**Design of Wireless Secured Organisation Network**

**Table of Contents**

[Brief Idea and Overview 3](#_Toc138278894)

[Organizational Network 3](#_Toc138278895)

[Network Attacks and Security Issues 3](#_Toc138278896)

[Gateway Routing Protocol and Network Security 4](#_Toc138278897)

[Gateway Routing Protocol 4](#_Toc138278898)

[Advantages 4](#_Toc138278899)

[Scope of Research 5](#_Toc138278900)

[Project Aim 5](#_Toc138278901)

[Research Questions 5](#_Toc138278902)

[Objectives of Project 5](#_Toc138278903)

[Tool to be Used 6](#_Toc138278904)

[Project Planning 7](#_Toc138278905)

[References 8](#_Toc138278906)

# **Brief Idea and Overview**

## **Organizational Network**

Organizational networks have become increasingly complex in the modern business world. With the advent of new technologies, organizations have adopted new ways of conducting business, which has led to increased complexity in network architectures. This complexity has also increased the risk of cybersecurity threats to organizations (Ahmed, et al., 2022). Organizations are increasingly deploying a wide range of security measures to protect their networks from these threats. However, these measures are not without their own set of issues (Abomhara & Køien, 2014). The present project will explore the design of the wireless network for organizations with integral security to overcome or avoid possible network and data breaches using network security.

## **Network Attacks and Security Issues**

Organizational networks are used by many people out of which some are well aware of the technical aspects and others do not (Abbas & Yu, 2018) . These mixed behaviours and usability of the network may raise different issues which may pose the security of the organisation. Some of the possible issues have been discussed below:

1. One of the primary organizational network issues is the lack of a centralized network architecture. Many organizations have complex network architectures that have been built over time, leading to a lack of centralization (Yajing & Fang, 2018). This makes it difficult to manage network resources and detect security threats. In addition, it can be difficult to maintain network performance across such a complex network architecture.
2. Another organizational network issue is the lack of standardization. With the increasing use of cloud services, organizations are deploying a wide range of technologies that may not be standardized (Nastase, 2017). This can lead to compatibility issues, making it difficult to integrate different technologies and services. This lack of standardization can also lead to security vulnerabilities, making it easier for hackers to exploit weaknesses in the network.
3. Organizational security issues are also a concern for businesses. One of the primary security issues is the lack of employee awareness (Nastase, 2017). Many employees are not aware of the risks associated with cybersecurity. This can lead to employees inadvertently becoming the weak link in the security chain. To address this issue, organizations need to provide regular training to their employees to increase their awareness of cybersecurity risks and best practices.
4. Another security issue is the lack of security policies and procedures. Organizations need to have clear policies and procedures in place to address security risks (Ashok, et al., 2021). This includes policies around password management, access controls, and data protection. Without clear policies and procedures, organizations are more vulnerable to security threats.

## **Gateway Routing Protocol and Network Security**

### **Gateway Routing Protocol**

As technology advances, so do cyber threats, and organizations need to stay ahead of the game to protect their data and systems. One of the most crucial aspects of network security is the selection of the right routing protocol (Alhamry & Alomary, 2022). Gateway Routing Protocol (GRP) is a protocol used to exchange routing information between routers in a network. It is a type of distance vector routing protocol that uses hop count as the primary metric for path selection (Agarwal, et al., 2019). GRP is used in smaller networks and is simpler to configure than other routing protocols like OSPF and BGP.

### **Advantages**

GRP has several advantages when it comes to network security.

* Firstly, it allows for the efficient exchange of routing information between routers, which means that network traffic can be directed along the most efficient path (Abbas & Yu, 2018). This reduces the risk of congestion and improves the overall performance of the network.
* Secondly, GRP supports authentication, which means that only authorized routers can exchange routing information. This prevents unauthorized access to the network and reduces the risk of attacks like spoofing and hijacking (Nastase, 2017).
* Thirdly, GRP is a reliable protocol that can quickly detect and respond to changes in the network topology. This means that if a router goes down or a link fails, the network can quickly reroute traffic along an alternative path, reducing the risk of downtime and improving network availability (Zahid, et al., 2020).

