vWLAN™ Whitepaper

The Next Generation Solution for
Today's Secure Wireless Needs

Version 1.0

Corporate Headquarters
10 North Avenue
Burlington, MA 01803
USA
+1 781 328 0888
www.bluesocket.com

Table of Contents

Bluesocket's Next Generation Secure Wireless Solution

Market Evolution

Over the past several years, the availability of wireless devices and demand for wireless networking has skyrocketed. Increasingly, secure, robust wireless networking is a mission critical component of the communications needs of any organization. The growth of high bandwidth devices and applications has created the need for high performance, secure wireless service deployed over large areas such as corporate or university campuses, hospitals, municipalities and arenas. As more and more wireless applications evolve, wireless networks will need the capability to expand to meet the ever-increasing demand.

A leader in providing secure wireless solutions since 1999, Bluesocket has engineered its next generation secure wireless solution called vWLAN™ to meet this explosive growth.

vWLAN's architecture unifies the wireless and wired networks to deliver maximum efficiency by separating the data plane from the wireless network management and control plane. This is achieved through the use of smart 802.11n access points which can support traffic forwarding decisions at the edge of the network.

vWLAN offers customers the "3S" Competitive Advantage, Security, Scalability and Sustainability.

Smart 802.11n Access Points Support State-of-the-Art Security

Bluesocket's well-known security capabilities were integrated into vWLAN to provide comprehensive protection including network access control (NAC), authentication server integration, enhanced guest access, and role-based policy enforcement. These security features were optimized in the next generation architecture for enhanced performance and scalability. vWLAN's identity-based access control removes restrictions that were part of traditional WLAN solutions and provides more flexibility in managing wireless access.

Role-based policy enforcement permits a granular level of control over what each user is allowed to do on the network. Role-based privileges can be based on time, bandwidth use, type of traffic and location.

vWLAN's distributed mobility solution handles subnet roaming at the edge, while its sophisticated centralized control software works at the core to determine the optimal tunneling endpoint and to guarantee seamless mobility. The algorithm incorporates intelligent tunnel load balancing, a subnet discovery protocol, and

even a mechanism to detect and accommodate for misconfigured devices in the wired infrastructure to guarantee that wireless users can always access the network.

Bluesocket's 802.11n Access Points incorporate our award winning fairness algorithm to provide optimal voice performance in a mix mode deployment. Prioritizing traffic at the edge is just one of the key, industry-leading features to support the highly secure and efficient vWLAN design.

Delivering Massive Scalability

Bluesocket's innovative solution is architected to scale from 5 to 1500 access points on Bluesocket's current hardware platform, an increase of up to 90% over existing technology. As the number of wireless devices steadily increases, Bluesocket's vWLAN makes it easy and efficient for their customers to scale their wireless networks. Customers can simply add additional APs and licenses to expand the footprint of their network and/or the number of users/devices supported. Flexible, software-based architecture greatly simplifies expanding, reconfiguring, and managing the wireless network, resulting in significant reduction in operating cost for customers.

Sustainability Means Maximizing Efficiency

Bluesocket's vWLAN energy efficient configuration supports customer sustainability efforts by reducing carbon emissions in two ways. First, vWLAN reduces hardware requirements up to 80%, thereby eliminating the energy required to produce, ship, install, store, maintain and dispose of that hardware. Second, significantly less required hardware reduces the amount of electricity required to operate the vWLAN. Since electricity generation is one of the largest producers of CO2, the vWLAN can be a strong contributor to a company's sustainability initiatives and the reduction of a company's CO2 footprint.

vWLAN's Innovative Approach

Designed from the start with support for intelligent distributed switching at the edge, the Bluesocket solution leverages existing switching infrastructure to handle high-speed traffic and provide an optimal mix of security, control and quality of service (QoS). This approach delivers wired equivalent performance through edge forwarding thus eliminating network complexity and disruptive upgrades.

vWLAN™ is easy to add to your existing network because it does not require network redesign, additional subnets or DHCP servers. vWLAN integrates directly into your existing network and leverages your pre-configured VLANs at Layer 2 or existing Layer 3 networks. The wireless users receive the same IP address as the wired users, simplifying your network management for both wired and wireless users.

The vWLAN appliance can reside anywhere as long as the access points have network connectivity to the appliance. Since the vWLAN appliance provides control and management functionality, it is truly an out of band solution and can reside anywhere in the network.

