International Journal of Modern Achievement in Science, Engineering and Technology (IJSET)
ISSN 3023-459X
DOI: 10.63053/ijset.52

Examining The VTP Protocol, Identifying the Risks of Its Use and Providing Risk Reduction Solutions in The Computer Networks of Offices and Large Organizations

Mohammad Abbasi Rad[1]

1. Bachelor's student, Computer Engineering, Farabi School, University of Tehran, Iran

ARTICLE INFO

Keywords:
VTP Protocol, Cisco, Risk Reduction, Computer Networks

ABSTRACT

Today, one of the challenges of computer networks implemented in large offices and organizations is maintaining the stability and security of networks, as well as the ease and automation of their configuration to save the time and energy of network administrators. The VTP protocol is a tool to ease and reduce the burden of manually configuring changes to VLANs on Cisco switches. However, the use of this protocol, despite having advantages such as automatic configuration and centralized management of VLANs, has great risks such as the complexity of implementation in large networks and the loss of settings in case of wrong configuration. The problem studied in this article is to investigate the characteristics and function of this protocol and to recognize the possible risks and dangers associated with its use. In the following, solutions are provided to reduce these risks so that the benefits of this protocol can be used and at the same time protect the stability and security of the network implemented in the organization. By using this evaluation, network administrators can have an optimal and more informed use of this protocol.

Copyright: © 2024 by the author(s).

This article is an open-access article distributed under the terms and Conditions of the Creative Commons Attribution (CC BY 4.0) license.

Introduction

VTP or VLAN Trunking Protocol is a layer 2 protocol exclusive to Cisco. The main function of this protocol is the optimal and centralized management of VLANs. For example, in a network that has a large number of switches and VLANs implemented in it, and we also need to constantly apply changes such as deletion, addition, or name change to these created VLANs; VTP protocol can be used; By applying the desired changes to one switch and these changes are automatically applied to the rest of the switches. For example, we may have 30 switches in the corporate network and need to add a new VLAN. Normally, we should SSH to all these switches and create a new VLAN on them; But using VTP, this is done manually on one switch and automatically on other switches. This protocol is enabled by default on Cisco switches and does not require manual activation. Only users should configure it according to their needs.

VTP Advertising

The packets sent by this protocol are sent on ports working in trunk mode; For this reason, in order to use this protocol, we must set the links on which VTP packets need to be sent and received in Trunk mode.

VTP packets are sent under the title of VTP Advertisement. These packets are sent as multicast. Also, by default, packets are sent every 5 minutes and when a change is made in VLANs.

Switches notice changes in VLANs through a number called Revision Number. This number is zero at the beginning and whenever a change is made in the discussion of VLANs, one unit is added to this number. Inside the VTP Advertisement packets, there is this Revision Number, and when every switch receives this packet, it compares this number with its own Revision Number, and if it is bigger, it realizes that there has been a change in VLANs, while it has not received that change. , thereby deleting its entire VLAN database and obtaining a new database from that switch.

VTP Advertisement packets are sent as VTP Summary, VTP Subset and VTP Request packets. In VTP Summary packets, there is a series of general information such as Revision Number, VTP Domain and VTP Version. When a switch receives the VTP Summary packet, it compares the Revision Number inside the packet with its own Revision Number, and if its Revision Number is lower, it sends a VTP Request packet and requests the switch to update its database information. to provide The database information of that switch reaches the source switch under the title of VTP Subset packets, and in this way, the databases of the switches in the network are matched with each other.

VTP Domain

To use the VTP protocol, one of the settings that must be done is creating a VTP Domain. VTP Domain is a name that must be created for management. In the switches that we want to have VTP communication with each other, we must create the same name so that their domains are also the same. The switches located in the same domain match their VLAN database and the changes related to their VLANs are sent and received between them by the VTP protocol. For example, in Figure 1, an example of a VTP Domain is presented.

In order for the switches to be placed in a VTP Domain, several rules must be followed. First, the domain name of all switches must be the same. Then, it is necessary to have trunk ports in the network so that VTP packets can be advertised in the network. Finally, if we use a password, we need to use the same password for the switches

