ICT TODAY

THE OFFICIAL TRADE JOURNAL OF BICSI

January/February/March 2024
Volume 45, Number 1

EMBRACING THE AI REVOLUTION:

HARNESSING THE POWER OF ChatGPT

PLUS:

+ The Case for Multicast in Smart Buildings
+ Your Building Has a Story to Tell: Let AI Narrate It

BICSI®

The Case for MULTICAST in Smart Buildings

By Akram Khalis

As the number of internet of things (IoT) sensors and devices grows, it is imperative that technology developers think strategically about how these devices communicate. To achieve optimal reliability, efficiency, and scalability of smart-building investments, engineers must consider not only the infrastructure challenges of today but also those of tomorrow—when 17 billion endpoints easily could become 17 trillion.

Multicast routing is among the most effective solutions (Figure 1). The protocol has the potential to accelerate the impact of smart buildings across a range of outcomes, including:

- Preserving bandwidth
- Enhancing user experiences
- Improving security
- Achieving sustainability

Advocating for multicast does not necessitate the diminishment of other communication protocols. Unicast and broadcast, for example, are each effective in defined use cases. Multicast, however, is the optimal protocol for iterative smart buildings, specifically those with owners who intend to continuously improve their properties alongside fast-advancing IoT solutions.

FIGURE 1: Multicast network topology grouping allows for floor-by-floor or even room-by-room configuration in smart buildings. This enhances the user experience, improves security, preserves bandwidth, and achieves sustainability.

Because one source sends data to multiple interested recipient devices simultaneously, multicast excels at efficiency. The reduction of network load and congestion, not to mention the enhanced security that comes from selective transmission, makes the protocol a highly reliable and scalable alternative for larger, enterprise-level networks.

NETWORK COMPLEXITY IS SECOND NATURE FOR MANY

The ICT space is, of course, familiar with multicast. It is commonly found powering low-voltage systems, such as voice over internet protocol (VoIP), internet protocol (IP) cameras, and closed-circuit communication platforms. Today, however, the smart building ecosystem brings many more devices to the table for the deployment of multicast. This includes lighting, every building's highest-density component. The opportunity for ICT to now "own" lighting could be perceived as overly burdensome; it could also be seen as potentially empowering, given the opportunity to further demonstrate the power of connectivity.

Because of the familiarity with the protocol, many of the perceived challenges around the network complexity of multicast may have been solved thanks to fully functioning—or, minimally, fully replicable—networking infrastructures already in place.

That said, there are some design and installation considerations ICT pros will want to think through and plan for. These include bandwidth requirements, network topology, device grouping, system agility, and cybersecurity.

BANDWIDTH REQUIREMENTS

Multicast technology can be a strategic asset in addressing bandwidth requirements in smart buildings. By enabling the simultaneous delivery of information to multiple endpoints, multicast conserves bandwidth. This is particularly true for internet of things (IoT) environments with devices that frequently require the same data—such as updates, streaming video, or real-time analytics. By sending a single stream of data that all devices subscribe to, multicast reduces the network load. The approach ensures that bandwidth is used more efficiently and is available for critical tasks, leading to improved overall network performance.

The ability to throttle equipment is important. The goal is to enable high speeds only when necessary and dial those speeds back when they are not needed. Lighting platforms are not configured for optical fiber cables. But access points and cameras are because they need to send large volumes of data at high speeds.

We can now transmit at a high speed, but it does not mean we want to send data back upstream again. We want it to be on edge, which means that the infrastructure needs to support it. With multicast, you are basically doing everything on-premise.

NETWORK TOPOLOGY

Multicast groups can be configured however the smart building's networking team desires. Maybe it is floor-by-floor, or maybe it is room-by-room. The idea is to eliminate the need for IoT devices to decipher whether a particular message is intended for them. Such unnecessary filtering creates latency.

Regardless of the layout, multicast needs Layer 3 network topology at a minimum to function properly.

When it comes to topology design, ICT professionals should consider two best practices: avoiding overcomplication and carving out time for validation. For example, one multicast group per zone is a best practice for preventing unnecessary complexity. Validation is similarly important. Once a multicast grouping is deployed, it is important for the team to take the time to evaluate the results. Are they what you expected, or do you need to make changes?

With the democratization of artificial intelligence (AI), testing and validating are becoming much simpler and more automated. Generative AI is also making it much less complicated for stakeholders with varying degrees of technical skill to use these tools. A user could, for instance, tell a GenAI multicast design program to create the ideal grouping for a building with 400 lights, 300 shades, 20 HVAC systems, and 40 conference rooms. The user could then direct the program to validate the configuration after deployment.

DEVICE GROUPING

Within a multicast framework, devices subscribe to a single group. They are connected, which means the network itself, rather than an outside routing mechanism, is doing the job.

