**CCNA**

640-802

**Virtual LANs (VLAN)**







Revision no.: PPT/2K804/04

Revision no.: PPT/2K804/04



# VLAN Basics

## By default, routers allow broadcasts only within the originating network, but switches forward broadcasts to all segments. The reason it’s called a flat network is because it’s one Broadcast domain , not because its design is physically flat.



* Flat Network Structure

**layer 2 switched network is that it creates individual collision domain segments for each device plugged into each port on the switch.**

****

Revision no.: PPT/2K804/04



**VLAN Basics (contd.)**

## Network adds, moves, and changes are achieved by configuring a port into the appropriate VLAN.



* A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them.
* As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
* VLANs can enhance network security.
* VLANs increase the number of broadcast domains while decreasing their size.



Revision no.: PPT/2K804/04



**VLAN Basics (contd.)**

* Broadcasts occur in every protocol, but how often they occur depends upon three things:



* + Type of protocol
  + The application(s) running on the internetwork
  + How these services are used



Revision no.: PPT/2K804/04



**VLAN Basics (contd.)**

## Security



* + A flat internetwork’s security used to be tackled by connecting hubs and switches together with routers which maintains security.
  + Anyone connecting to the physical network could access the network resources located on that physical LAN.
  + Anyone would observe any and all traffic happening in that network was to simply just plug a network analyzer into the hub which is non- security.
  + In VLAN creating multiple broadcast groups, administrators can have control over each port and user, and whatever resources that port can access.
  + If you need inter-VLAN communication, you can implement restrictions on a router to achieve it. You can also place restrictions on hardware addresses, protocols, and applications.



Revision no.: PPT/2K804/04



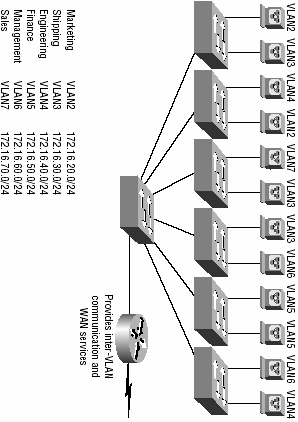
**VLAN Basics (contd.)**

## Flexibility and Scalability



* + layer 2 switches only read frames for filtering—they don’t look at the Network layer protocol.
  + Implementing VLANs, you’re essentially creating smaller broadcast domains at layer 2.Broadcasts sent out from a node in one VLAN won’t be forwarded to ports configured to be in a different VLAN.
  + A VLAN can exist on a single switch or span multiple switches. It can include stations in a single building or multiple-building infrastructures, or it can connect across WANs.

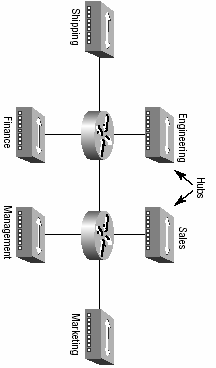






Revision no.: PPT/2K804/04

**VLAN Basics (contd.)**



Revision no.: PPT/2K804/04



# VLAN Membership

## Static VLAN



* + Static VLANs are the usual way of creating VLANs, they’re created by administrator and also the most secure.
  + This type of VLAN configuration is comparatively easy to set up and monitor.
  + Assignment of VLAN to port is configured statically by an administrator.



Revision no.: PPT/2K804/04



**VLAN Membership (contd.)**

## Dynamic VLAN



* + A dynamic VLAN determines a node’s VLAN assignment automatically.
  + It makes management and configuration easier because if a user moves, the switch will assign them to the correct VLAN automatically.
  + A dynamic port can belong to only one VLAN at a time. Multiple hosts can be active on a dynamic port only if they all belong to the same VLAN.
  + Administrators can use the VLAN Management Policy Server (VMPS). A VMPS database maps MAC addresses to VLANs.



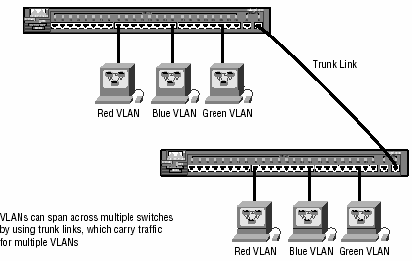
Revision no.: PPT/2K804/04



# Identifying VLANs

## Access links



* + This type of link is only part of one VLAN, and it’s referred to as the native VLAN of the port. Any device attached to an access link is unaware of a VLAN membership—the device just assumes it’s part of a broadcast domain, but it has no understanding of the physical network.
  + Switches remove any VLAN information from the frame before it’s sent to an access- link device.



