IJRSET 2018 Volume 5, Special-Issue-2 Pages: 1-7

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

AN OVERVIEW OF NETWORK OPERATION AND MANAGEMENT

[1] A. Priyadharshini
[1] Assistant Professor,
[1] Department of Computer Science,
[1] Rathinam College of Arts and Science,
[1] Coimbatore-21.

ABSTRACT: A network operations center (NOC, pronounced like the word knock), also known as a "network management center", is one or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication[1] or satellite[2] network. NOCs are implemented by business organizations, public utilities, universities, and government agencies that oversee complex networking environments that require high availability. NOC personnel are responsible for monitoring one or many networks for certain conditions that may require special attention to avoid degraded service. Organizations may operate more than one NOC, either to manage different networks or to provide geographic redundancy in the event of one site becoming unavailable. In addition to monitoring internal and external networks of related infrastructure, NOCs can monitor social networks to get a head-start on disruptive events.[4]

Keywords: [Network operations center, Network monitoring, Health care,military,forest,animal planet]

1. INTRODUCTION

Early versions of NOCs have been around since the 1960s. A Network Control Center was opened in New York by AT&T in 1962 that used status boards to display switch and route information, in real-time, from AT&T's most important toll switches. AT&T later replaced their Network Control Center with a NOC in 1977 in Bedminster, New Jersey.[3]. tands for "Network Operations Center." It is the central location where a company's servers and networking equipment are located. The NOC may reside either within a company's campus or at an external location. Smaller businesses and organizations often have an internal NOC, in which local technicians administer and monitor the servers. Larger companies may have a NOC setup at a location developed specifically to house server equipment.Network operations centers, often called datacenters, are almost always connected to a high-speed Internet connection. Large NOCs, such as those used by Web hosting companies, are often connected directly to the Internet backbone. This gives the servers the most bandwidth possible.

While NOCs are used by all Web hosting companies and ISPs, they are also useful to companies whose services are not related to the Internet. Many companies use a NOC to manage internal communications, administer

employee e-mail accounts, and backup data. Because maintaining an Internet connection is vital to most businesses today, most NOCs are monitored 24/7, with automatic alerts that notify technicians when servers or network connections are down.

2. FUNCTIONS OF NOC

NOCs analyze problems, perform troubleshooting, communicate with site technicians and other NOCs, and track problems through resolution. When necessary, NOCs escalate problems to the appropriate stakeholders. For severe conditions that are impossible to anticipate, such as a power failure or a cut optical fiber cable, NOCs have procedures in place to immediately contact technicians to remedy the problem].

Primary responsibilities of NOC personnel may include:

Network monitoring Incident response Communications management Reporting problems

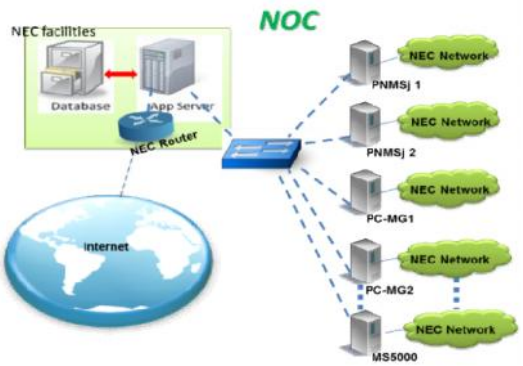

Figure: Network operation center(NOC)

NOCs often escalate issues in a hierarchic manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation. NOCs sometimes have multiple tiers of personnel, which define how experienced and/or skilled a NOC technician is. A newly hired NOC technician might be considered a "tier 1", whereas a technician that has several years of experience may be considered "tier 3" or "tier 4". As such, some problems are escalated within a NOC before a site technician or other network engineer is contacted.

NOC personnel may perform extra duties; a network with equipment in public areas (such as a mobile network Base Transceiver Station) may be required to have a telephone number attached to the equipment for emergencies; as the NOC may be the only continuously staffed part of the business, these calls will often be answered there.

2.1 NETWORK MONITORING

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is part of network management. Network Monitoring and Analysis Tools for System Adminstrator Monitor & control web activity Manage bandwidth & internet usage Secure downloads & web browsing Control of applications & stronger policy Automate multiple OS patching Scan for vulnerabilities Audit hardware and software Run compliance reports While an intrusion detection system monitors a network for threats from the outside, a network monitoring system monitors the network for problems caused by overloaded and/or crashed servers, network connections or other devices.

