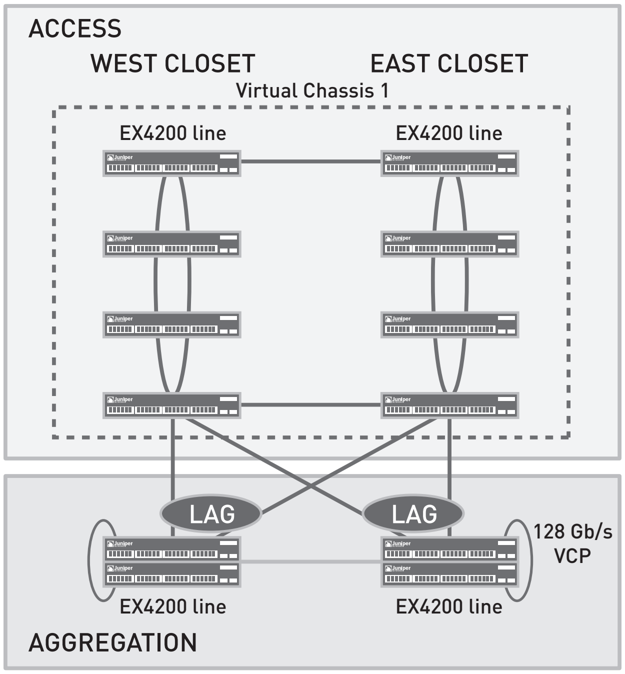


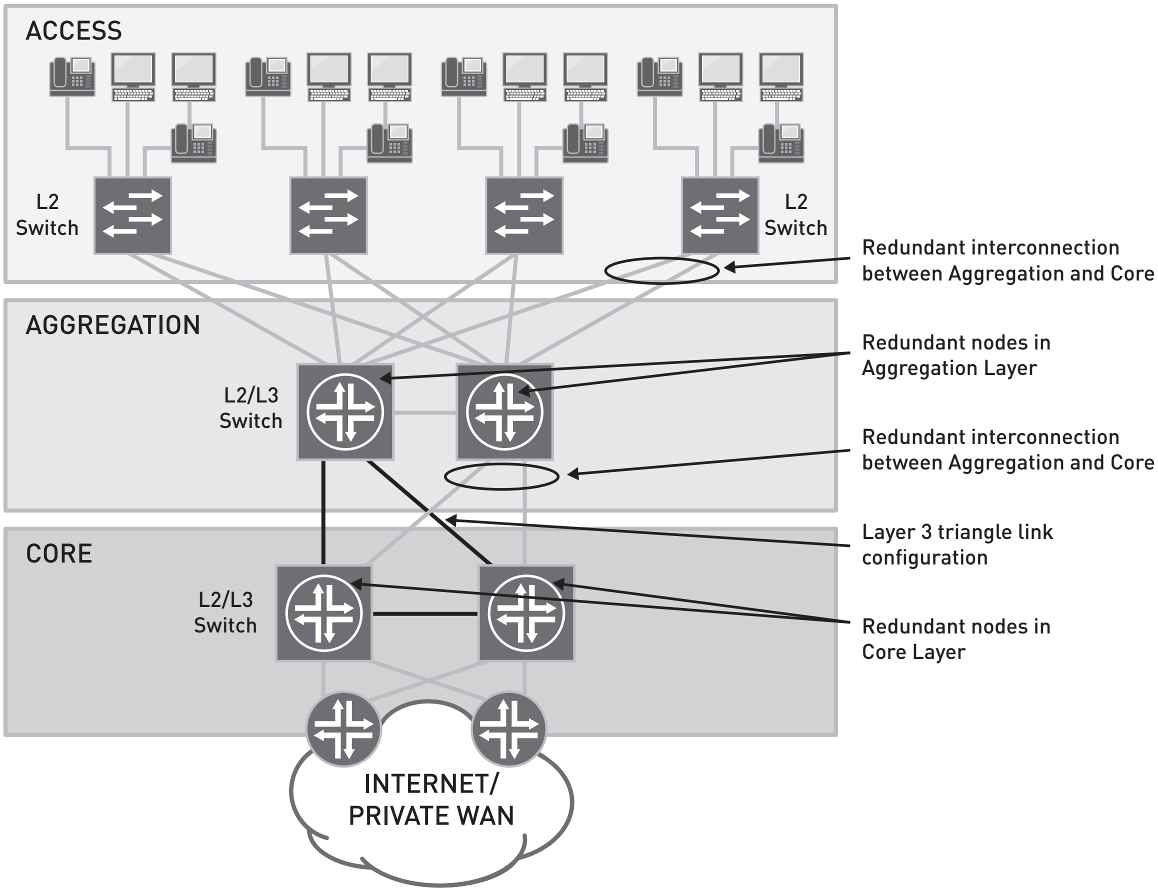
Figure 15: Virtual Chassis and LAG

EX4200 switches with Virtual Chassis technology can be configured into multiple Virtual Chassis groups within a single wiring closet or across multiple wiring closets. The uplinks from the closest Virtual Chassis groups extend across multiple EX4200 units in the aggregation layer. In this simplified design, STP is not required, yet redundancy is increased when uplinks are distributed across multiple EX4200 switches within a single Virtual Chassis group. This leads to cost and operational savings and increased HA as all uplinks are redundant and offer load sharing.

Redundant Trunk Group

Redundant Trunk Group (RTG) is an HA link feature of the Juniper Networks EX Series Ethernet Switches that eliminates the need for STP. Ideally implemented on a switch with a dual-home connection, RTG configures one link as active and forwarding traffic, and the other as blocking and backup to the active link. RTG provides extremely fast convergence in the event of a link failure. It is similar in practice to RSTP Root and Alternate port, but without the need of configuring RSTP.

Best Practices for Campus Link Redundancy


ACCESS
L2 Switch
L2 Switch
AGGREGATION
L2/L3 Switch
CORE
L2/L3 Switch
INTERNET/ PRIVATE WAN
Redundant interconnection between Aggregation and Core
Redundant nodes in Aggregation Layer
Redundant interconnection between Aggregation and Core
Layer 3 triangle link configuration
Redundant nodes in Core Layer

Putting that all together, Juniper recommends the following link configuration.

Figure 16: Best practices link redundancy

The access layer switches should be "dual-homed" to redundant nodes in the aggregation layer. The aggregation and core layers are both built with dual-homed interconnects. Each alternate path uses Layer 3 for optimal convergence. The core layer switches are also dual-homed to WAN edge routers. At all layers, link bandwidth and node capacity are designed to withstand link or node failure.

Network Software HA

JUNOS Software is the consistent operating system that powers all of Juniper's switch, router, and firewall solutions, providing carrier-class network software to the campus. JUNOS supports features like nonstop forwarding (NSF), graceful restart, unified in-service software upgrade (ISSU), Bidirectional Forwarding Detection protocol (BFD), and other features that together make IP networking as failure-safe and reliable as telephony networks. JUNOS Software's modularity and uniform implementation of all features enables even the smallest campus to benefit from the same hardened services in their JUNOS devices as the largest service providers.

