

Configuring VTP Servers Clients

Overview:

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Scenario:

In this CCNA Lab Packet tracer activity we will be configure a single VTP Domain over three switches, one as the VTP Server and the other two as VTP Clients. We will configure a VTP password for security.

VTP Domain:

A VTP domain (also called a VLAN management domain) is made up of one or more interconnected switches that share the same VTP domain name. A switch can be configured to be in one and only one VTP domain. You make global VLAN configuration changes for the domain using either the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

VTP Server:

In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.

VTP Client:

VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.

VTP Advertisements:

Each switch in the VTP domain sends periodic advertisements out each trunk port to a reserved multicast address. VTP advertisements are received by neighboring switches, which update their VTP and VLAN configurations as necessary.

The following global configuration information is distributed in VTP advertisements:

- VLAN IDs (ISL and 802.1Q)
- Emulated LAN names (for ATM LANE)
- 802.10 SAID values (FDDI)
- VTP domain name
- VTP configuration revision number
- VLAN configuration, including the maximum transmission unit (MTU) size for each VLAN
- Frame format

Lab Objective:

The objective of this Free CCNA Lab Packet Tracer Activity is for you to learn and understand how to configure VTP Server and Client mode on Cisco Catalyst switches.

- Learn to create a VTP domain.
- Learn how to password protect the VTP domain.
- Learn to configure VTP mode command.
- Learn to configure Trunk lines between switches.
- Learn to create VLANs within the VTP domain
- Learn to assign ports to VLANs.
- Learn to use show commands to verify VTP operation.

Procedure:

1. Basic switch configuration.
 - Hostnames.
 - Passwords.
 - Disable ip domain-lookup.
 - Disable timeout.
2. Configure the VTP domain on all three switches as CCNA
3. Set the VTP domain password as cisco on all three switches.
4. Configure DSW-1 as a VTP Server switch.
5. Configure ASW-1 and ASW-2 as a VTP Client switch.
6. Configure and verify an 802.1q trunk between Gig0/1 on DSW-1 and Gig1/1ASW-1.
7. Configure and verify an 802.1q trunk between Gig0/2 on DSW-1 and Gig1/2ASW-2.
8. Configure and verify VLANs 10 and 20 on DSW-1 with the names provided in the table below.
9. Assign the VLANs to fa0/1 and fa0/2 of ASW-1 and ASW-2 as shown in the table below.
10. Assign IP address to PC-1, 2, 3, and 4 as shown in the network diagram.
11. Test connectivity via your VLANs by pinging PC-3 from PC-1 and vice versa.
12. Test connectivity via your VLANs by pinging PC-4 from PC-2 and vice versa.

VLAN	NAME	SWITCH	PORT
10	Administration	ASW-1 & ASW-2	Fa0/1
20	Sales	ASW-1 & ASW-2	Fa0/2