aruba
a Hewlett Packard Enterprise company

TECH BRIEF

SINGLE VLAN DESIGN FOR WIRELESS LAN

INTRODUCTION

The explosion of smartphones, tablets and Internet of Things (IoT) devices is transforming the way we communicate, consume services, and manage our work. Technologies such as fast Wi-Fi and mobile UC has given the #GenMobile workforce the ability to work anytime, anywhere. To accommodate this surge of devices and mobile users, network administrators started adding more VLANs for wireless users, and VLAN pooling became a popular concept. VLAN pooling enables you to group multiple wireless controller VLANs to form a VLAN pool.

While VLAN pooling worked for a while, today's mobile demands have placed greater pressure on the Wireless LAN (WLAN) compared to a decade ago. The huge growth of consumer devices connecting to the WLAN has increased the usage of IPv6 and continuous roaming of mobile devices throughout the enterprise campus has forced network architects to re-think VLAN pooling and subnet design.

This paper proposes a new architecture — Single VLAN Design — that refers to one large flat subnet for thousands of clients connecting to the WLAN. Aruba controllers, access points, and the intelligence built into ArubaOS software allow the network to accommodate the Single VLAN design, while scaling the network to large subnets without the challenges traditionally seen with large VLANs in wireless networks. This design reduces the complexity of WLAN architecture, and addresses the challenges associated with VLAN pooling.

KEY CHALLENGES WITH VLAN POOLING

Although VLAN Pooling has been popular for enterprise WLANs, the following challenges exist:

1. Unnecssary network traffic impacts wireless performance

One of the reasons for using VLAN pooling and smaller subnets is to reduce broadcast and multicast traffic. While multiple VLANs do not create problems in wired network, they can negatively impact wireless networks. In the wireless scenario, we see multicast and broadcast traffic on one VLAN hitting clients on another VLAN, creating redundant traffic and degrading overall wireless performance.

2. Unreliable wireless networks in IPV6

When network administrators started implementing IPv6, they noticed that clients on the same access point were getting IP addresses from a different VLAN, resulting in dropped traffic. This wouldn't have occurred if all the clients on one access point were on the same VLAN.

3. Complex network design

As the number of VLANs increases, network administrators need to maintain the integrity of VLANs across multiple switches, routers and firewalls, resulting in network complexity. Also, current methods of assigning VLANs to an SSID is not efficient and can often result in the over-utilization or under-utilization of some VLANs.

4. Problems with roaming

When multiple VLANs are used in a multi-controller WLAN, network administrators need to configure either Layer 2 (VLAN Mobility) or Layer 3 (IP Mobility) roaming features. Configuring both layers increases complexity of design and causes scalability challenges for large campus environments.

SINGLE VLAN DESIGN MEETS THE DEMANDS OF TODAY'S WIRELESS ARCHITECTURE

Single VLAN design refers to one large flat subnet for thousands of clients connecting to the wireless LAN. Aruba controllers, APs, and the intelligence built into ArubaOS software allow the network to scale to large subnets, without the problems that led IT to break the network into many small VLANs.

The Single VLAN architecture uses one large subnet for all the clients connecting to an SSID. It is also possible to use separate VLANs for clients connecting to separate SSIDs. Ideally, in campus WLANs, you should use separate VLANs for employee and guest SSIDs.

The Single VLAN design uses the same VLAN throughout the campus for areas with contiguous wireless coverage. If you have multiple buildings in different locations (for example, school districts or corporate branches spread across different cities or towns), you should use different VLANs and subnets for each building to ensure seamless roaming.

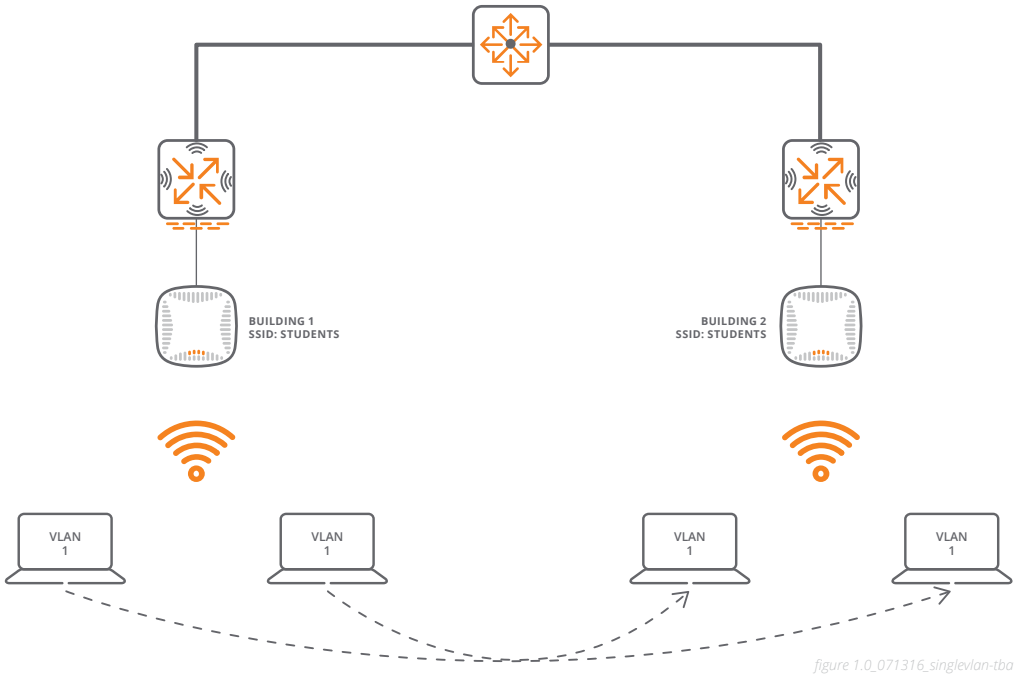

Figure 1: Single VLAN Design

Also wired and wireless clients should not be sharing the same VLAN. We recommend using separate VLANs for wired clients and, if needed, use multiple smaller subnets to restrict broadcast domain for wired devices. The Single VLAN architecture is for the wireless LAN only, as the controller has a lot of visibility and control over wireless users, but none for wired devices.

Here are two of the top reasons to use the a Single VLAN Design architecture:

1. A simple design that's easy to support

The Single VLAN Design can greatly reduce the complexity of your WLAN architecture while allowing for the wireless network to have seamless roaming and high performance.

No matter where the client roams, either on a different access point on the same controller or on a different controller, the client in this new Single VLAN Design does not need to change its IP address, resulting in a much simpler process.

Also as the WLAN design is simplifed, it is easier for network administrators to manage and troubleshoot this design.

2. Reliable network performance for IPV6

The Single VLAN results in more reliable traffic delivery via wireless because it removes the IPV6 issue of assigning the wrong address to clients.

The Single VLAN architecture enables you to meet the requirements of your wireless network with the built in intelligence in ArubaOS to filter, forward, prioritize and block inappropriate traffic. Large enterprises with multiple buildings or large universities can take the maximum advantage of this design as they have thousands of wireless clients across their campus.

To get more details on Single VLAN Design and deployment guidelines, please see the detailed white paper on Airheads community.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com