Using Wireless Mesh Networks for Video Surveillance

ARUBA networks

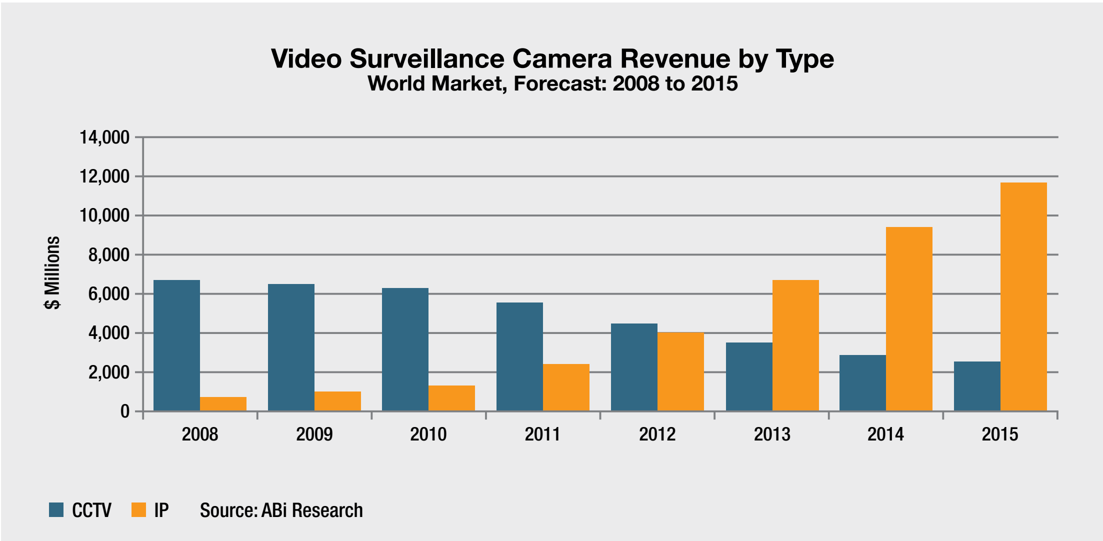
Table of Contents

Video surveillance is moving to IP

Video surveillance originated in the 1960s when closed-circuit television (CCTV) was first used to monitor and record events. Today, the video surveillance market is quickly transitioning to enterprise IP networks. By 2012, more IP video cameras will be sold than CCTV cameras, according to ABI Research.

IP cameras have many advantages over CCTV cameras, including higher image resolution and more efficient data storage. In addition, modern IP-based surveillance applications provide more sophisticated data analysis.

Importantly, with IP video surveillance, organizations can leverage their existing data networks for transport rather than relying on a single-purpose, proprietary network. With a high-performance, multiservice wireless network, organizations can support multiple applications and user groups on the same infrastructure, while simplifying the network and lowering operational expenses.



IP cameras are quickly overtaking CCTV cameras
as the preferred method for video surveillance.

Video wireless mesh networks

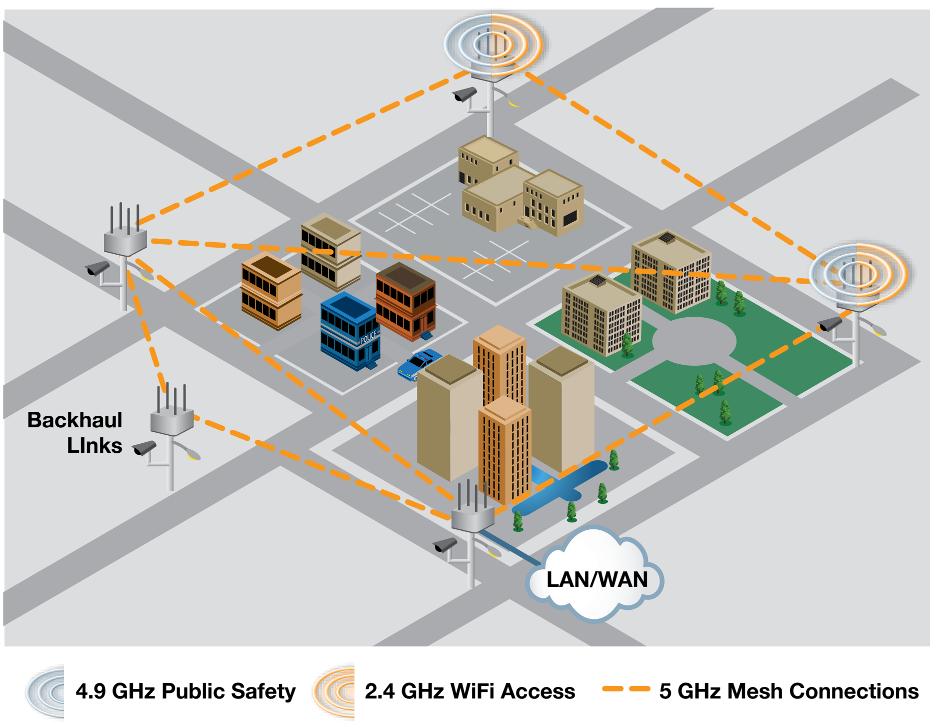
Wireless mesh networks offer a practical and cost-effective way for municipalities, public safety agencies and enterprises to deploy IP video surveillance. In addition to video surveillance, wireless mesh networks can concurrently support enterprise voice and data applications across a multiple paths and multiple LAN/WAN hops.

