Enterprise Network Design

Case Study

On

Networking for Five Star Hotel

By

Amrish Sanjay Tembe (T-16-0029)

Swaraj Sadanand Shinde (T-16-0085)

Tanvi Anil Sawant (T-16-0083)

Under the Guidance of

Prof. Atul B. Yadav

Associate Professor, IT Department, FAMT

Department of Information Technology

Hope Foundation's

Finolex Academy of Management and Technology

Ratnagiri, Maharashtra-415639

OCTOBER 2019

CERTIFICATE

This is to certify that the Project Entitled “Networking for Five Star Hotel”

Amrish Sanjay Tembe (T-16-0029)

Swaraj Sadanand Shinde (T-16-0085)

Tanvi Anil Sawant (T-16-0083)

Submitted to the University of Mumbai in partial fulfilment of the requirement for the Network Design Lab.

Signature: ----------Signature: ----------

Prof. Atul Yadav	**Dr. Vinayak Bharadi**
Assistant Professor,	HOD, Assistant Professor
IT Department, FAMT	IT Department, FAMT

Date:

Place :Finolex Academy of Management and Technology.

This Case study entitled **Networking for Five Star Hotel**

By,

Amrish Sanjay Tembe (T-16-0029)

Swaraj Sadanand Shinde (T-16-0085)

Tanvi Anil Sawant (T-16-0083)

Is approved for the subject of ***Network Design lab.***

Examiners

1.Signature: ----------

Name:

2.Signature: ----------

Name:

Date:

Place: Finolex Academy of Management and Technology, Ratnagiri

Index

Introduction

Today, technology has the power to impact every aspect of your hotel's operations and your guests' experiences. The network should be able to support traffic when the hotel is at full capacity during an event, However, because media headlines are often filled with reports about data breaches and cyber-attacks, security remains a concern and a barrier for many hotels.

One of the biggest challenges of hotels today is keeping the in-venue experience more compelling for guests. The efficient networking is the topmost concern in order to increase the guest experience. The network should satisfy the basic requirements in order to provide efficient networking including availability, efficiency (Bandwidth), performance. The networking control should be easy to use for the hotel owner. That is the network should be easy to control for the non-technical person.

The current networking present is tedious to control for non-technical user. The control of the network is controlled by the network provider. So, the dependency over the provider increases resulting into increased maintenance cost.

1. Prepare Phase

1.1 Organizational Goals: -

- A highly scalable, single network architecture designed specifically for events and entertainment venues.
- Allow guest to continue their typical online activities, such as streaming movies, participating in a video conference call for work, or uploading vacation photos on social media.
- Increase operational efficiency through staff communication and collaboration. Accommodates all aspects of your business: Integrated communication and collaboration, mobile services, safety and security.
- Hotel Wi-Fi solution, which provides a single converged Wi-Fi platform for guest, employees and operations.

1.2 Network specification required: -

- **Hierarchical in design:** Collapsed core-distribution and access layers
- **Resilient:** Redundant switches and redundant load-sharing, and high-speed uplinks
- **Modular:** Functional areas divided into service blocks with dedicated resources and redundant connections to the network

- **High-performance:** Network bandwidth and capacity designed to withstand node or link failure, with load balancing and redundancy
- **Higher profitability**: Effective network design optimizes investments in capital-intensive assets, lowers operational costs, and helps to reduce working capital in the supply chain while maintaining the targeted customer service.

1.3 Networking Requirement

• All the rooms must include installed computer systems.
• The computers in all the rooms should have the internet connection.
• The swimming pool area and lobby must have the wireless access to the internet.
• It is also required that Conference room must have wireless internet with the accessibility of Video conference.
• The hotel must ensure the free internet facility and accessibility to the guests in the rooms.
• The computers should have installed the appropriate security software.
• The hotel management staff and the guests should be on different networks.
• There are total of thirteen users on the hotel management who need computers.
• A hotel management server must have separate setup for the use of hotel management staff which should not be accessible by the guests.
• There should be secured wireless access in the lobby and swimming pool area.

