Research Paper

19 December 20223

Table of Contents

[Section 1 3](#_Toc153743118)

[Section 2 6](#_Toc153743119)

[Section 3 9](#_Toc153743120)

[Section 5 11](#_Toc153743121)

[Section 6 12](#_Toc153743122)

[Section 7 14](#_Toc153743123)

COMPUTER NETWORKS MODELING AND ANALYSIS

## Section 1

I've taken a careful and methodical approach to creating the network strategy for the five hotels in issue. Each of the five routers in the network design represents a different hotel in the group. The planning procedure entails the painstaking construction of several VLANs (Virtual Local Area Networks), each one assigned to distinct user groups found in every hotel: Rooms, Staff, Finance, Management, and Visitors. This segmentation is necessary to optimize network administration in the unique operational context of a hotel setting, in addition to improving security.

In terms of selecting the primary router, I have decided to utilize the Cisco Router 1841. The router's broad industry acceptance and well-established reputation for dependability serve as the foundation for this selection. Moreover, it provides all-encompassing assistance for all the different needs of my network setup, such as OSPF routing protocol deployment.

In the realm of switches, I have deliberately selected the Cisco 2950-24 switch. This particular choice is motivated by its capacity to effectively manage VLANs, a fundamental component of my network setup. This strategic selection ensures that the network infrastructure is fully equipped to address the diverse needs and demands inherent to the hospitality sector.

One particularly important component of my project is the implementation of VLANs, which I choose to use for pragmatic reasons. In the hotel industry, where workers and visitors use the network in significantly different ways, VLANs are a practical way to manage network traffic.

This section has two main objectives. First of all, it makes sure that visitors' demands for internet connection don't interfere with hotel operations. Through network segmentation, we protect the hotel's essential operations from possible disturbances brought on by heavy visitor traffic while ensuring a seamless experience for visitors.

Second, by keeping private internal communications separate from visitor access, VLANs improve network security. This division improves the network's overall security posture by reducing the possibility of unwanted access to vital hotel management systems.

It's important to note that we also thought about buying different switches for every network section as a backup plan. On the other hand, this solution would have required much more money and complicated configuration and management. VLANs were therefore the most sensible and economical option for our project.Top of Form

A critical component of this network design is the careful IP addressing scheme that is assigned to every VLAN across the chain of hotels. The efficient running of the network is greatly dependent upon this methodical approach to IP administration, particularly when considering a large-scale enterprise such as a chain of hotels.

Different IP addressing methods are used for a variety of reasons. First of all, it makes it simple to identify and maintain every network section. In a network this size, this degree of order is especially crucial since it makes monitoring and troubleshooting much easier.

For instance, consider VLAN 10, designated for guests, with IP addresses following the pattern 192.168.10.X. Similarly, VLAN 20 for staff uses IP addresses like 192.168.12.X. This straightforward system aids network administrators in quickly understanding the network to which a particular device is connected and its associated VLAN. The numerical structure, with the "1" representing the hotel and the "2" indicating VLAN 20, simplifies this process.

Its forward-thinking methodology also allows for network growth in the future and scalability without requiring significant infrastructure changes. In the event that the hotel chain changes and its network requirements develop, it lays the groundwork for expansion and adaptation.

Routers are essential to this configuration. They provide a role that extends beyond simple internet gateways; they are essential in controlling traffic flow across VLANs, guaranteeing effective intra-hotel communication. This is especially crucial for the hospitality sector, since maintaining excellent service and facilitating smooth operations between departments need effective communication.

To sum it up, our network design serves as a compelling illustration of meticulous planning tailored to meet the intricate requirements of the hospitality sector. It adeptly harmonizes essential factors including security, efficiency, and adaptability, all of which hold paramount significance in a technology-driven service industry like hotels.

## Section 2

Careful planning is essential when it comes to network design, especially in complicated situations such as the hotel sector. The strategic choice to deploy Virtual Local Area Networks (VLANs) gives our hotel chain the ability to efficiently separate and control network traffic. In addition to improving security, this segmentation makes the best use of network resources by guaranteeing that the requirements of every user group are satisfied.

Each hotel has four unique VLANs designated in our network architecture: VLAN 10 for Visitors, VLAN 20 for Employees, VLAN 30 for Rooms, VLAN 40 for Finance, and an extra VLAN 99 for Management. Every VLAN is intended to serve a particular function, and the IP addressing system has been carefully constructed to support these functions.

Firstly, VLAN 10, which caters to our Guests, employs the IP range of 192.168.10.0/24 with a subnet mask of 255.255.255.0. This allocation ensures that there are 254 available IP addresses, which aligns with the varying number of guests in our hotels. It strikes a balance between providing ample addresses while avoiding resource waste.