Revision no.: PPT/2K804/04



**Identifying VLANs (contd.)**

* Trunk links



* + Trunks can carry multiple VLANs and originally gained their name after the telephone system trunks that carry multiple telephone conversations.
  + A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router, or between a switch and server. These carry the traffic of multiple VLANs—from1 to 1005 at a time.
  + Trunking allows you to make a single port part of multiple VLANs at the same time.
  + All VLANs are configured on a trunked link unless cleared by an administrator by hand.



Revision no.: PPT/2K804/04



**Identifying VLANs (contd.)**

* Frame Tagging



* + Frame identification method uniquely assigns a user-defined ID to each frame, also know as VLAN ID.
  + As the frame reaches a switch it must first identify the VLAN ID from the frame tag, then it finds out what to do with the frame by looking at the information in the filter table.
  + Once the frame reaches an exit to an access link matching the frames VLAN ID, the switch removes the VLAN identifier.



Revision no.: PPT/2K804/04



**Identifying VLANs (contd.)**

## VLAN Identification Methods



* + VLAN identification is what switches use to keep track of all those frames as they’re traversing a switch fabric. It’s how switches identify which frames belong to which VLANs, and there’s more than one trunking method :
    - Inter-Switch Link (ISL)
    - IEEE 802.1Q



Revision no.: PPT/2K804/04



**Identifying VLANs (contd.)**

## Inter-Switch Link (ISL)



* + This is proprietary to Cisco switches, and it’s used for Fast Ethernet and Gigabit Ethernet links only.
  + ISL routing can be used on a switch port, router interfaces, and server interface cards to trunk a server.
  + A trunked server is part of all VLANs (broadcast domains) simultaneously, so users don’t have to cross a layer 3 device to access it.



Revision no.: PPT/2K804/04



**Identifying VLANs (contd.)**

## IEEE 802.1Q



* + Created by the IEEE as a standard method of frame tagging,
  + It inserts a field into the frame to identify the VLAN. If you’re trunking between a Cisco switched link and a different brand of switch, you have to use 802.1Q for the trunk to work.
  + You must designate each 802.1Q port to be associated with a

specific VLAN ID.



Revision no.: PPT/2K804/04



# Inter-Switch Link (ISL) Protocol

## Inter-Switch Link (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame.



* This tagging information allows VLANs to be multiplexed over a trunk link through an external encapsulation method (ISL).
* which allows the switch to identify the VLAN membership of a frame over the trunked link.
* you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links.
* ISL functions at layer 2 by encapsulating a data frame with a new header and cyclic redundancy check (CRC).



Revision no.: PPT/2K804/04



# Inter-Switch Link (ISL) Protocol (contd.)

## ISL is an external tagging process, the original frame isn’t altered—it’s only encapsulated with a new 26-byte ISL header.



* It also adds a second 4-byte Frame Check Sequence (FCS) field at the end of the frame, frames can be up to a 1522 bytes long!
* The frame encapsulated by ISL information, only ISL-aware devices can read it.
* ISL VLAN information is added to a frame only if the frame is forwarded out a port configured as a trunk link.



Revision no.: PPT/2K804/04



# VLAN Trunking Protocol (VTP)

## VLAN Trunking Protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network.



* VTP allows an administrator to add, delete, and rename VLANs-information that is then propagated to all other switches in the VTP domain.



Revision no.: PPT/2K804/04



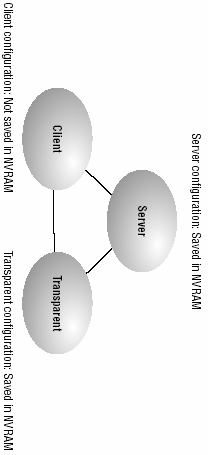
**VLAN Trunking Protocol (VTP) (contd.)**

## Benefits of VLAN Trunking Protocol (VTP)



* + Consistent VLAN configuration across all switches in the network
  + Allows VLANs to be trunked over mixed networks, such as Ethernet to ATM LANE or even FDDI
  + Accurate tracking and monitoring of VLANs
  + Dynamic reporting of added VLANs to all switches in the VTP domain
  + Plug-and-Play VLAN adding









Revision no.: PPT/2K804/04

**VTP Modes of Operation**

•

Three different modes of operation within a VTP domain.