1.4 Technology Used: -

Video delivery

- Vision Director
- Digital Media Player
- Encoders, transcoders, and receivers (dependent on video feeds)
- Switches (video distribution switches)

Voice services

- Cisco Unified Communications Manager 8.6 (2a) or 9.1(2)
- Cisco Unified IP Phone 7975 or 9971
- Integrated Services Router (for Voice Gateway Services)

WLAN access

- Access Points
- Wireless LAN Controller (WLC)

- Wireless Services Module (WiSM2)

Software Requirements

- Windows XP or.
- Windows 7 or.
- Windows 8 platform.
- Packet Tracer 5.3.3

1.5 Architecture: -

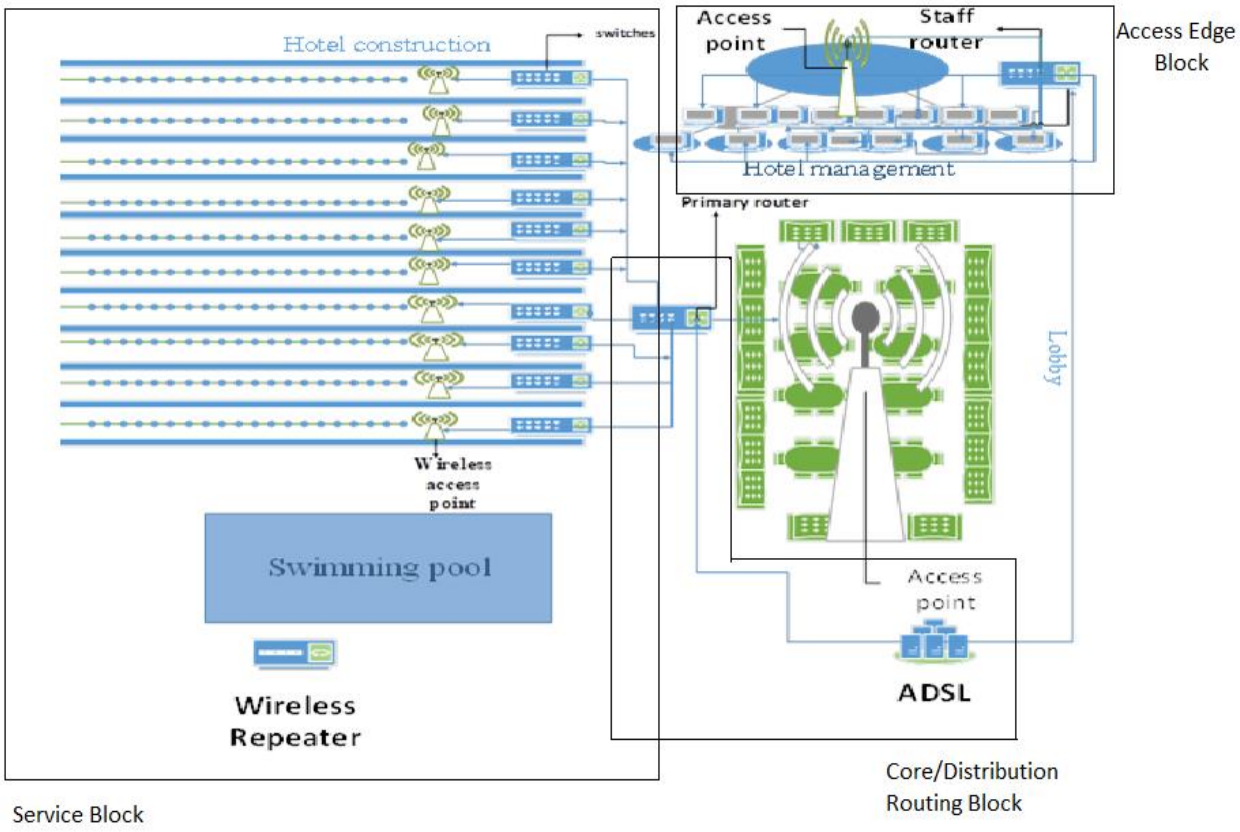

Figure 1: Architecture for networking the hotel

Architecture explanation: -

The proposed enterprise network architecture uses a hierarchical and modular architecture, including a collapsed core/distribution layer, an access layer, and a set of Service Blocks for delivering services to the network.

● The core/distribution layer consists of fully redundant pair of switches and provides the high-speed, redundant switching of packets traversing the network.

