JUNIPer NETWORKS

MAXIMIZING WIRELESS LAN RELIABILITY

Advanced Resiliency Capabilities and Unified Infrastructure and Services Management Combine to Deliver a Nonstop Wireless Experience

Challenge

Wireless LANs are a critical and growing portion of the enterprise LAN access infrastructure. As dependence on WLANs increases, so do SLA requirements for mission critical applications. But that is a tall order, considering Wi-Fi is shared Ethernet over an unlicensed spectrum.

Solution

From advanced planning capabilities that anticipate and enable automatic mitigation of coverage gaps, to advanced load balancing techniques that maximize resource availability and hitless failover that prevents session timeouts, even under duress, Juniper delivers nonstop wireless availability for all sessions.

Benefits

- Continuous connectivity with a predictable user experience
- Maximum coverage and capacity for all users at all times
- Seamless mobility with fast roaming indoors and outdoors
- Continuous uptime for all sessions including voice, even under failure scenarios
- Ability to perform in-service maintenance with zero downtime

As enterprises of all types deploy wireless as the primary access layer, the spotlight is naturally turning to the reliability challenges inherent in wireless technologies. Many mobility applications are mission critical, and in some cases such as healthcare, a matter of life and death. The number of users and devices is increasing rapidly, and the spectrum is getting more crowded. Hence, there is already pressure to look beyond minimum expectations for continuous signal availability and seamless roaming to meet the requirements of mobility service-level agreements (SLAs). As demand for mobility increases, wireless LAN reliability is a growing concern, and to-date only Juniper Networks delivers a nonstop wireless solution.

The Challenge

As enterprises roll out wireless LANs to enable campus-wide mobility, many organizations are now asking how they can make wireless access as reliable as wireline access. Everyone knows that wireless networks are vulnerable to interference from a variety of devices and that all clients are subject to variable association rates, depending on a user's proximity to the access point. As if this isn't enough, Wi-Fi itself is a shared medium, and users are constantly on the move, requiring the ability to roam seamlessly from one access point to another, with the expectation that the resources needed before the roam remain available during and after the roam, without any disruption.

With all of these factors to consider, it is apparent that accomplishing wire-like reliability at the session level becomes quite a balancing act. It requires a holistic approach to system-level resiliency, which takes into account the integrity of the signal in the face of performance degrading interference sources, the management of bandwidth availability in the face of competing demands, and the resiliency to timeouts and session disconnects, which can result from excessive roaming delays or network component failures.

With the right mobility architecture, however, nonstop wireless availability for all sessions is achievable—and also affordable. And contrary to popular belief, it does not have to be at the expense of management simplicity. In fact Juniper's approach, makes it is possible to configure campus-wide hitless failover for any session including active voice calls, even under failure conditions, with considerably less effort than it takes to configure the inferior hot-standby alternative, offered by other vendors. Such a capability also yields additional flexibility for IT by allowing in-service adds, moves, and changes with zero downtime for users.

The Juniper Networks Wireless LAN Solution

Holistic Approach to Wireless Reliability

The Juniper approach to system-level reliability recognizes that the ultimate goal is to ensure reliable operation for mission critical applications—in short, SLAs that are not compromised by prevailing network conditions, competing traffic flows, or the cleanliness of the airwaves. It also recognizes that reliability and resource management should be simple, not complex. Juniper's track record of innovation in wireless LAN reliability stems from its unique Juniper Networks Smart Mobile® architecture, which offers advancements in five separate areas:

1. **Over the Air Signal Integrity**—To ensure ubiquitous coverage and seamless mobility, users need reliable signals wherever they go. As the unlicensed spectrum gets more crowded, interference sources must be detected quickly so that they can be isolated or avoided. Similarly, if an access point fails, it causes a coverage hole. Adjacent access points are designed to automatically adjust power and channel settings in a coordinated fashion, to fill in until the failed access point is repaired or replaced.
2. **Availability of Resources**—Great signal strength without sufficient guaranteed bandwidth for a voice call is of little use. As demand and traffic increases, how well the load is balanced over available bands, access points, and controllers can greatly impact the user experience, especially if bandwidth abusers cannot be curbed, and available resources are left unmanaged.
3. **Reliable Mobility**—Do not mistake wireless access for mobility. They are simply not the same thing. Many business users of wireless are nomadic, but not truly "mobile." True mobility requires continuous connectivity while on the move with roaming handoffs between access points within 50 ms regardless of indoor/outdoor location, and regardless of what controllers or access points are involved.
4. **System Reliability**—The most important of all, system-level reliability, goes far beyond the component level. It defines how the wireless system as a whole maintains session availability in the event of controller failures, and how adds, moves, and changes affect service availability. The Juniper wireless LAN architecture enables an inherently reliable virtualized approach to system availability that completely eliminates downtime.
5. **Reliability Management**—Far too often, reliability techniques add significantly to the complexity of day-to-day management. Further, the growing number of mobility services that are typically installed and managed in silos create a potential barrier to coordinated provisioning of attainable SLAs. The Juniper wireless management framework unifies wireless infrastructure, security, and mobility services management, and in doing so, reduces total cost of ownership.

