The What and Why of Converged Networks for Hotels

AUTHOR

Richard Wagner

Director of Certification and Compliance at Nomadix

Building to support property and guest technology, now and into the future

**TV Casting … Television over IP …
the Internet of Things….**

Onboarding new solutions onto traditional networks has built-in cost and complexity - each time you add a new technology, you have to dig deeper into your pocket, find ways to knit together different hardware – sometimes even build a whole new network.

But with new technologies coming online all the time, and with high-speed, always-on, hotel-wide Wi-Fi a minimum requirement, how do you cost-efficiently keep up with the expectations of your guests, staff and the requirements of IoT, now and into the future?

Converged Networks remove the challenge of constantly building and reequipping networks for new applications by creating one seamless and scalable network for the needs of today – and the unknown needs of the future.

Here's how.
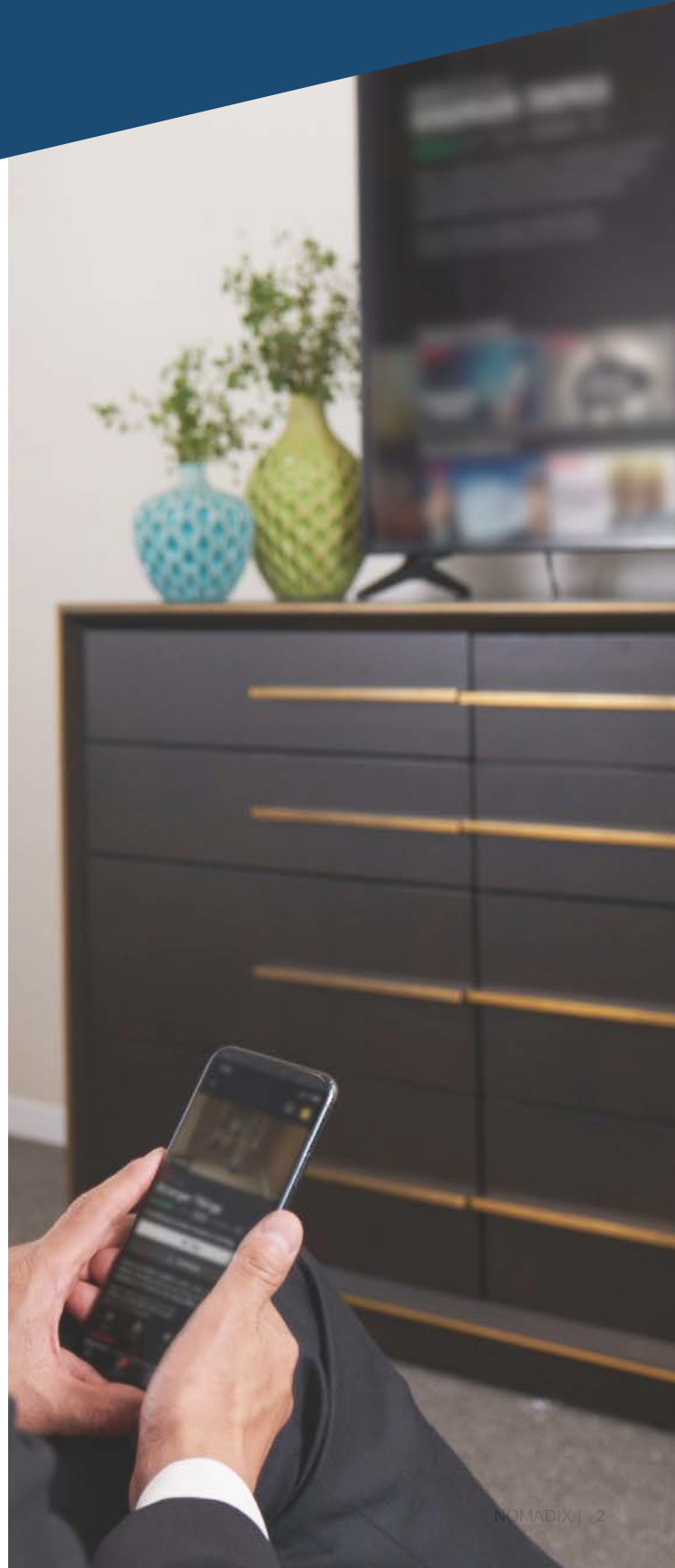
What … is a Converged Network?
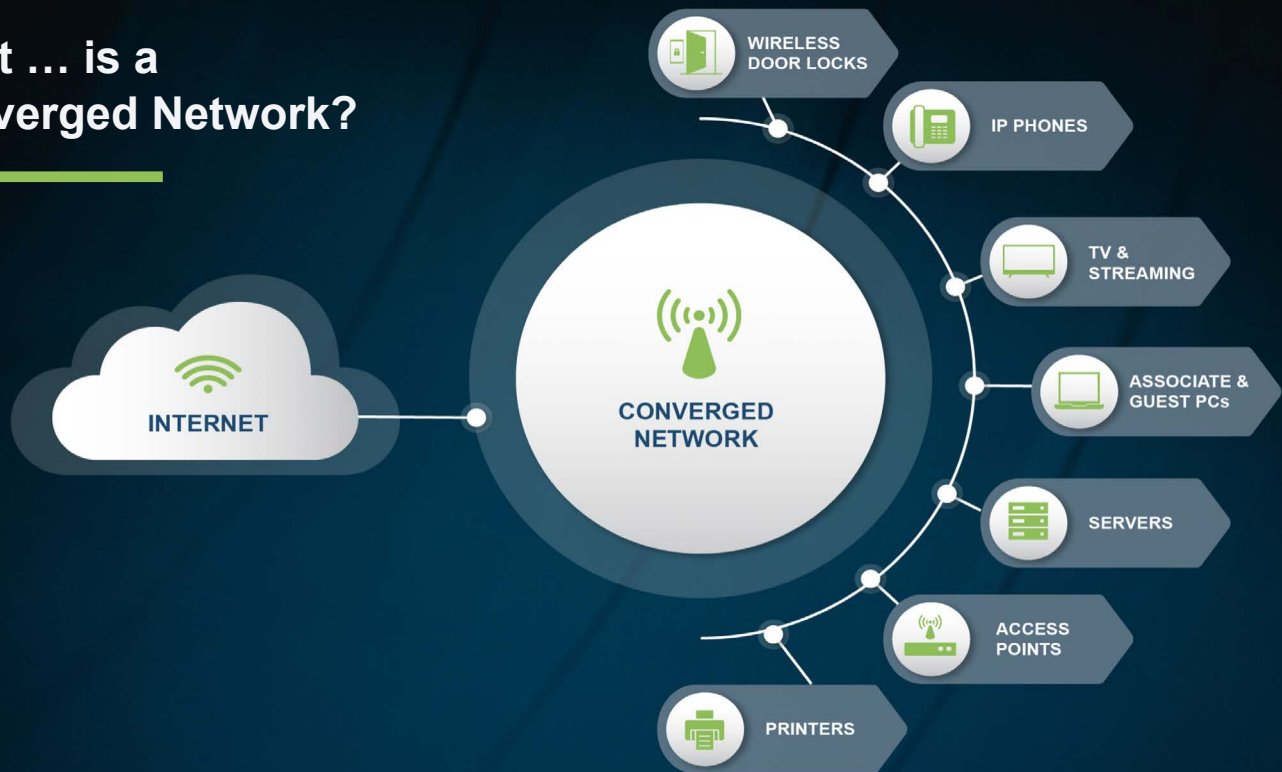
A converged network is one in which all communication requirements are delivered by a single integrated network. With no need for separate networks, guest services, back office, voice, data, streaming and more are all delivered in a single, efficient and seamless package.

