Cambium Networks™

SOLUTION PAPER

IoT Access Solutions Delivered with Security, Scalability, and Simplicity

Contents

Introduction

The Internet of Things (IoT) refers to the global network of physical devices (things) embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. These devices range from ordinary household items to sophisticated industrial tools, enabling a smarter, more interconnected world. IoT has transformed industries by connecting devices, enabling automation, and improving data-driven decision-making.

With the broad adoption and rapid growth of IoT, significant security challenges have emerged, including vulnerabilities to cyber-attacks, data breaches, and unauthorized access. These challenges necessitate robust security measures to protect sensitive data and ensure the integrity of connected devices.

This paper aims to explore how Cambium Networks is recognized for offering robust solutions that address these challenges, ensuring secure and reliable IoT deployments.

IoT Use Cases

IoT is revolutionizing how we interact with the world around us by connecting everyday objects to the internet. This vast network of connected devices collects and exchanges data, enabling smarter decision-making and automation across various sectors. IoT technology is enhancing efficiency, improving convenience, and driving innovation in ways we never imagined. Below are example use cases across different markets:

Hospitality	• Guest experience: Personalized room settings and services for an enhanced guest experience • Operational efficiency: Streamlined and automated check-in/check-out and housekeeping processes • Security: Enhanced guest safety with smart locks and connected surveillance systems
Industrial	• Smart manufacturing and supply chain management: Automated manufacturing processes to increase efficiency and reduce downtime; tracking goods in real time to optimize logistics and inventory • Predictive maintenance and energy management: Monitoring machinery health to predict failures and schedule maintenance; optimized energy distribution and consumption with smart grids and meters
Managed Service Providers (MSP)	• Remote infrastructure management: Monitoring network and server health • Asset management: Device tracking and lifecycle management
Education	• Smart classrooms and enhanced learning experience: Automated lighting, climate control, interactive whiteboards, VR/AR for immersive learning, connected lab equipment, and attendance tracking • Campus safety: Smart surveillance and emergency notification systems • Personalized learning: Adaptive learning platforms and wearables for monitoring engagement and health
Healthcare	• Remote patient monitoring and smart devices: Wearable devices that send vital sign data to healthcare providers; connected devices providing real-time health data and automated treatment • Elderly care management and facilities management: Sensors that monitor health and safety, ensuring timely assistance for elderly patients; tracking medical equipment and monitoring environmental conditions
Smart Cities	• Traffic management and waste management: Sensors and cameras that reduce congestion by managing traffic flow; smart bins optimizing waste collection routes based on fill levels • Public safety and infrastructure: Connected surveillance and emergency response systems enhancing safety; smart lighting and parking systems that improve urban infrastructure efficiency
Consumer	• Smart home and connected appliances: Control of lighting, heating, smart refrigerators, washing machines, smart TVs, gaming consoles, and other appliances remotely for convenience and energy savings; voice assistants that enhance everyday tasks • Wearables: Tracking physical activity and health metrics

12112024

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

IoT Growth

The IoT market is set for significant expansion, fueled by advancements in technology, the widespread adoption of smart devices, and increasing demand across multiple industries. As of 2024, the number of IoT-connected devices worldwide has reached approximately 17.08 billion. This represents a significant increase from previous years, with projections indicating that the number of IoT devices will nearly double to 29.42 billion by 2030 (Exploding Topics). As of 2023, the global IoT market was valued at about $662.21 billion. Mordor Intelligence (Mordor Intelligence) forecasts suggest it will grow to $1.17 trillion by 2024 and $2.37 trillion by 2029. Market Data Forecast (Market Data Forecast) suggests annual growth rate (CAGR) of 26.9% over the forecast period.

Key Factors Driving IoT Growth

- **Advancements in telecommunications:** Improved connectivity through 5G networks enhances the efficiency and reliability of IoT devices.
- **Increased internet penetration:** Broader internet and broadband access enables more devices to connect and communicate seamlessly.
- **Demand for data analytics:** Businesses increasingly rely on IoT data for insights, driving the adoption of connected devices.
- **Security solutions:** The need for advanced security and surveillance solutions is pushing IoT adoption in both consumer and industrial sectors.
- **Industry adoption:** IoT optimizes process through predictive maintenance and real-time monitoring and enhances inventory management.

