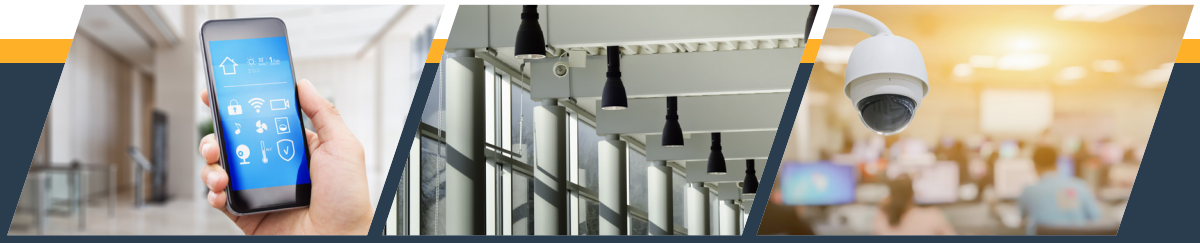
INDUSTRY PERSPECTIVE

CAMPUS TECHNOLOGY



How the Internet of Things Is Changing Campus Wi-Fi

Seamlessly connecting a variety of devices to a single network infrastructure is a challenge. Here are three things to consider.

Sponsored by Riverbed Xirrus

The number of smart devices connecting to the Internet is exploding. This trend has serious implications for how campus technology leaders approach the way they design and manage their Wi-Fi networks.

According to industry researcher Gartner, the number of Internet-connected devices has quadrupled worldwide since 2012. By 2020, there will be an estimated 30 billion devices online, says Gartner—nearly three times the number of humans on earth. The majority of those devices will not be laptops, tablets, or smartphones; but sensors, controllers, and other objects that are part of the Internet of Things (IoT).

Colleges and universities are not isolated from the growth of the IoT. Many institutions have security cameras, thermostats, lighting systems, door locks, and other kinds of devices that are connected and controlled online. And students arriving on campus bring with them a growing number of personal devices, such as printers, smart watches, gaming consoles, and smart TVs.

In October 2016, a massive Distributed Denial of Service attack crippled Internet sites including Netflix, Twitter, and PayPal. The attack spread through millions of unsecured, Internet-connected devices such as surveillance cameras. And it happened because the default passwords for these devices were never changed when they were deployed. To avoid this kind of scenario, campus IT leaders need an easy way to secure the IoT

objects connecting to their networks at scale.

Seamlessly connecting such a wide variety of devices within a single network environment can be a significant challenge. It requires campus IT leaders to rethink the design of their Wi-Fi infrastructure. There are three critical aspects to consider when focusing on network design to accommodate the new array of devices:

1.Scalability: A few years ago, colleges had to supply Internet access for only one or two devices per student. Today, the average college student owns at least five devices that require connectivity, according to Refuel Agency's 2017 College Explorer Market Research Study. As the number of Internet-connected devices grows exponentially, colleges and universities must design Wi-Fi networks that can handle this additional traffic.

A scalable and flexible Wi-Fi infrastructure is critical. For example, multi-radio, high-density access points provide the capacity to handle growing numbers of devices with less equipment. And software-defined radios help campus IT leaders adapt their Wi-Fi infrastructure over time as needs evolve.

To onboard and secure a wide range of device types efficiently within a single, mixed-use network environment, campus technology leaders need an intelligent Wi-Fi infrastructure that automatically identifies smart devices when they connect to the network and provisions them with appropriate security policies based on their device profile.

"If I'm deploying a thousand sensors across my campus, I need to be able to do that easily at scale, not program them one by one," says Bruce Miller, vice president of product marketing for Riverbed Xirrus.

2. Simplicity: A related challenge is easily connecting IoT devices to the network. Devices generally have to be properly configured in order to connect to a Wi-Fi network. To join a Wi-Fi network using a smartphone, for example, your device has to recognize the network to which you are connecting, then you enter a password to log on. One of the key challenges with the IoT, however, is that many devices are "headless," meaning they don't have a screen or keyboard. Campus IT leaders need a way to onboard those devices simply and at scale.

Managing this range of device types with differing requirements can be a significant challenge. Wi-fi access points should contain built-in intelligence that can identify devices by type, manufacturer, and operating system. "When a device connects to the network," says Miller, "we can tell: Is it a laptop? A Fitbit? A Nest thermostat? An iPhone?" The software characterizes the device, authenticates it, and applies the correct policy—all without needing human intervention.

3. Security: Getting IoT devices on the network easily is just the beginning. Campus IT leaders must also ensure the devices are secure and can't be a way for hackers to gain access to network resources. Most IoT objects are built to perform a specific function—and security is often an afterthought in their manufacture. In its 2017 Internet Security Threat Report, Symantec reported many IoT devices can be compromised by skilled hackers within two minutes of connecting.

Implementing a network access control solution that simplifies but does not compromise security is essential for handling the IoT. The ability to lock down access and communication to and from these devices through policies defined by network administrators solves the IoT security challenge, which lets devices operate as they need to without disrupting other network traffic.

IT staff can put all connected thermostats into the same profile with the same limited network privileges, for example. "They all go onto a separate VLAN, with rules created to isolate them from everything else on the network," says Miller. That way, a hacker would not be able to access other parts of the network using those devices.

WI-FI EVERYWHERE

College and university campuses need to deliver fast and reliable Wi-Fi to their students and staff. IT departments need a scalable and affordable way to do this. Every Riverbed Xirrus access point integrates distributed control and application intelligence, delivering utility-grade service and making lives easier for both users and IT staff. Some of the advantages of the Riverbed Xirrus solution include:

- Granular application-based policy control by user, device type, and location.
- Integrated guest/BYOD access control, including Microsoft Azure and Google integration.
- Lower total cost of ownership, with up to 75% less equipment required.
- Software-defined hardware that adapts to changing usage patterns.

FLEXIBILITY IS ESSENTIAL

As the number of devices connecting to campus networks continues to increase, universities need flexible solutions that can address all three of those concerns. They must be able to create secure usage policies for these devices at scale, not just for the personal devices used by students and staff but also the myriad IoT devices connecting to their networks. As more devices come online, it's important for campus IT leaders to have a flexible, intelligent Wi-Fi system that can automatically identify and control a wide range of device types.

"The use cases for different devices are distinct, yet they are all operating together on the same network. They each need their own network policies, levels of access, and security," says Miller. "Colleges and universities need a flexible system to support and manage those use cases appropriately."