ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Impact of Information and Communication Technology in the Development of Network Services

Vishnu Kumar[1], Surendra Kumar Patel [2], Dr.S.K.Shrivastava[3]

[1]*DR.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA,*
MPHIL SCHOLAR

[2]*DR.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA,*
PHD SCHOLAR

PROFESSOR
[3]*RAJEEV GANDHI GOVT.P.G.COLLEGE, AMBIKAPUR (SURGUJA)*

Abstract- A simple IP Subnet VLAN is implemented. By using implicit tagging, the problem related to packet tagging is removed. The distinction between hybrid port and trunk port is no longer important. Leaky VLAN implementation enables the switch to perform packet classification only when it is necessary. This dramatically reduces the processing requirement in each switch. It is also found that for IP subnet VLAN, the VLAN registration protocol can be simply replaced by the router. There is no need for the switches to run any VLAN registration protocol if the router can send out a periodic multicast VLAN packet to all switches. Switches can detect their port mode by using spanning tree protocol and checking the source MAC address of the spanning tree packet. Some conformance testing has also been done to verify the correctness of the implementation, VLANs offer significant cost and performance befits for a majority of the LANs installed today. These benefits are realized as network managers migrate to switched LAN architectures across the enterprise. VLANs are more than simply a shared hub, routing, switching, or network management solution. It is the combination of all these components that provides powerful segmentation and efficient administration across the network

Keywords: IP Subnet, IT network, recovery processes, switch's, implementation, VLANs.

I. INTRODUCTION

Under the structured IT network, required facilities are to be set up to quickly detect problems across different technology layers in Network, IT & Communication Infrastructure, isolate them and fix them proactively before users are affected. Historical data regarding the usage and performance of IT infrastructure is also to be built up as part of ongoing process for analysis and projection of future requirements for timely provisioning [1]. So this project shall meet the following broad objectives:

a. Business Requirements and Goals

Data Network and IT systems infrastructure in have grown considerably in size and complexity. Usage of Network for business has also increased. In this situation, High availability and performance of Network systems has become a mandatory requirement, which is a challenge. Management of end-to-end service levels is getting difficult due to the complexity of infrastructure and the way it is managed [2]. It is now desired to move away from a resource intensive, reactive break-fix problem solving approach to a pro-active and preventive process of problem discovery, diagnosis and repair [3]. The proposed solution shall reduce Mean Time to Recovery (MTTR) and increase availability of Business systems by pro-actively managing the IT infrastructure repair and recovery processes.

b. Aligning IT with Business

In today's scenario IT applications are implemented to boost the business. It is the business that demands IT infrastructure to

support various business applications. needs a complete IT Infrastructure management solution, which can be delivered from a Service Oriented approach[4]. The infrastructure shall be mapped to major business applications or Services e.g. E-mail, Internet, SCADA etc. The EMS tools shall provide a high level view of the availability and performance of the infrastructure for these services. It shall also provide real-time visibility into critical availability and performance problems with applications, systems or networks so that corrective action can be taken in time [5].

c .Management of IT service Levels

If most of the management tasks can be self managed, then IT operations can spend more time on developing strategies to manage IT infrastructure according to business priorities. Thus to improve efficiency of the organization, IT service levels are to be improved upon [6]. It shall be possible to measure and report the current service levels, resources required for further improving the service levels, Coordinating other service management functions and Reviewing SLAs to meet changing business needs.

d. Increase productivity

Traditionally IT responds when users complain about poor response by checking each infrastructure component supporting the application. This can lead to lengthy resolution cycles, missed service levels, and dissatisfied end-users [7]. The Application Performance Monitor must help IT avoid this situation by monitoring application performance from an end-user perspective, notifying IT when response falls below acceptable levels and identifying the infrastructure component at fault (i.e. server/ application, Local Network or WAN Connectivity).

e. Managing Risk

New technology initiatives can provide business value and reduced cost, but are at risk if they cannot be managed is looking for the Infrastructure Management tools which help in managing the risks involved in various IT operations [8].

f. Efficient utilization of technology

Manage resources more effectively based on the business needs and priorities. For this purpose, suitable reporting, notification and auditing functions are to be provided based on standard processes. Central repository of the enterprise level IT assets and events generated by the Network, systems & applications is to be maintained [9].

