Bonjour Gateway

Table of Contents

Enterprise-level "Zero-Configuration Networking" for Apple Devices

Bring Your Own Device (BYOD) and the consumerization of IT may be overused as market terms but they are unquestionably a trend that is changing network architectures in almost every enterprise. In a recent survey by Dimensional Research of 750 front-line IT professionals, managers, and executives, 87% say that today their employees already use personal devices for work-related activities. These results are verified by more and more surveys across different verticals every day. These devices, 80% of which are identified as smart mobile devices, are simplified for ease of use and therefore enhance employee productivity. However, for the IT department, it means a shift in network intelligence and capability out of the device and puts more onus onto the network infrastructure.

Aerohive has developed the industry's most intelligent edge architecture and built it from the ground up for the shift to smart mobile devices (smart phones, tablets, and mobile laptops) as the primary access device and the consumerization of IT (corporate-owned consumer devices). Cloud-enabled networks with distributed intelligence provide inherent network-based mobile device management, corral the "iEverything" BYOD explosion, and simplify the very complex enterprise network problem of how to deal with high-speed mobile smart devices.

There are many challenges with the BYOD trend but one of the key attributes that makes a network purpose-built for mobility and operationally simple for BYOD and the consumerization of IT is the ability to create "Zero-Configuration Networking" available to large organizations and enterprises so that consumer devices work on the enterprise network with no end user expertise. In order to fully realize this concept the network infrastructure must become "service-aware" and simply provide service availability seamlessly across the network and control access to those services based on a users' context – identity, location, application, and device in use. In a service-aware network, an authorized user should instantly see services available to them such as printers, video projection, and collaboration applications, without configuring their smart mobile device. This is the ultimate achievement in the attempt to make BYOD not just manageable as an IT initiative, but desirable as it makes the BYOD user both less expensive from a capital expenditure (as the employee has purchased the device) and from an operational expense as policy and service availability is set by user context and automatically connected to the end device.

Aerohive has a history of defining the future of networking and is once again paving the way with the introduction of the first service aware infrastructure technology. 72% of the devices brought into the enterprise by users are Apple devices, according to Dynamic Research, and as such Aerohive has introduced native Bonjour awareness and control into our Cooperative Control architecture to support Apple's "Zero-Configuration Networking" for products in the enterprise and larger educational institutions.
To make networks service-aware and make BYOD with Apple devices a native part of every network, Aerohive has built a Bonjour Gateway to manage and control Apple service availability (such as AirPrint™, AirPlay®, file sharing, collaboration applications, etc.) across an entire enterprise network. This patent-pending functionality is a native part of Aerohive's HiveOS network operating system and as such even non-Aerohive legacy networks can manage their services by attaching a single Aerohive device, via a trunk port, to the network – the gateway functionality works out-of-band. Managing Apple services across an enterprise network is now extraordinarily simple: If a service,

such as a printer, announces itself, Aerohive can ensure that the printer advertisement is made available across the entire network or, if necessary, make sure it's available only to the networks allowed to view the service (i.e. control the service advertisements).

Bonjour Gateway in an Aerohive network

Bonjour Gateway in a legacy non-Aerohive network
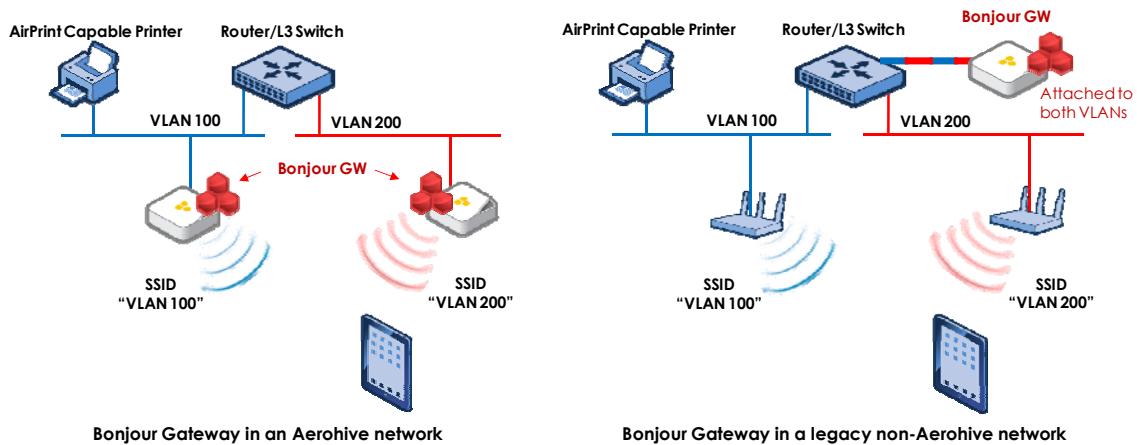
Bonjour Gateway and Apple's Bonjour Protocol

