![Nemertes logo — Better data. Better decisions.]

Power Up the Connected Fan Experience

Convention, concert, or game: innovative attendee services require exceptional technology to power them.

By John Burke, CTO
Jerry Murphy, Senior VP

Nemertes

March 2024

Table of Contents

1. The Issue: It's All About the Experience

Attending a concert, big sporting event, or convention has become a digitally enhanced multimedia experience, with attendees connecting to the venue's web of customer facing and operational technologies as well as their own personal constellation of media. Table stakes in the new universe of digitally enhanced venues include in-venue mobile food ordering, in-venue payment apps, food and drink delivery, touchless parking management, assistive listening services, lost-child alerts, and general lost-and-found.

Venue owners and operators know that staying competitive and cutting-edge means doing innovative things to attract and engage visitors to events—whether games, conventions, concerts, or other—such as:

- Throw attendee selfies up on the jumbotron or flash them on attendees' phone screens with a dedicated event app
- Put attendees in the game by mounting cameras on a player's helmet to drive immersive viewing and instant replay with VR headsets
- Show attendee's their own location within the facility via live mapping, as well as routes to the nearest restroom, lounge, or (for business conferences) to the specific suites and breakout rooms their agenda requires
- Conduct virtual scavenger hunts in the facility using AR apps
- Secure event-specific on-premises chat for attendees and players/celebs/speakers

To make this happen, owners and operators need to create solid technology underpinnings, designed and implemented with not just table-stakes services in mind but also emerging new use cases like these, and trends in attendee technology use generally.

2. Key Enabling Technologies

With the key goal of driving attendance through engaging new experiences, venue owners have to build out infrastructures that can cope with an event at maximum occupancy without missing a beat—or dropping a bit—even with demanding new uses like AR/VR in play. That means having not just a wireless infrastructure that can support that many humans in the space but also the layers of infrastructure, security, observability, and management needed to engage attendees with these innovative applications safely.

2.1 Dense, High-Speed Wireless Coverage

How many devices will the average attendee bring to an event? How much data will they consume? These are key considerations for any venue's technology architecture. And the trend is "more, more, more" – more people with devices, more devices per person, more data per person.

Usage stats show the average is under 1 device per person on venue wireless at recent major sporting events like college or professional football championships, at least for now. However, the gradual penetration of tablets, smart watches, health monitors, and eventually AR or VR headsets or other devices will gradually ratchet that up above 1 device per person.

For conventions, though, the average is likely already above 1 and closer to 2, given that most attendees at a professional convention will have not just a phone but also a laptop and/or a tablet.

The amount of data consumed by an event attendee is climbing steadily, even for sporting events. Fans at the 2023 US professional football championship consumed 643MB per connected device, for example, according to the [Stadium Tech Report](#)[1], a new record at the time. Of course, some folks will use far more than the average amount of data, others far less. This highlights another requirement: venue infrastructure must handle high-demand sessions wherever and whenever they pop up without shortchanging other nearby sessions due to oversubscription.

Adding to this is the steady growth in connected devices *not* associated with attendees, such as temperature sensors, security cameras, motion detectors, mobile point-of-sale devices for wandering refreshment vendors, information and sales kiosks, and digital signage. Some, like temperature sensors, are low-bandwidth devices that generate little data individually. Some, like digital video signs, consume a lot of bandwidth. The operator's network infrastructure has to be able to support all these bandwidth sources.

2.1.1 Wireless Technology: Advanced WiFi, Private 5G and LTE, LoraWAN and More

To meet these challenges, venue operators need to deploy future-ready technologies. WiFi 6 is rapidly becoming the norm, as is 5G cellular wireless, and WiFi 7 and 6G are already in the offing. Both are designed to support the new levels of device density and increasing demand for both data speed and data volume alongside that higher density. Both incorporate significant technical improvements, including:

- MU-MIMO (multi-user multiple input multiple output), which allows an access point to serve multiple devices for multiple people simultaneously by sending physically separated signals at them via a technique called "beamforming" (note, before MIMO, access points only appeared to serve multiple users simultaneously when in fact they were serving each one separately and just cycling through them very rapidly)
- MU-OFDMA (multi-user orthogonal frequency division multiple access), which allows an access point to subdivide each of its primary frequency channels into as many as 256 sub-carriers and then bundle slices together into "resource units" sized to meet each device's needs; devices rolling live video would get larger resource units than devices being used to send texts
- Full incorporation of the lower-frequency channels that characterized previous generations of wireless, meaning the 2.4GHz channels for WiFi 6 (the previous standard, 802.11ac, did not use them) or the 4G LTE spectrum for 5G, to better serve the needs of lower power, long distance, or high-interference use cases
- Better collision detection and avoidance on data channels than earlier standards; WiFi 6, for example, can hit up to 90% of theoretical maximum capacity in a channel where previous WiFi standards topped out below 70%

---

[1] https://stadiumtechreport.com/feature/super-bowl-lvii-sees-31-5-tb-of-wi-fi-data-sets-new-record-for-per-device-data-used/

In addition to extending the carrier-neutral distributed array systems that support 4G LTE to support 5G traffic too, venue operators will increasingly deploy true private wireless: 5G run by—or for—the venue.