Device grouping allows a set of devices to be addressed all at once. In the context of smart buildings, this means that instructions or data can be sent to multiple IoT devices simultaneously rather than individually. This approach not only enhances the efficiency of the network by reducing the number of messages that need to be sent, but it also conserves bandwidth, as a single data packet can serve multiple devices. It is particularly useful for applications like software updates, audio/video streaming, or synchronizing settings across a system of devices, ensuring that all devices receive the same data simultaneously.

When it comes to determining device grouping, it is best to start with a good control narrative developed by process engineers in close collaboration with contractors and designers. What is the sequence of operation that will create the best user experience? ICT pros can then use that control narrative to define nodes, optimize them, and then logically separate them based on functionality. If devices do not need to talk to each other, they do not need to be in the same group.

That said, devices that do not need to communicate today may need to tomorrow. This is again where multicast is beneficial. The protocol is ideal for iterative smart buildings with owners who intend to continuously improve their properties alongside fast-advancing IoT solutions.

SYSTEM AGILITY

In multicast networking, system agility refers to the network's ability to easily adapt to changes, such as adding new devices or enabling communication between previously disconnected devices. This flexibility is crucial in dynamic environments like smart buildings, where the network landscape is continually evolving with the addition of new IoT devices and systems.

Multicast allows these changes to be made with minimal effort—often just a simple configuration change that tells the device which multicast group it belongs to. The network then automatically incorporates this device into the group communication streams, ensuring seamless integration and communication without the need for complex reconfiguration or manual intervention.

When a new device is added or when two legacy devices that did not talk now need to, it is a simple logical movement that tells the device it now belongs to a new group. You are simply changing a network configuration, and the network automatically adjusts going forward.

CYBERSECURITY

Multicast goes a step further than virtual local area network (VLAN), which was created to virtually separate or segment multiple silos. It allows devices to cross-communicate, but in a smaller group. It also reduces complexity. VLAN logical segmentation can get difficult. What is more, VLAN only scales horizontally.

Tagging devices for a particular multicast group communication restricts other devices and their components from talking to those outside the group. This is a nightmare for cyber intruders who typically enter a system through the path of least resistance and then jump from one endpoint to another, seeing how far into the network they can get … and how much data or control they can steal along the way.

In a multicast environment, several cybersecurity considerations should be solved during the design and installation phase. These include:

- **Secure Multicast Protocols:** Implement protocols that support secure multicast transmission, like internet protocol security (IPsec) for encryption.

- **Authentication of Multicast Sources:** Ensure the source of multicast streams is authenticated to prevent spoofing.

- **Group Key Management:** Develop a robust key management system for encrypting multicast traffic, ensuring only authorized devices can join the multicast group.

- **Multicast Traffic Control:** Control multicast traffic at the network level to prevent unauthorized access and ensure that only legitimate multicast data is transmitted.

- **Network Resilience Planning:** Plan for network resilience to ensure the stability of multicast streams against distributed denial of service (DDoS) attacks.

- **Security Policy Compliance:** Ensure that the multicast design complies with relevant security policies and standards, such as those provided by the National Institute of Standards and Technology (NIST).

- **Device Hardening:** Harden IoT devices against attacks by disabling unnecessary services and securing configuration settings.

- **Logging and Monitoring:** Implement comprehensive logging and monitoring strategies for multicast traffic to quickly detect and respond to potential security incidents.

SMART BUILDING PROJECTS BEGIN IN THE MINDS OF TECHNOLOGISTS

The most effective multicast integrations will come as a result of building projects with a master systems integrator (MSI) contributing from the outset. This practice aligns with a foundational shift in the holistic design of smart buildings. Whereas yesterday's blueprints often began in the minds and AutoCAD modules of architects, many of today's innovative building projects are beginning with technologists.

The most successful builds start with networking IT professionals who map out the nodes, switches, and protocols necessary for optimal performance of all things "smart." This initial step empowers architects and other designers to bring a big vision to life without compromising the efficacy of a client's investment in intelligent spaces.

In the fall of 2022, Chuck Wilson, the CEO of National Systems Contractors (NSCA), wrote about the emerging market need for MSIs: "… there will likely come a time when building owners will have so many systems that they want to work with one company that can take sole responsibility for them all."[1]

Mr. Wilson was correct. That time is now. Multicast is but a single example of the innovations these experts will inject into the field, vastly accelerating the reliability, efficiency, and scalability stakeholders expect when they set up a smart building.

AUTHOR BIOGRAPHY:

Akram "AK" Khalis is CEO of MHT Technologies, a smart building technology firm based in New York, and co-founder of MHT's flagship product, Inspextor. AK led the development of Inspextor's advanced smart building automation platform, which is built on a Power-over-Ethernet (PoE) structured cabling backbone. He is also a member of the PoE Consortium. AK can be reached at ak@mht-technologies.com.

REFERENCES:

1. "*Becoming a Master Systems Integrator.*" *National Systems Contractors Association*, 25 October 2022, www.nsca.org/becoming-a-master-systems-integrator