ON METHODS AND MEANS OF COMPUTER NETWORK MONITORING

Ramiz Shikhaliyev

Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

Conduction of monitoring of existing computer networks (CN) is a very important task. The source of obtaining of objective data about functioning of CN, certainly, is network monitoring, without which it would be difficult to obtain authentic information about the condition of CN and make a decision on their administration. On the other side, without conduction of network monitoring it is difficult to obtain an objective conclusion about configuration of network's CN hardware and software, as well as about results of changes performed in them. Thus, condition of current CN must be continuously controlled, which would be impossible without conduction of network monitoring. Also, there are several other reasons for conduction of CN.

Firstly, increasing complexity and scale of current CN, as well quantity of network services and application, protection mechanisms, hardware and software used in them, result in occurrence of a very large volume of traffic with different types of information. Moreover, because of use of such application as P2P, VoIP, IPTV etc in CN, characteristics and volume of network traffic and range of malfunctions of network devices are changed, also, probability of their occurrence increases. As a result, tasks of diagnosis of condition and administration of CN, as well as provision of acceptable level of QoS (Quality of Service) become more complicated. Furthermore, possibility of continuous obtaining of necessary information about condition of network devices, services, application as well as actions of users in the work become important for CN administrators. Based on this information, administrators of CN can make operative decisions on network administration.

Secondly, conduction of network monitoring allows improvement of the network configuration and infrastructure of CN, which increases the effectiveness of its functioning. For example, early detection and improvement of errors or malfunctions in configuration of infrastructure of CN can prevent serious problems that can result in decreasing of the level of productiveness of CN and even their shutdown.

Thirdly, network monitoring allows provision of the CN security. Observation of main network devices of CN over a long period of time, allows determining the reasons of their shutdowns. Finally, consecutive and continuous monitoring of CN allows a better planning of their further modernization and reconfiguration. For example, elements of CN which must be improved and reconfigured can be detected as a result of network monitoring. For this reason, network monitoring is a very important task that must be solved by CN administrators and those responsible for its maintenance.

Usually network monitoring of CN is conducted through several directions: 1) monitoring of devices (or cross points) of CN; 2) monitoring of network applications, resources and services, which are performed on separate network devices. Both of these directions are very important for conduction of CN monitoring. Besides, it is necessary to preliminarily determine which devices and applications, resources or services must be undergoing monitoring. Also it is necessary to note that, network monitoring of CN (especially of large ones), can be an extremely difficult task if it's not preliminarily planned. Certainly, the best CN monitoring strategy would be monitoring of all devices, applications, resources and services. However in that case, the process of monitoring itself can generate large service traffic and consume a vast amount of system resources, which can lead to malfunctions of CN, as well as reduction of credibility of monitoring results. Thus, as a rule, instead of all devices of CN, monitoring of only main (or critical) network devices [1], such as servers, routers switches, hubs and firewalls is carried out.

Except main network devices, monitoring of other devices such as workstations, terminals etc can be performed. That’s why, depending on set tasks, choice of methods and tools of CN monitoring are very important.

There are several methods of monitoring which allow minimize the effect of CN monitoring process on CN network traffic [2, 3, 4]. One of the methods is based on limitation of the traffic, generated by the system of network monitoring. Mainly, according to the method, network administrators in network monitoring system can adjust optimal ultimate level for volume of the traffic generated by it. As a result, traffic of the network monitoring system will be minimized and reliability of the results will increase. Another method consists of monitoring of only critical cross points of CN, such as routers or servers. It is reasonable to apply this method in large CN, where number of routers is calculated by thousands and monitoring of all routers would be inefficient. Besides, in [1], we consider methods which allow optimizing the traffic of network, server and application clients.

During network monitoring of CN, it is important to monitor not only different types of network devices, but also applications conducted in them. For example, system administrator must be confident that operating systems of network devices (for example: servers, routers, switches etc) are configured and functioning correctly. Besides, monitoring of application mainly is used for checking of current condition of cross points, for example servers. Depending on the type of cross points, monitoring of specific characteristics for this device can be carried out. Based on collected data of these features, condition of this device, as well as facts of exceeding of value of one or another critical level characteristic can be determined. Moreover, during network monitoring of CN, decision regarding application of centralized (i.e. monitoring on one point) or distributed monitoring (i.e. simultaneously in several points) must be made.

Currently, different network monitoring tools (NMT) are used for monitoring of CN. Following are included in NMT: collection of values of characteristics of transmitting channels and routing equipment of CN, detection of abnormal situations, as well as bottlenecks in CN, forecasting of results of changes in CN topology, monitoring of actions of CN users etc. The most perspective NMT are those used in intellectual technology of network scanning and monitoring.

Depending on NMT application field, they can be divided in following: monitoring tools of the basic system, monitoring tools of system integrity, monitoring tools of system functioning and monitoring tools are service activeness. Current NMT allow presenting the condition of CN both in numerical and graphical form.

Some NMT are specific (for example: ping-, trace route-utilities etc) and are based on measurement of several characteristics of CN (for example: transmitting time of packets between two cross points of the network), others are more universal, i.e. they can simultaneously measure a variety of CN characteristics.

Ping utility [5] was created in 1983 for UNIX platform, and later was transferred to other platforms becoming the standard CN monitoring tool. Its purpose is controlling CN devices for the presence of connection, deliveries of test packets to it, and receiving of reply packets. Hereby time spent on transmittal and approval of receiving of test packets by network devices is determined and as a result, their preparedness and availability is determined. Based on this check it is possible to easily determine the characteristics of the network such as latency and availability.

