KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS

Fault-Tracking in Computer Networks Using GIS

CRP 514 Term project

Project Report

Proposed to Dr. Baqer Al-Ramadhan

Team Members
Saeed Al-Sowail 201003220
Rashad Balfaqih 201001240

01/01/2012

TABLE OF CONTENTS

ABSTRACT

With the increasing complexity in computer networks, there is more need to network management tools that simplify the task of the network administrators. Most of the available tools use text-based interfaces that complicate the process of tracking a problem location. In this project, we designed and implemented a network-monitoring tool that uses Geographic Information Systems (GIS) to facilitate the management efforts. Our tool utilizes ArcGIS to provide a graphical user interface that makes fault tracking easier for network administrators.

1. INTRODUCTION

Computer networks have grown significantly in the recent years. Companies with large number of branches around the globe might have networks that interconnect devices in numbers of tens of thousands. These companies might need to use thousands of networking devices to connect computers, servers, and other devices to the network. Another example of complex networks is the network of Internet Service Provider (ISP) which spans the entire country. Thousands of networking devices are used in such a network to provide the service to millions, or hundreds of millions, of customers across the country.

The two examples above indicate how computer networks have largely grown. These large networks need lots of work in order to monitor and manage them. Hardware failures can happen anywhere in these networks. Not only hardware failures, certain software services can also crash; or they may fail due to a mistake in the configuration entered by a network engineer. All, these faults and errors along with the changes in the topology of the network must be tracked by the network management team. But unfortunately, unlike the public switched network, which is will planned, much of the computer networks growth done in

unorganized way. This had led to efficiency, reliability, and maintenance issues and problems [1].

There are many software packages specialized in network monitoring available in the market. Each has its advantages and disadvantages. In this project, using Geographic Information Systems (GIS), we are designed and implemented a network monitoring tool that will help making tracking the network easier. Using GIS, we can monitor the network using colorful electronic maps. The use of electronic maps makes monitoring easier than using and tracking tables and reading log files.

2. Problem Statement

The management of a large network that consists of a large number of networking devices interconnecting in a complicated way is a tough task. Faults and errors in these networks cannot be avoided, but the point that has to be avoided is the long time of unavailability. Internet service providers do not wish their services to be unavailable to their customers, but if that happened somehow inadvertently, the service must be returned to customers as soon as possible. This requires the use of complex Network Management Systems (NMS). Although these NMSs can give some information about the geographical location of the fault and about the network problems in general, however, network engineers still facing some difficulties in tracking all the warnings, errors, and changes in the network. They usually consume time to identify the sources of such error messages, and it becomes more difficult when more than one error come out from the same device (this happens if it is a core device, which will report any related device errors).

A method that can be used to simplify the management task is the use geographic information systems GIS. A GIS-based network management tool can combine all the monitoring efforts into a single electronic map. Network

management team to track all components from one place can use the GIS electronic map.

3. OBJECTIVE

In our project, we are trying to design and implement a GIS based network-monitoring tool. A tool that simplifies the network administrator tasks in terms of quick fault-position locating and service recovery. In addition, we going to integrate the functionality of Network Management Systems (NMSs) to improve the decision-making process, the process that will help in enhancing the overall network performance.

4. LITERATURE REVIEW

The authors of [1] propose a network management system that is built on the top of a GIS system in order to automate the update process and avoid the static behavior of the previous systems. Their proposed architecture is described in the following figure (1):