Highly Scalable NAC solution

When designing a WLAN system for scalability and performance, it is important to evaluate every component in the system and optimize its behavior. Bluesocket designed their robust security modules to operate out-of-band or at the edge of the network in order to achieve wired-equivalent performance throughout the system.

Security Role Enforcement at the AP

vWLAN's policy enforcement permits a granular level of control over what each user is allowed to do on the network. Role-based privileges can be based on time, bandwidth use, and location.

In vWLAN, the user's policy is determined based on the user's identity. User roles are managed by the central control software but are enforced by the access point. The roles contain multiple attributes including VLAN/Subnet assignment, bandwidth and QoS, and other security related attributes. Since vWLAN is based on identity-based access control, a single SSID can be used to support multiple roles eliminating the need to manage multiple SSIDs.

Each user role can have an associated schedule, which determines when the role is active (date and time). This is particularly useful for guest users or in a facility that has specific operating hours, for instance, between 9am-5pm. .

Distributed Encryption

The access points perform Layer 2 encryption/decryption for WPA/WPA2 using specialized hardware in the radio module. This approach ensures the system scalability, especially with 802.11n data transfer rates.

Out-of-Band Endpoint Compliance

BlueProtect™ is Bluesocket's integrated endpoint client scanning solution. With BlueProtect, IT Staff can be confident that client devices connecting to the corporate wireless network are safe and will not introduce threats into the network environment.

BlueProtect traffic, including client scanning and remediation, is forwarded to the centralized appliance while the client is deemed "unclean". After completing the scan, the AP receives the updated role information and begins switching the client traffic locally.

Managed via the administration GUI of vWLAN, BlueProtect allows IT staff to monitor, control and enforce policies relating to the following:

- Anti-Virus
- Anti-Spyware
- Firewall
- Files / Registry
- Custom Rules
- Peer-to-Peer Applications
- OS/Patch Level

Distributed Wireless IDS Analysis

The BlueSecure WIDS is integrated into vWLAN and is used to identity and contain rogue APs and a host of WLAN DoS and spoofing attacks that threaten the security of your network.

The AP contains an analysis engine, which pre-processes wireless data and then sends event reports to vWLAN appliance thereby minimizing the uplink bandwidth requirement and offloads the vWLAN appliance from performing the analysis on the raw data. The APs can run in full time W-IDS mode to identify behavior based attacks or part-time mode where it can identify network events.

Convergence Results in a Simple, Higher Performance Network

vWLAN tightly integrates with the wired network to guarantee wired-equivalent performance for high bandwidth and time sensitive applications. Adding vWLAN to your existing network is a simple plug-in rather than requiring time-consuming reconfigurations.

All data traffic in the system is handled by the APs and switched directly onto the layer 2 network. If the user's role specifies a particular VLAN, their traffic is tagged appropriately.

vWLAN has a concept of "locations" which is defined as a unique subnet and VLAN id combination. Here are a few examples of locations:

Location 1:
Subnet: 192.168.100.0 mask 255.255.255.0
VLAN id: 0
Location 2:
Subnet: 192.168.100.0 mask 255.255.255.0
VLAN id: 10
Location 3:
Subnet: 192.168.160.0 mask 255.255.255.0
VLAN id: 0

The locations can be pre-configured through the management UI or automatically discovered by the AP through probing the switch port where they are connected. A location can be assigned to one or more APs.

Once clients are assigned to a role, the role places the user into a particular location. If the client is associated to an AP that supports the user's location, their traffic is switched directly onto the network. If the AP does not support the user's location (i.e. the AP doesn't have access to the VLAN), the client's traffic is tunneled to an access point that has access to the location.

vWLAN provides high-performance subnet roaming so that users can roam anywhere (keeping their original IP address) and continue passing traffic without interruption. Subnet roaming is handled by tunneling traffic between APs rather than forwarding traffic to a central controller. All user traffic from their original subnet is forwarded to the client, regardless of where they are on the network.

