**INTRUSION DETECTION SYSTEM**

A COMPUTER NETWORKS PROJECT REPORT

BY

**M Sri Charan Saichandra(RA1911028010128)**

**Gnana Ganesh(RA1911028010134)**

**M. Pranay(RA1911028010125)**

Under the guidance of

**Dr P. Balamurugan**

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

in

Department of networks and communications



**FACULTY OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**Kattankulathur, Chengalpattu District**

NOVEMBER 2021

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**(Under Section 3 of UGC Act, 1956)**

**BONAFIDE CERTIFICATE**

Certified that this project report **"Intrusion detection system"** is the bonafide work of **M. Sri Charan Saichandra(RA1911028010128), Gnana Ganesh(RA1911028010134), M.Pranay(RA1911028010125)** who carried out the project work under my supervision.

**SIGNATURE**  **SIGNATURE**

**Dr.P. BALAMURUGAN**  **Dr.E. SASIKALA,**

**Associate Proffessor Course Cordinator**

**Associate Proffessor Associate Professor,**

SRM Institute of Science and Technology Data Science and Business Systems

Potheri, SRM Nagar, Kattankulathur, SRM Institute of Science and Technology

Tamil Nadu 603203 Potheri, SRM Nagar, Kattankulathur,

Tamil Nadu 603203

**ACKNOWLEDGEMENT**

We express our heartfelt thanks to our honorable **Vice Chancellor Dr.**

**C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar**

**Dr. S. Ponnusamy,** for his encouragement

We express our profound gratitude to our **Dean (College of**

**Engineering and Technology) Dr. T. V.Gopal**, for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of

Computing **Dr. Revathi Venkataraman**, for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor Dr.M.LAKSHMI, Professor and Head, Data Science and Business Systems** and **Course Cordinator Dr.E. Sasikala, Associate Professor, Data Science and Business Systems** for their constant encouragement and support.

We are highly thankful to our Course project Internal guide **Dr.P.Balamurugan**, **Associate Professor, Department of Networking and Communications**, for his assistance, timely suggestion and guidance throughout the duration of this course project.

We extend my gratitude to **Dr. ANNAPURANI PANAIYAPPAN. K, Professor and Head, Department of Networking and Communications, School of Computing** and my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who

directly and indirectly contributed to the successful completion of our project. Above

all, I thank the almighty for showering his blessings on me to complete my

Course project

**CHAPTER 1**

**ABSTRACT**

Intrusion Detection System is a software or a device that can monitor all

the suspicious activities in the network. Any intrusion activity or violation is

reported or informed either to administrator or this information can be

centrally collected in a system called SIEM (Security Information and

Event Management). It collects and combine information from different

sources and it uses alarm filtering techniques. There are two most

common types of IDS. (NIDS) Network based Intrusion detection system

and (HIDS) Host based Intrusion detection system.

HIDS is used for monitoring important operating system files and NIDS are

used to analyze incoming network traffic. Here’s how IDS work, IDS when

placed at a strategic point or points within a network to monitor traffic to

and from all devices on the network, an IDS will perform an analysis of

passing traffic, and match the traffic that is passed on the subnets to the

library of known attacks. Once an attack is identified, or abnormal

behaviour is sensed, the alert can be sent to the administrator.

Modern networked business environments require a high level of security

to ensure safe and trusted communication of information between various

organizations. Cyber-attacks will only become more sophisticated, so it is

important that protection technologies adapt along with their threats.

