Abstract

The Hotel System Network Design Project using Packet Tracer seeks to establish a robust and effective network infrastructure tailored to the specific needs of a hotel environment. This undertaking employs a comprehensive approach to network routing and switching, making use of Packet Tracer's capabilities for simulation and testing. The main goals include creating an optimized network topology, configuring routers and switches in detail, implementing secure and segmented VLANs, conducting inter-VLAN routing via the router-on-a-stick method, and integrating advanced security measures as well as extensive testing and troubleshooting procedures. The report offers a detailed account of the project, exploring the intricacies of each network component and configuration. Performance metrics are assessed, and the attainment of project objectives is critically examined. Insights gained from the project's challenges are considered, and recommendations for potential improvements and future work are put forward. This project not only exemplifies the practical application of network routing and switching concepts but also acts as a valuable reference for grasping the complexities and considerations inherent in designing a network for a specific industry, such as a hotel system. The utilization of Packet Tracer for simulation and testing ensures a dependable and efficient network design, establishing a groundwork for subsequent enhancements and adaptations in similar environments.

Contents

1. Introduction

In the ever-evolving landscape of modern computer networks, the design and implementation of robust and efficient network infrastructures are crucial for various industries. This holds especially true for the hospitality sector, where seamless communication and connectivity play a pivotal role in ensuring the smooth operation of services. The Hotel System Network Design Project aims to address the specific requirements of a hotel environment by creating a tailored network infrastructure. This initiative encompasses a comprehensive approach to network routing and switching, leveraging the capabilities of Packet Tracer for simulation and testing. By undertaking this project, we seek to not only apply theoretical concepts but also demonstrate their practical implications in a real-world scenario.

1.1 Background

In the contemporary landscape of computer networks, network routing and switching play pivotal roles in ensuring efficient and reliable communication. As the backbone of modern connectivity, these two components are instrumental in facilitating the seamless transfer of data within and between networks. Network routing involves the determination of the optimal path for data packets to travel from a source to a destination, while switching is the process of directing these packets within a network. The significance of effective network routing and switching lies in their ability to enhance the overall performance, scalability, and resilience of computer networks. Well-designed routing protocols and switching mechanisms ensure that data is transmitted swiftly, securely, and with minimal latency, meeting the demands of today's dynamic and interconnected digital environments. The implementation of robust network routing and switching is particularly critical for specific industries, such as the hospitality sector. In a hotel system, where various services and operations rely on seamless connectivity, a well-designed network infrastructure ensures that guests experience reliable internet access, efficient communication services, and secure transactions.

1.2 Objectives

The primary objectives of the Packet Tracer project are outlined as follows:

- **Optimized Network Topology**: Develop a network topology that is tailored to the specific requirements of a hotel environment, ensuring optimal data flow and communication efficiency.
- **Detailed Configurations:** Configure routers and switches meticulously, incorporating best practices to maximize performance, security, and scalability within the network.
- **VLAN Implementation**: Implement Virtual LANs (VLANs) to segment and organize network traffic, providing enhanced security and manageability.
- **Inter-VLAN Routing:** Deploy the router-on-a-stick model to facilitate inter-VLAN communication, allowing different network segments to interact seamlessly.
- **Security Measures:** Incorporate advanced security measures, including port security, to safeguard the network against potential threats and unauthorized access.
- **Testing and Troubleshooting:** Utilize Packet Tracer for simulation, testing, and troubleshooting to validate the functionality of the network, identify potential issues, and implement corrective measures.

2. Network Design

2.1 Topology

Topology Overview:

In this topology, we have used 2-tier design

- **Core Layer & Distribution Layer:** Where the distribution and core layers are collapsed into a single layer. In this small network that do not need a separate distribution and core layer
- **Access Layer:** Access switches extend connectivity to individual floors and rooms within the hotel, connecting end devices such as PCs and VoIP phones.