For example, to determine the status of a webserver, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3.

Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools -- especially when it comes to measuring accurate end-to-end response time because they limit round trip visibility.[1] Status request failures - such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved - usually produce an action from the monitoring

system. These actions vary -- an alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.

Monitoring the performance of a network uplink is also known as network traffic measurement, and more software is listed there.

2.2 REAL-TIME MONITORING SUB-SYSTEM

The real-time monitoring sub-system captures images of the area of the home to be monitored and serves the client who accesses the server through the web or a smartphone. Figure: shows the operation process of the real-time monitoring sub-system. The server finds a video device and captures images. Then, it generates captured data and transforms the data format for RTP communication. After that, it generates the session manager and streams media data to the client. A client using the web or a smartphone generates the session manager and connects to the server. Then, it receives media data and displays the video. In this way, the client can monitor the in-home status in real-time.

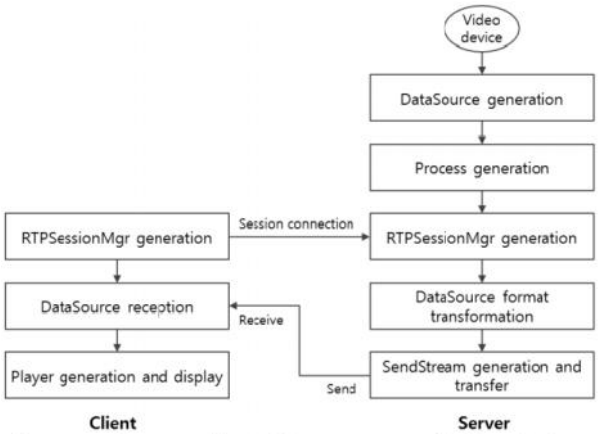

Figure: Operation Processes of Real-time Monitoring Sub-system

The operation of the sub-system is as follows.

A client program maintains a user interface which contains an on/off control panel.

A server which works as a gateway receives control commands from the client and relays the command to the ZigBee coordinator through the RS-232C serial communication.

The coordinator relays the control command which is received form the server to the end device through RF communication.

The end device receives the command from the coordinator and controls the port of the switch node.

The switch node controls the switch of the light

2.3 INTRUSION DETECTION SYSTEM

The purpose of the IDS is to detect certain well-known intrusion attacks on the host system and display warnings to the user and also store information regarding the IP addresses and allow the traffic based on that information. are at risk due to post-operative pain.

2.4 OVERVIEW INTRUSION DETECTION

The below sections give a short overview of networking attacks, classifications and various Components of Intrusion Detection System.

2.4.1. NETWORKING ATTACKS

This section is an overview of the four major categories of networking attacks. Every attack on a network can comfortably be placed into one of these groupings [21].

DENIAL OF SERVICE (DOS): A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine e.g. apache, smurf, neptune, ping of death, back, mail bomb, UDP storm etc. are all DoS attacks.

REMOTE TO USER ATTACKS (R2L)

A remote to user attack is an attack in which a user sends packets to a machine over the internet, which s/he does not have access to in order to expose the machines vulnerabilities and exploit privileges which a

local user would have on the computer e.g. xlock, guest, xnsnoop, phf, sendmail dictionary etc.

USER TO ROOT ATTACKS (U2R)

These attacks are exploitations in which the hacker startsoff on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges e.g. perl, xterm.

PROBING: Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, portsweep, mscan, nmap etc.

3. CLASSIFICATION OF INTRUSION DETECTION

Intrusions Detection can be classified into two main categories.

They are as follow: Host Based Intrusion Detection: HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files [22].

Network Based Intrusion Detection: NIDSs evaluate information captured from network communications, analyzing the stream of packets which travel across the network [22].

3.1. COMPONENTS OF INTRUSION DETECTION SYSTEM

An intrusion detection system normally consists of three functional components [23].

The first component of an intrusion detection system, also known as the event generator, is a data source. Data sources can be categorized into four categories namely Host-based monitors,

Network-based monitors, Application-based monitors and Target-based monitors.

The second component of an intrusion detection system is known as the analysis engine. This component takes information from the data source and examines the data for symptoms of attacks or other policy violations.

The analysis engine can use one or both of the following analysis approaches:

Misuse/Signature-Based Detection: This type of detection engine detects intrusions that follow well-known patterns of attacks (or signatures) that exploit known software International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 112 vulnerabilities [24][25]. The main limitation of this approach is that it only looks for the known weaknesses and may not care about detecting unknown future intrusions [26].

