JUNIPER NETWORKS | Driven by Experience™

THE AI-DRIVEN CAMPUS

Using artificial intelligence for the campus networks of the next decade

White Paper

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The network for the next decade centers around delivering better user experiences and simplifying IT operations. Traditional wired and wireless LAN solutions lack the scalability, reliability, security, performance, and agility needed to address today's challenges and diverse enterprise needs.

The AI-driven campus leverages the power of artificial intelligence (AI) in the era of cloud, mobile, and IoT. Juniper's campus solution combines a robust hardware portfolio with the power of Mist AI™ to streamline network operations, improve user experiences, and enable IT teams to focus on strategic initiatives. This white paper explains the components of an end-to-end, AI-driven campus network driven by Mist AI.

Introduction

Enterprise networks are undergoing massive transitions to accommodate the growing needs of cloud-ready networks, as well as a plethora of mobile and IoT devices. Unfortunately, as the number of devices grows, so does complexity. Cloud-based applications enable new business models, provide greater business agility, and support the adoption of key technologies such as unified communications, video, and other latency-sensitive applications. Additionally, the technological advances and widespread adoption of machine learning (ML) and AI can vastly improve operations and experiences for both IT teams and end users.

Network architects are redesigning their networks to accommodate the modern business requirements of cloud-ready applications for data, voice, and video using open standards and software-driven management platforms to reduce operational costs. The ultimate goal is to leverage simpler automation, telemetry, and AI capabilities to build out the network of the next decade.

The Juniper AI-Driven Campus Network

The Juniper Networks portfolio of cloud services, software, and hardware products delivers end-to-end campus network solutions, extending across the WAN, LAN, Wi-Fi, and security domains—all while supporting open standards like Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) to drive architectural simplicity, scale, and performance.

Juniper's AI-driven campus is composed of the following:

- A modern, microservices cloud AIOps platform
- AI-powered Wi-Fi and wired switching
- Campus fabrics running EVPN-VXLAN
- Cloud-ready campus Ethernet switches
- Enterprise-grade access points with Wi-Fi, Bluetooth LE, and IoT
- Juniper Connected Security and network segmentation
- Junos® operating system
- Junos telemetry

A Modern, Microservices Cloud AIOps Platform

The Juniper® Mist cloud architecture is built around microservices for unparalleled agility, scale, and resiliency. Cloud services scale up or down elastically as needed, eliminating the cost and complexity of monolithic hardware. New enhancements and bug fixes can be delivered almost weekly without network disruption. The platform is 100% programmable using open APIs for full automation and seamless integration with complementary third-party products. The Juniper Mist cloud architecture brings an innovative approach to enterprise networks combining AI, ML, and data science with the latest microservices technology to deliver a solution like no other.