Regional Insights

- **North America:** Leading in IoT adoption due to robust investment in technology and favorable regulatory environments.
- **Europe:** Significant growth driven by smart city initiatives, sustainable development and Industry 4.0 in manufacturing.
- **Asia-Pacific:** Rapid expansion due to a large population, urbanization, and government initiatives.
- **Latin America:** Moderate adoption driven by growing interest in digital transformation, improving infrastructure and emerging economics
- **Middle East and Africa:** Infrastructure development, government initiatives and increasing investments in technology driving the IoT adoption.

The IoT Security Challenge

The IoT landscape is rapidly evolving, with a significant impact across various sectors. Its implementation ranges from enhancing everyday consumer experiences to revolutionizing industrial processes. The current density of IoT devices underscores its growing importance and the move toward a more interconnected world. However, the proliferation of IoT devices introduces significant security challenges.

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

- **Device vulnerability:** Many IoT devices have limited processing power and memory, making it difficult to implement robust security measures.
- **Data privacy:** The vast amount of data collected by IoT devices can include sensitive personal information, raising privacy concerns.
- **Network security:** IoT devices often communicate over public or unsecured networks, increasing the risk of data interception and cyber attacks.
- **Authentication and authorization:** Ensuring that only authorized users and devices can access the IoT network is a significant challenge.

Onboarding IoT devices involves integrating new devices into an existing network or ecosystem securely and efficiently. This process is crucial to ensure that devices operate correctly and securely from the moment they are introduced.

This process can become tedious when adding IoT devices at scale in the 100s or 1000s of devices especially in a complex network environment. Manually adding individual devices introduces overhead and increases the risk of human errors in specifying the correct VLAN, policies, and other configurations.

ONE Network Solution for IoT

Cambium Networks' ONE Network simplifies the process of securely onboarding IoT devices onto the network and doing so at high scale. With Wi-Fi, switching, security, SD-WAN, and fiber/wireless backhaul solutions working together in an integrated offering, administrators can onboard IoT devices, lock down their security, and enforce appropriate policies network-wide, all while minimizing effort and errors.

Onboarding a device within the Cambium Networks ecosystem is designed to be as seamless as plug-and-play. This means that the system automates much of the configuration and setup process, reducing the need for manual intervention.

IoT Onboarding

EasyPass provides a powerful Wi-Fi access solution, enabling the simple and secure onboarding of all types of users and devices to the network. EasyPass consists of a set of different access or portal types for connecting employees, guests, public and devices of all types. For IoT devices in particular, EasyPass offers a streamlined and scalable process for integrating into the enterprise network.

EasyPass Onboarding

EasyPass Onboarding is the access service type designed for IoT and similar devices that lack screen or browser interfaces. It uses Cambium's Enhanced Pre-Shared Key (ePSK) feature that assigns each IoT device a unique security key which ensures only authorized devices connect to the network. Unlike traditional PSKs that are shared across many devices, ePSKs support per-device authentication which greatly reduces security risk by providing individualized security. This feature is particularly valuable in IoT environments, allowing