II.PROBLEM IDENTIFICATION

The problem is network size. Network size is very wide that's way whenever a user search the page related with work then user found many pages by using search engine. Search engines maintain indices for searching documents threw downloading pages constantly [4]. This process of crawling by web called web crawling technique. That mobile phone acts as a server in crawling technique. For searching the information so fast we should use mobile phone crawler that way it reduce the traffic and also reduce the load on remote side appreciably [5]. Java aglets can be help accomplishment of Mobile phone system.

III.LITERATURE SURVEY

a. Scientific data Processing Centers

The scientific systems are being used for handling Wells, Drilling, Logging, Reservoir and other E&P Data.EPINET (Exploration & Production Information NET work) Work Stations are installed at all Asset locations, Forward Bases and major work centers. For these systems, very high level of security is required to protect the scientific data. They are being managed by respective owner groups.

b. Business and other IT Infrastructure

ICE (Information Consolidation for efficiency).implemented SAP based ERP (Enterprise Resource Planning) system across the enterprise with Data Center at Delhi. It is one of the biggest global ERP project in Asia with 13000+ users spread over 400 locations of. It covers most of the business applications like Finance, Materials, HR, Plant Maintenance and Sales & Distribution etc [10].

Desktops: About 15000 Microsoft Windows based PCs/ Desktops/ Laptop are deployed at various places in for ICE, e-mail, Internet, Intranet and other applications. Which are likely to increase substantially in the near future with planned provisioning of laptops for all executives [11].

c. Telecom Infrastructure

ICNET (Integrated Communication network) Satcom .has a captive Satellite Network with 43 Earth Stations using C-band (4-8 GHz) transponder for providing Voice Channels in DAMA (Demand Assigned Multiple Access) and Data Channels in PAMA (Pre Assigned Multiple Access) mode. The Data channels are presently used to provide connectivity to offshore locations [12].

d. Upcoming Infrastructure

Upcoming IT systems

SCADA (Supervisory Control and Data Acquisition) system: For Real Time monitoring of Production and Drilling Installations, Enterprise wide SCADA is being implemented to cover about 300 locations. SCADA shall be based on three tiers Architecture. In tier-one, Windows based SCADA servers shall be installed at all the Production & Drilling Installations [13].

e. Upcoming Telecom Infrastructure

MF-TDMA based SATCOM: infrastructure is being setup to add 157 additional Earth Stations/ VSATs to meet the data connectivity requirements for SCADA, ICE, Internet/Intranet and other applications. This network shall also provide voice connectivity using VOIP facility and shall be seamlessly integrated with existing EPAXs already connected on VOIP [14].

IV.METHODOLOGY

Default Port Security Operation: The default port security setting for each port is off, or "continuous". That is, any device can access a port without causing a security reaction. Intruder Protection. A port that detects an "intruder" blocks the intruding device from transmitting to the network through that port [15].

Eavesdrop Protection: Using either the port-security command or the switch's web browser interface to enable port security on a given port automatically enables eavesdrop prevention on that port [16].

General Operation for Port Security: On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once port security is configured, you can then monitor the network for security violations through one or more of the following [17]:

■ Alert flags that are captured by network management tools Alert Log entries in the switch's web browser interface

■ Event Log entries in the console interface

■ Intrusion Log entries in the menu interface, CLI, or web browser interface

For any port, you can configure the following:

■ Action: Used when a port detects an intruder. Specifies whether to send an SNMP trap to a network management station and whether to disable the port.

■ Address Limit: Sets the number of authorized MAC addresses allowed on the port [8].

■ Learn-Mode: Specify how the port acquires authorized addresses.

Continuous: Allows the port to learn addresses from inbound traffic from any connected device. This is the default setting. Limited-Continuous: Sets a finite limit (1 - 32) to the number of learned addresses allowed per port. Static: Enables you to set a fixed limit on the number of MAC addresses authorized for the port and to specify some or all of the authorized addresses. Configured: Requires that you specify all MAC addresses authorized for the port. The port is not allowed to learn addresses from inbound traffic.