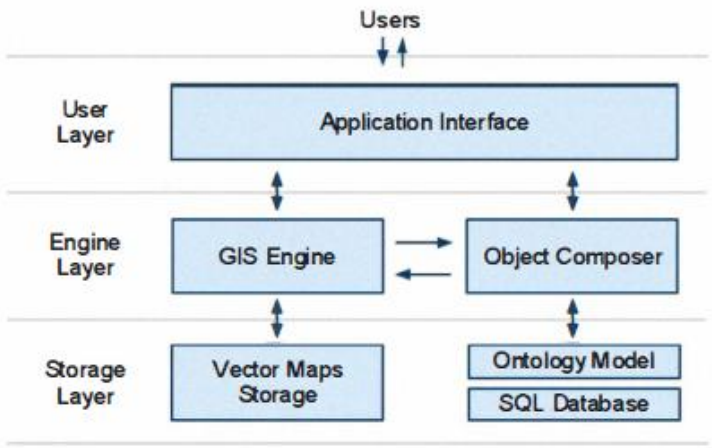

Figure 1

Dumitrescu et al. [2] developed a network management system using GIS and network ontology. Their main objective was to create a system the can monitor and control the status of data communication networks in real time. They

mentioned that all major players in Romanian Internet Service Providers and GSM segments use static GIS systems. These systems add new layers that describe the network infrastructure on the top of original city plans. The main problem with these systems is that they are static. Therefore, the network technicians have to update the data manually. This mechanism is slow and error-prone due to the fact that the user can enter wrong data by mistake.

Users interact with the application interface. The GIS engine displays the vector map which is stored on the local physical disk. The object composer interacts directly with the SQL database and assembles all the properties of the objects (devices). The application interface has the capability to navigate the map and to interact with objects. The application is located on client computers and connects to database server for object and map synchronization. The synchronization is done only at the start of the session. The system uses network pings to survey the network, and connect to devices using SNMP, Telnet, and SSH. This way, the data for active network devices with be updated periodically to the database server, and can displayed by the user when he starts a new session.

Niu et al [1] came up with new NMS model based on GIS, that is able to identify the geoposition of faulty devices. They used object-oriented network utilities management methods and combined traditional NMS methods with GIS. Some NMS methods use SNMP agents, so GIS objects are generated and defined. Those objects were built on e-maps to represent SNMP agents. Agents can response to NMS requests of data.

Due to large number of network devices that are spread over large geographical are, Niu et al used geo-positioning technique to facilitate boring tasks of ordinary NMS. They designed and implemented a fault alarm mechanism that utilized SNMP. This mechanism is depending on fault-message process algorithm. The algorithm works as following: First, check for alarm messages from

equipment. Second, lookup the database to extract spatial information. Third, locate the equipment on the map. Finally, set an alarm logo and store the alarm information to the database.

5. CASE STUDIES

A number of companies have used GIS to monitor their networks. These companies used an integrated management system that is built on the top of GIS. From these systems, a system called "Telcordia Network Engineer [3][4]" is widely used. It is a system created by both Esri and Telcordia to provide IT solutions to large companies [5]. It extends Esri's ArcGIS technology to support applications that are used to help planning, designing, and monitoring network infrastructures.

Here, we provide two case studies that used Telcordia. The first case study is about using the system in Qtel. The second case study explains the success of using the system in Bell Aliant. In both case studies, the use of GIS increased the productivity for both companies as explained below.

5.1. **Qtel**

Qatar Tel (Qtel) is the major telecommunication company in Qatar. In the first half of 2009, it was providing services to more than 2 million mobile customers. In 1998, it starts converting its 5000 paper maps to electronic maps and they started using ArcGIS. In addition to the great benefits that the Qtel gained by using GIS, the company needed more efficient way to enhance its work. After combining GIS to network management by using Telcordia, the company gained many other features. Now, the company's staff can plan, design, and monitor the construction of the network. The information about the network is accessible from any office. More information can be found in appendix (A).

5.2. **Bell Alian**

Bell Alian is a regional telecommunication provider. In 2009, it started a project to provide fiber-to-the-home to more than 33,000 houses in Atlantic Canada. In their plans, they are going to provide more than 660,000 premises by the end of 2012. When they started their work, everything was done manually. They do not have any previous experience with any GIS software. They had paper maps for the coverage areas. It takes long time if there is a need to validate the field data. After using ArcGIS with the network management system, Telcordia, the company could automate most of its work. Now, it takes short time to execute tasks that were done in days. More information can be found in appendix (B).