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

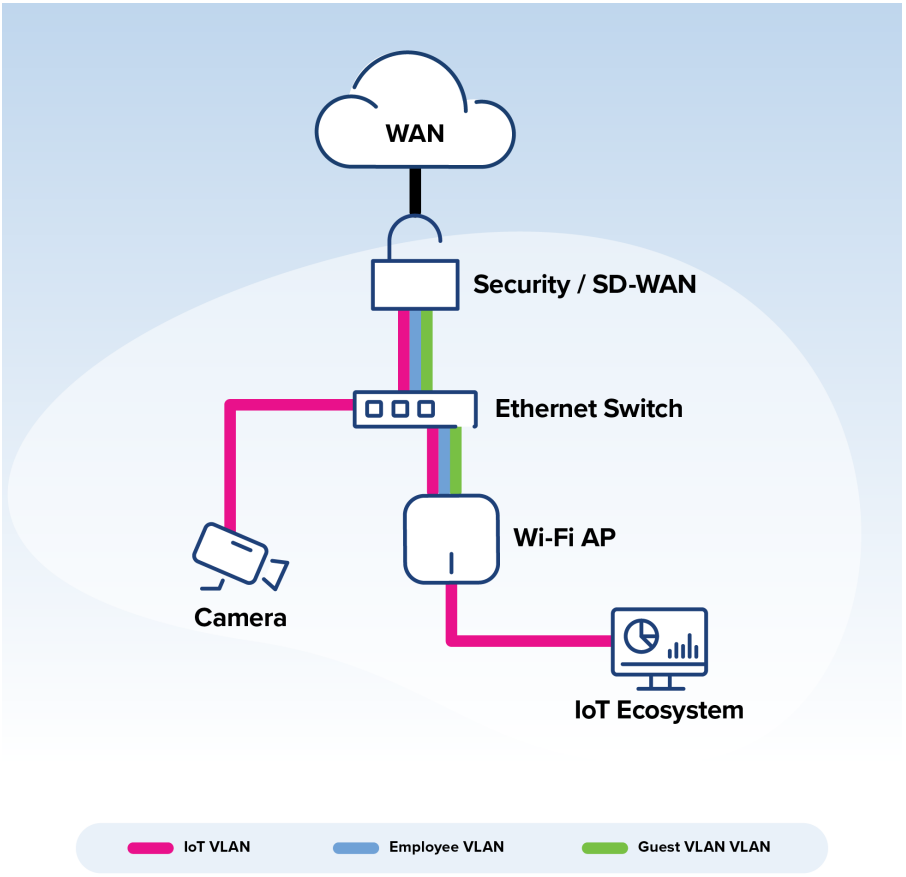
administrators to revoke or modify device access without impacting the entire network.

ePSKs can be generated manually or automatically, providing administrators with flexibility and granular control. EasyPass Onboarding uses the “ePSK Cloud” variation of ePSKs which are managed in the cloud. There are no limits on the number of ePSKs with this approach, offering scalability and convenience for growing IoT deployments. Alternatively, ePSKs can be managed locally on the Wi-Fi access points, a variation called “ePSK Local”. This type has a limit of 2000 ePSKs per network.

Micro-Segmentation and Automation of the Network

In a typical deployment, VLANs (virtual local area networks) are used to segregate network traffic based on user groups or device types. This segregation enhances security and network efficiency by isolating traffic and reducing the risk of unauthorized access.

- **Employees:** Assigned to specific VLANs based on their department or role within the organization. For instance, the finance department might use VLAN 10 (indicated in blue), while the IT department uses VLAN 20 (also indicated by blue).
- **Guests:** Allocated a separate VLAN to restrict their access to the internal network. For example, VLAN 30 (indicated in green) can be designated for guest access, providing them with internet access only.
- **IoT devices:** Assigned to a different VLAN, such as VLAN 40 (indicated in magenta). This ensures that IoT traffic is isolated from both internal staff and guest traffic.



12112024

The policy-based automation (PBA) feature in Cambium's cnMatrix™ switches automates the VLAN assignment with the help of match object and action objects.