_ Anomaly/Statistical Detection: An anomaly based detection engine will search for something rare or unusual [26]. They analyses system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. The primary disadvantages of this system are that they are highly expensive and they can recognize an intrusive behavior as normal behavior because of insufficient data The third component of an intrusion detection system is the response manager. In basic terms, the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing someone or something in the form of a response.

3.2 Functional Requirement

The requirements to develop the system or software can be listed at two levels of abstraction.

- To develop an application that is capable of sniffing the traffic, to and from the host machine.
- To develop an application that is capable of analyzing the network traffic and detects several pre-defined intrusion attacks and mappings.
- To develop an application that warns the owner of the host machine, about the possible

occurrence of an intrusion attack and provides information regarding that attack.

• To develop an application that is capable of blocking traffic to and from a machine that is identified to be potentially malicious and that is specified by the owner of the host machine.

B. Feasibility Study Feasibility study consists of following things:

1. Technical feasibility
2. Operational feasibility
3. Economical feasibility
4. Reliability
5. Efficiency
6. Portability

1) Technical Feasibility:

Technical feasibility determines whether the organization has the technology and skills necessary to carry out the project and how this is obtained. The existing resources are capable and can hold all the necessary data. The system is too flexible and it can be expanded further.

2) Operational feasibility:

Operational feasibility determines if the proposed system satisfied user objectives and can be fitted into the current system operation. The proposed system will not cause any problem under any circumstances. The proposed system will certainly satisfy the user objectives and it will also enhance their capability. The proposed system can be best fitted into current operation.

3) Economical Feasibility:

It determines whether projects goal can be within the resource limits allocated to it. It must determines whether it is worthwhile to process with the project all or whether the benefits obtained from the new system is not worth the costs. After conducting cost benefit analysis, it reveals that the objectives of the proposed system can be achieved within the allocated resources.

4) Reliability:

It is evaluated by measuring the frequency and severity of failure, the accuracy of output results, the mean-time-to-failure (MTTF), the ability to recover from failure, and the predictability of the program.

5) Efficiency:

The amount of computing resources and code required by program to perform its function. The degree to which the software makes optimal use of system resources as indicated by some attributes like time behaviour, resource behaviour.

6) Portability:

As java language is being used the program is portable i.e. platform independent .Effort required to transfer the program from one hardware and /or software system environment to another. The ease with which the software can be transposed from one environment to another as indicated by some attributes such as adaptability, installability, conformance, replaceability.

CONCLUSION

Here discussed Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is part of network management. Network traffic monitoring is an analysis and reporting tool. It works in all Windows based operating systems. It captures all traffic transport over both Ethernet and WLAN networks. Network traffic monitoring decodes all major TCP/IP protocols. With Network traffic monitoring , you can easily filter the network traffic to focus on the information that you are looking for. Comprehensive reports and graphic views allow you to understand network performance and usage quickly and identify problems in simple steps. Protocol decoders for TCP/IP and many application protocols including ARP/RARP, ICMP, IP, TCP, UDP, DNS, POP3, SMTP, IMAP, HTTP/HTTPS,

TELNET, FTP. Powerful and easy to set filters allow user to focus on useful traffic and narrow down the problem. Easy to use user interface i conclude with this information.i am continue my process with the implementation work.