Security

The increased mobility of users on campus, the growing use of contractors, the co-location of partners onsite, the proliferation of unified communications, and the demand for wireless access all intensify campus LAN security issues. IT must protect valuable campus resources from internal and external threats across large or multiple LANs as it delivers high-performance, secure, and ubiquitous LAN and WLAN access.

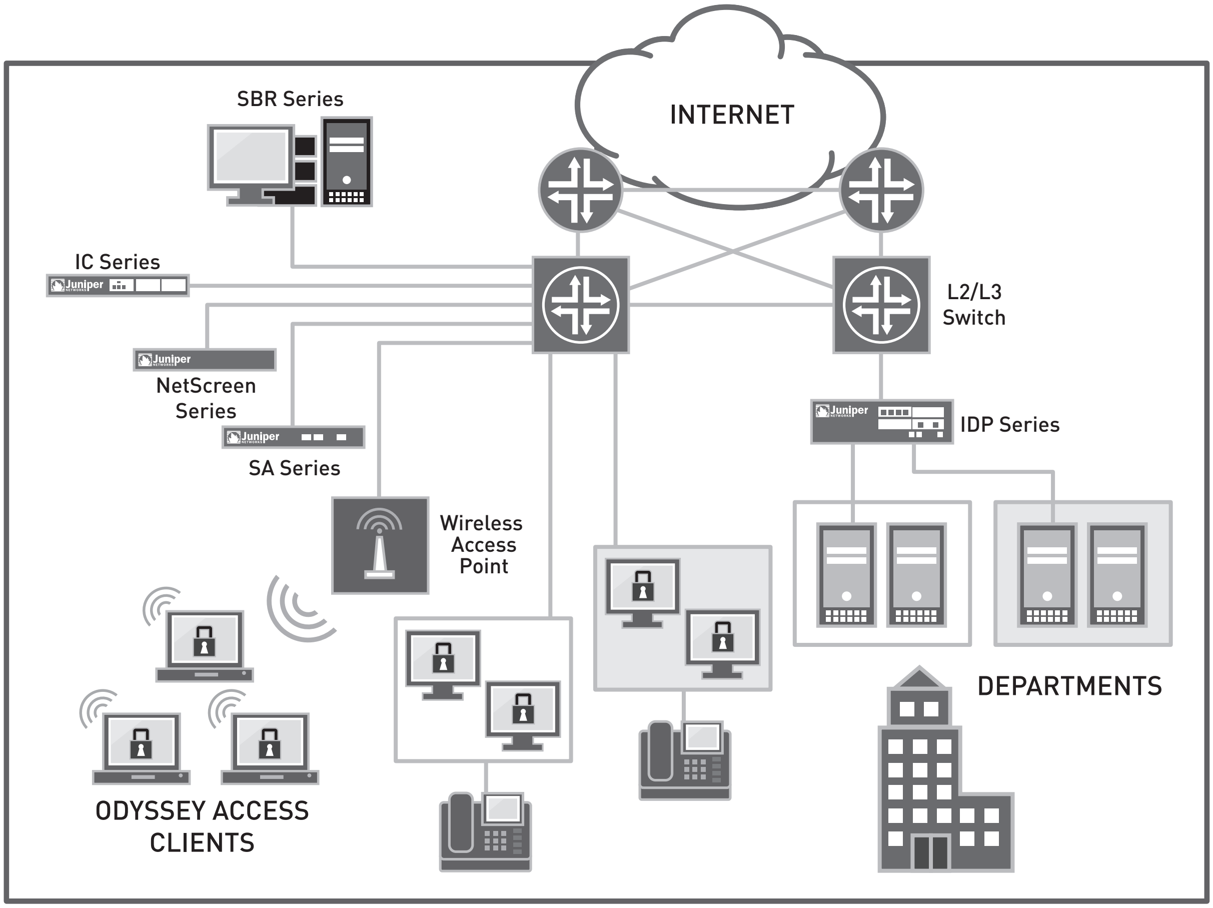


Figure 17: Campus security architecture

Increasing security threats and risks force campus LANs to remain secure and controlled on all fronts, yet also provide open and pervasive access to maintain and increase productivity. The most effective security architecture to ensure maximum protection from network and application layer threats is based on multilayered protection that's appropriate for each location of the network. Holistic solutions that offer comprehensive security features, proven reliability, and exceptional performance are needed. 802.1X and unified access control (UAC) should be used to effectively handle unmanaged devices and guest users attempting network access, as well as to support unmanageable devices, post admission control, and application access control, visibility and monitoring. Firewalls and intrusion detection and prevention (IDP) solutions are also needed to help ensure security across the LAN. In addition, QoS can be used as a security tool to identify, classify, and queue traffic. For example, QoS policies can protect access to departmental resources or ensure that high priority data flows are unaffected by malicious traffic.

Unified Access Control

A UAC solution, instrumental to LAN security, must provide:

- Network protection—ensuring that users are authenticated as they log in, only allowing authorized users access.
- Coordinated threat control—if an authorized user logs in and has a virus or worm or tries to hack the system, the Juniper Networks IC Series Unified Access Control Appliances and other security devices should work with the UAC to identify where the problematic data is coming from and shut off the port or contain the threat.

- Guest access—clearly defining who can access the LAN, what resources are available to them, and the time frame for such access.
- Identity-based QoS—giving classes of employees access to specific resources and also defining levels of service to specific applications. For example, those accessing email get best-effort QoS while financial services or other mission-critical functions get gold QoS.

Juniper Networks Unified Access Control combines identity-based policy and endpoint intelligence to give enterprises real-time visibility and policy control throughout the network. The UAC solution can make use of some or all of the following components: Juniper Networks IC Series Unified Access Control Appliances, which serve as a centralized policy manager; a UAC Agent, which is dynamically downloadable or agentless endpoint software; and several different forms of enforcement points that include both firewalls and vendor-agnostic 802.1X-compliant switches and/or WLAN access points. UAC provides a cost-effective solution to the problem of unmanaged or ill-managed endpoint security throughout the LAN. In essence, UAC enables the creation of a powerful network perimeter defense via robust admission controls that ensure endpoints comply with required OS updates, security patches, personal firewall requirements, virus signatures, before being allowed access to the LAN. UAC enables access control for guests, contractors, partners, and employees.