A key feature of converged networks is that all categories of hardware components are supplied by a single manufacturer – single-supplier switches and single-supplier access points (AP) in the case of an Ethernet switched network, or single-supplier Passive Optical Network (PON) equipment and single-supplier access points in an Ethernet PON.

In a network designed for convergence, hardware compatibility issues become a thing of the past.

In terms of cabling, too, a standardized approach means a reliable, controllable service:
*   An Ethernet switched network needs a single set of horizontal and riser copper cables.
*   An Ethernet PON needs a single set of horizontal and riser Fiber cables. Optionally, a single copper cable could be used to connect to guest room equipment, such as an AP.

For optimum performance, a single management platform, preferably cloud-based, is required to optimize the management interface for converged networks.

In a standard network design, traffic segmentation is achieved by VLANs and policy routing, security by firewalls and Access Control Lists, plus standard reporting and network auditing features.

Why … a Converged Network?

A converged network future proofs your network; there's nothing that can't be added to the network with minimal disruption, and you won't need to redesign your solution to do it.

Having hardware from the same suppliers means the network is easily scalable, reduces the need to refresh network components and ensures time-efficient upgrades are achieved across the network. Centralized management lowers costs, enables deployment of bandwidth based on specific hotel requirements and maximizes Wi-Fi access for multiple users and applications.

