Design and Implementation of a Hotel Management Network Using Cisco Packet Tracer

1st Hari Babu Hasini
AM.EN.U4ECE22122
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

2nd N.Harshitha
AM.EN.U4ECE22123
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

3rd Teena S
AM.EN.U4ECE22144
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

4th Maddu Siri Varshini
AM.EN.U4ECE22150
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

5th M Kanimozhi Harshini
AM.EN.U4ECE22157
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

***Abstract*—This work proposes design and simulation a highly secure, scalable and efficient network architecture for a multi-floor hotel scenario with the help of Cisco Packet Tracer. The network design allows for departmental and guest traffic to be securely logically segmented by using VLANs. Every department - reception, housekeeping, management, etc. has its own dedicated VLAN to achieve isolation and reduce broadcast domains, with guest access also segregated to protect the privacy and security of guest data.It utilizes the Open Shortest Path First (OSPF) protocol to offer dynamic routing and stable path selection between storeys.The centralized network services such as DHCP, DNS, FTP and web servers are also combined into the environment for the purpose of handling IP address allocation, domain names resolution, file transfer, and web hosting. Security is increased with SSH for remote and secure device management,and with ACLs to restrict traffic and help protect the network.The design prioritizes security, scalability, and efficient communication while enabling future integration with advanced network management systems.**

***Index Terms*—VLAN, OSPF, Cisco Packet Tracer, DHCP, SSH, ACL, Hotel Network Design**

I. Introduction

Network Infrastructure for Modern Hotels Today's hotels must maintain a strong network infrastructure to support administrative operations, guest connectivity, and secure communication across multiple departments. The requirements of reliability, scalability and security in hotel networks have required the development of structured network designs that are service-chaining capable. This simulation represents such a network for a hotel, with reception, HR, IT and finance departments scattered over a number of floors. It utilizes Cisco Packet Tracer to design a modular network with VLANs, DHCP, inter-VLAN routing, and essential network services. The design prioritizes security, scalability, and efficient communication while enabling future integration with advanced network management systems.

II. Related Work

Several publications have illustrated the importance of network segmentation and strong security in hospitality environments so as to protect sensitive information and keep services operational. In [1], the application of Virtual Local Area Networks (VLANs), was suggested as one of the main methods of segmenting guest traffic from management traffic, which lessens the potential for contamination of authorized traffic, and also lessens unnecessary broadcast traffic. Likewise, [2] considered dynamic routing protocols; which included Open Shortest Path First (OSPF), in a multi-site campus model and contrasted it against static rate protocols because of its fast convergence, efficient calculation of paths, and scaling capabilities. Prior simulations like those in have primarily considered single-floor spaces or slightly more complex spaces with networking services like DHCP, DNS, FTP, and web hosting (though none have demonstrated integrated networking services). In addition to relatively simple spaces, previous simulations typically do not consider secure access to devices and the fine-grained control of traffic that are both essential in a practical implementation. This project provides one example of a simulation that is suitable for students and professors by integrating networking features like multi-floor OSPF-based routing, centrally managed services, VLANs, SSH, and Access Control Lists (ACLs), into a coherent and realistic scenario commonly found in hotels. This provides an accurate representation of current best practices/procedures and a scalable and secure model for modern hotel and hospitality network infrastructure.

III. System Architecture

The network uses a hierarchical design model and is divided into three layers: Access, Distribution, and Core.

A. Access Layer

Layer 2 switches are located on each floor, connecting end devices: PCs, printers, and access points. Different departments are assigned different VLANs on each floor:

- **Floor 1**: Reception (VLAN 80), Store (VLAN 70), Logistics (VLAN 60)
- **Floor 2**: Finance (VLAN 50), HR (VLAN 30), Sales (VLAN 40)
- **Floor 3**: IT (VLAN 10), Admin (VLAN 20)

B. Distribution Layer

Each switch is trunk-linked to a router, dedicated to that floor. These routers are responsible for Inter-VLAN routing and uses a router-on-a-stick model. Each router FastEthernet port has one or more sub-interfaces configured to manage VLAN traffic.

C. Core Layer

The core layer contains a central router connected to an array of services hosted on servers:

- **DHCP Server:** Dynamic IP allocation.
- **DNS Server:** Domain name resolution.
- **FTP Server:** Enables file sharing between departments.
- **Mail Server:** For internal communication.
- **Web Server:** To host web applications for the hotel.