**Table of Contents**

**CHAPTERS CONTENTS PAGE NO.**

1. **ABSTRACT**  4

2. **INTRODUCTION** 6

3. **REQUIREMENT ANALYSIS**  8

4.  **ARCHITECTURE AND DESIGN**  11

5. **IMPLEMENTATION**  18

6. **EXPERIMENT RESULTS & ANALYSIS**  21

**6.1. RESULTS**

**6.2. RESULT ANALYSIS**

**6.3. CONCLUSION & FUTURE WORK**

7.  **REFRENCES** 27

**CHAPTER 2**

**INTRODUCTION**

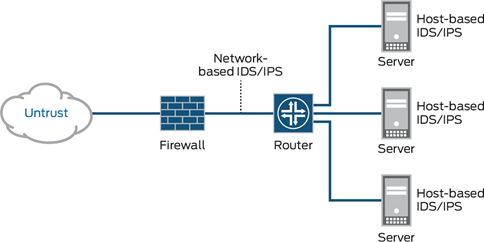
An IDS is basically a software or device that is categorised into two common parts

one is NID i.e. Network Intrusion Detection and second is HID i.e. Host Intrusion

Detection. The work of both the NID & HID is same but their level is different. But

IDS are categorised into 5 types – NIDS, HIDS, PIDS, Hybrid IDS & APIDS. Work is

same to detect intrusions but they are used at different levels.



You are now clear that where HIDSs are used and where NIDSs are used.

In this project I have implemented Intrusion Detection System by creating 3

different networks. Implementing the IDS is very challenging task as it needs the

implementor to have proper knowledge with prior knowledge with some

common and special network devices and ethernet cables. We have to know that

how to deal with the CLI i.e. Command Line Interface. As I am performing this

project on Cisco Packet Tracer – A best available simulation tool which allows

users to see the working of network in real time.

A layout of the network should be made prior to implementation of IDS as I’m

implementing NIDS. There are parameters which are to be kept in mind while I

designed network and configure IDS. Here are some ‘can’s and ‘can not’s about

the IDS.

- CAN recognize and report alterations to data.

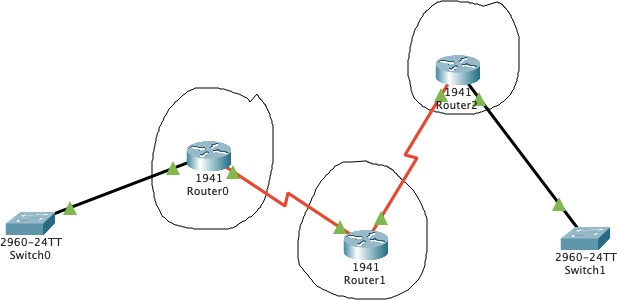
- CAN detect when your system is under attack.

- CAN detect errors in your system configuration.

- CAN NOT analyse all the traffic on a busy network.

- CAN NOT prevent system from that attack which it detects.

- CAN NOT deal with some of the modern network hardware and features.



**CHAPTER 3**

**REQUIREMENT SPECIFICATION**

**Software Requirements**

Itis required to have (CISCO PACKET TRACER) installed on the System. Every

implementation is done on this tool.

**Hardware Requirements**

-Intel Pentium 4, 2.53GHz or equivalent Processor

- 2GB Ram

- 1GB of free storage space

- Display of resolution 1024\*768

- Language fonts supporting Unicode encoding

- Latest video card and OS updates

**Cisco Packet Tracing**

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems

that allows users to create network topologies and imitate modern computer

networks. The software allows users to simulate the configuration of Cisco

routers and switches using a simulated command line interface. Packet Tracer

makes use of a drag and drop user interface, allowing users to add and remove

simulated network devices as they see fit. The software mainly focus towards

Certified Cisco Network Associate Academy students as an educational tool for

helping them learn fundamental CCNA concepts. Previously students enrolled in

CCNA Academy program could freely download and use the tool free of charge

for educational use.

**Command Line Interface**

•To configure any device in packet tracer you are required to open or access its

CLI. You can do it by clicking any device and then navigating to CLI tab. Once you

are at CLI you can perform all Cisco Commands here.

•A Cisco IOS router command line interface can be accessed through a console or

connection, modem connection, or a telnet/ssh session.

