WHITE PAPER

DISTRIBUTED INTELLIGENCE: THE FUTURE OF WIRELESS NETWORKING ARCHITECTURE

MOTOROLA

EXECUTIVE SUMMARY

The era of hyper connectivity is upon us. There is tremendous growth in the number of devices including Smartphones and tablets that are capable of attaching to WiFi and wireless broadband networks. There is not only an exponential growth in the number of wirelessly connected users but the amount of bandwidth being consumed on enterprise networks is also increasing exponentially driven by video and other enterprise applications. Secondly for a distributed enterprise, the network infrastructure needs to support a high degree of scalability, performance and reliability supported by centralized monitoring and network assurance tools. IT administrators need to have the right wireless networking architecture to deal with these challenges in the most cost effective manner. This paper looks at available enterprise wireless architectures and makes the case for one that is based on distributed intelligence.

NETWORKING CHALLENGES IN ENTERPRISES

Although each networking environment is unique, the most common network challenges in an enterprise environment revolve around scalability, reliability and manageability.

SCALABILITY

There is a rapid growth in the number of wireless devices that are attaching to corporate networks and the type of bandwidth and latency sensitive applications being accessed. This requires the network to easily scale to accommodate the growth in a cost effective manner.

RELIABILITY

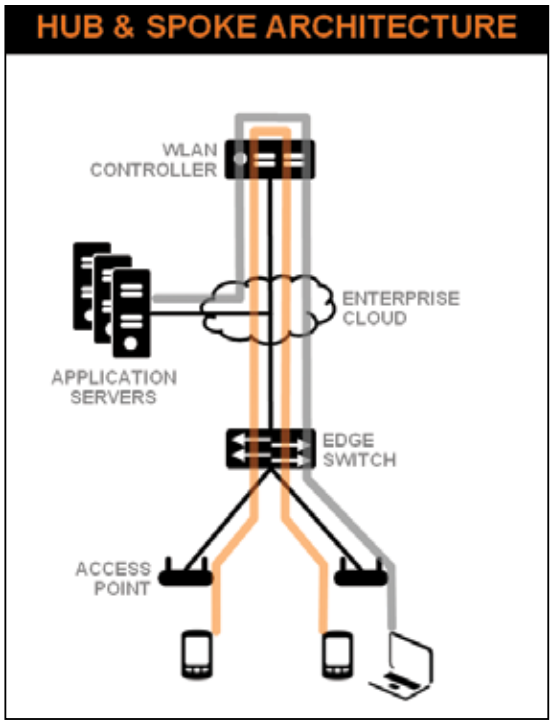
Enterprise users need access to corporate networks and applications at the point of activity whether it is in the corporate HQ or in remote locations. The remote network has to be highly reliable and provide several levels of redundancies and failover mechanisms to provide continuous network service in case of outages. In addition. RF networks must deliver reliable and predictable wireless coverage for the users they support.

MANAGEMENT OF DISTRIBUTED NETWORKS

Enterprises also need networks that can easily accommodate a distributed environment, such as headquarters, branch offices and multi-building campuses. Too often, each entity implements its own network, requiring additional personnel to administer regional pieces of that network, and complicating network management. In such fragmented environments, daily administrative tasks such as upgrading firmware, detecting unauthorized network access and applying network policies happen regionally, with little or no central visibility.

HUB AND SPOKE ARCHITECTURE

Traditional deployments with controllers are based on a "hub and spoke" architecture. In this architecture, less expensive "thin" Access Points (APs) forward all traffic to the controller which acts as the central point of management and where all the network and security policies are defined and enforced. This worked well especially with older 802.11 technologies and in vertical markets like retail that did not have high bandwidth applications.



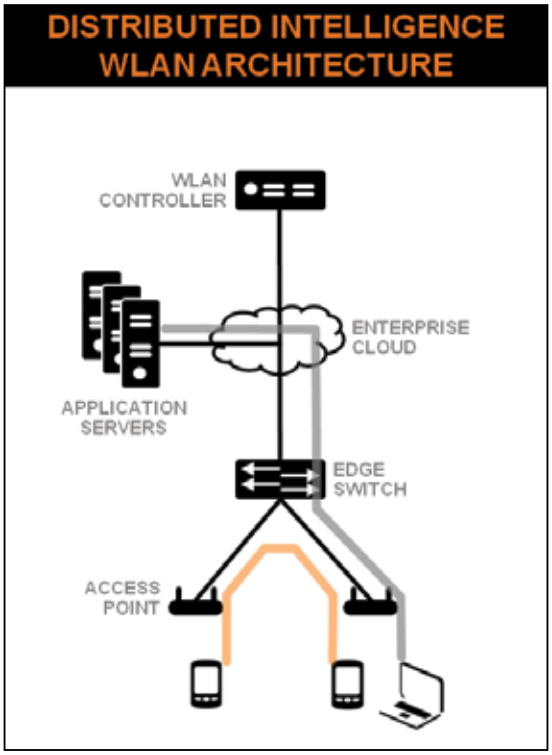
This architecture is now showing its age driven by two primary factors. The first is the increased use of media rich, real time and bandwidth intensive applications like video in the enterprise. The second is the evolution of 802.11n which integrates a number of technologies to significantly increase data throughput. It is easy to see how high throughputs associated with 802.11n create a bottleneck in the network as all traffic must be forwarded to the controller with centralized intelligence. This architecture implies that in order to handle increased bandwidth, a significant increase in controller processing power is needed – thereby increasing costs. Forwarding all traffic to the controller also negatively impacts the performance of real time applications such as video.

