

# **Small Business Network System with Secure E-Commerce Server**

**18CSS202J- Computer Communication Project Report**

*Submitted by*

**V.R.Rishendra-(RA2111026010221)**

**S.Rakesh            -(RA2111026010222)**

**S.d Azhar           -(RA2111026010220)**

**SR.Balakathir -(RA2111026010218)**

*Submitted to*

**Dr.Anitha D**

Assistant Professor, Department of Computational Intelligence

*in partial fulfilment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

In

**COMPUTER SCIENCE ENGINEERING  
WITH SPECIALIZATION IN  
ARTIFICIAL INTELLIGENCE AND  
MACHINE LEARNING**



**SRM**

INSTITUTE OF SCIENCE & TECHNOLOGY  
*Deemed to be University u/s 3 of UGC Act, 1956*

**SCHOOL OF COMPUTING**

**DEPARTMENT OF COMPUTATIONAL INTELLIGENCE**

**COLLEGE OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR- 603 203**

**April 2023**



**SRM**  
INSTITUTE OF SCIENCE & TECHNOLOGY  
Deemed to be University u/s 3 of UGC Act, 1956

**SRM INSTITUTION OF SCIENCE AND TECHNOLOGY  
KATTANKULATHUR-603203**

**BONAFIDE CERTIFICATE**

Certified that this Course Project Report titled “**Small Business Network System with E-Commerce**” is the bonafide work done by V.R.Rishendra-(RA2111026010221),S.Rakesh -(RA2111026010222),S.d Azhar(RA2111026010220), SR.Balakathir -(RA2111026010218) who carried out under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

**SIGNATURE**

Faculty In-Charge

**Dr. Anitha**

Assistant Professor

Department of CINTEL

SRM Institute of Science and Technology

Kattankulathur Campus, Chennai

**HEAD OF THE DEPARTMENT**

**Dr. R Annie Uthra**

Professor and Head ,

Department of Computational Intelligence,

SRM Institute of Science and Technology

Kattankulathur Campus, Chennai

# Table of Contents

Abstract:..... 4

Introduction..... 5

Objective:..... 6

Project scope ..... 7

Requirements ..... 7

Requirement Analysis..... 7

Network Diagram..... 8

TCP/IP Table ..... 9

Router configuration ..... 9

IP address..... 9

NAT ..... 10

ACL..... 11

Solution explanation ..... 12

Hardware List..... 12

Conclusion: ..... 13

References :..... 14



## Abstract:

Small business e-commerce websites make an excellent target for malicious attacks. Small businesses do not have the resources needed to effectively deal with attacks. Large and some mid-size organization have teams that are dedicated to dealing with security incidents and preventing future attacks. Most small businesses do not have the capabilities of dealing with incidents the way large organizations do.

Security of e-commerce websites is essential for compliance with laws and regulations as well as gaining and maintaining the trust of consumers, partners and stakeholders. Many security standards have been established by various organizations to help guide security of small business servers, however, many of those standards or guidelines are too costly or time consuming. This paper<sup>1</sup> will discuss how attacks are carried out and how a small business can effectively secure their networks with minimum cost.

The network system integrates e-commerce to provide businesses with a platform to sell their products and services online, expanding their reach to a larger customer base. Additionally, the network system allows for better communication and collaboration among employees, partners, and customers, increasing productivity and customer satisfaction. Overall, the system provides small businesses with a comprehensive solution for managing their operations and growing their business in the digital age.

Small businesses face unique challenges in the current digital landscape. While e-commerce provides a significant opportunity for growth and expansion, it can also be overwhelming to navigate. A small business network system that integrates e-commerce can provide businesses with the tools they need to succeed in the online marketplace.

The network system allows small businesses to streamline their operations and reduce costs by providing a central platform for managing inventory, orders, and payments. It also enables businesses to optimize their online presence with customizable websites, search engine optimization, and digital marketing tools. This can help businesses attract new customers and build brand awareness.