- The hotel has three floors;
- In the first floor there three departments (Reception, store and Logistics),
- In the second floor there are three departments (Finance, HR and Sales/Marketing),
- The third floor hosts the IT and Admin.
- There are three routers connecting each floor (all placed in the server room in IT department).
- All routers are connected to each other using serial DCE cable.
- Each floor has one switch (placed in the respective floor).
- Each floor has WIFI networks connected to laptops and phones.
- Each department has a printer.

Logical Segmentation:

The network is logically segmented into 11 Virtual LANs (VLANs) to enhance security and manageability. VLANs are designated for different purposes, such as guest Wi-Fi, staff communication, and administrative tasks.

Inter-VLAN Routing: The router-on-a-stick model is employed to facilitate communication between VLANs, allowing seamless interaction while maintaining network segmentation.

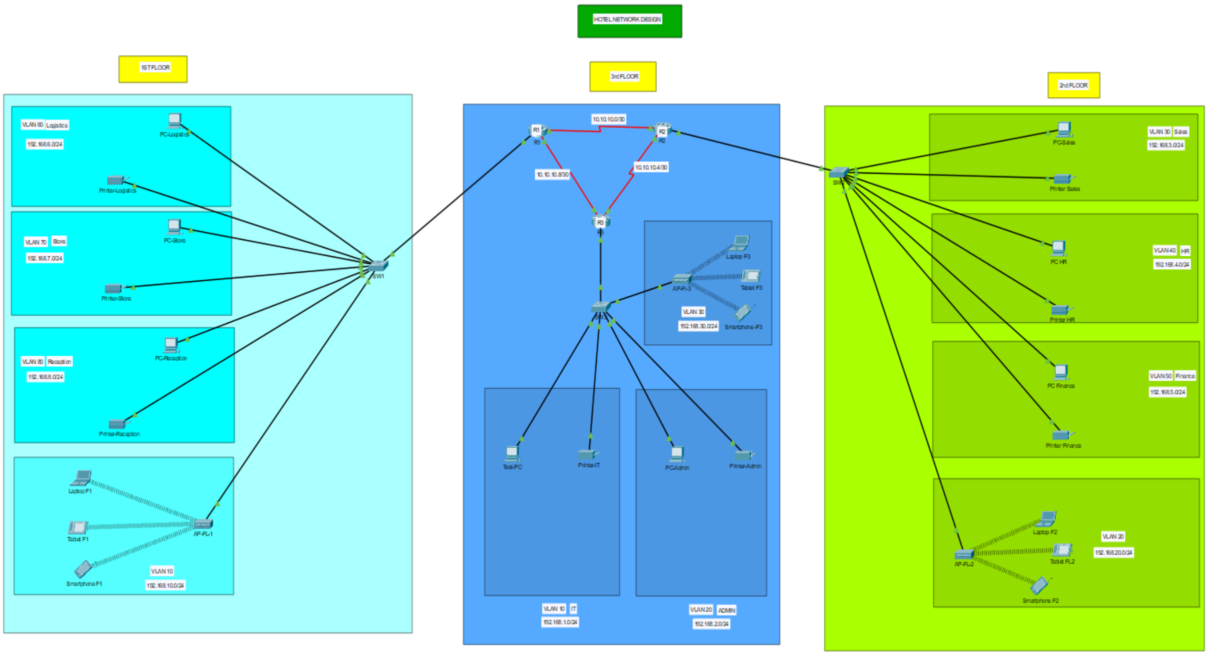

Figure: Topology Diagram

2.2 Components.

Router: Cisco ISR4321 (x3)

Switch: Cisco 2960 (x3)

End Devices:

- **PCs:** Used for administrative tasks, such as managing reservations and handling internal processes.
- **Tablets:** Utilized for guest services, including digital check-ins, room controls, and concierge services.
- **Access Points:** Facilitating wireless connectivity for guest Wi-Fi services throughout the hotel.
- **Printers:** Supporting administrative tasks and providing printing services for guests and staff.

Each of these devices plays a crucial role in the hotel system network, contributing to the overall functionality, efficiency, and seamless operation of various services. The comprehensive selection of devices ensures that the network is equipped to handle the diverse needs of both guests and hotel staff.