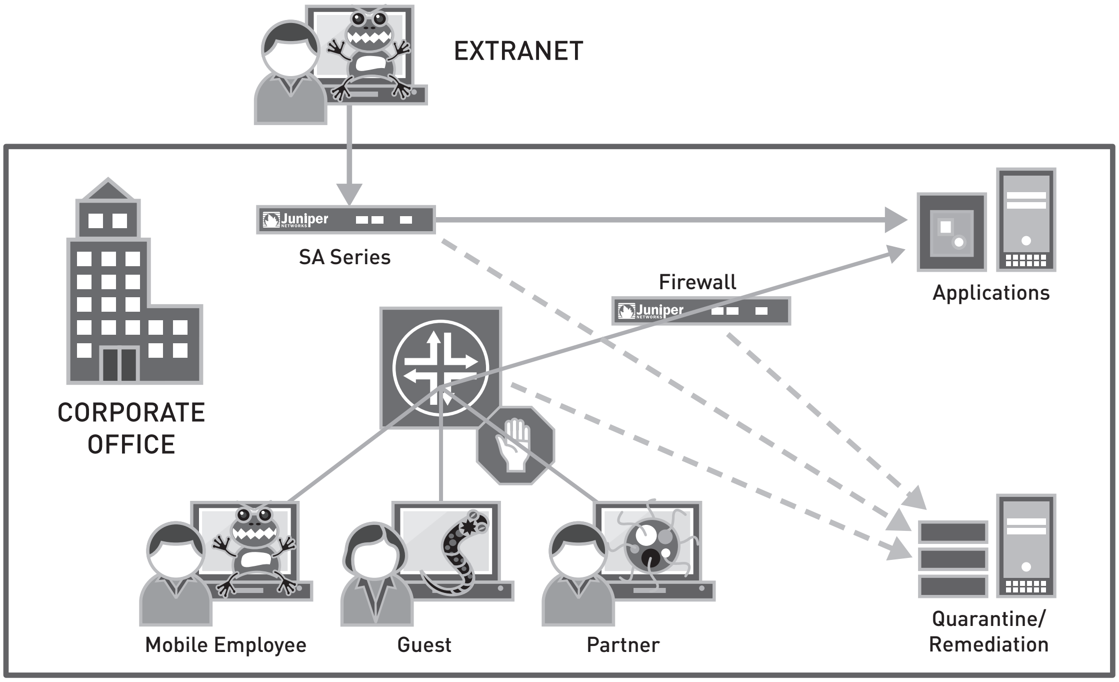


Figure 18: Enforcing endpoint health policy for all user types

IEEE 802.1X

The 802.1X standard provides a strong framework for authentication, access control, and data privacy for port-based network access control. An 802.1X access control solution completes the authentication of network credentials even before a network IP address is assigned, thus preventing unauthorized access and ensuring that viruses and other threats are halted before they can spread into an organization. After login, dynamic port-based role configuration is used to restrict use of specific resources.

Ubiquitous Access

Today's 24/7 global environment requires that employees, customers, partners, and other network users have real-time access to network resources and applications from anywhere and from virtually any device. On the campus, this includes wired and wireless access for PCs, laptops, PDAs, Internet-enabled smartphones, and other IP devices. When on the road at a remote location such as a partner site, hotel room, Internet café, or anywhere with Internet access, users must also be able to connect to LAN resources via a VPN or other secure connection.

Segmentation

Unbound by physical interfaces, segmentation logically divides networks into separate zones based on user definition.

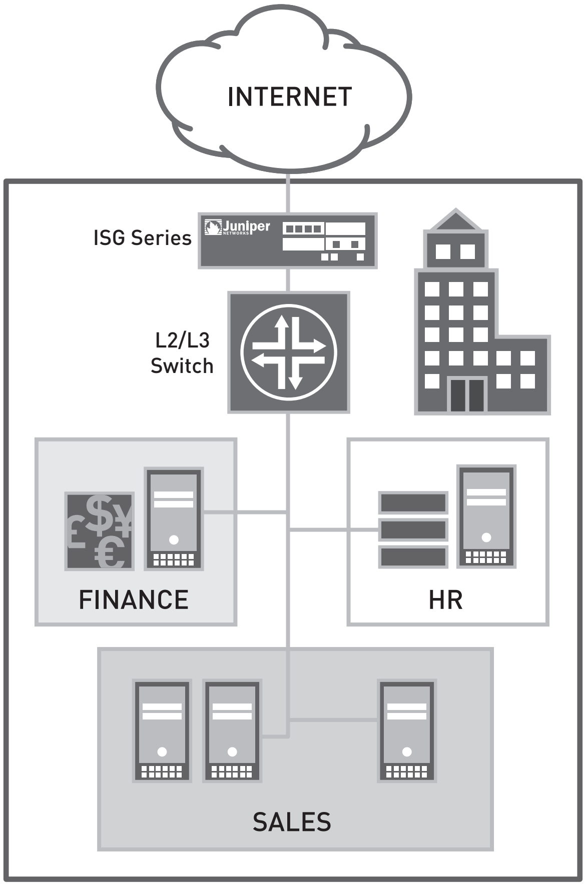


Figure 19: Enforcing security policies between different departments, resources and services

Supporting distributed security requirements without the added cost, segmentation simplifies policy configuration and management. Segmentation is ideal for grouping users so that they can access specific resources. For example, all those in the HR department can be given access to the HR database and other personnel resources. Segmentation is provided through VLANs and with other virtualization technologies.

Access Control Lists

Compliance requirements are driving enterprises to demonstrate control for access to mission-sensitive data. Enterprises need to prove that only authorized users have access to sensitive company data. They also need to monitor, audit, and log user access to valuable corporate resources. Mainly a wireless issue at most campuses, guests need restricted access on the network. Enterprises can apply risk mitigation by ensuring that users can't even reach applications unless policy gives permission. For example, enterprises can dynamically enforce access to guests or open specific services to guests upon login using access control lists (ACLs). The use of an ACL is also sometimes referred to as filtering because it regulates traffic by allowing or denying network access. ACLs prevent traffic from entering or exiting the network. Firewall filter parameters can be configured locally or sent vendor-specific attributes by the RADIUS server.

Additional Access Security

Several other port security and threat detection measures should be used to defend against internal and external spoofing, man-in-the-middle, and DoS attacks. These include MAC limiting, Dynamic Host Configuration Protocol (DHCP) snooping, Dynamic Address Resolution Protocol (ARP) Inspection, and IP source guard.

1. MAC limiting

   Network adapters, including those built-in or otherwise, have an attached media access control (MAC) address. This Layer 2 identifier uniquely marks the computer on the network. However, since MAC addresses are not divided into host and network portions like IP addresses, a host can't determine from the MAC address of another host if the two share the same Layer 2 network segment. This means that it's possible to change a MAC address, often referred to as MAC spoofing, and access restricted resources from a trusted host. MAC limiting is configurable on some switches to prevent MAC flooding and spoofing attacks.

2. DHCP snooping

   Another Layer 2 switch port security feature, DHCP snooping helps protect domain integrity. Working in conjunction with a DHCP server, DHCP snooping allows only clients with specific IP/MAC addresses access to the network when the DHCP server is allocating IP addresses to LAN clients. With DHCP snooping, only a "whitelist" of IP addresses may access the network. The whitelist is configured at the switch port level, and the DHCP server manages access control. Only specific IP addresses with specific MAC addresses on specific ports may access the IP network. Additionally, DHCP requests on all untrusted access ports require inspection and verification. This stops attackers from adding their own DHCP servers on the network and prevents DHCP DoS and rogue DHCP server attacks.

   DHCP snooping security filters maintain a DHCP snooping binding table of untrusted DHCP messages by preventing DHCP DoS and rogue DHCP server attacks.