## Introduction

A Small Business Network System with secure E-Commerce server refers to the use of computer networking technology to connect different devices and systems within a small business organization, enabling them to share resources and communicate efficiently. The addition of an e-commerce component to the network system means that the business can conduct its commercial transactions online, such as selling products or services over the internet.

Many businesses have come to the realization that, in order to compete in the market, key business processes need to be part of the Internet. E-commerce has become a popular adaptation for businesses, which has been a major transformation for many businesses. The popularity of the Internet has transformed traditional commerce into e-commerce, which has proven to be a successful platform for many businesses. Small businesses provide an easy target for attackers because they typically have limited funds and do not have dedicated personnel to monitor, update and defend their systems. The attacks on small businesses continue to rise each year

In essence, a small business network system with e-commerce enables a business to operate more efficiently by streamlining its operations and increasing its reach. With the use of this system, small businesses can reach a wider audience, reduce their overhead costs, and increase their revenues. It also allows for better inventory management, real-time order tracking, and quicker payments, among other benefits.

The key components of a small business network system with e-commerce may include hardware such as routers, switches, servers, and computers, as well as software for managing orders, inventory, and customer data. Security measures such as firewalls, encryption, and backup systems are also essential to protect the business from cyber threats.

Overall, a small business network system with e-commerce can provide many benefits to small businesses looking to expand their reach and streamline their operations. By leveraging the power of technology, small businesses can compete on a more level playing field with larger companies and improve their overall success.

## Objective:

The objective of implementing a Small Business Network System with E-Commerce is to improve the efficiency and profitability of a small business by leveraging technology to streamline its operations and expand its reach.

The specific objectives of such a system may include:

**Facilitating online sales:** Enabling customers to purchase products or services directly from the business website or online store, leading to increased sales and revenue.

**Improving inventory management:** Keeping track of inventory levels in real-time, making it easier to manage stock levels, reduce stockouts, and optimize ordering.

**Enhancing customer service:** Providing customers with easy access to product information, order status, and support through online platforms, leading to higher customer satisfaction and retention.

**Streamlining business processes:** Automating routine tasks such as order processing, billing, and inventory management, reducing manual labor and errors while increasing efficiency.

**Securing business data:** Protecting sensitive business information and customer data from cyber threats such as hacking, malware, and data breaches.

Overall, the objective of a Small Business Network System with E-Commerce is to create a secure and efficient digital platform that enables small businesses to compete in the modern business environment and achieve their strategic goals.

## Project scope

A network has to be designed for a small business organization which has 100 users. The organization hosts an e-commerce application on a server which is accessible to internet users using https and with a public IP address.

