Reliability Measurement of Internet Services

Deris Stiawan[1] , Abdul Hanan[2] , Mohd. Yazid Idrus[2]
[1&2)] Computer Engineering Department, Faculty of Computer Sciences, Sriwijaya University
deris.stiawan@gmail.com
[2)] Faculty Computer Sciences & Information System, Universiti Teknologi Malaysia
{hanan.yazid}@utm.my

***Abstract*—** In this paper we propose an approach fundamental keys factor to impact directly causing Reliability aspect, with provides an analysis, evaluation, and management of the reliability of systems in wide as the heterogeneity of devices and the complexity of interconnection network. The aspect of Availability, Performance and Security have an important role in creating aspect to make High Reliability and that its can be still need improvement, especially in the Internet Services system with many devices and applications systems. With this description and analysis of expected service providers or companies that use IT as a primary strategies can make this as a framework in making the rules and policy. In this paper we presented measurement influencing factors for make high Reliability especially of internet services. This factors not be separated, is must combine to integrated systems

Keywords- *Reliability, Internetwork, Performance factors, QoS, Network Management*

I. INTRODUCTION

Customer demand for multi-service network is also increasing rapidly. An ultimate goal for modern Internet services is the development of scalable, high-performance, highly available and fault-tolerant systems. Internet services can benefit from dynamically choosing availability consistency tradeoffs in response to current network, service and access characteristics [1],[2].

Reliability is one of the most important performance measures for emerging technologies. Network reliability analysis mainly deals with the evaluation of the performance of a network in terms of its ability to withstand the failure of its components, used to measurement the stability of network components, internetwork, and application under heavy loads [3]. Reliability measurement is important now especially for service provider (SP) to make improve customer services.

Internetworking is currently to describe the integration of all networks in one centralized network, which previously separate networks between data, voice and video, now has become an internet service in one services integrated. Today user access can be anywhere, anytime and anyplace, when services has Spread, Integrated, and Distributed, it needed a guarantee of service to guarantee for that.

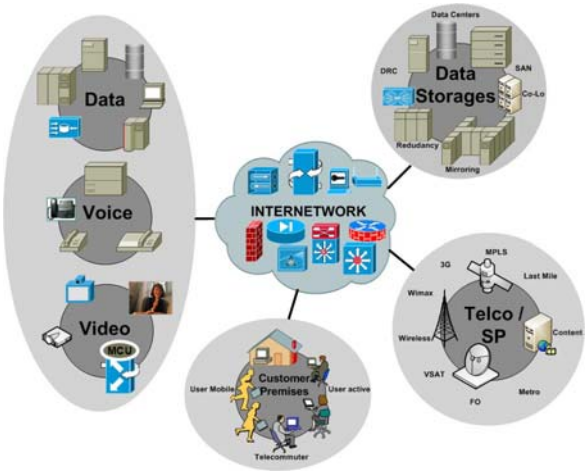

Figure 1. Internetwork Convergence connecting

This paper is intended to include security parameter as one of the parameters in reliability measurement. In previous work [6],[7],[8],[9] security parameter was measured separately however it has been proven that this parameter can affect the availability [14],15],[16].

This paper is organized as follows: Section 2 is background and related work. Section 3, describes several factors influencing the Reliability, focus on Availability, Performance, and Security aspect. Section 4, Improvement approach for Reliability presents the mapping to prove the factors in the reliability not only performance or availability factor, and Section 5 is a conclusion.

II. RELATED WORK

Network devices currently on the system internetwork services, it needed a mechanism for monitoring and management the network to wake up and the Reliability factors can be known early network anomaly or breaking it.

There have been many that describe the basic methods of implementation of the QoS or performance measurement in a project or scientific publication, but it is still rare and separate that discuss factors that affect the Reliability of a service level of the other aspects, this thing is important because the system could not be reliable established if it does not consider other factors that support it, found in studies conducted which proved

that the reliability cleaner a network service depends on the aspect of Availability, Performance and Security.

Availability evaluation addresses it is possible to ascertain the operational status of the whole system by monitoring at a single point, such system can be computed by calculating the Main Time To Failure (MTTF) and Mean Time To Repair (MTTR) from direct measurement of Times To Failure (TTF) and Times To Repair (TTR) of the systems, and in the paper to described too about calculated failure time, the boot up time, and the repair time with Markov model [15].