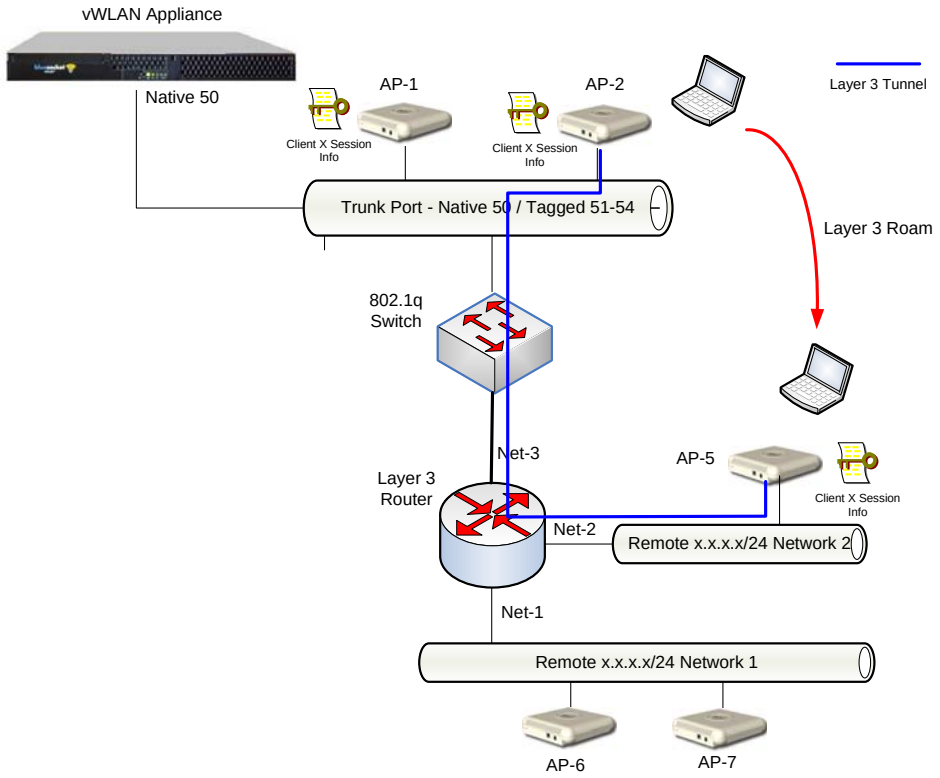
Seamlessly Roam to Anywhere

The thoughtful design and distributed nature of vWLAN made it both possible and easy to support highly versatile and complex deployment scenarios with amazingly simple configuration, planning and integration effort.

vWLAN™ enables wireless users to truly 'be anywhere' and still have access to their native VLAN or home network without requiring any complex integration or switch configuration.

vWLAN tracks user location and session information at the AP level to guarantee seamless roaming, whereever the client roams. Seamless roaming means that a client's security key material and role information is present in the roamed-to AP before the client arrives at the AP thus the client maintains their authentication state and IP address.

In this example, the client is assigned location 1 based on their assigned role (i.e. Student). Location 1 was learned by AP2 to be 192.168.51.0 on VLAN 51. When the client roams from AP-2 to AP-5, the vWLAN knows that AP-5 doesn't support location 1 and therefore must tunnel the client's traffic back to AP-2.



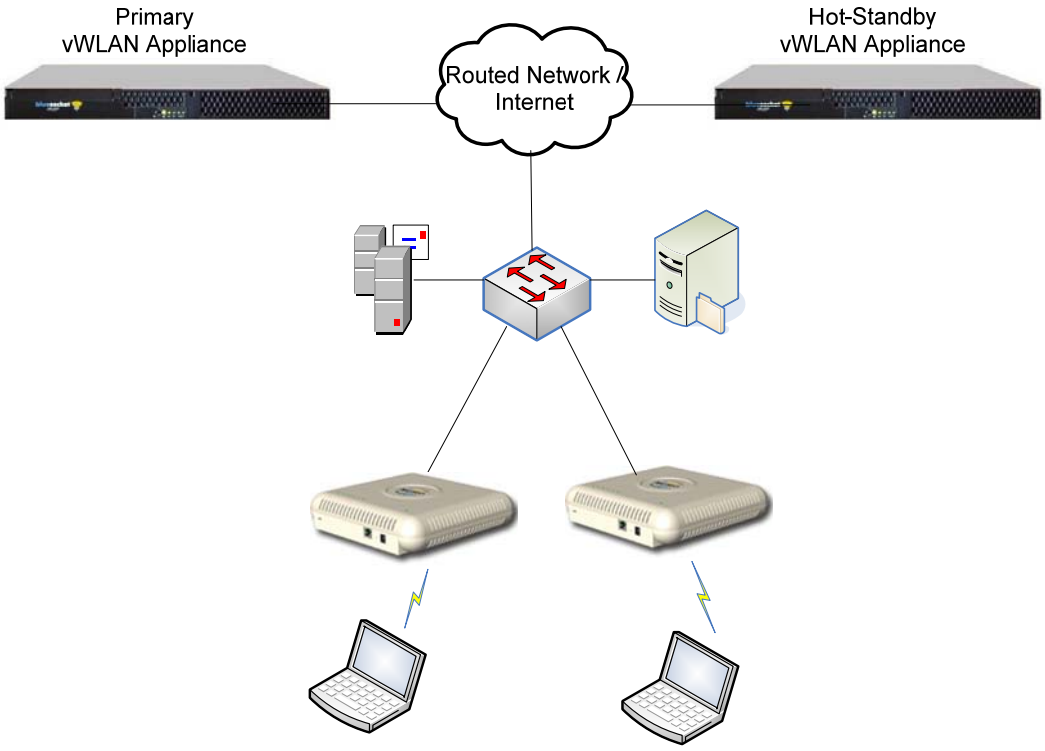
vWLAN leverages its integrated RF management functionality to detect and organize adjacent APs into groups called vNeighbor clusters. vWLAN proactively shares client information between APs in the vNeighbor cluster (roles, 802.1x