Moving on to VLAN 20, tailored for our Staff, it utilizes the IP range 192.168.12.0/26 with a subnet mask of 255.255.255.192. This subnetting decision allows for 62 available IP addresses, which is an adequate number to accommodate our staff members without incurring unnecessary IP address overhead. This choice optimizes resource utilization.

VLAN 30, dedicated to hotel Rooms, adopts the IP range 192.168.13.0/27 with a subnet mask of 255.255.255.224. Here, we ensure 30 usable IP addresses, which is more than sufficient for devices such as TVs, computers, and various in-room appliances, aligning precisely with our needs without unnecessary address surplus.

In the realm of finance, VLAN 40 takes a security-conscious approach. It operates with the IP range 192.168.14.0/28 and a subnet mask of 255.255.255.240. This allocation provides 14 available IP addresses. The emphasis here is on security by limiting the number of IPs, reducing potential exposure and aligning with the specific requirements of finance operations.

Lastly, VLAN 99, designated for Management, employs the IP range 192.168.19.0/29 with a subnet mask of 255.255.255.248. In this case, a minimal number of 6 usable IP addresses is allocated. This approach underscores the importance of security in management operations, ensuring that only essential personnel have access.

Furthermore, it's worth noting that the management-specific IP is precisely defined as 192.168.19.2. This level of granularity adds a layer of clarity and precision to our network configuration.  
With a few small adjustments to accommodate each hotel's particular needs, our chain of hotels all use the same approach to VLANs and IP addresses. Scalability, effectiveness, and security are guaranteed by this standardized design. Hotel 1 employs 192.168.10.0/24 for VLAN 10 (Guests), whereas Hotel 2 follows the same pattern for other VLANs and utilizes 192.168.20.0/24. This method gives network administration a defined framework and streamlines it. Within the same subnetting framework, each hotel is assigned a unique IP address, such as VLAN 20 for Staff or VLAN 99 for Management. This consistency paves the way for a strong and flexible network architecture, which is essential given how quickly the hotel sector is changing.

## Section 3

In my situation, I believe that OSPF (Open Shortest Path First) is the best option for my setup. For intricate networks, such as a hotel chain with several subnets, OSPF, a dynamic routing system that uses a link-state algorithm, is quite effective.

The primary benefit of OSPF is its capacity to adjust swiftly to changes in the network, including broken links. High reliability is ensured, which is important in the hotel industry because network outages may have a big impact on both visitor happiness and operational effectiveness. Finding the shortest and most effective path for data transmission is one of OSPF's primary functions in effectively managing network traffic, which is important in hotel networks where large data traffic volumes are typical.

Specific OSPF instructions are important during the setup phase. IP addresses are linked to OSPF processes by the 'network' command, while the 'router ospf' command starts OSPF configuration on a router. Through the exchange of routing data and upholding of network integrity, these instructions provide successful router communication.

When it comes to hotel chain networks, OSPF's capabilities surpass those of other protocols such as EIGRP (Enhanced Interior Gateway Routing Protocol) and RIP (Routing Information Protocol). Due to its delayed convergence and lower hop count, RIP is less effective for bigger networks while being simpler. Given the scale and complexity of the hotel chain, OSPF is a better fit due to its quicker convergence and support for larger network designs.

Regarding network designs that incorporate diverse hardware, OSPF offers greater compatibility across various vendors and devices compared to EIGRP. A key attribute of OSPF is its capability to segment the network into more manageable parts, an advantage particularly relevant for networks spanning multiple hotels, where efficient and manageable routing tables are vital.

Finaly, OSPF enhances network efficiency by minimizing unnecessary traffic via its load balancing features and accurate, prompt routing information. In the hotel industry, where network demands can vary greatly, this is particularly beneficial as it guarantees consistent and rapid connectivity.

## Section 5

Our hotel chain's suggested network architecture blends cutting-edge technology with an innovative strategy. It may need a large upfront expenditure, but it's meant to maintain our chain's seamless operations as it expands. Our routing protocol of choice, OSPF, is more scalable and effective than more straightforward options like RIP or EIGRP, which plays a significant role in our design.

We've now made some wise decisions about expenses. Our investment is the Cisco 1841 router, which is adaptable and capable of managing our intricate network requirements, encompassing VPNs and OSPF. Even when purchased brand-new, this router is surprisingly affordable, coming in at just $200. Additionally, you may locate used ones for less money if you're trying to save money.

Additionally, we have selected the Cisco 2950-24 switch, which is renowned for its dependability and versatility in managing various network functions, such as facilitating Virtual LANs (VLANs). This swap is an affordable option, coming in at about $90.

Our dedication to superior cabling is another crucial factor. To future-proof our network, I used Cat 7 cables in my situation. Although they cost three times as much up front as Cat 6 cables ($75 per 100 meters), the investment pays off in the long run by prolonging the life of our network and lowering the frequency of required upgrades. This is especially important for the hotel sector, as the provision of trustworthy digital services is critical to visitor pleasure.