With less overhead due to network costs and issues, you can focus on faster deployment of new technologies and applications, satisfying ever-changing and ever more sophisticated guest and property requirements.
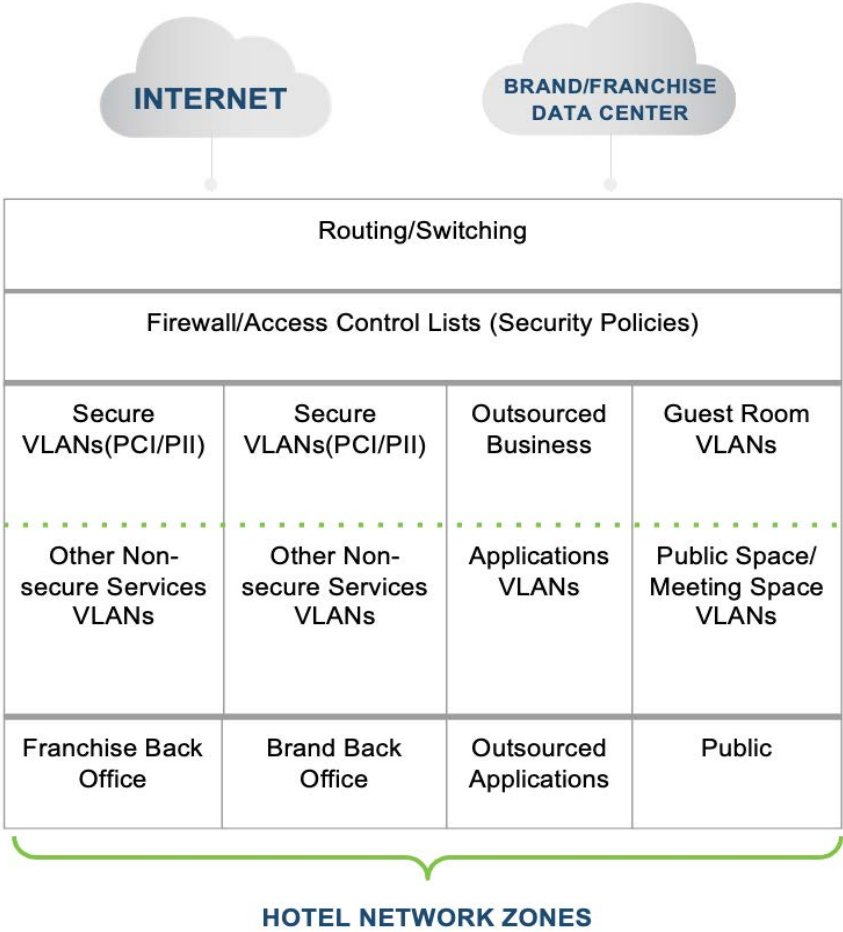
Security policies are easily enabled and adapted via segmentation and authorization (for example, PCI compliance).

How … is a Converged Network Organized?

A typical converged network hotel can be divided into the following network zones.

VLANs are used for application segmentation in this example.

INTERNET

BRAND/FRANCHISE DATA CENTER

Routing/Switching			
Firewall/Access Control Lists (Security Policies)			
Secure VLANs(PCI/PII)	Secure VLANs(PCI/PII)	Outsourced Business	Guest Room VLANs
Other Non-secure Services VLANs	Other Non-secure Services VLANs	Applications VLANs	Public Space/ Meeting Space VLANs
Franchise Back Office	Brand Back Office	Outsourced Applications	Public

HOTEL NETWORK ZONES

Which Applications Can Use a Converged Network?

Any or all of the following applications can become part of a converged network. This isn't an exhaustive list - there's no limit to what can be supported:

Application Category	Example Applications
Networking (outsourced)	Network switches, PON, Wireless, Firewall
Networking (internal)	SD-WAN, Network switches, PON, Wireless, Firewall
Telecommunications	PBX, Voicemail, Call Accounting, Cloud IP Telephony
Facilities – Building	Door Lock System, Access Control, Elevators, Energy Management
Facilities – Guest Room (outsourced)	Thermostats, Safes, IPTV, Minibar, Casting, IoT
Facilities – Guest Room (internal)	Thermostats, Safes, IPTV, Minibar, Casting, IoT
Facilities – Back Office	Surveillance, Fire & Safety, Access Control, Associate Alerts, IoT
Operations (outsourced)	PMS, POS, SPA, Gold
Operations (internal)	PMS, POS, Reservations, Server, PC & Mobile Device Management

...Any Challenges?