Revision no.: PPT/2K804/04



**VTP Modes of Operation (contd.)**

## Server :



* + This is the default for all Catalyst switches. You need at least one server in your VTP domain to propagate VLAN information throughout the domain.
  + The switch must be in server mode to be able to create, add, or delete VLANs in a VTP domain.
  + Any change made to a switch in server mode will be advertised to the entire VTP domain.



Revision no.: PPT/2K804/04



**VTP Modes of Operation (contd.)**

## Client :



* + In client mode, switches receive information from VTP servers, and they also send and receive updates. But they can’t make any changes.
  + None of the ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch of the new VLAN.



Revision no.: PPT/2K804/04



**VTP Modes of Operation (contd.)**

## Transparent :



* + Switches in transparent mode don’t participate in the VTP domain, but they’ll still forward VTP advertisements through any configured trunk links.
  + These switches can’t add and delete VLANs because they keep their own database which not share with other switch
  + The VLAN database in Transparent mode is really considered locally significant only.



Revision no.: PPT/2K804/04



# VTP Pruning

## Preserves bandwidth by configuring it to reduce the amount of broadcasts, multicasts, and unicast packets.



* VTP pruning only sends broadcasts to trunk links that truly must have the information.
* Enabling pruning on a VTP server, enables it for the entire domain.
* By default, VLANs 2 through 1005 are pruning-eligible, but VLAN 1 can never prune because it’s an administrative VLAN.



Revision no.: PPT/2K804/04



# Routing between VLANs

## VLANs create network partitioning and traffic separation at layer 2 of the OSI.



* If you want hosts or any other IP addressable device to communicate between VLANs, a layer 3 device is absolutely necessary.
* You can use a router that has an interface for each VLAN or a router that supports ISL routing.
* Router that supports ISL routing is the 2600 series router. The 1600, 1700, and 2500 series don’t support ISL routing.



Revision no.: PPT/2K804/04



**Routing between VLANs (contd.)**

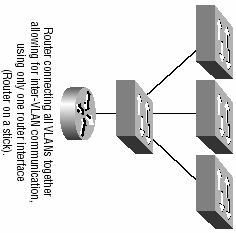
## This means that each of the routers’ interface IP addresses would then become the default gateway address for each host in each VLAN.



* + If you have more VLANs available than router interfaces, you can either run ISL trunking on one Fast Ethernet interface or buy a layer 3 switch such as the Cisco 3550.
  + A Fast Ethernet interface on a router configured with ISL or 802.1Q trunking allows all VLANs to communicate through one interface. Cisco calls this a

“router on a stick.”

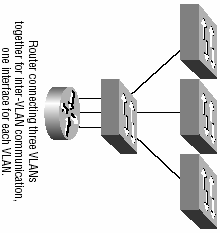






Revision no.: PPT/2K804/04

**Routing between VLANs (contd.)**



Revision no.: PPT/2K804/04



# Configuring VLANs

## To configure VLANs on a 1900 switch, use the vlan vlan# name name [vlan#] command.



* >en
* #config t
* Enter configuration commands, one per line. End with CNTL/Z
* (config)#hostname 1900
* 1900(config)#vlan 2 name sales
* 1900(config)#vlan 3 name marketing
* 1900(config)#vlan 4 name mis
* 1900(config)#exit



Revision no.: PPT/2K804/04



**Configuring VLANs (contd.)**

## The show vlan command :



1900#**sh vlan**

VLAN Name Status Ports

--------------------------------------

1. default Enabled 1-12, AUI, A, B
2. sales Enabled
3. marketing Enabled
4. mis Enabled

|  |  |
| --- | --- |
| 1002 | fddi-default Suspended |
| 1003 | token-ring-default Suspended |
| 1004 | fddinet-default Suspended |
| 1005 | trnet-default Suspended |