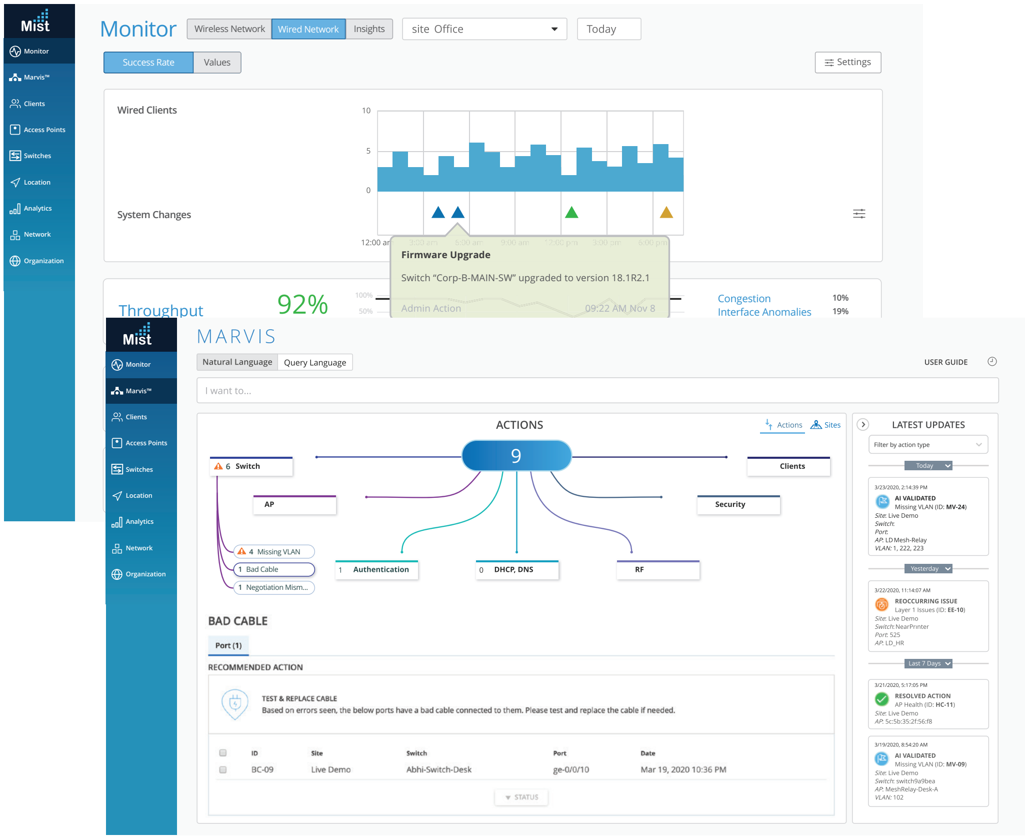
AI-Powered Wi-Fi and Wired Switching

Juniper applies Mist AI to campus networks, optimizing user experiences and simplifying IT operations across a unified wired and wireless solution. Traditional solutions are more than 15 years old and leverage monolithic code bases that are expensive to scale, prone to bugs, and difficult to manage. User experience is the new uptime—the single most important metric for measuring a successful network infrastructure. How does Juniper do it?

Juniper Mist Wi-Fi Assurance replaces manual troubleshooting tasks with automated wireless operations, making Wi-Fi predictable, reliable, and measurable with visibility into user service levels. Anomaly detection automates triggers to capture packets for event correlation, building network intelligence with Radio Resource Management (RRM) at the client level for unprecedented visibility into the user's experience with the wireless network.

Juniper Mist Wired Assurance (see Figure 1) brings AI-powered automation to wired devices. It leverages rich Junos telemetry from Juniper Networks® EX Series Ethernet Switches to enable simpler operations, shorter mean time to repair (MTTR), and improved visibility for end-user experiences of IoT devices, servers, printers, and so on. Juniper Mist Wired Assurance simplifies all aspects of EX Series switching—from onboarding to provisioning to managing from the Juniper Mist cloud architecture.

Marvis Virtual Network Assistant (Figure 1) is purpose built with Mist AI for enterprise WLAN, LAN, and WAN



Firmware Upgrade

Switch "Corp-B-MAIN-SW" upgraded to version 18.1R2.1

Admin Action 09:22 AM Nov 8

TEST & REPLACE CABLE

Based on errors seen, the below ports have a bad cable connected to them. Please test and replace the cable if needed.

ID	Site	Switch	Port	Date
BC-09	Live Demo	Abhi-Switch-Desk	ge-0/0/10	Mar 19, 2020 10:36 PM

3/23/2020, 2:14:39 PM
AI VALIDATED
Missing VLAN (ID: **MV-24**)
Site: Live Demo
Switch:
Port:
AP: LD Mesh-Relay
VLAN: 1, 222, 223

3/22/2020, 11:14:07 AM
REOCCURRING ISSUE
Layer 1 Issues (ID: **EE-10**)
Site: Live Demo
Switch: NearPrinter
Port: 525
AP: LD_HR

3/21/2020, 5:17:05 PM
RESOLVED ACTION
AP Health (ID: **HC-11**)
Site: Live Demo
AP: 5c:5b:35:2f:56:f8

3/19/2020, 8:54:20 AM
AI VALIDATED
Missing VLAN (ID: **MV-09**)
Site: Live Demo
Switch: switch9a9bea
AP: MeshRelay-Desk-A
VLAN: 102

Figure 1: Wired Assurance and Marvis Virtual Network Assistant

networks. It applies natural language so users can directly interact with the Mist AI engine, transforming network operations from reactive troubleshooting to proactive remediation through self-driving actions. Marvis increases IT efficiencies, minimizes support tickets, and reduces time to resolution. As AI for IT Operations (AIOps) continues to accelerate, Marvis empowers organizations to manage IT operations at scale with efficiency and accuracy.

Campus Fabrics

The increasing use of IoT devices in the campus dictates that networks be able to scale rapidly without adding complexity. Since many of these devices have limited networking capabilities, they require L2 adjacency across buildings or campuses. However, L2 networks lead to loops, slow convergence upon faults, and security concerns because of data plane flooding. The security problem was traditionally solved by proprietary private VLANs, but the other issues of loops and slow convergence remained with a L2 network. This approach, however, is inefficient and hard to manage—inefficient due to excess consumption of network bandwidth, and difficult to manage because VLANs need to be extended to new network ports.

EVPN-VXLAN

The AI-driven campus architecture decouples the overlay network from the underlay with technologies such as open-standards Ethernet VPN (EVPN) and Virtual Extensible LAN (VXLAN). This provides for a loop-free network with faster convergence, and it addresses the needs of the modern enterprise network by allowing network administrators to create logical L2 networks across different L3 networks. An EVPN-VXLAN also enables microsegmentation by separating traffic among IoT devices, thus providing additional security. Juniper supports the following validated EVPN-VXLAN campus fabrics:

- **EVPN multihoming (on collapsed core or distribution)**: EVPN multihoming at the distribution of the network allows access switches to LAG across a pair of devices in the distribution. This eliminates the need for Spanning Tree Protocol (STP) across campus networks by providing multihoming capabilities from the access layer to the distribution layer. This also enables the distribution and core layers to be collapsed.
- **Campus fabric core distribution**: A pair of interconnected EX Series core or distribution switches provide L2 EVPN and L3 VXLAN gateway support. The IP Clos network between the distribution and core layers offers two modes: centrally or edge routed bridging overlay.
- **Campus Fabric IP Clos:** The Campus Fabric IP Clos architecture pushes VXLAN L2 gateway functionality to the access layer, which enables microsegmentation using standards-based, group-based policies.