Clearly, property types and sizes will vary, along with hotel construction. Some of the challenges this may present include:

- Limited-service hotels may have less budget than Full-service or Luxury hotels. Yet, even smaller hotels can benefit from convergence on a smaller scale.

- Historic buildings converted to hotels can create deployment challenges. Cost-effective ways can still be found to optimize networks.

Franchise owners may support multiple brands with differing brand requirements.

Greenfield Sites are usually preferable to Brownfield Sites because Greenfield allows easier deployment of converged infrastructure (via new fiber and copper). Brownfield can sometimes limit the deployment of converged infrastructure. Decisions may need to be made about how to cost effectively deploy new network infrastructure components.

Application deployment requirements may vary based on corporate standards, or country and government requirements. For example, China typically requires a separate network for country passport review.

Corporate brand standards may restrict use of fire and safety as well as surveillance on a converged network. This can mean a customized network for these applications.

Satisfying ever-changing security requirements may or may not be a challenge and depends upon the brand requirements and the design of the converged network. The latter challenge can be alleviated if the converged network is segmented effectively at the design stage.

None of these challenges is insurmountable – a small amount of customization to meet these challenges does not take away from the overall advantages of convergence.

Hotel Application Mapping

Prior to implementing an application into a converged network, you'll need to perform the following mapping process:

Application	Cloud Outbound Connectivity	Back-Office Connectivity	Dedicated IP Segment Connection	Remote Management Connectivity	Specific Security Requirements
Specific Application	Y/N	Y/N	Y/N	Y/N	Specify

For example, a mapping for a Casting application might look like this:

Application	Cloud Outbound connectivity	Back-Office Connectivity	Dedicated IP Segment Connection	Remote Management Connectivity	Specific Security Requirements
Casting	Y	Y (if interfacing with PMS)	Y (requires use of guest and isolated network segment)	Y	Casting proxy server wireless network must not have client isolation turned on

Hotel Application Mapping

Example 1: TV Casting

Casting is the ability to cast movies, videos and photos from streaming-enabled applications to Android and Apple devices:
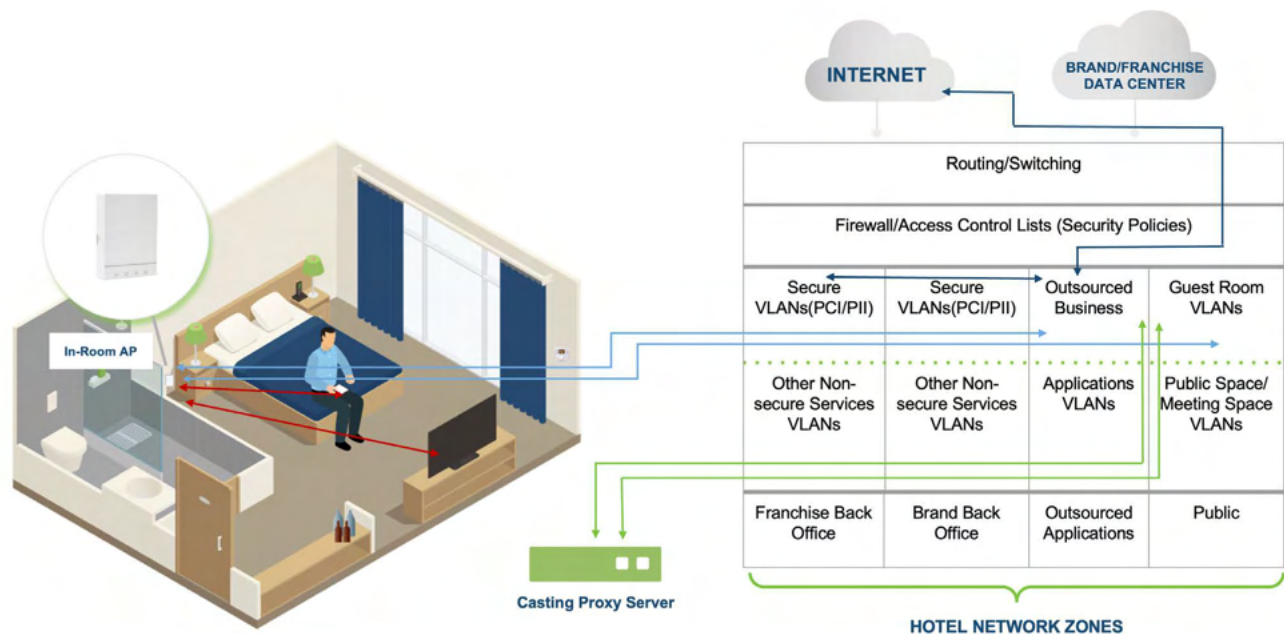
In this example, all in-room APs would already have the guest SSID (and associated VLAN) configured.