--------------------------------------



Revision no.: PPT/2K804/04



**Configuring VLANs (contd.)**

## Creating VLANs for the 2950 switch is very different. You configure them in what is called a VLAN database.



Switch#**vlan database**

Switch(vlan)#**vlan 1 name Sales**

A default VLAN may not have its name changed. Switch(vlan)#**vlan 2 name Marketing**

VLAN 2 modified:

Name: Marketing

Switch(vlan)#**vlan 3 name Accounting**

VLAN 3 added:

Name: Accounting Switch(vlan)#**Vlan 4 name Shipping** VLAN 4 added:

Name: Shipping Switch(vlan)#**apply** APPLY completed.

Switch(vlan)#**control+c** Switch#



Revision no.: PPT/2K804/04



**Configuring VLANs (contd.)**

* To see the VLAN database, use the show vlan command or the show vlan brief command:



Switch#**sh vlan brief**

VLAN Name Status Ports

---- --------------------------- --------- --------------------------

1. default active Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8,

Fa0/9, Fa0/10, Fa0/11, Fa0/12

1. Marketing active
2. Accounting active
3. Shipping active
4. VLAN0021 active
5. VLAN0022 active
6. VLAN0051 active
7. VLAN0052 active

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active Switch#



Revision no.: PPT/2K804/04



# Assigning Switch Ports to VLANs

## Configure each port on a 1900 switch to be in a VLAN by using the vlan-membership command.



* + You can only configure VLANs one port at a time.
  + You can configure either static memberships or dynamic memberships on a port.



Revision no.: PPT/2K804/04



# Assigning Switch Ports to VLANs (contd.)

1900#**config t**



Enter configuration commands, one per line. End with CNTL/Z 1900(config)#**int e0/2**

1900(config-if)#**vlan-membership ?**

dynamic Set VLAN membership type as dynamic static Set VLAN membership type as static

|  |  |  |
| --- | --- | --- |
| 1900(config-if)#**vlan-membership** | **static** | **?** |
| <1-1005> ISL VLAN index |  |  |
| 1900(config-if)#**vlan-membership** | **static** | **2** |
| 1900(config-if)#**int e0/4** |  |  |
| 1900(config-if)#**vlan-membership**  1900(config-if)#**int e0/5** | **static** | **3** |
| 1900(config-if)#**vlan-membership** | **static** | **4** |
| 1900(config-if)#**exit** |  |  |
| 1900(config)#**exit** |  |  |



Revision no.: PPT/2K804/04



# Assigning Switch Ports to VLANs (contd.)

## The show vlan command use to see the ports assigned to each VLAN



1900#**sh vlan**

VLAN Name Status Ports

--------------------------------------

1. default Enabled 1, 3, 6-12, AUI, A, B
2. sales Enabled 2
3. marketing Enabled 4
4. mis Enabled 5

|  |  |
| --- | --- |
| 1002 | fddi-default Suspended |
| 1003 | token-ring-defau Suspended |
| 1004 | fddinet-default Suspended |
| 1005 | trnet-default Suspended |

--------------------------------------



Revision no.: PPT/2K804/04



# Assigning Switch Ports to VLANs (contd.)

## To configure a 2950 with VLANs



Switch(config-if)#**int f0/2**

Switch(config-if)#**switchport access vlan 2**

Switch(config-if)#**int f0/3**

Switch(config-if)#**switchport access vlan 3**

Switch(config-if)#**int f0/4**

Switch(config-if)#**switchport access vlan 4**

Switch(config-if)#



Revision no.: PPT/2K804/04



# Assigning Switch Ports to VLANs (contd.)

## The show vlan or show vlan brief command to show you the VLANs with port assignments:



Switch#**sh vlan brief**

VLAN Name Status Ports

---- ------------------- --------- --------------------------

1. default active Fa0/1, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2. Marketing active Fa0/2
3. Accounting active Fa0/3
4. Shipping active Fa0/4



Revision no.: PPT/2K804/04



# Configuring Trunk Ports

* The 1900 switch only runs the Dynamic Inter-Switch Link (DISL) encapsulation method.



* To configure trunking on a FastEthernet port, use the interface command trunk [parameter].