•Regardless of which connection method is used, access to IOS command-line

interface is generally referred to as an EXEC session

•As a security feature, Cisco IOS separates EXEC sessions into two different

access levels — the user level and the privileged EXEC level.

•EXEC user level allows a person to access only a limited amount of basic

monitoring commands.

•Privileged EXEC level allows a person to access all the router’s commands (e.g.

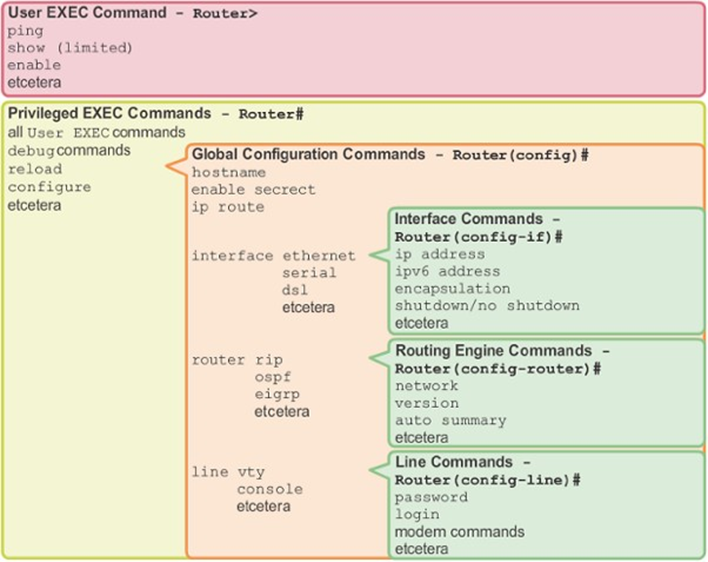
configuration and management) and can be password protected to allow only

authorized users the ability to configure or maintain the router.

•Once an EXEC session is established, commands within Cisco IOS are

hierarchically structured. In order to be able to configure the router, it is

important to understand this hierarchy.



**CHAPTER 4**

**ARCHITECTURE AND DESIGN**

**4.1 Project Overview**

In this section you will find all the explanations about this project and how it was

approached. All the software components and commands used for implementing

this project will be discussed in this project. Problems encountered during the

journey of this project will also be discussed in this section. The Ultimate goal of

this project is to log all the suspicious activity entering into the network. This

made possible with a specialised software called IDS.

**4.2 Research Stage**

The research stage was a critical stage that provided our team with the

knowledge necessary to complete the other stages of our project. This stage was

ongoing process throughout the project until it is completed. During the

development stage we have learnt many new things by researching in the web.

Our research encompassed a wide range of sources, which included studies done

at different universities and hobby enthusiast sources. Our research includes

different signatures used to activate detection against different types of traffic

Protocols

**4.3 Project Layout Stage**

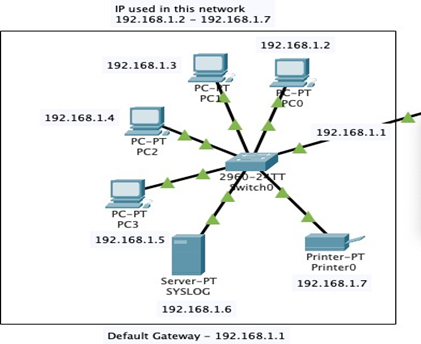
The network layout stage includes the whole network blueprint that on which

type of network our IDS will be implemented. We are using 3 different types of

networks which has some hosts and servers inside it.