3. Dynamic ARP Inspection (DAI)

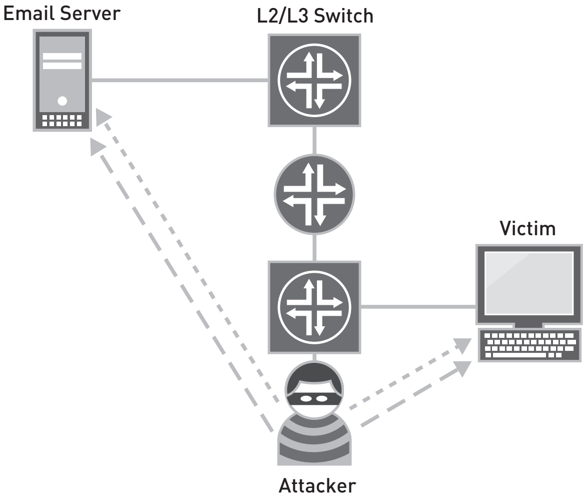


Figure 20: Dynamic ARP Inspection (DAI)

   ARP spoofing starts when an attacker sends spoofed ARP messages to an Ethernet LAN. The ARP spoofing occurs when a network node IP address, such as a server or gateway, is stolen and then applied to an attacker's computer. Network traffic is then sent to the computer of the attacker, who then can modify the data before sending it elsewhere in a man-in-the-middle attack. Alternately, the attacker could launch a DoS attack by associating a nonexistent MAC address to the IP address of the gateway. Or the attacker could simply forward the traffic to the actual node after passively sniffing the packets.

   Dynamic ARP Inspection (DAI) is a feature that intercepts ARP packets on untrusted ports and validates them against a DHCP snooping database. Nonmatching entries are dropped. This avoids forwarding of traffic to an address impersonating the valid device, preventing man-in-the-middle spoofing attacks and DoS.

4. IP source guard

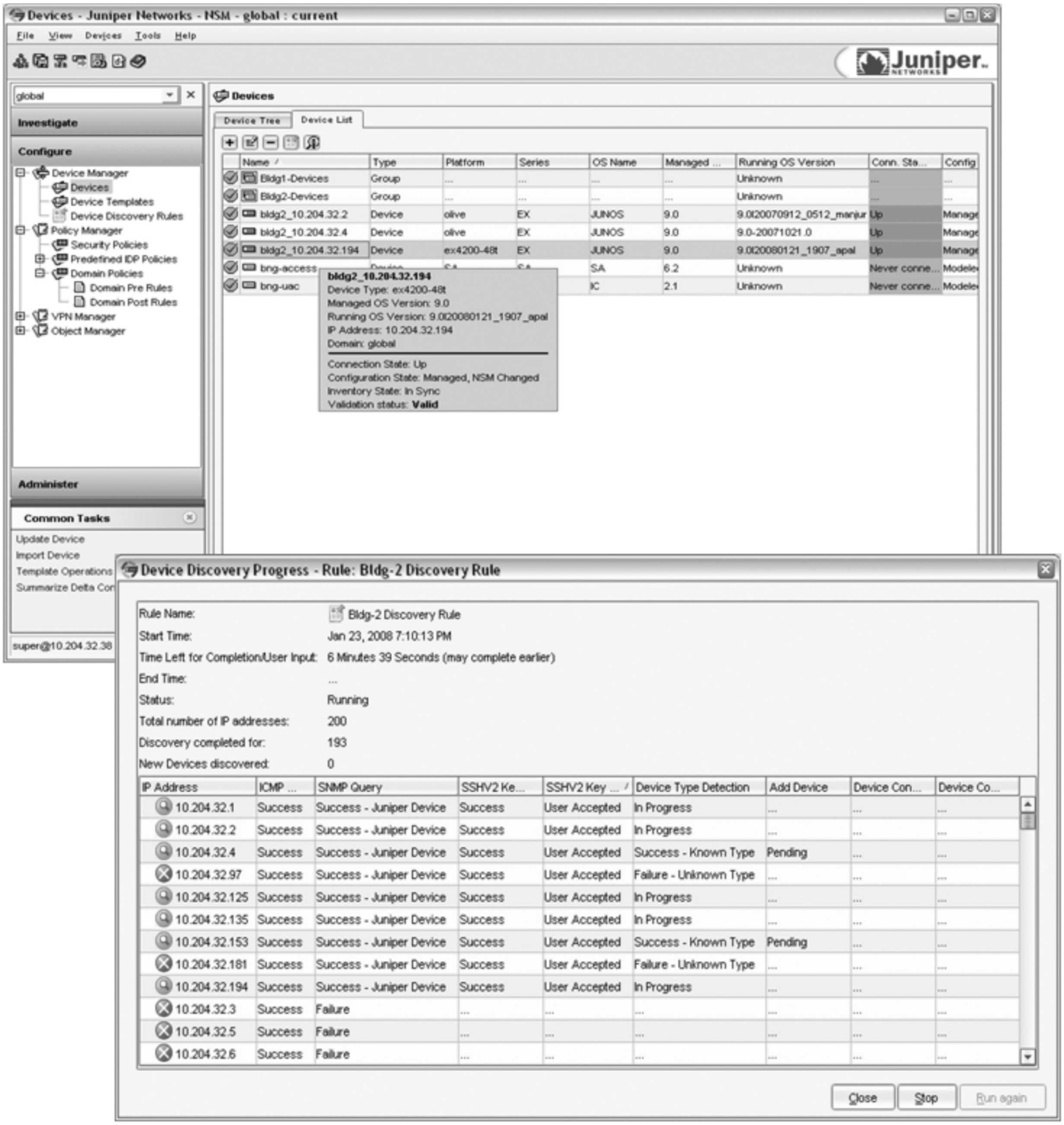
   Another port security feature that restricts IP traffic on untrusted Layer 2 access and trunk ports is IP source guard. Working in conjunction with DHCP snooping, IP source guard filters traffic based on manually configured IP source bindings or what is automatically learned by the DCHP snooping database. This prevents IP spoofing attacks. Any IP traffic coming into the watched ports with an IP address other than those automatically or statically assigned will be dropped.

Operational Simplicity and Unified Management

Unified Management with Juniper Networks Network and Security Manager (NSM)

Juniper Networks Network and Security Manager is a powerful, centralized management solution that controls the entire life cycle of routers, switches, firewall/IPsec VPN, and IDP Series devices, including centralized device, configuration and policy management, standard-based network topology discovery and tracking, hardware and software inventory management, as well as various monitoring and troubleshooting capabilities.

NSM's automated process not only allows new network devices to be automatically or manually added or removed, it also allows continuous device sync-up for status, configuration, and inventory with streamlined and scheduled device updates.