Routing from the floor routers from and to core services is managed via OSPF routing protocol, so that path selection between nodes is the shortest and always uses a loop-free route.

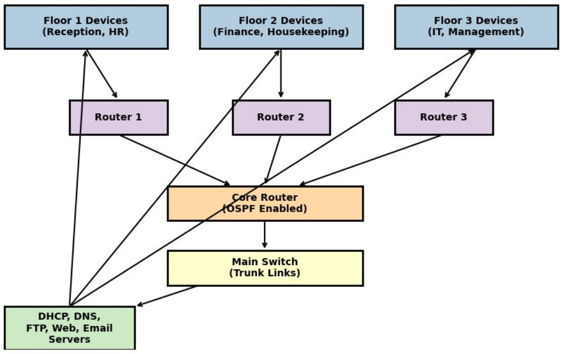


Fig. 1. Block diagram of the hotel management network architecture.

Fig. 1 shows a high-level view with three hierarchical layers. The Access Layer consists of department devices on each of the floors. The distribution layer consists of individual routers per floor. The core layer has a main router and main switch. There are centralized servers including, DHCP, DNS, FTP, Web and Email available to all departments connected to the main switch. Departments communicate between floors via, VLANs, OSPF routing, and trunk links. Guests and administrative traffic is kept isolated from departments.

IV. Implementation Details

A. Router Configuration

This setup consists of three floor routers and a single core central router that allows communication between the floors and distribution of services from the core point. Each router has its own OSPF router ID that allows OSPF to use dynamic advertisement of routes within the OSPF protocol. The routers are interconnected using serial DCE cables, and since the clock rate will be set manually (e.g. `clock rate 64000`) on the DCE interfaces, it will allow DCE to synchronize the serial links. The serial interfaces were assigned IP addresses from point-to-point subnets, and OSPF was configured on each router to advertise the directly connected networks allowing for efficient, and loop-free communications between the floor networks.

B. VLAN and Port Assignments

VLANs have been statically created on one of the Layer 2 switches on each floor to achieve network segmentation and broadcast domain isolation. Each department (e.g., Reception, IT, Admin) has a different VLAN ID. End devices (e.g., PCs and printers) are connected to access ports on the switches. Each access port is assigned the VLAN ID that reflects the end device location. Inter-VLAN routing is configured using a router-on-a-stick, where a physical interface is divided by sub-interfaces. Each sub-interface is tagged with a VLAN ID and an IP address that serves as the default gateway. Trunk ports were configured between the switches and the router, carrying traffic for multiple VLANs that were tagged using IEEE 802.1Q encapsulation, allowing for all VLAN-tagged frames to pass over a physical link at the same time without data loss.

C. DHCP Configuration

The DHCP service is used to provide dynamic IP address allocation, the DHCP service runs from the core router. A DHCP pool was created for each VLAN identifying the subnet range, default gateway, and DNS server. To prevent IP conflicts, the router interface IPs and a small range of addresses reserved for static allocations were excluded from the DHCP pool using the `ip dhcp excluded-address` command. All of this allows for the IP address configuration to be logical and efficient, and eliminates the need to manually configure end devices.

D. SSH and Port Security

To secure remote device management, SSH (Secure Shell) is configured on all routers. The process involves setting a hostname and domain name, generating RSA key pairs for encryption, and creating local user accounts with secure passwords. VTY lines are then configured to use SSH exclusively, preventing unauthorized access via unencrypted protocols like Telnet. Additionally, port security is enabled on the IT department's switch to limit physical device access. Using sticky MAC address learning, the switch dynamically captures and locks the MAC address of the first connected device on a specific port. A maximum limit of allowable MAC addresses is set to prevent unauthorized devices from gaining access to the network through that port.

E. ACL Implementation

ACLs (Access Control Lists) are utilized on router interfaces to manage traffic between VLANs as well as enforce the desired security policies. For example, we will have ACLs that restrict devices in the guest VLAN from gaining access to internal administrative resources. In this case, an extended ACL will only permit HTTP and DNS for guest users while denying everything else. This ACL will be defined and placed inbound on the sub-interface for the guest VLAN. In contrast, the VLANs for administrative and departmental users will be configured with more access according to their functional needs. In either case, the rules will only allow legitimate traffic across VLANs and help improve the overall security of the network.

