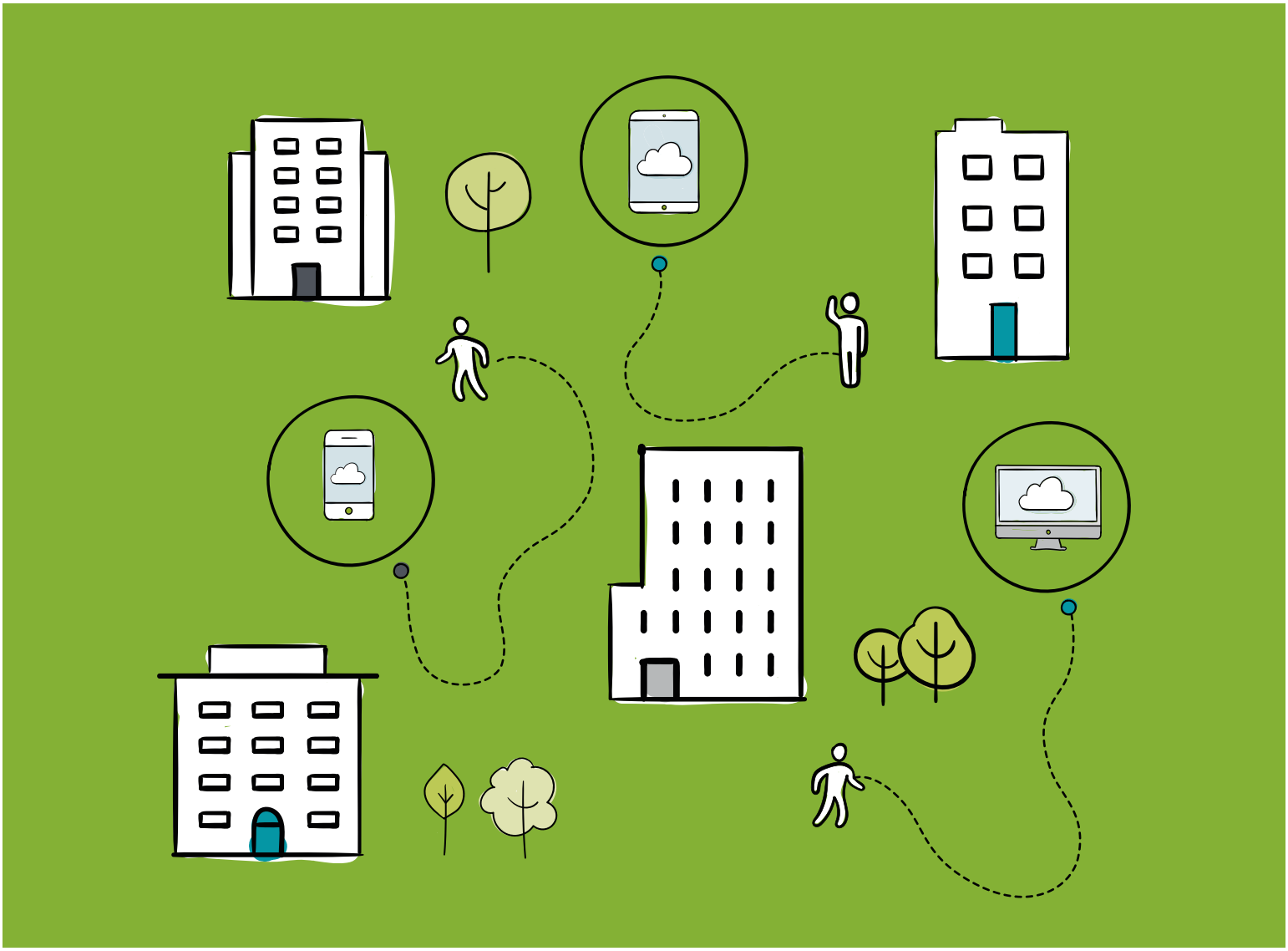
JUNIPER NETWORKS | Engineering Simplicity

eGuide

Everything You Need To Build An AI-Driven Enterprise

A Buyer's Guide to Optimizing Your Wired and Wireless Network



March 2020

Inside

Introduction **3**

Market Trends in Campus **4**
- Understand and Define the User Experience 4
- AI for IT 4
- Democratized and Distributed Operations 5
- Evolving to Automated Security 5
- Mobile Reality 5

Customer Challenges in Campus **6**
- KLO Activities 6
- Day 0/Day 1 6
- Ongoing, Daily Management and Monitoring 6
- Troubleshooting, When Things Go Wrong 6

Essential Campus Considerations **7**
- Centralized, Cloud-Based Management 7
- Advanced, Connected Security 7
- Self-Forming Campus Fabrics 8
- AI Tools, Analytics and Assistants 8
- Essential Campus Switching Features 9

Top 5 Reasons to Choose a Juniper Campus Network **10**
- 1. AI-Driven Campus and Beyond 10
- 2. Simplified Operations 10
- 3. Connected Security 11
- 4. Common Building Blocks for Investment Protection 11
- 5. Simple Campus Portfolio 12

Why Juniper Networks **13**

Juniper Campus Portfolio **13**
- Juniper Multicloud-Ready Campus and Branch Portfolio 13