Ability to model network performance is important for many area of network research. Performance measurement usually used Markov modeling to evaluate the probabilities of normal and fault system to measure the probability and performance impact of various faulty states. The P-Graph is a graphical representation of performance data that provides a more coherent view into the nature of system performance than traditional single-valued metrics, and allows assessment and comparison between products, configurations, architectures and workloads. Almost not directly related, traffic analysis is always included into network performance modeling as its main component [16],[19],[20].

Influences of security on the performance of services and network with SoS parameters mapping from SLS to policy. The paper make a compare EU negotiated, mapping AAA, and finally Described the mapping of SLS on policies [5].

Policy management is an active area of research and a number of approaches to policy specification and enforcement have been put forward, perhaps the best known is DEN-Ng and the IETF QoS policy model [4],[5]. DEN-ng recognized the need for variety of formalisms to express policies and policy continuum accounting policy programming language (APPLE) and Policy Execution Environment for Accounting and Charging (PEACH) is located at the system. Policies formulate and express these goals in context specific term e.q. security policies, QoS policies, routing policies, traffic management and AAA policies. In making a rule there are standards that are often used, and the standard has been fully explained and described about the framework in making a policy [13],[14].

The relationship Performance and Availability with Security factor will be directly related, for example :

1. The influence of availability of a network will be annoyed by DoS / DDoS, UDP Flooding, worm or botnet attacks, cause that many users cannot be served.
2. Phishing or other vulnerability web activities will be impaired users by new methods to identity theft. This is related to validity of a web service guarantees.
3. The result from broadcast multicast network will be affect the performance, using the device layer 2 / 3 is a solution to divide segmentation and forwarding data packets.
4. Many users can be login with access right level and authorization scheme. This situation will be impact to decrease services and directly to affect the performance.

From the description and the relationship with the study, it can be seen that in determining a Reliable system or not, have to see from above aspects. The problem is what the factor system can be make Reliability. Therefore in this paper will be outlined and described that the factors Security is also impact to make High Reliability of a Internetwork Services, because the value depends that can not be separated.

III. THE PROPOSE METHOD

RELIABILITY = PERFORMANCE + AVAILABILITY + SECURITY

Figure 2. The Reliability factors service

In this section an extended of additional element for measurement reliability method, we propose to make Reliability or Unreliability internet services is not only measured from availability and performance factors, but the security factor is also one critical factor.

Figure 2, describes our extended propose method to make reliability factor. Figure 3, describes about impact factor for a reliability value, every factor is one system and not to be separated.

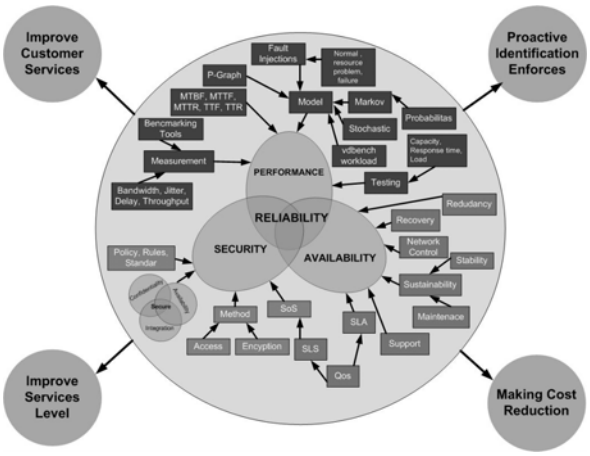

Figure 3. Impact Factor for High Reliability

A. *Availability*

Availability of a system can be defined as the fraction of time the system is providing services to its users. Service must be awake 24 hours nonstop without desisting without influenced by weather, office hours, vacations or nationality day, employee leave, extinct electrics and etc, where services and resource must can be given without desisting.

In critical applications, there also need to be a reasonable confidence in the estimated value a system availability, in the other words, the quality or precision of the estimated value needs to be known too. Availability modeling is used to calculated the probability of the various faulty and normal states. Therefore, computing the interval estimates of availability to also essential [14],[19].