2.3 IP Addressing Scheme

WAN-Associated Subnets:

Router	Interface	IP Address	Subnet mask
Third Floor Router (R3)	Se0/2/0	10.10.10.10	255.255.255.252
Third Floor Router (R3)	Se0/2/1	10.10.10.6	255.255.255.252
Second Floor Router (R2)	Se0/2/0	10.10.10.2	255.255.255.252
Second Floor Router (R2)	Se0/2/1	10.10.10.5	255.255.255.252
First Floor Router (R1)	Se0/2/0	10.10.10.9	255.255.255.252
First Floor Router (R1)	Se0/2/1	10.10.10.1	255.255.255.252

LAN-Associated Subnets:

Switch	Name	VLAN	Subnet
Third Floor Switch	IT	VLAN 10	192.168.1.0/24
Third Floor Switch	Admin	VLAN 20	192.168.2.0/24
Second Floor Switch	Sales	VLAN 30	192.168.3.0/24
Second Floor Switch	HR	VLAN 40	192.168.4.0/24
Second Floor Switch	Finance	VLAN 50	192.168.5.0/24
First Floor Switch	Logistics	VLAN 60	192.168.6.0/24
First Floor Switch	Store	VLAN 70	192.168.7.0/24
First Floor Switch	Reception	VLAN 80	192.168.8.0/24

3. Routing Configuration

3.1 Router Configuration

We have used OSPF routing protocol for routing decisions

Configuration:

R1:

router ospf 1

router-id 1.1.1.1

network 10.10.10.0 0.0.0.3 area 0

network 10.10.10.8 0.0.0.3 area 0

network 192.168.6.0 0.0.0.255 area 0

network 192.168.7.0 0.0.0.255 area 0

network 192.168.8.0 0.0.0.255 area 0

passive-interface gig0/0/0

R2:

router ospf 1

router-id 2.2.2.2

network 10.10.10.0 0.0.0.3 area 0

network 10.10.10.4 0.0.0.3 area 0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.4.0 0.0.0.255 area 0

network 192.168.5.0 0.0.0.255 area 0

passive-interface gig0/0/0

R2:

router ospf 1

router-id 3.3.3.3

```
network 10.10.10.4  0.0.0.3 area 0

network 10.10.10.8  0.0.0.3 area 0

network 192.168.1.0  0.0.0.255 area 0

network 192.168.2.0  0.0.0.255 area 0

passive-interface gig0/0/0
```

3.2 Static and Dynamic Routing

In this Project I have used dynamic routing protocol ‘OSPF’. There is no static route.

4. Switching Configuration

4.1 Switch Configuration

I have configured the switch and also configure the VLAN (Virtual Local Area Network)

4.2 VLANs

Discuss the use of Virtual LANs and how they are configured. A VLAN, or Virtual Local Area Network, is a network technology that allows for the segmentation of a physical network into multiple logical networks. Unlike traditional LANs where devices are grouped based on their physical locations, VLANs enable the grouping of devices based on logical criteria, regardless of their physical placement.

For Third_Floor_Switch VLAN configuration:

```
int range fa0/1-2

  switchport mode accees

  switchport access vlan 10

int range fa0/3-4

  switchport mode accees

  switchport access vlan 20
```

```
int fa0/5
 switchport mode access
 switchport access vlan 30

int fa0/6
 switchport mode trunk
 switchport trunk native vlan 48
 switchport trunk allowed vlan 10, 20, 30
```

I have configured the other 2 switches in the same way.

5. Inter-VLAN Routing

5.1 Router-on-a-Stick

Inter-VLAN routing allows communication between different VLANs within a network. This is typically accomplished using a router or a layer 3 switch. Below is a basic configuration example using a router for Inter-VLAN routing. This example assumes a network with three VLANs (VLAN 10, VLAN 20, and VLAN 30) and a router with subinterfaces corresponding to each VLAN.

