VLAN Trunking Protocol
Introduction

• Early VLANs were difficult to implement across networks
  – Each VLAN was manually configured on each switch
  – Each manufacturer had different VLAN capability methods

• To solve these problems, VLAN trunking was developed
VLAN Trunking Protocol
Introduction

- Trunking allows many VLANs to be identified throughout an organization by adding tags to frames
  - The tags identify the VLANs to which the frames belong
  - Frames from many VLANs can be carried on a common trunk
  - VLAN trunking is widely implemented with the IEEE 802.1Q trunking protocol
  - Inter-Switch Link (ISL) is a Cisco-proprietary protocol that can be implemented in Cisco networks
VLAN Trunking Protocol
Introduction

• Cisco created **VLAN Trunking Protocol (VTP)**
  – Automates many VLAN configuration tasks
  – Configurations on a VTP server are automatically propagated to other switches in the VTP domain

• VLAN technology offers advantages:
  – Helps control Layer 3 broadcasts, improve network security, logically group network users

• VLAN limitations:
  – Operate at Layer 2; cannot communicate without use of routers (or Layer 3 switches) and network layer addresses
Trunking
Introduction

• Trunking goes back to the origin of radio and telephone switching technologies
  – In radio, a trunk is a single line that carries multiple channels of radio signals
  – In the telephone industry, a trunk is the communication path or channel between two points
    • Can carry simultaneous, multiple lines of communication
    • Central Offices (CO) are connected by trunks
    • Shared trunks are created for redundancy
    • Multiplexers combine several voice signals into a single trunk line and demultiplex the signal at the other end
Traditionally, telephone trunk lines carry multiple simultaneous conversations.
Trunking
Introduction

Shared Telephone Trunks Between COs Provide Redundancy
Trunking
Introduction

• The concept used by radio and telephone industries was adopted by data communications
  – A backbone link between a main distribution facility (MDF) and an intermediate distribution facility is composed of several trunks

• The same concept is applied to switching technologies
  – A trunk is a physical and logical connection between two switches
  – Network traffic travels across the trunk
  – A trunk is a single transmission channel between two points (a point-to-point link)
VLAN Trunking
Trunking
VLAN Trunking Operation

- Switching tables at both ends of the trunk are used to make forwarding decisions based on destination MAC addresses of the frames
  - As number of VLANs increases, this process becomes slower
  - Larger switching tables take longer to process
- Trunking protocols were developed to efficiently manage the transfer of frames from different VLANs on a single physical line
Trunking
VLAN Trunking Operation

- Modern trunking protocols use frame tagging
  - Faster delivery of frames
  - Easier management
- The single physical link between two switches can carry frames for multiple VLANs
  - Each frame is tagged to identify the VLAN to which it belongs
  - Different tagging schemes exist
    - Cisco’s ISL
    - IEEE 802.1Q
  - The tag is removed when the frame leaves the trunk
Trunking
VLAN Trunking Operation

- With **ISL**, an Ethernet frame is encapsulated with an additional header that contains a VLAN ID
- With **IEEE 802.1Q**, a tag containing the VLAN ID is embedded in the Ethernet Frame
- A trunk link does not belong to a specific VLAN
  – It is a conduit for VLANs between switches and routers
Trunking

VLAN Trunking Operation

VLAN Trunking Multiplexing Data from Multiple VLANs onto a Single Link
Trunking
IEEE 802.1Q Trunking

• The IEEE 802.1Q protocol:
  – Interconnects multiple switches and routers
  – Defines VLAN topologies
  – Cisco supports IEEE 802.1Q for FastEthernet and Gigabit Ethernet interfaces
  – Can carry traffic for multiple VLANs over a single link on a multivendor network
  – Extends IP routing capabilities to include support for IP frame types
Trunking
IEEE 802.1Q Trunking

- The two ports on the ends of an IEEE 802.1Q trunk are assigned to a native VLAN
  - (VLAN 1 by default)
  - Can be assigned to another VLAN
  - All untagged frames are assigned to the native VLAN
    - Ordinary end stations are able to read the untagged frames but not the tagged frames
IEEE 802.1Q Trunking
Frames Associated with the Native VLAN Are Untagged and Are Readable by End Stations
Trunking
IEEE 802.1Q Trunking

• Adding a frame tag results in the recomputation of the frame check sequence (FCS)
  – Embedded tag increases the size of the Ethernet frame

Recomputation of the FCS
The IEEE 802.1Q standard defines a unique spanning-tree instance running on the native VLAN for all the network VLANs.

