WhitePaper

Wireless LAN Virtualization: Twice the Network at Half the Cost

The Drive towards the All Wireless Enterprise

Creating networks that can run business-critical applications is one of the core focuses of the enterprise IT department. This has traditionally meant wired Ethernet, with wireless often seen as an afterthought for convenience rather than the network of choice. But as aging wired infrastructure approaches its next expensive refresh cycle and users demand mobility IT departments are looking for an alternative. In uncertain economic times, a networking technology that radically cuts per-port costs and eliminates most cabling would seem to be ideal.

Wireless LANs provide that answer. With the introduction of 802.11n, WLAN radio data rates of 300Mbps and peak throughput not too far behind have propelled the speed of wireless networks past wired Ethernet. With the increase in bandwidth comes the prospect of eliminating the vast majority of wireline switch ports. Wireless radios can blast networking connectivity through walls and cover an increasingly mobile workforce, saving the enterprise money in the short term and unlocking the potential for productivity gains in the long term. Collaboration increases as employees lose their tethers to their desks and start to move to where the work is actually being done.

The incremental cost of adding a wireless LAN has come down dramatically. Nearly every laptop sold to businesses today comes with a Wi-Fi radio. Unplugging users from their desks and adding enough access points to cover a campus is often an easier and more affordable path than suffering through another wired Ethernet forklift upgrade.

Challenges to this Vision

The vision of an all-wireless enterprise assumes that wireless is as predictable in cost, performance, and management capabilities as the wires it replaces. But for most WLAN offerings available to the enterprise today, it is nowhere close.

Costs are Unpredictable

Though building a wired network is expensive, at least its costs are known and easy to determine. Nearly every IT organization has experience in laying out wireline Ethernet. And once a network is installed, management tools are well understood. Diagnosing network problems is a matter of following a well-rehearsed program: track down the source of the outage, isolate the problem device and then replace it.

The costs for WLAN networks are much less well understood. Choosing the location for access points is not based solely on convenience, but rather on how well invisible radio waves travel through buildings made of material that only the builder might know about.

Because wireless LANs use open, public radio bands, the network is unpredictable. Conditions change from minute to minute, making it difficult to plan the coverage area of each access point accurately. Fault diagnosis is a mystery. Did the laptop disconnect yesterday at 4 pm because the user accidentally switched to the wrong network, or did the network itself change its coverage pattern, putting the user in a dead zone? And once a suspect client device is found, how can the administrator isolate it if it is

connected to the same wireless radio as dozens of perfectly healthy clients? One change to help the problem client will hurt the functioning ones.

Both initial deployment costs and operating expenses soar, eating into the money saved by moving to a wireless network in the first place. Furthermore, the poor reliability may force users back to wires.

The Growth Path is Uncertain

For wired networks, the growth path is clear. To increase capacity, add more ports. The costs of growth are understood. IT organizations can make intelligent choices on how much network to buy now, and how much they'll need to buy as the company grows.

But with WLANs based on "micro-cell" architecture, adding an access point doesn't necessarily increase capacity. It may even do the opposite, as nearby access points need to shrink their coverage areas to prevent interference with the new one. More money might provide less networking, not more. And what do you do once the limit has been reached?

Wireless networking needs to be more like wired networking. With "micro-cell" based WLANs, it is closer to the state of wired networking 15 years ago when Ethernet was based on hubs: unpredictable performance, unknown costs and all users contending for access to the same limited resource.

The Need for Virtualization

"Micro-cell" WLAN technologies require purchasing more access points than needed, provisioning for the rainy day. They require complex radio management tools which can seem like black magic, requiring administrators to understand the intricacies of RF signals and wave diffraction just to get the network functioning. They are inflexible, often requiring multiple parallel networks to support different applications (such as voice and data) in the same building. Worst of all, they are unpredictable, responding to everyday events by changing dramatically. A single spot of localized interference can cause a cascade of changes across the network as access points retune to avoid it.

When resources are shared and the side-effects of the sharing quickly become a problem, the solution is virtualization. Virtualization steps in between the physical resource and the user of the resource, protecting users from the complexities underneath. The ill effects of the discrete, physical nature of the resource are removed, setting both administrators and users free from worries about finding and allocating capacity.

Virtualization reduces costs by removing waste through economies of scale, then introducing predictability and determinism. For example, if a storage file system overruns its physical bounds, storage virtualization lets an administrator seamlessly add disks without worrying about copying or backing up a single file. When two server applications cannot coexist on the same server farm, server virtualization allows the network administrator to put each application in its own virtual machine, sheltering each application from the effects of the other without requiring two separate, parallel infrastructures.

