**A picture containing logo

Description automatically generatedDAYANANDA SAGAR COLLEGE OF ENGINEERING**

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with ‘A’ grade, Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.

**Minor Project Report**

**on**

**“Syslog Server”**

Submitted By

Madhulika Singh (1DS20CS113)

Madugundu Lingesh Rohith (1DS20CS114)

Mahantesh Masali (1DS20CS115)

**Fifth Semester B.E (CSE)**

**in**

**Computer Networks**

**19CS5DLCNL**

Under the guidance of

**Dr. Nagaraja J.**

**Associate Professor**

**Dept. of CSE**

**DSCE, Bangalore**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Contents** | **Page** |
| 1 | Introduction | 1-2 |
| 2 | Design and Configuration | 3-5 |
| 3 | Topology | 6 |
| 4 | Real time and Simulation Mode Results | 7-8 |
| 5 | Conclusion and Future Enhancement | 9 |
|  |  |  |

**INTRODUCTION**

Syslog stands for **System Logging Protocol**and is a standard protocol used to **send system log or event messages to a specific server**, called a syslog server.  It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.

Monitoring numerous logs over an equally numerous routers, switches, and systems would be time consuming and impractical. Syslog helps solve this issue by forwarding those events to a centralized server.

Traditionally, Syslog uses the UDP protocol on port 514 but can be configured to use any port. In addition, some devices will use TCP 1468 to send syslog data to get confirmed message delivery.

The syslog servers have the following components: Syslog listener, database, Management, and filtering software.

* **Syslog Listener**: A Syslog server needs to receive messages sent over the network. A listener process gathers syslog data sent over UDP port 514 or TCP 1468.
* **Database**: A proper Syslog servers will use a database to store syslog data for quick retrieval.
* **Management and Filtering Software**: It is better that we use a syslog server that both automates part of the work and makes it easy to filter and view important log messages.

Syslog messages have several severity levels**.** The below provided image shows the 8 severity levels in Syslog messages

Table

Description automatically generated

**DESIGN AND CONFIGURATION**

Design:

The project has a total of 11 sub networks with IP address of 10.0.0.0 and subnet mask 255.240.0.0. It has one DHCP server, a DNS server, a Web server, and a SYSLOG server. It contains 6 routers, 5 switches and one data centre. The designing of the subnets is shown below

**For a network of 11 subnets with IP address of 10.0.0.0(class A):**

The formula 2^n where n is the number of bits borrowed from the binary representation of the subnet mask from second octet of subnet mask.

2^4 = 16>11 so we need to convert 4 bits in second octet of subnet mask.

Representation of subnet mask in binary form:

Old Subnet Mask: 255.00000000.00000000.00000000

(255.0.0.0)

Convert to 1 the 4 bits from MSB in the second octet of the subnet mask:

(For 16 networks)

New Subnet Mask: 255.11110000.00000000.00000000

(255.240.0.0)

Block size: 2^4=16

Number of hosts per subnet = 2^20 - 2 = 1048574

|  |  |  |  |
| --- | --- | --- | --- |
| NUMBER | NETWORK | RANGE | BROADCAST |
| 1 | 10.0.0.0 | 10.0.0.1 to 10.15.255.254 | 10.15.255.255 |
| 2 | 10.16.0.0 | 10.16.0.1 to 10.31.255.254 | 10.31.255.255 |
| 3 | 10.32.0.0 | 10.32.0.1 to 10.47.255.254 | 10.47.255.255 |
| 4 | 10.48.0.0 | 10.48.0.1 to 10.63.255.254 | 10.63.255.255 |
| 5 | 10.64.0.0 | 10.64.0.1 to 10.79.255.254 | 10.79.255.255 |
| 6 | 10.80.0.0 | 10.80.0.1 to 10.95.255.254 | 10.95.255.255 |
| 7 | 10.96.0.0 | 10.96.0.1 to 10.111.255.254 | 10.111.255.255 |
| 8 | 10.112.0.0 | 10.112.0.1 to 10.127.255.254 | 10.127.255.255 |
| 9 | 10.128.0.0 | 10.128.0.1 to 10.143.255.254 | 10.143.255.255 |
| 10 | 10.144.0.0 | 10.144.0.1 to 10.144.255.254 | 10.159.255.255 |
| 11 | 10.160.0.0 | 10.160.0.1 to 10.175.255.254 | 10.175.255.255 |
| 12 | 10.176.0.0 | 10.176.0.1 to 10.191.255.254 | 10.191.255.255 |
| 13 | 10.192.0.0 | 10.192.0.1 to 10.207.255.254 | 10.207.255.255 |
| 14 | 10.208.0.0 | 10.208.0.1 to 10.223.255.254 | 10.223.255.255 |
| 15 | 10.224.0.0 | 10.224.0.1 to 10.239.255.254 | 10.239.255.255 |
| 16 | 10.240.0.0 | 10.240.0.1 to 10.254.255.254 | 10.255.255.255 |

Configuration:

First the RIP configuration is done in all the routers. Then Static IPs are given to the servers and IP pools for each subnet is mentioned in the DHCP server. In DNS we record the domain-name of the server and its IP address. Web server provides the website.

For DHCP configuration:

Router> enable

Router# config t

Router(config)# int g0/0 (g0/0 is the router interface to which networks are connected)

Router(config-if) # Ip helper-address 10.0.0.1 (here 10.0.0.1 is the static address provided to the DHCP server)

Router(config-if) # exit

Router(config)# exit

For SYSLOG server configuration:

Router> enable

Router# config t

Router(config)# logging on

Router(config)# logging 10.0.0.11 (10.0.0.11 is the address of syslog server)

Router(config)# logging trap debugging

Router(config)# exit

**TOPOLOGY**

**Graphical user interface, diagram

Description automatically generated**

**Real time and Simulation Mode Results:**

**Sending message from PC0 to PC5 in real time mode**

**Chart

Description automatically generated**

**Sending message from PC0 to PC5 in simulation mode**

**Graphical user interface, table

Description automatically generated**

**Diagram

Description automatically generated**

**Syslog server (when the interface g0/1 of router 5 is turned off and then back on)**

**Table

Description automatically generated**

**CONCLUSION AND FUTURE ENHANCEMENT**

Understanding what is going on in your network environment is crucial to health of your system. Using a syslog server enables you to send event messages and multiple logs from your network devices to a centralized unit.

Using a sys log server has many advantages like reduced downtime, easy to troubleshoot errors, alerting etc. and thus a good option for monitoring the network health.

There are several potential enhancements that could be made like:

1. Adding support for filtering and categorizing syslog messages: This could involve implementing features like keyword searches, regular expression matching, and custom tags to help users find and group relevant messages more easily.
2. Adding support for remote syslog servers: This could involve implementing features like secure communication protocols (e.g. SSL/TLS) and the ability to forward syslog messages to other servers over a network.
3. Integrating with other tools and services: It might be useful to integrate the syslog server with other tools or services, such as a ticketing system, a monitoring platform, Sor a chat application.
4. Improving scalability and performance: As the syslog server grows in popularity and usage, it may be necessary to optimize its performance and scalability to handle large volumes of syslog data. This could involve implementing features like message batching and parallel processing.