The First Network is made of IPv4 Addressing having the IP addresses in range

of 192.168.1.2 – 192.168.1.7 Default Gateway for this Network is 192.168.1.1



•Devices in this network –

-4 Different PCs

-1 SYSLOG Server

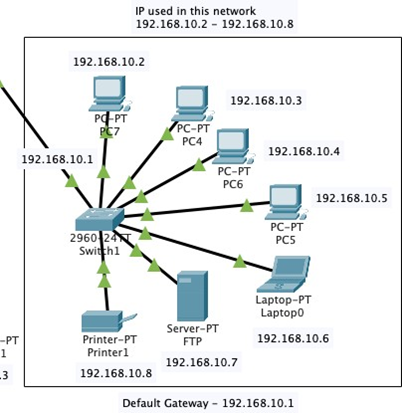
-1 Printer

-1 Switch as shown in Figure

The First Network is made of IPv4 Addressing having the IP addresses in range

of 192.168.10.2 – 192.168.10.8

Default Gateway for this Network is 192.168.10.1



•Devices in this network –

* 4 Different PCs
* 1 FTP Server
* 1 Printer
* 1 Laptop
* 1 Switch as shown in figure above

The Third Network is made of IPv4 Addressing having the IP addresses in the

range of 192.168.30.2 – 192.168.30.4

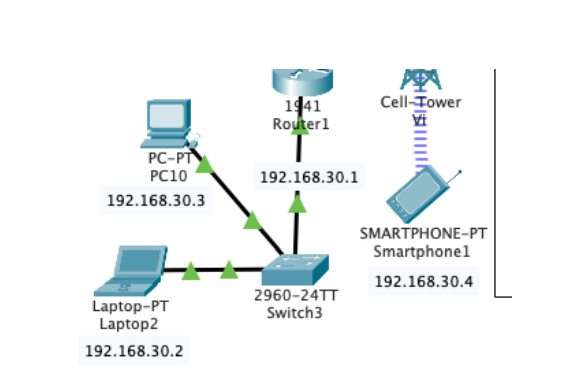
Default Gateway for this Network is 192.168.30.1

Devices in this network –

- 1 PC

- 1 Laptop

- 1 Switch as shown in Fig below



3 (1941) Routers are used to connect all these 3 LANs together. Dynamic routing

is used to route traffic all across 3 networks.

Networks Connected with Router 1 (router0)

- 192.168.1.0

- 100.0.0.0

- 10.0.0.0

Networks Connected with Router 2 (router1)

- 10.0.0.0

- 20.0.0.0

- 192.168.30.0

Networks Connected with Router 3 (router2)

- 20.0.0.0

- 192.168.10.0

**4.4 Network Devices and Connection Stage**

Network Devices used in this Network

-1941 Router with 2 Gigabit Ethernets and 4 Serial Connection Ports

-HTTP Server

-FTP Server

-2960 Switch with 24 Fast Ethernets and 2 Gigabit Ethernet Ports

-PT Printer

-Personal Computer

-SYSLOG Server

-Laptop

-Mobile Tower with 3G/4G Service

-4G Compatible Smart Phone

Cabling used in this Network

* Copper Straight-through Cable
* Serial DCE Cable

Straight-Through Cable is used between

* PC to Switch
* Switch to Router
* Laptop to Switch
* Server to Switch

Serial Cable is used between

* Router to Router

2 Different Servers are put across the networks to perform some more functions

like Web Access, File transfer.

These Servers are HTTP and FTP.

HTTP is used for Web traffic like if we want to access any website HTTP protocol

or server comes into play.

FTP is used for file transfer like if we want to store some files on the server or

download some files from a server FTP protocol or server comes into play.

In proper connection IP addresses are very important to communicate across the

network. IP used in this network is Class A and Class C.

From Class A IPs used are--

100.50.0.1 @ router interface gigabit ethernet 0/1

100.50.0.2 @ HTTP Server Port fast ethernet 0

10.10.10.1 @ router interface Serial 0/0/0

10.10.10.2 @ router interface Serial 0/0/0

20.20.20.1 @ router interface Serial 0/0/1

20.20.20.2 @ router interface Serial 0/0/0

As large number of IPs are from Class C because it has the most number of hosts

from other classes such as A and B.