To support casting, a second SSID (and a different VLAN) would need to be configured on all the in-room APs.

The guest SSID would already be configured to access the internet. In addition, the casting SSID would also need to be configured for internet access.

In addition, the Casting Proxy Server would need to be connected to both the Guest and Casting VLANs.

Finally, for the Casting Proxy Server to be connected to the cloud-based casting management portal, a VPN tunnel would be configured between the Casting Proxy Server and the cloud management portal.

Hotel Application Mapping

Example 2: IPTV

IPTV (Internet Protocol television) provides television programming and other video content using the TCP/IP protocol (as opposed to broadcast TV, cable TV or satellite signals).

Local programming is received through an antenna on the property roof and combined with other TV content over the IP-connected TV.
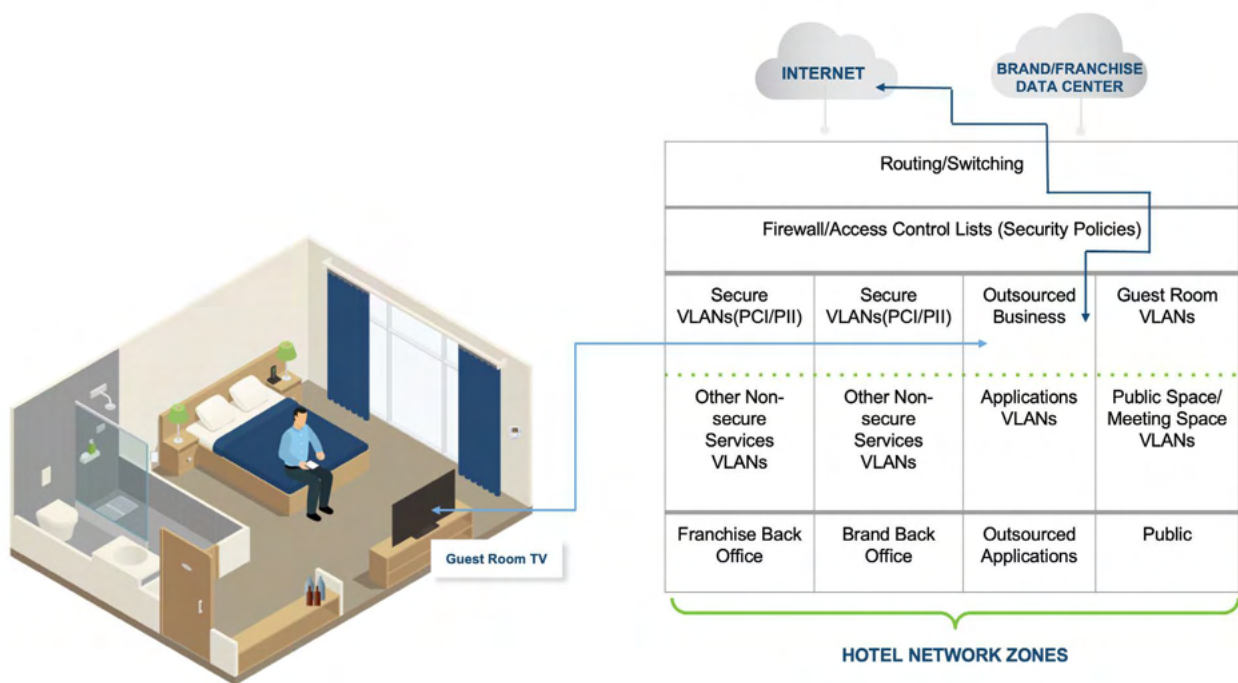
In this example, an IPTV VLAN (or multiple IPTV VLANs) must be configured in the Outsourced Applications Zone.

Each of these IPTV VLAN(s) must be configured for full internet access.

Next, each guest room TV needs to be connected to an IPTV VLAN via either a wired or wireless connection.