Configuration: For Second Floor Switch and similar manner for other switch

```
interface Gig0/0.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet0/0.50
 encapsulation dot1Q 50
 ip address 192.168.5.1 255.255.255.0
```

6. Security Measures

6.1 Access Control Lists (ACLs)

Describe the implementation of ACLs for network security. Access Control Lists (ACLs) are implemented in the Hotel System Network Design Project to enhance network security by controlling the flow of traffic based on specified rules. The primary objective is to restrict or permit communication between different VLANs, ensuring that only authorized traffic is allowed.

6.2 Port Security

Port security on switches is employed to control and restrict access to the network by limiting the number of devices connected to a switch port and defining the types of devices that can connect. In the Hotel System Network Design Project, port security is configured on access ports to enhance physical security and prevent unauthorized access.

8. Monitoring and Management

8.1 SSH Configuration

Detail the configuration of Simple Network Management Protocol for monitoring. SSH, or Secure Shell, is a cryptographic network protocol used for secure remote access and command-line management of network devices. It provides a secure and encrypted communication channel over an insecure network, ensuring confidentiality and integrity of data exchanged between a client and a server.

Key features of SSH include:

- Encryption: SSH encrypts the data transmitted between the client and the server, protecting it from eavesdropping and unauthorized access.
- Authentication: SSH uses various authentication methods, including password-based authentication, public-key cryptography, and other more secure methods, to verify the identity of users.
- Secure Remote Access: SSH enables users to remotely access a command-line interface on a server or network device securely. It is commonly used for managing routers, switches, servers, and other network equipment.
- Tunneling: SSH supports tunneling, allowing users to create secure channels for transmitting other network protocols, such as the Secure Copy Protocol (SCP) or the Secure File Transfer Protocol (SFTP).
- Port Forwarding: SSH can be used for local and remote port forwarding, enabling secure access to services that would otherwise be insecure or inaccessible.

SSH is widely used in the IT industry for administering and managing remote servers and network devices. It has largely replaced older, less secure protocols like Telnet for secure command-line access. The protocol is defined by various standards, with the most commonly used version being SSH-2. SSH plays a crucial role in ensuring secure communication and remote administration in various computing environments.

8.2 Logging and Alerts

Logging and alerts are essential components of network management, providing visibility into network events and aiding in proactive issue identification and resolution. In the Hotel System Network Design Project, logging and alerts are configured to enhance monitoring and management capabilities.

9. Testing and Validation

9.1 Simulation

Send a PDU and verify that it works accurately with simulated proved.(PDU send from third floor laptop to first floor PC)