An end-to-end EVPN-VXLAN architecture lets you manage your campus and data center as a single IP fabric, with over-the-top (OTT) policy and control provided by Juniper. It also simplifies policy enforcement using group-based policies across the network. Any number of switches can be connected in a Clos network or IP fabric, with EVPN-VLAN extending the fabric and connecting multiple enterprise buildings, and VXLAN stretching L2 across the network.

For more information, visit www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510643-en.pdf.

Aside from EVPN-VXLAN-based architectures, Juniper also supports Virtual Chassis technology, allowing up to 10 interconnected switches to operate as a single, logical device with one IP address. Virtual Chassis technology enables enterprises to separate physical topology from logical groupings of endpoints, ensuring efficient resource utilization.

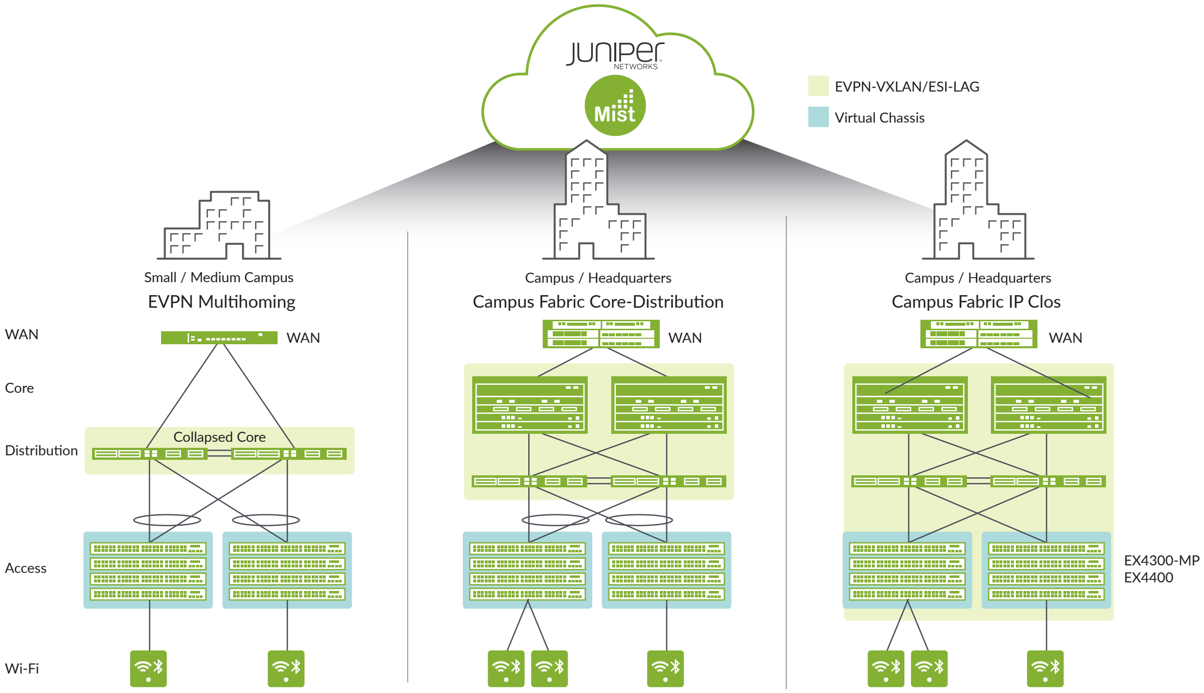


Figure 2: Campus fabrics showing Virtual Chassis and EVPN-VXLAN based architectures.

Cloud-Ready Campus Ethernet Switches

Juniper offers an AI-driven, programmable, and open portfolio of access and core/distribution switches for enterprise campus networks. The access switches are cloud ready and support Juniper Mist Wired Assurance, bringing AIOps to access layer switching. The switches meet a number of campus requirements, such as:

- Cloud-ready and managed by the Juniper Mist cloud architecture
- Multigigabit support
- Media Access Control Security (MACsec) AES256
- Power over Ethernet (PoE/PoE+/PoE++)
- Scalable fabric architectures via Virtual Chassis and EVPN-VXLAN
- Multivendor support
- Standards-based microsegmentation using group-based policies (GBP)
- Flow-based telemetry