- An 802.1Q mono spanning tree (MST) lacks some flexibility compared with a per-VLAN spanning tree + (PVST+) that runs one instance of Spanning Tree Protocol (STP) per VLAN.
Trunking
IEEE 802.1Q Trunking

- A mono spanning tree has only one instance of spanning tree for all VLANs
- Per-VLAN spanning tree (PVST) maintains a spanning tree instance for each VLAN
  - Uses ISL trunking
  - Cisco developed **PVST+** to enable running of several STP instances and to allow connection of an MST zone to a PVST zone
Trunking
IEEE 802.1Q Trunking

Cisco PVST+ Interoperates with Other Vendors’ STP Implementations
Trunking
IEEE 802.1Q Trunking

- PVST+ provides support for 802.1Q trunks and the mapping of multiple spanning trees to the single spanning tree of 802.1Q switches
  - Must be in a treelike structure for proper STP operation
- PVST+ architecture has three types of regions:
  - PVST region
  - PVST+ region
  - MST region
Trunking
IEEE 802.1Q Trunking

• Each region consists of a homogenous switch
  – Can connect a PVST region to a PVST+ region by connecting two ISL ports
  – Can connect a PVST+ region to an MST region by connecting two 802.1Q ports

• The existing Cisco STP implementation was extended to become PVST+
  – Added support for tunneling across an IEEE 802.1Q MST region
    • Tunneling means that BPDUs are flooded through the MST region along the single spanning tree in the MST region
    • PVST+ is thus compatible with 802.1Q and PVST
The existing Cisco STP implementation was extended to become PVST+ (continued)

- PVST+ adds verification mechanisms to ensure consistent port configuration and needs no additional configuration commands

- IEEE 802.1Q trunks impose some limitations on trunking strategy for a network:
  - The native VLAN on for an 802.1Q trunk must be the same on both ends of the link
  - The network must be loop-free before STP is disabled
Interaction Between 802.1Q Features and Trunk Ports

<table>
<thead>
<tr>
<th>Switch Feature</th>
<th>Trunk Port Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure ports</td>
<td>A trunk port cannot be a secure port.</td>
</tr>
<tr>
<td>Port grouping</td>
<td>802.1Q trunks can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration.</td>
</tr>
</tbody>
</table>

When a group is first created, all ports follow the parameters that are set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you enter to all ports in the group. The settings include the following:

- Allowed VLAN list
- STP path cost for each VLAN
- STP port priority for each VLAN
- STP PortFast setting
- Trunk status (if one port in a port group ceases to be a trunk, all ports cease to be trunks)
ISL Trunking
Introduction

• ISL characteristics and features:
  – Cisco proprietary
  – Interconnects multiple switches and maintains VLAN information as traffic travels between switches
  – Full wire-speed performance over FastEthernet
  – Full- or half-duplex mode
    • Full-duplex recommended
  – Operates in a point-to point environment
ISL Trunking
Introduction

• ISL characteristics and features (continued):
  – Uses frame tagging that is a low-latency mechanism for multiplexing traffic from multiple VLANs on a single physical path
  – Implemented for connections among switches, routers, and NICs that are used on nodes such as servers
ISL Trunking
Introduction

• To support ISL, each device must be ISL configured
  – An ISL-configured router allows inter-VLAN communication
  – Non-ISL devices that receive ISL frames might consider them to be errors as the size of the frame exceeds the maximum transmission unit (MTU) size
  • MTU for Ethernet is 1500 bytes
ISL Trunking

Introduction

• ISL functions at Layer 2
  – Encapsulates a data frame with a new header and a cyclic redundancy check (CRC)

• ISL is protocol independent for any type of upper-layer protocol
  – Used to maintain redundant links and load balance traffic between parallel links using STP
**ISL Trunking**

**Introduction**

- Ports configured as ISL trunk ports encapsulate each frame with a 26-byte ISL header and a 4-byte CRC before sending it out the trunk port
  - ISL is implemented in ASICs, so frames are tagged at wire-speed
- The number of VLANs supported by a switch depends on the switch hardware
ISL Trunking

Introduction

ISL Header and CRC Added to Ethernet Frames on ISL Trunks
ISL Trunking

Introduction

• Information in the ISL header:
  – DA: 40-bit multicast destination address
  – Type: 4-bit descriptor of the encapsulated frame type
  – User: 4-bit descriptor used as the type field extension or to define the Ethernet priorities
  – SA: 48-bit source MAC address of the transmitting Catalyst switch
  – LEN: 16-bit frame-length descriptor minus DA, Type, User, SA, LEN, and CRC
ISL Trunking