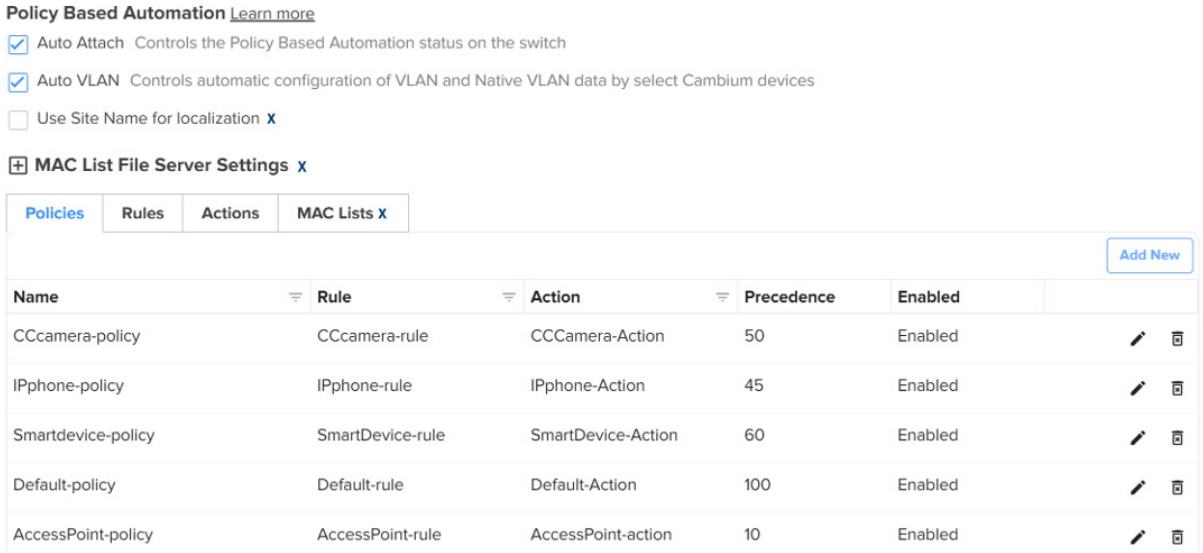


Figure 1: Policy-based automation policies

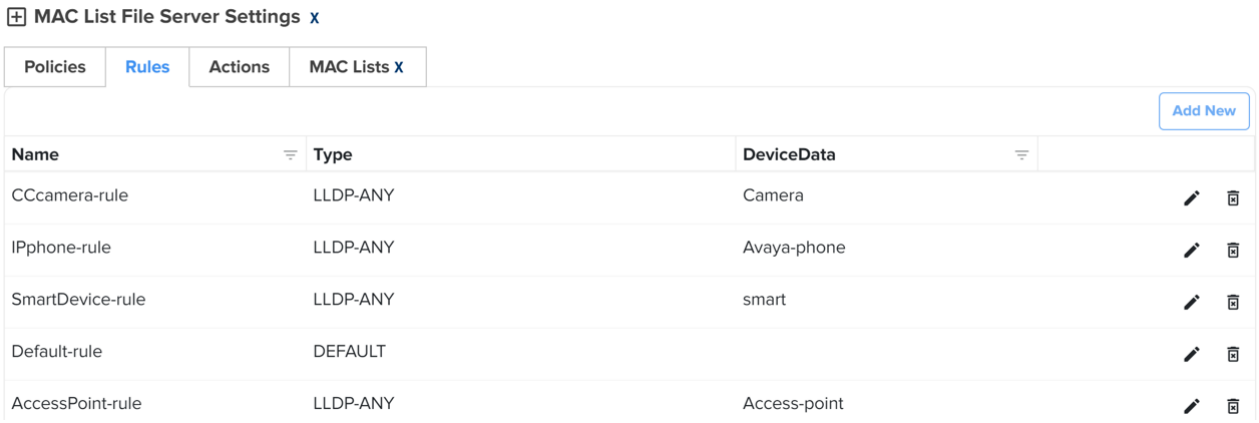


Figure 2: Policy-based automation rules

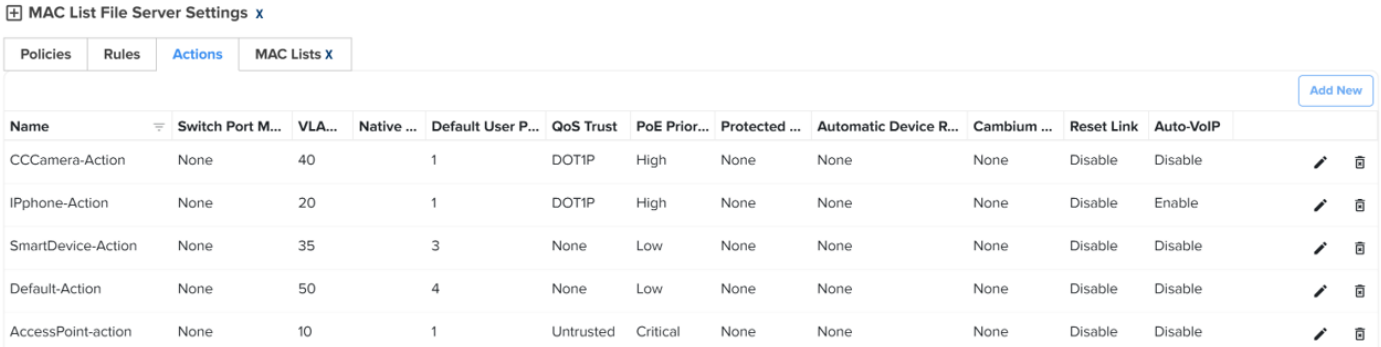


Figure 3: Policy-based automation action

12112024

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

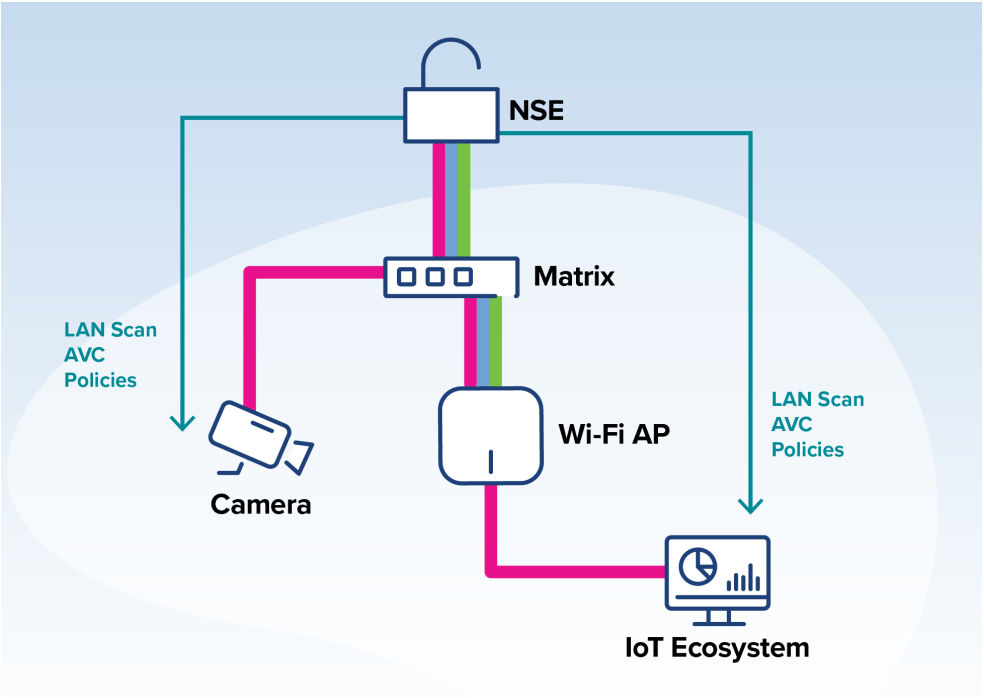
- **Match Objects:** Criteria that identify specific devices or users based on attributes like MAC addresses, device types, or user roles.
- **Action Objects:** The actions to be taken once a match is found, such as assigning a VLAN, applying access controls, or configuring quality of service (QoS).

By segregating traffic through micro-segmentation and applying strict access controls via PBA, the Cambium ecosystem enhances overall network security and efficiency. Internal users can access all necessary resources, guests are restricted to internet access only, and IoT devices are limited to their specific operational needs.

IoT Security

IoT devices typically rely on specific ports and outbound connections essential for their functionality, such as communicating with cloud services or sending data to central servers. However, if these devices are not secured properly, they can become vulnerable entry points for cyber attackers. Hackers can exploit these vulnerabilities to gain unauthorized access to the network, potentially reaching restricted resources and sensitive data.