	Name	Type	Platform	Series	OS Name	Managed ...	Running OS Version	Conn. Sta...	Config
✓	Bldg1-Devices	Group	...	...	...	...	Unknown	...	...
✓	Bldg2-Devices	Group	...	...	...	...	Unknown	...	...
✓	bldg2_10.204.32.2	Device	olive	EX	JUNOS	9.0	9.0I20070912_0512_manjur	Up	Manage
✓	bldg2_10.204.32.4	Device	olive	EX	JUNOS	9.0	9.0-20071021.0	Up	Manage
✓	bldg2_10.204.32.194	Device	ex4200-48t	EX	JUNOS	9.0	9.0I20080121_1907_apal	Up	Manage
✓	bng-access	Device	SA	SA	SA	6.2	Unknown	Never conne...	Modele
✓	bng-uac				IC	2.1	Unknown	Never conne...	Modele

bldg2_10.204.32.194
Device Type: ex4200-48t
Managed OS Version: 9.0
Running OS Version: 9.0I20080121_1907_apal
IP Address: 10.204.32.194
Domain: global

Connection State: Up
Configuration State: Managed, NSM Changed
Inventory State: In Sync
Validation status: **Valid**

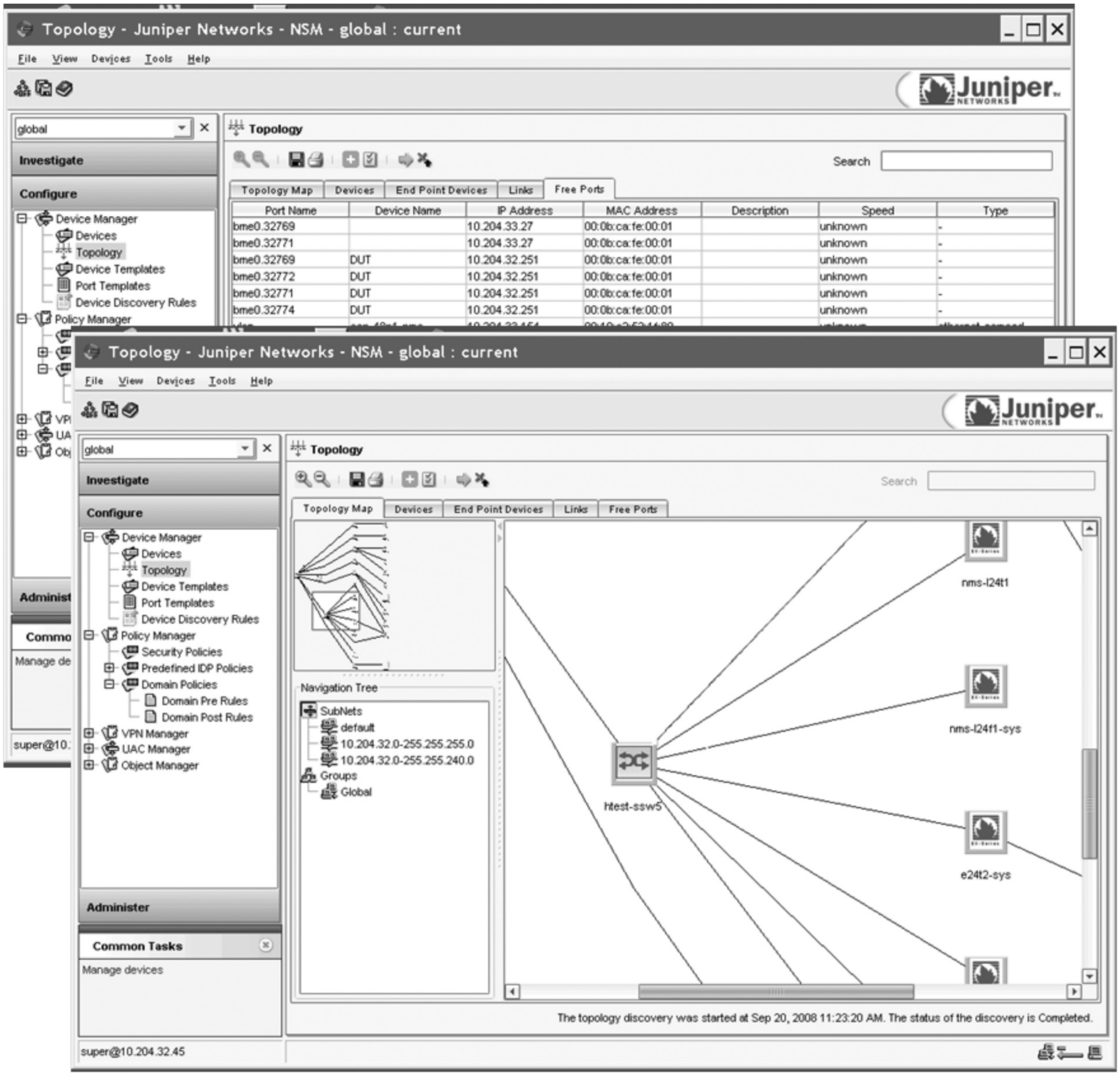
Device Discovery Progress - Rule: Bldg-2 Discovery Rule

Rule Name:	Bldg-2 Discovery Rule
Start Time:	Jan 23, 2008 7:10:13 PM
Time Left for Completion/User Input:	6 Minutes 39 Seconds (may complete earlier)
End Time:	...
Status:	Running
Total number of IP addresses:	200
Discovery completed for:	193
New Devices discovered:	0

IP Address	ICMP ...	SNMP Query	SSHV2 Ke...	SSHV2 Key ...	Device Type Detection	Add Device	Device Con...	Device Co...
10.204.32.1	Success	Success - Juniper Device	Success	User Accepted	In Progress	...	...	...
10.204.32.2	Success	Success - Juniper Device	Success	User Accepted	In Progress	...	...	...
10.204.32.4	Success	Success - Juniper Device	Success	User Accepted	Success - Known Type	Pending	...	...
⊗ 10.204.32.97	Success	Success - Juniper Device	Success	User Accepted	Failure - Unknown Type	...	...	...
10.204.32.125	Success	Success - Juniper Device	Success	User Accepted	In Progress	...	...	...
10.204.32.135	Success	Success - Juniper Device	Success	User Accepted	In Progress	...	...	...
10.204.32.153	Success	Success - Juniper Device	Success	User Accepted	Success - Known Type	Pending	...	...
⊗ 10.204.32.181	Success	Success - Juniper Device	Success	User Accepted	Failure - Unknown Type	...	...	...
10.204.32.194	Success	Success - Juniper Device	Success	User Accepted	In Progress	...	...	...
⊗ 10.204.32.3	Success	Failure	...	...	...	...	...	...
⊗ 10.204.32.5	Success	Failure	...	...	...	...	...	...
⊗ 10.204.32.6	Success	Failure	...	...	...	...	...	...

Figure 21: NSM Device Management and Device Auto Discovery

With NSM's topology manager, all Juniper and non-Juniper network devices such as routers, switches and security appliances can be discovered and mapped into a topology map with proper hierarchical segments, endpoints and hosts. This can then be connected to the network devices, included in the discovery and organized into a searchable database for ease of management.

