Effective Remote Management for Inter-VLAN Routing Networks

Rajiv O. Verma
Asst. Professor, Guru Nanak Institute of Engineering & Technology, Nagpur.
rajiv_verma44@hotmail.com

ABSTRACT
VLANs are extensively used in enterprise network to ease management of hosts to improve scalability and flexibility. Despite their wide usage in enterprise network, VLAN security is a greater concern for the network administrator due to very little attention has been paid on error prone, unsystematic, high risk of misconfiguration in the design and management of enterprise VLAN network [20]. This paper extends the consideration of how to handle remote access to VLAN switches. We have shown the management of VLAN switches from remote location by using protocols such as telnet, SSH, etc. We proposed effective ways to restrict access to management functions from remote sources. We have used access-control-lists to filter the traffic of inter-VLAN routing as well as to restrict remote access to VLAN switches designed in VTP model. Unless otherwise stated this paper is based upon configuration & hardware implementation in a Cisco environment. We demonstrate the security optimization techniques in designing VLAN both for Inter-VLAN communication and addressing VTP issues.

Keywords-- VLAN; VTP; DTP; SSH; ACL

1. INTRODUCTION
Today’s enterprise network is undergoing a stringent complexity due to frequent change in design of their networks for new organizational needs. Configuration changes are required due to movement of departments and user, addition of new hosts, revision of security policies, company mergers and malicious intruders. The frequency and complexity of configuration changes results in error-prone enterprise networks [5]. However, yet these challenges in enterprise network have received little attention from the research community. One prominent example is VLAN design which is extensively used in enterprise networks[2].VLAN’s were initially intended to connect a group of hosts in the same broadcast domain, independent of their physical location. The expectation for today’s VLAN has increases due to better security, flexibility and scalability requirements [1]. CISCO’s VLAN trunking protocol reduces administration in a switched network [4]. VTP has some issues but not much research has been done for complexities arise in VTP based configuration. In this paper, we focus strongly on various security aspects of VLAN design using with VTP to reduce the much administrative work apart from optimal Inter-VLAN routing design. We proposed various security aspects like access-lists based layer 3 securities in Inter-VLAN routing, deactivating native VLAN1 to secure Layer 2 traffic in VTP model, application of authentication on VTP server and nonnegotiating Dynamic Trunking Protocol mode to counter the effect of inserting a rogue switch/trunk with higher config revision number [20]. Cisco Catalyst switches can provide a remote administration and management interface into the switch which can be configured with an IP address. These management interfaces are referred to as in-band management interfaces because they are attached to and can be accessed from the data network.
2. INTER-VLAN ROUTING

In this section a simulated VLAN design is used using VLAN Trunking protocol (VTP) to fulfill our objective to reduce the much administrative work with less costing. In the first part we have configure the VTP model by interconnecting four switches such that one acts as VTP Server and the other three are clients. VTP server will automatically update the summary/subset advertisement to all the connected clients. In the second part we have connected a router with single interface with the VTP Server switch to simulate inter-VLAN Routing.

<table>
<thead>
<tr>
<th>Table I. Interface ports for Network in Figure 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTER0</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>A</td>
</tr>
<tr>
<td>PC1</td>
</tr>
<tr>
<td>PC2</td>
</tr>
<tr>
<td>PC3</td>
</tr>
<tr>
<td>PC0</td>
</tr>
<tr>
<td>ROUTER1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table II. IP Address Allocation in Figure 1.</th>
</tr>
</thead>
</table>

Organized By: GNI Nagpur, India
VLAN’s allow you to isolate users from each other by placing them in different VLAN’s but how do you pass traffic from one VLAN to another VLAN? Doing so involves the use of Layer 3 device to route the traffic from one VLAN to another [10]. The best way is to use a router for inter-VLAN communication. In traditional method, each of the router interfaces is connected to an access links that in turn is connected to hosts. Such design requires 3 physical interfaces for three VLAN’s (as per our example). In our proposed method, router interface is not connected to an access links; instead the router fast Ethernet interface is connected to the VTP server switch interface and configured with ISL or 802.1q trunking. The benefit of using a trunk link is to reduce the number of router and switch interfaces used. A single trunk link saves the cost and minimizes configuration complexity. One fast Ethernet interface f0/0 is divided into three sub-interfaces and VLAN encapsulation is defined for each sub-interface. The configuration of sub-interfaces is shown below:

```
Router#show run
interface FastEthernet0/0
   no ip address
duplex full
   speed 100

   interface FastEthernet0/0.1
      encapsulation dot1Q 10
      ip address 192.168.1.254 255.255.255.0

   interface FastEthernet0/0.2
      encapsulation dot1Q 11
      ip address 192.168.2.254 255.255.255.0

   interface FastEthernet0/0.3
      encapsulation dot1Q 12
      ip address 192.168.3.254 255.255.255.0