Traceroute [5] utility was developed in 1988 for different versions of Unix (tracert utility is its analog for Windows platforms) and became a standard tool used for CN monitoring. This utility describes the route of packets from CN cross point to remote host, and at this time indicates intermediate routers. It sends test packets which pass through all intermediate routers to remote host.

Several metrics are used during CN monitoring. Following were proposed as main metrics for CAIDA network monitoring (Cooperative Association for Internet Data Analysis) Metrics Working Group [6]: latency, packet loss, throughput, utilization and availability.

Term "latency" has different definitions, but in CN monitoring context it can be defined as time necessary for the packet to move from network one cross point to another and back (RTT – Round Trip Time).

Network packet loss is defined as quantity of packets which are lost in a determined interval of time during their transmission from one network cross point to another and back. Packet loss is expressed in percentage from the general quantity of packets transmitted among cross points in a determined interval of time. Usually 15% of packets out of the general quantity are lost in a typical CN. If the packets loss is higher than 15% then it affects the efficiency of CN.

Throughput of the network can be defined as quantity of data transmitted from network cross point to another in a unit of time and is usually measured in bytes per second. Untypical performance of the network while using bandwidth can be determined during conduction of CN monitoring based on this metrics.

Utilization is defined as percentage ratio of network resource usage time to predetermined period of time, and allows determining fields of CN where usage of other network resources is hindered or used in excess. This information can serve as a basis for changing CN configuration and this way increasing its functional effectiveness.

Availability can be defined as ratio of availability time for normal usage of a separate network device of resource to predetermined period of time. Usually availability of a network device can be tested using ping utility.

After defining all CN (devices, application, resources, services etc) elements that must necessarily be controlled, it is also very important to determine the monitoring conduction method. For example, monitoring process of a small size CN (for example local calculation networks) can significantly differ from monitoring of large and very complicated CN. Generally, there are two existing methods for conduction of CN network monitoring: active and passive [7, 8]. Active or passive methods can be used depending on task solved by network monitoring.

Usually, active monitoring is conducted through input of standard test packets to CN (for example ping packets, traceroute, pathchar, ICMP protocols) and allows administrators to determine the correctness of replies from network cross points to standard requests, for example ping requests. However, active monitoring has some disadvantages: firstly, input of test packages can affect the network traffic and infringe normal functioning of CN which in its turn, will affect the results of monitoring; secondly simultaneous monitoring of a great number of CN cross points, i.e. generation of a large amount of tests packages can infringe the normal CN functioning.

Passive monitoring is conducted based on analysis of data collected from one or several cross points. Different tools of passive monitoring can be used for passive CN monitoring (for example MRTG (Multi Router Traffic Grapher), NetFlow, Nagios etc), which will allow to detect different malfunctions, delays, abnormalities (for example abnormality in user activity) etc in CN. During passive monitoring, there is no necessity of sending test packages and this means that network traffic is not infringed and nothing affects the monitoring results. Usually passive monitoring is used for monitoring of network devices and measurement of network traffic created by them, and as well as operation stations.

Network monitoring device MRTG [9] performs monitoring of network connections of CN, using SNMP-protocol [10], in addition it provides visualization (usually as a web-page) of incoming and outgoing network traffics of CN. Disadvantage of MRTG consists of inability to determine bottleneck, as well as type of traffic or protocol in CN.

Net-Flow protocol [11] was developed by Cisco Company as an alternative to SNMP protocol and was designated for collection of IP-traffic. Cisco routers can generate NetFlow-information in form of UDP-packets. In comparison with SNMP protocol, advantage of NetFlow protocol is that it consumes a less amount of processing resource and provides more detailed information about used protocols and ports. a clear conception about contents and volume of CN traffic can be obtained upon analyzing this information.

Nagios [12] is a program, designated for monitoring of hosts and services of CN. It operates on Linux or BSD platform and allows detection of problems arising in CN. Upon detection of a problem, Nagios alerts the CN administrators through mail, SMS etc.

Reference

1. Эд Уилсон. Мониторинг и анализ сетей. Методы выявления неисправностей. Изд. «Лори», 2002, 350 с.
2. Yuri Breitbart, Feodor F. Dragan, Hassan Gobjuka: Effective Network Monitoring. Proceedings of the International Conference On Computer Communications and Networks (ICCCN 2004), October 11-13, 2004, Chicago, IL, USA, pp. 394-399.
3. Y. Breitbart, C. Y. Chan, M. Garofalakis, R. Rastogi, and A. Silberschatz, Efficiently Monitoring Bandwidth and Latency in IP Networks, In Proceedings of IEEE INFOCOM, (2000).
4. Y. Breitbart, F. Dragan, H. Gobjuka, Effective Monitor Placement in Internet Networks, Journal of Networks, Vol 4, No 7 (2009), 657-666, Sep 2009
5. http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#ping
6. www.caida.org
7. T. Lindh. A new approach to performance monitoring in IP networks — combining active and passive methods. Proc. of Passive and Active Measurements (PAM 2002), 2002.
8. Deliverable MS.3.7.5: Report on Passive Monitoring Pilot, SA3 activity, GN2 project, August 2008.
9. http://oss.oetiker.ch/mrtg
10. RFC 1157 - Simple Network Management Protocol (SNMP) (http://ip-doc.com/rfc/rfc1157)
11. http://en.wikipedia.org/wiki/Netflow
12. http://nagios.org