

WIRELESS NET Design Line

DECEMBER 5, 2005

How AWPP will make mesh networks easier to deploy

AWPP dynamically discovers neighboring radios and establishes an optimal path through a mesh of wireless nodes to a wired gateway.

By Neal Castagnoli, Cisco Systems

Wireless routing is a key technology enabling the deployment of large wireless mesh networks that expand broadband wireless connectivity from hot "spots" to hot "zones."

A new protocol for wireless mesh networks, called the Adaptive Wireless Path Protocol (AWPP), is expected to play a central role in the building of reliable wireless mesh networks, making them easy to manage and deploy.

AWPP establishes an optimal path through a mesh of wireless nodes to a wired gateway, creating a self-configuring, self-healing wireless mesh backhaul. AWPP addresses the challenges of routing packets over wireless links, which have very complex packet loss characteristics compared to wired networks. AWPP comes out of Cisco's long experience and leadership in routing protocols as well as indoor and outdoor wireless networks.

AWPP basics

Taking high-speed wireless broadband networks outdoors inherently leads to picocell architectures with high base-station densities up to 30 nodes per square mile. Such a high density of base stations makes running a wire to each one cost-prohibitive. Ideally, one would like to simply hang access points (APs) and have them link with each other and with the wired network quickly, reliably and inexpensively. Until now, wireless backhaul has required intensive RF design and management.

AWPP replaces the work done by RF engineers with a protocol that dynamically discovers neighboring radios and calculates the quality of all possible paths to the wired network. These calculations are continuously updated, allowing network connectivity and paths to change as the traffic patterns on wireless links change. The ability of AWPP to quickly adapt to changing links eliminates any single point of failure and dramatically boosts the network's reliability. Its compelling characteristics include fault tolerance, reliability, scalability

and adaptability to a wide range of wireless environments.

No need for RF engineering

AWPP configures the mesh nodes by selecting the APs that represent the best paths to the wired network. AWPP path selection optimizes link quality, while minimizing shared bandwidth usage. This eliminates the need to engineer each link in the RF network.

AWPP reduces the number of hops taken by packets in transit in the mesh, while ensuring the same success rate for the individual packets. Fewer hops mean higher performance from an AP to the wired backhaul. Furthermore, the use of the shared channel is minimized, which improves the overall capacity of AWPP networks.

The benefits of this self-configuring, wireless mesh solution are substantial.

Extensive RF engineering and analysis can be replaced by more efficient statistical analysis for AP placement. As AWPP constantly monitors the network, mesh nodes that fail are quickly bypassed through a list of alternative paths always maintained by AWPP. As coverage requirements change, the mesh adapts and forms a new topology optimized for the particular placement of APs and the RF characteristics of the aggregate wireless mesh.

Management has been another problem for wireless networks located outdoors. The Cisco Unified Wireless Network architecture unifies indoor and outdoor Wi-Fi solutions, enabling system administrators to manage both networks the same way. As a result, all wireless APs and clients can be authenticated and assigned access permissions from a centralized controller.

Another vital element of the Cisco's wireless mesh solution is a dual-channel AP with one radio for access and another for backhaul links. The backhaul radio operates in the 5.8GHz

radio band (802.11a protocol), while the access radio operates in the 2.4 GHz radio band (802.11b protocol). As backhaul and access traffic do not compete, this configuration has smaller path-loss coefficients and signal strength remains stronger longer, delivering clearer, more direct signals to clients. In fact, the entire network is more stable than single-channel solutions.

AWPP in the field

1. A Public School Systems

Public schools have been eager consumers of wireless technology as they seek ways to extend their wired networks cost-effectively and enhance security on their campuses. Such is the case for this large school district in Florida. Like many in that state, it is growing quickly, and its campuses are housing students in temporary classrooms that are not wired to the network in the main school buildings. As a result, the district has many islands of networking, LANs that are disconnected from the enterprise and from one another.

To address this problem, the district deployed a wireless mesh network based upon AWPP and Cisco's dual-channel APs. By establishing an optimal path to the root, the solution reduces hops, preserves bandwidth and lowers the error rate. With reliable, real-time links, the district's schools have been able to easily connect their computers and peripherals from their temporary classrooms to the main wired network.

