RESEARCH ARTICLE OPEN ACCESS

An Approach towards Optimization of Enterprise Network and Firewall Environment

Faisal Rahman, Parves Kamal
Lecturer, International Islamic University Chittagong, Dhaka, Bangladesh
B.S.C in Computer security & forensics, University of Bedfordshire (U.K), CCNA, Security

Abstract
We must admit that there information technology is the most vital part of most of the business operational environment where the companies performs immense information transaction from workstations to workstations, from servers to servers, and from LAN to WAN. So an optimized, planned and secure Information and communication system should be in place for an optimized business operation. Here we are concerned about enterprise network environment where this paper will help IT engineers to initiate an organized IT infrastructure deployment and finally to make it secure. Network setup and server installation is a common practice on any Business environment now a day. This paper will focus on how to optimize the whole setting and how to maintain a concurrency within each layer of IT operation.

Index Terms **-**Network optimization; date center design; virtualization; layered approach; security; infrastructure mapping

I. INTRODUCTION

Use of advanced communication system in any medium and in enterprise business in not an un-even scenario now a day and technologies are out in the market to meet the need of the requirements of the company. Implementing right things on right place is vital as it points out few different key objectives when it comes to a matter of installing new technologies in operational environment. From technical point of view these are the network and endpoints components, design architecture and end user need. Local area network management is the key goal of this paper and here we shall discuss on how to migrate new objects in Enterprise IT operation maintaining a seamless connectivity. The research actually starts from the baseline of IT infrastructure development and will discuss about integration of all kinds of communication system like LAN networking devices, optimal configuration on them with efficient firewall and VLAN VSLM ideas as well as it will discuss about centralize control unit deployment like Central datacenter, Server and will point out successful migration of any new objects in the existing domain. So virtualization will be a key element that will be covered in this paper.

One of the main challenges that managers in a company always face with the IT infrastructure development is keeping the IT infrastructure work like a profit centre and in most of the cases it managers try to use existing infrastructure for further user demand mitigation process. Survey shows that about 80% hardware in a single stand-alone datacenter or in any stand-alone server is not utilized during operations. Even the report shows that the average network bandwidth utilization in LAN network is about 5%. So this is a great concern for the managers during the decision taking period regarding the extension of IT infrastructure and calculating the usability of the existing one. Extra network devices increase the network usage overhead and it increases the need for high network availability.

In most cases the usability of the network devices are not significant. Our concern in this paper is to show an optimized network design as well as optimizing the gateway firewall and demonstrate the optimization process results using physical network implementation as well as using the simulation program.

II. RELATED WORK

Network and hardware utilization is the objective of this paper where network transformation was described on [1]. VDI implementation is described in [2], Network segmentation and performance boost from isolation of workstations according to the role is described in a journal publication at [3], and Network security based on proxy installation on site is described at [4].System testing and network planning was presented in [5]. Router virtualization and redundancy protocol has been studied from [6] and configuration applied in Mikrotik router environment from [7] Firewall optimization concept is described in [8].

III. OUR APPROACH

Our proposed framework is “Collect-experiment-analysis-decision”. Based on the framework, we collected information relevant to the objectives of this paper, we implemented configuration based on the collection, analyzed the output after implementation, and proposed our decision on this paper towards optimization of network performance and security based on the analysis.