Coordinated Spectrum Management

Juniper's approach to over-the-air reliability tackles three separate reliability threats. First, access point or radio downtime, resulting from a network failure or faulty access point, is eliminated by automatic tuning capabilities that detect and compensate for coverage gaps. Second, by detecting rogue and neighboring access points that might be conflicting, the Juniper WLAN system can isolate the rogues and avoid the airspace occupied by neighbors. And third, by identifying the position of non Wi-Fi transmitters such as microwaves that share the unlicensed spectrum, their contaminating effects can also be avoided or reduced by transmitting on different channels.

Juniper's approach to maximizing quality transmission focuses first on preventative measures, rather than being limited only to mitigation after the fact. Reliable signal quality begins with good planning. With the advanced capabilities of Juniper Networks RingMaster, network administrators can identify the location of all static interference sources up-front during the planning stage, so that the system can automatically calculate the best channel and power settings to avoid them. And where they cannot be fully avoided, the source and its severity can be classified in advance, to avoid wasting IT resources with critical-alarm "fire-drills" every time an employee uses a microwave. By incorporating interferer information in the RF plan, those sources and their physical position can be monitored and tracked, and if they move location, the settings of nearby access points can be adjusted accordingly.

Like Juniper, most vendors support automatic tuning of access points, but few recognize the importance of delayed enforcement based on current session activity. Indiscriminate tuning and retuning of access point settings can cause constant ripples of changes in the network, which do more harm than good. Due care and consideration must be made for the live sessions. For example, voice services prefer consistent signal strength across all coverage areas. Consequently, wireless VoIP devices generally experience problems when signal strength is altered "on the fly" during a call, so Juniper's wireless solution waits until calls have ended before adjusting power settings on any one radio.

Intelligent Use of Wireless Resources

Juniper also excels in the efficient utilization and management of available resources. With local switching capabilities that offload encryption, packet inspection, and packet forwarding to the access points, Juniper's solution as well as numerous bandwidth and resource management techniques can recover 30-40% more network capacity, simply by using existing resources better.

- Local switching: Unlike most wireless LAN systems which are performance constrained by their dependence on the WLAN controller for deep packet inspection, packet forwarding, and in some cases encryption, Juniper can offload these functions to access points on a per service set identifier (SSID) or per application basis. By spreading the load, Juniper's approach is more efficient and more reliable, because it leverages the processing capacity that each new access point adds to the network, and reduces the likelihood of congestion and high latency than can cripple real-time applications.

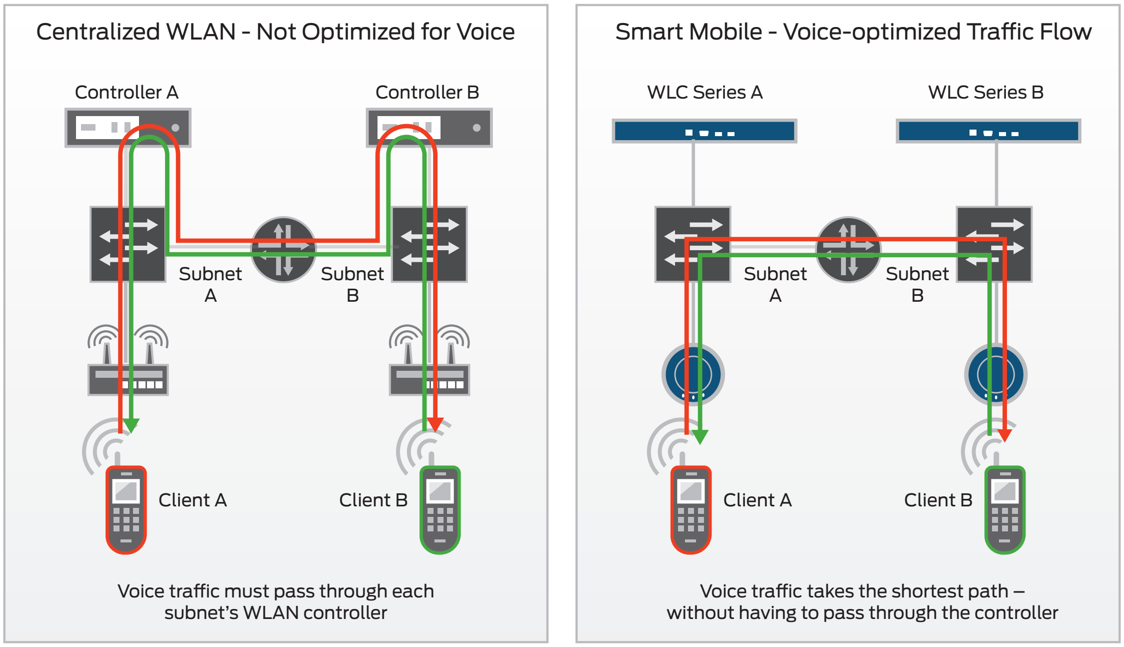
Centralized WLAN - Not Optimized for Voice
Controller A
Controller B
Subnet A
Subnet B
Client A
Client B
Voice traffic must pass through each subnet's WLAN controller
Smart Mobile - Voice-optimized Traffic Flow
WLC Series A
WLC Series B
Subnet A
Subnet B
Client A
Client B
Voice traffic takes the shortest path – without having to pass through the controller

