

Understand VLAN Trunk Protocol (VTP)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Understand VTP](#)

[VTP Messages in Detail](#)

[Configuration Revision Number](#)

[Summary Advertisements](#)

[Subset Advertisements](#)

[Advertisement Requests](#)

[Other VTP Options](#)

[VTP Modes](#)

[VTP V2](#)

[VTP Password](#)

[VTP Pruning](#)

[Use VTP in a Network](#)

[Configure VTP](#)

[Troubleshoot VTP](#)

[Conclusion](#)

[Related Information](#)

Introduction

This document describes how to configure a new VLAN on one VTP server and distribute it through all switches on the domain.

Prerequisites

Requirements

There are no specific requirements for this document.


Components Used

This document is not restricted to specific software or hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

VLAN Trunk Protocol (VTP) reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products.

 **Note:** This document does not cover VTP Version 3. VTP Version 3 differs from VTP Version 1 (V1) and Version 2 (V2), and it incorporates many changes from these versions. Make certain that you understand the differences between VTP Version 3 and earlier versions before you alter your network configuration.

Refer to one of these sections of [VLAN Trunking Protocol \(VTP\)](#) for more information:

- [Understanding VTP Version 3](#)
- [VLAN Interaction](#)

Understand VTP

VTP Messages in Detail

VTP packets are sent in either Inter-Switch Link (ISL) frames or in IEEE 802.1Q (dot1q) frames. These packets are sent to the destination MAC address 01-00-0C-CC-CC-CC with a logical link control (LLC) code of Subnetwork Access Protocol (SNAP) (AAAA) and a type of 2003 (in the SNAP header). This is the format of a VTP packet that is encapsulated in ISL frames:

ISL Header	Ethernet Header DA: 01-00-00-00-00-00	LLC Header SSAP: AA DSAP: AA	SNAP Header OUI: cisco Type 2003	VTP Header	VTP Message	CRC
26 bytes	14 bytes	3 bytes	3 bytes	VARIABLE LENGTH (SEE AFTER)		

VTP Packet Encapsulated in ISL Frames

Of course, you can have a VTP packet inside 802.1Q frames. In that case, the ISL header and cyclic redundancy check (CRC) is replaced by dot1q tagging.

Now, consider the detail of a VTP packet. The format of the VTP header can vary, based on the type of VTP message. But all VTP packets contain these fields in the header:

- VTP protocol version: 1, 2, or 3
- VTP message types:
 - Summary advertisements
 - Subset advertisement
 - Advertisement requests
 - VTP join messages

- Management domain length
- Management domain name

Configuration Revision Number

The configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it. Most of the VTP packets contain the VTP configuration revision number of the sender.

This information is used in order to determine whether the received information is more recent than the current version. Each time that you make a VLAN change in a VTP device, the configuration revision is incremented by one. In order to reset the configuration revision of a switch, change the VTP domain name, and then change the name back to the original name.

Summary Advertisements

By default, Catalyst switches issue summary advertisements in five-minute increments. Summary advertisements inform adjacent Catalysts of the current VTP domain name and the configuration revision number.

When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch simply ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent.

Summary Advert Packet Format:

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9 0 1
Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 bytes)			
MD5 Digest (16 bytes)			

This list clarifies what the fields mean in the summary advertisement packet:

- The Followers field indicates that this packet is followed by a Subset Advertisement packet.
- The Updater Identity is the IP address of the switch that is the last to have incremented the configuration revision.
- The Update Timestamp is the date and time of the last increment of the configuration revision.
- Message Digest 5 (MD5) carries the VTP password, if MD5 is configured and used to authenticate the validation of a VTP update.

Subset Advertisements

When you add, delete, or change a VLAN in a Catalyst, the server Catalyst where the changes are made increments the configuration revision and issues a summary advertisement. One or several subset advertisements go with the summary advertisement. A subset advertisement contains a list of VLAN information. If there are several VLANs, more than one subset advertisement can be required in order to advertise all the VLANs.