6. DATA

For our project, we need the following data:

1. IP addresses of the network devices.
2. The location of the devices.
3. The type of the devices.
4. The SNMP community string (a password used to access a network device for management purposes).

The data mentioned above is considered very sensitive. If a hacker put his hand on this data about a network of a company, he will use it as a map to hack this network. For this reason, network administrators never reveal this data to anyone outside the IT team.

The network department of university ITC gave us the IP addresses, the location, and the type of the devices. But, they could not give us the SNMP community string for the security issues discussed above.

To run and test the system, the given data was enough. However, to test the system to collect statistical information about the network, the SNMP community string is necessary. The statistical information is important to generate queries that help the network administrator in decision-making. The system can be used directly when this data is given.

7. Methodology & System Architecture

In this project, we are pursuing the point of how to integrate a GIS and NMS and utilize each system capabilities to achieve our projective objective. To do so, we used *ArcGIS* (a well-known GIS) and we built our specific NMS that monitors certain performance parameters. Hence, we designed our system to involve two main parts: *ArcGIS* and monitoring application, figure (2).

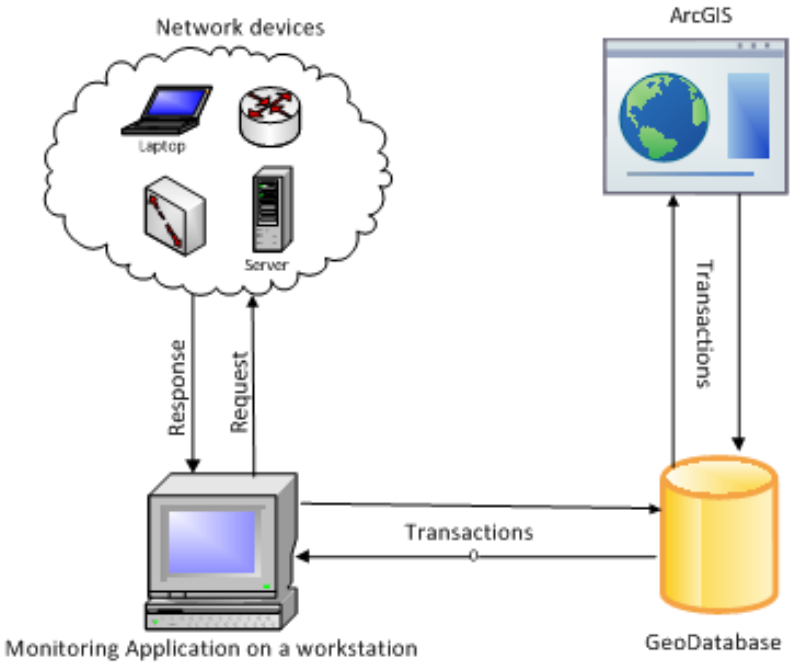

Figure 2

7.1. In ArcGIS, we used two of its components:

7.1.1. *ArcCatalog*: we utilized this tool in adding the geodatabase and the map. In geodatabase, we added an extra table named Network Devices to accomplish our objective. This table consists of the following fields:

Field	Description
OBJECTID	Object identifier (set by default)
SHAPE	Identify the shape of the feature (set by default)
Device_Type	The type of the network device
State	The current status of a device (OK, Problem)
Location	Where it is located
CntProblem	Counter for the problems encounter on a device
CntPacket	Number of data packets pass through a device
IP	The IP address of a device

Table 1

In addition, we used it to set some data fields of the attribute table to some conveniences, such as the domain of Device_Type field (R= Router, S= Switch), and State field (0= OK, 1= problem).

7.1.2. ArcMap: we created a new layer, Network Devices. On this layer, that contains information about the actual locations of the network devices, we drew point features to represent each network device. We defined two categories for the feature symbology, figure (3):

- OK: with a green color indicates that a device (Router/Switch) is available.
- Problem: a feature becomes in red color indicates that a device (Router/Switch) has encountered a problem.