V. Experimental Results and Evaluation

A. Simulation Environment

The network was created through a simulation in Cisco Packet Tracer version 8.2.0. The network topology consists of three floors, each having its own router and switch and various departments with VLANs. The core services DHCP, DNS, FTP, and Web, were hosted in a central location. The simulation includes 3 routers, 3 switches, 25 devices, and 1 server1. The network protocols and functions used in this network simulation include VLAN, DHCP, DNS, HTTP, FTP, SMTP, OSPF, SSH, and ACL.

B. Connectivity Tests

Ping tests were performed between end devices across VLANs as well as across floors to confirm inter-VLAN routing functionality. On one occasion, the first ping attempt from PC7 to PC5 timed out, but this was due to the first Address Resolution Protocol - ARP resolution. The subsequent packets were successfully delivered with an average of 1ms latency. This confirmed OSPF routing, and router-on-a-stick configuration was working.

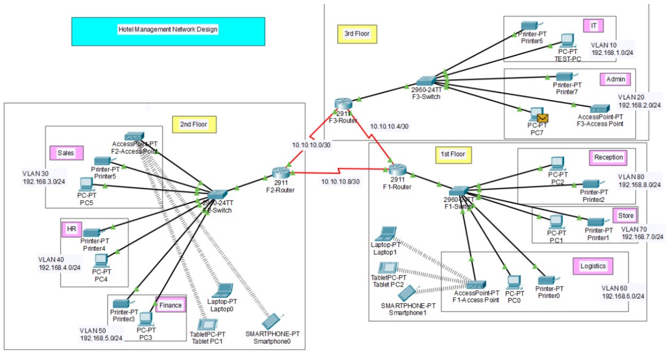


Fig. 2. Design in Packet Tracer showing multi-floor layout.

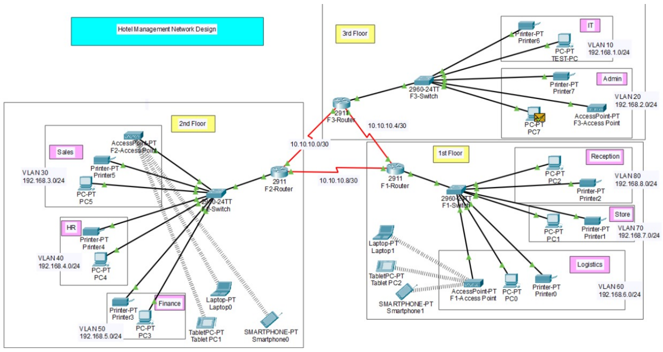
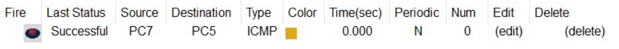


Fig. 3. Packet from PC7 to PC5 is successfully acknowledged, showing that inter-VLAN and inter-floor communication is working correctly.

Fig. 2 shows the completed hotel network topology created in Cisco Packet Tracer. It comprises three floors that are connected via routers utilizing departmental VLANs.

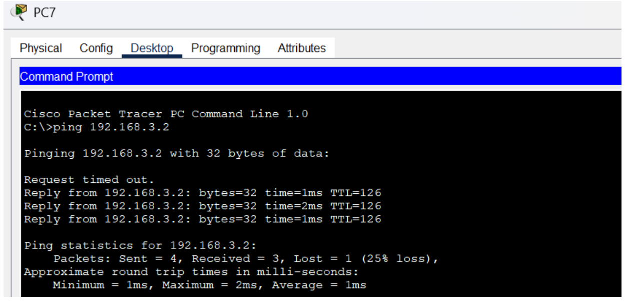
Fig. 3 This figure displays a successful ping test which demonstrated sending a message from PC7 (in the Admin department on the 3rd floor) to PC5 (in the Sales department on the 2nd floor). The green arrow indicates the returning of acknowledgment (reply) packet to PC7, which confirms successful inter-VLAN communication and inter-floor communication. This proves that the network configuration allows for communication between different floors and departments using VLANs and routing.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC7	PC5	ICMP	🟨	0.000	N	0	(edit)	(delete)

Fig. 4. Successful Packet Transmission from PC7 TO PC5.