2. Universities

College campuses are another hot area for the spread of Wi-Fi technology. Cisco wireless solutions are now commonplace in college and university settings.

Typically, these institutions have deployed wireless to extend their wired LANs, both indoors and outdoors. One university is now testing the Cisco Wireless Mesh Network solution to enhance the performance of its wireless network and lower its operating costs. This system is allowing students, faculty, and staff to connect from anywhere on campus, achieving seamless indoor-outdoor connectivity.

In addition, the university plans to use its wireless solution for an unusual application – extending the mesh to indoor locations. At this school, some indoor places on campus, like the coffee shop, are not linked to the enterprise. The wireless mesh is an easy, cost-effective, and reliable way to extend the wired LAN into interior locations without cabling.

3. Municipalities

More and more municipalities are installing Wi-Fi in public areas where large numbers of people gather, often in downtown locations. The goal is to enhance city and town centers as places to meet, work and play, thereby solidifying the relationship between citizens and their communities.

Currently, several cities are running beta tests of the Cisco Wireless Mesh Network solution to provide hot spots. The technology, is allowing them to extend their range of wireless connectivity both geographically and in terms of users.

Some governments have more ambitious plans. Many regions, especially those outside major metropolitan areas, do not have access to DSL service. Therefore, localities in these areas, working in conjunction with service providers, hope to use wireless mesh technology to extend high-quality, high-speed Internet access to their citizens. For them, wireless mesh networking can deliver a vital, much-needed service and do so affordably. Wireless mesh networking is not limited to these applications and environments: in fact, many sectors can benefit from the spread of this technology. In addition to educational institutions and municipalities, the technology well-suited for public safety groups, healthcare organizations, and corporate campuses, to name just a few sectors. Wireless mesh networking is likely to spread rapidly almost anywhere that mobility can enhance the quality of work, learning and community.

Wireless Evolution

The Cisco Wireless Mesh Network solution employs a unique approach in which AWPP eliminates the need for higher-level protocol configurations. Its dual-radio design further enhances the performance and reliability of the wireless mesh. Together, these innovations create a single, integrated mesh network infrastructure that supports multiple user groups with an easy-to-deploy, self-healing, self-organizing and dynamic route architecture.

The Cisco Wireless Mesh Network solution will speed the transition to a mesh infrastructure from current wireless networks, which can be difficult to deploy, manage and integrate. This evolution will deliver tremendous new capabilities and possibilities for wireless systems everywhere.

Architecture to centralize control

Taking WLANs outdoors creates several challenges that must be met to ensure widespread adoption, including easy network deployment and management, real-time RF management and advanced security.

To help meet these challenges, an architecture has emerged in the outdoor WLAN mesh space that centralizes intelligence and control to help service providers, businesses and/or municipalities easily manage and operate outdoor mesh wireless networks with minimal operational costs.

In this new architecture, a WLAN controller system is used to create and enforce policies across many different lightweight access points. By centralizing intelligence within these devices, security, mobility, quality of service (QoS), and other functions essential to outdoor WLAN operations can be efficiently managed across an entire wireless enterprise.

Furthermore, by splitting functions between the access point and the controller, service providers can accelerate time-to-market, simplify management, improve performance, and increase security of large outdoor wireless networks.

Limits of traditional architectures

Traditional WLAN solutions distribute all traffic handling, RF control, security, and mobility functions to the access point

itself. However, this architecture limits visibility of 802.11 traffic to an individual access point only. This means:

- Individual access points, when used without a management device, must be managed individually, which can increase operations costs and staffing requirements
- Network-wide attacks and interference are not visible across a system, which means: (1) Single point of enforcement for security policies across Layer 1, Layer 2, and Layer 3 and (2) Inability to detect and mitigate denial of service (DoS) attacks across an entire WLAN
- A system cannot correlate or predict activity across an enterprise, which means (1) Limits the ability to enable optimized, real-time load balancing and (2) Clients cannot perform fast handoffs, which are required to support real-time services such as voice and video