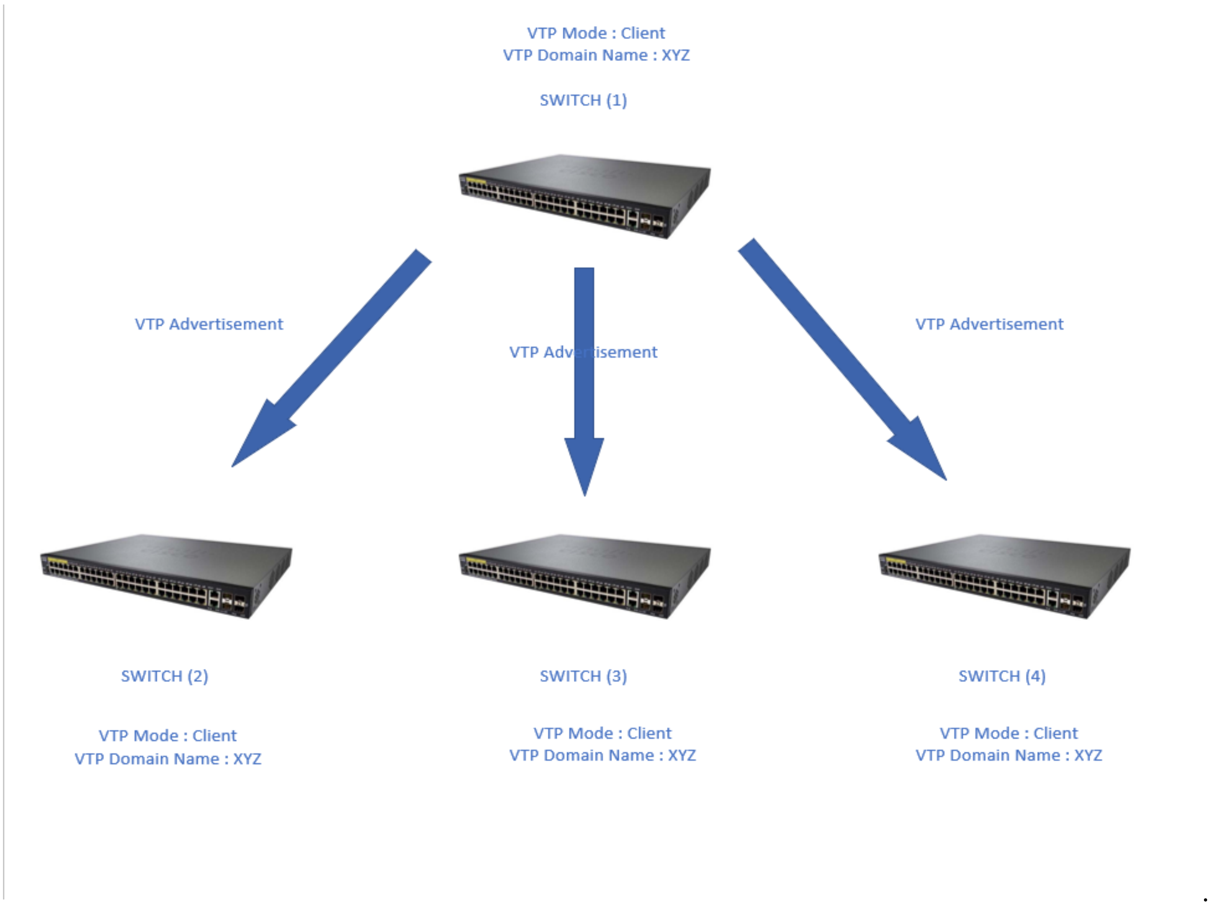


Figure 1 - An example of a VTP Domain

VTP Modes

The switches on which the VTP protocol is configured can work in four modes: Server, Client, Transparent and Off. By default, the mode of all switches is Server. In a switch whose mode is Server, all possible changes can be applied to VLANs. For example, delete, create, rename, etc. Also, a switch with this mode can send VTP Advertisement packets every 5 minutes and also when there is a change in VLANs.

In the switch whose mode is Client, no changes are allowed on VLANs and only this switch can receive changes from the switch which has Server mode and update its database using the received information. A switch in Client mode sends VTP Advertisement packets; But only every 5 minutes.

In transparent mode, the VLAN database is local. In this mode, any changes can be made on VLANs and this switch will not announce the changes to other switches. In fact, this switch has nothing to do with the changes reached by VTP and does not consider those changes.

In the Off mode, VTP is completely disabled. The difference between this mode and Transparent is that in Transparent mode, the switch is inside the VTP Domain and passes VTP Advertisement packets; It somehow forwards these packets; because it is possible that these switches are in the way of other switches; But switches in the Off mode don't even pass VTP Advertisement anymore.

VTP Versions

VTP has different versions. Its first version is also called the classic version, which dates back to the 90s. By default, this version is active on the switches, and if we want to use higher versions, we must activate that version with the command. In the first version, if we put a switch in Transparent mode, that switch checks the specifications of VTP Advertisement packets and passes this packet if its domain name and version are the same as its specifications.

In the second version, these switches do not check the specifications of the VTP Advertisement packet and pass the packets without checking it. Also, in the second version, Token Ring networks are also supported.

In the third version, Extended VLAN and Private VLAN are supported. This version has a better authentication mechanism. It also has a mechanism called Primary and Secondary Server. In this mechanism, one switch is selected as Primary Server and other switches that are in Server mode are placed as Secondary Server. In this situation, only the Primary Server is allowed to make changes to VLANs. When the third version is activated on the switches of an organization, even if only one switch is in Server mode, the VTP Primary VLAN command must be applied to this switch so that VTP starts working. In this version, VTP can also be enabled or disabled per-port. In fact, we can determine the ports we want to send and receive VTP packets; Not on all trunk ports.

VTP Pruning Another feature that this protocol provides to users is VTP Pruning. With this feature, we can have better control over Broadcast traffic and avoid unnecessary Broadcast traffic. For example, in Figure 2, client number 2 sends a Broadcast traffic in the network, and the switches in the network also send it on all their ports after receiving the traffic; But it is possible that there is no desired VLAN behind this trunk port on which the Broadcast packet is sent, and unnecessary traffic is created in the network and unnecessary processing is done on the devices. But if VTP Pruning is used, the switches check their trunk ports to find out which VLANs are reached through these trunk ports and only send the Broadcast packet on the ports that reach the desired VLAN. For example, in Figure 2, when Switch 3 checks and sees that VLAN 10 is being reached from only the port connected to Switch 1, it will no longer forward this packet on the port connected to Switch 5, and In this way, unnecessary traffic in the network is prevented.