● The access layer provides ports for network devices such as IP phones, digital media players, wireless access points, video surveillance cameras, point of sale to connect to the network.

Services are segregated using VLANs to contain traffic within confined work areas and avoid broadcast or Layer 2 network problems from affecting other areas.

● Service blocks provide the services required for the different applications used over the network consisting of all nodes, swimming pool, and all the 10 floors of hotel.

● The core/distribution layer provides internet connectivity through ADSL (Asymmetric Digital Subscriber line). It is a type of DSL broadband communication technology used for connecting to the internet. Along with ADSL the layer consists of a primary router.

● The access edge layer provides connection to all the hotel management nodes consisting of Reception counter to all the nodes present in the hotel ensuring high availability and performance.

2. Plan Phase

2.1 Gap Analysis: -

The case study hotel can accommodate 800 guests at a time with different sections as mentioned in the figure. The hotel rooms are located on the 10 floors of the hotel. The basement of the hotel consists of many private shops, canopies, bar area, spa longue, reception area and meeting room.

The main lobby consists of number of computers which are used by reception, shop owner, administrator, meeting room, conference room, etc. All these computer nodes need to be arranged in a network to synchronise properly with ensuring consistency of the database.

The main building consists of event hall and a conference room which needs to have feature like call blocking. The existing RF coverage coming from surrounding macro sites is fair to good in the main lobby and all the rooms, but poor apart from it, in back offices, in conference rooms, and in concession areas. The macro sites that cover the hotel report high call blocking during venue events.

The call blocking feature is not also restricted for conference room and event hall but also whenever required according to the hotel owners wish. The transit area include parking lot having capacity of 350 cars, pedestrian walkaway below the basement for easy access to remote sites. The hotel network needs to provide coverage and capacity both to the hotel and to nearby transit areas. The network should be able to support traffic when the hotel is at full capacity during an event, and also the traffic near the venue before and after an event.