The availability of a system or service must stay awake every time and any time without stopping, and do

not be influenced by various factors (technical or non technical), e.q : weather, work hours, holidays, employee resign, power outages. Services and resources should be must given without end. Examples of some common cases ;

1. As a national holiday service server farm can not be accessed because the server crashes and EDP IT staff out of office.
2. Access to the server have a many constraints while at the office hours and services bottleneck, access can be done at 19:00 pm the at "low-access peek".
3. The connection to the server farm is often down have a high latency, this often happens during such rainy or cloudy days because last mile using wireless devices are not reliable with weather changes.
4. Disrupted services at the time of electricity supply down in a long time because backup power is not available
5. Application services is not optimal, such as email can be accessed with a login authentication, but can not receive and send mail or only local intranet webpage to browse.

B. Performance

Performance from system or services hardly influenced by peripheral or devices applied, from peripheral core, distribution, access must awake doesn't happened failure and causes downtime because classic problems like incompatible, crash, hang, lack of support hardware and technical service, etc.

Performance measurement is a rather complex problem, it is because that modern computer network is an integrated system which contains vast relating isomeric elements [19].

Performance of the system service is influenced by the devices are used, the device core, distribution, access must be maintained not to occur causing failure and downtime due to classical problems, such as incompatible, crashes, hangs, lack of hardware support and technical services. Event that often occur regarding performance issues ;

1. Router not performance because it used in the complex routing, because a lot many packet, high and many one second time, such as in the BGP routing.
2. Used server specification standard that cause the process services can be lack and server collapse, this happened usually to high request.
3. Missed configuration of the device causing the device performance is not optimal, especially devices that require a unique command settings
4. Using a service that is not appropriate, for example in the network with high traffic is still using the Ethernet and Fast Ethernet, or limited bandwidth usage when access to services is very high

C. Security

In today's large networked environments security is a major concern. A great variety of security technologies and mechanisms are employed in these environments in order to offer protection against network-based attacks. Useless of expensive peripheral with good performance but not safe, security and safety is concerning problem privacy and this more sensitive problem for absence of safe system whilst still be made man hand, system built only can be improved its and safety out of one level to other level.

To ensure this availability an implementation must be secure, but these security mechanism must themselves no reduce the availability of the overall systems [17].Useless expensive devices with guaranteed availability and good performance but it is not safe, security concerns and privacy are very sensitive issue. Some classic views that often appear, for example;

1. Top-level management considers that by using a layered firewalls and the new technology to prevent illegal action
2. We have a team IT support to defense attack from internet and worked every days continuously to monitor network infrastructure
3. Information to publish on the Internet is public information and not confidential information
4. Publish information on the Internet is public information and trade secrets is not a problem
5. All the people on the Internet is good man and there is no feel to illegal actions.
6. Configuration and still use weak passwords and default
7. With a security system can be easily to access, because the systems many an vulnerability
8. The system can not be accessed due to malware or botnet infection that causes the system not available.

IV. INFLUENCING FACTOR

From the previous, figure 3, can be described as factors that will influence to increase reliability in a Internet services.

Availability influencing factors,

- Recovery : is needed to restore the network to quickly return to normal, for example the use of Layer 2 / 3, using the Spanning-Tree and routing protocol configuration for alternate path to awareness and fast convergence
- Network Control : control on the network also needed to ensure that services continue to run, there are several procedures in the control network, including Planning, Configuration Management, Fault Management, Performance Management, Accounting Management, Material Management, Workforce Management, this control make verify network readiness and health
- Support Failure Application : In a large system, such as using the ERP system, needed a solution to support that system can be resilient to failure.
- Stability : this system must be ensuring a stable network through proper physical, STP and routing design and processes to reduce human errors. Stability in the system also includes as a whole in order to maintain services
- Redundancy / backup : current system needed to be downtime can be reduced, one of the most

commonly used is the Network Load balancing, a technique used to separate between two or more network links. Have many links with the optimization of resource utilization, throughput, or response time would be better because it has more than one link that can back up each other when the network connection is down and can be multiplied at the normal network, this solution is suitable that require high reliability need 100% connection uptime and this solution can also be used to divide the upstream and downstream connections to different routing packet