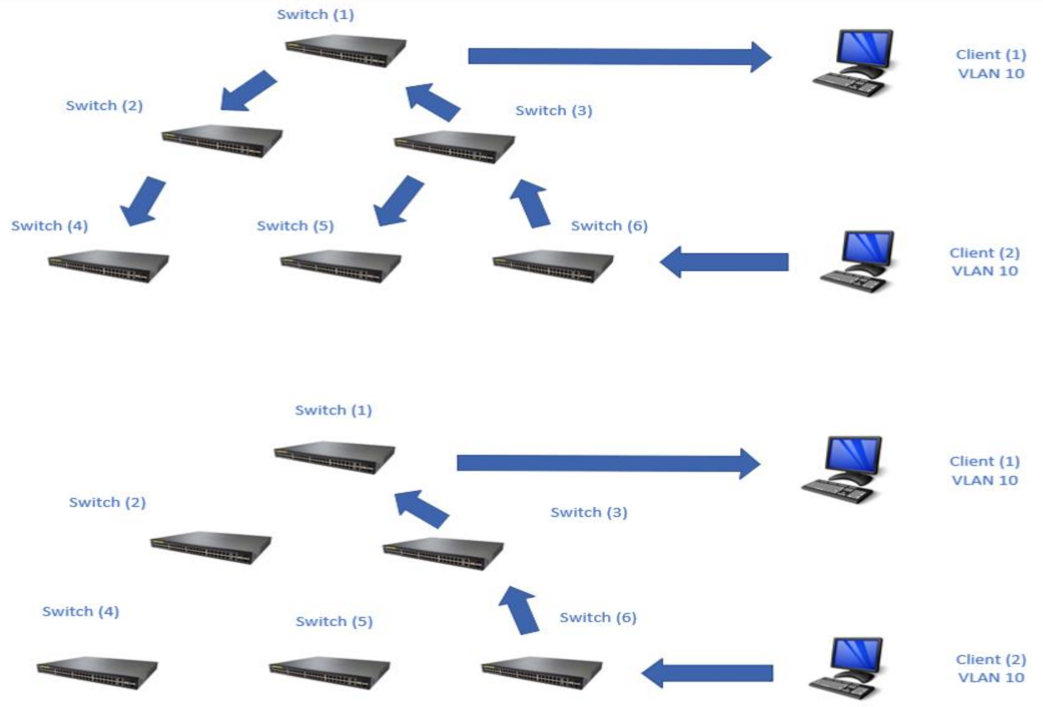


Figure 2 - An example of how the VTP Pruning feature works

VTP protocol configuration

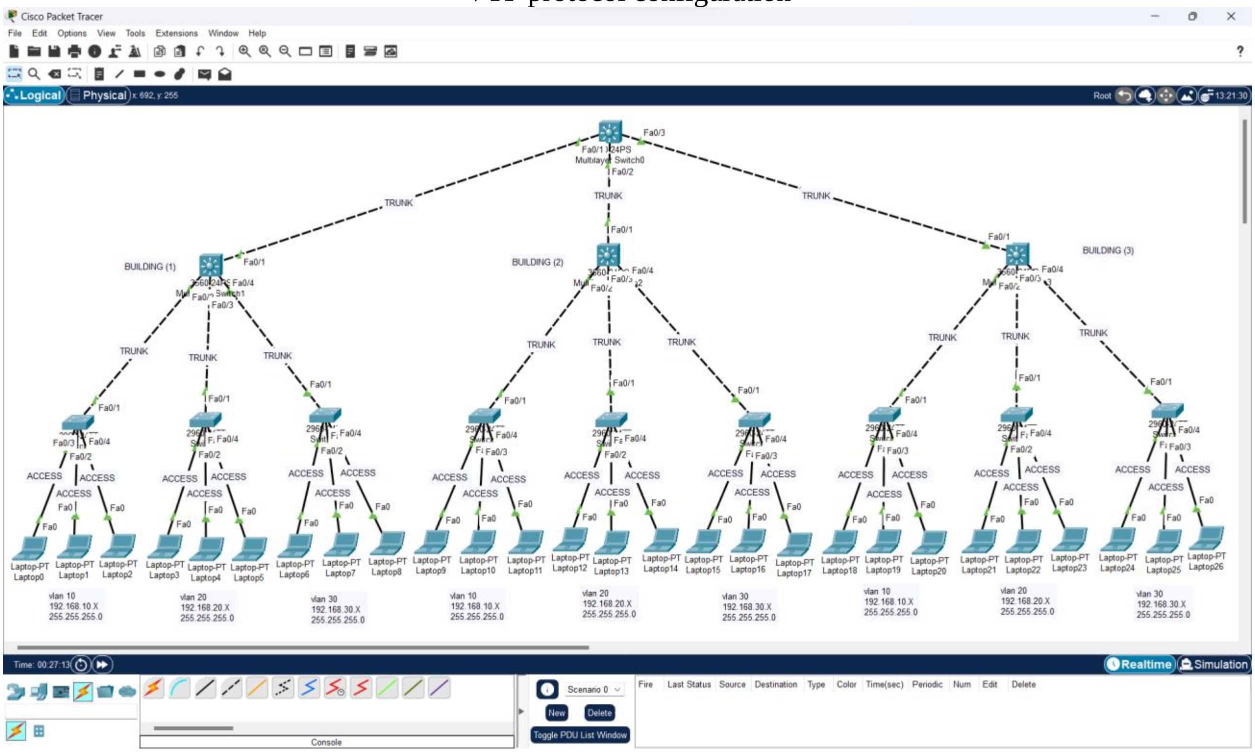
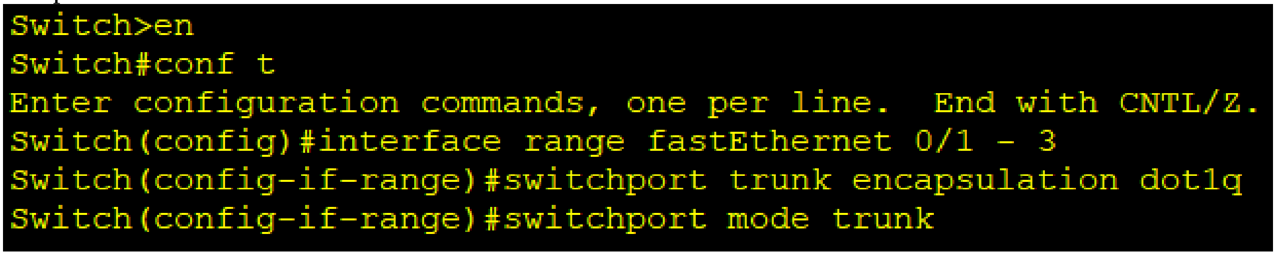


Figure 3 - An example of an organization's network

For example, Figure 3 is an example of an organization with 3 office buildings, in each building, there is a 3560 switch as a Distribution layer switch and three 2960 switches as an Access layer switch. The distribution switches of each building are connected to the Core layer switch in the server room. VTP protocol packets are sent on trunk ports; So the communication links between the switches must be of the Trunk type so that the changes applied to the VLANs can reach other switches in the network through the VTP protocol. Also, the communication between Access layer switches and PCs must be of Access type.