Juniper Campus Portfolio **14**
- EX Series Ethernet Portfolio 14

Mist Wireless LAN Platform **15**

Introduction

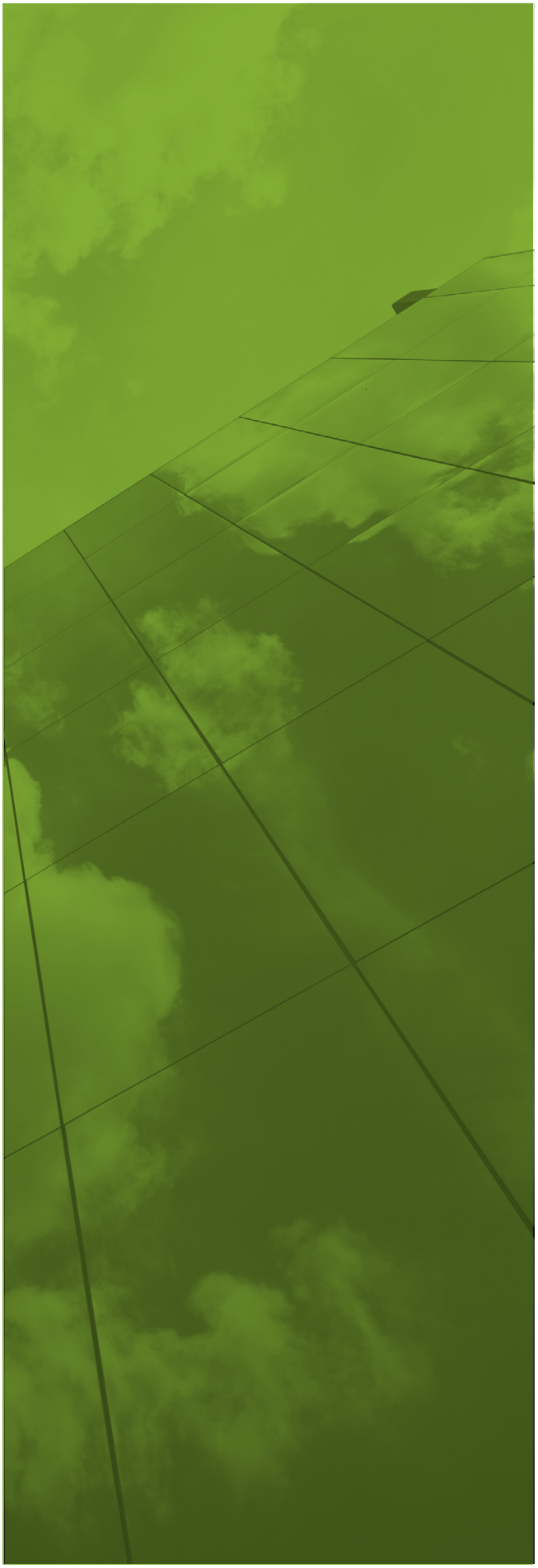
The AI-Driven Enterprise embraces experience as the new uptime. It's about leveraging tools interfaces and data to reduce reliance on manual actions, as the future becomes more focused on operations. And the campus network is critical to this future.

From configuring and deploying your network, to monitoring and controlling it, a Juniper Networks-based campus solution simplifies your life and brings you a step closer to realizing the benefits of a secure and automated multicloud enterprise.

Juniper Networks (Mist Systems) was included in the 2019 Gartner Magic Quadrant and Critical Capabilities for Wired and Wireless LAN Access Infrastructure and we believe customers should evaluate Juniper and Mist for all wired and wireless access layer opportunities globally. We were ranked within the three highest scores in all 6 of 6 Use Cases, while also being positioned as a Visionary in the Magic Quadrant.*

Read the Magic Quadrant report and the Critical Capabilities report to learn more.

Take advantage of your refresh and expansion opportunities to make changes that will help you on your journey.



Gartner Magic Quadrant for Wired and Wireless LAN Access Infrastructure, Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint, 24 September 2019.

Gartner Critical Capabilities for Wired and Wireless LAN Access Infrastructure, Christian Canales, Tim Zimmerman, Bill Menezes, Mike Toussaint, 26 September 2019.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

Market Trends in Campus

Understand and Define the User Experience

Ensuring a positive user experience is a crucial component for campus productivity, efficiency, and collaboration. The user's digital onramp to services in a campus network begins at the access edge and has many invisible and critical dependencies. Previously, basic monitoring and uptime were used to infer user experience; however, now considered table stakes, it's the quality of experience defined through with heightened SLEs (Service Level Expectations) that set the bar. To meet these expectations, IT operations must shift from reactive troubleshooting to proactive remediation. A shift away from reactive to proactive operations is underway. It's a move facilitated by AI that enables teams to keep their service promise.

All across the campus, a new breed of AI for IT observes, learns, and correlates events based on the characteristics of your specific network. It enables meaningful SLEs to be set, met, and often exceeded. Wired and wireless telemetry is streamed and ingested continuously to gain better visibility into end-user experience, to shorten MTTR (Mean Time To Repair), and to highlight and fix misconfigurations before users even know there is an issue.

Campus users expect secure, fluid, and reliable connectivity at all times, regardless of application and device type. The AI-Driven Enterprise delivers on Wired and Wireless Assurance with proactive anomaly detection, self-driving remediation, and an AI engine all in support of lowering IT costs.

