Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.elsevier.com/locate/jii

# Design and implementation of an automated network monitoring and reporting back system

Rafiullah Khan*,[a], Sarmad Ullah Khan[b]

[a] Queen's University Belfast, Belfast, United Kingdom
[b] Politecnico Di Torino, Turin 10129, Italy

ARTICLE INFO

*Keywords:*
Network monitoring
Network management
Universal Plug & Play
Ticketing system
Reporting back system
Nagios

ABSTRACT

The task of network monitoring becomes tedious with increase in the network size, heterogeneity and complexity. The available network monitoring and management solutions are not only expensive but also difficult to use, configure and maintain. Manually pin pointing a faulty device in the large complex network is very tricky and time consuming for network administrators. Thus, an automated system is needed that immediately reports to network administrator about fault type and location as soon as it arises. This paper presents design and implementation of an intelligent network monitoring and reporting back system for large size organizations/industries. It is based on programming open-source tools (such as Nagios and RT) and intelligently integrating them to monitor network devices such as switches and routers. To monitor end-user devices in the network, a software package has been developed using Universal Plug & Play (UPnP) technology. The developed monitoring system immediately notifies network administrator as soon as a network problem arises. The notification message clearly pin points the fault location in network topology, its type and impact on rest of the network. If the network problem is not resolved within the pre-specified deadline, a second notification is sent out to the next responsible person. Thus, all people in the priority list are notified one by one with pre-specified deadlines until the problem is resolved.

## 1. Introduction

Industry 4.0 revolutionizes industries by making them more connected than ever before. This disruptive innovation connects plethora of heterogeneous devices which are communicating among each other to perform complex tasks [1]. Due to relying mostly on IP based communication, ensuring availability of devices and services is utmost necessary. Thus, an automatic, flexible and scalable network monitoring and management system is essential for industries. The monitoring system constantly checks the whole network topology for any failing component, device or service interruption and immediately notifies the administrator [2]. The notification messages carry information about faulty services and devices which may have been caused due to misconfiguration, overloaded or crashed servers, cyber attack, network cable disconnection or device power disconnection [3,4]. Due to heterogeneity and complexity in large size industrial networks, manual monitoring the state of each device is very tedious and time consuming task. Further, troubleshooting or pin pointing the fault location and its impact on rest of the network is very challenging [5].

Many network monitoring systems can either monitor core network devices (such as switches and routers) or end-user devices (such as PCs, printers, scanners, etc). Further existing solutions have limited flexibility, scalability and provide insufficient information about the fault location and its impact on rest of the network. This paper addresses network monitoring and management challenges in a more flexible way with the design of a new system. The proposed system is based on programming and integrating open-source tools such as Nagios and Request Tracker (RT) and developing a software package using University Plug & Play (UPnP) technology. The proposed system is not only able to monitor intermediate core network devices but also end-user devices located in private sub-networks. Thus, the network monitoring and management task is divided into two parts: (i) monitoring devices directly accessible from ISP or network control center of the organization, and (ii) monitoring devices located in private LANs.

The proposed network monitoring and management system is applicable to any large size organization or industry. However, this paper focuses on university network as a use case example. Fig. 1 depicts the scenario of a university that has several campuses. Each campus has different departments and each department has several private networks (e.g., classes, laboratories, offices, etc). Thus, a large-size

[*] Corresponding author.
*E-mail addresses:* rafiullah.khan@qub.ac.uk (R. Khan), sarmad.khan@polito.it (S.U. Khan).

https://doi.org/10.1016/j.jii.2017.11.001
Received 8 September 2017; Received in revised form 16 November 2017; Accepted 17 November 2017