In Fig. 4, shows the successful transmission of an packet from PC7 to PC5 in Cisco Packet Tracer simulation. The ”Last Status” field confirms that the packet was delivered successfully which confirms the end-to-end connectivity between PC7 and PC5. The simulation used ICMP protocol which tested for communication with a response time of 0.000 seconds indicating perfect network conditions with the simulated environment. At this point we have confirmed that the network topology and configurations (IP addressing, cabling and device setup) were working properly.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Fig. 5. Command prompt Output from PC7

Fig. 5 illustrates the command prompt output from PC7 after it had tried to ping PC5. The first packet was unsuccessful because the system had to search for the MAC address of the destination, but the rest were successful. This shows that the routing between VLANs is operating correctly and both devices have obtained a proper DHCP address.

C. Security Validation

SSH connectivity was tested on all routers. Attempts to log in on authorized devices were successful. This confirmed secure remote access. ACLs were placed on the guest VLAN to permit HTTP and DNS and all other traffic were denied access to the administrative VLANs. All the ACLs were tested via ping to confirm what worked and what was restricted when access was attempted. All the testing behaved as it was expected to behave.

D. Server Access and DHCP Functionality

IP addresses were dynamically allocated from DHCP pools configured on the core router to devices on each VLAN. Server access was verified by performing DNS lookups and FTP transfers. While not shown here, testing uploads of files to the FTP server and browsing to the internal web server was successfully done in practice, verifying that services are reachable across the VLANs.

E. Performance Comparison

The VLAN-OSPF-based plan was analyzed against a flat network plan for comparison. As highlighted in Table I, the benefits of the VLAN-based approach were evident. The VLAN-based design provided superior security, scalability, and manageability.

TABLE I
COMPARISON WITH FLAT NETWORK ARCHITECTURE

Feature	**Flat Network**	**Proposed Design**
Guest/Admin Isolation	No	Yes
Dynamic IP Allocation	Poor	DHCP-enabled
Routing Efficiency	Poor	OSPF-based
Security via ACLs/SSH	Not present	Implemented
Central Services	Limited	Fully Integrated

VI. CONCLUSION

This project detailed the design and simulation of a secure, scalable, and efficient hotel network utilizing Cisco Packet Tracer. The network was designed following a hierarchical design which consisted of an access layer, distribution layer, and core layer. VLANs were used to distinguish between department traffic and guest traffic which improved network security and performance. To allow for communication between the guest and department VLANs, inter-VLAN routing was implemented using a single Layer 3 interface (router-on-a-stick). Routing decisions between the floors utilized the Open Shortest Path First (OSPF) routing protocol. Centralized services such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), and Web services (HTTP) were integrated into the network to support typical hotel operations. Security measures including Secure Shell (SSH) and Access Control Lists (ACLs) were implemented to secure the devices against non-privileged access, and secure tunnel access for remote administration, and to maintain traffic controls based on policy. A simulation test was performed for validation purposes and the analysis and results confirmed that the network was configured correctly. Successful connectivity in terms of direct and tagged VLAN access with appropriate access based on security field addresses, available services (e.g., DHCP), and enforcement of security measures, including denied service from a port VLAN based on ACL filtering, were provided during the simulation. The network was established correctly compared against the model specifications that were detailed and can be used as a practical reference free of charge for implementing a hotel network infrastructure.

VII. FUTURE WORK

Future enhancements can include:

- Incorporation of IoT-based devices like smart locks and camera systems.
- Organization of Wi-Fi VLANs and mobile access control.
- Monitoring and automation system using SNMP - Simple Network Management Protocol.
- Hot Standby Router Protocol-HSRP can be implemented for router redundancy and failover and provide continuous connectivity for routing in case of failure. Enhanced Interior Gateway Routing Protocol-EIGRP can also allow routes to converge faster and improved path selection in a dynamic environment.
- Hardware implement and stress-test in real-time.

REFERENCES

[1] A. Smith, “Designing Scalable Campus Networks,” *IEEE Communications*, vol. 59, no. 4, pp. 112–118, 2021.

[2] J. Lee, “VLAN Implementation in Simulated Environments,” *International Journal of Networking*, vol. 8, no. 2, pp. 45–52, 2020.