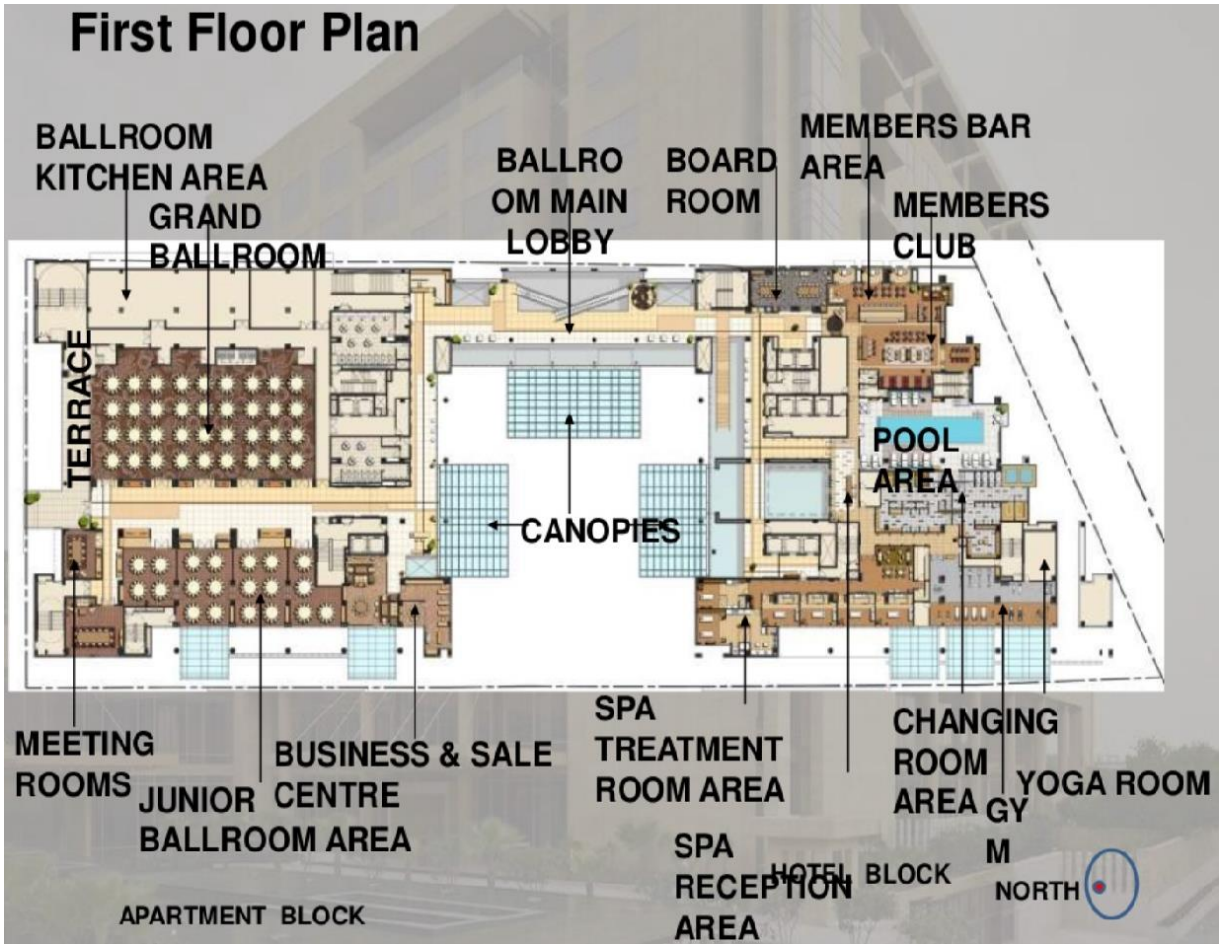

Figure 2: Architectural plan of first floor

2.2 Hotel Infrastructure

• The hotel has ten floors along with ten rooms in each floor.

• The Hotel also has one reserved room on the ground floor specially, where all the networking equipment are stored.

• The hotel has a spacious lobby and a relaxing swimming pool area.

• The hotel also has a conference room located on the Ground Floor.

• The hotel also has the DSL high speed Internet available for the public use.

Explanation: -

Although there is some residual macro RF coverage in the lobby area, the main problem is lack of capacity from the surrounding macro sites. The hotel therefore needs its own RF network to satisfy demand during events. All commercial wireless service providers (WSPs) want to be included in the hotel network. The network must also include public safety and the venue operations trunked radios. An IEEE 802.11 (Wi-Fi) network needs to be included as well. Although transit areas outside the hotel have good coverage, they suffer from inadequate

capacity before and after events. The DAS therefore has to be extended to those areas as well. The DAS signal has to be stronger than the residual macro signal to guarantee that subscribers connect to the hotel network rather than to the surrounding macro network. To provide high availability of signal to all the sites of the hotel, all the floors of the network are provided with switch and the access point which provides high availability and performance to all the users.
During the Plan phase, the network designer performs a comprehensive site and operations assessment. This assessment evaluates the current network, operations, and network management infrastructure.

The Networking Company staff identifies all physical, environmental, and electrical modifications. They assess the ability of the current operations and network management infrastructure to support the new technology solution. All changes to infrastructure, personnel, processes, and tools must be completed before the implementation of the new technology solution. Custom applications that add to the feature and functionality requirements for the new network are also identified in this phase.

2.3 Guest expectations: -

As technology becomes more integrated into our daily lives, guests' expectations regarding technology during their stay continues to rise. Guests arrive with the following expectations:

● Ability to connect multiple devices — Hotels now expect guests to arrive with their own devices, but the number of devices continues to rise. Forty-five percent of guests travel with two or more devices, and forty percent have at least three devices in their luggage. The network management should provide efficient way to interact with these devices in order to provide enhanced user experience.

● Fast and reliable network — Wireless access has become increasingly important to guests in recent years. Slow and unreliable internet service decreases guest satisfaction and is often a topic of online reviews.

2.4 The Project Plan

In this phase, the Networking Company staff and hotel management create a plan to help manage the project. The project plan includes the following:

■ Tasks

■ Time lines and critical milestones

■ Risks and constraints

■ Responsibilities

■ Resources required

The plan needs to be within the scope, cost, and resource limits established in the original business goals. Both the hotel management and the Networking Company assign individuals to manage the project. The Hotel Network follows the Network architecture, which is hierarchical and modular in design. The design offers a highly scalable and redundant architecture based on standard venue requirements, including provision of video distribution, IP telephony, video surveillance, ticketing and point of sale services, and fan and luxury suite guest access, all through one easily-managed, flexible network.