AI for IT

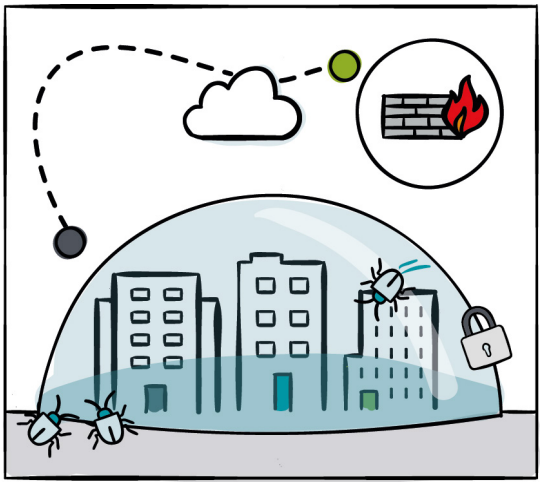
The path to AI for IT starts with the campus network. Toil is manual, repetitive work with no enduring value. It is considered an overhead and often scales linearly with your IT footprint. Operations is plagued with examples of troubleshooting toil, often codified as manual steps in operational playbooks and SOPs (Standard Operating Procedures). This toil contributes to burnout and diminishes morale. Once toil is reduced by AI and automation, humans can spend time focusing on more interesting customer and engineering challenges, such as innovation and creative problem-solving.

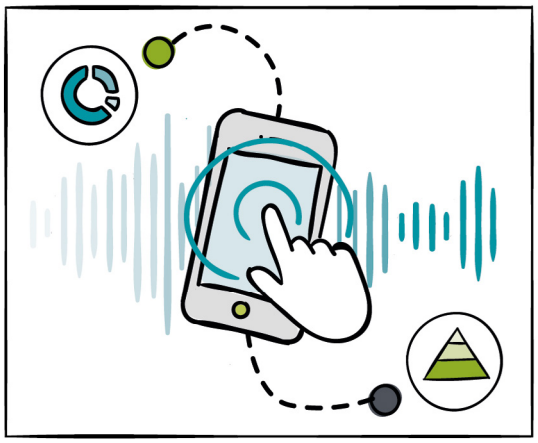
High-performing operational teams leverage modern platforms and smarter tools to scale and multiply their effectiveness. The less time they spend keeping the lights on means the more time, energy and motivation for them to be forward-looking and strategic.

Democratized and Distributed Operation

The struggle to keep pace with technology is bewildering, not only for specialists, but also general operations teams. By leveraging AI technologies, teams across the board can more easily understand network health using natural language questions. These systems continually surface root causes and enable corrective actions.

This ability to identify issues and easily troubleshoot helps accelerate service restoration and increase confidence across teams. Additionally, the capability of AI-powered platforms to proactively and automatically take packet captures from devices experiencing problems means that the support staff does not have to be engaged or present in realtime.





Evolving to Automated Security

The security of campus networks – and the IT resources located on campus – is a major concern, and one that is growing in importance. As networks increase in size and/or complexity, the volume of malicious attacks has increased commensurate with the attack surface. The attack surface of campus networks is exploding, fueled by the adoption of mobile, cloud services and IoT devices.

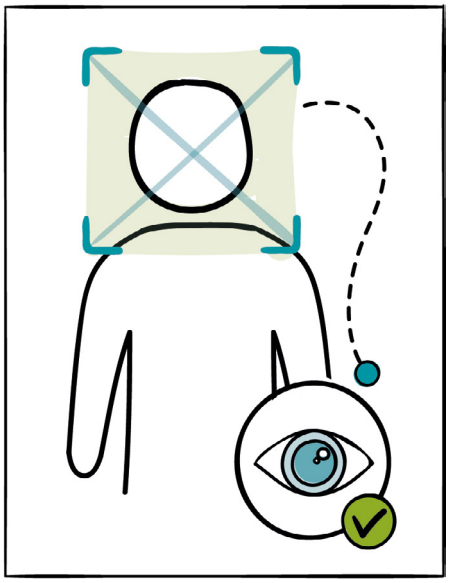
While hiding behind a perimeter firewall was never a recommended security posture, long gone are the days where even the deliberately ignorant can pretend that perimeter firewalls and sifting through log files is adequate. Advanced threat protection and real-time global sharing of threat intel, coupled with AI driven auto-remediation solutions, are now the new normal.

Mobile Reality

Mobility (WLAN) applications, coupled with real-time, location-based data, continue to drive mobile adoption and a perpetual hunger for more wireless throughput.

The soaring numbers of mobile and IoT devices continue to drive the upgrade cycles of campus wireless infrastructure, moving from 802.11n to 802.11ac and now we are entering the transition to 802.11ax (referred to as Wi-Fi 6).

These upgrades are also having a ripple effect driving the uplinks from gigabit Ethernet to multigigabit Ethernet, including the new 802.3bz standard (2.5/5 Gbps). Power over Ethernet (PoE) connections are also seeing upgrade pressures, as modern wireless access points have been demanding increasing power, from 802.3af (15.4W) to 802.3at (25.5W) and soon will start to drive a migration to 802.3bt (>30W).



Customer Challenges in Campus

KLO Activities

'Keeping the Lights On' (KLO for short), have increased in scope as the business grows and changes. This expanding scope of responsibilities, combined with the ever-expanding ratio of workloads per administrator, is putting tremendous pressure on IT teams.