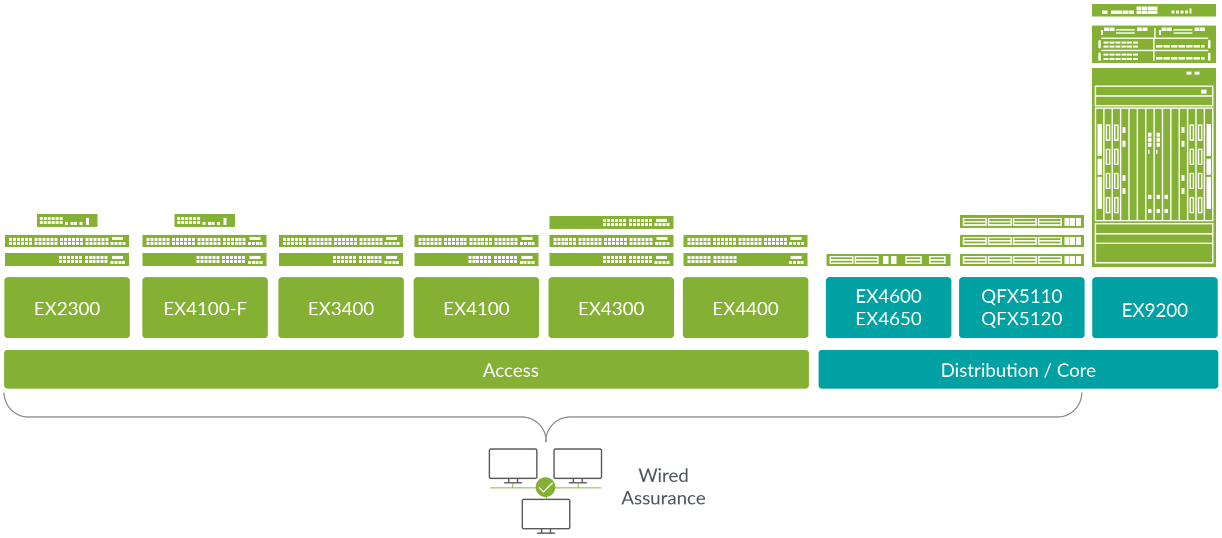
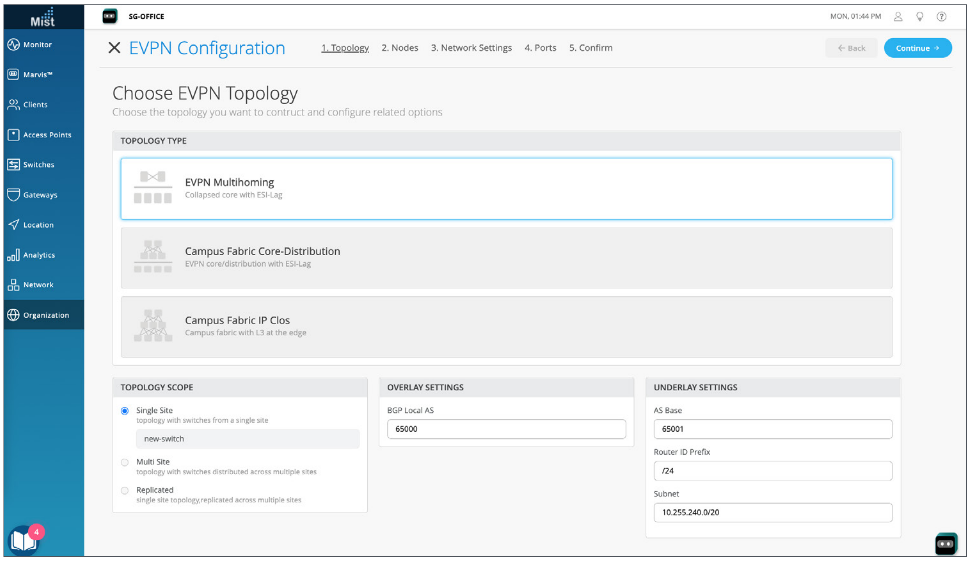


Figure 3: The campus portfolio of EX Series and QFX Series Switches.

Deploying an AI-Driven Campus Fabric

Configuring campus fabrics manually can cause inconsistency and unforced errors in deployments. Juniper solves this operational burden by enabling EVPN-VXLAN campus fabrics to be easily managed via the Juniper Mist cloud. More specifically, administrators can choose a topology (EVPN multihoming, distribution-core, or IP CLOS), and let the software do the rest (see Figure 4). This AI-driven approach unifies management across the LAN, WLAN, and WAN environments in the campus and branch while assuring the wired and wireless campus network delivers great user experiences.