Speed, dependability, and security are the main functional priorities in the network's architecture. With the large volume and diversity of network needs seen in hotels, the OSPF protocol makes it possible for quick data transfer and effective routing. By partitioning the network, the use of VLANs raises security even further and safeguards critical hotel management data while offering visitors safe access to the internet.

The intricacy of configuring and managing OSPF and VLANs is one of the design's most noticeable difficulties. It is crucial to invest in both technological infrastructure and human resources because this calls for competent IT personnel for correct configuration and continuous management.

Considering other strategies, such as the potential for less complex routing protocols or wireless solutions, may at first seem like more affordable and doable choices. However, it's important to recognize that these options typically fall short of the scalability and performance that come with our selected architecture.

Let's take EIGRP as an example, which while it may offer a cost benefit over OSPF, is not nearly as scalable or as efficient in terms of operations. Moreover, it may appear reasonable to acquire specialized switches for each particular purpose rather than circumventing the VLAN setting on the switches. But when practicalities is taken into account, this strategy would actually result in greater total costs.

## Section 6

Setting up Virtual Local Area Networks (VLANs) on the network switches for the hotel chain is essential to ensuring effective, secure communication. Because they enable a network to be divided into smaller, more isolated subnetworks, each serving a distinct purpose (such as guest access, staff operations, management, etc.), VLANs are essential.

Determining the VLANs on each switch is the first step in the configuration process. To do this, each segment must be given an own VLAN ID. Guests should use VLAN 10, staff should use VLAN 20, and so on. This segmentation increases network efficiency by lowering congestion while also enhancing security by isolating distinct user groups.

Assigning switch ports to VLANs is the next step after defining them. This entails identifying which switch ports will be a part of each VLAN. For example, the ports linked to the access points in the guest rooms would fall under the Guest VLAN, but the ports linked to the staff PCs would fall under the Staff VLAN.

Another important consideration is inter-VLAN routing. It is necessary for tasks like staff access to the administration servers and guest network use monitoring as it enables communication between several VLANs. A router-on-a-stick setup or a Layer 3 switch can be used to do this. But in our case will go with router-on-a-stick setup because we don’t have a Layer 3 switch.

Importantly, the switches' trunk ports must be configured. In order to maintain traffic separation, these ports are in charge of sending traffic from all VLANs to other switches and routers via the main network structure while maintaining VLAN tags.

Furthermore, implementing security controls like VLAN Access Control Lists (VACLs) is essential. Guidelines for the transfer of traffic between VLANs are established in large part by VACLs. Since they control how several VLANs communicate with one another, they significantly improve network security.

## Section 7

We require a complete plan that covers Wireless Security, IPSec/VPN, and Access Lists (ACLs) to make our hotel chain's network more secure. Similar to a security gatekeeper, access lists determine who is allowed access to and from our network. Access Lists allow us to establish rules that permit or prohibit access depending on many factors, including IP addresses, port numbers, and internet traffic kinds. We can ensure that only authorized users and gadgets have access in this way. Setting up these Access Lists is essential, particularly in our situation where we need to maintain everything secure but yet provide some access for hotel visitors. Our executive team's Access Lists also require significantly stricter security guidelines.

VPNs (Virtual Private Networks) and IPSec (Internet Protocol Security) must be used in order to provide the highest level of security for data transferred over the internet. This is especially valid for operations such as remote administration and guest virtual private network services. Maintaining data integrity and secrecy is made possible in large part by IPSec's strong end-to-end encryption technology. Meanwhile, the creation of virtual private networks, or VPNs, is essential as it creates a safe and reliable route for data transport. Our network architecture is woven with these security measures, which serve as the cornerstone of our complete data protection approach.

Wireless security is critical in a hospitality setting where guests often use Wi-Fi. Our PT-REPEATER-NM-1C Access Point is more secure since we employ WPA2-PSK encryption to make sure guests enjoy a safe and secure Wi-Fi experience. For the convenience of our staff, each hotel also features an additional secure access point where they may connect their devices securely as needed.

We place a high priority on upholding excellent security procedures since we are aware of the inherent weaknesses in wireless networks. For protection against possible breaches, this entails frequent firmware upgrades and a strict password policy. Additionally, we separate the guest Wi-Fi network from the internal network as one of our proactive defensive strategies. In order to provide the highest level of security for every network user, we also make use of sophisticated monitoring systems that can quickly detect and block such attacks.

In conclusion, a multi-layered security approach, combining ACLs, IPSec/VPN, and robust wireless security, is imperative for protecting the hotel chain’s network against various cyber threats, ensuring the safety of guest information and smooth hotel operations.