2.5 Major design aspects of the hotel network include:

● Unicast and multicast support.

● Hierarchical, tiered design with a collapsed core-distribution and access layer.

● Core-distribution layer that provides high-speed, redundant switching using switches with dual 10-Gbps uplinks to the access layer switches

● User areas segregated using VLANs to contain traffic within confined work areas to avoid broadcast or Layer 2 network problems from affecting other areas

● Power over Ethernet Plus (PoE+) in access layer switches for powering digital media players (DMPs), IP phones, and access points

● Enhanced Interior Gateway Routing Protocol (EIGRP), which scales well and provides extremely quick convergence times with minimal network traffic

● Quality-of-service (QoS) support in access layer switches to mark, queue, and police at the edge of the network, with queuing enabled on the core to help ensure high-quality video and voice transport

● Protocol Independent Multicast (PIM) routing protocol in sparse mode for efficient multicast distribution

● Anycast rendezvous points (RPs) to provide load sharing and redundancy of RPs configured in the core switches (Multicast Source Discovery Protocol [MSDP] is the mechanism used to allow RPs to share information about active sources, and Anycast RP is used for non-broadcast-video multicast applications)

● PriorityCast, an innovative Cisco-invented technology that provides multicast video source and RP redundancy to protect against node or link failure within the hotel network

● Modular architecture for limiting fault domains and scaling the network with minimal disruption

● Due to the shared nature of the hotel network, use of a service provider security model that applies layered security measures for protecting hotel server assets

● Optional Layer 2 demilitarized zone (DMZ) network edge for providing further traffic isolation to support guest access or special events

3. Design Phase

3.1 Network Design Strategy

• It is required that the guests and hotel management must be having two different IP networks. The proposed IP network for guests is 202.168.1.0/24 and for hotel management is 202.168.2.0/24.

• For the separate network setting, a VLAN based infrastructure is proposed to segregate the guest and management networks.

• The guests must be disallowed to have the accessibility of Hotel management application server through the configuration of An Access control lists.

• A single DHCP server with multiple scopes is to be setup in order to provide differential IP addresses to the users and guests.

• Access points need to be configured and installed on each floor or placed on strategic points so as to allow un-interrupted wireless connectivity to all guests in their rooms.

• Access points also require to be configured as well as installed in the lobby and swimming pool area.

• The wireless communication in the lobby and swimming pool area must be secured and protected with encryption algorithms such as WPA/ WPA2.

3.2 Design Principles

The network is designed keeping three principles in mind:

■ Modularity

1.Modularity is one of the fundamental principles of a structured network that defines the enterprise network as an assembly of multiple building blocks designed separately using a systematic approach and applying hierarchy and redundancy where
appropriate.

■ Hierarchy

1.Hierarchy is one of the key pillars for a good network design. Each module described in the previous section requires having hierarchy and resiliency built into the network designs.

2.For the business environment and underlying communication to continue to evolve, the network designs must be adaptive enough to roll out new end devices and applications, or increase capacity without going through a major forklift upgrade.

■ Resiliency

1.In addition to building modular and hierarchical network designs, it is important for network architects to consider resiliency along every step of the network design. Integrating resiliency to avoid single points of failure is key for ensuring high availability and business continuity.

2.The coordinated use of resiliency capabilities within the switch, link, and network design is required across all the different modules and layers that have been discussed previously. For example, enabling redundant supervisors in the access layer can ensure business continuity even when the active supervisor fails. This helps ensure that there is no impact to network convergence on the distribution layer.

The network for hotel management includes following key features:

1. Resource sharing
2. High reliability
3. Inter-process communication
4. Flexible access
5. Quality of Service
6. Collaboration

3.3 Cost Effectiveness

The hotels are expecting a cost-effective network to maximize return on investment with the aim of squeezing the profit with the intention of depleting the competition present in the industry. The all IP networks that are currently replacing traditional TDM, CATV, and analog networks offer strong economic viability; for instance, an integrated IP platform ensures the high-speed data transmission channels as well as voice communication, while allowing customers and hotel staff to communicate at the global scale. The cost to implement this network may vary from about Rs. 50k to 70k.