Another drawback of the hub and spoke architecture is its ability to handle the failure of the wireless controller or the wired network connection. Site survivability is critical as organizations become more distributed.

CIOs looking to help their organizations stay competitive are finding that direct routing hub-and-spoke solutions with centralized intelligence have many drawbacks. A better alternative consists of a wireless LAN (WLAN) architecture capable of supporting greater intelligence at the network's edge to optimize traffic flow without compromising security or quality of service, while keeping solution costs low.

DISTRIBUTED INTELLIGENCE ARCHITECTURE

An evolution of the wireless architecture is necessary to meet the demands of increased bandwidth consumption, better reliability to deliver applications such as video, increasingly handle distributed deployments while minimizing network bottlenecks. Such an architecture should maximize network performance and traffic without compromising Quality of Service (QoS) for video and voice applications, security, mobility or survivability while at the same time minimizing both capital and operational expenditures for a lower total cost of ownership (TCO).



With this architecture the system becomes highly scalable - a single controller can supervise up to 8 times the number of access points compared to the traditional hub-and-spoke model. This frees up controllers to focus more on large scale network and policy management as well as other services, resulting in a more efficient architecture.

Distributed intelligence allows optimized routing of data internally on the network or to the Internet without having the APs forward traffic to the controller - thereby avoiding one of the key bottlenecks. Moving the controller intelligence or smarts down to the APs allows critical decisions to be made locally and for the network to be more responsive to the dynamic nature of RF environment.

While 802.11n integrates many technology enhancements to deliver superior performance compared to previous generation of 802.11 networks, enterprises need to turn their attention to deployment architectures that best meet the needs of scalability, reliability, application performance, security and overall cost of ownership. Solution architectures vary greatly in terms of these key metrics and careful attention needs to be paid to how flexible and scalable the architecture is.

Some of the key questions that need to be asked while deploying large scale and distributed 802.11n solution include:

- How easy is it to deploy the system?
- How is the system going to scale and how easy is it to add capacity?
- Will security, QoS and network routing policies be impacted if the remote APs lose connectivity to controllers?
- How many controllers are required to support the network of APs? And does every remote site need to have a controller?
- How are latency sensitive applications handled?
- How does the system react to dynamic RF changes?

The network can be much easier to deploy and be able to deliver a better quality of experience when the foundational architecture distributes intelligence among the APs. The ease of deployment in complex network environments is manifested when the APs are VLAN-aware, in which case it would not require any re-engineering of the network's VLANs in order to add APs. By having more intelligence in the APs, the network can deliver higher performance, support low latency roaming and handle latency sensitive applications such as voice and video in the most reliable manner.

One of the key benefits of this architecture is site survivability – the ability of APs to continue to function even when it loses communication to the controller. These APs would continue to bridge traffic while still enforcing QoS and security policies – including statefully inspecting Layer2 (locally bridged) or Layer 3 traffic.

Another important effect of this distributed intelligence architecture is that it allows a number of APs to be deployed in remote locations **without the need for a local controller**. The APs in remote sites would coordinate with each other to provide optimized routing and self healing functionality and deliver a superior quality of experience for business critical applications. The number of APs that can be deployed in a single location without a controller will be dependent on the capabilities of the APs but a significant number of branch offices need less than a couple of dozen APs. This means that in most branch offices there is no need for additional controller elements.

In effect, greater intelligence at the edge of the network makes the IT budgets go farther, offering advantages in both capital and operational expenditures. Adding 802.11n access points to the network would be less expensive than adding more wireless controllers, and can result in significant savings.

Another key architecture consideration for enterprises is security policy enforcement and network assurance. Here, APs that are designed to provide simultaneous client access and full time sensors for security and troubleshooting eliminate extra installation and power costs. Networks with distributed intelligence enable real-time troubleshooting and spectral analysis for greater RF visibility and reduced maintenance costs.

The best distributed intelligence solutions will even factor in power consumption as a cost-saving feature, optimizing the power draw of APs to fall below 13W in most cases thereby allowing enterprises to leverage lower cost standard Power over Ethernet (POE) infrastructure instead of having to upgrade to newer systems.

The overall solution architecture has to offer real time network visibility and proactive tools to minimize outages. Without the right network assurance tools, the ongoing operational expenses can easily outpace the initial capital overlay within a few years.

CONCLUSION

The future wireless network architecture relies on distributed intelligence to meet the performance demands of the new wireless world without compromising security or quality of service while at the same time providing flexibility and simplicity of deployment. The centralized hub-and-spoke architecture helped bring more cost effective 802.11b/g solutions to organizations. But with increased network traffic creating bottlenecks at the controller and an unreliable user experience, the industry clearly needs to move toward a more distributed model. Only an architecture that provides fully distributed intelligence at the network edge can provide the full benefits of what 802.11n has to offer for the distributed enterprise.

ABOUT MOTOROLA

Motorola offers true end-to-end mobility solutions for field service and more that include: a comprehensive portfolio of mobile devices with extensive wireless communications capabilities; affiliations with the leading wireless public network providers; a portfolio of private wide area and local area network infrastructure; a partner channel delivering best-in-class applications; and a complete range of pre- and post-deployment services to help you get and keep your mobility solutions up and running at peak performance. And when you choose Motorola, you choose the strength only an industry leader can offer, with proven technology in successful customer deployments in many industries around the world.

To find out how Motorola can streamline your field service operations, please visit us on the web at www.motorola.com/cross-industry-solutions/fieldservice-solution or call us at 1-866-416-8593.