Hotel Application Mapping

Example 3: Cloud Telephony

Cloud Telephony or cloud-based PBX provides a hotel with a cost-effective replacement option for an aging, on-site PBX solution, while providing the on-demand communication capabilities that today's guests need.
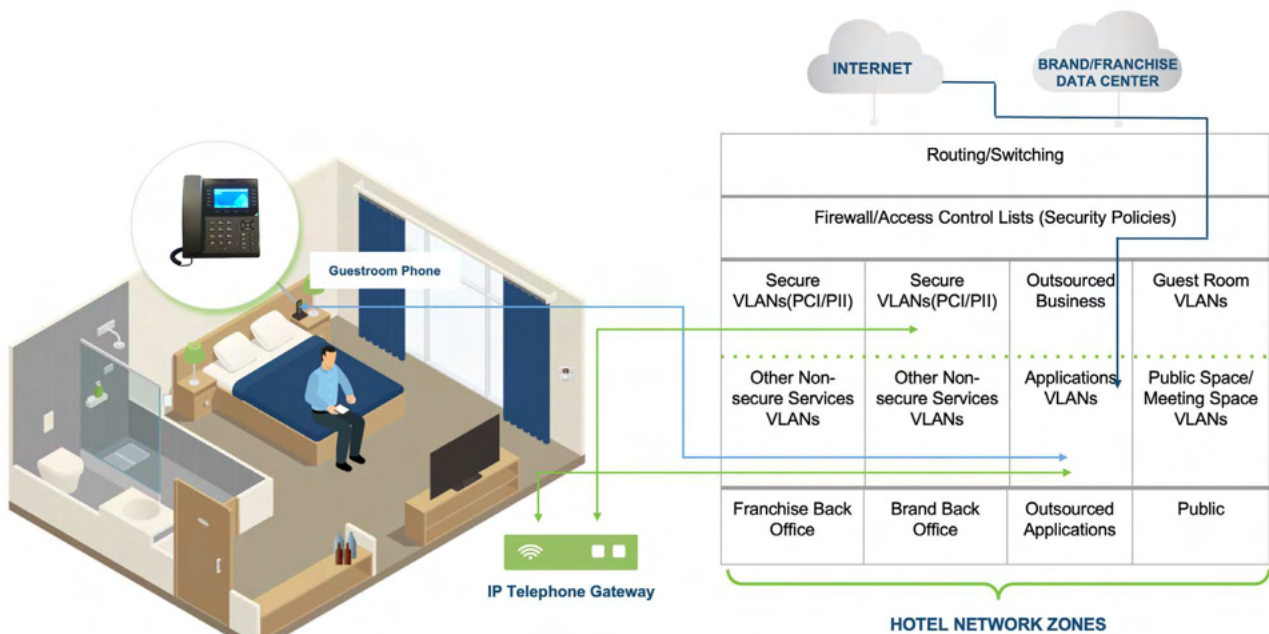
In this example, an IP Telephony VLAN (or multiple IP Telephony VLANs) must be configured in the Outsourced Applications Zone.

In addition, if an IP Telephony gateway needs to be deployed, the gateway needs to be connected (via a VLAN) to the Brand Back Office Secure zone, to allow it to connect to the property's property management system (PMS).

The IP Telephony Gateway also needs to connect to the IP Telephony VLAN(s), in order to connect the IP Telephone to the cloud controller.

Hotel Application Mapping

Example 4: Hotel Staff Safety

A staff panic alert device is a notification solution that provides increased safety to hotel staff that could be subject to threats and/or harassment.

**Some devices also monitor the health of the hotel's Wi-Fi.**
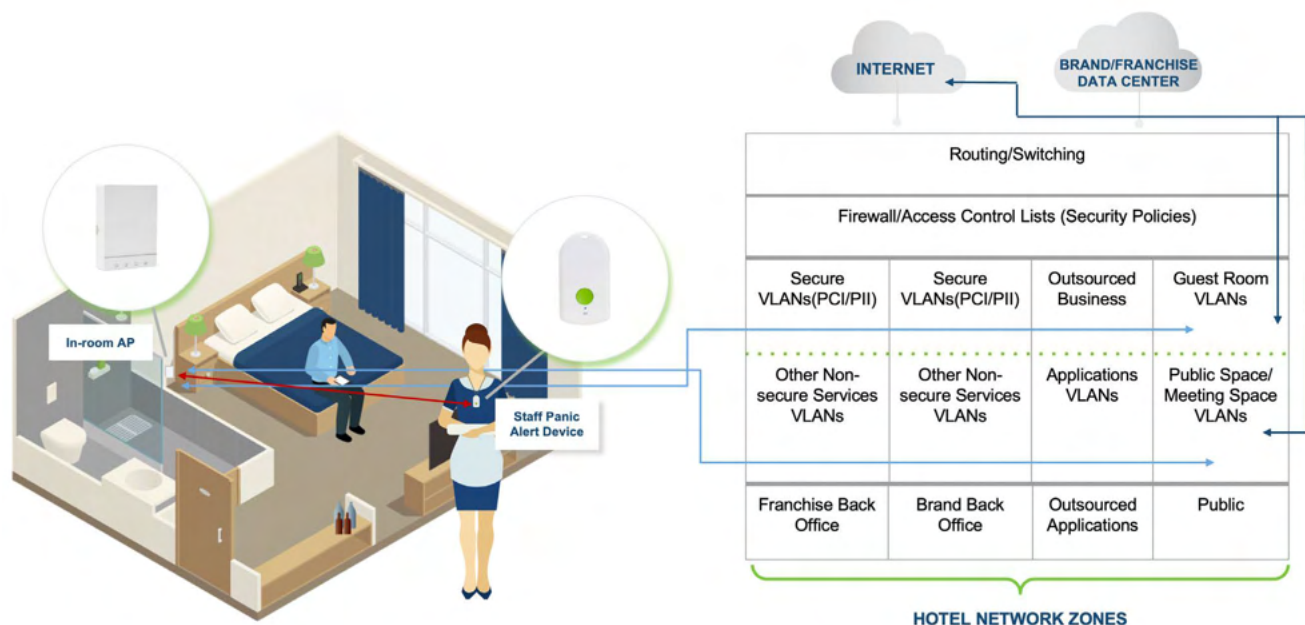
In this example, all in-room APs as well as other public facing APs need to be configured with an SSID that will be used for monitoring. (The guest SSID can be used for this.)