The ability to be rapidly installed without reliance upon a fixed infrastructure makes wireless mesh networks ideal for temporary deployments. A mesh can be set up and used for monitoring and surveillance during an incident or public event, and is easily packed up and moved to the next location.

Wireless mesh network are also low maintenance. They automatically select the best path through the network, and operate reliably even if a mesh node or RF link fails. Mesh networks integrate easily with wired networks, so they can be used to extend an existing deployment.

Using wireless mesh networks eliminates the high cost and disruption associated with pulling fiber – or the recurring monthly fees paid to a service provider for leased lines or broadband Internet.

Any organization can deploy a wireless mesh network in the unlicensed 2.4-GHz and 5-GHz band, and U.S. public safety agencies can use the 4.9-GHz public safety band.



Automatic configuration and routing enables the AirMesh networks to be self-forming and self-healing, which reduces operational costs.

Challenges of delivering HD-quality video surveillance

Delivering high-quality video surveillance over legacy wireless mesh networks was met with obstacles in the areas of performance, scalability, video quality, roaming and quality of service.

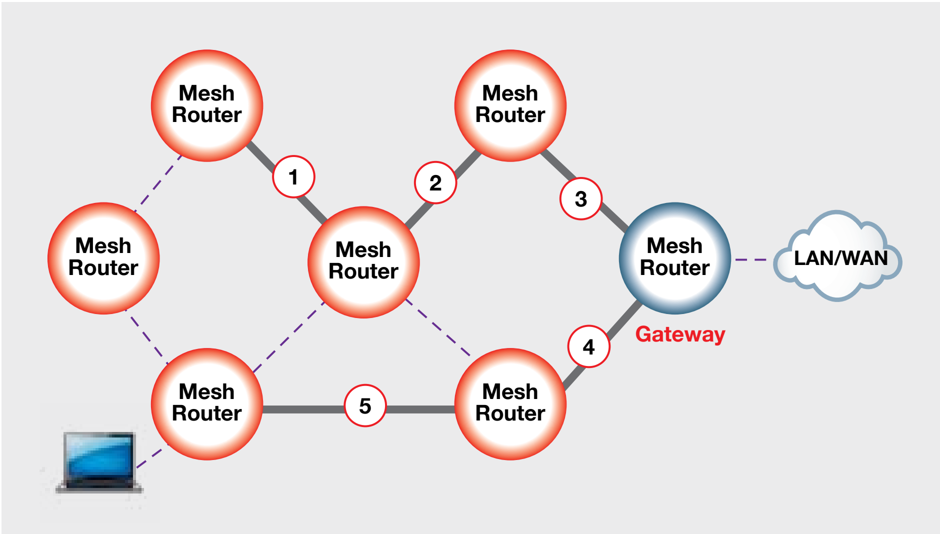
- **Limited capacity –** Mesh nodes may contain multiple radios, and the mesh nodes that use separate radios for client access and for wireless backhaul deliver better performance than single-radio nodes.