4. Implementation Phase

There are copious benefits underlying the effective integration of the room service, hotel management systems and isolating services such as: the design ensures the security of the internal hotel network and customer services, lessens network construction and maintenance costs, and shrinks egress link lease fees by using a VPN (Byers, 2009, pp. 314-328). Foreground services are transmitted in different VLANs before being broadcast to the core switch through aggregation switches.

This proposed solution simplifies the process of storage of data, employs service interworking and association, offers unified network management, and abridges the O&M. The AR G3 series of routers such as the AR3200 and AR2200 series, are the optimal choice for the egress under the proposed solution. The AR G3 routers integrate the firewall and IPSec VPN and provide hardware-based QoS technologies in order to ensure quality of service without distressing the forwarding performance. Moreover, Voice, video, and data services are processed on the AR G3 by effectively using the HQoS. Hence the expansion of 3G services ensures 3G as a cost-effective connection backup mode that can replace the legacy dual-line backup (Park, 2010, pp. 121-125).The S7700 core switch controls wireless users through a built in AC board. The aggregation switches convey outstanding performance, competence, and consistency using redundancy and load balancing.

The preceding figure shows that devices in the core telecommunications room monitor multiple buildings and centrally manage data. The vertical subsystem connects the building and floor telecommunications rooms using a low voltage system. The building gateway telecommunications rooms holds floor switches and the devices of some distributed subsystems. The devices in the building gateway telecommunications room aggregate the core services of a single building (Burns, 2010, pp. 194–196).

The horizontal subsystem employs the APs or access switches to connect to each of the service systems with the centre of telecommunications room. Since, the hotel investment features can vary in terms of scale and building structure and the proposed solution can also differ in terms of device selection, bandwidth, networking, network architecture, cable layout (Walk, 2010, pp. 133-138).

4.1 Selecting Access Devices

At times of selecting devices the PoE can be used in wireless areas where in;

• switches that can provide remote power for APs.

• Across the hotel chain, use the S2700 series as access switches because they ensure excellent control and management along with the provision of various 100M access switches (Blinn, 2010, pp. 144-148).

• S5700 switches can also be used as it ensures the 1000M access switches at the access layer as they incorporate advanced technologies with the capabilities of strong service expansion. The S5700EI or S5700SI is a cost-efficient 1000M Layer 2 switch that can use 10 Gbit/s fibres as uplinks. This allows high bandwidth for each user or terminal that meets the requirements for heavy traffic of multimedia services.

Selecting Core Devices

At the time of selecting the core device, the following points must be taken into consideration;

• Faults on core devices impact the entire hotel network; therefore, core devices must feature high reliability, stability and capacity, flexible scalability, and strong security capabilities (McKnight, 2010, pp. 53-59).

• The S5700 and S7700 are mature core switches that successfully employ dozens of security and consistency mechanisms, as demonstrated in existing deployment scenarios.

• The core switches must incorporate security boards where the security technologies can be deployed in order to isolate the services of different departments and defend against the threats and danger of external network. The cost-effective switches assimilate various boards, that include the firewall board which implements robust security measures.

• The S7700 unifies AP management switches with the integrations of AC functions.

4.2 Proposed Solution Characteristics

The following mentioned points elaborates the characteristics of the proposed solutions;

• The integration of the customer service system and hotel management system lowers network construction and maintenance costs along with the reduction in egress link lease fees.

• Each layer has clear functions and a stable topology, making the network easy to expand and maintain through the multi-layer designs.

• The AR G3 routers ensure network stability and reliability with the provision of the capabilities to support 3G networks, multiple services; and provide load balancing and functionality to link backup (Crowston, 2012, pp. 75-79).

• It ensures the open design hence the proposed solution implements the international standards along with the provision of strong interworking capabilities. It supports IPv4 and IPv6 deployment and connects the egress to the Internet, WAN, and PSTN.

Internal network security

Different security features are deployed at the core layer to protect internal network security; for example, the access layer can use MAC Forced Forwarding (MFF) with the intention to prevent unauthorized access. The core layer can use IP source guards to avoid IP spoofing attacks and implement DHCP packet rate with the aim of limiting to prevent DHCP flooding attacks. Strict ARP learning or ARP gateway anti-collision can be configured on gateways to defend against attacks from bogus gateways, and ARP source suppression can protect the gateways from ARP flooding attacks. In 802.11 networks, clients can authenticate with an AP using many methods. The following are some of the most common means of connecting to a WLAN. It is worth noting that the level of security provided varies under the different methods. These methods are listed in order of the level of security which they provide, starting with the oldest and generally accepted as least secure.