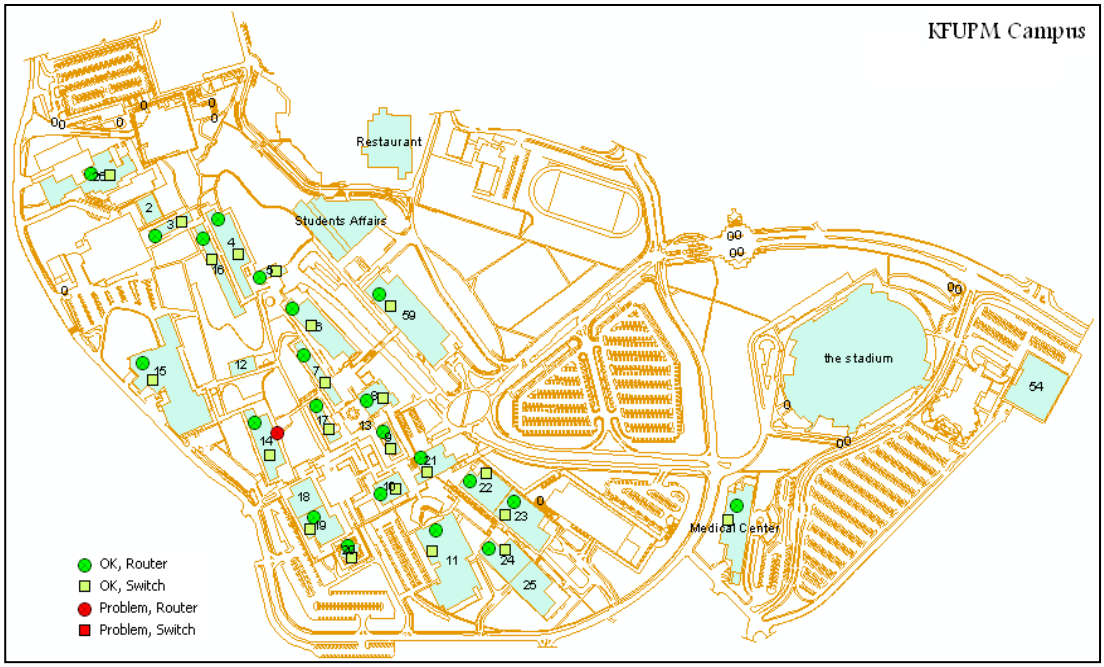

Figure 3

7.2. The monitoring application:

We developed this application to request and collect specific performance information from network devices. We designed it be run in the background of a manager workstation (i.e. has no user interaction). The application uses two network protocols to attain its functionality. Those protocols are Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP). ICMP is used to generate ping commands that are used in checking device availability, while SNMP is used to gather the performance statistics associated with each device. We programmed this application with C# programming language.

7.3. System Functionality

In this section, we are going to explain how the different components of our tool are interacting with each other to obtain the project objective. The functionality is divided into two sections, first devices availability, and second performance statistics.

7.3.1. Devices availability:

Availability means that a device can be reached and it is working properly. The monitoring application is responsible of checking for devices' status, it checks them on a regular predefined-basis (we used an interval of 30 seconds as a checking round robin). On the other hand, ArcMap refreshes its interface every 10 seconds to keep synchronized with geodatabase. Here we have two scenarios: normal situation and abnormal situation.

7.3.1.1. Normal situation:

The monitoring application requests the status of a certain device. The device responses with a message indicating availability. Consequently, the application updates the status field of that device in the geodatabase (in case that the previous status of that device is OK, the application do nothing). After that, when ArcMap refreshes its interface, the symbol color of that device becomes green.

7.3.1.2. Abnormal situation:

If the monitoring application checks the status of a device that gives no response, then it waits for a certain period (we used 500 milliseconds as timeout interval), after that, the application updates the status of that device in the database to '0', indicating a problem, and ArcMap by turn changes the symbol color into red. Additionally, the application increments *CntProblem* field to be used later.