Today's IT teams are under pressure to adopt emerging technologies, such as IoT or AI, in order to keep up with the efficiency and agility of their competitors. As a result, IT teams regularly find themselves facing a conundrum: they must find time to perform KLO activities while also devoting time to perpetual innovation.

KLO activities can be broken down into three basic categories:

1) **Day 0/Day 1:** these include installing a new device, adding a new application or service, or bringing up a new site.
2) **Ongoing, Daily Management and Monitoring:** these include monitoring network health and configuring the network with policy updates as needed.
3) **Troubleshooting:** this includes dealing with unplanned outages, degradations in the network's performance or perhaps a security breach.

Common Day 0/Day 1 Challenges Include:

- Lack of local expertise to install, troubleshoot, or configure new equipment
- Difficulty in discovering newly installed devices, and bringing them under management
- Difficulty applying secure defaults for new users/devices across all infrastructures that are part of the organization's multicloud

Ongoing, Daily Management and Monitoring:

- Managing policies across multiple infrastructures is increasingly complex, resulting in the inconsistent and error prone application of policies
- Operating systems, applications, and devices are often out of date, and need patching. Network equipment, such as switches and routers are often the worst culprits
- Access Control List conflicts: "ACLs are like cockroaches. They come but they never go!"

Troubleshooting, When Things Go Wrong:

- Troubleshooting is tedious and time consuming
- Disaggregated data sources: "I have to sift through multiple logs from many sources to hunt for a root cause"
- Information overload: "I am being flooded with meaningless alerts"
- Aging equipment failing

By reducing the KLO burden, IT can invest more in innovation, which is essential to ensuring the organization remains agile and competitive.

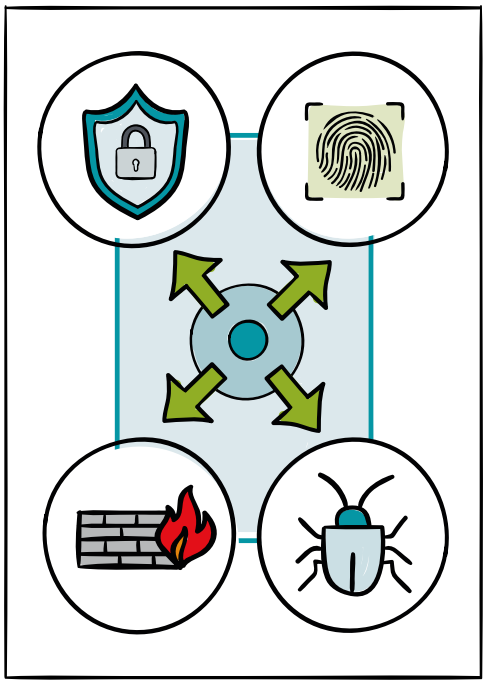
Essential Campus Considerations

Centralized, Cloud-Based Management

Reduce or eliminate KLO activities by centralizing the management of your campus networks.

Whether these networks consist of multiple campus sites, distributed remote sites, or some combination of the two, by leveraging a professionally secured, cloud-based management solution, you eliminate the need to have onsite IT expertise to handle daily management activities.

With zero-touch provisioning technology in your networking devices, bringing up a new site can be accomplished seamlessly, remotely, from anywhere you access a browser.



Advanced, Connected Security

Traditional security approaches are unable to keep up with the increasing volume of threats. To successfully defend their networks, today's organizations require deep network visibility, and multiple points of enforcement throughout the network. This includes advanced threat protection, where threat intelligence uncovered by one organization is shared by all.

Everything passes through the network, including threats. As a result, the entire network can be part of an organization's security solution.

Modern, automated network security enables an organization's centralized security solution to collect information from multiple points throughout the network, as well as apply policy to all network devices, right down to the access switching layer. ACLs and other network configuration functions become part of automated policy enforcement through all layers of the network.

Today's networks are heterogeneous mixes of products and services from multiple vendors, and frequently stretch across multiple infrastructures, creating a multicloud environment. Defense in depth thus requires multiple security products from multiple vendors working in concert.

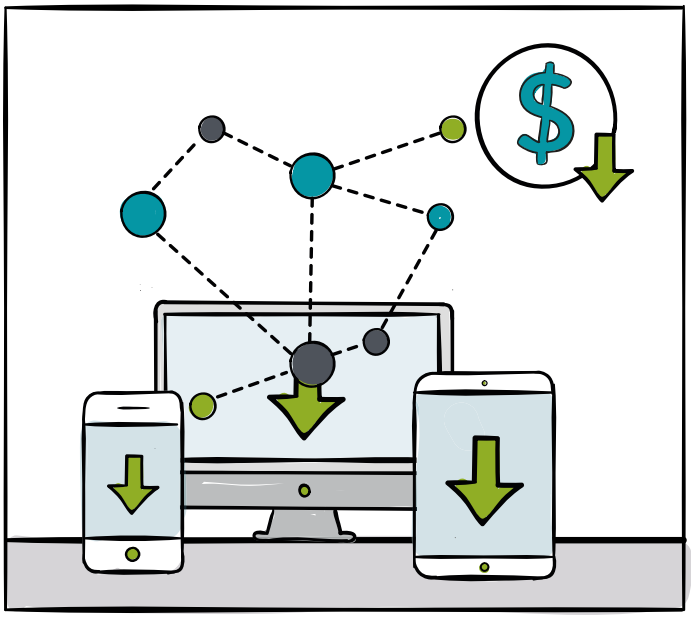
Organizations need the ability to detect threats, and apply policy in a unified fashion, no matter where a workload or data happen to live within an organization's infrastructure.