Another key change in event venue technology: operators will embrace other IoT-specific communications standards, such as LoRaWAN, a wireless standard focused specifically on low-bandwidth, low-volume use cases. It allows long-range, low-power communications for devices such as temperature and motion sensors that don't transmit or receive data continuously, or send or receive much data at a time. Such protocols make a fully instrumented space, replete with sensors of various sorts, more affordable and maintainable.

2.2 Connecting to the World

All the wireless capacity in the world is not much help if the venue's Internet link is overloaded. So, in order to provide the best experience possible to attendees, operators need high-capacity, low-latency, ultra-reliable connectivity. The stadium's bandwidth demand for the 2023 football championship game spiked close to 26 Gbps. In most venues, operators will not see that kind of demand soon. But as attendee expectations and app suites evolve with an expectation of higher edge speeds (thanks to 5G and WiFi 6) operators will see demand rise steadily and quickly. So, links have to be rock solid and capacious. They have to accommodate traffic to sites people go to no matter where they are—for video streaming, gaming, or social media—and to event-relevant cloud destinations such as broadcasters and sponsors.
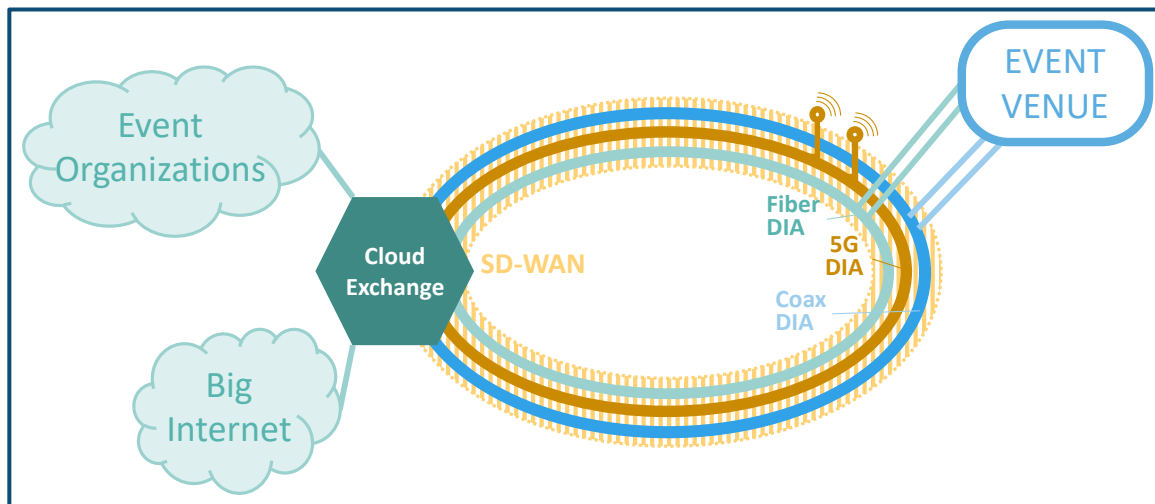

Figure 1: Many Paths, Multiple Providers, Always On

For ultra-reliable connectivity in and to the venue, operators and facility IT architects will continue to lean on optical fiber MANs and LANs. However, they can include other multi-gigabit-capable media for redundancy and resiliency, both within venues and between venues and service providers. Some will certainly add 5G as the buildout of 5G Standalone networks supporting bandwidth slicing and millimeter-wave infrastructure continues, bringing fixed wireless at multi-gigabit speeds to the market.

Ideally, venue IT architects incorporate network connections coming from multiple providers, following different physical paths to it, and coming in via different physical entry points to the

facility. A single cable cut, failed router software push, or power outage shouldn't be able to interrupt service during an event.

SD-WAN is a great fit for such designs, as it can distribute traffic across all available connections, both for resilience and to allow optimization based on protocol and destination. This will deliver the lowest-latency experience for attendees as well as the smoothest adjustment to shifting demands and Internet conditions.

2.2.1 Venues Join the Edge

A related technology shift venue designers need to take into account is the rise of shared-infrastructure edge data centers. As more user-facing applications get distributed out to edge infrastructure to reduce response times and localize data-intense operations, the demand for such applications in event venues will likely increase as well—to say nothing of applications developed specifically for events. If the game-day app's user front end can run on server capacity in the venue, with data cached there, response times will be cut to as near zero as possible.

As standards for edge infrastructure sharing mature (in the 5G space) they can be ported over to the wired and WiFi infrastructures as well. Then this sort of edge optimization can happen easily no matter whose event is coming through or what apps people in attendance want to use.

