How to configure VTP?

Before VLANs can be configured, VTP must be configured. By default, every switch will operate in VTP server mode for the management domain NULL, with no password or secure mode. The following sections discuss the commands and considerations that should be used to configure a switch for VTP operation.

Configuring a VTP Management Domain

Before a switch is added into a network, the VTP management domain should be identified. If this switch is the first one on the network, the management domain will need to be created. Otherwise, the switch may have to join an existing management domain with other existing switches.The following command can be used to assign a switch to a management domain on an IOS-based switch:

```
Switch# vlan database
Switch(vlan)# vtp domain domain_name
```

To assign a switch to a management domain on a CLI-based switch, use the following command:

Switch(enable) set vtp [domain domain_name

Configuring the VTP Mode

Once you have assigned the switch to a VTP management domain, you need to select the VTP mode for the new switch. There are three VTP modes that can be selected: server mode, client mode and transparent mode.

On an IOS-based switch, the following commands can be used to configure the VTP mode:

```
Switch# vlan database
Switch(vlan)# vtp domain domain_name
Switch(vlan)# vtp { server | client | transparent }
Switch(vlan)# vtp password password
```

On a CLI-based switch, the following command can be used to configure the VTP mode:

```
Switch(enable) set vtp [ domain domain_name ]
[ mode{ server | client | transparent }] [ password password ]
```

If the domain is operating in secure mode, a password can be included in the command line. The password can have 8 to 64 characters.

Configuring the VTP Version

Two versions of VTP, VTP version 1 and VTP version 2, are available for use in a management domain. Although VTP version 1 is the default protocol on a Catalyst switch, Catalyst switches are capable of running both versions; however, the two versions are not interoperable within a management domain. Thus, the same VTP version must be configured on each switch in a domain. However, a switch running VTP version 2 may coexist with other version 1 switches, if its VTP version 2 is not enabled. This situation becomes important if you want to use version 2 in a domain. Then, only one server mode switch needs to have VTP version 2 enabled. The new version number is propagated to all other version 2-capable switches in the domain, causing them to enable version 2 for use. By default, VTP version 1 is enabled. Version 2 can be enabled or disabled using the v2 option. The two versions of VTP differ in the features they support. VTP version 2 offers the following additional features over version 1:

. In transparent mode VTP version 1 matches the VTP version and domain name before forwarding the information to other switches using VTP. On the other hand, VTP version 2 in transparent mode forwards the VTP messages without checking the version number.

. VTP version 2 performs consistency checks on the VTP and VLAN parameters entered from the CLI or by Simple Network

Management Protocol (SNMP). This checking helps prevent errors in such things as VLAN names and numbers from being propagated to other switches in the domain. However, no consistency checks are performed on VTP messages that are received on trunk links or on configuration and database data that is read from NVRAM.

. VTP version 2 supports the use of Token Ring switching and Token Ring VLANs.

. VTP version 2 has Unrecognized Type-Length-Value (TLV) support, which means that VTP version 2 switches will propagate received configuration change messages out other trunk links, even if the switch supervisor is not able to parse or understand the message.

On an IOS-based switch, the VTP version number is configured using the following commands:

Switch# vlan database Switch(vlan)# vtp v2-mode

On a CLI-based switch, the VTP version number is configured using the following command:

Switch(enable) set vtp v2 enable