EVPN Configuration

1. Topology 2. Nodes 3. Network Settings 4. Ports 5. Confirm

Choose EVPN Topology

Choose the topology you want to contruct and configure related options

TOPOLOGY TYPE

EVPN Multihoming
Collapsed core with ESI-Lag

Campus Fabric Core-Distribution
EVPN core/distribution with ESI-Lag

Campus Fabric IP Clos
Campus fabric with L3 at the edge

TOPOLOGY SCOPE

● Single Site
topology with switches from a single site
new-switch

○ Multi Site
topology with switches distributed across multiple sites

○ Replicated
single site topology,replicated across multiple sites

OVERLAY SETTINGS

BGP Local AS: 65000

UNDERLAY SETTINGS

AS Base: 65001

Router ID Prefix: /24

Subnet: 10.255.240.0/20

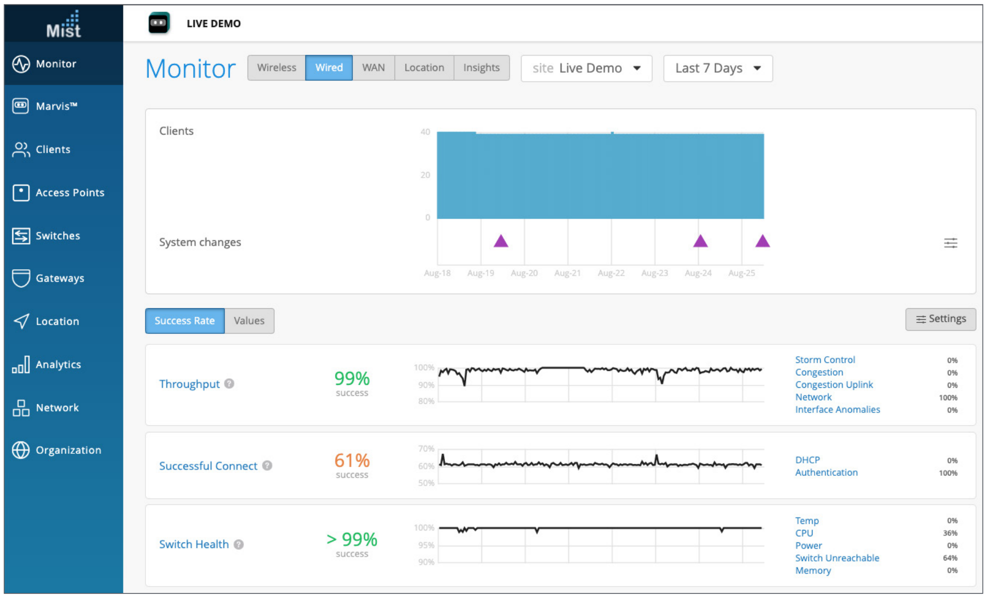
Figure 4: Juniper Mist Wired Assurance campus fabric design

*EVPN-multihoming initially supported, additional architectures supported in future releases.

Operating an AI-Driven Campus Fabric

Juniper Mist™ Wired Assurance claims, configures, manages, and troubleshoots cloud-managed EX Series Ethernet switches. The cloud-based service delivers AI-powered automation and service levels to ensure a better experience for connected devices. Juniper Mist Wired Assurance leverages rich Junos® operating system switch telemetry data to simplify operations, reduce mean time to repair, and improve visibility. Key features for Day 0 through Day 2 operations are:

- Day 0 operations—Onboard switches seamlessly by claiming a greenfield switch or adopting a brownfield switch with a single activation code for true plug-and-play simplicity.
- Day 1 operations—Implement a template-based configuration model for bulk rollouts of traditional and campus fabric deployments, while retaining the flexibility and control required to apply custom site- or switch-specific attributes. Automate provisioning of ports via Dynamic Port Profiles.
- Day 2 operations—Leverage the AI in Juniper Mist Wired Assurance to meet service-level expectations such as throughput, successful connects, and switch health with key pre- and post-connection metrics (see Figure 5). Add the self-driving capabilities in Marvis Actions to detect loops, add missing VLANs, fix misconfigured ports, identify bad cables, isolate flapping ports, and discover persistently failing clients (see Figure 6). And perform software upgrades easily through Juniper Mist cloud.



Throughput 99% success

Storm Control	0%
Congestion	0%
Congestion Uplink	0%
Network	100%
Interface Anomalies	0%