Virtualization in wireless LANs is a dramatically different approach to thinking about wireless networking. Every device is given its own virtual network, allowing all to avoid the negative consequences of sharing a resource. Users no longer need to be concerned with the physical nature of the resource, as all physical management tasks are handled automatically. From the application's perspective, the network

behaves exactly like wired Ethernet but is mobile.

Like all forms of virtualization before it, Wireless LAN Virtualization is built on the two concepts of pooling and partitioning.

Pooling the WLAN: Virtual Cell

The first step in virtualizing a WLAN is to eliminate the physical boundaries between the wireless resources. All of the access points need to be interchangeable, to operate as one without reducing capacity. This is the job of the Virtual Cell.

A Virtual Cell is formed when multiple virtualizable access points are placed within a floor or building. The radios on the access points cooperate to form a single, solid layer of wireless coverage, melding their transmissions together to appear as one larger access point.

Just as a virtualized disk farm will appear as one logical disk to applications while the disks retain their individual capacities, the Virtual Cell is still composed of multiple radios. The Virtual Cell's capacity is the same as it would be if the APs were functioning independently. The key difference is that the different radios are made to appear as one. The wireless client device cannot tell which radio is serving it. Instead, it sees a uniform layer of strong coverage throughout every square foot of the network. The administrator does not need to tune this layer. Instead, the coverage remains stable, not changing power levels or coverage areas during day-to-day operations.

Because the Virtual Cell consumes only one channel, other channels are freed instead of wasted. Capacity growth becomes simple. Adding layers of Virtual Cells ensures that the network capacity grows linearly with each radio: Add a radio, add capacity. With dozens of available channels, it is nearly impossible to reach the capacity limits on a virtualized WLAN system.

This spectral efficiency is especially important in the 2.4 GHz band, where spectrum is so limited that a traditional architecture cannot support even one full-rate 802.11n network without interference, let alone operate two simultaneously. Running multiple Virtual Cells also increases reliability, as clients always have multiple options for network connectivity. Because Channel Layering produces channels with identical coverage areas, it is easy to substitute one for another.

This concept of making it as easy to deploy WLAN radios as to place lamps in a room is the cornerstone of the virtualized approach to WLAN. Wireless resource pooling provides network invariance — a stronger form of predictability that means the network never changes during normal operation.

The user is freed from needing to understand the effects of being at his location, as coverage is now uniform. Mobility is trivial: Every user believes that the access point follows her around the building, never going out of range and never fading to black. The network is stable, just as with wireline, but is mobile in the way that only wireless can provide.

Partitioning the WLAN: Virtual Port

Pooling is the foundation of virtualization, but partitioning ensures that the resources get distributed without concern about the side effects of rampant sharing. In wireless LAN virtualization, the pooled network resource is partitioned into Virtual Ports.

A Virtual Port is a virtual wireless LAN dedicated a single mobile device. Each wireless device has its own

dedicated Virtual Port that follows it throughout the network. This virtual wireless LAN has only two devices connected to it: the client and the virtualized access point itself. Each Virtual Port is distinguished by having its own unique network address, not shared with any other client. All traffic to and from a client passes through its private Virtual Port. The Virtual Port acts as a tight, virtual resource bound that entirely contains the wireless traffic of the client, just as virtual machines contain compute processes on a server. Virtual Ports operate within the Virtual Cell, partitioning the pooled RF resources and ensuring that one client's over-the-air behavior cannot affect the rest of the network.

Virtual Ports are the wireless equivalent of the wired switch port. Just as a switch ensures that the behavior of one device connected to a switch port does not affect others on the same physical Ethernet network, the Virtual Port protects devices on the same physical wireless network from each other. Because each client is connected to its own virtual Port, the behavior of one single device cannot impact the network.

The Virtual Port is:

- private: the client does not share it with any other device.
- predictable: the same Virtual Port travels with the client throughout the network, providing the same elements of service and the same view of the network regardless of where the client is.
- controllable: by introducing per-device granularity into wireless networks for the first time, the administrator gains tremendous insight into the behavior of each client.

Partitioning the WLAN into Virtual Ports does not require the client's cooperation. If the client exceeds its resource bounds, it can be stopped unilaterally, even for upstream traffic that has not even passed into the network yet. This flow control is simply not possible on non-virtualized WLANs.