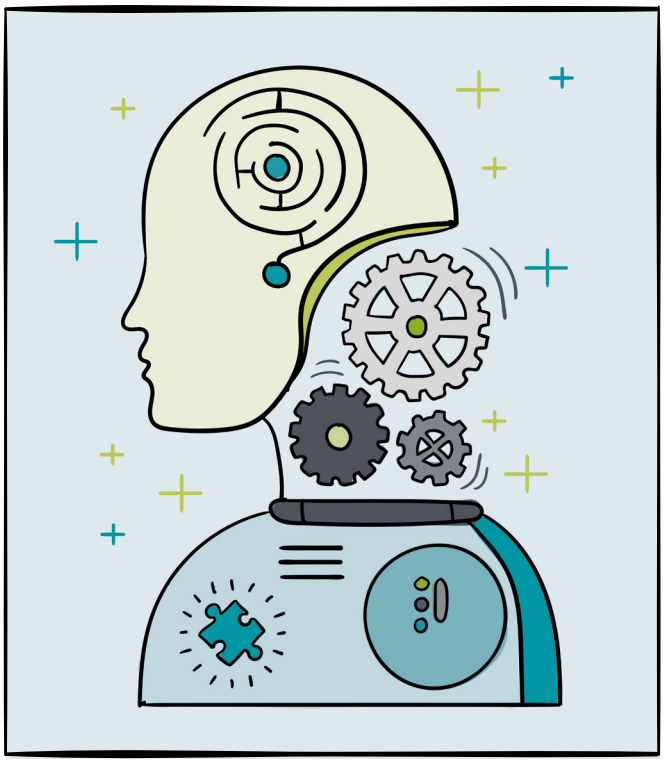
Self-Forming Campus Fabrics

Self-forming campus fabrics drive efficiency and simplify IT operations. A campus fabric helps reduce the number of managed devices in your campus switching infrastructure. In turn, this will drive down your KLO budget, and can significantly improve your OpEx.

Modern fabric technologies help you collapse and eliminate network layers while also eliminating the need for throughput-crippling Spanning Tree Protocol (STP). These fabrics simplify deployments with easy plug-and-play solutions, reducing outages caused by installation errors, and simplifying Day 0/1 operations.

An open, standards-based automation and management architecture is useful for network fabrics. These allow organizations to operate from a single Network Operations Center (NOC) with shared management and automation solutions. Leveraging open, standards-based technologies also helps avoid costly rip and replace, ensuring you can apply a uniform security policy throughout your network, from the individual campus to the entire multicloud.





AI Tools, Analytics and Assistants

Increasingly, your campus environment generates more data as your users bring more diverse devices, beyond typical smart phones and compute devices (PCs, Macbooks, etc.). Whether devices are personal wearables or business-intended IoT devices, they add to the diversity and complexity unique to your campus environment. Regardless of how these devices connect, wired or wirelessly, they introduce a new level of unpredictability and variability to your campus network environment.

Artificial Intelligence (AI) tools and techniques can help you make sense of this new campus environment. Third party tools and assistants can be adapted to make it easy to collect, structure and process the mountains of data generated in your network. This in turn gives you the ability to automate responses and decisions or to simply regulate your network. An AI or an AI assistant can make it easy to deliver a remarkable user experience in your campus.

Essential Campus Features

AI-Driven Operations: AI-Driven Operations: When experiences are the new uptime, the role the campus network plays becomes much more critical. The network shift towards a self-driving network leverages data for AI and automation to quickly and effectively surface anomalies and identify root causes. But beyond that, we now expect to be able to use natural language questions rather than esoteric commands to engage with complex systems to ask basic questions like “who are the unhappy clients in the office” or “how is AP ap-1” for the ultimate user experiences

Power over Ethernet (PoE): As with any decades-old technology, there are several versions of PoE. The various standards allow delivery of power, from 15W to 100W allowed by the new PoE++.