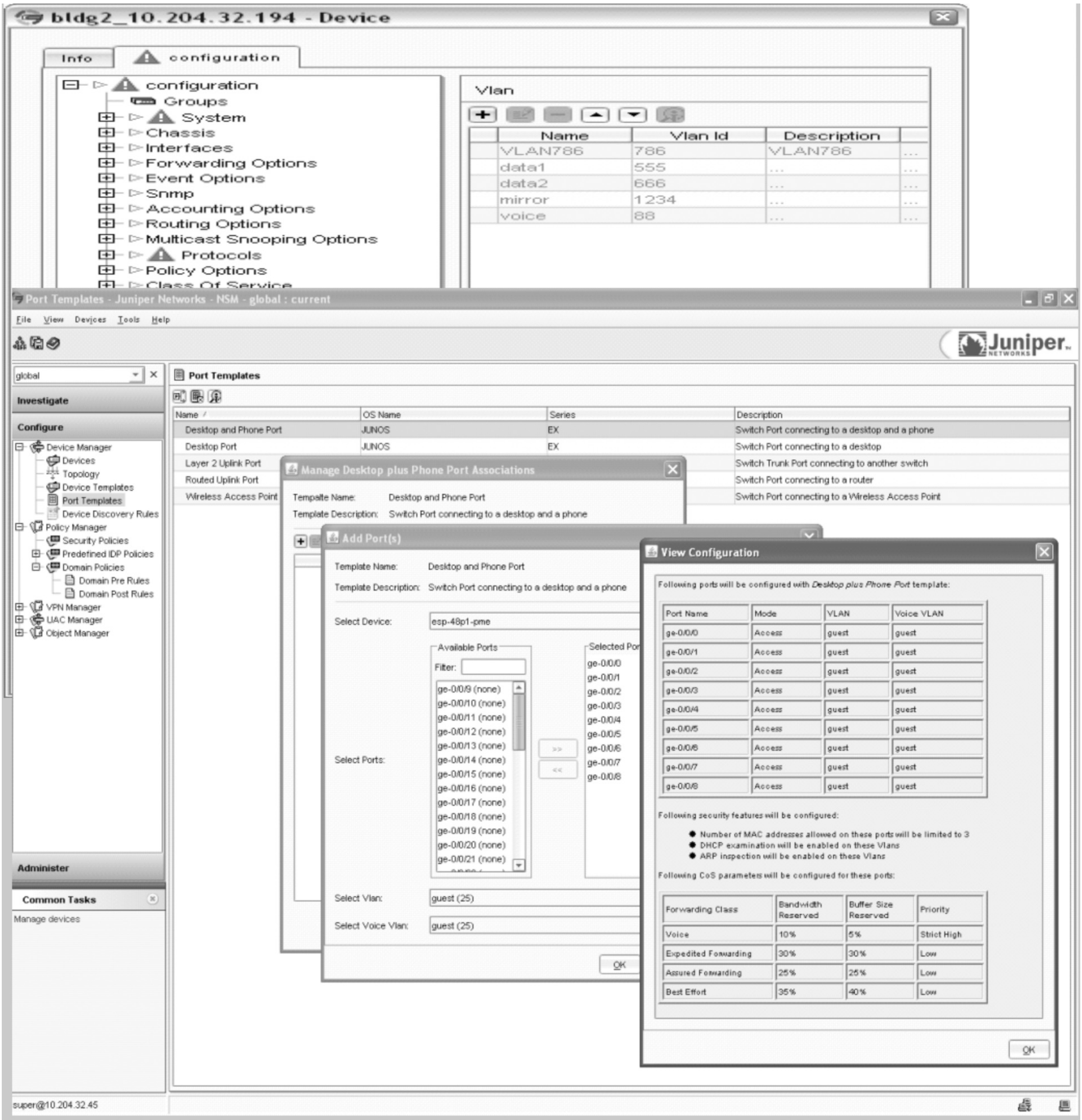


Port Name	Device Name	IP Address	MAC Address	Description	Speed	Type
bme0.32769		10.204.33.27	00:0b:ca:fe:00:01		unknown	-
bme0.32771		10.204.33.27	00:0b:ca:fe:00:01		unknown	-
bme0.32769	DUT	10.204.32.251	00:0b:ca:fe:00:01		unknown	-
bme0.32772	DUT	10.204.32.251	00:0b:ca:fe:00:01		unknown	-
bme0.32771	DUT	10.204.32.251	00:0b:ca:fe:00:01		unknown	-
bme0.32774	DUT	10.204.32.251	00:0b:ca:fe:00:01		unknown	-

The topology discovery was started at Sep 20, 2008 11:23:20 AM. The status of the discovery is Completed.

Figure 22: NSM Topology Discovery

To help reduce the workload and simplify the task in configuring tens to thousands of network devices for network administrators, NSM supports a set of pre-defined as well as customizable device and port configuration templates that can be applied to one or more devices at the same time. The pre-defined configuration templates are designed and built around Juniper's best practice recommendations for each of the relevant deployment scenarios. Whenever template based configuration is not applicable, NSM's "click & select" based configuration user interface covers all device feature details and provides users the alternative to CLI.



Vlan

	Name	Vlan Id	Description	
	VLAN786	786	VLAN786	...
	data1	555	...	...
	data2	666	...	...
	mirror	1234	...	...
	voice	88	...	...

Port Templates

Name	OS Name	Series	Description
Desktop and Phone Port	JUNOS	EX	Switch Port connecting to a desktop and a phone
Desktop Port	JUNOS	EX	Switch Port connecting to a desktop
Layer 2 Uplink Port			Switch Trunk Port connecting to another switch
Routed Uplink Port			Switch Port connecting to a router
Wireless Access Point			Switch Port connecting to a Wireless Access Point

Tempalte Name: Desktop and Phone Port

Template Description: Switch Port connecting to a desktop and a phone

Template Name: Desktop and Phone Port

Template Description: Switch Port connecting to a desktop and a phone

Select Device: esp-48p1-pme

Select Ports:

Available Ports: ge-0/0/9 (none), ge-0/0/10 (none), ge-0/0/11 (none), ge-0/0/12 (none), ge-0/0/13 (none), ge-0/0/14 (none), ge-0/0/15 (none), ge-0/0/16 (none), ge-0/0/17 (none), ge-0/0/18 (none), ge-0/0/19 (none), ge-0/0/20 (none), ge-0/0/21 (none)

Selected Por: ge-0/0/0, ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/4, ge-0/0/5, ge-0/0/6, ge-0/0/7, ge-0/0/8

Select Vlan: guest (25)

Select Voice Vlan: guest (25)

Following ports will be configured with *Desktop plus Phone Port* template:

Port Name	Mode	VLAN	Voice VLAN
ge-0/0/0	Access	guest	guest
ge-0/0/1	Access	guest	guest
ge-0/0/2	Access	guest	guest
ge-0/0/3	Access	guest	guest
ge-0/0/4	Access	guest	guest
ge-0/0/5	Access	guest	guest
ge-0/0/6	Access	guest	guest
ge-0/0/7	Access	guest	guest
ge-0/0/8	Access	guest	guest