Subset Advert Packet Format:

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9 0 1
Version	Code	Sequence Number	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision			
VLAN-info field 1			
.....			
VLAN-info field N			

Subset Advertisement Required to Advertise All VLANs

This formatted example shows that each VLAN information field contains information for a different VLAN. It is ordered so that lowered-valued ISL VLAN IDs occur first:

V-info-len	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 index			
VLAN-name (padded with zeros to multiple of 4 bytes)			

Each VLAN Information Field Contains Information for a Different VLAN

Most of the fields in this packet are easy to understand. These are two clarifications:

- Code — The format for this is 0x02 for subset advertisement.
- Sequence number — This is the sequence of the packet in the stream of packets that go with a summary advertisement. The sequence starts with 1.

Advertisement Requests

A switch needs a VTP advertisement request in these situations:

- The switch has been reset.
- The VTP domain name has been changed.
- The switch has received a VTP summary advertisement with a higher configuration revision than its own.

When an advertisement request is received, a VTP device sends a summary advertisement. One or more subset advertisements go with the summary advertisement. This is an example:

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
Version	Code	Rsvd	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start-Value			

VTP Device Sends a Summary Advertisement

- Code — The format for this is 0x03 for an advertisement request.

- **Start-Value** — This is used in cases in which there are several subset advertisements. If the first (n) subset advertisement has been received and the subsequent one ($n+1$) has not been received, the Catalyst only requests advertisements from the ($n+1$)th one.

Other VTP Options

VTP Modes

You can configure a switch to operate in any one of these VTP modes:

- **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.
- **Client** — VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
- **Transparent** — VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.
- **Off** — In the three described modes, VTP advertisements are received and transmitted as soon as the switch enters the management domain state. In the VTP off mode, switches behave the same as in VTP transparent mode with the exception that VTP advertisements are not forwarded.

VTP V2

VTP V2 is not much different than VTP V1. The major difference is that VTP V2 introduces support for Token Ring VLANs. If you use Token Ring VLANs, you must enable VTP V2. Otherwise, there is no reason to use VTP V2. Change of the VTP version from 1 to 2 does not cause a switch to reload.