- Sustainability : system that was built to be still resistant to the conditions that have been in predicting before, for example, the system will automatically backup while system crash, the system can independently conduct occurred while restoring data failed and failed resistant tolerant, the system will perform data redundancy in the system Disaster Recovery Center occurred while force majeure.
- SLA : service level agreement is about promises with CP and EU, SLA can make business objectives with guaranteed service levels, on SLA are technically complex to pull off from on operational stand-point, focus of thing incident records, service request, escalating, monitoring, etc .The role most commonly given SLA can generally into six areas Defines roles and accountability, Manage expectations, Control implementation and execution, provide verification, enable communication and return on investment

Performance influencing factors,

1. Measurement : how the measurement process is performed to determine the level of performance, usually used compare with another application program, or stretching with torture tests to get adaptable standard value. There are some factor of measurement, e.q Round Trip Time, Packet Loss, Network Jitter, Destination of Stats, connectivity. That is very critical factor From this we have see to overall values but measurement technique and methods to be used in adjusting the topology scheme will be measured.
2. Classification : Marking the packet with a specific priority denoting a requirement for special service from the network
3. Provisioning : Accurately calculating the required bandwidth for all applications plus element overhead
4. Schedule : periodically required to perform certain activities, such as maintenance, update, restart, to make system still optimal.
5. Model : use of a particular algorithm also has an effect on performance, the algorithm is usually very close to the model or the way a system will run, failure, inconsistency systems need more resources could be the fault of the algorithm used.
6. QoS : Mechanism usually guaranty metrics related to bandwidth, delay, jitter. Services classes, signaling, and connection admission control (CAC). Include : (a) conditioning, ex : policing, shaping or dropping. (b) queue management, ex : random early detection (RED), (c) queue scheduling, ex: weighted fair queuing (WFQ) and (d) Link-layer mechanisms.
7. Maintenance : this activity must be control and planning, with planning plan that reduce down time will be minimize and reduce deployment time.
8. Infrastructure (hardware, software, application), selection of hardware specs will greatly affect the performance of the equipment, which does not use will reduce the performance standards, as well as the reliability of the operating system, specification hardware or application in use, most system failures caused by infrastructure factors

Security influencing factors,

1. Integrated : integrated system as a whole is going to improve the accuracy of the data, but also will lead to other problems of security, because the integration of data, all data and information can get and query. Connected with branch offices, mobile users, branch, external business, and etc, will have an impact on the security problem.
2. Technologies and standards, used will be a factor in security, like VPN, AAA, RADIUS, Encryption, protocols, IDS, Firewall, PKI, Digital Certificate and etc, of concern also is the new thread and attack method, and that virus variants, DDoS, XSS, Buffer Overflow, DNS poison, injections, penetration systems, Phishing, Spoofing, Wireless hacking and etc.
3. SoS : Security of Services derived from Service Level Specification (SLS) and the description of the Quality of services (QoS). Review security business goals, objectives, and requirements. Focuses on developing, interpreting, and enforcing computer and network *security* policies. SoS create method for providing security, ranging from the simple creation and use of passwords to performing security investigations and analyses.
4. Confidentiality, Authentication, Authority, Non-repudiation, integration : is the standard factors that should be considered in developing a security system built.
5. Access : difficult if not noticed authorization factor, access rights should be regulated, when, where, and how long should be regulated.
6. User : some many users, the more complex the problem, should be made clear rules such as rights of Authentication, Authorization, and Accounting of each user. Should be divided into several groups and rights of each group. For example admin groups, DB admin groups, guest, etc.
7. Policy : There was no standard policy in the security field that has been used would be devastating to the security system that has been made, there are many standards in the field of

security policy which will be detailed set of security issues as a whole.

8. Awareness : Full awareness of all levels of management, this should be an emphasis on a security system that will be made, without any consciousness of all levels in the company of any sophisticated equipment will not be optimally used.

From the analysis conducted and describes so the results obtained are : Performance + Availability + Security = High Reliability, high reliability with a lot of benefits, including ;

- Improving Efficiently and Effectively, company would more Concentrating only is its business process which in the end product which will more effective and efficient
- Making cost reduction, with a reliable system will be able to reduce costs which were burdened with the cost of maintenance or deployment time high, resulted in the transfer cost at the other sector and enable the company making for other business process
- Improve customer services, company will be able to concentrate on services to enhance customer service and satisfaction to collaborate to better create new services more Performance visibility.
- Prove service levels, company can prove service levels with lower mean time to restore and downtime for services.
- Proactive identification of issues enforces higher reliability and making enhance acceptance of business-critical services

V. CONCLUSION & FUTURE WORK

In this paper, we presented influencing factors for make high Reliability especially of internet services, security is key factors not only performance and availability. This factors not be separated, is must combine to integrated systems. Future work, we plan to collect data with experiment on cases domain, describes for make analysis measurement proved.