Introduction

• Information in the ISL header (continued):
  – AAAA03: standard Subnetwork Access Protocol (SNAP) 802.2 LLC header
  – HSA: first three bytes of the SA (OUI)
  – VLAN ID: 15-bit VLAN ID
  – BPDU: 1-bit descriptor that identifies whether the frame is a spanning-tree BPDU
  – INDX: 16-bit descriptor that identifies transmitting port ID
  – RES: 16-bit field used for additional information, such as FDDI frame control
• Becoming less common to use ISL
• More common to use IEEE 802.1Q
  – Older Catalyst switches support both
  – Some newer models support both, some support only 802.1Q (Catalyst 2950)
• On a Catalyst 2950 switch, 802.1Q is configured automatically when trunking is enabled on the interface
  – Use the `switchport mode trunk` command
• The `switchport mode` command has four options:
  – `trunk` – configures the port into permanent 802.1Q mode
  – `access` – disables trunk mode and negotiates with the connected device to covert the link to nontrunk
The `switchport mode` command has four options (continued):

- **dynamic desirable** – triggers the port to negotiate from nontrunk to trunk mode
- **dynamic auto** – enables a port to become a trunk only if the connected device has the state set to trunk or desirable; otherwise the port becomes a nontrunk port
• The `switchport nonnegotiate` command (Catalyst 2950) specifies that Dynamic Trunking Protocol (DTP) negotiation packets not be sent on Layer 2 interfaces
  – Switch does not engage in DTP negotiation on this interface
  – Command valid only when the interface access mode is access or trunk
# ISL Trunking
## Configuring VLAN Trunking
### 802.1Q Trunk Configuration

## Steps to Configure a Switch Port as a Trunk Port

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1.   | Enter the interface configuration mode and the port to be configured for trunking:  
      
      AccessSwitch(config)#interface interface | After the interface configuration is entered, the prompt changes from (config)# to (config-if)#. |
| 2.   | Configure the port as a VLAN trunk:  
      
      AccessSwitch(config-if)#switchport mode trunk. | Enable trunking on the selected interface. |
| 3.   | Specify the default VLAN:  
      
      AccessSwitch(config-if)#switchport access vlan vlan-id | (Optional) Specifies the default VLAN used if the interface stops trunking. |
| 4.   | Specify the native VLAN:  
      
      AccessSwitch(config-if)#switchport trunk native vlan vlan-id | Required for the native VLAN. If the native VLAN is 1, this step is not necessary. |
ISL Trunking
Configuring VLAN Trunking
ISL Trunk Configuration

• For Catalyst switches supporting ISL
  – Use the `switchport trunk encapsulation` interface command
  – Encapsulation types:
    • `dot1q`: uses only 802.1Q trunking encapsulation
    • `isl`: uses only ISL trunking encapsulation with a peer on the interface
    • `negotiate`: device negotiates trunking encapsulation with peer on the interface
Configuring ISL Trunking