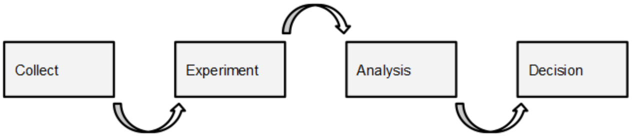


Figure 1: Research waypoint

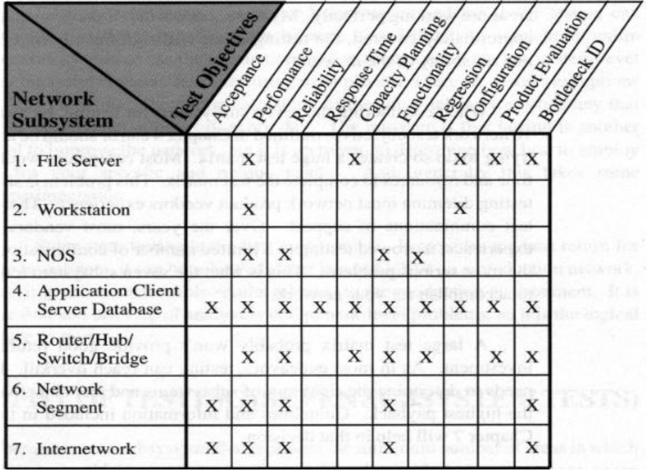
Note that, this paper is not describing any configuration not related to networking. This paper is all about network configuration optimization to get best user experience using the existing IT-infrastructure and with least cost consideration in installation and maintenance and of course this paper is considering the network security with the optimization practice. And note that this paper will discuss the layered approach while designing an enterprise network from scratch.

IV. EXPERIMENT ENVIRONMENT

The experiment is done on physical, virtual and in simulation like Packet tracer. The physical environment is built with one Mikrotik 450G Router-board and with couple of switches with Gigabyte Ethernet ports. The virtual environment is built with two Mikrotik Router-boards, Vmware virtual switch and with a test windows OS computer for route redundancy and firewall test. All experiments are designed using Cisco packet tracer before live experiment.

LAYER 1: PLANNING REQUIREMENTS

While planning for a scalable network design, simply we considered few stages according to [5] as following:



Network Subsystem / Test Objectives	Acceptance	Performance	Reliability	Response Time	Capacity Planning	Functionality	Regression	Configuration	Product Evaluation	Bottleneck ID
1. File Server		X			X			X	X	X
2. Workstation		X						X		
3. NOS		X	X			X	X			
4. Application Client Server Database	X	X	X	X	X	X	X	X	X	X
5. Router/Hub/ Switch/Bridge		X	X		X	X	X		X	X
6. Network Segment	X	X	X			X				X
7. Internetwork	X	X	X			X				X

Figure 2: A matrix to identify network objects test requirements [5].

So we decided what services an enterprise network might require at the first stage and planned hardware (network devices) implementations based on this. Based on the work in this paper we are presenting a priority based table to determine our required throughput in the LAN and WAN network environment.

Network components	Service priority	Expected Availability (%)
Router	High	99.95%
Switches	High	99.99%
Directory services	High	99.9%
File Server	High	99.5%
NOS server	High	99%
Workstations	Medium	99%
Anti-virus Server (update agent)	Medium	95%

Table 1: System availability requirement

It seems that we require high availability for most of the basic services on enterprise network but for our desired service availability, we had to calculate a downtime [6].

Availability (%)	Downtime / Year
99.99	53 minutes
99.95	4.38 hour
99.9	8.76 hours
99.5	1.83 days
99	3.65 days
95	18.25 days

Table 2: System downtime per year

So table 2 show us that having 99% service availability is not expected in our backbone devices. Internal backbone switches must have high availability that the backbone router as in corporate enterprise network most of the services are based on local network, file service, application service, NOS service, directory service, end user protection services like IDS and IPS are all based on local network. We shall compare the availability with simple no redundancy, simple LAN services redundancy and with full redundancy. And will see the downtime comparison in the network. It must be noted that system uptime does not means that the system is available for service. So our consideration here is to ensure High Availability with network services and determine a stable network topology.

LAYER 2: NETWORK DEPLOYMENT

This is a challenging phase while engineers need to work on initial installation of network components according to the planning placed on phase one. The core network elements like routers and switches should meet the requirements at first and for enterprise network there should have planned network access device (routers) cluster configured with proper load balancing method to utilize the maximum bandwidth purchased from.

Network can be designed in different way. The most common network architecture in small enterprise network is as followed:

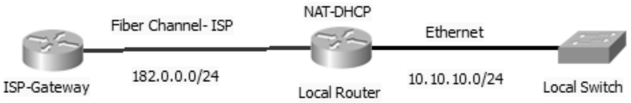


Figure 2: Small enterprise network design.

This type of design has major flow as it can be single point failure due to lack of redundancy. This type of network is pretty similar to SOHO network. But for large enterprise network considering couple of branches where intranet and extranet facilities should be in place, means where there will be service servers that should be available for business operation at 24/7, this type of network design is a disaster.