  However, with dual-radio nodes, the backhaul network still shares a single channel and requires omni-directional antennas. This results in congestion and degraded performance on each hop, which limits the size and performance of the mesh.

- **Reliability and scalability –** Many mesh products use Layer 2 switching and a spanning-tree type protocol to form the mesh itself. Unfortunately, spanning tree does not perform well in large networks. Latency grows with every network hop, which degrades video performance.

  A Layer 2 mesh is also slow to adapt to rapidly changing conditions that are typical of a wireless network. When link changes occur because of RF interference, a Layer 2 mesh converges very slowly over several minutes. Again, this has a major impact on the network's ability to support video surveillance, voice and other time-sensitive applications.

  In addition, the gateway node in a Layer 2 mesh that connects to the Internet or an external network is a single point of failure that can compromise service availability.



The flat architecture of a Layer 2 mesh causes performance and reliability issues. Network latency is high because of extra hops through the network and the mesh node to the external LAN/WAN is a single point of failure.

- **Common video impairments –** Lost packets, out-of-sequence packets and jitter can visibly degrade video quality.

  When video or voice packets are lost, the underlying user datagram protocol (UDP) cannot retransmit the lost or corrupted packets. And with compressed video, any amount of packet loss is noticeable.

  Packets can arrive at their destination in a different order than they were sent, usually because the route changed during a session. With compressed digital video, out-of-sequence packets disrupt the decoding process and can degrade quality.

  Jitter, or variable delay, causes the video quality to degrade with noticeable pixilation or blurring of the image. Jitter is caused by delay at the sender, variable data link rates along the path, changing traffic conditions, changes in routers, and roaming.

  Digital video compression algorithms are stateful, which means that the arriving bit stream is used to make changes to the existing image, rather than constructing a new image for each frame interval.

  Stateful compression is highly efficient, but it is intolerant of packet loss. If packet loss, out-of-sequence packets, or jitter becomes too severe, the video encoder and decoder will have to resynchronize, which impacts the image quality.

- **Seamless roaming** – Users and devices should be able to maintain their video surveillance, voice conversations and even data connections while moving from one mesh node to another – whether they are on foot or in vehicles.

  However, many vendor solutions for seamless roaming with session persistence across IP subnets require the addition of complex mobility controllers or client software, which adds to the complexity and cost of the network.

- **Quality of service (QoS)** – Multiple user groups and multiple applications should be able to share the air. With QoS and traffic management, organizations can define and enforce service levels as appropriate. For instance, video surveillance and voice can have priority access to a specific amount of bandwidth, while data applications have a lower priority.

Aruba’s high-performance mesh network

AirMesh from Aruba Networks® brings unprecedented levels of scale, capacity and reliability to outdoor wireless mesh networks. The AirMesh multiservice platform is optimized to deliver HD-quality video surveillance, as well as voice and data.

AirMesh routers use an 802.11n, multi-radio architecture that delivers massive capacity – up to 300 Mbps per radio. They come in single, dual and quad radio platforms that are software-configurable so that each radio can operate as a mesh backhaul link or as an 802.11n access point (AP), as well as in the 2.4-GHz, 5-GHz and U.S. public safety 4.9-GHz frequency bands.

The mesh backhaul network is comprised of multiple point-to-point links, with each link operating on a different RF channel for optimal frequency reuse. And with enhancements to support distance, long-range directional links can be established up to 5 kilometers (3.1 miles).

Scalability and fast convergence with intelligent routing

Intelligent, Layer 3 routing brings unprecedented scalability and reliability to mesh networks. Aruba's patented Adaptive Wireless Routing™ (AWR™) automatically optimizes traffic routes between multiple wireless mesh routers. The resulting adaptive mesh infrastructure adjusts dynamically to traffic levels and RF signal strength to ensure high availability and zero performance degradation across multiple hops.