Figure 1: Local forwarding at the access point minimizes latency

- Client steering: Juniper's patented automatic band steering moves clients from the oversubscribed 2.4 Ghz band to the underutilized 5 Ghz band, freeing up more capacity for legacy clients, smartphones, PDAs, and other devices that support only the 2.4 GHz band. Similarly, client and access point load balancing makes better use of access point and controller capacity by spreading client loads more evenly over those access points and controllers that are least used.
- Bandwidth and QoS: In addition to these various load-balancing options, the Juniper wireless solution offers granular control over the bandwidth available to each client, and this can be adjusted dynamically as resource availability shrinks and grows. Quality-of-service (QoS) profiles and bandwidth limits can be set on a per user, per SSID, and per application basis to enable minimum service-level guarantees. User-centric policies can be used to adjust those profiles, depending on the application usage and other behaviors of the client.

These various enhancements reduce resource waste and result in a more reliable mobility experience. They all serve to ensure that users can gain access to the medium, and once connected, consistently receive a sufficient supply of bandwidth to meet the needs of the applications they use.

Fast, Seamless, and Secure Roaming

A common error made when evaluating wireless LAN solutions is to confuse roaming and wireless access. They are not the same thing. Only truly mobile users—people who use wireless services such as voice, video, telemetry, and location services continuously while on the move—get to experience the reliability and efficacy of the vendor's roaming capabilities. And they are often disappointed by unexpected session timeouts and dropped voice calls when they unwittingly cross an arbitrary network boundary. Wireless voice applications and other real-time applications that require a handoff of 50 ms or less, as well as many legacy database applications, are particularly susceptible to session timeouts with the smallest interruption of connectivity or as a result of long round-trip delays.

The reason for this lies in the centralized mobility architecture of most wireless LAN systems, which simply cannot be optimized for fast and reliable session roaming as clients move around, especially when they move between access points managed by different controllers.

Unlike systems that require roaming clients to tunnel back to their "home controller" to reach their security credentials, Juniper's distributed security/authentication model propagates session keys to all access points in advance of client roams. Thus, when clients roam to a new access point, the access point can automatically and immediately recognize the client and exchange security keys, without requiring reauthentication or tunneling. Without the need for latency inducing tunnels, which can cause sessions to timeout, users can roam from floor to floor, building to building—across access points and across controllers—confident that no disruption to voice calls or any other application will occur.

Zero Downtime System-Level Resilience

Juniper Networks is the only company that has successfully stepped away from the limitations, costs, and complexity of active/standby redundancy approaches to wireless LANs. Juniper's Virtual Controller Cluster™ approach uses proven virtualization techniques to form a cluster of cooperating WLAN controllers. These are managed as one, and together they share control and management of all access points. With the Juniper approach, there is no longer a one-to-one relationship between an access point and the controller managing it, with the resulting benefit being that if any one controller in the cluster were to go out of service for any reason, the other controllers can automatically take over the load, without losing active sessions. This many-to-many resiliency is superior to traditional active/standby alternatives in several ways. It enables hitless failover for all active sessions. It facilitates in-service upgrades with zero downtime. It is much easier to configure, and yet costs less. Because all controllers in the cluster are in active use, no expensive, fully loaded "hot standby" (that will likely lay idle 99% of its life) is ever needed.