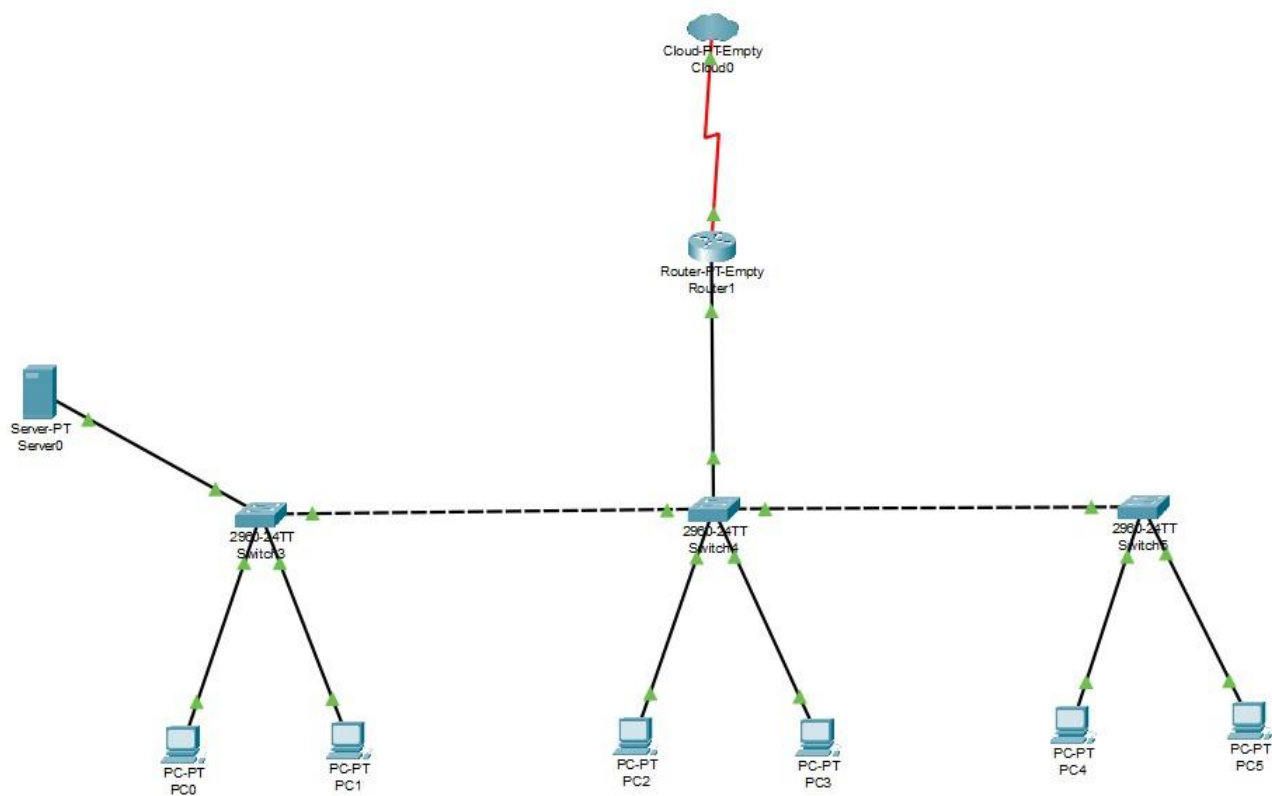
## Requirements

1. Identify the appropriate hardware which would be used (Cisco )
2. Users on the internet should be able to access only https on the e-commerce server.
3. Users on the internet should have access only to the public IP address of the server and not the private IP address.
4. The users in the organization should have full access to the server.
5. TCP/IP Network design with IP addressing
6. Features and configuration required on the hardware with explanation.

## Requirement Analysis

1. The server has a public IP address which is used by internet users for accessing the e-commerce application. The server is required to be accessible by users on the LAN. This requirement can be implemented by the use of static nat feature which is available on Cisco routers. Static NAT feature is configured which would create a mapping with the private and public IP address of the server.
2. There are 100 users on the LAN network. The server and the router is also part of the network. A total of 102 devices are there on the network for which 102 ports on the switch is required. 3 nos of 48 port switches are recommended (considering future expansion plans as well) to accommodate the 102 devices.
3. ACL, which stands for access control lists are required to be available on the router, for configuring access control to the server for users on the internet.
4. Cisco router which supports NAT and ACL and 3 nos of 48 port switches would be required in total. The details of the make and model are provided at the end of the report.

# Network Diagram



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC5	Router1	ICMP		0.000	N	0	(edit)	
	Successful	Server0	PC3	ICMP		0.000	N	1	(edit)	
	Successful	PC0	PC4	ICMP		0.000	N	2	(edit)	



## TCP/IP Table

Device	IP address
<b>Router LAN</b>	192.168.1.1
<b>Server IP</b>	192.168.1.2
<b>PC's (100)</b>	192.168.1.3 – 192.168.1.102

## Router configuration

### IP address

The LAN ip address of the router is 192.168.1.2. The details of the configuration are shown below.

*Router(config)#interface fastethernet 0/0*

*Router(config-if)# ip address 192.168.1.1 255.255.255.0*

*Router(config-if)#no shutdown*

The interface which is connected to the internet would receive the IP address from the ISP.