1900#**config t**

Enter configuration commands, one per line. End with CNTL/Z 1900(config)#**int f0/26**

1900(config-if)#**trunk ?**

auto Set DISL state to AUTO

desirable Set DISL state to DESIRABLE nonegotiate Set DISL state to NONEGOTIATE off Set DISL state to OFF

on Set DISL state to ON 1900(config-if)#**trunk on**

****

Revision no.: PPT/2K804/04



**Configuring Trunk Ports (contd.)**

## The following list describes the different options available when setting a trunk interface:



* + **Auto** The interface will become trunked only if the connected device is set to on or desirable.
  + **Desirable** If a connected device is on either desirable or auto, it will negotiate to become a trunk port. Nonegotiate, when mated with desirable, will result in a trunk link, as well.
  + **Nonegotiate** The interface becomes a permanent ISL trunk port and will not negotiate with any attached device.
  + **Off** The interface is disabled from running trunking and tries to convert any attached device to be trunked as well.
  + **On** The interface becomes a permanent ISL trunk port. It can negotiate with a connected device to convert the link to trunk mode.



Revision no.: PPT/2K804/04



**Configuring Trunk Ports (contd.)**

## The 2950 you use the switchport command



* Switch#config t
* Enter configuration commands, one per line. End with CNTL/Z.
* Switch(config)#int f0/12
* Switch(config-if)#switchport mode trunk
* Switch(config-if)#^Z
* Switch#



Revision no.: PPT/2K804/04



**Configuring Trunk Ports (contd.)**

* + To disable trunking on an interface, use the switchport mode access command. You can verify your configuration with the show running-config command:



!

interface FastEthernet0/2 switchport access vlan 2 no ip address

!

interface FastEthernet0/3 switchport access vlan 3 no ip address

!

interface FastEthernet0/4 switchport access vlan 4 no ip address

!

interface FastEthernet0/12 switchport mode trunk

no ip address



Revision no.: PPT/2K804/04



# Trunking with the Cisco Catalyst 3560 switch

* Cisco Catalyst 3560 can provide layer 3 services and the 2960 can’t.



* The 3560 can run both the ISL and the IEEE 802.1Q trunking encapsulation methods, the 2960 can only run 802.1Q.
* The 3560 has the encapsulation command, which the 2960 switch doesn’t:

Core(config-if)#switchport trunk encapsulation dot1q Core(config-if)#switchport mode trunk

* We got the option to add either the IEEE 802.1Q (dot1q) encapsulation or the ISL encapsulation to the 3560 switch. After you set the encapsulation, you still have to set the interface mode to trunk.



Revision no.: PPT/2K804/04

.



# Defining the Allowed VLANs on a Trunk

* Trunk ports send and receive information from all VLANs by default, and if a frame is untagged, it’s sent to the management VLAN (by default vlan1).



* But we can remove VLANs from the allowed list to prevent traffic from certain VLANs from traversing a trunked link.
* S1#config t
* S1(config)#int f0/1
* S1(config-if)#switchport trunk allowed vlan ?
* WORD VLAN IDs of the allowed VLANs when this port is in trunking mode
* add add VLANs to the current list
* all all VLANs
* except all VLANs except the following
* none no VLANs
* remove remove VLANs from the current list
* S1(config-if)#switchport trunk allowed vlan remove ?
* WORD VLAN IDs of disallowed VLANS when this port is in trunking mode
* S1(config-if)#switchport trunk allowed vlan remove 4



Revision no.: PPT/2K804/04



* The preceding command stopped the trunk link configured on S1 port f0/1, causing it to drop all traffic sent and received for VLAN 4.
* To remove a range of VLANs
* S1(config-if)#switchport trunk allowed vlan remove 4-8
* If by chance someone has removed some VLANs from a trunk link and you want to set the trunk back to default, just use this command:
* S1(config-if)#switchport trunk allowed vlan all



Revision no.: PPT/2K804/04



# Changing or Modifying the Trunk Native VLAN

To change the native VLAN, use the following command:



* S1#config t
* S1(config)#int f0/1
* S1(config-if)#switchport trunk ?
* Allowed Set allowed VLAN characteristics when interface is in trunking mode
* Native Set trunking native characteristics when interface is in trunking mode
* Pruning Set pruning VLAN characteristics when interface is in trunking mode



Revision no.: PPT/2K804/04



* S1(config-if)#switchport trunk native ?

vlan Set native VLAN when interface is in trunking mode

* S1(config-if)#switchport trunk native vlan ?
* <1-4094> VLAN ID of the native VLAN when this port is in trunking mode
* S1(config-if)#switchport trunk native vlan 40
* S1(config-if)#^Z
* So we’ve changed our native VLAN on our trunk link to 40
* S1(config-if)#no switchport trunk native vlan
* Now our trunk link is using the default VLAN 1 as the native VLAN.