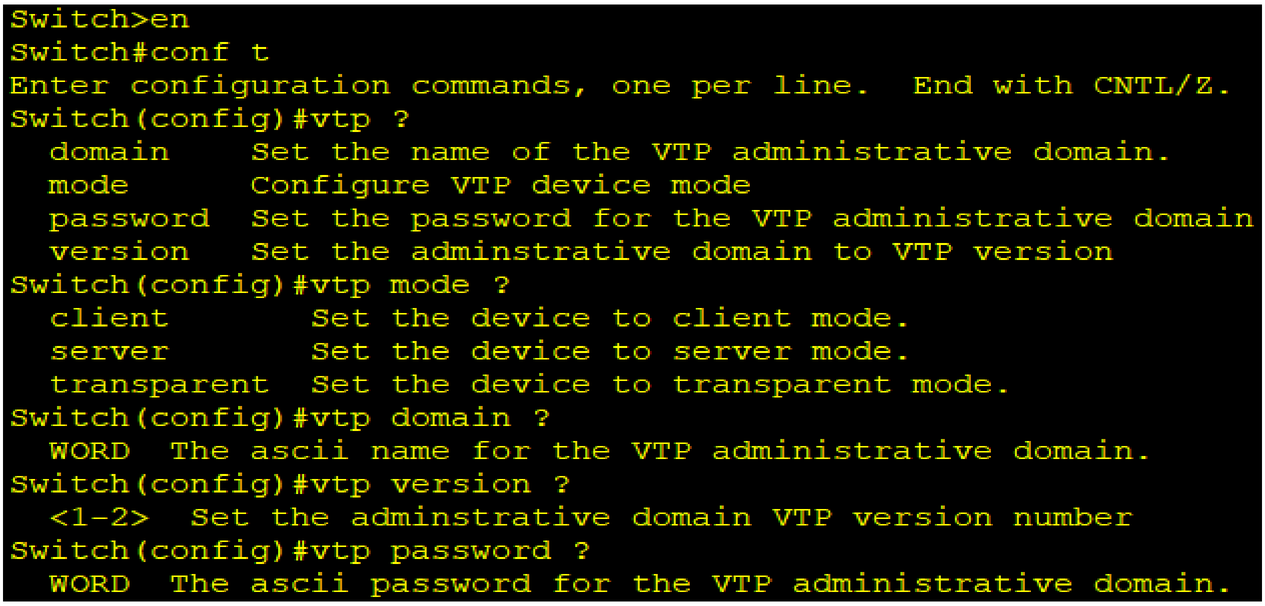
By means of the commands shown in Figure 4, we select the desired ports that are supposed to be Trunk and put it in Trunk mode.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1 - 3
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
```

Figure 4 - Trunk ports configuration commands

After trunking the desired ports, we need to configure the VTP protocol. To configure this protocol, we must enter the commands shown in Figure 5 in the Global Configuration environment of all the organization's switches.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
Switch(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
Switch(config)#vtp domain ?
  WORD  The ascii name for the VTP administrative domain.
Switch(config)#vtp version ?
  <1-2>  Set the adminstrative domain VTP version number
Switch(config)#vtp password ?
  WORD  The ascii password for the VTP administrative domain.
```

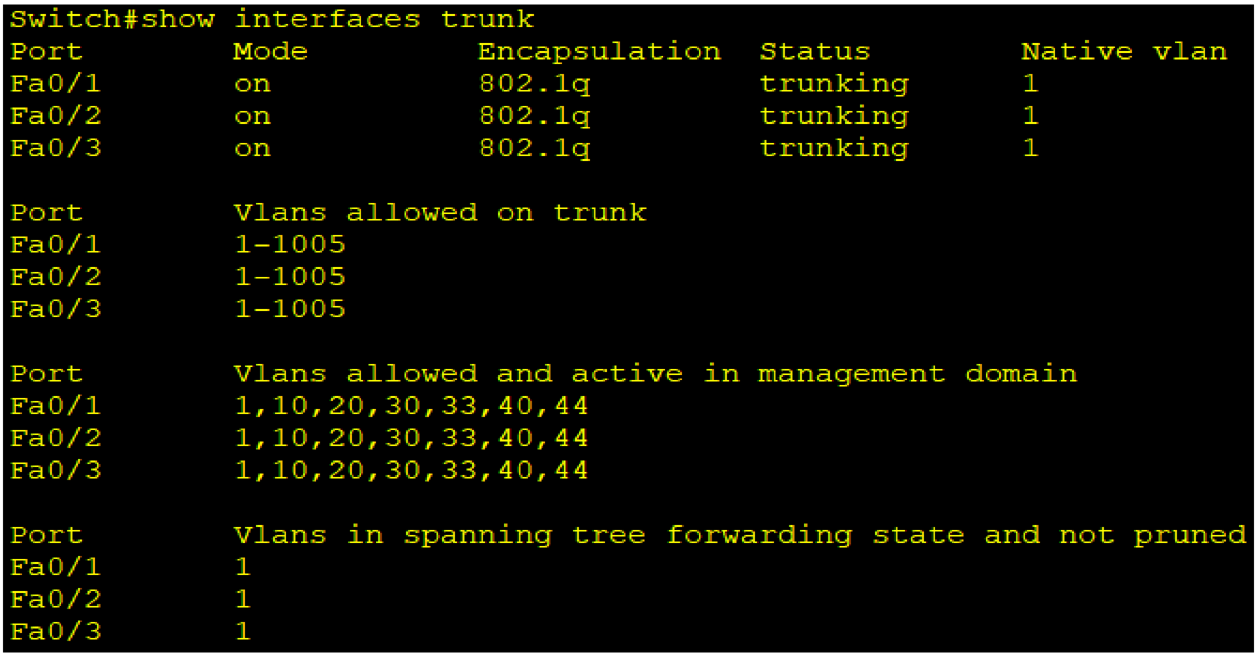
Figure 5 - VTP protocol configuration commands

With the VTP Mode command, we can determine how this switch works in VTP. This mode can include Server, Client and Transparent modes. Also, if our VTP version is 3, we can use the Off mode. With the VTP Domain command, we can assign a name as a domain for VTP so that switches with the same domain name can match their VLAN database. With the VTP Version command, we can determine the VTP version in the desired switch. With the VTP Password command, we can set a password for VTP.

To activate the Pruning function, the VTP pruning command must be entered in the Global Configuration environment.

In order to make only one of several switches working in Server mode as Primary and the other switches as Secondary, the VTP primary VLAN command must be entered in the Privileged EXEC environment of the Primary switch.

Using the two commands shown in Figures 6 and 7, we can get a report of the current status of the trunked ports and the VTP status.