```

### 2.1 Remote Management of VLAN

The remote connectivity can be done by using any routing protocols from static or dynamic. In our paper we use static routing protocol. We have configured telnet port vty along with other required authentication. Your management VLAN does not have to be the same as your Native VLAN. Matter of fact, it is good practice to make sure that they are different. Your management VLAN should only carry in-band management traffic and should not be the default VLAN. We have specified an ip address to vlan 10 & make sure that they are not shutdown. Also specify ip default gateway to router0 in the server switch. The configuration of server switch A for telnet support is given below:

![Diagram of network layout](image-url)
interface Vlan10
  ip address 192.168.1.10 255.255.255.0
!
  ip default-gateway 192.168.1.254
!
  line con 0
    password 7 08224340
    login
!
  line vty 0 4
    password 7 08375857
    login
line vty 5 15
  password 7 08375857
  login
!
end

2.2 Access-List Based Inter-VLAN Communication

ACL’s are used to secure and control traffic into or out of networks. In modern implementations, central file servers and services are usually placed in their own isolated VLAN, securing them from possible network attacks while controlling access to them. An administrator can smartly disable ICMP echoes and other protocols used to detect a live host, avoiding possible detection by an attacker host located over a different VLAN [10]. After configuring ACL, router works as a firewall and checks each statement sequentially before forwarding the traffic to its destination. By using standard or extended access-lists, a router processes each ACL from top to bottom, one statement at a time. We propose extended ACL’s to filter the traffic between VLAN’s or between hosts of a VLAN. Also we can use standard ACL to restrict telnet access from the remote network. The configuration of ACL as per figure 1 on router0 is shown below:

access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 101 permit ip any any

To configure a more restrictive ACL, create permit entries and omit the permit any entry at the end of the standard ACL.
access-list 15 permit host 192.168.4.1 209.157.22.32
access-list 15 permit 192.168.4.0 0 0.0.0.255
telnet access-group 15

3. SECURITY FOR VLAN HOPPING ATTACK

VLAN hopping attack allows a user on a VLAN to unauthorized access to another VLAN. This can be done by using a native VLAN1 (default). Normally 802.1q trunking does not tag frames for native VLAN. An attacker can connect a rogue switch/trunk to an unused port & spoofs DTP messages to automatically negotiate and thus turn on trunking between the rogue switch and the target switch. An attacker can also send a double-tagging 802.1q frame to access the victim switch. The outer header has the VLAN tag of the attacker, which is the same as the native VLAN of the trunk port. To mitigate this type of attack the best approach is to ensure that the native VLAN of the trunk ports is different from the native VLAN of the other ports. In our proposed model we have changed the native VLAN to VLAN 90; we have disallowed VLAN 1 from the trunk ports and keep the desired VLANs allowed. Also we proposed that either disable the remaining ports or change them to access ports in non-negotiate mode. Set nonnegotiate mode on both side of the trunk. From figure 2, PC5 is an attacker which is connected to VTP client 1 switch, and trunk port F0/1 is connected to VTP server switch.
4. CONCLUSION

The security of VLAN technology is reliable and robust. The problem arises only due to user misconfiguration or improper use of features. In this paper our primary contribution is to show the security measures arise due to Inter-VLAN communication both locally and remotely, and issues in using VTP in an enterprise network. Solutions proposed to secure Inter-VLAN communication and to address VTP issues are brought into practice using simulated network configuration. We proposed access-list based security on layer 3 to prevent unauthorized access to different VLANs. We proposed security solutions emerges due to VLAN hopping attacks by deactivating the native VLAN1 which is the root cause of such type of attacks. For secured remote administration the management VLAN should not have to be same as your Native VLAN or default VLAN 1.

REFERENCES


**AUTHOR’S PROFILE**

A. Rajiv O. Verma

The author Rajiv O. Verma is born in Gorakhpur (UP), India on 11th of November,1967. He has done Bachelor of Engineering in Electronics Engineering from Yeshwantrao Chavan College of Engineering at Nagpur, Maharashtra, India, in the year 1990. Currently he is a student of Mech in Communication & working as an Asst. Professor in Guru Nanak Institute og Engineering & Technology, Nagpur, India.. Computer Communication Network is the author’s major field of study.