Revision no.: PPT/2K804/04



# Configuring Inter-VLAN Routing

## Hosts that are members of the same VLAN can communicate.



* To allow inter-VLAN communication to be possible, you need a router or a layer 3 switch.
* To support ISL or 802.1Q routing on a FastEthernet interface, the router’s interface is divided into logical interfaces—one for each VLAN. These are called subinterfaces.
* You cannot provide trunking between the 1900 and 2950 switch by default because the 1900 switch only supports ISL routing and the 2950 switch only supports 802.1Q routing.
* You can set the interface to trunk with the encapsulation

command.



Revision no.: PPT/2K804/04



**Configuring Inter-VLAN Routing (contd.)**

## For a connection to a 1900 trunk port (ISL), use the following command:



2600#**config t**

2600(config)#**int f0/0.1**

2600(config-subif)#**encapsulation isl** vlan#

## For a router trunk connection to a 2950 switch (802.1Q), use the following command:

2600(config)#int f0/0.1

2600(config-subif)#encapsulation dot1q vlan#



Revision no.: PPT/2K804/04



# Configuring VTP

## Both the Catalyst 1900 and 2950 switches—actually, all switches—are configured to be VTP servers by default.



* To configure VTP, first you have to configure the domain name you want to use.



Revision no.: PPT/2K804/04



**Configuring VTP (contd.)**

## Once you configure the VTP information on a switch, you need to verify it.



1900(config)#**vtp ?**

client VTP client

domain Set VTP domain name password Set VTP password pruning VTP pruning

server VTP server transparent VTP transparent trap VTP trap 1900(config)#**vtp server**

1900(config)#**vtp domain lammle**

1900(config)#vtp password todd



Revision no.: PPT/2K804/04



**Configuring VTP (contd.)**

## You can verify VTP information, with the show vtp command:



1900#**sh vtp**

VTP version: 1

Configuration revision: 0

Maximum VLANs supported locally: 1005 Number of existing VLANs: 5

VTP domain name : lammle VTP password : todd

VTP operating mode : Server VTP pruning mode : Disabled VTP traps generation : Enabled

Configuration last modified by: 0.0.0.0 at 00-00-0000 00:00:00

1900#



Revision no.: PPT/2K804/04



**Configuring VTP (contd.)**

* To configure VTP on the 2950 switch, configure the domain name to be use first.



.

* Configure the VTP information on a switch to verify it.
* Use the vtp global configuration mode command to set this information.

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 mode server**

Device mode already VTP SERVER. Switch(config)#**vtp domain ?**

WORD The ascii name for the VTP administrative domain.

Switch(config)#**vtp domain routersim**

Changing VTP domain name from NULL to routersim Switch(config)#



Revision no.: PPT/2K804/04



**Configuring VTP (contd.)**

## After configuring the VTP information, verify it with the show vtp command:



SwitchA#sh vtp status VTP Version : 2

Configuration Revision : 1

Maximum VLANs supported locally : 64 Number of existing VLANs : 7

VTP Operating Mode : Server VTP Domain Name : routersim VTP Pruning Mode : Disabled VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x4C 0x60 0xA6 0x5D 0xD7 0x41 0x8C 0x37 Configuration last modified by 172.16.10.1 at 3-1-94 06:40:09

Local updater ID is 172.16.10.1 on interface Vl1 (lowest numbered VLAN interfacefound)



Revision no.: PPT/2K804/04



# Telephony: Configuring Voice VLANs

* The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.



* When a switch is connected to a Cisco IP phone, the IP phone sends voice traffic with layer 3 IP precedence and layer 2 class of service (CoS) values, which are both set to 5 for voice traffic, all other traffic defaults to 0.