Where a new SSID is configured, this SSID must have full access to the internet.

Each of the panic alert devices must also have access to locally installed Bluetooth beacons, where Bluetooth is used for location finding.

# Hotel Application Mapping

Example 5: Wi-Fi Authentication
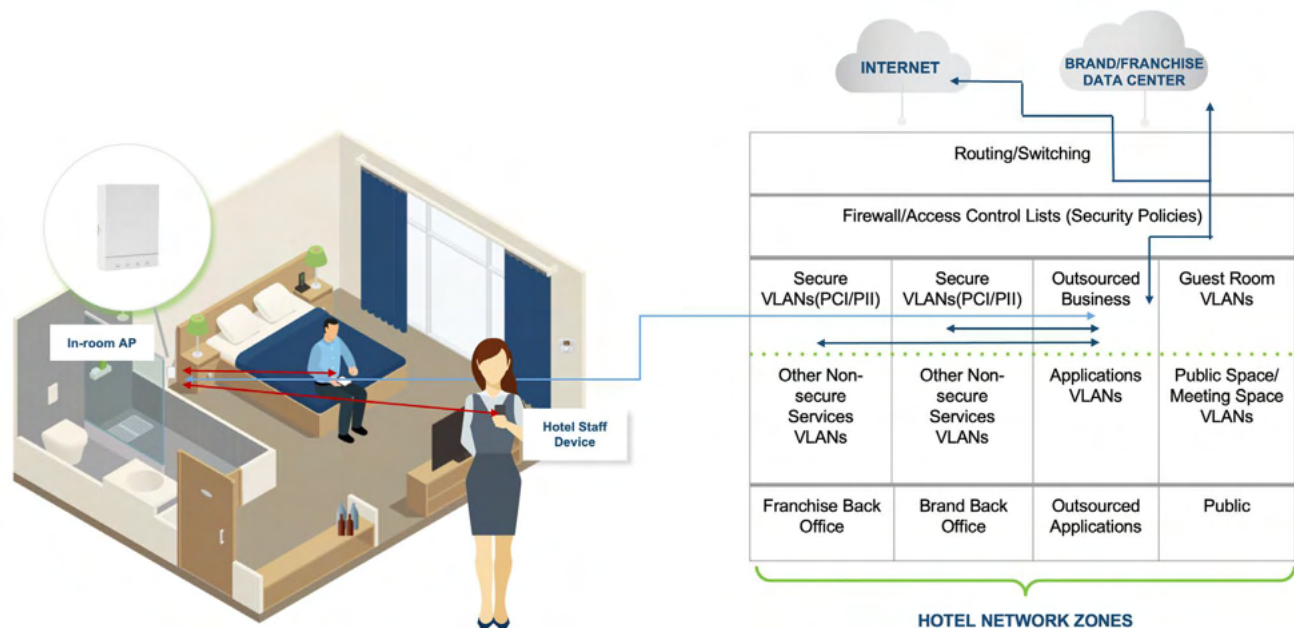
A number of authentication protocols could be used in a converged network. The best fit, however, is the Passpoint standard, as it provides a seamless roaming capability using device-installed profiles, while maintaining a secure Wi-Fi connection. In order to enable Passpoint, all in-room APs, as well as other public facing APs, need to be configured with an SSID that supports Passpoint authentication.