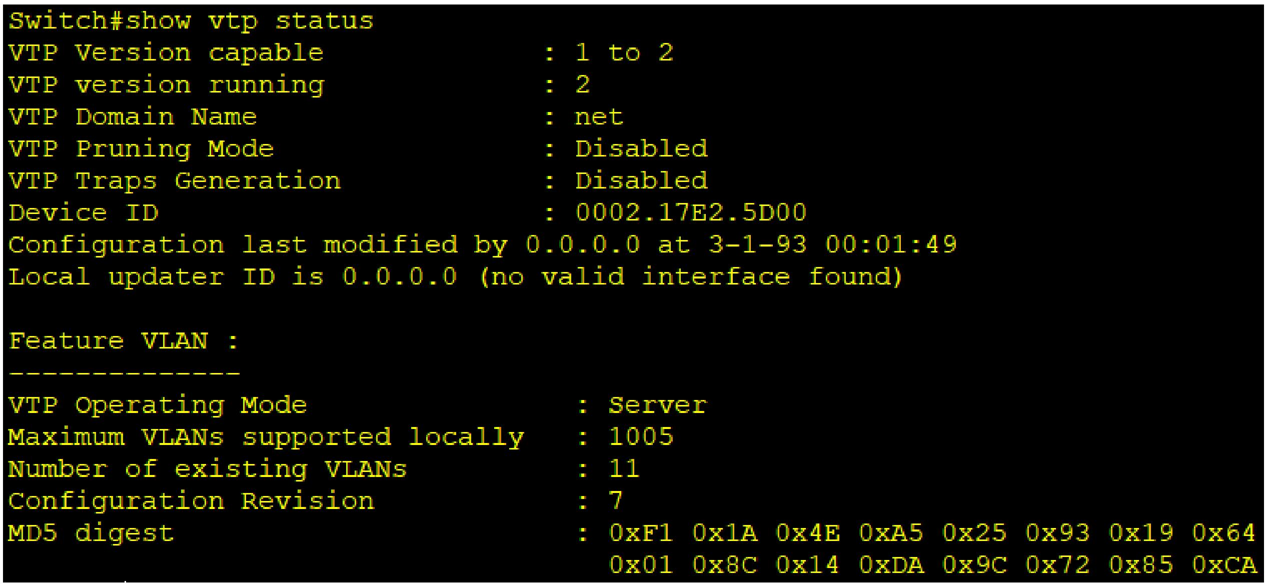


```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,33,40,44
Fa0/2       1,10,20,30,33,40,44
Fa0/3       1,10,20,30,33,40,44

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/2       1
Fa0/3       1
```

Figure 6 - Trunk port reporting command

In the report of this command, the trunk port numbers are specified. Other specifications such as Encapsulation, Native VLAN number and VLANs that are allowed to pass through these trunked ports are also displayed. One of the problems that cause errors in VTP is wrong settings on trunk ports

.



```
Switch#show vtp status
VTP Version capable               : 1 to 2
VTP version running               : 2
VTP Domain Name                   : net
VTP Pruning Mode                  : Disabled
VTP Traps Generation              : Disabled
Device ID                         : 0002.17E2.5D00
Configuration last modified by 0.0.0.0 at 3-1-93 00:01:49
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                  : Server
Maximum VLANs supported locally     : 1005
Number of existing VLANs            : 11
Configuration Revision              : 7
MD5 digest                          : 0xF1 0x1A 0x4E 0xA5 0x25 0x93 0x19 0x64
                                      0x01 0x8C 0x14 0xDA 0x9C 0x72 0x85 0xCA
```

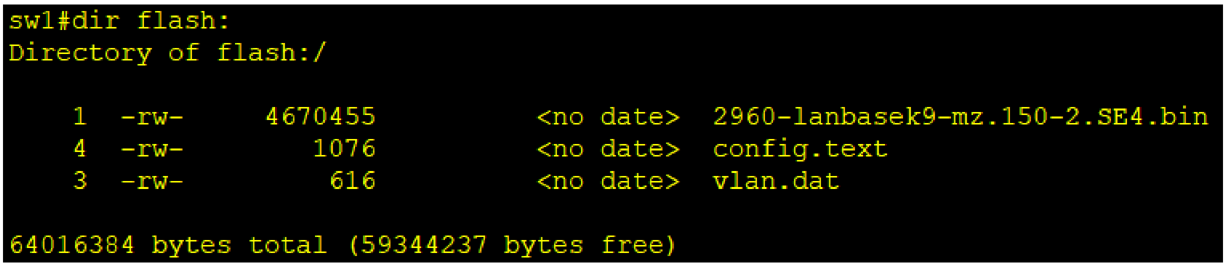
Figure 7 - VTP status reporting command

In the output of this command, a report of the current state of VTP is displayed. Things like the version that VTP is using now, the domain name that has been assigned, whether the VTP Pruning feature is active or inactive, the working mode of this switch, and also the Revision Number. To check the VTP status, the command in Figure 7 is very useful.

The findings

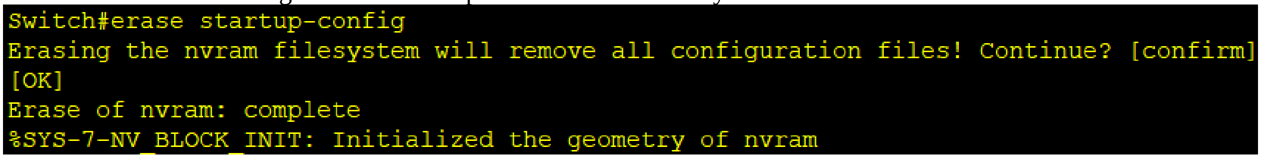
As mentioned, the use of VTP protocol in large networks such as organizations and offices with a large number of switches and problem management provides good management benefits to users; But it brings risks, any of which, if neglected, can lead to the failure of the entire network.

For example, one of the most important risks that happens more often is connecting a switch that has already been used in a network and has been added to the network without erasing the previous settings. If by mistake or intentionally by an attacker, this switch is connected to the implemented network and has a higher revision number than the switches that currently exist in the network; This switch sends VTP Advertisement inside the network and the switches adjust their VLAN database with it. As a result, VLANs that already exist in the network may be removed, and VLANs that exist in the connected switch may be applied to the network and disable the network. To avoid this problem, before connecting a new switch to the network, we must reset its revision number so that its number becomes zero, and then apply VTP settings and connect it to the network. Resetting this number can be done in two ways. We can change the Domain Name of the switch or put the switch in Transparent mode. By applying any of these tasks, the Revision Number becomes zero. We can also remove the entire VLAN and VTP settings to be more secure. The settings related to these two are stored in a separate file of Startup-Config.txt, which is related to saving the settings, in the Flash memory of the switches. The name of this file is Vlan.dat. This mistake has happened a lot that the network administrator has simply deleted the configuration file and connected the switch to the network to connect the new switch to the network, and since the VLAN and VTP settings are in a separate file, it has caused a failure in the network. Is