**CHAPTER 5**

**IMPLEMENTATION**

**5.1 Configuring the Network**

Placing devices and connecting it with cables is not enough! We have to do far

more than this. After connecting with cables first task is to assign them IP

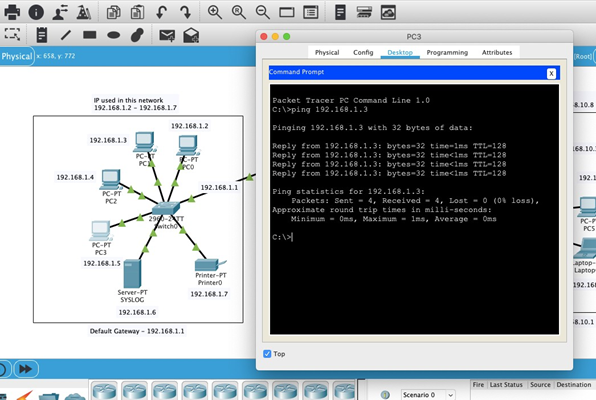
addresses. As discussed above Class A and C IPv4 are used. After assigning IP to

each interface in the network. Next step is to check connectivity from one PC to

another. But here connectivity only works inside the network, our network is still

not capable of communicating with outside PCs as you can see in Figures above

and below.



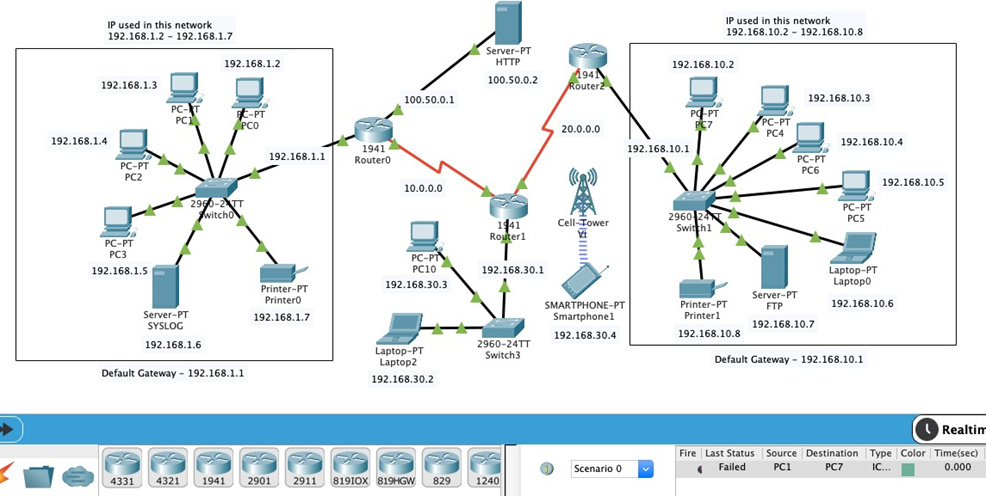
Ping is a command used to test connectivity between two hosts or devices.

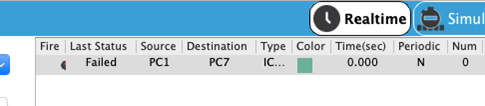
Ping test from PC3 to PC1 is successful.

Let’s take another test of sending a ICMP packet from PC 3 to PC7 (other

network) and check whether it successfully reached or not.

In below figure it failed.





This failure occurs because we have not told router, where it should send the

packet it comes to it.

The concept of Routing comes here. There are two types of routing.

-Static Routing

-Dynamic Routing

For our project we have used dynamic routing concept because it is more easy to

use.

Another task for configuring this network was configuration of Servers i.e. Syslog,

HTTP, FTP. For Syslog server I have turned down all the service except logging

service called ‘SYSLOG’ so that it can focus only to logging information come from

IDS.

For configuring HTTP same concept like syslog. Here I made a custom webpage

which can be accessed from any host in the any network by IP address called

100.50.0.2

For configuring FTP same concept. Here I made a user called ‘harsh’ and

password ‘123’.

