VEMANA INSTITUTE OF TECHNOLOGY

Koramangala, Bengaluru-34.

Department of Computer Science and Engineering

Project Phase-I Review 0

NETWORK MONITOR

By

RAJASHREE – 1VI17CS114

PAVITHRA K – 1VI17CS071

BIRD VIEW

- Objectives
- Existing System
- Proposed System

OBJECTIVES

- Network Monitor is a scripted tool that alerts the User about various status changes and updates such as Reachability, Firmware version changes, Issues, Resource usage, Device Information and so on in network nodes such as Servers, Endpoint PCs, Routers, Switches, Virtual Machines, Datastores and so on.
- Alerts can be sent through various modes such as GUI, Email, SMS and so on.
- Various Protocols are used for obtaining these information such as ICMP, ARP, LLDP, SNMP and so on.
- ICMP is used to obtain the reachability status, latency, availability and network level of the device.
- ARP is used to obtain the Mac address of the device by sending a forced broadcast.
- LLDP is used to obtain the device type, transmit stats and so on.
- SNMP is used to obtain software level changes in the device such as firmware upgrades, resource utilization and so on.

EXISTING SYSTEM

- Networks serve as the backbone for any enterprise. Any network outage during working hours is huge loss for the organizations.
- As a result, they employ a separate team to look after their labs by constantly logging into several system interfaces and checking their statuses.
- A typical organization that consists of say 100 employees, the network includes at least 3 routers, 5-6 switches, 100-150 PCs, 3-5 servers, a cloud environment consisting of its 3-5 instances and 1-2 data stores, 20-30 VMs for testing their product.
- It is a tedious task to login to each of these nodes, check if they are reachable and check their health status constantly.
- As the enterprise grows, the numbers increases exponentially.

PROPOSED SYSTEM

- Network Monitor is a web application that reports various status changes and updates of various network nodes in an organization
- The system basically comprises of 3 parts
  - Front End: Main functionalities include the following:
    - Logging into the system
    - Adding a device
    - Editing a device
    - Deleting a device
    - Displaying the ‘Devices’ table
  - Database: It comprises of two tables:
    - UserLogin is the administer the secure login activity to network monitor.
    - Device table consists of the device name, locally generated device id, IP Address and System Parameters such as Reachability, Availability, Latency, Mac Address and so on.
  - Back End: A Python script that runs every 10 seconds to obtain information of all network nodes using different protocols and updates the same in the Database.

THANK YOU