3. Tight Security in (W)LAN and WAN

5G and WiFi 6 (and other protocols including LoRaWAN) include built-in security features ranging from improved mutual authentication of endpoints and access points to improved security among service components in the core (for 5G). But protocol-level provisions are only the beginning. Venue security architects need to provide a layered defense in depth, a true zero trust architecture.
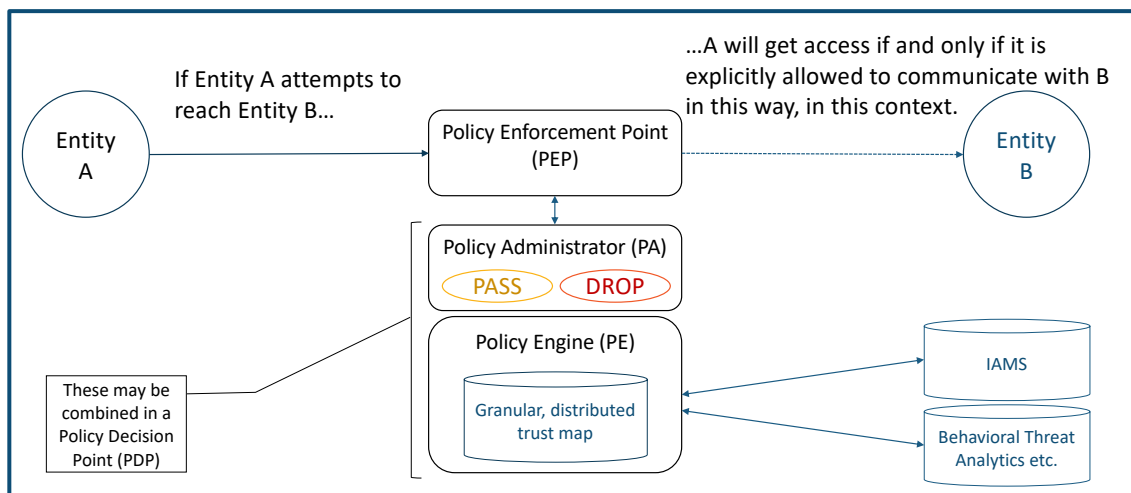

Figure 2: Simplified NIST zero trust Architecture

This means that in addition to any logical and physical partitioning of wireless networks on premises, security architects will design for authenticated and access controlled wired networks. Further, they will wrap every system in zero trust access control: those not granted explicit permission to use a system will be unable to reach it. Ideally, they will go one step further and ensure that when anyone attempts to gain unauthorized access to any system, the attempt will fail

as though there was no such system on the network, and will trigger an immediate alert to a security operations center.

To realize a full zero trust environment, security architects will include behavioral monitoring systems able to immediately tell the zero trust controller that something on the network—a person, a device, an application—is acting suspiciously. Then the controller, based on policy, can take action: increase monitoring on that entity, or limit further what it has access to, or even shut down access for it entirely.

Beyond zero trust, venue security engineers and operations teams need to be even more vigilant than most in keeping infrastructural systems fully patched and up-to-date, to eliminate as fully as possible any known vulnerabilities at that level. They should, for the same reason, emphasize use of hardened operating system images and appliances to deliver any services hosted on premises.

4. Monitoring and Management

To maintain the quality of the attendee experience, despite the fast-changing array of services and customers at play in a venue, the venue operators need a robust portfolio of monitoring systems and management tools. They must populate that portfolio with both performance and security monitoring systems, and ideally run from a combined network and security operations center staffed 24/7 (at least on event days and the days immediately preceding and following).

To keep up with the pace of service-affecting events and security incidents, venue architects and engineers must tie together management and monitoring systems with reliable automation. This automation will include multiple layers, some deep in the infrastructure—e.g., the SD-WAN's built in automation of path selection—and others layered atop or wrapped around infrastructure systems, like a security operations and response (SOAR) tool.

And to help deal with the problem of optimizing consumption of human cybersecurity and operational attention, security engineers will come to prefer management platforms that incorporate meaningful AI functionality. "Meaningful" in this case meaning, AI that improves problem resolution times, for example by reducing the number of operator alerts sent for false alarms, or by assisting staff in taking the correct action to resolve a problem.

5. Partnering for Success

The array of skills and the amount of skilled attention required to provide a state-of-the-art, well-secured, and well-managed venue infrastructure can be daunting. Rather than maintain the size of staff needed to have the range of skills required, venue operators can and often do choose instead to outsource much of the work. They can work with one or many providers to handle any part of the job, from design to installation and configuration to ongoing management and NOC/SOC operation. Using managed services from providers with significant focus in each area can bring a deep bench of highly skilled professionals to bear on each set of problems for as long as needed without having to keep them on the payroll full time.

6. Conclusions and Recommendations

To support a new generation of cutting-edge in-event experiences for attendees, venue operators must invest in every layer of the technology environment, from physical access to a merged

SOC/NOC. They have to undertake the work at every layer and in every part of the environment with an emphasis on security—protecting the services from the users and the users from each other. Technology teams should:

- Redesign connectivity to the venue for a fully redundant, zero-downtime network
- Fully support WiFi 6 and 5G in all spaces, and other wireless as needed for IoT systems
- Lean into automation in management and security
- Implement zero trust throughout the environment
- Evaluate managed service partners for each area of activity, from connectivity to SOC/NOC operation.

DN11215