■ Authorized (MAC) Addresses: Specify up to eight

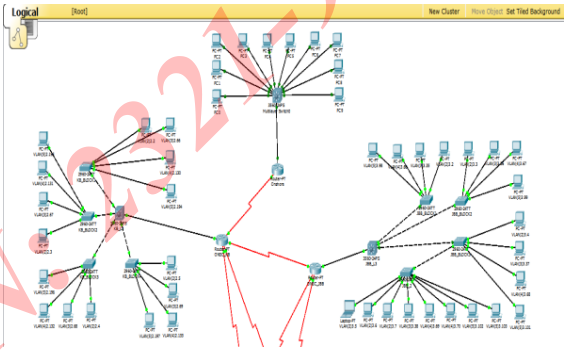

FIG:1. Port Security configured in the switches

devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:

- Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
- Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port [6,7].

■ Port Access: Allows only the MAC address of a device authenticated through the switch's 802.1X Port-Based access control.

Blocking Unauthorized Traffic

Unless you configure the switch to disable a port on which a security violation is detected, the switch security measures block unauthorized traffic without disabling the port [8]. This implementation enables you to apply the security configuration to ports on which hubs, switches, or other devices are connected, and to maintain security while also maintaining network access to authorized users. For example:

ISSN: 2321-9653

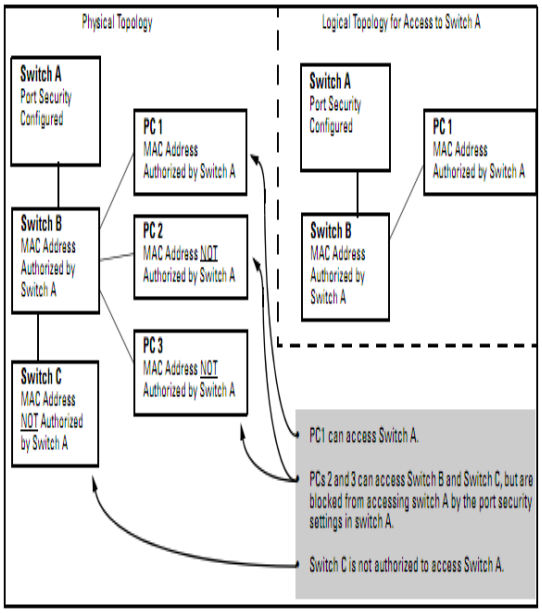

FIG:2. Example of How Port Security Controls Access

V.EXPERIMENTS AND RESULTS

.In order to test the correctness of the network configuration after considering the proposed security methods, an experimental test bed represents the network was built. The purpose was to test the network security robustness against different types of attacks [8,11].

The following procedures were taken to examine the network operation:

1 A correctly monitoring network can give warning of a number of network security violations ethereal program one program was used to monitor traffic over the network and between the VLANs.

2- Used some programs and tools such as Dsniff (a collection of tools to do ARP spoofing and MAC flooding), Macof tools to do MAC spoofing and CAM table overflow attacks. Also used DHCP gobbler programs to do DHCP starvation attacks , arp spoof tools, IP and ports scan, and sniffer program (as the hacker does before his attack), these security techniques can applied on switch and router[11].

3- The illegal log in to the network as well as unauthorized access to some services and resources are prevented.

4-Trying to use the TELNET service or PING command are stopped by the switches and routers by implementing access lists.

Also, several additional tests were made on the network to check the activity of the other security methods. It was found that protection of a network could not be achieved by a Single technique but with an integrated bundle of solutions [13].

5-Apply port security on the switch to mitigate CAM table overflow attacks. The type of action taken when a port security violation occurs falls into the following three categories: Protect, Restrict, Shutdown [3].

VI.CONCLUSION AND DISCUSSION

The main objective behind this research work is Network Security Model using Static VLAN and port security, ACLs and authentication. Today VLANs are not only used as an integral part of the LAN environment, they are now also being used as a means of providing WAN / MAN services. Common problems associated with this technology, these realized as network administrator should take this into account when implementing VLANs to achieve security on network and protect against the types of threats and attacks. One of the primary security issues with VLANs is poor configuration in network devices. There are many configuration issues that need to be addressed during the configuration process in a switching architecture [7]. After doing test to the network security model, showed a very efficient security performance keeping a high performance of the network speed and services. On the other hand, the added security methods should not affect seriously on the network management or its performance.

VII. FUTURE WORK

In Future such implementation can be done so that we can use these following ways of mobile phone crawler's server implementation:

Conduct experiment with crawling approach that way efficiency of our mobile crawlers are improved. By using digital signature, it can introduce a recognition mechanism. That's way we implement security oriented design of the mobile phone crawler. we are reporting analysis part of two-phased crawling which currently implemented. Mobile phone as a server work and crawl the data and give it to client, it should also click live image and can see the data [5].