Bonjour underlies many services that are widely used on Apple-centric networks. By monitoring Bonjour advertisements, clients can learn the location (IP address and port) of any service, and then connect to it as with any other service. Bonjour transforms the manual process of configuring IP addresses and port numbers into a "plug-and-play" experience where users reference services by type and a human-readable name. Two notable examples are AirPrint and AirPlay. Both advertise themselves through Bonjour to enable clients to print and display screens, respectively. AirPlay is especially valuable in many contexts for remote display from iOS devices, and the recent announcement that AirPlay will be available in the next version of Mac OS® (code-named Mountain Lion) only makes it more compelling.

The capabilities that Bonjour enables are very attractive to enterprises and educational institutions for their ease of use and ability to help make BYOD initiatives more productive (where IT doesn't have to install all the services on every device – even the ones it doesn't own). The problem comes in when one tries to scale Bonjour from home applications to broad, multi-vendor, multi-segment networks. Because Bonjour relies on an underlying multicast DNS advertisement, it is restricted to the scope that that advertisement travels across the network. As an example, on a network that lacks the Aerohive Bonjour Gateway, AirPlay will only function when both the Apple TV and the display source are both attached to the same broadcast link. Client devices cannot use AirPlay unless they are attached to the same VLAN as the Apple TV. In many enterprise and education networks, this restriction is unattractive.

One of the key building blocks that Bonjour is built on is multicast DNS. Services send advertisements to a link-local IP address, and clients build a list of available services by listening to those advertisements. On networks that consist of a single broadcast domain, the use of link-local IP addressing is acceptable. Once a network is built with segmented broadcast domains for scalability, however, multicast DNS advertisements no longer reach all devices on the network. While many services will be local to the immediate network link, not all will be.

Copyright ©2012, Aerohive Networks, Inc.

As an example, consider the network in Figure 1. VLAN 100 on the left side of the provides multiple services. A printer advertises AirPrint capabilities through Bonjour, the Apple TV advertises AirPlay service, and the server provides file sharing. When the tablet is attached to the VLAN 100 Network SSID on the left-hand AP, it is able to use any services on that network. If it moves across the router by attaching to the VLAN 200 Network SSID, it will no longer receive multicast DNS advertisements for any of those services.
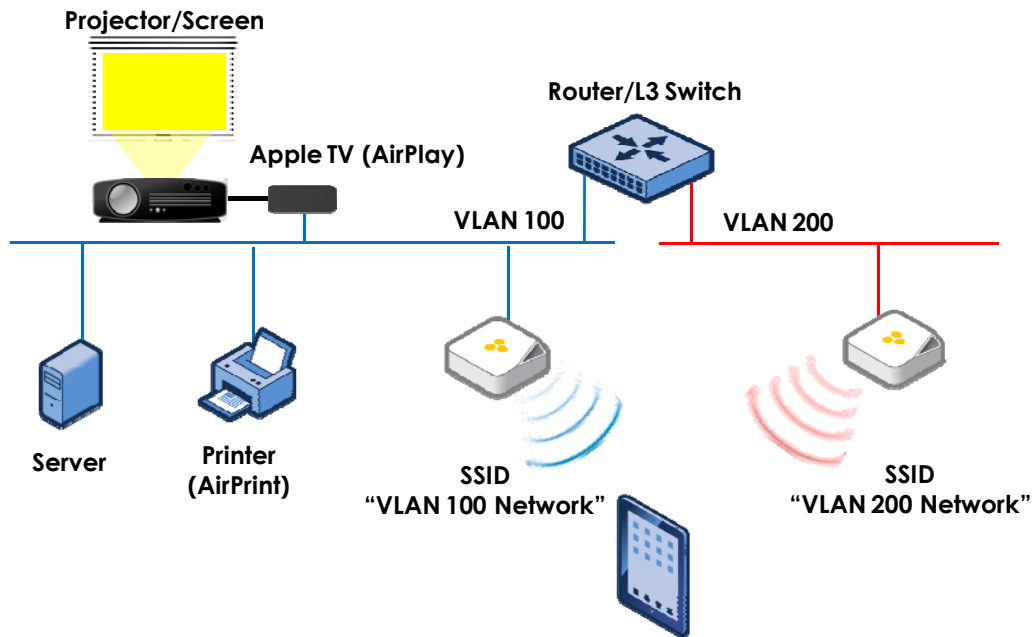
Projector/Screen