There is always ways out there in market which can give HA but if we bring extra core network devices in operation which in turn will cost the company a lot. To minimize the single point of failure situation from ISP operation we can have connection from multiple ISPs and we can configure NAT fail-over on the router. But for companies who mostly depends on LAN network for most of operational services, this is not a good solution. Here we are considering a network with one DNS server, Web server, File-server, Print server and NOS server for an enterprise network where all servers are under same switch and on the same LAN. Other computers in the company are in the same LAN as well.

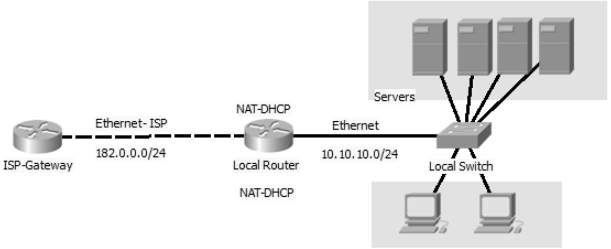


Figure 3: Single gateway-single LAN

This kind of network can be implemented when the company has very few employees and lack of dependencies on internal servers and still we have single point of failure in place. So we can’t rely on this structure and we shall keep this practice out of our consideration. Again placing all servers under same LAN is not a good practice for security as increases attack risk factor on the servers. Besides data transfer rate is not same for all servers. If we consider our servers, only File-server and NOS server will require high LAN bandwidth. For this we can use Gigabyte Ethernet between server and switch. As we are not discussing server configuration here in this paper we will not talk about HA cluster configuration among servers. But we shall consider that there is VmwareESXi virtualization in place and ESXi hosts are sharing same NFS iSCSI drive as storage solution and there is HA and DRS cluster configured within the ESXi Hosts and for optimized security, we are considering Vshield is there for virtual environment security. Separation of LAN using VLAN is essential to improve network performance as VLAN should not be considered as security measure in the network because there is attack called VLAN hopping to compromise VLANs. If we consider the following network with two VLANs and inter VLAN routing between them, we shall see there is lot of performance change as we separated ESXi hosts in that VLAN and transformed that network from Ethernet to Fibre optic channel mode.

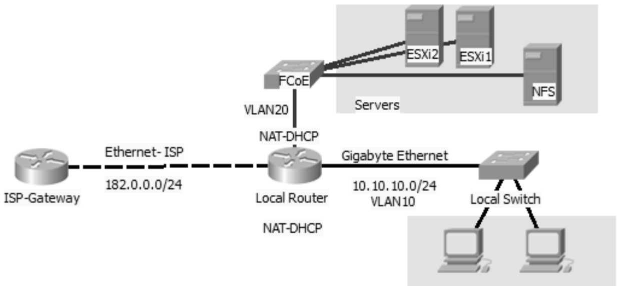


Figure 4: Single gateway-multiple LAN

Figure 2, 3 and 4 show slight improvement accordingly but still we have single point of failure in place. But for transformation to high performance LAN network, figure 4 is ideal. Figure 5 can give us quite good redundancy and high speed backbone networking. But still

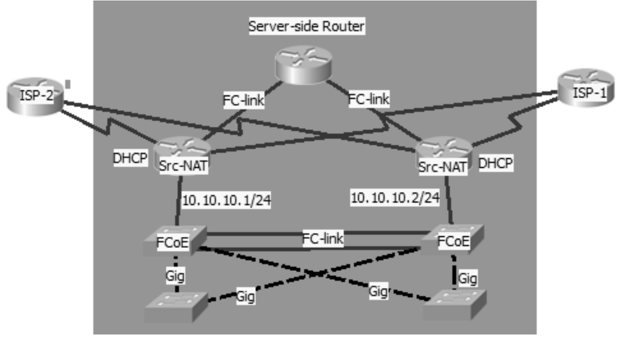


Figure 5: Multiple gateway-single gateway utilization-no load balance installed.

LAYER 3: NETWORK OPTIMIZATION

We have planned network and deployed network according to our requirements. Figure 5 gives us a solution for network fail-over.