Most important, Virtual Ports do not require the administrator's attention. Just as a wired switch provides the port isolation inherent in switching by default, without requiring the administrator to monitor or analyze each port, the virtualized WLAN provides Virtual Ports by default, without requiring the administrator to think about their presence. The administrative overhead is reduced when Virtual Ports are provided. Later, if the administrator wants to apply distinct policies, the granularity of the Virtual Port allows for fine-grained administrative policies on a per-device basis that cannot be provided on non-virtualized networks.

Wireless resource partitioning provides per-device invariance, with a unique virtual WLAN for each device. Privacy and per-user controls are maintained without regard to the nature of the underlying device. No special client software or driver version is needed. Resource bounding is employed to provide the IT organization with predictability in network behavior that drives down operating expenses, freeing scarce IT resources and time for other, more important projects than actively babysitting wireless networks.

Summary

Wireless LAN Virtualization is available today with the concepts of resource pooling through Virtual Cells and per-device network partitioning through Virtual Ports. Together, they enable a dramatic departure from the unpredictability of costs and resource drains that non-virtualized wireless networks force upon IT organizations.

By removing the physical boundaries between resources and allowing for network invariance to become the core part of the experience of wireless LANs, Wireless LAN Virtualization drives down both initial deployment costs and ongoing operating expenses. WLAN Virtualization pushes wireless networking to exceed the expectations of wired networking, giving a stable wire-like experience while unlocking the power of collaboration through mobility that wireless networking provides.

Glossary

Air Traffic Control
Meru technology that exercises a high degree of control over all transmissions within a wireless network. Unlike superficially similar technologies from other vendors, Air Traffic Control coordinates uplink and downlink transmissions on a single 802.11 channel in such a manner that the effects of co-channel and adjacent channel interference are eliminated and all access points on a network can share a single radio channel. It also load balances traffic across channels when using Channel Layering, ensuring optimum use of resources.

BSSID (Basic Service Set Identifier)
A 48-bit Ethernet MAC address used to identify an 802.11 wireless service. In a Virtual Cell, all same-channel APs may appear to have the same BSSID, thus virtualizing the network from the client's perspective. When Virtual Ports are used, each client sees a different BSSID, appearing to get its own private AP.

Channel Bonding
The combination of two non-overlapping 20 MHz. channels into a single 40 MHz. channel, doubling the amount of data that can be transmitted in a given time but halving the number of available channels. It is a key innovation in the 802.11n standard, necessary to achieve the highest 300 Mbps data rate..

Channel Layering
Wireless LAN architecture in which several Virtual Cells are located in the same physical space but on non-overlapping channels, multiplying the available capacity. This additional capacity can be used for redundancy or to support higher data rates or user density. It can be enabled through multiple radios on one AP or by using multiple APs placed close together, so the total capacity is limited only be the number of non-overlapping channels available.

Co-channel Interference
Radio interference that occurs when two transmitters use the same frequency without being closely synchronized. Legacy wireless systems cannot achieve this kind of synchronization, so access points or cell towers that transmit on one channel must be spaced far apart. The result is coverage gaps that must be filled in with radios tuned to another channel, resulting in an inefficient and complex microcell architecture. Air Traffic Control technology avoids co-channel interference, enabling adjacent APs to use the same channel.

Fourth Generation
Term coined by analyst firm Gartner to describe a wireless LAN system in which the controller governs handoffs, such as one utilizing Virtual Cells. Gartner contrasts this with third generation (micro-cell architecture) systems, in which the controller is only responsible for managing access points and clients must decide for themselves when to initiate a handoff. Second generation systems rely on standalone APs and lack a controller altogether, whereas the first generation used proprietary, non-802.11 systems.

Handoff
The transfer of a wireless client device's network connection from one access point to another as the client moves through a network. In legacy microcell networks, Wi-Fi clients themselves control the timing and manner of handoff, meaning that the quality of the link and the overall network performance is dependent on each client's implementation of 802.11 roaming algorithms. In Virtual Cell and Virtual Port networks, the network itself governs handoffs as clients remain connected to a single virtual AP.

Microcell
Wireless architecture which extends coverage by laying out a complex mosaic of small wireless cells, each tied to a particular AP. Adjacent APs must be tuned to different, non-overlapping channels to mitigate co-channel interference. This requires complex channel planning both before the network is built and whenever a change is made, and uses spectrum so inefficiently that some co-channel interference still occurs, especially at 2,4 GHz. Microcell architectures were common in 2G cell phone systems. They are not used in 3G cellular networks or in wireless LAN systems that use Air Traffic Control, as these allow all access points to share a single channel.