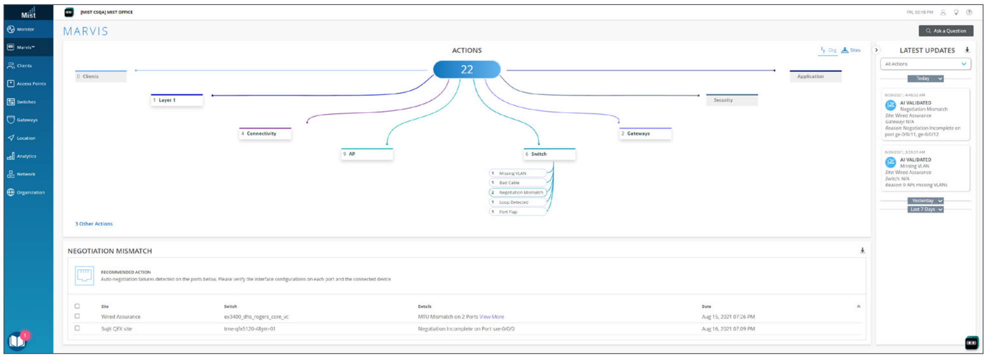
Successful Connect 61% success

DHCP	0%
Authentication	100%

Switch Health > 99% success

Temp	0%
CPU	36%
Power	0%
Switch Unreachable	64%
Memory	0%

Figure 5: Juniper Mist Wired Assurance service-level expectations



8/20/2021, 4:46:32 AM
AI VALIDATED
Negotiation Mismatch
Site: Wired Assurance
Gateway: N/A
Reason: Negotiation Incomplete on port ge-0/0/11, ge-0/0/12

8/20/2021, 3:59:57 AM
AI VALIDATED
Missing VLAN
Site: Wired Assurance
Switch: N/A
Reason: 0 APs missing VLANs

NEGOTIATION MISMATCH

RECOMMENDED ACTION
Auto-negotiation failures detected on the ports below. Please verify the interface configurations on each port and the connected device.

	Site	Switch	Details	Date
□	Wired Assurance	ex3400_dhs_rogers_core_vc	MTU Mismatch on 2 Ports View More	Aug 15, 2021 07:26 PM
□	Sujit QFX site	tme-qfx5120-48ym-01	Negotiation Incomplete on Port sxe-0/0/0	Aug 16, 2021 07:09 PM

Figure 6: Marvis Actions for wired switches

For more information on Juniper Mist™ Wired Assurance.

Enterprise-Grade Wi-Fi Access Points

Juniper leads the convergence of Wi-Fi, Bluetooth Low Energy (BLE), and IoT with enterprise-grade access points. These products leverage machine learning and event correlation to offer data collection, analysis, and policy enforcement capabilities. The Juniper AP 43 and AP 45 Series of High-Performance Access Points has a patented dynamic vBLE 16-element antenna array for the industry's most accurate and scalable location services. Juniper Access Points are purpose-built to collect metadata for more than 150 states that flow into the Mist AI engine.

Feature	AP45	AP34	AP43	AP63	AP33	AP32	AP12
Wi-Fi standard	Wi-Fi 6E 802.11ax (Wi-Fi 6) 4x4: 4SS	Wi-Fi 6E 802.11ax (Wi-Fi 6) 2x2: 2SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 4x4: 4SS	802.11ax (Wi-Fi 6) 5GHz: 4x4 : 4SS 2.4GHz: 2x2: 2SS	802.11ax (Wi-Fi 6) 5GHz: 4x4 : 4SS 2.4GHz: 2x2 : 2SS	802.11ax (Wi-Fi 6) 2x2 : 2SS
Antenna options	Internal/ External	Internal	Internal/ External	Internal/ External	Internal	Internal/ External	Internal
Virtual BLE	✓	–	✓	✓	✓	–	–

Juniper Connected Security

ZDNet reported in 2020 that attack complaints to the FBI increased 69% year over year. Now, more than ever, it is essential that every organization, no matter its size, has an effective security strategy. To keep the network protected, organizations need to see the complete picture, and they can't afford major visibility gaps—this goes for both what they are protecting and what they are protecting against. Even with all the network security innovation realized during the past ten years, the industry has not put a dent in the number of successful attacks. It's clear that what's needed is for security to exist at every connection point throughout the campus. That way the network can mount a successful defense leveraging AI and defend itself more quickly and successfully.

Juniper® Connected Security extends security visibility, intelligence, and enforcement to every point of connection on the network, from client to workload. By leveraging all connection points to gain insight into who and what is on the network at the campus, and AI to determine risk at that moment, organizations can mitigate risk and balance securing the campus while ensuring campus resources are accessible.

Data. Security should protect two things: data in the data center and access to that data at the edge. While all the other elements of zero trust are designed to protect data and data access, protecting the data requires encryption in transit, encryption at rest, and a secure connection.

- Secure Vector Routing allows for segmentation based on routing vector, making it much more difficult for attackers to intercept data in transit.
- Secure Connect provides Zero Trust Network Access (ZTNA) for network connections coming from anywhere and encapsulates them in a private tunnel.
- Intent-based security controls automate data security policy enforcement within public cloud environments through Junos automation. Any data within newly created Amazon S3 buckets, for example, is encrypted at rest, and authorized data access is enforced without having to configure rules manually.

The Network

Packets traversing the network from point to point should be legitimate, not contain an exploit or malware, and be authorized to go from point A to point B. Traffic must be inspected or profiled for malicious content.

The Next-Generation Firewall (NGFW) has evolved to become the ideal solution for traffic inspection. While signatures are usually applied to packet headers and bodies and groups of packets to determine whether the traffic is malicious, AI can quickly assess unknown files, system behaviors, and traffic patterns to decide whether an attack is being attempted.