A similar secure key is defined statically on the AP and the user. If the two keys form a match, the user is provided with the accessibility to the network. It must be kept in mind that the process of authentication in the aforementioned methods halts at the AP. PSK and open authentication are regarded as legacy systems as they cannot be scaled nor they are entirely secure or protected. Open authentication is generally the standard setting and does not screen or check the users in any manner. Any user can log in to the network without having to obtain the verification of any type. Naturally, the SSID becomes the sole authentication required on such a network. Though this is the easy and simplified method as it provides security to the wireless LAN. Moreover, open authentication possesses no means of decryption of data that is relayed to the wireless LAN. The pre-shared authentication key makes use of a comprehensive WEP certificate that is saved on the AP and the client. The AP does not render any kind of resistance to avert unauthorized access in case when a user wants to create a link with a wireless LAN.

5. Operate Phase

5.1 Service integration

The head office can deploy AR3200s which provides the firewall and IPSec VPN functions. The HQoS can also be applied to transmit voice, video, and data services.

5.2 Border security-firewall deployment

The hotel security proposed solution controls each area by isolating the physical areas and service areas. Firewalls are deployed to guarantee the security between the core switches and

Internet routers. The egress routers, firewalls, and core switches adopt a redundancy design to improve reliability based on the size and security requirements of the hotel network.

Firewalls provide the capabilities and assurance for comprehensive security defence. The firewall access control policy allows Internet users to access only the specified interfaces of the DMZ servers. Internet access is controlled through their IP addresses and the security zones are divided in order to avoid security threats.

The proposed solution defends the entire network, applications, or data against the threats and other dangers.

Firewalls make sure the border security at different network layers.

Coverage Policies for Guest Rooms

Policy 1: An AP is specially deployed for guest rooms with the purpose to cover every corner of the rooms. This policy allows the implementation of the project phase-by-phase.

Policy 2: AP +power splitter +RF cable + antenna is low cost but averts project implementation in phases.

These policies can effectively be applied to the hotels with various building structures. The standard rooms and deluxe rooms featured by high signal shielding capabilities, high user density, and many computers must be deployed with the Omni-directional ceiling mount antennas. This method uses multiple antennas and little power to ensure coverage overlap in addition to provide and ensure the adequate edge signal strength. Although an antenna is mounted on the corridor ceiling between two neighbouring rooms with the aim at reducing signal loss caused by wall penetration. If there are many standard rooms and computers, and the number of access users needs to be limited, policy 2 can deploy a POE-powered AP on each floor in the HUB room on the west side of the corridor. However, the network cable between switch and the AP cannot exceed 90 meters.

5.3 The proposed System configurations:

• The 802.11n network must be compatible with 802.11a/b/g access.

• A maximum of 600 Mbit/s bandwidth is provided, which dramatically exceeds 100 Mbit/s wired access.

• The core switch integrates the AC function and works with multiple APs to meet with the requirements of deployment for multiple application scenarios that include roaming, smart antenna, dynamic load balancing, and multi-SSID management.

• APs are powered by PoE devices through network cables.

5.4 Operations to maintain health and prevent problems:

Use of a virtualized server for zero-downtime recovery: -

Servers backed up with Nordic Backup Server Pro Preferred include our Preferred Server Hosting and can be pre-emptively virtualized so that there is no waiting before a user can access a cloud backup server.

Identify single points of failure: -

The easiest and most economical way to improve network availability is to remove single points of failure. A single point of failure occurs when there is just one physical connection between parts of a network. Many different network topologies can help you remove single points of failure. The basic principle is to connect more nodes to individual servers and other network resources. If one of the nodes fails, traffic can be rerouted around the failed system.

Plan for fault tolerance

Fault-tolerant networks have very few single points of failure, if any. In addition, fault-tolerant networks have disaster-recovery hardware at each node. Typical hardware measures per node include:

Replicated hardware subsystems

If a network is important enough, a second server, router, or other device is available at each node in case of system failure of the primary device.

Standby hardware

An example of standby hardware is a redundant array of independent disks (RAID), which enables hot-swappable storage media.