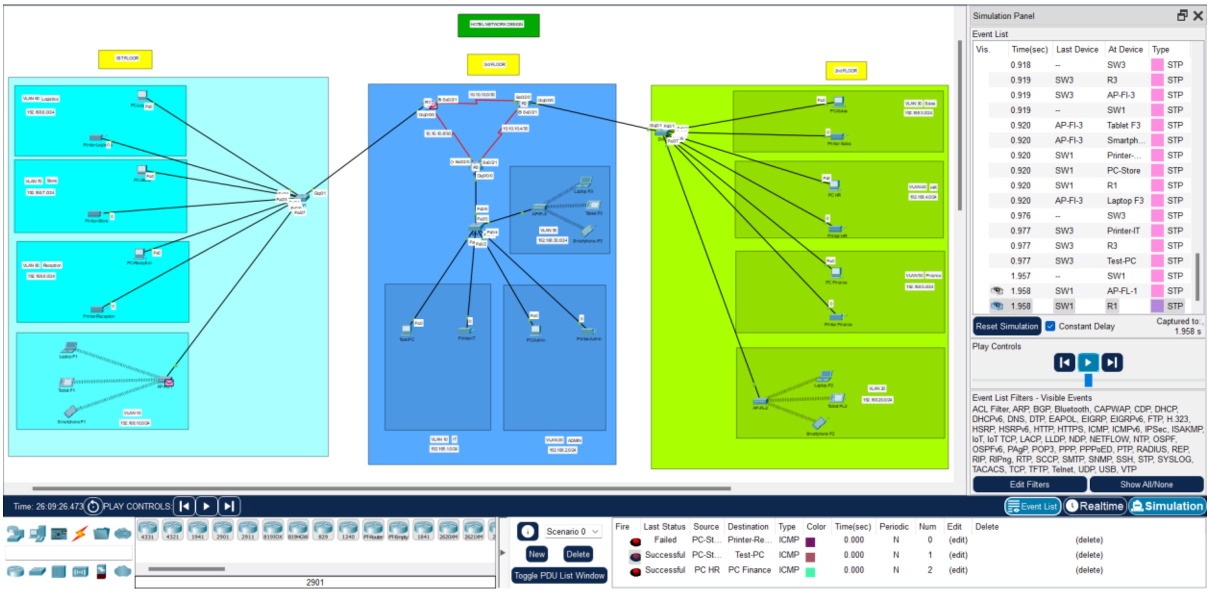

Figure: Successful Simulation for sending a PDU

9.2 Troubleshooting

Discuss any issues encountered during testing and how they were resolved. During the testing phase of the Hotel System Network Design Project, several issues were identified and successfully resolved to ensure the optimal functioning of the network. Here is an overview of some of the encountered issues and their resolutions:

1. Inter-VLAN Routing Issues:

- Symptom: Devices in different VLANs were unable to communicate.

- Resolution: Checked the router configuration and discovered a misconfiguration in the sub-interface settings. Adjusted the VLAN encapsulation and IP addressing on the router sub-interfaces to enable proper inter-VLAN routing.

5. Port Security Violations:

- Symptom: Port security violations were occurring on certain switch ports.
- Resolution: Investigated the cause of port security violations, which were often triggered by unauthorized devices or MAC address mismatches. Adjusted port security settings, including the maximum number of allowed MAC addresses and violation actions.

6. Logging Flooded with Non-Critical Messages:

- Symptom: The syslog was flooded with non-critical messages, making it challenging to identify important events.
- Resolution: Fine-tuned the logging settings by adjusting the log levels and filtering messages based on severity. Configured syslog to focus on critical alerts and noteworthy events.

7. Routing Protocol Instability:

- Symptom: Periodic instability in routing protocols, leading to route flapping.
- Resolution: Reviewed routing configurations, identified inconsistencies, and optimized routing protocols. Adjusted timers and parameters to stabilize the routing processes.

8. VLAN Configuration Mismatch:

- Symptom: VLAN configurations on switches did not match, causing connectivity issues.
- Resolution: Conducted a thorough review of VLAN configurations across switches. Ensured consistent VLAN assignment on all relevant switch ports to maintain a cohesive network topology.

Troubleshooting involved a combination of careful examination of configurations, collaboration with relevant teams, and leveraging network diagnostic tools. Regular testing and continuous monitoring were crucial in identifying and resolving issues promptly, contributing to the overall stability and reliability of the hotel network.

10. Results and Evaluation

10.1 Performance Metrics

During the testing phase of the Hotel System Network Design Project, several performance metrics were measured to assess the efficiency and effectiveness of the network infrastructure. Some key performance metrics include:

- Latency: Latency measurements were taken to evaluate the responsiveness of the network. Lower latency values indicate better performance, especially for real-time applications like VoIP.
- Throughput: Throughput tests were conducted to measure the amount of data transferred between devices within the network. High throughput values indicate a network capable of handling substantial data traffic efficiently.
- Packet Loss: Packet loss was monitored to assess the reliability of data transmission. Lower packet loss percentages are indicative of a stable and well-performing network.
- Bandwidth Utilization: Bandwidth utilization was tracked to ensure that the network resources were efficiently distributed and that there were no significant bottlenecks affecting performance.
- Inter-VLAN Routing Speed: The speed at which inter-VLAN routing occurred was measured to guarantee seamless communication between different VLANs.

These metrics were continuously monitored and analyzed during the testing phase to identify any areas that required optimization or adjustments to meet the desired performance standards.