But this type of network is not efficient enough for heavy production network where internet access is must for accessing remote services from remote locations. Besides it can manage to use only 50% of total network bandwidth due to single gateway use at a time. Indeed there is no single point failure in this network type but it gives network downtime for any backbone device failure. Network devices takes time to switch in other network and that is not a good practice for seamless services in enterprise network. In this circumstance figure 6 network type is much efficient where we plan to do Router clustering or fail-over configuration [6] using VRRP.

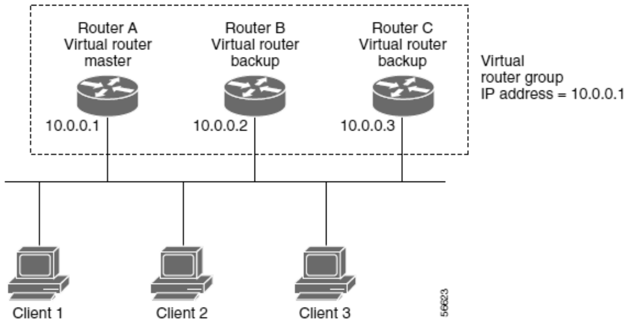


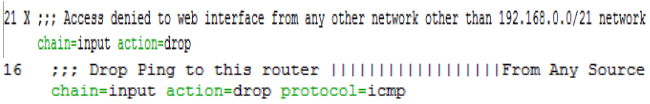
Figure 6: VRRP design architecture. [6]

The following table shows network address configuration of a workstation before and after implementing VRRP HA cluster in our Mikrotik lab environment. We planned to use two VM RouterOS 5.18 and a test Windows OS workstation, each of these systems with vmnet8 (NAT). Built a complete isolated VM network where the LAN is 10.10.10.0/24. Two VM routers considered to have individual ISP connections.

	Before	After
Configuration	Host IP: 10.10.10.120 Mask: 255.255.255.0 Gateway: 10.10.10.1	Host IP: 10.10.10.120 Mask: 255.255.255.0 Gateway: 10.10.10.254
Number of gateways	1	2
VRRP interface address	NA	10.10.10.254
Auto-failover	No	Yes
Downtime	Yes	No
Load balance	No	Yes (Configured)

LAYER 4: FIREWALL OPTIMIZATION

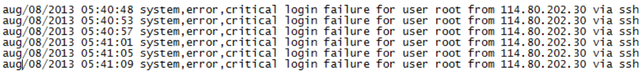
This is well known to everyone and each network use a minimum level of firewall built into the gateway router. A default firewall configuration can be a result of performance bottleneck. Our focus here on network firewall optimization. In most cases small and medium enterprise network leave there default firewall configuration on their gateway. Network managers leave remote Internet access on the router to do remote troubleshooting and that is significant risk for network. Our research showed that when we left our firewall configuration like:



```
21 X ;;; Access denied to web interface from any other network other than 192.168.0.0/21 network
     chain=input action=drop
16    ;;; Drop Ping to this router ||||||||||||||||||From Any Source
      chain=input action=drop protocol=icmp
```

Figure-result 1: Disabled filter rules on Mikrotik 450G

When this filter rules are disabled, following unauthorized access attempts from public internet network was found with different false random credential.



```
aug/08/2013 05:40:48 system,error,critical login failure for user root from 114.80.202.30 via ssh
aug/08/2013 05:40:53 system,error,critical login failure for user root from 114.80.202.30 via ssh
aug/08/2013 05:40:57 system,error,critical login failure for user root from 114.80.202.30 via ssh
aug/08/2013 05:41:01 system,error,critical login failure for user root from 114.80.202.30 via ssh
aug/08/2013 05:41:05 system,error,critical login failure for user root from 114.80.202.30 via ssh
aug/08/2013 05:41:09 system,error,critical login failure for user root from 114.80.202.30 via ssh
```

Figure-result 2: Unauthorized logon attempt to the gateway router.

Enabling these rules makes the gateway router untraceable from internet and it prevents any remote access on the router from internet. But VPN tunnelling on the router can give us solution for network administrators to administrate the routers locally from internet according to the following scenario built in our lab. Note that we have to create a VPN network exception on the firewall.