Fast boot methods

You need to be able to dump and reboot in the shortest possible time to maximize uptime.

Backup power

Plan to connect as many nodes as you can to uninterruptible power supplies. Large data centers should have backup generators as well.

Total remote management

You should be able to remotely diagnose and reboot servers regardless of their state.

Concurrent backup and restore

Make sure that you can use the backup system as soon as a failure is detected, and begin backing up again in real time.

6. Optimize Phase

6.1 Major Risk

Risk 1: Not have enough capability of making efficient decisions

Risk 2: Inadequate access to Project Manager of Reporting Authority

Risk 3: Insufficient authority of project manager

Risk 4: The number of decision makers far exceeds than the requirement

Risk 5: Consumption of precious time on insignificant or petty affairs

Risk 6: Significant changes will be made in the project at a later stage

Risk 7: Not keeping in mind the timeline of the project

Risk 8: Inability to recognize casualties

Risk 9: Malfunctioning

After deploying network in hotel management area system face some issues which are need to be solved before affecting entire network and business.

1. Wireless network shows signal but won't work

Some notebooks and computers occasionally show a strong signal from the wireless router but still don't connect. A network card occasionally receives a strong signal but doesn't transmit as effectively. Updating the network card's drivers might solve this problem, but it is also possible that you may need to replace the hardware entirely should this occur.

2. Network outage and inaccessible files

If you experience a high number of network outages at unpredictable times or you find your employees unable to access files they are supposed to have access to, you might be experiencing a NetBIOS conflict. This problem tends to be most common on older systems, particularly when they use Windows NT, but the issue exists in other Windows systems as well. You can bypass this problem by disabling WINS/NetBT name resolution unless it is required by a specific program. You could also rename a computer or domain to resolve possible naming issues.

3. IP conflicts

By default, Windows ensures that only one IP address per device has place on the network at once. However, sometimes two devices wind up getting assigned the same address. In this case, the network might wind up blocking one of the devices, which prevents access to protected files and can cause network lag not only for the conflicting devices but for all connected machines. You can avoid this problem by reconfiguring your DHCP setup to ensure that static IP addresses are excluded from the pool. This will reconfigure IP addresses appropriately,

which will resolve the conflict and in return will lead to all machines on the network getting the proper access that they are supposed to get.

4. Slow application response

A common issue networks encounter is a slow reaction time for applications, especially shortly after a computer starts up or connects to a network. This is usually a sign of high bandwidth use. Enforcing proper network use may be a good way of keeping your bandwidth use in hand. you should look into upgrading your network to properly fit your expanding hotel management needs.

5. Poor VoIP Quality

Stutters, delays, and other problems with VoIP can hamper a network's productivity and hurt telecommunications efforts. The most common issue with business VoIP is a network stutter. This can be resolved by installing jitter buffers, which cache VoIP packets and allow them to be accessed during the communication in order to ensure a smooth stream.

Conclusion

In the case study we have studied an enterprise network system for Five-star hotel management system, by following guidelines specified by CISCO for Enterprise Network Design PPDIOO phases. We have gathered all the information from the hotel management and have done feasibility study on that and then we contacted the management to ask about the specifications to management if required. Later we informed them with our project design. On the approval of project design, we will start the work.

References: -

1. https://www.slideshare.net/jagrutib22/hotel-casestudy-hyatt-regency-pune
2. https://www.al-enterprise.com/-/media/assets/internet/documents/ale-hospitality-networking-guide-en.pdf
3. http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3
4. https://www.uniassignment.com/essay-samples/information-technology/design-project-for-a-5-star-hotel-information-technology-essay.php#
5. https://www.zyxel.com/solutions/Zyxel-Network-Solution-Shapes-Guests-Journey-at-Turkish-Five-Star-Hotel-20180213-499102.shtml
6. https://networkprojects.e-junkie.com/product/1091751
7. https://www.conceptdraw.com/How-To-Guide/hotel-network-topology-diagram
8. https://www.scte.org/documents/pdf/CCNA4%20Sample.pdf
9.https://www.cisco.com/web/partners/services/promos/accelerate/downloads/lifecycle_services_sg.pdf
10. https://www.ccexpert.us/network-design/network-design-methodology.html