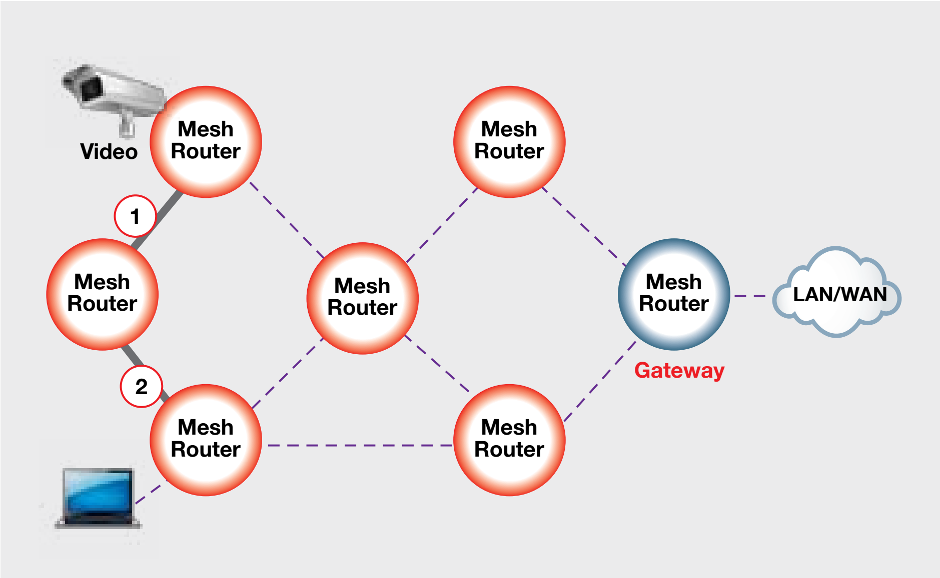
With AWR, traffic is instantly rerouted around congestion or link failures. Traffic is load balanced across the network to optimize the flow, even when levels of RF interference is high, which makes the network resilient and scalable.

AWR maximizes user throughput by taking into consideration the quality of the radio link in its routing decisions. Link failures may be rare in wired networks, but wireless mesh networks are susceptible to sources of RF interference that can cause a link to degrade or fail. As an RF-aware routing protocol, AWR eliminates bottlenecks and single points of failure, which results in superior resiliency and throughput.

AWR is designed to rapidly converge the network when routing changes occur, which is an essential characteristic of a resilient, highly available network. In contrast, a traditional Layer 2 network can literally take minutes to converge.

Routing protocols such as OSPF can easily flood the network when handling the rapidly changing conditions typical on a wireless network. AWR can converge changes very rapidly, which makes AirMesh ideal for time-sensitive applications like emergency response.

AWR supports IP multicasting to provide more efficient bandwidth utilization for video and other applications that need to broadcast to multiple destinations.



A mesh operating at Layer 3 provides intelligence that allows for optimal performance, scalability and reliability. All traffic does not need to flow through a single gateway, as with a Layer 2 mesh. And Layer 2 services can be delivered over the Layer 3 infrastructure.

High-definition video surveillance

Aruba's innovative Active Video Transport™ (AVT™) employs traffic management and load balancing across long-range directional links to deliver HD-quality video surveillance from fixed and mobile IP cameras, monitors and recording systems. With AVT, progressive, non-interlaced video can be delivered at up to 30 frames per second.

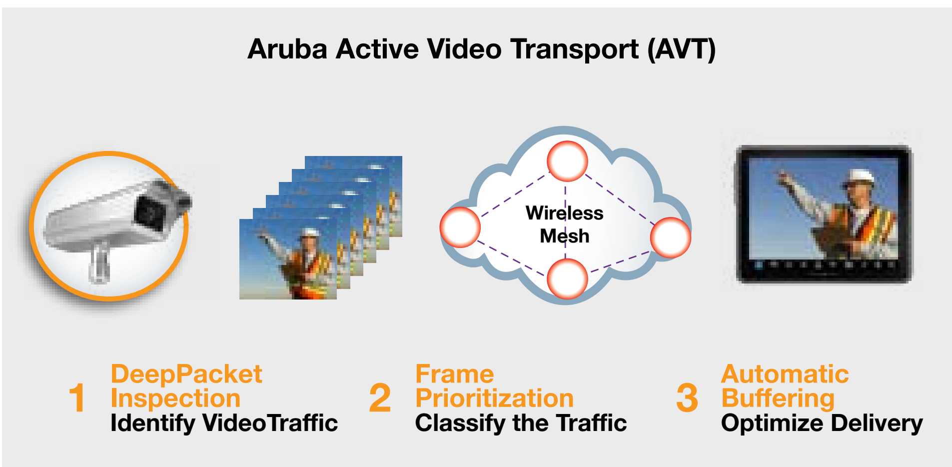
AVT delivers HD-quality video by making intelligent tradeoffs between latency and the impairments to video quality. Buffering compensates for packet loss, re-ordering out-of-of-sequence packets, and jitter while any increased latency is imperceptible to users. What is perceptible is a significant improvement in video quality.