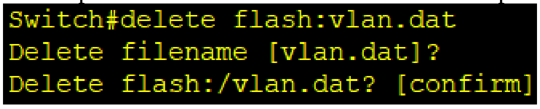
```
sw1#dir flash:
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin
    4  -rw-        1076          <no date>  config.text
    3  -rw-         616          <no date>  vlan.dat

64016384 bytes total (59344237 bytes free)
```

Figure 8 - An example of the Flash memory contents of a 2960 switch



```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

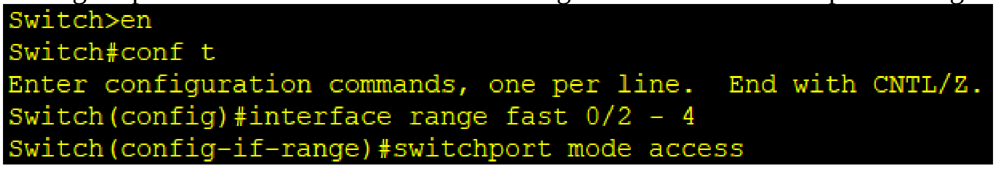
Figure 9 - An example of the command to delete the Startup-Config.txt file



```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
```

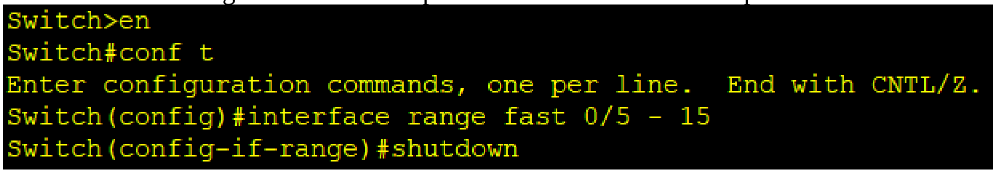
Figure 10 - An example of the command to delete the Vlan.dat file

Also, so that the Attacker cannot connect to the network switches physically or by using communication protocols, arrangements must be made. To prevent physical access, the switches should be stored in locked racks, and the room where the racks are located should also have the necessary security. For example, the room must be unlocked with a password and fingerprint, and the room must have a CCTV camera. Only the network administrators and their assistants should be allowed to enter the room and open the racks, and it is necessary to completely prevent the access of unauthorized people. Also, for more certainty, the unused ports of the switch must be in Shutdown mode so that even if the attacker gains access to the switches and connects his switch to the empty ports, the attack will be prevented due to the shutdown of the port. Also, the ports connected to PCs must be in Access mode, so that even if the attacker disconnects the cable connected to the PC from the switch and connects his switch, the attack will still be prevented. Also, the working mode of the switch ports connected to the PC should not be left without manual configuration; Because switch ports are in Dynamic Auto mode by default, and when they are connected to the PC, they are in Access mode because the PC is passive. Now, if the attacker puts a port of his switch manually in one of the Trunk or Dynamic Desirable modes and the administrator has not manually set the switch ports connected to the PC in Access mode, the port will be in Trunk mode and It causes the entire network of the organization to fail. For this purpose, the switch ports that are supposed to be connected to the PC must be manually set to Access mode and the unused ports must be turned off. Also, the ports that are supposed to be Trunk and VTP packets are sent on it, must be configured manually to reduce the risk of using this protocol. An example of the command to manually configure ports in Access mode is shown in Figure 11 and to turn off ports in Figure 12.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fast 0/2 - 4
Switch(config-if-range)#switchport mode access
```

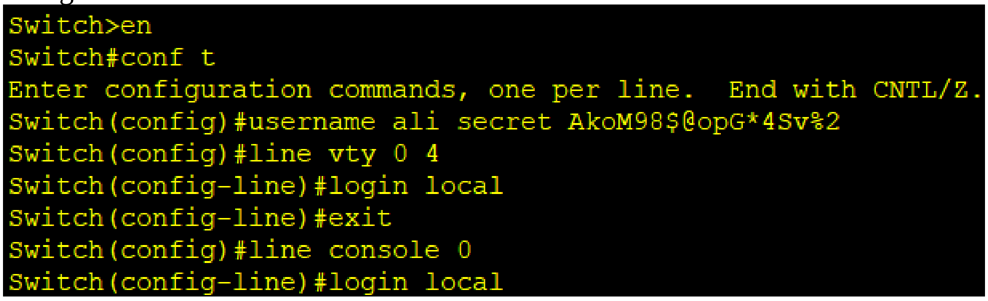
Figure 11 - An example of the command to access ports