## NAT

NAT, which stands for Network address translation is configured for mapping the public IP address of the server to the private IP address. This would also achieve the requirement of internet users to access the server with the public IP address and hide the private IP address. The details of the configuration are shown below

The public IP address which is provided by the ISP, is assumed to be 1.2.3.4

```
Router(config)# ip nat inside source static 192.168.1.2 1.2.3.4
```

```
Router(config)#interface fastethernet 0/0 (LAN interface)
```

```
Router(config-if)#ip nat inside
```

```
Router(config)#interface serial 0/0 (Internet interface)
```

```
Router(config-if)#ip nat outside
```

The first line creates a static nat entry which would map the private IP address of the server which is 192.168.1.2, with its public IP address.

The second and third line applies the inside interface for NAT as LAN interface.

The fourth and fifth line applies the outside interface for NAT as the internet interface.

## ACL

ACL, which stands for access control lists, is used for controlling access to the e-commerce server to the internet users. The details of the ACL configuration are shown below.

```
Router (config)#access-list 101 permit tcp any host 1.2.3.4 eq 443
```

```
Router(config)#access-list 101 deny ip any any
```

The first line creates an extended ACL with number 101 which permits any host to access tcp port 443 which is for https servers to the public IP address of the e-commerce server which is 1.2.3.4

The second line denies all other traffic to all systems.

```
Router(config)#interface serial 0/0
```

```
Router(config-if)#ip access-group 101 in
```

The above configuration applies the ACL as inbound on the internet interface. This would ensure that all users from the internet would only have https access to the e-commerce server and all other traffic from the internet would be denied into the LAN network.

## Solution explanation

1. Users on the LAN network would have complete access to the server as they reside on the same network address of 192.168.1.0/24 and there is no access control configured.
2. Users from the internet would only have access to the https service on the e-commerce server. All other communication is blocked for internet users to the LAN using ACL 101.
3. Users from the internet would have access to the server using the public IP address of 1.2.3.4. Static NAT also hides the private IP address of the server and prevents users from directly accessing the system using the private IP address.

## Hardware List

Item	Description	Qty
Router	CISCO 1841 Integrated Services Router	1
Switch	Cisco WS-C3750-48PS-S	3

## Conclusion:

E-commerce is an effective way to do business. It allows businesses to provide products and services to a wider population than they could with traditional brick and mortar operations. However, e-commerce also comes with a wide variety of risks that need to be mitigated to operate securely. Small businesses provide an easy target for attackers because they typically have limited funding and do not have dedicated network professionals to monitor and protect their network. Hackers have a wide variety of tools that allow them to attack networks even with little technical knowledge. Hackers use a system along with their tools to attack systems. They first need to gather as much information as possible about the target system, scan for open ports, scan for vulnerabilities and then conduct their attack. Along with technical attacks, some attackers might try physical attacks through social engineering and gain access to the business servers by pretending to be someone they are not.

Small businesses need to take as many precautions as possible to protect their systems, even if it means spending extra money to do so. There is really no way of completely securing a network, but there are ways to minimize the chances of becoming a victim. Limiting the chances of becoming a victim is better than trying to repair the damages after an attack, which may not be repairable. Attacks come in many forms, so it is imperative to ensure that as many security measures are put in place as possible. The implementation of various security measures is important for the protection of family, business continuity and national security. With the possible outcomes of an attack on a network, businesses should take network security very seriously and properly protect their systems.



## References :

- 1) <https://khyberacademy.com/importance-uses-of-computer-in-communication/>
- 2) <https://www.researchgate.net/>
- 3) <https://www.wikipedia.com/>
- 4) <https://www.cisco.com/site/in/en/index.html>
- 5) <https://geekflare.com/secure-ecommerce-site/>
- 6) <https://goabacus.com/secure-a-small-business-network-guide-checklist-and-advice/>
- 7) <https://www.business.com>
- 8) <https://www.bigcommerce.com/>
- 9) <https://smallbusiness.chron.com/>
- 10) <https://www.grin.com/>