Advanced controller clustering features also make it possible to define a preferred group of controllers to be nominated as the backup for each individual controller, in the event that it fails. For large enterprises with multiple data centers, this capability provides WLAN immunity to the most catastrophic failure of all—a data center burnout. Any controller that is lost in one data center is "backed up" by the pool of controllers residing in another.

Not only does controller clustering maximize reliability, it entirely removes all of the previous complexity associated with configuring hot standby schema using protocols such the Virtual Router Redundancy Protocol (VRRP). First, instead of configuring and managing each controller one by one, they are all configured as a single system. Second, with the ability to dynamically move, add, or change access points or even controllers, without service interruption, network administrators can make network adjustments on the fly without affecting users.

No other vendor comes close to matching the unprecedented reliability benchmark set by Juniper Networks in 2008 on controller virtualization. Virtual Controller Cluster was independently proven to have sub-second failover under worst case failure conditions - a big difference from the tens of seconds or minutes recovery time and dropped sessions that are typical for most other WLAN systems.

System Resiliency Models Compared

Table 1. Virtual Controller Cluster vs. Active/Standby Approach

	VIRTUAL CONTROLLER CLUSTER APPROACH	ACTIVE/STANDBY APPROACH
Controller resiliency	• Uninterrupted sessions and data flows. • All other controllers collectively assume AP load.	• Minimum of several seconds outage for hundreds of users. • Standby controller must assume all AP load.
Access point impact	• No impact—APs already have a connection with other cluster members.	• APs reboot or restart to form new connection with standby controller.
User experience during system failover	• No impact, not even on active voice calls.	• Reauthentication is required for all sessions. • Longer restart delays if client has crypto session with controller instead of AP.
System behavior during failover	• All controllers already active and "known working." • Complete failure load balanced across community. • Easy to design/recover from multiple failures.	• Standby behavior is untested until failure occurs. • Recoverable load may be limited by capacity of standby controller • Multiple failures must have multiple manually designated standby controllers.
Configuration and management	• Only need to configure one controller in entire cluster. • Configuration distributed automatically through cluster.	• Need to configure each controller individually. • Must duplicate "one for one" configuration for each active controller.
Maintenance, moves, adds, changes	• Plug-and -Play moves, adds, and changes. • No downtime required.	• Requires reconfiguration of primary and standby devices. • Outage highly likely.
Capital costs	• Lower upfront and TCO due to granular right-sizing of resources based on "slice of capacity" model.	• Must duplicate largest controller. • Must duplicate again if protecting against multiple failures.
"Green" considerations	• All devices active, fewer and/or smaller devices needed.	• Idle, powered standby system(s) that duplicates largest controller(s).

Unified Infrastructure and Services Management

Reliable infrastructure is one thing, but what about the services? As more and more mobility services are enabled on the same "shared Ethernet" infrastructure, they start competing for resources. For any hope of providing application SLAs, those services must have complete awareness of the available network resources at the user's point of presence. This can only be achieved by unifying infrastructure management and service provisioning, which today is mostly not the case. Typical WLAN solutions manage both the infrastructure and the individual mobility services running on that infrastructure in complete isolation from one another. But only when resources are allocated with the full knowledge of competing demands is it possible to administer and enforce application SLAs. With its innovative WLAN management software, Juniper Networks leads the industry in eliminating mobility services management silos and unifying the management of WLAN infrastructure, security, and services through a single console.