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fast 0/5 - 15
Switch(config-if-range)#shutdown
```

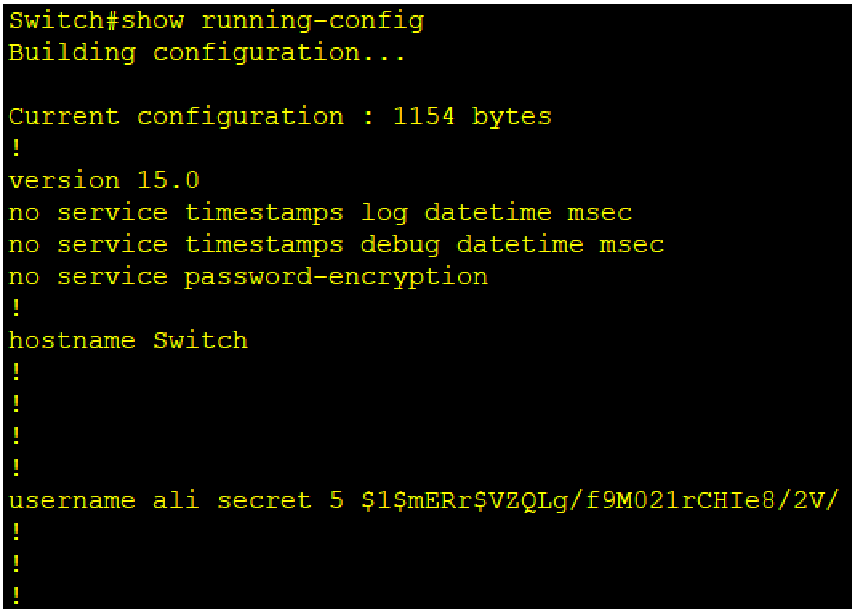
Figure 12 - An example of the command to disable ports

To prevent Remote Attacker access, some things must be observed. For example, never use Telnet protocol to communicate with switches; Because this protocol is Clear Text and does not encrypt data during sending and receiving. For this reason, there is a possibility of data eavesdropping, and the passwords related to Line Vty, which are used to configure communication protocols, may be provided to the eavesdropper. Now this person can connect to the switch that is in server mode and make changes in the database related to its VLANs. In this case, similar to before, these changes are advertised within the network and a failure is created in the organization's network; Therefore, the SSH protocol must be used for remote control so that the data is not intercepted. Also, for Line Vty, Login should not be only with a Password. It is better to use Username and Password instead. If the Service Password Encryption command is used along with the password, the password will be hashed with level 7 and stored in the settings; But if Secret is used instead of Password, Password with level 5 will be hashed and saved without using Service Password Encryption command. In this case, security increases. Its level 7 is easily cracked, But its level 5 has a better encryption algorithm; But it is still possible to crack it with software such as Cain & Abel. The password cracking operation is done using Dictionary and Brute-Force. In this way, the user enters the Hash along with his guess of the contents of the password. For example, it guesses that the password contains small and large English words along with numbers or only contains numbers and characters. Depending on the contents and number of characters of the password, more time should be spent to break the password. If a complex password is used, as shown in Figure 16, cracking the password may take several years. For example, AkoM98$@opG*4Sv%2 is a complex password. The best way to maintain security is to use Username and Secret to prevent the Attacker from connecting remotely or through the Console port. Password must be complex and have at least 10 characters. For more security, you can get the level 5 hash of the desired password in advance, and when configuring the switch, enter that hash along with its level, instead of the original password, so that if someone is in the room during the configuration, he won't notice the original password. For more security, instead of creating a password locally, you can create a password on a Radius or TACACS+ server. In this situation, the server is responsible for authenticating the connected person. If the mentioned items are not followed and the Attacker can access the Primary Server switch; It can disrupt the network by removing and creating VLANs. By complying with the mentioned conditions, the risk of unauthorized access can be greatly reduced. Forms 13, 14 and 15 are respectively examples of the necessary commands to configure the Password, the form of saving the Password in the settings and storing the Hash instead of the original Password.



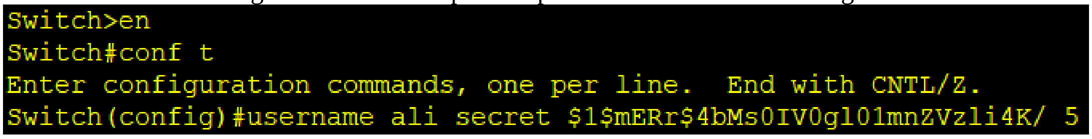
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username ali secret AkoM98$@opG*4Sv%2
Switch(config)#line vty 0 4
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#line console 0
Switch(config-line)#login local
```

Figure 13 - Example of Password configuration for Line VTY and Line Console



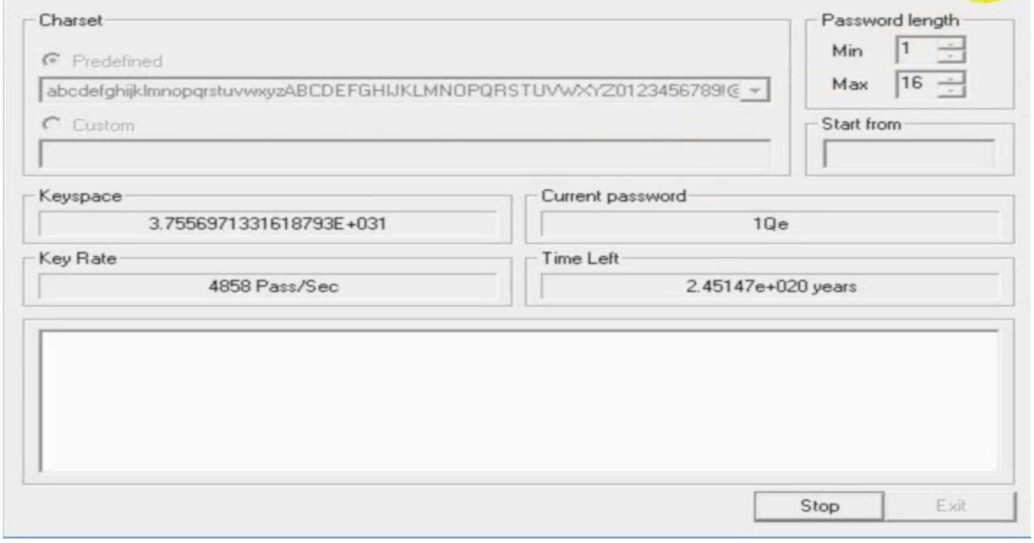
```
Switch#show running-config
Building configuration...

Current configuration : 1154 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
username ali secret 5 $1$mERr$VZQLg/f9M021rCHIe8/2V/
!
!
!
```