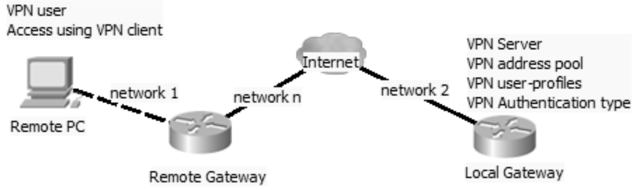


Figure 7: VPN tunnelling for administrative purpose.

So administrators from remote network can create a VPN tunnel connection in order to get access to the office router.

Another fact in order to optimize network bandwidth and to minimizing the chance to create a bottleneck on gateway, the following filter rules can be created on the firewall:

- Enable established connections.
- Drop invalid connections.

These rules can simply give an optimized connection stability as well as quality. Besides I had to comply with the concept described in [8] where few things pointed out in order to optimize firewall for QoS. Those are:

- Ensuring and monitoring that the outbound traffic is fully complied with policies.
- Filtering unwanted traffics.
- Removing unwanted rules and policies.
- Reducing the rule based complexity.

V. CONCLUSION

Our Aim was to present different network design level efficiency and described the redundancy in operation. Along with that we presented network load balancing configuration to utilize maximum available bandwidth using redundant link. Finally firewall optimization was in place which is vital in enterprise IT solution for better performance and security management. We planning on taking our design concepts on optimizing security at enterprise levels

VI. Acknowledgement

This research wouldn't have been possible if we were not been funded and given the opportunities to use the computer Lab at International Islamic

University Chittagong. We therefore would like to thank all the stuffs, lecturers that helped us in conducting our research and made this paper possible to make.

REFERENCES

[1] Shameemraj M Nadaf, Hemant Kumar Rath and AnanthaSimha, “A novel approach of enterprise network transformation and optimization,” *IEEE*, 2012.

[2] "Virtual desktop infrastructure planning overview", [online]http://*ws.iaitam.org/Misc/Scalable_Virtual_WP.pdf*.

[3] "Boost network performance with segmentation", [online]http://www.rockwellautomation.com/news/the-journal/exclusive/2013/march4.page, March 2013.

[4] Dwen-Ren Tsai,Allen Y. Chang, Sheng-Chieh Chung, You Sheng Li "A Proxy-based Real-time Protection Mechanism for Social Networking Sites", *IEEE, 2010*

[5] Victor Y.T Wang, "Testing of Ethernet switch",[online] http://speed.cis.nctu.edu.tw/~ydlin/course/cn/srouter/test.pdf, *Acute Communication Corporation*,2010.

[6] Cisco, "Configuring VRRP", *Cisco System Inc., May*, 2005.

[7] Mikrotik wiki, "Mikrotik VRRP manual", [online] http://wiki.mikrotik.com/wiki/Manual:VRRP-examples*Mikrotik wiki*, September 2011.

[8] Reuven Harrison, “How to Optimize Your Firewalls for Maximum Performance” [online] - http://www.eweek.com/c/a/Security/How-to-Optimize-Your-Firewalls-for-Maximum-Performance/, *Eweek*, February 23, 2010.

AUTHORS BIOGRAPHY

PARVES KAMAL: Parves Kamal Has Completed BSc With honor’s in Computer Security & Forensics from University of Bedfordshire (U.K), Cisco CCNA & COMPTIA SECURITY+ Certified.
EMAIL: Parves.kamal@gmail.com

Author of the research paper titled A state of the art survey on computer security incident handlings At: http://www.ijser.org/onlineResearchPaperViewer.aspx?A-State-of-the-Art-Survey-on-Computer-Security-Incident-Handling.pdf Research Interests in Computer security, live and dead forensics, ethical hacking, wired and wireless networking.

FAISAL RAHMAN: Faisal Rahman Has Completed BSc With honor’s in Computer Security & Forensics from University of Bedfordshire (U.K).He is currently Manager In IT-operation, Academy of Management and Science, Dhaka
Email: f.rahman.uob@gmail.com