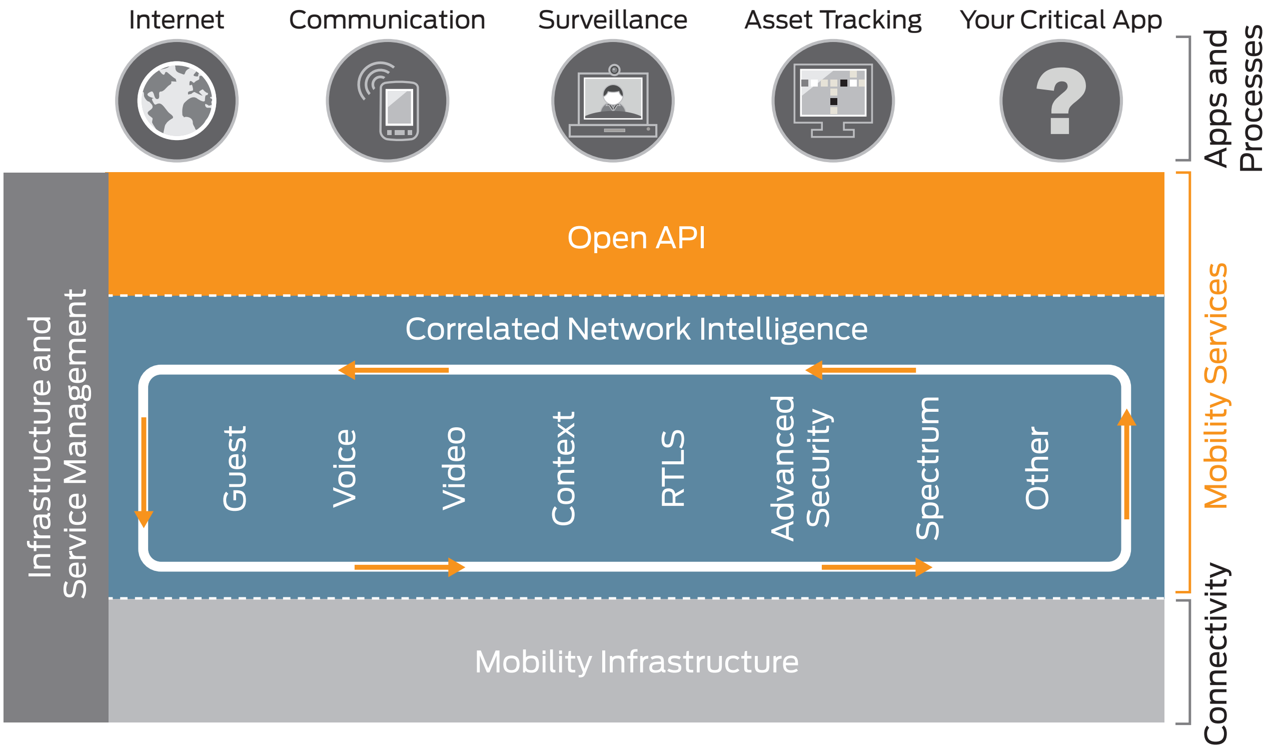

Figure 2: RingMaster unifies infrastructure and mobility services management

Features and Benefits

Table 2. Features and Benefits of Juniper's Nonstop Wireless Solution

FEATURE	BENEFIT
Wireless LAN controllers	· Virtual controller clustering that affords seamless integration of reliable, scalable, and secure wireless LANs with existing wired infrastructures for nonstop wireless access and session-level availability · For installations of any size, from small branch offices to the largest businesses and university campuses
Wireless LAN access points	· Secure, high-performance, reliable mobility indoors and outdoors for any Wi-Fi enabled device · Reduced latency, massive scalability, and high performance for wireless VoIP, video and location services · Complete access point, mesh, and bridging services
Wireless LAN management	· Advanced wireless planning, configuration, and deployment tools · Unified infrastructure, security, and services management · Real-time location awareness and access control for all users and devices · Easy guest access provisioning for nontechnical staff

Solution Components

Juniper Networks WLC Series Wireless LAN Controllers—WLC Series controllers provide users with a seamless, secure, and exceptionally reliable roaming experience wherever they are and no matter what device they are using. Meeting the needs of any size network, from small branch offices or retail outlets to large enterprises and university campuses, identity-based networking policies enable users to have a common experience with consistent services across wide geographies.

Juniper Networks WLA Series Wireless LAN Access Points—Provides indoor and outdoor connectivity for any installation size or type. The WLA Series LAN Access Points deliver reduced latency, massive scalability, and performance for wireless VoIP, video and location services.

Juniper Networks WLM Series Wireless LAN Management—The WLM Series Wireless LAN Management suite unifies infrastructure, security, and services management, enabling network administrators to plan, configure, deploy, monitor, and optimize wireless networks of any size and geography, from one console.

Summary—Juniper Networks Nonstop Wireless Solution

In the post desktop PC era, laptops are standard issue for 80% of employees, and we are witnessing spectacular growth in the number of Wi-Fi enabled personal mobile devices such as tablets and dual-mode smartphones now expecting continuous access to the network. Wireless has become a critical and growing part of the enterprise LAN access infrastructure, the onramp of choice, in fact. The time is now for the unwired enterprise to be made as reliable as the tethered one.

Juniper Networks has always known this day would come, and has been focused on reliability and large-scale WLAN manageability from the outset. Our unique mobility architecture delivers more reliable roaming, and the only hitless failover capability available in the industry. When it comes to all-around reliability, the Juniper Networks wireless LAN solution is second to none.

Next Steps

To learn more about Juniper's wireless LAN solution, please contact your Juniper account representative.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

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
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

3510394-001-EN   May 2011   ♻ Printed on recycled paper