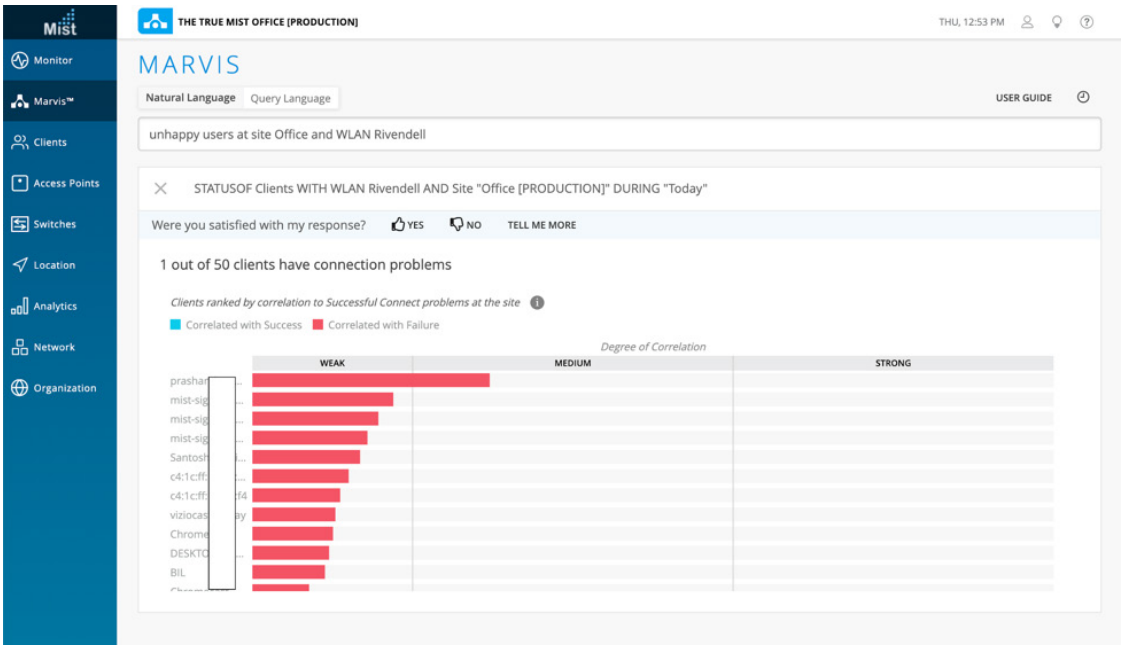
PoE significantly simplifies campus physical wiring since it reduces the number of cables by up to half. Depending on your applications and devices, you’ll need to select campus access switching with the appropriate number PoE ports, total PoE budget and the amount of power per PoE port.

Multigigabit Ethernet: The shift from traditional 802.11n Wi-Fi networks to new Wi-Fi 6 standards requires more throughput than 1GbE access speeds to the Wi-Fi access point. Upgrading to multigigabit Ethernet allows you to support these higher throughput access points using existing cabling infrastructure.

Modern campus switches allow ports with 1GbE and 2.5GbE access, with many offering ports with 1GbE, 2.5GbE, 5GbE, and 10GbE. When your next network refresh opportunity arrives, consider adding multigigabit Ethernet ports.

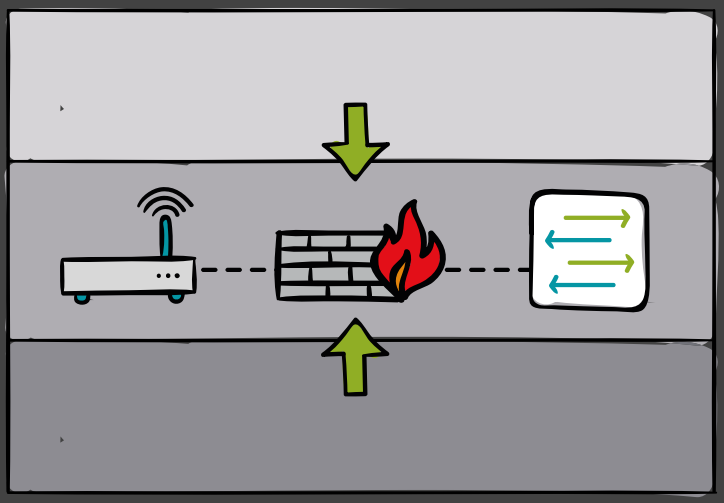
MACsec: Many federal government agencies mandate the use of MACsec encryption between access switches and various compute devices in the campus environment.
Many other industries and verticals are also adopting this additional level of security to prevent the theft of business data by hackers. MACsec encryption can now be found in access, aggregation and core switching devices, protecting copper and fiber-based links at 1GbE through 10GbE and even higher speeds.

Compact and Fanless Access Devices: Advancements in integrated circuits now allow organizations to deploy silent, fanless switches throughout their campus environment. These can be deployed in open office work areas, in classrooms, or even in hotel rooms – anywhere with strict reduced noise levels are mandatory. Silent, fanless switches are often compact, with flexible mounting options that allow them to be deployed in many configurations. These switches increase the number of devices that can be securely hard-wired into the network while still providing a fully automatable, securable network access port for each device.



Top 5 Reasons to Choose
a Juniper Campus Network

1 AI-Driven Campus and Beyond



Juniper's Mist AI-driven platform gives you a powerful wired and wireless solution by combining AI, machine learning and data sciences, all delivered through a modern and elastic microservices cloud. This allows you to optimize the user experience for your customers while bringing unprecedented insights and automation into the network.

The Mist platform delivers services for Wi-Fi assurance, Marvis virtual network assistance, Bluetooth LE user engagement and Bluetooth LE asset visibility.

Mist Assurance integrates the wired and wireless portfolio to provide end-to-end visibility into the user experience and network operations.

2 Simplified Operations

Executing operational and configurational tasks on each individual switch in your network can be taxing. To simplify switch management, Juniper supports various fabric architectures that address your unique scalability requirements.

Virtual Chassis and standardized technologies such as MC-LAG and EVPN-VXLAN reduce network complexity and operational expenses by allowing multiple distributed Juniper switches to be interconnected and managed as a single, logical device.

Contrail Service Orchestration (CSO) brings centralized, cloud-based management to your operations for software-defined LAN, WAN and Wi-Fi. With support for zero-touch deployment, your network will be up and running in no time. CSO supports all Juniper devices, including the EX Series Ethernet switches, SRX Series next generation firewalls, and the NFX Series virtual services devices. It can even provide visibility of a unified WAN and LAN for wired and wireless operations.