AVT is implemented in every AirMesh router so that the video optimization is enforced across the entire mesh. Multiple technologies, including deep packet inspection, MAC protocol optimization, and in-network retransmission protocol, and adaptive video jitter removal, are used in a three step process.

1. Deep packet inspection – Upon ingress, AVT performs deep packet inspection to identify and extract the compression algorithm, video decoding buffer model, video frame-type boundary, and video timing used by the packet stream. This information is used to optimally deliver the traffic through the network.

2. Frame prioritization – AVT applies a special frame format used by the traffic management process and interleaves batches of frames during transmission.

3. Automatic buffering – Upon egress, AVT performs adaptive video jitter removal. It issues in-network retransmission requests when lost and corrupted frames are detected, reorders any out-of-sequence frames, and releases the video frames at a consistent rate at the end of the playback deadline.



Active Video Transport uses a three-step process to optimize video across the mesh. All AirMesh routers implement AVT, so high-definition video can be delivered end-to-end.

Seamless roaming with session persistence

Aruba's innovative Active Video Transport™ (AVT™) employs traffic management and load balancing across long-range directional links to deliver HD-quality video surveillance from fixed and mobile IP cameras, monitors and recording systems. With AVT, progressive, non-interlaced video can be delivered at up to 30 frames per second.

With Aruba's MobileMatrix™ technology, users can roam at high speeds across the mesh network while maintaining their application session – even latency-sensitive video and voice. With seamless roaming, digital images from an incident scene can be streamed to patrol cars, ambulances and fire trucks, giving first responders greater situational awareness.

Clients roam from one mesh router to another in less than 50 milliseconds while maintaining their session and IP address. MobileMatrix builds on AWR to support fast, seamless roaming in vehicles moving up to 60 miles per hour.

The MobileMatrix capability works with ordinary Wi-Fi clients, and does not require any special software or hardware.

Enforcing service levels on a multiservice mesh

Enforcing QoS allows the Aruba mesh to support different groups of users and different applications on the same infrastructure, while ensuring that each receives the appropriate service levels.

With QoS, mission-critical applications such as voice and video have priority access to the network bandwidth, while less time-sensitive traffic such as e-mail or web traffic, have lower priority.

Aruba supports multiple methods of QoS enforcement from end to end across the mesh, including DiffServ, IEEE 802.11e and IEEE 802.1Q virtual LANs (VLANs).

DiffServ is the preferred way to enforce QoS in a routed network. It provides a way to classify and manage network traffic for mission-critical applications, such as video and voice, while maintaining acceptable service levels for all other applications.

802.11e defines QoS enhancements for wireless LANs at Layer 2. In addition to 802.11e, Aruba also supports Wi-Fi Multimedia (WMM) and Wireless Multimedia Extensions (WME) from the Wi-Fi Alliance.

In this method, separate queues are allocated for voice, video, best effort and background traffic. With AirMesh, the priorities established with DiffServ can be mapped into these Layer 2 flow categories.

VLANs allow organizations to segment the network at Layer 2. Segmentation creates an additional layer of security and can help manage service levels. VLANs are typically used to isolate Wi-Fi devices that do not support 802.11e. With AirMesh, a VLAN ID can be associated with a WLAN service set identifier (SSID), which extends the VLAN's QoS priorities to users and applications associated with different SSIDs.

Video surveillance with no strings attached

With Aruba AirMesh wireless mesh networks, organizations can count on the highest performance and most reliable outdoor infrastructure for video surveillance. Exhibiting exceptional capacity and scalability, AirMesh meets expanding business requirements for video surveillance and monitoring, and scales to support many other services, including Wi-Fi access, voice over wireless and a wide range of other mission-critical enterprise applications.

About Aruba Networks

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook.

arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com