Network Service Edge (NSE) is a security/SD-WAN solution from Cambium Networks. It is a high-performance SD-WAN and a UTM device that has next-generation firewall capabilities.



12112024

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

NSE enforces policies on IoT devices from layer 3 to layer 7, not only isolating IoT VLAN traffic from other VLANs in the network, but also filtering traffic bound for the internet. Using firewall capabilities, traffic can be filtered based on IP addresses or applications. Geo-IP filtering restricts traffic based on geographic locations.

NSE's application visibility and control feature supports over 2,000 applications, enabling traffic management based on specific applications or categories. With IoT devices, policy enforcement becomes more straightforward because most of these devices require access to specific applications. By creating rules that permit only the required applications and that block the rest, we can ensure that IoT devices make only legitimate connections, thereby, securing the network.

DNS-based content filtering in NSE is an advanced feature known for its high accuracy and reliability. NSE provides this feature with over 80 categories and subcategories, ensuring IoT devices access only the necessary content. It blocks any illegitimate connections generated by IoT devices and helps prevent access to malicious content.

These features protect IoT devices from external threats, but what about threats and vulnerabilities within the same network? Vulnerabilities in IoT devices can allow attackers to access sensitive information. Cambium offers a unique LAN vulnerability assessment that identifies device vulnerabilities and provides detailed reports on each vulnerability, including its severity, exploitation probability, and whether it has been exploited in the wild. Additionally, it offers remediation information.

Typically, LAN vulnerability assessments are conducted quarterly or annually, giving attackers ample time to exploit vulnerabilities. However, NSE performs a LAN scan as soon as a device is connected and then every 12 to 24 hours, maintaining an active and current track of vulnerabilities. This frequent scanning helps to quickly identify and address vulnerabilities, significantly reducing the window of opportunity for attackers.

All Active Vulnerabilities

Apply Filter(s) Export

Severity	Identifier	Known Exploit	Exploitation Probability	Product	Clients Impacted
Major	CVE-2014-0160	Yes	97%	FileZilla ftpd	1
Critical	CVE-2017-12629	No	97%	JBoss Enterprise Application Platform	1
Major	CVE-2014-0224	No	97%	FileZilla ftpd	1
Critical	CVE-2017-12149	Yes	97%	JBoss Enterprise Application Platform	1
Major	CVE-2010-1871	Yes	97%	JBoss Enterprise Application Platform	1
Critical	CVE-2018-7489	No	94%	JBoss Enterprise Application Platform	1
Critical	CVE-2009-0388	No	90%	TightVNC	3
Critical	CVE-2019-9514	No	82%	JBoss Enterprise Application Platform	1
Critical	CVE-2017-7525	No	57%	JBoss Enterprise Application Platform	1
Critical	CVE-2017-7504	No	31%	JBoss Enterprise Application Platform	1

Visibility and Analytics

IoT has been a blind spot in the network industry. With the increasing number of IoT devices being onboarded, visibility into these devices is crucial. Cambium addresses this need with its advanced fingerprinting technique, which identifies IoT devices on the network and provides comprehensive details, including hostname, MAC address, IP address, manufacturer details, device type, operating system, and OS version. This information helps administrators ensure that only authorized devices are present on the network.