## **Scope of Research**

The organizational network will be designed in the project with the application of gateway routing protocol so that possible network issues such as breaches can be avoided. In this context, the network devices will be connected to design the entire network and the protocol will be incorporated into the network router so that it will prohibit any unauthorised access to the network.

# **Project Aim**

The project aims to design a Wireless network for organizational usage with the application of network security through the gateway routing protocol.

# **Research Questions**

The research questions are as follows:

1. What are the possible challenges that may be faced at the time of network design and device connectivities?
2. How can the gateway routing protocol protect the organizational network and its users from data breaches?
3. Can the network be designed with less cost compared to the existing models with similar technologies?

# **Objectives of Project**

The project objectives have been discussed below:

1. To gather the necessary ideas concerning the network design with the implication of different network devices.

Deliverables and Outcomes: Understanding the process of designing a network by connecting necessary network devices.

Time: 1 week

1. To study and review the previous research papers concerning network design along with the security implication on the organizational network.

Deliverables and Outcomes: Literature review and gathering of necessary knowledge on network design and network security for organisations.

Time: 3 weeks

1. To select the network design tool (Packet Tracer) using which the organisational network will be designed by taking all necessary network devices into concern; Using this tool, the devices will be connected and the IP addresses will be assigned

Deliverables and Outcomes: Selection of network design tool and design of the organisational network with the assignment of IP addresses in all connected devices.

Time: 1 week

1. To apply Gateway Routing Protocol for network security by configuring the network router.

Deliverables and Outcomes: Application of network security using GRP.

Time: 1 week

1. To simulate and test the network using the PDU transfer process and Ping Process.

Deliverables and Outcomes: Testing Secured Organizational Network.

Time:

1. To prepare the final project report.

Deliverables and Outcomes: Final Project Report

Time: 3 weeks

# **Tool to be Used**

For the project, Packet Tracer has been chosen as the network design and simulation tool because of the below-mentioned reasons:

1. It provides all necessary network devices which can be used to design the organisational network.
2. It can be used without any purchase
3. It provides the PDU transfer process through which the real-time simulation can be done to test the network.
4. It provides the real-time Ping process (the same which can be done through the command prompt of the computer).

# **Project Planning**

The Gantt chart for the project is shown below:



# **References**

Abbas, N. & Yu, F., 2018. Design and Implementation of a Video Surveillance System for Linear Wireless Multimedia Sensor Networks. *3rd International Conference on Image, Vision and Computing (ICIVC),* pp. 524-527.

Abomhara, M. & Køien, G. M., 2014. Security and privacy in the Internet of Things: Current status and open issues. *International Conference on Privacy and Security in Mobile Systems (PRISMS).*

Agarwal, K., Agarwal, A. & Misra, G., 2019. Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT. *Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* pp. 112-118.

Ahmed, A. J., Rashid, S. A. & Hamdi, M. M., 2022. A review of Wireless Sensor Network. *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA),* pp. 1-5.

Alhamry, M. & Alomary, A., 2022. Exploring Wi-Fi WPA2-PSK protocol weaknesses. *International Conference on Data Analytics for Business and Industry (ICDABI),* pp. 1-4.

Ashok, et al., 2021. Implementation-Of-Smart-Home-By-Using-Packet-Tracer. *IJSTR.*

Nastase, L., 2017. Security in the Internet of Things: A Survey on Application Layer Protocols. *Control Systems and Computer Science (CSCS) 2017 21st International Conference,* pp. 659-666.

Yajing, L. & Fang, L., 2018. Research on Security Isolation Method for Wireless Public Network Oriented to Smart Power Distribution Service. *2018 IEEE 4th International Conference on Computer and Communications (ICCC),* pp. 1160-1165.

Yang, A. et al., 2019. Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms. *IEEE Internet of Things Journal,* pp. 2521 - 2530.

Zahid, M. N., Jiang, J. & Lu, H., 2020. Security Issues and Challenges in RFID, Wireless Sensor Network and Optical Communication Networks and Solutions. *3rd International Conference of Safe Production and Informatization (IICSPI),* pp. 592-599.

Zielonka, A. et al., 2021. Smart Homes: How Much Will They Support Us? A Research on Recent Trends and Advances. *IEEE Access ,* pp. 26388 - 26419.