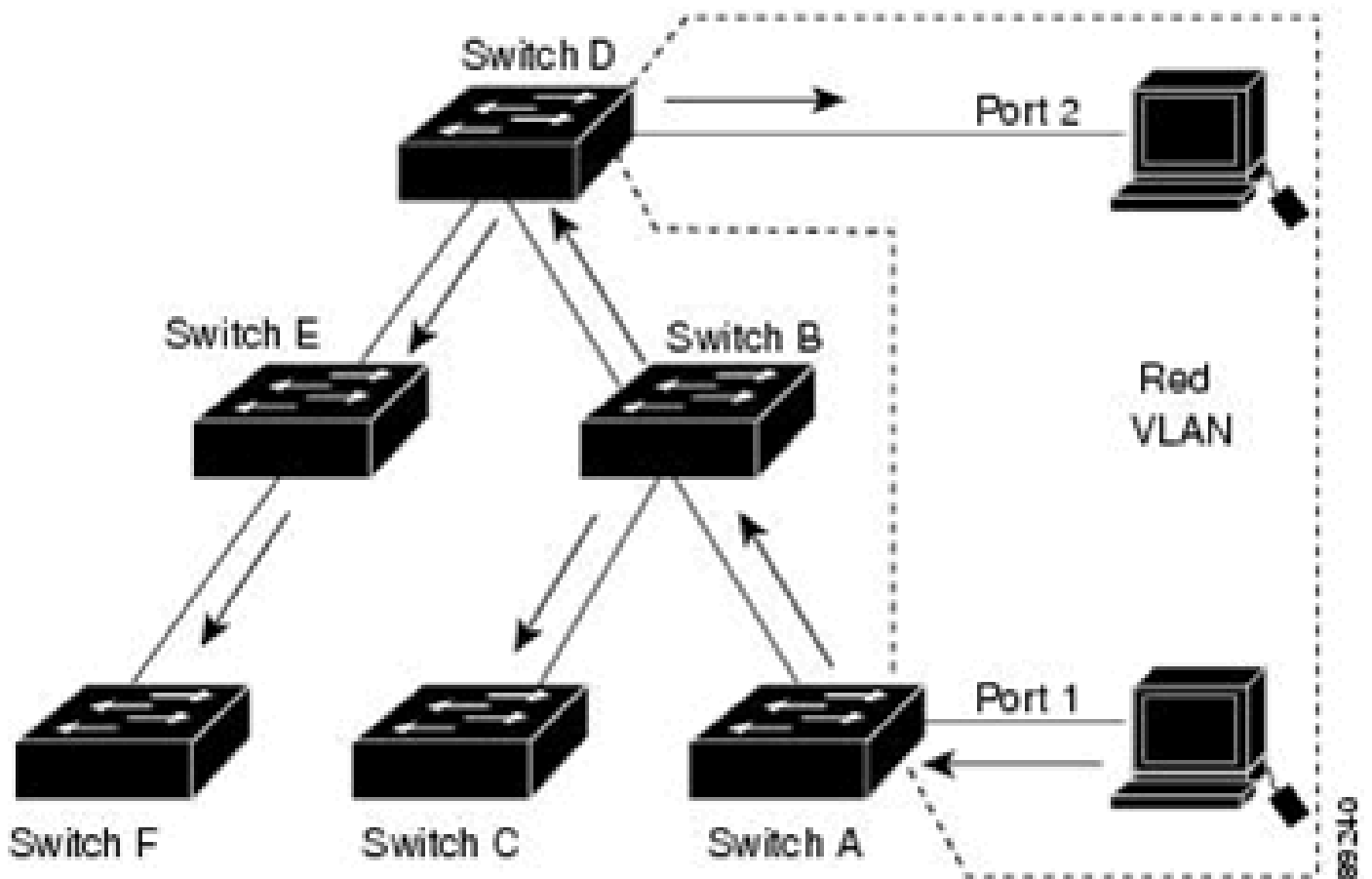
VTP Password

If you configure a password for VTP, you must configure the password on all switches in the VTP domain. The password must be the same password on all those switches. The VTP password that you configure is translated by algorithm into a 16-byte word (MD5 value) that is carried in all summary-advertisement VTP packets.

VTP Pruning

VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or pruned this unnecessary traffic.

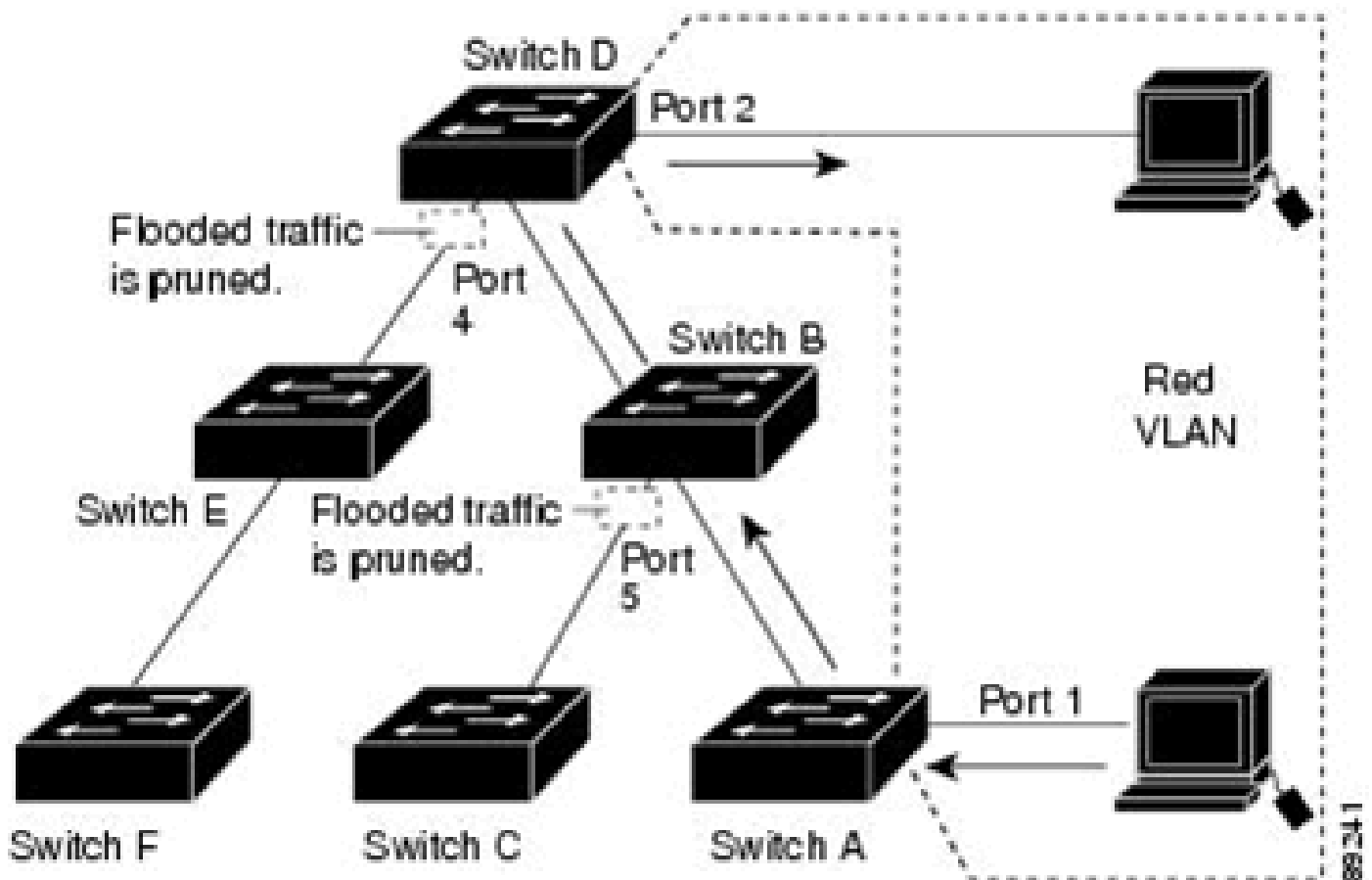
Broadcast Traffic in a Switched Network Without Pruning