The authentication source would typically be a centralized, cloud-based authentication service. However, the authentication may also require PMS authentication for hotel staff.

Hotel Application Mapping

Example 6: IoT

The Internet of Things (IoT) is the collection of electronic components and devices that can be connected via internet protocols to create a holistic ecosystem. These IoT devices typically provide a combination of computing, sensing and controlling capabilities.
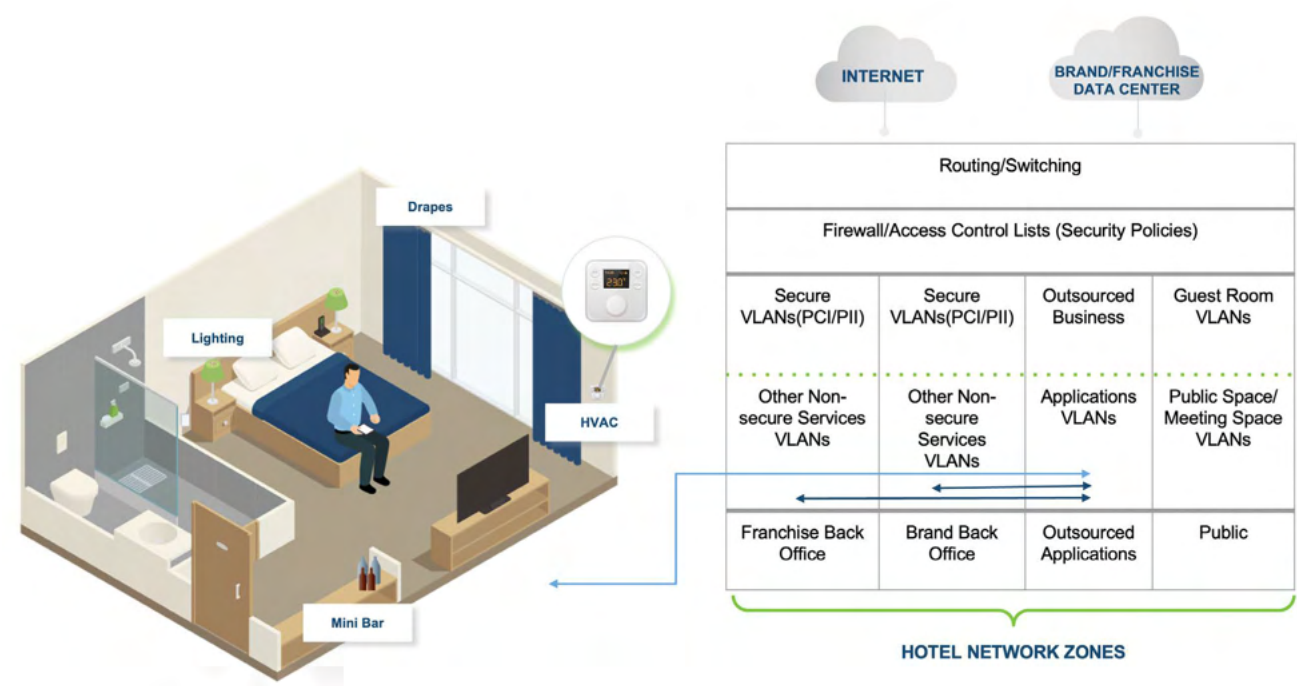
In this example, an IoT gateway is required to manage the traffic between various IoT devices. Because different IoT devices may require different protocols, additional gateways may be required for IoT traffic management.

Each of these gateways would need to connect to specific VLANs in the Outsourced Applications zone, as well as connecting to the internet.

Finally, for some applications (e.g., door locks and thermostats), a connection between the Outsourced Applications VLANs and the back-office VLAN would need to be configured. This would enable the IoT devices to query the PMS for guestroom information.

Want to Know More…?

Richard Wagner will be speaking about this topic at The Hospitality Show

June 28, 2023 | 2:25 PM PT

The HTNG Workgroup

The expansion of new technologies and services is pushing hotel networks and associated infrastructure toward a requirement for a converged, ubiquitous hotel network which may result in expensive retrofits, lost business capabilities and potential hotel opening delays.

To address this issue, the HTNG Next Generation Technology Infrastructure Workgroup was initiated to create a simplified reference network design and infrastructure that converges multiple networks to support the current and anticipated future services of a hotel. The workgroup has completed a whitepaper and will be presenting the high-level results of this effort at the Hospitality Show via a panel of some of the workgroup's participants.