REFERENCES

[1] A. Sevtap Selcuk, M. Semih Yu¨cemen, "Reliability of lifeline networks under seismic hazard", Reliability Engineering and System Safety 65 (1999) 213–227

[2] Haifeng Yu Amin Vahdat, "Building Replicated Internet Services Using TACT: A Toolkit for Tunable Availability and Consistency Tradeoffs", Advanced Issues of E-Commerce and Web-Based Information Systems, 2000. WECWIS 2000. Second International Workshop on 8-9 June 2000 Page(s):75 – 84

[3] Bo Chen,Weidong Zhu, Yaping Zhou, Lionel z. Li, "Internet Service Control Based on Customer Choice", Proceedings of the 7th. World Congress on Intelligent Control and Automation June 25 - 27, 2008, Chongqing, China

[4] K. Ravindran, " End-to-end 'Data Connectivity' Management for Multimedia Networking" , Proceedings 8th International Conference on Management of Multimedia Network and Services, MMNS, pp 190-2003 (2005).

[5] Sandrine Duflos, Valerie C.Gay, Brigitte Kervella, Eric Horlait, "Improving the SLA-Based Management of QoS for Secure Multimedia Services", Proceedings 8th International Conference on Management of Multimedia Network and Services, MMNS, pp 204-215 (2005).

[6] CADENUS (Creation and Deployment of End-User Service in Premium I Networks) Project, http://www-rp.lip6.fr/adanets/, [last access on 28th December 2009

[7] AQUILA Adaptive Resource Control for QoS Using an IP-Bases Layered Architecture) Project, http://www-rp.lip6.fr/aquila/, [last access on 28th December 2009]

[8] MESCA (Management of End-to-end Quality of Service Across the Internet at Large) project, http://www.ist-world.org/ProjectDetails.aspx?ProjectId, [last access on 28th December 2009]

[9] Service Availability Forum, http://www.saforum.org/link/linkshow.asp?link_id=222310 [last access on 24th December 2009]

[10] Guerrero, J. Garcia, F. Valera, A. Azcorra, "Qos Management in Fixed Broadband Residential Gateways", Proceedings 8th International Conferenc on Management of Multimedia Network and Services, MMNS, pp 338-449 (2005).

[11] Antony Oodan, Keith Ward, et al, " Telecommunications Quality of Service Management", The Institution of Electrical Engineers, 2003

[12] Geralh Ash, Bruce Davie, et all, "Network Quality of Services Know it All", Elsevier, USA, 2009.

[13] K.R.Rao, Zoran S. Bojkovic, Dragorad A. Milovanovic, "Introduction Multimedia Communications, Application, Middleware, Networking", John Wiley, USA, 2006

[14] Kesari Mishra, Kishor S. Trivedi, "Model Based Approach for Autonomic Availability Management", Proceedings, 3th International Service Availability Symposium, ISAS 2006, Finland, pp 1- 15, (2006)

[15] Pat. PW. Chan, Michael R. Lynu, Miroslaw Malek, "Making Service Fault Tolerant", Proceedings, 3th International Service Availability Symposium, ISAS 2006, Finland, pp 43- 61, (2006)

[16] Antoni Wolski, Vilho Raatikka, "Performance Measurement and Tuning of Hot-Standby Database",Proceedings, 3th International Service Availability Symposium, ISAS 2006, Finland, pp 149-206, (2006)

[17] P. Badovinatz, S. Balakrishnan, et.al, " The Service Availability Forum Security Service (SEC) Status and Future Directions", Proceedings, 3th International Service Availability Symposium, ISAS 2006, Finland, pp 271- 287, (2006)

[18] Hairong Sun, Tina Tyan, Steven Johson, et. Al, " Performability Analysis of storage system in practice Methodology and tools", Proceedings, 3th International Service Availability Symposium, ISAS 2006, Finland, May 2006

[19] Marat Zhanikev,Yoshiaki Tanaka, "Modelling and Analysis of End-to-End Network Performance", IEICE, 2008