So now our entire network is configured properly.

**CHAPTER 6**

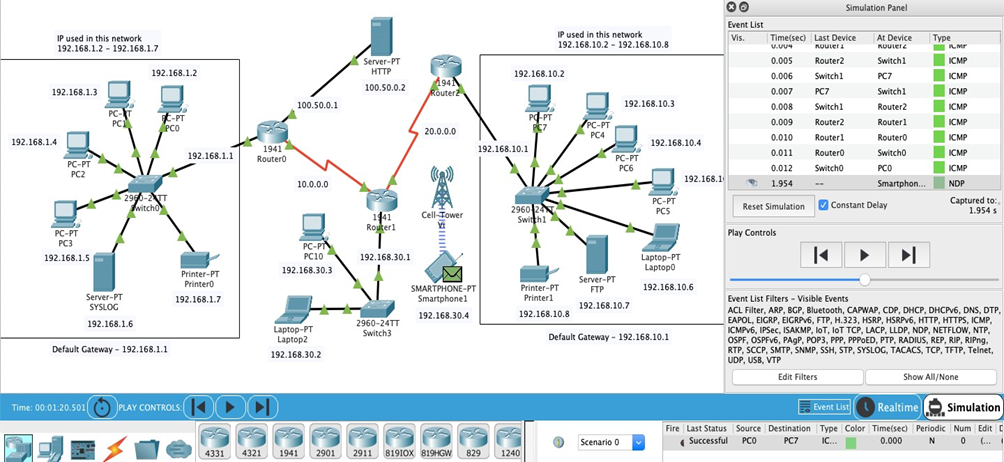
**EXPERIMENTAL RESULTS, TESTING AND ANALYSIS**

**6.1 RESULT**

Before moving towards the implementation of IDS. It is important to test the

connectivity of the entire network.

So here are the testing results.



In this a Packet is sent to PC7 from PC1 and acknowledgement of that packet is

received back to the PC1 and the whole process is successfully completed.

**6.1.1 Implementation of NIDS using CLI**

Now the main task has reached. We have to apply IDS into this network for

securing it.

Our IDS will be implemented on Router0 on interface (gigabit ethernet 0/0). Our

IDS will scan all the ICMP traffic which is coming into the Network 1 from this

interface. For that we have used IPS Signature 2004

2004 ICMP Echo Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP

header set to 1 (ICMP) and the “type” field in the ICMP header set to 8 (Echo

Request).

Although we have a list of different Signatures which made for different types of

data traffic. Some signatures are –

-2001 ICMP Host Unreachable (Info, Atomic)

-1101 Unknown IP Protocol (Attack, Atomic)

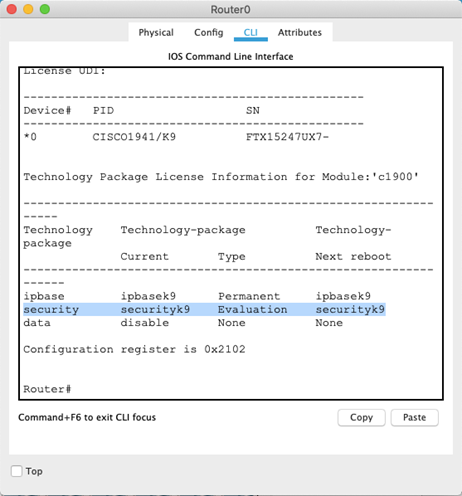
-2007 ICMP Timestamp Request (Info, Atomic)

-3040 TCP - no bits set in flags (Attack, Atomic)