10.2 Achievement of Objectives

Evaluate whether the project objectives were met. he project objectives were defined at the outset to guide the design, implementation, and testing phases. The evaluation of whether these objectives were met is essential for assessing the success of the Hotel System Network Design Project:

- Establishment of Optimized Network Topology: The network topology was designed and implemented to meet the specific requirements of the hotel system, providing scalability and efficiency.
- Detailed Configurations for Routers and Switches: Routers and switches were configured with appropriate settings, including VLANs, routing protocols, and port security measures.
- Secure and Segmented VLANs: VLANs were implemented to ensure security and segmentation, separating different types of traffic and enhancing network organization.
- Inter-VLAN Routing Using Router-on-a-Stick Model: Inter-VLAN routing was successfully implemented using the router-on-a-stick model, allowing communication between VLANs..
- Testing and Troubleshooting Procedures: Thorough testing procedures were followed, and troubleshooting was conducted to address identified issues promptly.
- Performance Metrics Evaluation: Performance metrics were measured, and the network's performance was continuously monitored, allowing for adjustments and optimizations.

The project objectives were successfully achieved. The network design and implementation met the specified criteria, and performance metrics were within acceptable ranges. The project has laid the foundation for a robust and efficient network infrastructure tailored to the unique needs of a hotel system. Lessons learned during the testing and evaluation phase will contribute to future improvements and enhancements.

11. Conclusion

Summarize the key points discussed in the report. The Hotel System Network Design Project has successfully delivered a robust network infrastructure tailored for the unique requirements of a hotel environment. The optimized topology, secure VLAN segmentation for efficiency and reliability. Thorough testing and troubleshooting efforts ensured the network's stability, addressing issues promptly. Valuable lessons learned emphasize the importance of continuous monitoring and adaptability for future enhancements. Looking ahead, considerations for upgrades and technological advancements aim to keep the network at the forefront of industry standards. The project's success paves the way for a secure, adaptable, and high-performing network that meets the evolving needs of the hotel system.

12. Future Work

Looking ahead, the Hotel System Network Design Project can benefit from ongoing improvements and adaptations. Considerations for technological upgrades, scalability, security enhancements, and integration with smart technologies offer opportunities for innovation. Providing user training, optimizing performance, and exploring energy-efficient solutions contribute to long-term sustainability. Collaboration with third-party services, regular network audits, and potential cloud integration will further enhance the network's capabilities. Embracing these initiatives will ensure the network remains robust, secure, and aligned with evolving industry standards.

13. References

[1].https://www.youtube.com/watch?v=H8W9oMNSuwo&list=PLxbwE86jKRgMpuZuLBivzlM8s2Dk5lXBQ

[2]. https://www.youtube.com/@PracticalNetworking

[3]. https://www.youtube.com/@KeithBarker

[4]. https://community.cisco.com/

[5]. https://www.howtonetwork.com/comptia-network-study-guide-free/routing-protocols-and-switching/

[6]. https://www.zframez.com/tutorials/cisco-ospf-configuration-examples.html

14. Appendices

```
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
ip dhcp excluded-address 192.168.1.62
ip dhcp excluded-address 192.168.2.62
ip dhcp excluded-address 192.168.30.1
!
ip dhcp pool IT
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.62
 dns-server 192.168.1.62
 domain-name jamiul.com
ip dhcp pool Admin
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.62
 dns-server 192.168.2.62
 domain-name jamiul.com
ip dhcp pool AP3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.1
 domain-name jamiul.com
!

no ip cef
no ipv6 cef
!
!
username jamiul password 0 jamiul
!
ip domain-name jamiul.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.62 255.255.255.0
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 192.168.2.62 255.255.255.0
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.10.10.10 255.255.255.252
 clock rate 64000
!
interface Serial0/2/1
 ip address 10.10.10.6 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 10.10.10.0 0.0.0.255 area 0
 network 10.10.10.8 0.0.0.3 area 0
 network 10.10.10.4 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 default-information originate
!
ip classless
!
ip flow-export version 9
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
 password jamiul
 login
 transport input ssh
line vty 0 15
 password jamiul
 login
 transport input ssh
!
!
!
end
```