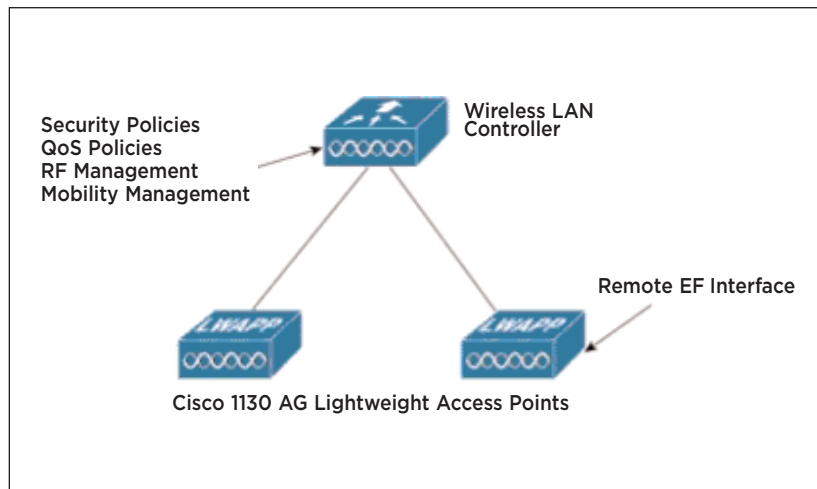
As more products emerge that use lightweight access points with centralized WLAN intelligence, there is a need for an industry standard that governs how these devices communicate with one another. The Lightweight Access Point Protocol (LWAPP) has been recommended by an IETF working group to address this issue. LWAPP standardizes the communications protocol between access points and WLAN systems (controllers, switches, routers, etc.). The goal of this initiative, as described in the IETF specification, is to:

- Reduce the amount of processing within an access point, enabling the limited computing resources within these devices to focus on wireless access, as opposed to filtering and policy enforcement
 - Enable a scheme whereby traffic handling, authentication, encryption, and policy enforcement (QoS, security, etc) can be centralized for an entire WLAN system
 - Provide a generic encapsulation and transport mechanism for multi-vendor access point interoperability, either by means of a Layer 2 infrastructure or an IP routed network
- The LWAPP specification works to address these issues by defining the following types of activities:
- Access point device discovery, information exchange, and configuration
 - Access point certification and software control
 - Packet encapsulation, fragmentation, and formatting
 - Communications control and management between access point and wireless system device

Putting LWAPP to work

When LWAPP was first introduced to the WLAN industry in 2002, it revolutionized the way WLAN deployments were managed with the concept of a "split MAC" the ability to separate the real-time aspects of the 802.11 protocol from most of its management aspects (Figure 1).

In particular, real-time frame exchange and certain real-time portions of MAC management are accomplished within



1. Cisco 1500 mesh access points

the access point, while authentication, security management, and mobility are handled by WLAN controllers.

Combining LWAPP with intelligent RF management capabilities brings numerous benefits to customers deploying outdoor WLAN mesh networks.

Management

- Dynamic, system-wide RF management, including a host of features for smooth wireless operations, such as dynamic channel assignment, transmit power control, and load balancing. For outdoor environments where RF interference issues can be significant, this is a crucial capability.
- Single graphical interface for network-wide policies, including VLANs, security, and QoS.

Security

- Network-wide security policies that encompass all layers of a wireless network, from the radio layer through the MAC layer, and into the network layer. This makes it easier to provide uniformly enforced security and QoS or user policies that can address the particular capabilities of different classes of devices, such as handheld scanners, PDAs, or notebook computers.
- Discovery and mitigation of DoS attacks, and detection and denial of rogue access points. These functions occur across an entire LWAPP-based WLAN mesh network.

Mobility

- Cellular-like fast handoffs.
- Excellent support for real-time, mobile applications such as voice over WLAN.

LWAPP is rapidly becoming an essential building block for outdoor mesh wireless networks. It is a foundation upon which large-scale, heterogeneous WLANs can be constructed. By providing a standardized approach for RF internetworking, LWAPP simplifies RF management, and optimizes wireless networking for small, medium-sized, and large-scale outdoor WLAN deployments.