Figure 14 - An example of a password stored in the settings



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username ali secret $1$mERr$4bMs0IV0gl01mnZVzli4K/ 5
```

Figure 15 - An example of Hash storage instead of the original Password



Charset
○ Predefined
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@
○ Custom

Password length
Min 1
Max 16

Start from

Keyspace
3.7556971331618793E+031

Current password
1Qe

Key Rate
4858 Pass/Sec

Time Left
2.45147e+020 years

Figure 16 - An example of the amount of time needed to crack a Complex Password

Another way to reduce risk and increase security is to use the third version of VTP; Because we can choose only one switch as the Primary Server from among all the Server switches in the network, and only the Primary Server is allowed to change VLANs. In this case, even if the Attacker gains access to the Secondary Servers, he cannot change the network and the changes can only be applied from one point.

VTP Password can also be used to reduce the risk. In the case of using a password, even if a switch with a higher revision number is added to the domain, until the password is applied to that switch, it cannot be a member of the domain and receive or apply a change in the network.

Another risk is misconfiguration of this protocol in large networks. For example, when a Domain Name is created on a switch, this domain name is immediately applied to all switches that have a trunk connection with that switch. This domain name is created on any switch, that switch sends VTP Advertisement and applies its database to the rest of the switches in the network. Before connecting the switches, the network administrator may have created the required VLANs on the Primary Server switch and did not know to create the domain name on another switch on which VLANs are not defined. In this case, the created VLANs will be deleted. For this reason, a Domain Name must always be created on the Primary Server or the switch on which all VLANs are built, so as not to cause any damage to the network. It is also possible to enter the Switchport access vlan 50 command in one of its ports in a switch whose working mode is Client and VLAN number 50 is not present. In these cases, the log is not displayed for the user to notice his configuration error. A switch may even be configured with a different VTP version than other switches. To prevent this from happening, especially in large networks that are constantly expanding, configurations must be accurately and completely documented and available at each stage of the configuration, so that they can be analyzed and errors in the stage can be avoided. then prevented Network monitoring software can also be used to control traffic and identify incorrect traffic. In addition, to ensure that there are no errors in the configuration, the entire network can be implemented in simulator software, such as Cisco Packet Tracer and GNS3, so that if there is an error in the configuration, it can be noticed. Backups of VTP settings should also be taken continuously, so that if configuration problems occur with all these arrangements, the settings can be restored immediately. In this way, the risk of incorrect configuration can be avoided.

Another risk of using this protocol is VLAN Hopping attack. This is a layer 2 attack that penetrates from one VLAN to another VLAN without using a router. This attack is carried out in two ways: Switch Spoofing and Double Tagging. As explained, in the Switch Spoofing method, the Attacker can access other created VLANs by connecting another switch through a port configured as a Trunk. As mentioned, the solution to prevent this attack is to manually determine the working mode of the switch ports; So that the ports connected to PCs are in Access mode and the unused ports are in Shutdown mode. Because according to the previous explanations, if the port is left in Dynamic mode, the final working mode of the port may become Trunk if the two switches negotiate. In the Double Tagging method, the attacker penetrates through the Native VLAN.

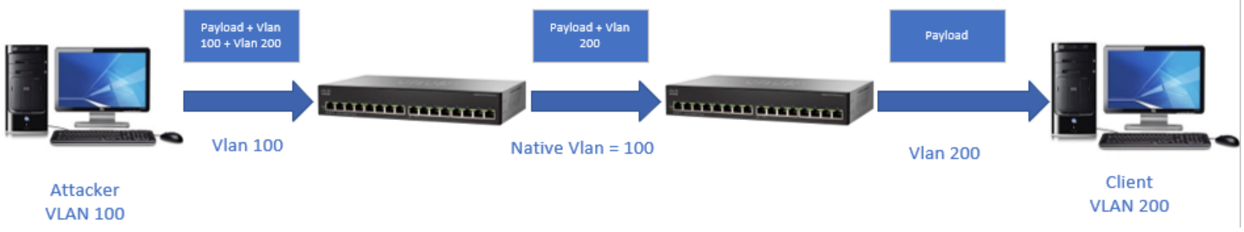


Figure 17 - An example of a tagging attack

According to Figure 17, the Native VLAN number is 100 and the VLAN in which the Attacker is located is also 100. In this example, the attacker wants to infiltrate VLAN 200. For this purpose, it sends its packet with VLAN tag number 200. When the packet reaches the first switch, due to the native VLAN number 100, no tag is added on the packet, and on the trunk link, the packet is sent with the VLAN tag number 200, and when the second switch arrives, due to having the VLAN tag number 200, its switch sends on ports that are members of VLAN 200. In this way, the attacker penetrates from VLAN 100 to VLAN 200. To reduce the risk of attack, we must enter the switchport trunk native vlan tag command in the Specific Configuration environment so that packets related to Native VLAN are also sent with the tag. Due to security issues, a VLAN that is unused should be selected as the Native VLAN. VACL or VLAN Access Control List can also be used to control traffic between VLANs.

The next risk is the possibility of bugs and software vulnerabilities in the VTP implementation that may lead to security problems in the network. For this purpose, the operating system of the switches should always be updated and the network should always be analyzed and monitored so that problems can be identified immediately and security vulnerabilities can be avoided.

The next risk is the increase in traffic load and decrease in performance. One of the reasons is the increase in the number of VLANs in a VTP Domain, which, especially in very large enterprise networks, can create an additional load on the switches and lead to a decrease in performance. In order to prevent, the creation of additional and unnecessary VLANs should be avoided; Because as the number of VLANs increases, the Broadcast Domain also increases.

In some organizations where the number of switches is not large and the organization does not have the conditions to create sufficient security for the devices, it is better not to use VTP. In this situation, if the switches support the third version, we set the working mode of all switches to Off to completely disable VTP; But if the switches only support the first and second versions, we set the working mode of all switches to Transparent so that the VLAN database of all switches becomes local so that the changes made on one switch are not applied to the other switches.

Discussion and conclusion

The review of VTP shows that this protocol can be an efficient tool to facilitate the management and control of VLANs in large computer networks of organizations. However, using this protocol without sufficient understanding of how it works and how to properly configure it can cause network disruptions, security issues, and the loss of some configurations. By examining the possible risks of using this protocol, this article

provides solutions to reduce these risks and increase the security of organizational networks.
Considering the management benefits and solving the challenges of this protocol will help administrators to reduce the occurrence of risks while using the maximum capacity of their implemented networks. Using the suggestions presented in the article can have a significant impact on the optimal use of this protocol by network administrators .

Resources

1- Hossein Qalipour, Masoud, 1401, CCNA 200-125 practical and visual training, third edition, Tehran, Kian University Press

2- Hossein Qalipour, Masoud, 2013, CCNP Switch 642-813 practical training, second edition, Tehran, Kian University Press

3- Hossein Qalipour, Masoud, 2013, Cisco CCNA Security 553-640 practical training, second edition, Tehran, Kian University Press

4- Nobri, Sabina, Ab Niki, Ruholah, Aghazadeh, Sakineh, 2013, Computer Networks, First Edition, Tehran, Farahosh PublicationsBarnes, David and Sakandar Basir. (2004). Cisco LAN Switching Fundamentals. Cisco Press

5- Wendell, Odom. (2013). CCNA Routing and Switching 200-120 Official Cert Guide Library. Pearson Education

6- Hucaby, David. (2014). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Pearson Education

7- Tetz, Edward. (2011). Cisco Networking All-in-One For Dummies. Wiley