REFERENCE

[1]. Jeff Cormier (24 February 2011). "Exclusive : Inside AT&T's top-secret Network Operations Center (NOC)". Retrieved 25 August 2012.
[2]. "Network Operations Center opens to handle satellite bandwidth". 25 July 2012. Retrieved 25 August 2012.
[3]. AT&T. "History of Network Management". Retrieved 25 August 2012.
[4] Todd Haselton (26 July 2011). "A Look Inside AT&T's Global Network Operations Center (GNOC)".
[5]. The impact of WAN Optimization on NetFlow/IPFIX measurements
[6]. Int. J. Communications, Network and System Sciences, 2009, 6, 528-539 doi:10.4236/ijcns.2009.26058 Published Online September (http://www.SciRP.org/journal/ijcns/).
[7].International Journal of Software Engineering and Its Applications Vol. 6, No. 3, July, 2012 Soyoung Hwang and Donghui Yu* [8]. Volume 2, Issue 1, January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com .National Center for Health Statistics, URL:http://www.cdc.gov/nchs/Default.html,
[9].International Journal of Network Security & ItsApplications (IJNSA),Vol.4,No.2,March2012DOI:10.5121/ijnsa.2012.4208109 Mohammad Sazzadul Hoque1, Md. Abdul Mukit2 and Md. Abu Naser Bikas
[10]."Hewlett Packard Bench Briefs" (PDF). Hewlett Packard. Retrieved 14 October 2011.
[11]. Sullivan, Mike (Nov 15, 2000). "Secrets of a super geek: Use half splitting to solve difficult problems". TechRepublic. Archived from the original on 8 July 2012. Retrieved 22 October 2010.
[12].http://www.ocf.berkeley.edu/~joyoung/trouble/page1.shtml
[13]. A Scalable Architecture for Network Traffic Monitoring and Analysis Using Free Open Source Software Olatunde ABIONA1, Temitope ALADESANMI2, Clement ONIME3, Adeniran OLUWARANTI4, Ayodeji OLUWATOPE5, Olakanmi ADEWARA6, Tricha ANJALI7, Lawrence KEHINDE
[14]. Distribution-based anomaly detection in 3G mobile networks: from theory to practice Alessandro D'Alconzo1,*, Angelo Coluccia2 and Peter Romirer-Maierhofer1 Article first published online: 30 AUG 2010 DOI: 10.1002/nem.747
[15]. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-3, August 2012 Comparative Study of Network Monitoring Tools Shrutika Suri, Vandna Batra
[16]. N.C. Hutchinson and L. L. Peterson, "The X-Kernel: An architecture for implementing network protocols," IEEE Transactions on Software Engineering, Vol. 17, No. 1, pp. 64–76, 1991.
[17]. E. Kohler, R. Morris, B. Chert, J. Jannotti, and M. Frans Kaashoek, "The click modular router," ACM Transactions on Computer Systems, Vol. 18, No. 3, pp. 263–197, August 2000.
[18]. J. Allen, Cricket homepage, 2000, http://cricket.sourceforge.net.
[19]. J. D. Case, M. Fedor, M. L. Schoffstall, and C. Davin, Simple Network Management Protocol (SNMP), May 1990, http://www.faqs.org/rfcs/rfc1157.html.
[20]. V. Jacobson, C. Leres, and S. McCanne, "Tcpdump-the protocol packet capture and dumper program," http:// www. tcp dmp.org.
[21]. T. Oetiker, "Monitoring your IT gear: The MRTG story," IEEE IT Profesionals, Vol. 3, No. 6, pp. 44–48, December 2001.
[22]. G. Robert Malan and Farnam Jahanian, "An extensible probe for network protocol

performance measurement," in Proceedings SIGCOMM'98, pp. 215–227, September 1998.
[23]. J. Hong, S. Kwon, and J. Kim, "WebTrafMon: Web-based internetintranet network traffic monitoring and analysis system," Elsevier Computer Communica-tions, Vol. 22, No. 14, pp. 1333–1342, September 1999.
[24]. L. Deri and S. Suin, "Effective traffic measurement using ntop," IEEE Communication Magazine, Vol. 38, No. 5, pp. 138–143, May 2000.
[25]. L. Deri, R. Carbone and S. Suin, "Monitoring networks using ntop," Proceedings of IEEE/IFIP International Symposium on Integrated Network Management, pp. 199–212, May 2001.
[26]. L. Deri and S. Suin, "Practical network security experi-ences with ntop," Computer Networks, Vol. 34, pp. 873–880, 2000.
[27]. A. Hussain, G. Bartlett, Y. Pryadkin, J. Heidemann, C. Papadopoulos and J. Bannister, "Experiences with a continous network tracing infrastructure," in Proceedings of ACMSIGCOMM Workshop on Mining Network Data, pp. 185–190, August 2005.
[28]. O. O. Abiona, C. E. Onime, A. I. Oluwaranti, E. R. Adagunodo, L. O. Kehinde, and S. M. Radicella, "Development of a non intrusive network traffic monitoring and analysis system," African Journal of Science and Technology (AJST) Science and Engineering series, Vol. 7, No. 2, pp. 54–69, December 2006.
[29]. G. R. Wright and W. R. Stevens, "TCP/IP illustrated," 2 Addison-Wesley, Reading, M. A., 1994.
[30]. G. P. Java, IPTraf: http://iptraf.seul.org/ 2001.
[31]. T. Oetiker and D. Rand, "MRTG: Multi router traffic grapher," http://tobi.oetiker.ch/ 2008.