A MODEL ENTERPRISE NETWORK USING VLAN AND VTP

Sivakumar S[1], Vinod Kumar P P[2]

[1]*M-Tech (Network Computing), School of Engineering ,CUSAT*
siva17191@gmail.com
[2]*Associate Professor, Division of Computer Engineering, School of Engineering ,CUSAT*
ppvinod@gmail.com

Abstract

Enterprise network is built by organization to interconnect its various departments such as Production, Marketing accounts in order to share computer resources. Sometimes the Various segments of an enterprise network is needed to be isolated depending on the nature of the organization. Virtual LAN (VLAN) is an eminent solution for this problem .VLANS help to logically divide a physically divided networks and keep isolated from each other. VLANs help to improve the scalability and flexibility at various layers of network. VLANs are now becoming more popular due their easiness of use. But the administration of networks in which VLAN is implemented is usually found to be complex. Our paper focused on the use of VLANs in the network and How VTP reduces the administrative work on VLANs and different challenges and issues of VLAN and VTP such as insertion of rouge switch .This paper is based on configuration of Cisco switches and routers.

Keywords: *Virtual LAN, VLAN Trunking Protocol, VTP pruning, Configuration Revision Number*

----------***----------

1. INTRODUCTION

Need for VLANs and VTP

An Organization may need some of their departments to be isolated from each other whereas some may have to be interconnected with each other. Besides this changes in configuration are frequent because of changes that occur in the departments such as the addition of new hosts , changes in organizational policies etc.[5]. These requirements are often challenges to administrators .In this paper we strongly focus on VTP(VLAN Trunking Protocol), Cisco proprietary protocol which reduces the administrative work in VLANs[4] and its various security issues and countermeasures. Using VTP we can have a centralized system for configuration changes, so that other switches will automatically update the same. Thus VTP reduces the network configuration inconsistencies such as duplication of VLAN names to a great extent.[16]

VLAN Architecture, Configuration and Simulation

We simulated a network consisting of 6 switches and 28 hosts in ring topology using cisco packet tracer . After that we created a 3 VLANs production marketing and guest .after configuring the network a network we verified the isolation between two vlans.

In next part we configured VTP to reduce the administrative work by configuring four of the switches as VTP server and remaining as client .VTP server switches automatically updates the network changes to all connected client switches. Default mode of cisco switch is VTP Server mode.

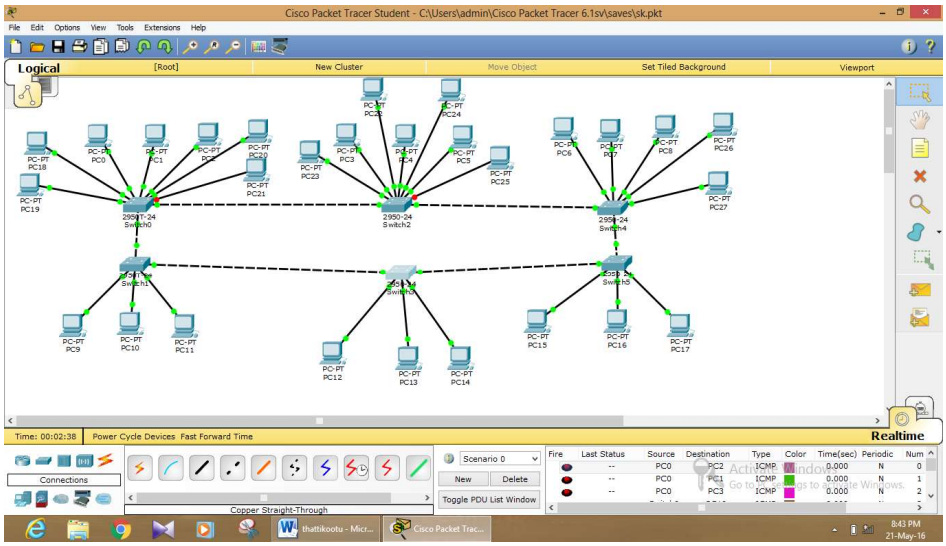

Figure1- Sample enterprise network created with 28 nodes

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
up


sw6>en
sw6#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   production                       active    Fa0/1, Fa0/2, Fa0/3
15   guest                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
15   enet  100015     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

Figure 2- Command line interface(CLI) of switch 6

VLAN Security Issues

VLANs and VTP has many advantages in enterprise networks but they still have some areas of concerns in network security such as redirection of packets to another VLAN[15]. The following sections discuss about such scenarios

Insertion of a Foreign Client Switch

If an attacker inserts a foreign switch having a configuration revision number higher than the server switch ,entire network will be affected as the whole VLAN database gets deleted. This is because the inserted switch , which has higher configuration revision number sends summary updates to all other switches resulting in the deletion and or addition of unwanted VLANs.[4]Then we shall need to reconfigure the entire network but the network would be in a vulnerable state untill the reconfiguration is completed. So it is always better to configure either a VTP password or VACL on server switches which will restrict unwanted traffic .Figure 3 shows a rogue switch in network