3 Connected Security

Juniper Connected Security provides top to bottom and end-to-end network security, to see, automate and protect across an organization's entire multicloud infrastructure. Juniper Connected Security provides deep network security and multiple points of enforcement throughout the network.

Juniper Connected Security combines Advanced Threat Protection, integrated identity management, next-generation user-based firewalls, and advanced analytics with dynamic, automated policy enforcement. All network elements, including EX Series switches, participate in securing the network.

Juniper Connected Security goes beyond perimeter protection to include network segmentation, turning an organization's entire network infrastructure into an enforcement domain.

One example of a simple and straightforward Connected Security feature is MACsec. MACSec is an encryption mechanism that prevents attackers from eavesdropping on transmission between two network nodes. From the access layer switches, to core and aggregation switches, the EX Series family of Ethernet switches provides support for MACSec, providing the added peace of mind that data is safe, no matter where it is in its journey across the network.

4 Common Building Blocks for Investment Protection

As demand for throughput and capacity grows, you'll likely expand your campus network. Juniper's Virtual Chassis technology allows you to grow your configuration to support up to 10 switches. It also allows you to combine different EX Series switches in the same deployment, giving you a mix of 1GbE, 10GbE, 40GbE, and 100GbE interfaces for painless upgrades to higher throughput.

For even greater scalability, look to an EVPN-VXLAN fabric architecture. This technology allows you to easily add more core, aggregation and access layer devices to match your business needs without having to redesign the network or perform a forklift upgrade.

5 Simple Campus Portfolio

From access to core and aggregation to your campus edge, Juniper offers a simple and programmable set of choices that meet all your campus infrastructure needs. A simple and diverse enterprise access point portfolio that integrates Wi-Fi, Bluetooth LE and IoT technologies with models for indoor and outdoor deployments. PoE++ and multigigabit in the access supports the latest WLAN standards and most power-hungry IoT devices. A rich set of fixed and modular 10-, 40-, and 100GbE core and aggregation devices offer high availability to support any sized campus deployment. And a feature-rich portfolio of WAN edge devices provides next generation firewall capabilities, secure routing, SD-WAN, and a robust, battle-tested routing stack.

> **“Surpass your users’ expectations. Junos and Mist deliver client Service Level Expectations (SLEs) for assurance.”**

Why Juniper Networks

Juniper Networks delivers secure and automated campus networks. Using a common set of building blocks based on both merchant and custom silicon, Juniper routers, switches, and firewalls span a full range of scale and cost.

With Juniper Networks Junos® operating system as the foundation, campus networking and security devices share a common automation framework that includes programmatic interfaces, real-time telemetry, and integration with management tools.

The combined Juniper Mist solution delivers an elastic, simplified architecture with distributed intelligence across the wired and wireless network for greater levels of performance, security, and reliability that ultimately results in better end-user experience.

Juniper Campus Portfolio

Juniper Multicloud-Ready Campus and Branch Portfolio

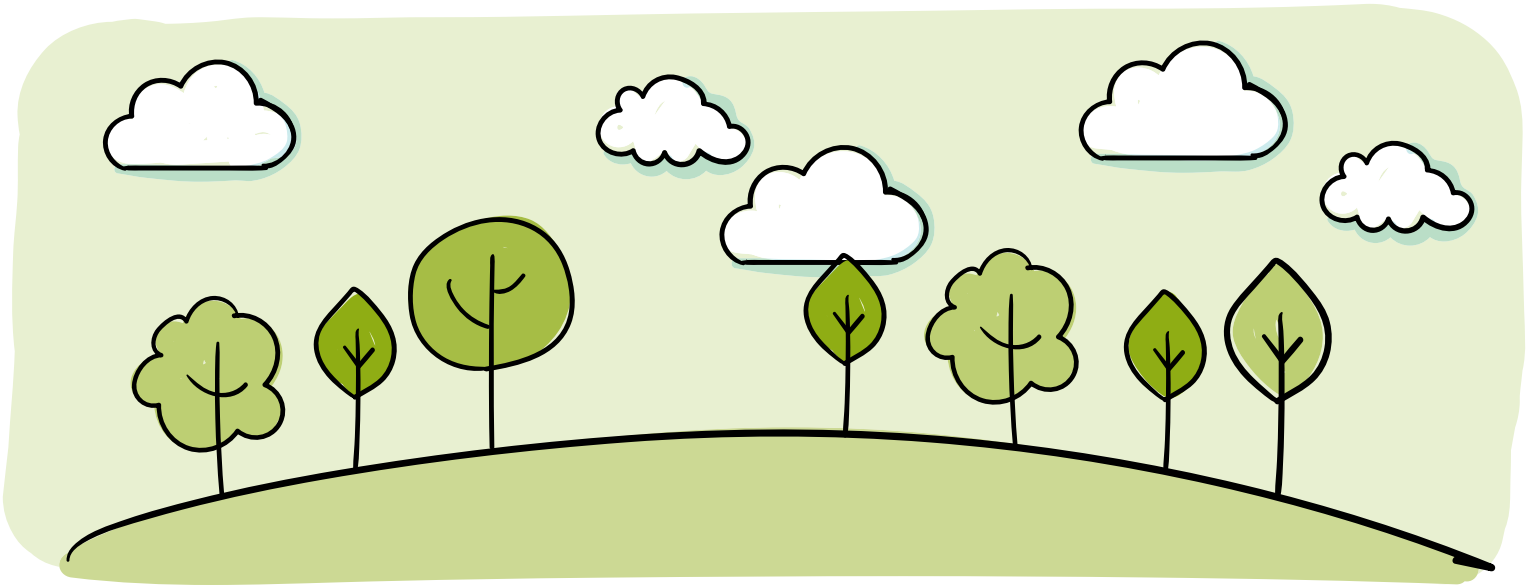
	ENTRY LEVEL	MID RANGE	PREMIUM	
EDGE	SRX/NFX Series	SRX Series	MX Series	
CORE / AGGREGATION	EX4600/4650	EX9250	EX9200	Juniper Sky Enterprise
ACCESS	EX2300	EX3400	EX4300	