Overlay Network
A dedicated network of radio sensors that are similar to access points but do not serve clients, scanning the airwaves full time for security or management issues. Overlay networks lack the flexibility of AP-based scanning, as radios cannot be redeployed between scanning and client access. They also lack deep integration with the main wireless network, necessary for real-time management and intrusion prevention.

Partitioning
Virtualization technique in which a single resource or a set of pooled resources is divided up into virtual resources, each dedicated to a particular application or user. Examples include the virtual machines in server virtualization, virtual disk drives in SANs and Virtual Ports in Wireless LAN Virtualization. The main advantages of partitioning are control and isolation: Each application or user can be given exactly the resources needed, protecting users from each other and ensuring that none consumes more than its allocated share of resources. In a wireless context, it makes a wireless LAN behave more

like a switched Ethernet port.

Pooling
Virtualization technique in which multiple physical resources are combined into a single virtual resource. Examples include the multiple disk drives in a virtual storage array, the multiple CPUs in a modern server and the multiple access points in a Meru Virtual Cell. The main advantages of pooling are agility, simplified management and optimized use of existing assets,: Resources can be moved between applications on demand, reducing the need for over-provisioning of physical equipment to accommodate fail-over or capacity shifts and freeing applications from dependence on a single piece of limited infrastructure.

Roaming
The process that takes places as a wireless client device moves between the coverage areas of different APs, necessitating a handoff. In microcell networks, handoff can be a complex procedure that risks dropped connections and drags down network performance, as the client is forced to decide when to disconnect from one AP and search for another. In networks using Virtual Cell and Virtual Port technology, the infrastructure controls roaming, automatically connecting each client to the optimum AP. This is achieved by the pooling of RF resources into the Virtual Cell or Virtual Port, to which the client remains connected at all times. The client sees only one AP and so never initiates a handoff.

Scanning
The process of checking the airwaves for rogue access points or attackers. Scanning APs are typically implemented as an Overlay Network, as most APs can not scan and serve traffic at the same time. Meru's APs are able to scan the airwaves and serve clients simultaneously, eliminating the need for an overlay.

Spectral Efficiency
The ratio of data rate to radio spectrum usage. A Virtual Cell is more spectrally efficient than a microcell architecture because microcells consume at least three non-overlapping channels to provide the coverage that a Virtual Cell offers with just one.

Single Channel
Used to describe a network in which all access points operate on the same channel, such as one using Virtual Cell technology. Single channel operation is more spectrally efficient than a microcell architecture, and improves intrusion detection and location tracking because every AP automatically receives transmissions from every client within range. It is also the foundation of the Virtual Cell architecture and necessary for network-controlled handoff, though not all single channel networks necessarily implement these more advanced technologies.

Virtual Cell
Wireless LAN architecture in which multiple access points are pooled into a single virtual resource. To the wireless client, individual APs are indistinguishable because they all use the same BSSID and radio channel . Clients remain connected to the same virtual AP as they move through a network, so no client-initiated handoffs are necessary. Instead, the WLAN controller automatically routes all radio connections through the most appropriate AP based on its knowledge of the entire network. This maximizes capacity, simplifies network management and conserves radio spectrum for scalability and redundancy.

Virtual Port
An extension of the Virtual Cell architecture which partitions available radio resources so that each client device has its own private connection to the network through a unique BSSID. From the client's perspective, it gets its own dedicated AP to which it remains connected no matter where it travels within the network. Like a switched Ethernet port, the Virtual Port eliminates latency, jitter and contention for bandwidth as there is only ever one client on each port. Unlike an Ethernet port, it can be personalized to fit each user or device, giving the network control over client behavior with no proprietary client-side software or extensions necessary.

VoFI (Voice over Wi-Fi) or VoWLAN (Voice over Wireless LAN) or VoWIP
Voice over IP links that run over a wireless network. VoIP does not usually require high data rates, but it stresses wireless networks in other ways by demanding low latencies and smooth handoffs.

Wi-Fi
Brand name for wireless LANs based on various 802.11 specifications. All products bearing the Wi-Fi logo have been tested for interoperability by the Wi-Fi Alliance, an industry group composing every major 802.11 client and infrastructure vendor.