Juniper Networks SRX Series Services Gateways provide visibility into and control over network traffic as well as additional security features to combat known and unknown threats with AI-driven security services such as:

- Threat prevention against new malware. Juniper ATP Cloud uses machine learning to quickly assess unknown files and determine whether they are malware or grayware by understanding file behaviors at run-time
- Visibility and control without decrypting. ATP Cloud also assesses risk from encrypted network traffic and connecting devices, including IoT, by understanding critical components of certificates used and traffic behaviors.

People/Users

Your users on the campus access internal resources and internet-facing resources. Users are a potential attack vector, and their access must be controlled and authenticated to limit risk.

User-based policies on the SRX Series Gateways allow for granular access control to any internal or external resource. The SRX Series integrates with any identity provider and allows for secure access and security policies to follow the user wherever they go. Additionally, ATP Cloud assesses whether the user account is compromised, dynamically adjusts to the appropriate security policy and/or VLAN, and applies additional layers of authentication as necessary.

Workloads

Workloads are the sometimes-ephemeral components that comprise applications. Protecting workloads from application exploits and segmenting them from other workloads and applications is a great way to provide a last line of defense for the crown jewels in your data center.

- Cloud Workload Protection automatically defends application workloads in any cloud or on-premises environment in and against zero-day exploits as they happen. It ensures that production applications always have a safety net against vulnerability exploits, keeping business-critical services connected and resilient. Without manual intervention, it leverages microsegmentation to protect individual databases, data collectors, and all individual resources, such as Run-Time Application Protection.
- Juniper Networks cSRX Container Firewall protects the application via a containerized firewall by segmenting and controlling traffic to and from an individual application.

Devices

Visibility into devices connecting to the network from the campus is a challenge because it includes user devices, the occasional server, and IoT devices. IoT devices can be all over your campus, from connected vending machines to coffee pots to printers. Unlike user-based devices, it may be challenging to identify the appropriate level of network access and current device posture because IoT devices aren’t always equipped with endpoint agents.

- ATP Cloud is Juniper’s threat intelligence hub for the network, including assessing risk on connecting devices, identifying different device types (including IoT), and orchestrating the appropriate action when a connecting device becomes compromised.

The following features within ATP Cloud help protect devices within a zero trust network:

Risk Profiling driven by Mist AI

This feature brings network security to the distributed access network edge. It empowers IT teams to defend their infrastructure by providing deep network visibility and enabling policy enforcement at every point of connection throughout the network. As part of the threat-aware network, campus networks are active participants in their defense.

Security Intelligence for Mist

Threat alerts detected by SRX Series and ATP Cloud quickly assess security risks when users and devices connect to wireless networks and take appropriate action such as quarantining or enforcing policies.

SecIntel for EX Series

ATP Cloud sends device compromise information to EX switches so that the switch can block or quarantine infected devices providing device control even when there is no endpoint agent.

Analytics and Automation

Visibility into what is happening on the network is only half the battle; taking the visibility and intelligence gathered and using it to enforce zero trust policies will further reduce risk while allowing for scalability within network and security teams. Organizations can gain visibility with:

- Security Director Cloud. Manage on-premises, cloud-based security controls, and cloud-delivered security controls from one user interface. Use Security Director Cloud to ensure security policies follow users, devices, and applications as they move locations, never breaking visibility or protective measures against threats. Security policy can be created once and extended to any user, device, and application regardless of location changes.
- Security Director Insights. Highlight attacks in progress and map detections to the Mitre ATT&CK framework with this feature of Security Director that ingests intelligence and detections from any third-party security tool. Security Director can then define appropriate actions either directly or through Ansible automation to provide orchestration to other tools in the network.
- Junos Automation. Enhance automation with Juniper's Junos operating system that possesses a robust set of APIs and other native automation elements. Organizations gain the unique ability to control and configure as well as audit the performance of nearly every process or capability across Juniper platforms. This ability to programmatically access the power of Junos simplifies operations to reduce both CapEx and OpEx by automating process tickets and customer change requests while ensuring the overall health of the entire architecture.

Segmentation in Campus Networks

Network architects can adopt a combination of techniques such as micro and macrosegmentation to secure data and assets. A universal EVPN-VXLAN architecture can extend across campuses and data centers for consistent end-to-end network segmentation of endpoints and applications. It also helps minimize Layer 2 flooding to reduce security threats and simplify the network.

- Macrosegmentation is a logical separation of the network inside shared network devices and across shared links. It is achieved in an EVPN-VXLAN network by using VLANs at Layer 2 and virtual routing and forwarding (VRF) at Layer 3. VRF provides isolation by keeping IP traffic between two VRF devices isolated from each other.
- Microsegmentation addresses critical network protection issues by reducing risk and adapting to security demands. Juniper helps implement microsegmentation based on access control lists (ACLs) or firewall filters to control intra-virtual network traffic.

