Order Versus Chaos In Student Housing

In dense housing, resident-owned wireless routers play havoc with internet quality. Sometimes a gentle reminder to turn off these routers isn't enough.

By Andrew Marshall / *Campus Technologies*

Student-housing residents have a very simple requirement for internet access: It should just work. It should work with any device, and it should work reliably all the time. If it doesn't, they may well move somewhere else.

On the surface, this sounds like a reasonably straightforward problem to solve. The reality, of course, is a lot more complicated.

There are two broad types of student-housing community in which internet access is provided to residents as an amenity – those that provide wired connections only and those that provide both wired and wireless connections.

In the first case, usually in older properties, residents usually arrive with wireless routers they've either purchased new or brought from home. In a typical 200-unit, 600-bed community, that means anywhere from 200 to 600 low-cost, totally unmanaged wireless routers are operating in very close proximity to one another, sometimes separated only by a piece of drywall or plywood.

Student-housing residents may not realize their wireless routers interfere with one another, degrading wireless service in a building.

Even worse, because most of these are operated on the default out-of-the-box settings, most are on the same channels. The result is an overwhelming storm of radio energy, with many routers interfering with one another and drastically raising what we refer to as the noise floor.

Of course, residents don't know this. They see strong, four-bar signals, and they believe the wireless is perfectly good because they're getting four bars. However, internet performance is pathetically slow (because of the high noise floor and interference, but they don't realize that), so they conclude the property internet service is defective – even though the wired service may be perfectly good.

The only way to fix this problem is to install a competent, enterprise-grade, dense, well-engineered wireless network. This brings us neatly to the second category of properties, those that provide wired and wireless internet networks for their residents.

MANAGED WI-FI NETWORKS

To be clear, a wired and wireless network isn't the kind cable modems provide. This article refers to engineered, professional, enterprise-grade, managed wired and wireless networks – the definitive standard for purpose-built student housing. In some student housing served by cable companies, a cable modem is installed in each unit, sometimes with Wi-Fi attached. This approach rarely, if ever, works to the standards student residents demand, and it is not considered in this article.

However, even if a student-housing property provides a wired and wireless service for residents, and even if the network is well designed and engineered and uses enterprise-class components, and even if it's managed, the property can still experience death by router.

Consider this example: A community starts with a wired network in which residents install their wireless routers. The owner now invests in a great managed wireless solution and has it installed and commissioned. The internet service is still awful.

Why? Because all the residents still have their own routers, only now, in addition to a few hundred resident-owned wireless routers, there are a couple of hundred managed wireless access points, and the noise level is deafening.

The obvious solution is to contact all residents and tell them to turn off and remove their devices. The problem is that the response to that request will be limited. The property network is barraged with interference, and it won't be fully reliable or stable, so residents put their own routers back.

This can be a very labor-intensive, frustrating problem to try to resolve. First you have to identify the interfering devices, then you have to make sure they're on your property and not next door. Then you have to identify which units they're in, contact the residents of the unit and try to persuade them to remove their routers.

AVAILABLE TOOLS

But wait, aren't there any technical tools to help?

Yes, there are some generally available tools. Most widely deployed enterprise-grade wireless management platforms, such as those supplied by Ruckus and Extreme, have tools to assist in identifying and approximately locating interfering devices. (These are frequently referred to as "rogue" devices.) The better management systems also attempt to work around the interference as best they can by changing channels and signal strength, but this is not a complete solution to the overall problem.

> The FCC doesn't look kindly on interference with wireless networks – but Campus Technologies found another way to deal with rogue wireless routers.

In addition, some management platforms have tools that allow a legitimate property wireless access point to issue messages to clients of rogue wireless devices that cause them to drop their connections. These tools aren't completely foolproof, and some recent litigation has made their use an extremely risky strategy. In 2014, Marriott Hotels settled for $600,000 a complaint brought by the FCC that it "interfered with and disabled Wi-Fi networks." Using over-the-air techniques to suppress rogue routers thus appears to conflict with FCC rules.

To solve this problem, therefore, technical and property staff must contact each resident multiple times and hope to persuade them to disconnect their rogue devices. This is time-consuming, frustrating and often not completely successful.

For student-housing technology providers, this is a tough problem. It has to be tackled, but it is very difficult and expensive to work through.

A NEW SOLUTION

At Campus Technologies Inc. (CTI), we may just have come up with a solution.

CTI has worked through many deployments in which we needed to deal with a rogue router problem, and over time we developed a set of best practices – but that wasn't enough. We had to have a better tool in our arsenal.

So CTI's in-house engineering team designed a module that could be installed in our gateway appliance (which is installed in every CTI managed network) and render all wireless routers on the network inoperable in a way that is completely legal, safe and nondestructive. This rogue suppression module can be turned on and off at the flick of a switch.

Because CTI's rogue router suppression system does not operate in the wireless domain, it does not interfere with Wi-Fi networks. However, turning on rogue suppression prevents anyone at the property from using an unauthorized wireless router. The propertywide network is unaffected and continues to work normally.

The best practice for using the rogue suppression system is the following:

- Check whether there are any rogue routers, then email or notice all residents that they need to remove their routers and switch to the property network.
- A few days later, repeat the first step.
- Turn on router suppression.
- Follow up with another email or notice.

CTI estimates that, in general, using this technology can cut the cost and effort to fix a rogue router problem by around 90 percent. This tool has been deployed in several student-housing communities over the last six months and will be deployed as standard in all CTI-managed networks going forward. ❖

Andrew Marshall is CEO of Campus Technologies Inc., which designs, deploys and manages networks in student-housing communities. Router Suppression technology is a proprietary product of Campus Technologies Inc.'s engineering labs and was designed and developed entirely in the United States. For more information, contact Katarina Shineleva at kshineleva@campustech.net.