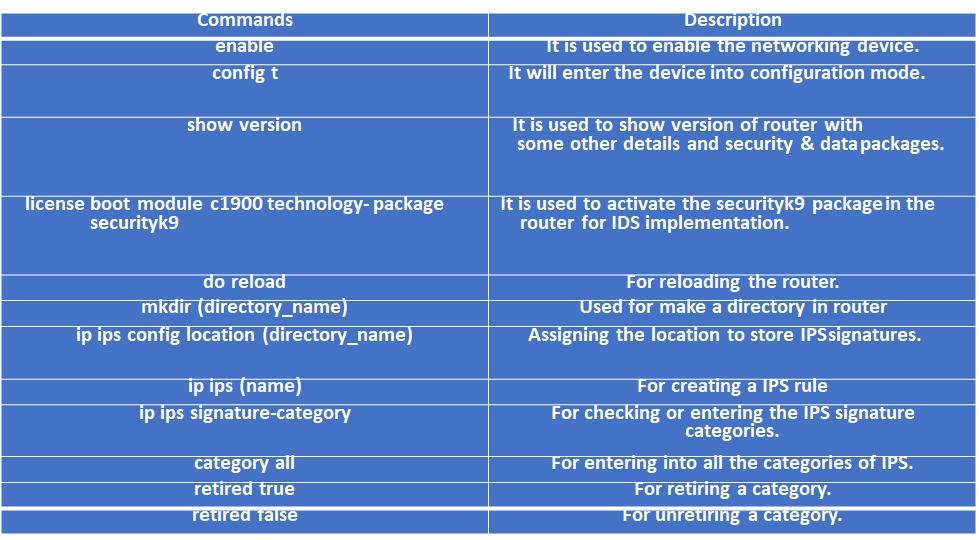
-3100 Smail Attack (Attack, Compound)

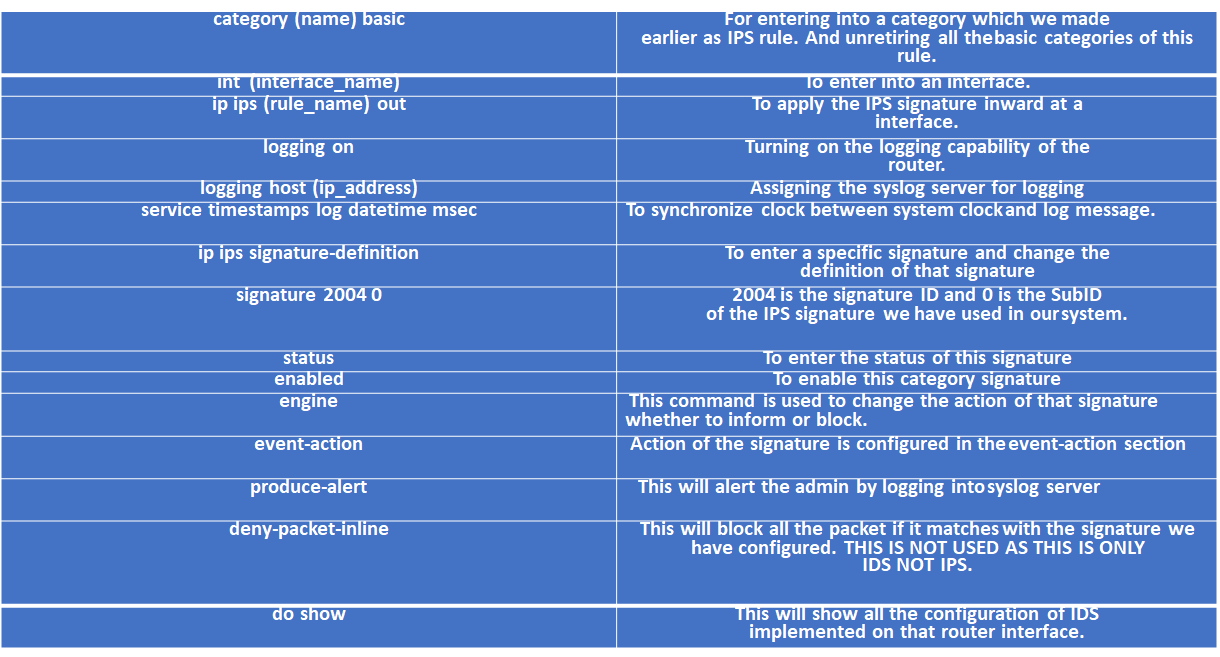
For implementing IDS on router0 we have to firstly activate security package of

