Network Security in the Multifamily Environment

LEO and Security

We take network security seriously, but we also understand the need for our end-users (residents) to have a simple onboarding process. We employ an array of technologies to deliver our services, however, will be focusing on two specific technologies for the purposes of this whitepaper: Dynamic VLANs (DVLAN) and DSPK.

We want to keep each resident secure and keep them isolated from other users on the network, however, ultimately the resident must use common sense to protect themselves from Internet exploits such as Ransomware, Malware and phishing schemes.

What is a VLAN?

A virtual LAN (VLAN) is a LAN that is logically partitioned to isolate network segments at the data link layer (L2). Most enterprises use VLAN's to separate different types of traffic (public vs private) or users within the LAN (departments, buildings and floors). Today, most service providers use 1-3 VLANs to segment the traffic on their switched Ethernet deployments (office/vendor/resident). While VLAN's are the building block for a great network, most service providers stop short.

All end-users/residents on the same VLAN can "see" each other. In residential environments, that means that a resident in Apartment 201 can potentially access the AppleTV in Apartment 401. Specifically, all traffic within the VLAN can be sniffed and analyzed by setting a device in probe mode to capture all the unencrypted traffic. Luckily most web content providers are moving to using SSL in all interactions (e.g. https). Google, Facebook, Apple and Microsoft require that all traffic corresponding to inherently unsecure applications like email be protected by SSL. That stated, there are still a lot more out there that people can see and ultimately compromise.

Our solution to this problem is the use of Dynamic VLANs which add an extra layer for security while also improving the overall experience.

What is a DYNAMIC VLAN?

Dynamic VLANs (DVLAN) are VLAN's that are dynamically allocated and deployed by a central management system (typically MAC based) based on a new (or unforeseen) need. Conversely, Static VLANs are statically allocated and implemented ahead of time based on a known need. Static VLAN's are the most common type of VLAN used today. The DVLAN solution will allocate and deploy a VLAN to a device based on criteria established by the administer. Most switched Ethernet deployments can handle up to 4,000 DVLAN's.

DVLAN Features and Benefits

We assigns DVLANs based on unit number so that only end-users/residents within a specific unit can see the other residents within said unit versus a static VLAN which likely encompasses all residents on a floor or building. The end user devices within a specific unit can see each other so HP Printers, AppleTV, Chromecast and a variety of other consumer devices can operate the way they were intended for the mass market. These DVLAN

groups reduce the overhead on the Ethernet switched network and ultimately provides a better, faster service. The networks within each unit are compartmentalized and therefore more secure which is better for everyone.

What is DPSK?

Most enterprise network managers believe that simply deploying a single pre-shared key or password to gain network access is not secure enough for their business. Service providers and vendors created a new onboarding methodology that mirrored the benefits of 802.1X/EAP with the user-friendly dynamic pre-share-key (DPSK). With DPSK, end-users/residents receive their own specific password to access the network instead of using an open network or a common password that is less secure. This unique resident passcode works in their apartment as well the as the amenity and common areas, allowing for a more seamless and better user experience. The credentials are centrally managed by the service provider and can be easily deployed to provide a secure wireless experience for the end-user/resident.

The following list summarizes the features & benefits of DPSK:

- More secure – Each tenant has their own passphrase that can be used globally across the community
- Easier to manage large number of users – people leave – credentials can be disabled and PSK does not need to be shared out again
- The WPA2 secure wireless session is a single session vs everyone on the same PSK. The credentials bind a key that makes that single session more secure.
- Central database of credentials – allows users to access the network wherever designated service is offered (sister properties, extend into retail spaces etc.)

Summary

We must blend of a variety of enterprise grade technologies to provide a better multifamily Internet experience. Network security is paramount and using tools like DVLANs and DSPK, as well as others, allows us to provide a great experience while maintaining the integrity of the network.