Preliminary organization of virtual network based on program monitoring

RADI ROMANSKY
TECHNICAL UNIVERSITY OF SOFIA (BULGARIA)

Contents

1. Introduction
2. An Overview of Network Traffic and Monitoring Means
    2.1. Features of network traffic
    2.2. Network monitoring tools
3. Initial Phases of Monitoring Organization in LAN
    3.1. Specifying the reason for monitoring servers
    3.2. Preliminary preparation for monitoring
    3.3. Network activity analysis using Performance Monitor
    3.4. Network performance monitoring
    3.5. Registration of events
4. Conclusion
References

Abstract

Virtual Local Area Network (VLAN) is a logical organization of communication resources and objects for maintaining efficient information processes based on network traffic. It is known that in the contemporary global network, traffic can be generated from various physical sources, which requires preliminary analysis and adequate management with the provision of the necessary information security. In this aspect, the proposed paper presents an opportunity to analyse supported network traffic in a virtual network environment by using program monitoring. In the computer field, various products are offered for measurement of parameters of information processes, including network communications. In this sense, a preliminary review of the main features of network traffic was conducted and possible solutions for the organization of adequate program measurement of parameters of information processes were discussed.

Keywords

virtual network, program monitoring, information processes, analysis.

1. INTRODUCTION

Virtual Local Area Network (VLAN) is a mechanism for logical grouping of users, services, and network devices in local computer networks. A critical analysis of this type of networks is made and the advantages are systematized. One of them is that by creating multiple networks with a single IP address class and by restricting communication between VLANs, it is possible to allow or deny users access to a particular network. To ensure the effectiveness of the architectural design with a defined main goal, it is necessary to conduct a preliminary study of the information processes and analysis of the network traffic before the final implementation.

The purpose of the article is to present an opportunity to analyse network traffic in a virtual network environment using programmatic monitoring. For this purpose, some features of the network traffic were reviewed and possible solutions for measuring parameters of information processes were discussed.

2. An Overview of Network Traffic and Monitoring Means

2.1.Features of network traffic

Network traffic analysis is essential to ensure the required level of network security by allowing potentially dangerous communications links and possible anomalies to be identified. In general, it is not enough to only detect malicious links, but what is important is to determine which node is the generator of malicious traffic. This will allow appropriate actions to be taken to increase the cybersecurity of the system, and the paper proposes that the analysis of node behaviour be performed by using the graphical information encoded in a connection network with a triple approach:

- ✓ applying temporal dissection to extract information, graphics-based;
- ✓ introduction of two new techniques for graph data level preprocessing (R-hybrid and SM-hybrid);
- ✓ using a neural network and two graph convolutional networks (GCNs) to classify the behaviour of nodes.

2.2. Network monitoring tools

As mentioned above, there are many tools for monitoring network processes and traffic (Nagios, Wireshark, SolarWinds, Zabbix, Hyperc, Capsa free, IBM Tivoli, Ganglia, Kiwi Monitor, etc.), some are open source and others are commercial products that require license fees. However, usually the information they collect about all the events in the network is not always complete. On the other hand, it is possible to log multiple events, which defines a huge amount of data, and their value can be assessed by comparing them with events recorded from other sources. The article presents a brief overview of several useful tools:

✓ Nagios is an open-source tool that can monitor applications, servers, and networks, allowing the addition of monitoring capabilities for almost any network process.

✓ SolarWinds has an excellent graphical user interface (GUI) and offers a set of monitoring tools, supporting operating systems such as Windows, Mac, Linux. Installation time depends on the complexity of the data, allowing customization by the user.

✓ Wireshark is rated as one of the best open-source packages for examining traffic in wired and wireless networks, analysing all network traffic, and allowing filtering of traffic selected for monitoring. The tool is available in different versions (graphical and command) and works with Windows, UNIX, and Linux platforms.

✓ IBM Tivoli supports Windows, Linux, and Unix, allows for easy installation, but requires specific configuration and refinement of analytical functions and responses.

3. Initial Phases of Monitoring Organization in LAN

A procedure for initial organization of research is presented below.

3.1. Specifying the reason for monitoring the servers

One primary reason for conducting network process monitoring research is to troubleshoot server performance issues. Another reason is a need to increase the performance of a server, which can be done by improving disk I/O operations, reducing CPU utilization, and reducing network traffic loading the server. This phase can solve some problems and will analyse different possible situations which will improve the general performance of the distributed processing.

3.2. Preliminary preparation for monitoring

Preliminary preparation requires at the beginning to establish the level of performance of a given server by measuring the parameters at different stages of its operation. Based on a suitable preliminary analysis, an experimental plan can be formulated from sample steps:

1. Determining the main events in the monitoring server.
2. Establishing filters to reduce the amount of information collected.
3. Configuring monitors and alarms to monitor events.
4. Logging event data in a way that allows for easy subsequent analysis.
5. Analysing the recorded data from the measurements.

3.3. Network activity analysis using Performance Monitor

Windows Performance Monitor is a powerful tool and displays graphical statistics for a selected set of performance parameters for a given server. For each of the parameters defined for monitoring, information is displayed, and a separate graph is created, and the interval for its update can be configured. An example of network study with several servers is presented in the article as a graphical diagram for “Graphical visualization of the observed counters”.

3.4. Network performance monitoring

In addition to the performance of each of the servers, the overall performance of the entire network needs to be monitored. One way to examine performance during initial network design is through the Task Manager. The basic information provided includes the name of the network adapter (Adapter Name), percentage of network utilization (Network Utilization), speed of interface connections (Link Speed) and working state (State). The figure represents the total number of bytes of network traffic. Upon request, additional information can be provided about the percentage of files received as a fraction of the total connection caps, the total volume, as well as the current connection capacity used by all traffic on the network adapter.

3.5. Registration of events

When monitoring is conducted, the recorded behaviour information is stored in files (event logs). The accumulated information enables decision-making to ensure the operability and security of the network system. Enabling the “Event Viewer” provides an opportunity to actively manage event registration, as a quantitative and qualitative analysis of popular techniques and methods is summarized in the Table 1.

Table 1. Log options of Event Viewer

Name of Log option	***Comments***
ApplicationC	Events logged by applications and monitored for all servers
Security	Monitor and trace events with local or global group policies for all servers
System	Events logged by the operating system or its components
Directory	Registrations from Active Directory and related services
DNS Service	Registration (recording) of DNS requests, responses and other DNS activities (tracked only on domain controllers)
File Replication Service	Logs (records) system file replication activities (only tracked on domain controllers)

4. Conclusion

Preliminary monitoring of the behaviour of network components is a necessary stage when designing a virtual local network in each corporation, and the main requirement is to choose an appropriate tool suitable for the specific network environment. A preliminary evaluation of possible software tools can be based on the following criteria.

- Ability to monitor all devices on the network from servers to end user devices.
- Relatively easy use of the offered options, which does not require additional training of technical support employees.
- Timely notification when a problem or failure of a given component occurs in the working network environment.

After specifying the selected criteria, they should be analysed based on the proposed (existing) solutions (program monitors), analysing the overall value of the research and its effectiveness against the set goal.

REFERENCES

18 publications are included in the list of references

Thank you for your attention

Radi Romansky, rrom@tu-sofia.bg