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

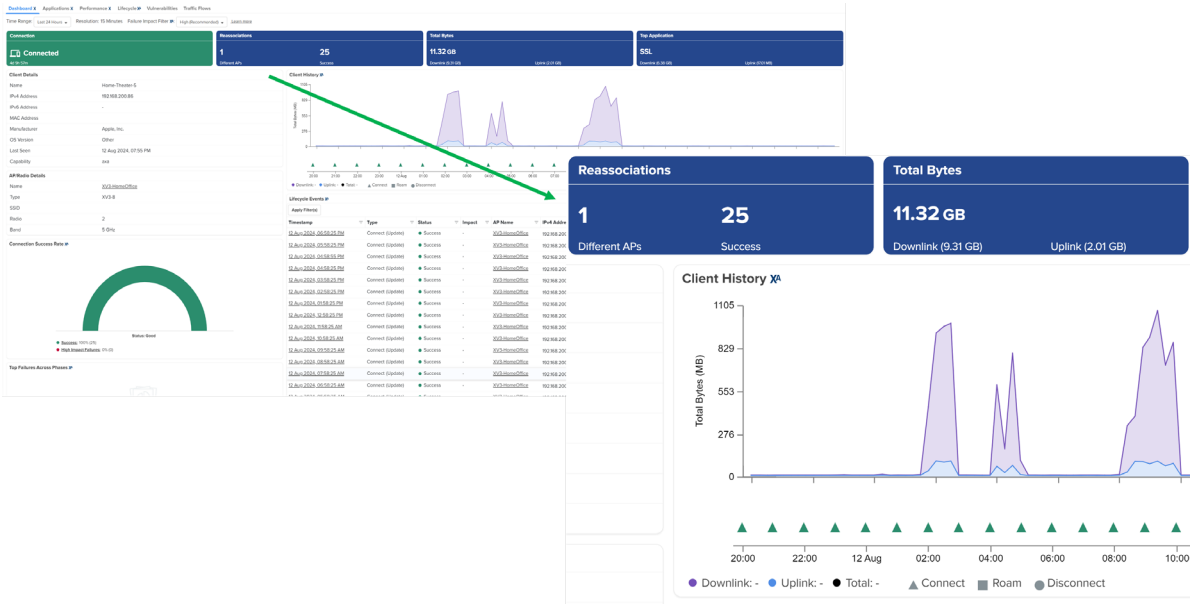
Local Remote

Apply Filter(s)

IP Address	Manufacturer	Device Type	Device OS
192.168.200.86	Apple	MEDIA_PLAYER	tvOS
192.168.200.115	Unknown	TELEVISION	Tizen
192.168.200.116	Sonos	VOICE_CONTROL	Sonos
192.168.200.97	Apple	TABLET	iPadOS
192.168.200.105	Apple	MOBILE	iOS
192.168.200.99	Apple	MOBILE	iOS
192.168.200.149	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.200.148	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.200.146	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.0.50	Cambium Networks	Network Service Edge	Cambium OS
192.168.200.147	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.200.117	Cambium Networks	Enterprise Switch	Cambium OS
192.168.200.125	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.200.112	Cambium Networks	Enterprise Switch	Cambium OS
192.168.200.50	Cambium Networks	Enterprise WiFi Access Point	Cambium OS
192.168.200.90	Apple	VOICE_CONTROL	AudioOS
192.168.200.103	Apple	VOICE_CONTROL	AudioOS
192.168.200.128	Apple	VOICE_CONTROL	AudioOS
192.168.200.93	Apple	VOICE_CONTROL	AudioOS
192.168.200.82	Ring	SURVEILLANCE_CAMERA	Android
192.168.200.79	Harman Kardon	STREAMING_DONGLE	Android

Note: MAC address and device OS version are hidden in the above image for security purposes.

Additionally, Cambium Networks provides detailed analytics and reports on these devices, giving administrators valuable insights into device behavior and network performance.



Device dashboard gives the complete information on the device. Administrators can clearly see how many times the device has reassociated, how long the uptime is, the amount of bandwidth it has used, and the timelines on usage, as well.

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA

The **application tab** gives information about the applications that are accessed, top applications, top category, and timeline on the applications.

The **performance tab** gives complete information on the timeline with respect to RSSI, SNR, data rate, usage, and application usage. (RSSI and SNR will be available if the device is connected over wireless.)

Conclusion

Cambium Network provides a robust solution for managing and securing IoT devices across multiple network layers. By isolating traffic, enforcing detailed policies, and using advanced filtering techniques, Cambium's NSE ensures that IoT devices operate securely and efficiently within the network. This comprehensive approach helps prevent unauthorized access and mitigates potential security threats, providing a secure and manageable IoT ecosystem.

About Cambium Networks

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences and device connectivity with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

12112024

2000 Center Drive Suite East A401, Hoffman Estates, Illinois 60192 USA