Juniper Campus Portfolio

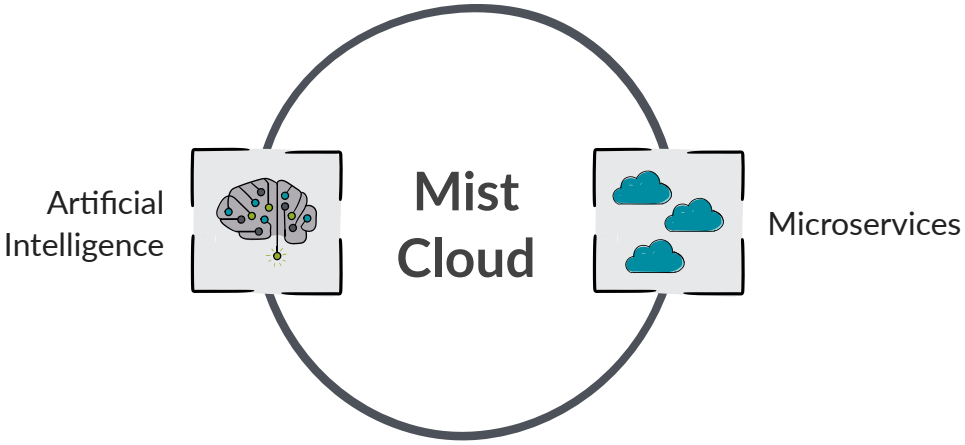
EX Series Ethernet Switch Portfolio

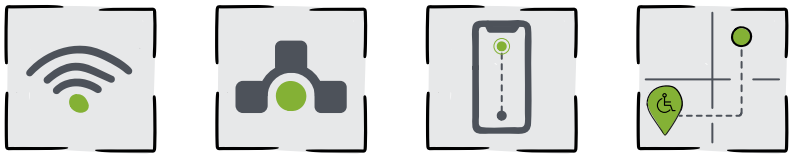
Access, Aggregation and Core LAN Switching

EX2300-C/EX2300	EX2300 Multigigabit	EX3400	EX4300	EX4300 Multigigabit	EX4600	EX4650	EX9200	EX9250
Access	Multigig Access	Access	Access & Aggregation	Multigig Access & Aggregation	Aggregation	Core & Aggregation	Core & Aggregation	Compact Core & Aggregation
12-24-28 x GE 2-4 x 10GE SFP+		24-48 x GE 4 x 10GE SFP+ 2 X 40GE QSFP+	24-48 X GE 4 X 10GE 4 X 40GE QSFP+		72 x 10GE SFP+ 12 x 40GE QSFP+	48 x 10GbE 8 x 100GbE	Up to 320 x 10GE Up to 60 x 40GE Up to 20 x 100GE	Up to 144 x 10GE Up to 36 x 40GE Up to 24 x 100GE
PoE / PoE+	PoE / PoE+	PoE / PoE+	PoE / PoE+	PoE / PoE+ / PoE++	N/A	N/A	N/A	N/A
Virtual Chassis (VC) Capable					VC & MC-LAG	MC-LAG & EVPN-VXLAN	MC-LAG	

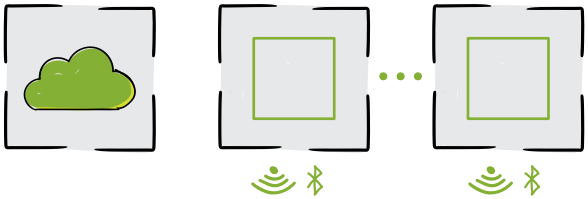


Mist Wireless LAN Platform





Subscription Services



Mist Edge Access Points

AP43: Highest performane 802.11ax Wi-Fi, Bluetooth® LE, and IoT

AP61: Outdoor Wi-Fi and Bluetooth®

AP41: Highest performane 802.11ac Wi-Fi, Bluetooth® LE, and IoT

AP21: Highest performane 802.11ac Wi-Fi and Bluetooth® LE

BT11: Enterprise-grade Bluetooth® LE

Register for a Toolkit Tuesdays webinar to see a live demo of Mist Wired Assurance. Sign up now.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888-JUNIPER
(888-586-4737) or +1.408.745.2000

Fax: +1.408.745.2100

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

Copyright 2020 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. In the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

PN 7400100-004-EN

Please Note:

This guide contains general information about legal matters.
The legal information is not advice, and should not be treated as such.

Any legal information in this guide is provided “as is” without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information in this guide.

You must not rely on the information in this guide as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this guide.

Information correct at time of publication (March 2020).

JUNIPER NETWORKS | Engineering Simplicity