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 2/24
Switch(config)#shutdown
Switch(config)#switchport trunk encapsulation isl
Switch(config)#switchport mode trunk
Switch(config)#no shutdown
```
VTP

Introduction

• Cisco created the proprietary VLAN Trunking Protocol (VTP) to solve operational problems in switched networks with VLANs
  – A domain may consist of several interconnected switches supporting multiple VLANs
  – To maintain connectivity within the VLANs, each VLAN must be manually configured on a switch
  – As additional switches are added to the network, they must be manually configured
  – A single incorrect configuration can cause cross-connected VLANs
• VTP reduces management and monitoring complexities
VTP

VTP Concepts

• VTP concepts and characteristics:
  – VTP is a Layer 2 messaging protocol
  – Maintains VLAN consistency by managing the addition, deletion, and name changes of VLANs across networks
    – Minimizes misconfigurations that can cause problems
• A VTP domain is an administrative unit consisting of one switch or several interconnected switches
  – A switch can be configured in only one VLAN domain
VTP Concepts

VTP Domain

1. New VLAN Added

2. 

3. Sync to the Latest VLAN Information
VTP
VTP Concepts

• By default, a Catalyst switch is in the no-management-domain state until it receives an advertisement over a trunk link or until a management domain is configured
  – Configurations are made to a single VTP server
    • A Catalyst switch on which configuration changes are propagated across links to all connected switches in the domain
    • VTP advertisements are sent on trunk ports only
VTP Operations

VTP operates in one of three modes:

- Server mode (default mode)
  - VLANs are not propagated until a management domain name is specified or learned
  - When a VLAN is created, modified, or deleted, the change is propagated to all switches in the VTP domain
  - VTP advertisements are transmitted out all trunk connections and synchronized with other VTP servers and clients
  - VTP information is saved in NVRAM
VTP
VTP Operations

• VTP operates in one of three modes (continued):
  – Transparent mode
    • When in transparent mode, VLAN creation, modification, or deletion affects only the local switch and is not propagated to other switches
    • VLAN information is saved in NVRAM
  – Client mode
    • Cannot create, modify, or delete VLANs when in client mode
    • VTP advertisements are forwarded when in client mode
    • VTP information is synchronized with other VTP clients and servers
    • VLAN information is saved in NVRAM
VTP Operations

- VLAN advertisements are flooded throughout the management domain
  - Sent every 5 minutes or when a change occurs
  - Transmitted over the default VLAN (VLAN 1) using a multicast frame
  - Revision numbers are used; a higher revision number indicates more current information
A critical component of VTP is the configuration revision number

- Each time information is changed, the VTP increments the configuration revision number by one
- The server then sends out a VTP advertisement with the new configuration revision number
- If this number is higher than the number stored on a switch, the switch overwrites its configuration information with the new information
- The configuration revision number in transparent mode is always 0
VTP

VTP Operations

VTP Messages Synchronizing VLAN Information Within a VTP (Management) Domain
A device receiving VTP advertisements must:
  – Check that the management domain name and password match that on the local switch
  – Check that the configuration revision number was created after the configuration currently in use

To reset the revision number, use the `delete vtp` privileged EXEC command
VTP

VTP Operations

• **VTP Pruning** uses VLAN advertisements to determine when a trunk is needlessly flooding traffic
  – VTP pruning results in prevention of unnecessary traffic
  – VTP pruning increases bandwidth by restricting traffic to those trunk links that the traffic must use to access appropriate devices

• By default, a trunk carries traffic for all VLANs in the VTP management domain
  – Some switches will not have ports configured in each VLAN

• VTP pruning is enabled on servers, not clients; if VTP is not deployed must set switches to transparent mode
VTP Pruning Preventing Unnecessary VLAN Traffic in a VTP Domain

Switch 4 (Port 2) is connected to Switch 5 and Switch 2. Switch 1 is connected to Switch 3 and Switch 6. Switch 5 is connected to Switch 6. Switch 2 is connected to Switch 3. Port 1 of Switch 1 connects to a device (A). Port 2 of Switch 4 connects to a device (B). The diagram shows that traffic is flooded to Switch 5, but the traffic is pruned for Switches 1, 2, 3, and 6.
• When creating VLANs, must decide whether to use VTP in the network
  – Allows configuration changes made on one switch to be propagated to all other switches in the VTP domain
  – Default values for a Catalyst 2950 switch:
    • **VTP domain name**: none, **VTP mode**: server, **VTP password**: none, **VTP pruning**: disabled, **VTP version**: 1, **VTP trap**: disabled
VTP
Configuring VTP

- VTP domain name can be configured or learned
  - Not set by default
- An optional password can be set for the VTP management domain
  - Must be the same password for each switch in the domain
- Enabling or disabling VTP pruning on a server propagates the change throughout the management domain
The `vtp` global configuration command is used to modify VTP configuration:

- `vtp {domain domain-name | file filename | interface name | mode {client | server | transparent} | password password | pruning | version number}`

When the VTP mode is transparent, the VTP configuration can be saved to the switch with the `copy running-config startup-config` command.
VTP
Configuring VTP

• With the Catalyst 2950, can use the `vtp` privileged EXEC command to configure VTP password, pruning and administrative version:
  – `Switch#vtp {password password | pruning | version number}`

• Domain name and password are case sensitive
  – Domain name cannot be removed after it is assigned; can only be reassigned
Configuring VTP

```plaintext
AccessSwitch#configure terminal
AccessSwitch(config)#vtp domain hawaii
AccessSwitch(config)#vtp mode transparent
AccessSwitch(config)#vtp password cisco
AccessSwitch(config)#vtp pruning
AccessSwitch(config)#end
AccessSwitch#show vtp status

VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 250
Number of existing VLANs : 6
VTP Operating Mode : Transparent
VTP Domain Name : hawaii
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xA6 0xE8 0x48 0x78 0x2F 0x5F 0x1A 0x71
Configuration last modified by 10.10.10.50 at 1-1-06 14:38:06
Local updater ID is 10.10.10.50 on interface Vl1 (lowest numbered VLAN interface found)
```
Inter-VLAN Routing Overview

Introduction

- Inter-VLAN communication occurs between broadcast domains through a Layer 3 device
  - Frames are switched only between ports in the same broadcast domain
  - VLANs perform network partitioning and traffic separation at Layer 2
  - Inter-VLAN communication cannot occur without a Layer 3 device
  - Inter-VLAN routing is routing between VLANs on a router or a Layer 3 switch
Inter-VLAN Routing Overview
Router-on-a-Stick

• The configuration between a router and a core switch is sometimes referred to as a router-on-a-stick
  – Router can receive packets on one VLAN and forward them to another VLAN
  – Must be a separate logical connection on the router for each VLAN
  – Must enable ISL or 802.1Q trunking on a single physical connection
    • Must subdivide the physical FastEthernet interface of the router into multiple logical, addressable interfaces, one per VLAN
    • These are called “subinterfaces”
Inter-VLAN Routing Overview

Router-on-a-Stick

Router-on-a-StickEmploying a Layer 2 Switch Trunked to a Router
Inter-VLAN Routing Overview
Router-on-a-Stick

Logical Subinterfaces on the Router End of a Trunk Link in a Router-on-a-Stick Topology
An interface can be logically divided into multiple virtual subinterfaces.

To define subinterfaces of a physical interface:

- Identify the interface
- Define the VLAN encapsulation
- Assign an IP address to the interface
Inter-VLAN Routing Overview

Configuring Inter-VLAN Routing

One Router with Three Subinterfaces Corresponding to Three VLANs in the Router-on-a-Stick Topology
• To identify the interface, use the `interface` command in global configuration mode

`Router(config)#interface fastethernet port-number subinterface-number`

– `port-number` identifies the physical interface and `subinterface-number` identifies the virtual interface
Inter-VLAN Routing Overview

Configuring Inter-VLAN Routing

A FastEthernet Interface Can Be Subdivided into Logical Subinterfaces Associated in a One-to-One Fashion with VLANs
To define the VLAN encapsulation, use the appropriate encapsulation command in interface configuration mode:

Router(config-if)#**encapsulation isl**  vlan-id

Router(config-if)#**encapsulation dot1q**  vlan-id [native]

To assign an IP address to the interface, use the following interface mode command:

Router(config-if)#**ip address**  ip-address  subnet  mask
Configuring Inter-VLAN Routing

Router(config)#interface FastEthernet 0/0.1
Router(config-subif)#description Management VLAN 1
Router(config-subif)#encapsulation dot1q 1 native
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#interface FastEthernet 0/0.2
Router(config-subif)#description Accounting VLAN 20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#interface FastEthernet 0/0.3
Router(config-subif)#description Sales VLAN 30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
A trunk is a physical and logical connection between two switches across which network traffic travels

- Concept goes back to origins of radio and telephone switching technology
- In LAN switching, a trunk is a point-to-point link that supports several VLANs
- Purpose is to conserve ports when creating a link between two devices implementing VLANs
- Multiple virtual links are bundled over one physical link
Summary

- Trunking protocols were developed to efficiently manage the transfer of frames from different VLANs on a single physical link
  - Trunking protocols establish agreement for the distribution of frames to both ends of the link
  - Trunking protocols use frame tagging to assign an identifier to frames
    - Functions at Layer 2
    - Cisco’s ISL and IEEE 802.1Q are the most common tagging schemes for Ethernet segments
Summary

- VTP was created to solve problems such as cross-connected VLANs caused by configuration inconsistencies
  - With VTP, VLAN configuration is consistently maintained across a VTP domain
    - A VTP domain is made up of one or more interconnected devices that share the same VTP domain name
    - A switch can be in only one VTP domain
  - VTP messages are encapsulated in a trunking protocol frame, such as ISL or IEEE 802.1Q
  - VTP switches operate in one of three modes: server, client, transparent
Summary

• With VTP, each switch advertises the following on its trunk ports:
  – Management domain
  – Configuration revision number
  – VLANs that it knows about
  – Parameters for the VLANs

• By default, server and client Catalyst switches send VTP advertisements every 5 minutes or when a change occurs
Summary

- VTP servers inform neighbors of the current configuration revision number
  - The revision number is compared to the one in memory and the switch overwrites the old configuration if the number is higher
- At least one server needs to be in a VTP domain
- Before adding a VTP client, use the `show vtp status` command to verify the VTP configuration revision number on other switches in the VTP domain
Summary

• When a host wants to communicate with a host in a different VLAN, a router or Layer 3 switch must be involved to facilitate inter-VLAN routing
  – A physical interface on the router can be divided into multiple logical subinterfaces
  – Subinterfaces provide a flexible solution for routing multiple data streams through a single physical interface