VIII.APPLICATIONS OF ANDROID TECHNOLOGY

Google Play or the Amazon App store are app stores through which user downloads images, this process done by third party applications or user could also downloading the application's APK. Applications filtered by user's device and developers restrict their application countries for business reasons. In September 2012 there are 837,000 apps available in Android Phones.

Development of Android Application

Google developed privately and released updates and also it point out source code is made available publicly. Nexus series of devices are mostly run source code which was not modified. Other proprietary binaries are making available by the developer in categorize for Android.

Linux

Linux kernel version 2.6 is used in Android. Google outside Linux kernel development cycle changed the Linux kernel architecture for Android's. Linux support set of standard GNU libraries. These libraries are by using this makes it difficult libraries to Android. It uses the JNI. Jagged Alliance 2 port for Android is the best example of Linux in java shim.

MEMORY MANAGEMENT

Ram is managed by Android it also usually battery-powered devices. It connected to unlimited mains electricity. When Android application is not in use it robotically suspends its memory. Suspended apps do not consume any resources, battery power or processing power. When in mobile memory space is low it automatically manages the applications and start killing app which inactive for a while [15].

Security and privacy

Using sandbox Android applications is run. The play store is displays all required permissions before installing an application. In androids mobile it needs SD cards space for installing a game. After that Android provide facility for user to accept or refuse them. It is installing application when user says yes for installing [9].

REFERENCES

[1]. Minli Zhu, Mart Molle, and Bala Brahmam, "Design and Implementation of Application-based Secure VLAN", Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) Available:ieeexplore.ieee.org/iel5/9433/29935/01367248.pdf

[2]. S. Rouiller. Virtual LAN security: Weaknesses and countermeasures. Technical report, SANS Institue, 2003

[3]. Rajaravivma, V.; "Virtual local area network technology and applications," Proceeding of the Twenty-Ninth Southeastern Symposium on, 9-1 1 March 1997 Pages49 –52.

[4]. Tomohiro Otsuka, "A Switch-tagged VLAN Routing Methodology for PC Clusters with Ethernet", Proceedings of the 2006 International Conference on Parallel Processing (ICPP'06)

[5]. T. Kudoh, H. Tezuka, M. Matsuda, Y. Kodama, O. Tatebe,and S. Sekiguchi. "VLAN-based Routing: Multi-path L2 Ethernet Network for HPC Clusters". In Proc. Of 2004 IEEE International Conference on Cluster Computing (Cluster2004), Sept. 2004.

[6]. Cole E., Krutz R. and Conley J., Network Security Bible, 1'st Edition, Wiley Publishing Inc., 2005.

[7]. David Barnes, Basir Sakandar, Cisco LAN Switching Fundamentals, Cisco Press, July 15, 2004

[8]. R. Khoussainov and A. Patel. "LAN security: Problems and solutions for ethernet networks". Computer Standards and Interfaces, 22:191–202, 2000.

[9]. "Overview Of Key Routing Protocol Concepts: Architectures, Protocol Types, Algorithms and Metrics". Tcpipguide.com. Retrieved 15 January 2011.

[10]. Requirements for IPv4 Routers,RFC 1812, F. Baker, June 1995

[11]. Requirements for Separation of IP Control and Forwarding,RFC 3654, H. Khosravi & T. Anderson, November 2003

[12]. "Setting uo Netflow on Cisco Routers". MY-Technet.com date unknown. Retrieved 15 January 2011.

[13]. "Windows Home Server: Router Setup". Microsoft Technet 14 Aug 2010. Retrieved 15 January 2011.

[14]. "Windows Small Business Server 2008: Router Setup". Microsoft Technet Nov 2010. Retrieved 15 january 2011.

[15]. "Core Network Planning". Microsoft Technet May 28, 2009. Retrieved 15 January 2011.

[16]. Vinton Cerf, Robert Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on

Communications, Volume 22, Issue 5, May 1974, pp. 637 - 648.

[17]. David Boggs, John Shoch, Edward Taft, Robert Metcalfe, "Pup: An Internetwork Architecture", IEEE Transactions on Communications, Volume 28, Issue 4, April 1980, pp. 612- 624.