Router/L3 Switch

Apple TV (AirPlay)

VLAN 100   **VLAN 200**

Server   **Printer (AirPrint)**

SSID "VLAN 100 Network"

SSID "VLAN 200 Network"

Figure 1: Example Multi-Subnet Network

Ensure Students are Connected – to the Right Content

When Aerohive first considered how to solve this problem, the first approach was a narrow solution to bring all devices together on to the same broadcast domain. Through Aerohive's layer-3 tunneling capabilities and private pre-shared key features, it would be possible to configure all Apple TVs throughout the network to attach to the same VLAN regardless of the underlying topology. However, most devices will need to use several services, so it is not generally possible to set up a VLAN for each service. If, for example, iPads® need to both print and use AirPlay, then all Apple TVs and all printers must be on the same VLAN. Taken to its extreme, the network becomes a single VLAN with all available services. Such a network concentrates all traffic through a set of "choke points" that lack scalability, redundancy, and sap the network of efficiency.

A second approach considered was to forward all multicast advertisements across router boundaries. Doing so would undoubtedly make services widely available, but forwarding link-local multicasts is explicitly forbidden by the router requirements RFC. Furthermore, many access network devices are constructed so that the core switch fabric forwards unicast packets, while multicast packets are either flooded to all ports or handled by the CPU outside of the switch fabric. Simply forwarding all multicast advertisements would cause an unacceptable load on the access network, both in

terms of processing power on the access layer as well as on network capacity. Forwarding all multicast advertisement frames results in every service on the network being advertised on every VLAN. On a large network, not every service should be advertised network-wide. A corallary to this problem is that of advertising services from devices (printers, Apple TVs, file services, etc.) that are spread all across the enterprise or campus and span multiple VLANs. If this multicast methodology were used then there would be a "multicast direction" issue, in other words, you wouldn't want VLAN1 services to be sent out to all other VLANs and then VLAN2 sending the multicast back across the router boundary advertising its services in return as these "blind" multicast forward mechanisms run the danger of causing a loop and harming network and service performance.

How it All Comes Together

In designing the Bonjour Gateway technology, Aerohive combined the ease of use of multicast forwarding with awareness of the underlying advertisement protocols. In Figure 1, the access point on VLAN 100 receives advertisements from the printer, Apple TV, and server. Information on available services is then selectively relayed to the access point on VLAN 200. Services that are shared between the two networks are then re-advertised on VLAN 200, and can be detected by attached devices. If permitted by security policies installed and enforced between the two VLANs, any devices attached to the right-hand SSID are able to find, configure, and use any services learned from VLAN 100.