keys and session information). The innovation around vNeighbor guarantees scalability, as a client roams between APs, the vNeighbor cluster follows the client, updating newly adjacent APs and removing the session information from the non-adjacent APs.

High Availability With Less Complexity

The vWLAN high availability approach is both unique and innovative. It allows customers to have the confidence to deploy large wireless networks without the concern of a service disruption. This high availability design guarantees zero-packet loss for users in the system during a failover event.

The 1+1 high availability scheme is based on installing both a primary vWLAN appliance with a Hot-standby vWLAN appliance. Both vWLAN appliances can be deployed anywhere as long as the access points have Layer 3 connectivity to the appliances (same building, across campus or over the Internet.)



In the event the primary appliance is unreachable by the Bluesocket APs, the APs establish a connection to the Hot-standby appliance and automatically sync existing client information to provide seamless failover. The users are totally unaware a failure occurred in the system. When the primary appliance is back online, the APs transition from the hot-standby appliance to the primary appliance, againwith no packet loss from the end user's perspective.

The hot-standby appliance is licensed as a high availability appliance. The high availability system uses the same appliance and provides the same number of APs as the primary appliance. The high availability license forces the hot-standby appliance to only operate in failover mode.

The high availability scheme can also be used for seamless software upgrades to the system. Instead of scheduling a maintenance window to perform a software upgrade, the hot-standby appliance can be upgraded and then a forced failure can be performed on the primary appliance where all the APs transition to the hot-standby appliance. After the primary is upgraded, all the APs automatically return to the primary appliance – again without disruption to the user.

Distributed Quality of Service

vWLAN supports quality of service at the edge, of which there are four main components: Bandwidth Management, Packet Prioritization, Over the Air Fairness, and Packet Remarking.

Bandwidth Management

vWLAN provides granular bandwidth management at the AP including:

- Ability to limit bandwidth on a per user basis
- Ability to limit bandwidth in the downstream (to the client) direction
- Ability to limit bandwidth in the upstream (from the client) direction

WMM/ Packet Prioritization

When WMM (WiFi Multimedia) is enabled, 802.11 frames contain a prioritization based on application. It is useful to prioritize and assign wireless traffic to certain roles. The Access Point prioritizes traffic based on the input wired packet QoS tags (either 802.1p or DSCP or the greater of the two), or can prioritize to a static value.

Airtime Fairness

Bluesocket's Airtime Fairness is integrated into all of its 802.11n APs. This algorithm guarantees that bandwidth is shared among clients in a mixed environment (legacy a/b/g and 802.11n clients) providing optimal network performance.

The Airtime Fairness algorithm factors in the user's role when determining fairness. If the administrator would like to "bias" users in a particular role higher than users in another role, the algorithm uses the bias when allocating tokens for transmission. For example, an administrator could de-prioritize traffic for guests allowing corporate users more airtime to send wireless traffic.

Packet Remarking

Packet remarking is useful when the upstream network (i.e. switches/routers) are CoS aware of 802.1p or DSCP. 802.1p uses the VLAN header to apply a priority on a packet (0-7 where 7 is highest priority). DSCP uses the IP header to apply a priority on a packet (0-63, where 63 is the highest). Alternately, the administrator can choose to set a static 802.1p or DSCP mark for all traffic in the role. This is useful for Roles like IP Phones or other voice devices.