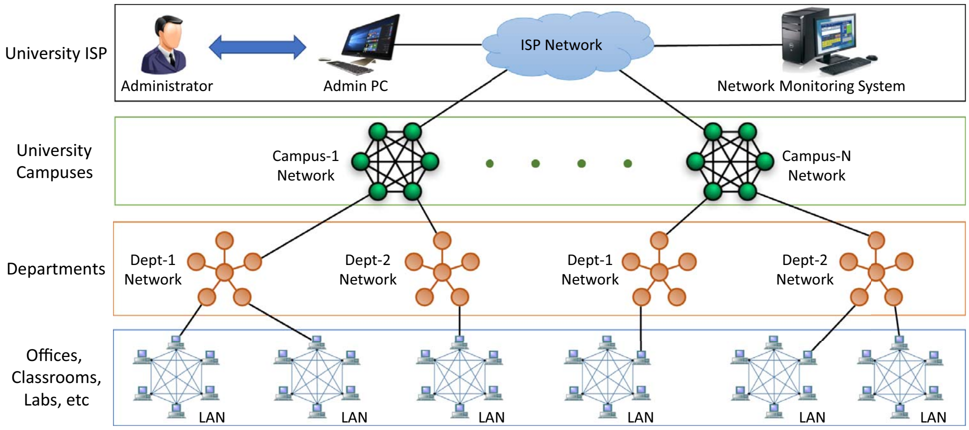

**Fig. 1.** Basic network topology of a large size university.

university consists of thousands of network devices. Due to limited IPv4 addressing space, universities are normally allocated certain number of public routable IP addresses. The university ISP or network control center intelligently utilizes these IP addresses for certain devices e.g., campuses and departments. However, network devices in laboratories, classrooms and offices normally have private IP addresses. In some cases, devices in the private subnets are not directly accessible from the university ISP. Thus, it is necessary that network monitoring and management system should be able to monitor all network devices regardless of their direct accessibility from the university ISP. To this aim, proposed system uses Nagios and RT in the university ISP for monitoring all devices in network topology which are directly accessible. A UPnP based monitoring system is developed for monitoring devices in laboratories, classrooms and offices which are not directly accessible from ISP.

In proposed system, the functionalities of network monitoring are performed by Nagios [6]. Nagios allows easy extension of functionalities and integration of custom modules or plugins. A complete network topology (i.e., consisting of devices directly accessible from university ISP) is created in Nagios and different monitoring services based on ICMP or SNMP are applied on them. Nagios continuously monitors the devices and services running on them and declares them critical or down after making several pre-defined number of attempts. When a network device or service is down, Nagios generates a notification which creates a ticket in RT ticketing system with problematic device information and its impact on rest of the network. RT is responsible for performing the task of fault/problem progress tracking and management [7]. Note that RT is heavily used worldwide by different organizations for tracking and effectively resolving issues/complaints from customers. The scope of RT is quite broad and provides multi-user interface for secure authentication and collaborative management of issues/complaints. The developed UPnP modules are used for monitoring devices in the private LANs. UPnP technology offers auto-discovery, zero-configuration and seamless networking features [8]. Further, UPnP is supported by plethora of heterogeneous devices and does not cause any interoperability and integration issues. The proposed network monitoring system immediately informs network administrator as soon as a network device goes down. If the administrator is busy or could not resolve issue within a set deadline, a new notification is sent out with a new deadline to the next responsible person in the priority list. Thus, all people in the priority list are informed one by one until the problem is resolved. The proposed system is intelligent enough to precisely pin point the problematic device and its impact on rest of the network. Further, a single notification is sent out if a parent device in network topology stops functioning instead of sending multiple notifications for all affected child devices.

The rest of the paper is organized as follows. Section 2 addresses background and related work. Section 3 presents the design of proposed network monitoring and management system. Section 4 provides implementation guidelines. Section 5 presents experimental evaluation of proposed system. Finally, Section 6 concludes the paper.

## 2. Background and related work

Several network monitoring and management tools have been developed over time. The Multi Router Traffic Grapher (MRTG) is one of the most commonly used tool for network monitoring that works on Windows and most Linux distributions [9]. It is written in Perl scripting language and uses Simple Network Management Protocol (SNMP). MRTG generates live visual graphs of all network devices in the HTML pages. These graphs provide information about the traffic load. Manually checking graphs of each network device in MRTG and identifying the problematic/faulty ones is very tedious, inefficient and time consuming task for the network administrator. Another most commonly used networking monitoring tool is Nagios [6]. Nagios is an open-source software tool and is specially designed for monitoring complete infrastructure of enterprise networks for availability of different network services [10]. If a network device is down or any of its network service is down, Nagios raises an alert to the technical staff. Nagios also provides statistics about devices and their services availability.

Several researchers have investigated remote monitoring and management of complex large size networks. Authors in [11] proposed an event monitoring and control system for enterprise networks. The system monitors traffic from network devices to determine their operational status and raises alert to network engineer when failure is detected. Authors in [12] addressed new services in Nagios for monitoring network bandwidth and new form of notifications through email and SMS. These new services increase Nagios scope for even better and improved network monitoring. Authors in [13] addressed how to securely deploy and maintain monitoring services based on Nagios for big enterprise networks. Authors in [2] presented a network monitoring system based on Nagios and designed a more user-friendly and interactive interface. They have extended monitoring functionalities and capabilities through plug-in modules without modifying the Nagios core. Some researchers have also proposed RFID based monitoring and management in industries [14,15]. Their focus is on tracking inventory and incoming/outgoing goods e.g., logistic industry. However, presented RFID approaches do not aim to check presence/availability of a network device or service.

Authors in [4] addressed remote monitoring of a LAN that mainly consists of server devices. The system not only monitors availability and operational status of server devices in remote LAN but also their environment. The monitoring system also uses sensor devices and raises SMS alert to administrator in case of a device failure or hazard (e.g., temperature, power fluctuation, humidity, fire, water, etc). Other similar works are addressed in [16–18]. Normally, organizations have