7.3.2. Performance statistics:

In this part, the monitoring application uses SNMP to collect performance information from network devices. The collected data from this section will help the network administrators in decision-making about possible improvement and enhancement to the network. We have two performance parameters as follows:

7.3.2.1. Frequent failures:

When the monitoring application detects a problem in a specific device (part 7.2.1.2), it increments *CntProblem* counter by one. Then, by using ArcMap, we are able to execute a query that shows on the map those devices that exceed the failure limit, figure (4). In our case, we set a threshold of four failures; this may vary from network to another depending on the performance quality required.

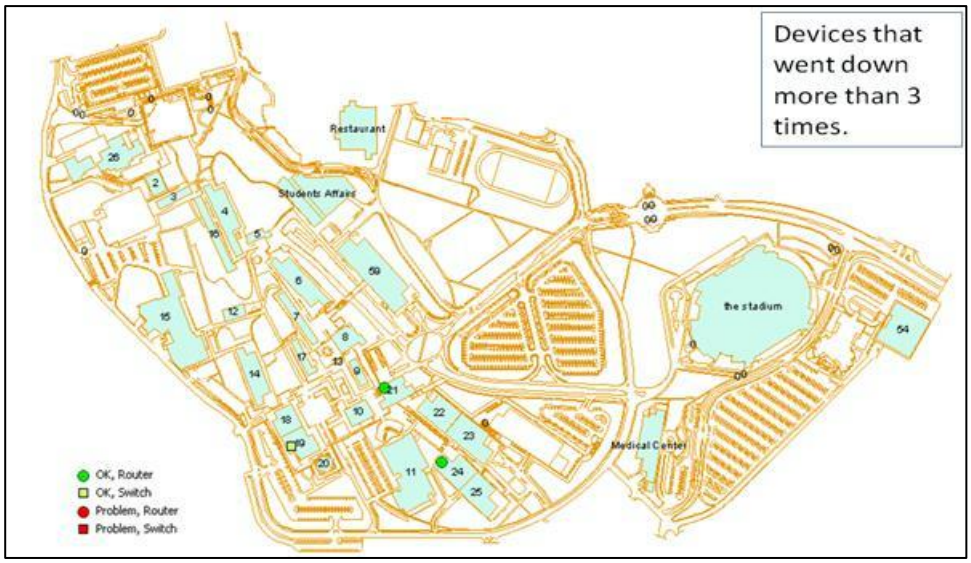

Figure 4

7.3.2.2. Overloaded devices:

Here, the monitoring application requests the values of *ifInOctets* parameter from the interfaces of a device. Those values are accumulative; we consider the summation of them as the overall load on that device. If the summation exceeds a certain limit, then ArcMap is able to show those devices on the map after executing a query about *CntPacket* field, figure (5). The specification of the limit depends on available bandwidth of those interfaces and - surely - the level of performance quality required. As a consequence, the network administrator may add a new networking device or reroute the network traffic on that device to another.