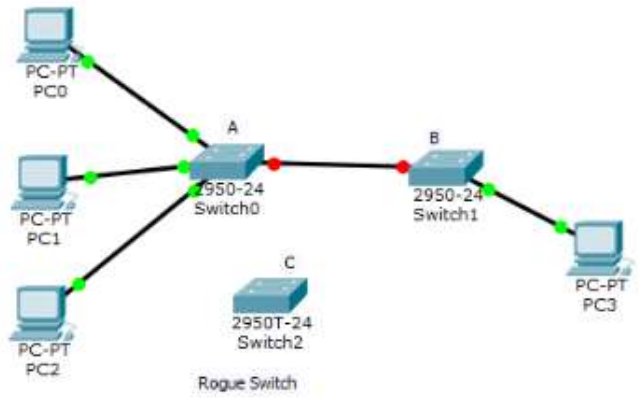

Figure 3

Creation of Unnecessary Traffic

VTP summary advertisements in VTP may sometimes cause unnecessary traffic. if VTP is enabled it makes sure that all switches in the VTP domain knows about VLANs in their domain. However, once in a while VTP can make superfluous traffic. In the event that an obscure unicasts and shows happens it is overwhelmed over the whole VLAN. Every switch will receive the message , irrespective of number of users connected in that VLAN.A solution is enabling VTP Pruning .But still it has limitations. Making changes in the VTP pruning will not the domain. Also it takes some time to become effective after we enable pruning in the domain. We cannot configure pruning for default , extended and reserved VLANs

CONCLUSION

The primary objective of this paper is to show how VLANs can be in enterprise networks. But the management of network becomes complex as the number of switches and the frequency of changes increases .For this VTP is an excellent solution. Yet, VTP has some issues, for example, it can't counter the impact of inserting a foreign switch with higher configuration number to the network . But these disadvantages can be overcome by some intelligent configuration by network administrators.

Another disadvantage is that VTP summary advertisements causes unnecessary traffic in the network. By enabling VTP pruning we limit the traffic to a certain extend . A scheduled algorithm can be applied in networks consisting of more than one server switch so that for only one of them advertises VTP messages in network at a time thus limiting the network traffic.

REFERENCES

[1] Milan Yu and Jennifer Rexford, Princeton University,Xin Sunand Sanjay Rao, Purdue University, Nick Feamster, Georgiainstitute of Technology. "A survey of Virtual LAN Usage inCampus Networks"IEEE Paper in IEEE Communications
Magazine" July 2011.
[2] Yu-Wei Eric Sung, Sanjay G. Rao, Geoffrey G. Xie,David AMaltz, Purdue University."Towards systematic Design ofEnterprise network"IEEE paper 2011.
[3] Kolbuchi M, Otsuka T, kudoh T, amano H. "A switch-taggedrouting methodology for PC clusters withVLAN Ethernet"IEEE Paper 2011.
[4] Johal, Hatinder Singh. "Access list based VLAN Maparchitecture & modified 802.1q frame scheme for addressingVTP issues." IEEE paper 2010.
[5] Xin Sun, Yu-Wei E Sung, Sunil D. Krothpalli, and SanjayG.Rao, Purdue University."A systematic Approach for evolvingVLAN Designs" IEEE paper 2010.
[6] Gobjuka, H. "Topology discovery for virtual local area" IEEEpaper 2010.
[7] Yamasak, Y, Miyamoto, Y, Yamoto, J, Goto, H, Sone, H."Flexible access management system for campus VLANbased on open-flow" IEEE paper 2011.
[8] Hirotsu T, Fukuda K, Abe H, Kurihara S, Akashi O,Sugawara T. "Dynamic & distributed routing control forvirtualized local area network" IEEE paper 2010.
[9] M casado, T. Garfinkel, A. Akella, M. Freedman, D. Boneh,N. Mckeron, and S. Shenker. SANE: A protection architecturefor enterprise networks. In Proc USENIX security, 2006.
[10] Maltz, G. Xie, J. Zhan, H. Zhang, G. Hjalmtysson,and A.Greenbug. Routing design in operational networks: A lookfrom inside. In Proc. ACM SIGCOMM, 2004.
[11] IEEE standard 802.1Q-2003. "Virtual Bridged LocalAreaNetworks".Technical report ISBN 0-7381-3662-X.
[12] Cisco, "Catalyst Family of LAN Switching" CLVco systemInc. product information, 1998.
[13] Garrett Leischner and codyTews, Security Through VLANsegmentation: Isolating and Securing Critical Assets WithoutLoss of Usability. Schweitzer engineering Laboratories, Inc.SEL 2007 TP6277-01.
[14]http://cisco.com/univered/cc/td/doc/product/lan/28201900/1928v8x/eescg8x/aleakyv.htm.
[15]"Secure use of VLANs": An@stake security assessment http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf.
[16]"UnderstandingVTP"http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_25_see/configuration/guide/swvtp.pdf.
[17]"Inter VLAN routing-Routing between VLAN Networks" http://www.firewall.cx/networking-topics/vlannetworks/222-intervlan-routing.html
[18] "VLAN Hopping Attack And Mitigation/Prevention": http://lonetsec.blogspot.in/2011/02/vlan-hoppingattacks