that router. We have activated ‘securityk9’ package



**6.1.2 Commands for Implementing IDS**





**6.1.3 IDS Enabled & Protected Network**

Network-based intrusion detection systems (NIDS) are devices intelligently

distributed within networks that passively inspect traffic traversing devices on

which they sit. NIDS can be hardware or software-based systems and, depending

on the manufacturer of the system, can attach to various network mediums such

as Ethernet, FDDI, and others. Oftentimes, NIDS have two network interfaces.

One is used for listening to network conversations in promiscuous mode and the

other is used for control and reporting. With the advent of switching, which

isolates unicast conversations to ingress and egress switch ports, network

infrastructure vendors have devised port-mirroring techniques to replicate all

network traffic to the NIDS. There are other means of supplying traffic to the IDS

such as network taps. Cisco uses Switched Port Analyzer (SPAN) functionality to

facilitate this capability on their network devices and, in some network

equipment, includes NIDS components directly within the switch. We’ll discuss

Cisco’s IDS products in the next chapter. While there are many NIDS vendors, all

systems tend to function in one of two ways; NIDS are either signature-based or

anomaly-based systems. Both are mechanisms that separate benign traffic from

its malicious brethren. Potential issues with NIDS include high-speed network

data overload, tuning difficulties, encryption, and signature development lag

time. We’ll cover how IDS work and the difficulties involved with them later in

this section.

**6.2 RESULT ANALYSIS**

- CAN recognize and report alterations to data.

- CAN detect when your system is under attack.

- CAN detect errors in your system configuration.

- CAN NOT analyse all the traffic on a busy network.

- CAN NOT prevent system from that attack which it detects.

- CAN NOT deal with some of the modern network hardware and features.

**6.3 CONCLUSION AND FUTURE WORK**

**CONCLUSION**

In this project of implementing an Intrusion detection System using Cisco Packet

Tracer, we created a network using different components likes pc’s, routers,

switches, servers, connecting wires, hubs, etc.

After Connecting the network, we accessed the networks and allotted different

protocols to different components like FTP, HTTP etc. to servers, IP’s to all the

devices in the network, And Shared ICMP packets through the network to ensure

its flawless working. Then we fed and flooded the network using Pings and

monitored the ping, type of message and connection status. This was done to

test the NIDS and implemented the IDS.

**FUTURE WORK**

In future reference we need to work on the Honeypot System to implement and

work the Intrusion Prevention System along with the Intrusion Detection System.

**CHAPTER 7**

**REFERENCES**

1) [What is an Intrusion Detection System (IDS)? - Check Point Software](https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/#)

2) [taxonomy.pdf (bstu.by)](https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf)

3) [Computer and Information Security Handbook - John R. Vacca - Google Books](https://books.google.co.in/books?id=TnE85sckwMAC&q=IDS+network+host+sig&redir_esc=y#v=onepage&q=IDS%20network%20host%20sig&f=false)

4) [Computer Security: Protecting Digital Resources - Robert Newman - Google Books](https://books.google.co.in/books?id=_R5ndK-i3vkC&q=%22intrusion+prevention+system%22+AND+(reaction+OR+reacti&redir_esc=y#v=snippet&q=%22intrusion%20prevention%20system%22%20AND%20(reaction%20OR%20reacti&f=false)

5) [Network and System Security - Google Books](https://books.google.co.in/books?id=ebbwmOFWvR8C&q=%22intrusion+prevent&redir_esc=y#v=snippet&q=%22intrusion%20prevent&f=false)