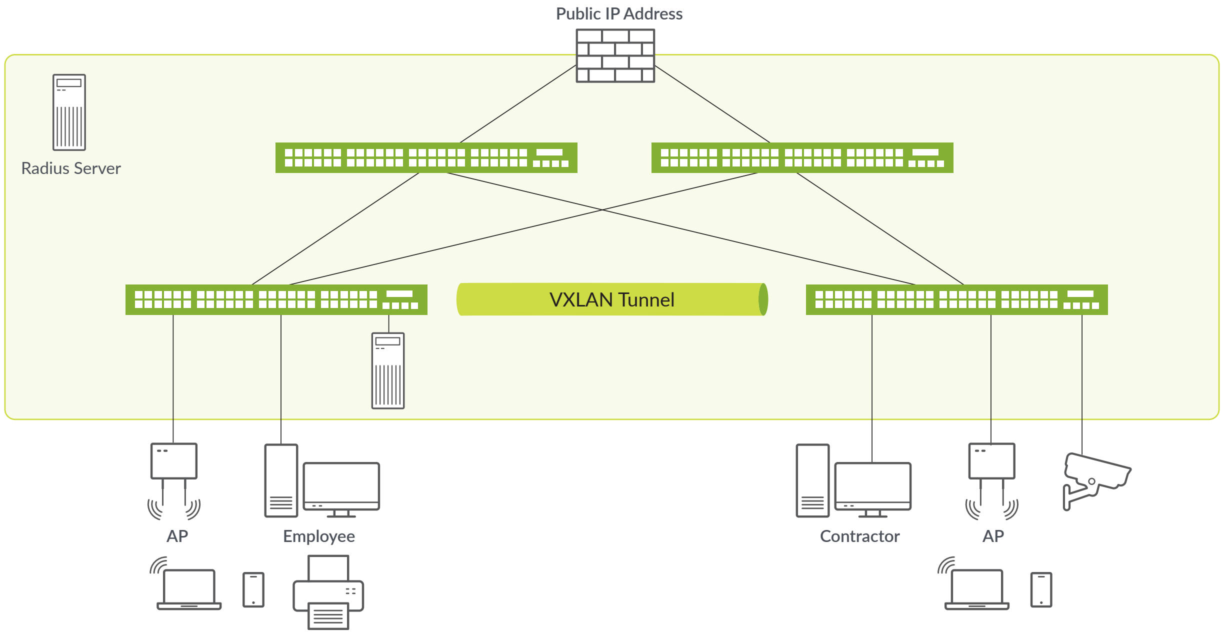


Figure 7: Network segmentation based on employee or IoT devices

Junos OS: The Foundation of High-Performance Networks

The Junos® operating system provides a common language across Juniper's routing, switching, and security devices. The power of one Junos OS reduces complexity in high-performance networks to increase availability and deploy services faster with lower TCO. The consistent user experience and automated toolsets of Junos OS make planning and training easier, increase the efficiency of day-to day operations, and allow changes to be implemented faster across the network.

What sets Junos OS apart from other network operating systems is the way it is built—one operating system delivered in one software release track and with one modular architecture. Key advantages include:

- One operating system across all types and sizes of platforms reduces the time and effort to plan, deploy, and operate network and security infrastructure.
- One release track meets changing needs in software with stable delivery of new functionality in a steady, time-tested cadence.
- One modular software architecture provides highly available, secure, and scalable software open to automation and partner innovation.

Junos Telemetry

Traditional data models that gather operational health statistics have reached the limits of network scale and efficiency. The Junos telemetry interface overcomes these limitations by relying on a push model to deliver data asynchronously, which eliminates polling. As a result, the Junos telemetry interface is highly scalable and can monitor thousands of objects in a network.

Junos telemetry interface lets you provision sensors to collect and export data for various system resources, such as physical interfaces and firewall filters. Two data models are supported:

- An open and extensible data model defined by Juniper Networks. Because this model features a distributed architecture, it scales easily.
- An OpenConfig data model that generates data as Google protocol buffer (gpb) structured messages in a universal key/value format. gRPC remote procedure calls are based on TCP, and support SSL encryption, so it is considered secure and reliable.

Conclusion

Juniper's AI-driven campus is designed to provide customers with a flexible, standards-based, modern architecture for a cloud-ready future. It meets today's stringent requirements without compromising reliability, security, and agility. Common building blocks, prepackaged automation workflows, and custom automation toolkits extend the benefits of predictive analytics from the data center to the campus and beyond.

Additional Resources

- Campus Design Center
- EX Series Family Webpage
- Juniper Mist Cloud Services
- Juniper Connected Security
- Live Demo: Wired and Wireless Wednesday
- Live Demo: The AI-Driven Enterprise
- Juniper Connected Security

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

JUNIPER NETWORKS | Driven by Experience™

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

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
www.juniper.net