Following security features will be configured:

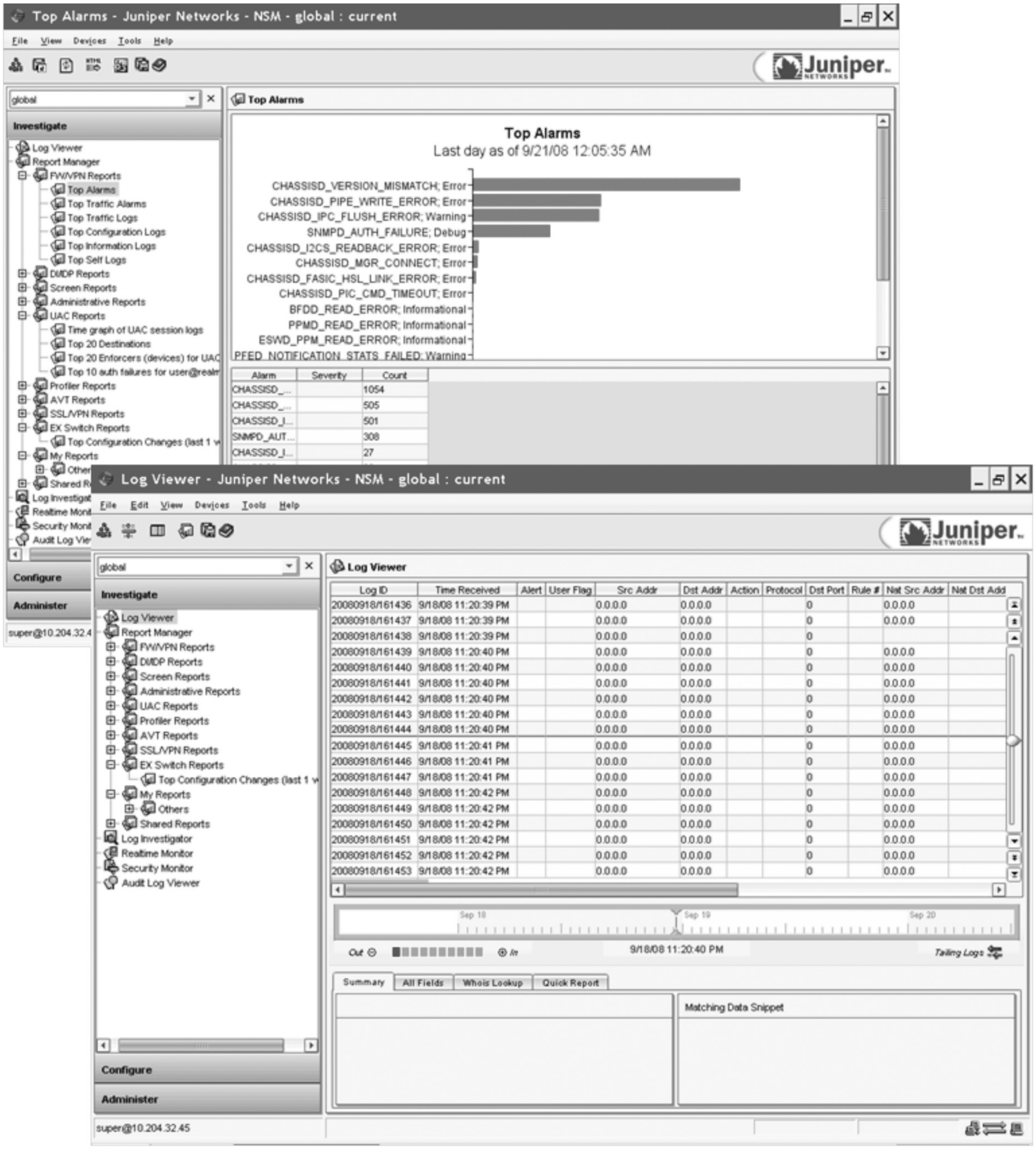
- Number of MAC addresses allowed on these ports will be limited to 3
- DHCP examination will be enabled on these Vlans
- ARP inspection will be enabled on these Vlans

Following CoS parameters will be configured for these ports:

Forwarding Class	Bandwidth Reserved	Buffer Size Reserved	Priority
Voice	10%	5%	Strict High
Expedited Forwarding	30%	30%	Low
Assured Forwarding	25%	25%	Low
Best Effort	35%	40%	Low

Figure 23: NSM Template Based Configuration

A wide range of reporting tools are available in NSM, enabling network administrators to view and analyze network traffic, device statistics and events, system resources, and other administrative information in real-time as well as for historical trends and records. Network administrators can also utilize a set of pre-defined and customizable templates and filters for commonly used reports and generate these reports on a regularly scheduled basis.


Top Alarms - Juniper Networks - NSM - global : current
File View Devices Tools Help
Juniper NETWORKS
global
Investigate
Log Viewer
Report Manager
FW/VPN Reports
Top Alarms
Top Traffic Alarms
Top Traffic Logs
Top Configuration Logs
Top Information Logs
Top Self Logs
DI/DP Reports
Screen Reports
Administrative Reports
UAC Reports
Time graph of UAC session logs
Top 20 Destinations
Top 20 Enforcers (devices) for UAC
Top 10 auth failures for user@realm
Profiler Reports
AVT Reports
SSL/VPN Reports
EX Switch Reports
Top Configuration Changes (last 1 w
My Reports
Others
Shared Reports
Log Investigator
Realtime Monitor
Security Monitor
Audit Log Viewer
Configure
Administer
super@10.204.32.4
Top Alarms
Top Alarms
Last day as of 9/21/08 12:05:35 AM
CHASSISD_VERSION_MISMATCH; Error
CHASSISD_PIPE_WRITE_ERROR; Error
CHASSISD_IPC_FLUSH_ERROR; Warning
SNMPD_AUTH_FAILURE; Debug
CHASSISD_I2CS_READBACK_ERROR; Error
CHASSISD_MGR_CONNECT; Error
CHASSISD_FASIC_HSL_LINK_ERROR; Error
CHASSISD_PIC_CMD_TIMEOUT; Error
BFDD_READ_ERROR; Informational
PPMD_READ_ERROR; Informational
ESWD_PPM_READ_ERROR; Informational
PFED_NOTIFICATION_STATS_FAILED; Warning
Log Viewer - Juniper Networks - NSM - global : current
File Edit View Devices Tools Help
Log Viewer
Sep 18
Sep 19
Sep 20
Out
In
Tailing Logs
Summary
All Fields
WhoIs Lookup
Quick Report
Matching Data Snippet
super@10.204.32.45

Alarm	Severity	Count
CHASSISD_...		1054
CHASSISD_...		505
CHASSISD_I...		501
SNMPD_AUT...		308
CHASSISD_I...		27