Broadcast Traffic in a Switched Network Without Pruning

This figure shows a switched network without VTP pruning enabled. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

Broadcast Traffic in a Switched Network With Pruning



Broadcast Traffic in a Switched Network With Pruning

This figure shows the same switched network with VTP pruning enabled. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).

When VTP pruning is enabled on a VTP server, pruning is enabled for the entire management domain. This feature makes VLANs pruning-eligible or pruning-ineligible and affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain). VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs greater than 1005) are also pruning-ineligible.

Use VTP in a Network

By default, all switches are configured to be VTP servers. This configuration is suitable for small-scale networks in which the size of the VLAN information is small and the information is easily stored in all switches (in NVRAM). In a large network, the network administrator must make a judgment call at some point when the NVRAM storage that is necessary is wasteful because it is duplicated on every switch. At this point, the network administrator must choose a few well-equipped switches and keep them as VTP servers. Everything else that participates in VTP can be turned into a client. The number of VTP servers must be chosen in order to provide the degree of redundancy that is desired in the network.

Considerations:

- You can configure VLAN(s) without the VTP domain name configured on the switch which runs Cisco IOS®.

- If a new Catalyst is attached in the border of two VTP domains, the new Catalyst keeps the domain name of the first switch that sends it a summary advertisement. The only way to attach this switch to another VTP domain is to manually set a different VTP domain name.
- Dynamic Trunking Protocol (DTP) sends the VTP domain name in a DTP packet. Therefore, if you have two ends of a link that belong to different VTP domains, the trunk does not come up if you use DTP. In this special case, you must configure the trunk mode as on or nonegotiate, on both sides, in order to allow the trunk to come up without DTP negotiation agreement.
- If the domain has a single VTP server and it crashes, the best and easiest way to restore the operation is to change any of the VTP clients in that domain to a VTP server. The configuration revision is still the same in the rest of the clients, even if the server crashes. Therefore, VTP works properly in the domain.

Configure VTP

Refer to [Configure VLAN Trunk Protocol \(VTP\)](#) for information to configure VTP.

Troubleshoot VTP

Refer to [Troubleshooting VLAN Trunk Protocol \(VTP\)](#) for information to troubleshoot VTP.

Conclusion

There are some disadvantages to the use of VTP. You must balance the ease of VTP administration against the inherent risk of a large STP domain and the potential instability and risks of STP. The greatest risk is an STP loop through the entire campus. When you use VTP, there are two things to which you must pay close attention:

- Remember the configuration revision and how to reset it each time that you insert a new switch in your network so that you do not bring down the entire network.
- Avoid as much as possible to have a VLAN that spans the entire network.

Related Information

- [Cisco Switches Support](#)
- [Cisco Technical Support & Downloads](#)