Figure 2: AirPlay in Use

When the gateway is activated, it enables the sharing of link-local service advertisements across the router boundary. Figure 3 shows an Apple iPad displaying the AirPlay service advertisement from an IP address on VLAN 100 (192.168.1.0/24) even though the iPad itself is attached to VLAN 200 (192.168.200.0/24).
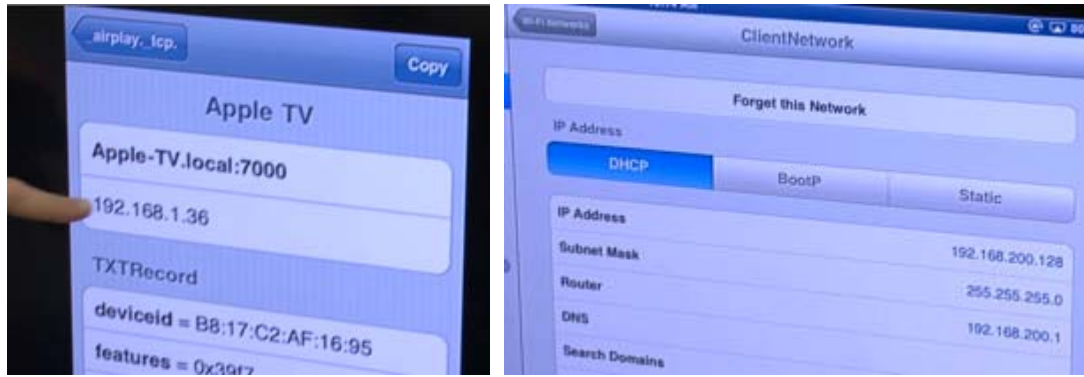
Copyright ©2012, Aerohive Networks, Inc.

Figure 3: AirPlay Advertisement Crossing Subnet Boundary

Many networks support a large number of services, and on networks with significant numbers of Apple devices, it may be undesirable to share all services across all networks. Depending on the applications supported by the network, it is likely that only a few services must be supported network-wide. For example, it might be desirable to make printers available across a network regardless of the underlying topology. If Apple TVs are used in many conference rooms or classrooms simultaneously, it may be desirable to share only Apple TV services.

To prevent network overload, the Bonjour Gateway supports service filtering. Figure 4 shows the service list available on an iPad. In the left screen shot, the screen mirroring shows a long list of services advertised from computer on VLAN 100 in the network diagram. In the right screen shot, the iPad has moved to VLAN 200. However, the Bonjour Gateway has been configured to allow only AirPlay to pass across the router.
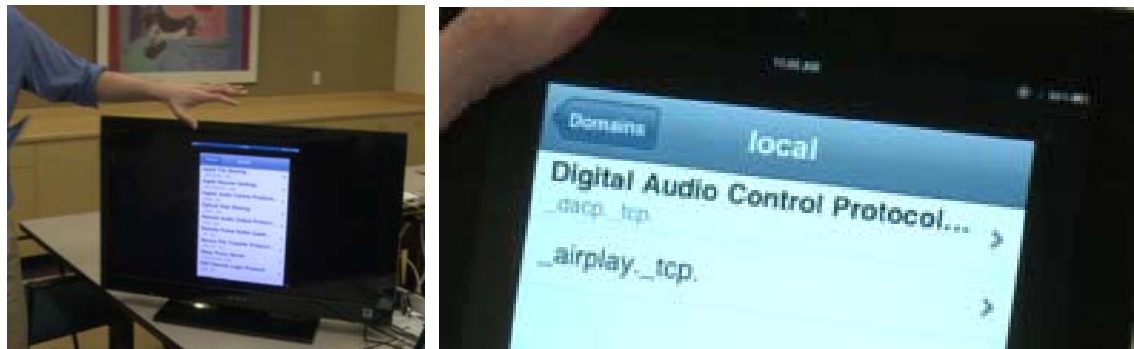

Figure 4: Filtering in Action

Summary

Aerohive's patent-pending Bonjour Gateway capability takes service advertisements that are restricted to a single broadcast link and makes those services available network-wide, without any client modifications or networking gymnasitics.

Aerohive Bonjour Gateway Benefits
- Multi-Vendor - Works in both Aerohive and Non-Aerohive networks
- Plug and Play - No requirement for VLAN and Multicast gymnastics
- Flexible - Supports bi-directional service advertisements, without fear of multicast loops and flooding
- Efficient – Gateway functionality enables - granular control, ability to respond to service queries and limits communication to changes in service availability
- Secure and Scalable – Preserves enterprise security policy and data forwarding methodology

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

SB1202403