Log ID	Time Received	Alert	User Flag	Src Addr	Dst Addr	Action	Protocol	Dst Port	Rule #	Nat Src Addr	Nat Dst Add
20080918/161436	9/18/08 11:20:39 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161437	9/18/08 11:20:39 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161438	9/18/08 11:20:39 PM			0.0.0.0	0.0.0.0			0			
20080918/161439	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161440	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161441	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161442	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161443	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161444	9/18/08 11:20:40 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161445	9/18/08 11:20:41 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161446	9/18/08 11:20:41 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161447	9/18/08 11:20:41 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161448	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161449	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161450	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161451	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161452	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	
20080918/161453	9/18/08 11:20:42 PM			0.0.0.0	0.0.0.0			0		0.0.0.0	

9/18/08 11:20:40 PM

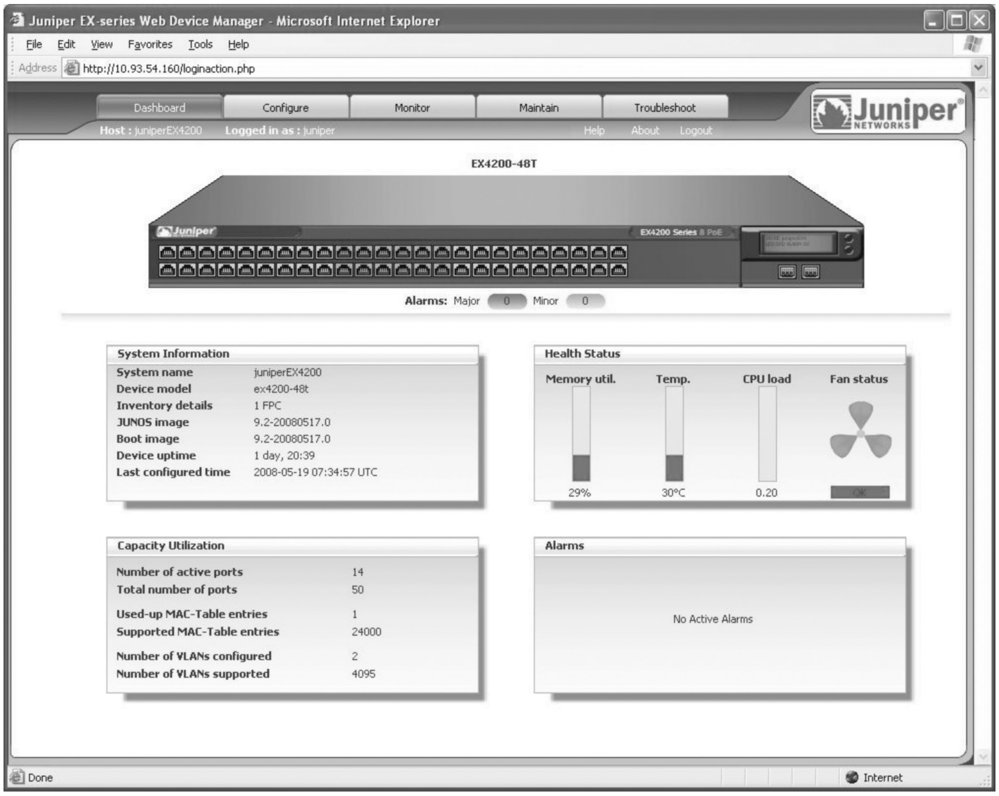
Figure 24: NSM Event and Log Management

NSM Benefits

NSM lowers operational costs by presenting a GUI to simplify complex tasks such as network topology discovery and mapping, device configuration, supplying device templates to minimize configuration errors, providing investigative tools for complete visibility into the network, and more.

Remote Configuration and Management with Juniper Networks J-Web Software

In addition to a full-featured command-line interface (CLI), J-Web, a web-based tool, is available to configure and manage any JUNOS-powered device.



Alarms: Major 0 Minor 0

System Information

System name	juniperEX4200
Device model	ex4200-48t
Inventory details	1 FPC
JUNOS image	9.2-20080517.0
Boot image	9.2-20080517.0
Device uptime	1 day, 20:39
Last configured time	2008-05-19 07:34:57 UTC

Health Status

Memory util.	Temp.	CPU load	Fan status
29%	30°C	0.20	OK

Capacity Utilization

Number of active ports	14
Total number of ports	50
Used-up MAC-Table entries	1
Supported MAC-Table entries	24000
Number of VLANs configured	2
Number of VLANs supported	4095

Alarms

No Active Alarms

Figure 25: Easy-to-use graphical J-Web interface

J-Web Benefits

Built on JUNOS Software, J-Web offers a graphical user interface for device management that complements the existing suite of element and service management products from Juniper Networks. J-Web provides IT administrators and network operators with simple-to-use tools to quickly and seamlessly monitor, configure, troubleshoot, and manage any switch, router, or firewall.

J-Web even allows non-technical users to commission and bring a router online quickly and easily. It offers seamless GUI access to all JUNOS features and functions, reducing timelines for new service deployments. J-Web can be quickly integrated into existing network management or operations support systems (OSS) applications such as Micromuse Netcool OMNIbus, Dorado RedCell Manager, IBM Tivoli, and HP Openview, thereby minimizing complexity for the service provider or enterprise customer. Fast, error free service changes and upgrades can be made with J-Web's quick configuration wizards, and new services can be rapidly created and deployed with the use of configuration and QoS wizards that allow for real-time changes to service parameters.

Summary

The highly visible enterprise LAN is a core asset that must be accessible any time from anywhere—offering secure, high-performance services regardless of location. A number of trends are increasing security and performance challenges that existing campus infrastructure solutions can't meet. In addition, existing solutions do not provide the centralized management capabilities critical for reducing costs and streamlining operations. A new campus LAN design that meets campus security, connectivity, and performance challenges while enabling key IT initiatives is needed. It also must scale, offer operational simplicity, and flexibly accommodate new computing trends without an entire redesign.

Juniper's solutions, including a new family of high-performance Ethernet switches, redefine the way businesses build campus networks. Offering high port densities, wire-speed connectivity, and high availability in compact, pay-as-you-grow platforms, Juniper's switches represent a powerful yet cost-effective alternative to the aging and expensive solutions pushed by today's dominant switch vendors. They enable the collapse of inefficient layers required by traditional solutions. By offering a smaller footprint in the wiring closet combined with lower power and cooling requirements, Juniper switches represent the efficient and "green" solutions users are looking for to power their networks of the future. In addition to a full suite of secure services, Juniper Networks products provide the end-to-end QoS required for sensitive and bandwidth-hungry applications such as unified communications.

JUNOS Software, a single, consistent operating system used across all Juniper switch, router, and firewall products, makes the network infrastructure exceedingly easy to deploy, configure, and upgrade, saving considerable time and operating resources that can be reallocated to further improve business operations and maximize customer satisfaction.

Juniper Networks infrastructure solutions advance the economics of networking, allowing businesses to "change the rules" with their IT investments and create a truly innovative and competitive environment that helps them increase revenue and raise productivity today and into the future.

About Juniper

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. 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

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
Fax: 35.31.8903.601

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

8020001-001-EN Apr 2009

Printed on recycled paper.