Simplification through Integration

vWLAN was designed with simplicity as a key design goal because Bluesocket believes that managing your WLAN solution should not require a lot of time. vWLAN has integrated guest access, management and reporting, as well as a host of other services.

Integrated Guest Access

Unlike traditional networking equipment that requires 3rd party products for Guest Access, vWLAN includes a fully integrated guest access solution. Guest accounts can be created by any staff member in an organization authorized to do so. Staff members could include receptionists, hotel staff, event organizers etc., all of whom could access the system and create Guest accounts – and print receipts for them. The administrator accounts reside in the vWLAN appliance and the privileges can be setup to allow the guest admin to create only guest accounts (all the other vWLAN configuration is hidden from them). A super-guest admin can then run reports based on the guest accounts that were created.

Reporting

Unlike traditional networking gear that has little persistent storage (NVRAM), and relies on remote syslog servers for report generation, vWLAN stores historical data for long-term report generation. Example reports are:

- Bandwidth Reports (per User or Role)
- User Reports (per User/MAC/IP, Role, SSID, or AP)
- Inventory Report
- Guest Access Creation and Usage Reports
- System Performance over Time Report

RF Management

Bluesocket's integrated RF management functionality ensures that your entire WLAN system is appropriately setup with a balance of channels and power. RF management reduces the effort to setup and maintain your wireless network. The system detects any non-optimal environmental conditions such as:

- General interference or noise
- Co-channel interference introduced by a neighboring AP

- Loss of connectivity to an AP
- Poor wireless client characteristics (low RSSIs, multiple failures or retries)
- High user load

and either automatically adjusts the RF parameters or provides the administrator with a list of recommended changes. RF management accounts for both 20Mhz and 40Mhz wide channels when performing its calculations.

Summary of Solution Benefits

Bluesocket's next-generation vWLAN™ architecture unifies wireless and existing wired networks to produce a truly integrated and optimized networking solution. vWLAN™ enables customers to dramatically reduce the cost of deploying and operating large-scale Wi-Fi networks while providing wired-equivalent performance to wireless users, with seamless roaming and enterprise-class security and policy management.

vWLAN™ architecture was designed around a concept of simplified scalability. In the era of wireless advancements including 802.11n, voice, and larger wireless networks, maintainability and total cost of ownership are at the forefront of new network designs. vWLAN™ removes the complexities of dealing with controller capacity by centralizing the management and control functions. Further, security and mobility are distributed at the edge of the network, the logical placement in networks that are designed for scalability and high availability. Adding additional access points to the vWLAN™ system is as easy as installing a Bluesocket software license, which extends coverage to thousands of APs without needing to worry about controller capacity.

Bluesocket's robust security architecture was integrated into vWLAN™ providing network access control (NAC), authentication server integration, enhanced guest access, and policy enforcement. These security features were optimized for performance and scalability. vWLAN™'s identify-based access control removes restrictions that were part of traditional WLAN solutions and provides more flexibility in managing wireless access.

vWLAN™'s distributed mobility solution handles subnet roaming at the edge, while its sophisticated control software works at the core to determine the optimal tunneling endpoint and guarantees seamless mobility. The algorithm incorporates intelligent tunnel load balancing, a subnet discovery protocol (SDP), and even a mechanism to detect and accommodate for misconfigurations in the wired infrastructure to guarantee that wireless users can always access the network. The APs incorporate Bluesocket's award winning fairness algorithm to provide optimal voice performance in a mix mode deployment.

WLAN systems, especially in large campus environments, are expected to provide minimal downtime as they support a significant number of users and critical applications. vWLAN™ addresses this requirement by providing a seamless, high availability solution that is transparent to the wireless users (with zero packet loss) while also providing flexible deployment options.

vWLAN™ provides a flexible solution that can operate in multiple deployments from a branch office to a large campus environment while offering low cost of ownership and optimal performance. Remote offices deployments are

demanding more from the WLAN networks and vWLAN™ responded by integrating flexibility into the security and data forwarding modules.

Finally, the integrated management module provides a rich set of visual tools for analyzing the state of the system and troubleshooting internetworking issues. The integrated management solution includes location maps, health summary, enhanced reporting, notifications, and summary of the overall RF environment.

vWLAN™ architecture is a combination of Bluesocket's core strengths in WLAN infrastructure and its vision of next-generation WLAN systems. The 802.11n market demands more than can be offered from traditional WLAN systems and Bluesocket has responded with this highly innovative solution.