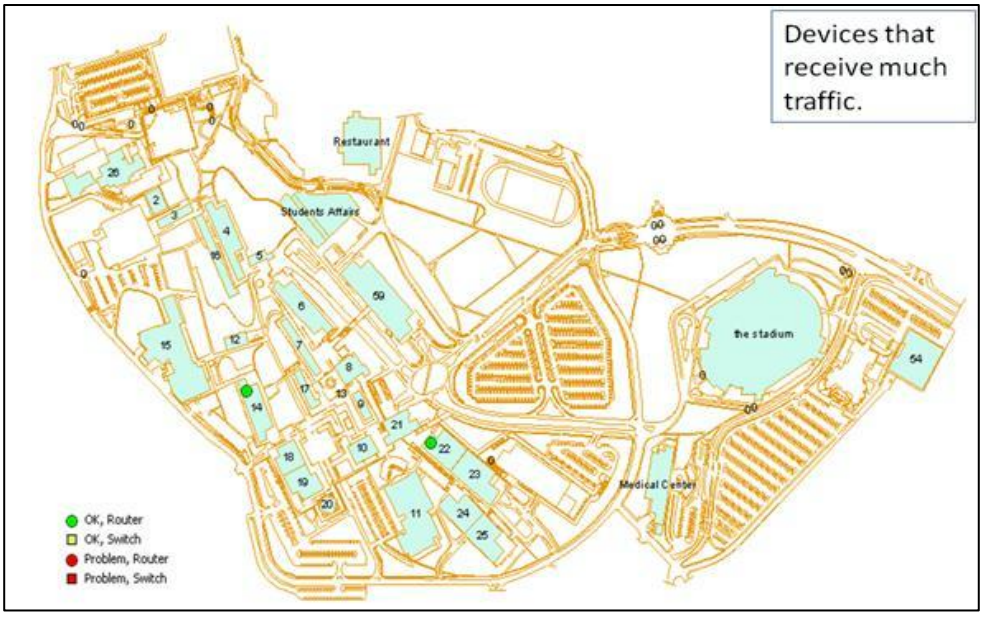

Figure 5

8. DISCUSSION

The text-based interfaces that are used in ordinary network management systems make the process of locating problems more difficult to administrators. The main reason for this is that the administrator has to map text data in tables, which is a tough process. For instance, an administrator will receive an alarm that the device with the IP address, say 10.10.23.240, is having problems. Now, the administrator does not know what is this device or where it is located. The administrator has to open another table that maps IP addresses to device types and locations. This is really tough and time consuming especially in large networks that may consist of thousands of devices.

We created our management tool with the objective of avoiding the tough process of the text-bases management tools that has been described above. We achieved our objective by using the help of GIS. The electronic map of the campus made it easier for the network administrators to track faults and changes in the network. The entire network could be displayed on a single screen in the network

operations center. Changing the color of a feature to red is enough for the administrator to directly indicate that a problem has happened. By one look to the map on the screen, the administrator is capable of determining what is the device that has the problem, what is its type, and where it is located. It is clear that using GIS greatly simplifies the tasks of the network administrator, and enhances the productivity of the network management too.

In addition to the simplicity that has been resulted from using GIS in network management, GIS was very helpful in providing performance statistics. In our project, we used ArcMap to query data about the frequent failures in the network and network devices that encounter heavy traffic volumes. This information is of high value to the network administrator. Knowing the location of frequent failures will make it easy for the administrator to track the root cause of the problem. For example, if the cause of the problem is bad hardware, the device can be replaces. If it is due to other reasons, the administrator can make the appropriate decisions. For the second feature, knowing devices with high traffic volumes, the administrator will avoid possible future problems like delay. The administrator can use this feature to find the appropriate time to upgrade a device or to balance the load between multiple devices, instead of aggregating much traffic in a single device. Many other performance statistics can be added when needed.

9. CONCLUSION

In this project, we proposed an integrated Fault-tracking system using GIS. The system includes ArcGIS and specific NMS. The responsiveness of system became faster, and it able to detect and specify the exact location of the problem. The proposed made the tasks of the network administrators easier. Also, it helped them in decision-making process about the network performance improvements and enhancements.

10. REFERENCES

[1] NIU, X., GAO, H., GU, Y., and YOU, L., 2010, A GIS based network management study and its application. *Computer Science and Education (ICCSE) 5th International Conference on*, 969–972.

[2] DUMITRESCU, S. D., SMEUREANU, A., DIOSTEANU, A., COTFAS, L. A., Adaptable Network Management System using GIS and network ontology, 2010. *Roedunet International Conference (RoEduNet),* 9, 310–315.

[3] http://www.telcordia.com.

[4] http://www.telcordia.com/collateral/brochures/net_engineer.pdf

[5] http://www.telcordia.com/success/esri.html.