Revision no.: PPT/2K804/04



* Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent,the switch supports quality of service (QoS) based on IEEE 802.1p CoS.
* (802.1p provides a mechanism for implementing QoS at the MAC level.) The 802.1p field is carried in the 802.1Q trunk header.
* If you look at the fields in an 802.1Q tag, you will see a field called the priority field; this is where the 802.1p information goes.



Revision no.: PPT/2K804/04



* The Cisco IP phone is a configurable device, and you can configure it to forward traffic with an IEEE 802.1p priority.
* The Cisco phone basically has a three-port switch: one to connect to the Cisco switch, one to a PC device, and one to the actual phone, which is internal



Revision no.: PPT/2K804/04



* You can also configure an access port with an attached Cisco IP phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone—like a PC.
* You can configure access ports on the switch to send Cisco Discovery Protocol (CDP) packets that instruct an attached Cisco IP phone to send voice traffic to the switch in any of these ways:
* In the voice VLAN tagged with a layer 2 CoS priority value
* In the access VLAN tagged with a layer 2 CoS priority value
* In the access VLAN, untagged (no layer 2 CoS priority value)



Revision no.: PPT/2K804/04



* You can configure layer 2 access ports on the switch to send CDP packets that instruct the attached Cisco IP phone to configure the IP phone access port in one of these modes:
* In trusted mode, all traffic received through the access port on the Cisco IP phone passes through the IP phone unchanged.
* In untrusted mode, all traffic in IEEE 802.1Q or IEEE 802.1p frames received through the access port on the IP phone receive a configured layer 2 CoS value. The default layer 2 CoS value is 0. Untrusted mode is the default.



Revision no.: PPT/2K804/04



# Configuring the Voice VLAN

* By default, the voice VLAN feature is disabled; you enable it by using the interface command switchport voice vlan.



* When the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.
* The CoS value is not trusted for IEEE 802.1p or IEEE 802.1Q tagged traffic.



Revision no.: PPT/2K804/04



**These are the voice VLAN configuration guidelines:**

* You should configure voice VLAN on switch access ports; voice VLAN isn’t supported on trunk ports, even though you can actually configure it!
* The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on it.
* Use the show vlan privileged EXEC command to see if the VLAN is present—if it is, it’ll be listed in the display.



Revision no.: PPT/2K804/04



* Before you enable the voice VLAN, it’s recommend that you enable QoS on the switch by entering the mls qos global configuration command and set the port trust state to trust by entering the mls qos trust cos interface configuration command.
* You must make sure that CDP is enabled on the switch port connected to the Cisco IPphone to send the configuration. This is on by default, so unless you disabled it, you shouldn’t have a problem.
* The PortFast feature is automatically enabled when the voice VLAN is configured, but when you disable the voice VLAN, the PortFast feature isn’t automatically disabled.
* To return the port to its default setting, use the no switchport voice vlan interface configuration command.



Revision no.: PPT/2K804/04



# Configuring IP Phone Voice Traffic

1. How to configure a port connected to an IP phone to use the CoS value for classifying incoming traffic



1. How to configure the port to use IEEE 802.1p priority tagging for voice traffic
2. How to configure it to use the Voice VLAN (10) to carry all voice traffic
3. And last, how to configure VLAN 3 to carry PC data



Revision no.: PPT/2K804/04



* Switch#configure t

**© CMS INSTITUTE, 2004**. All rights reserved. No part of this material may be reproduced, stored or emailed without the prior permission.

* Switch(config)#mls qos
* Switch(config)#interface f0/1
* Switch(config-if)#switchport priority extend ?
* cos Override 802.1p priority of devices on appliance
* trust Trust 802.1p priorities of devices on appliance
* Switch(config-if)#switchport priority extend trust
* Switch(config-if)#mls qos trust cos
* Switch(config-if)#switchport voice vlan dot1p
* Switch(config-if)#switchport mode access
* Switch(config-if)#switchport access vlan 3
* Switch(config-if)#switchport voice vlan 10



Revision no.: PPT/2K804/04



* The command mls qos trust cos will configure the interface to classify incoming traffic.
* packets by using the packet CoS value. For untagged packets, the port’s default CoS value will be used.
* But before configuring the port trust state, you must first globally enable QoS by using the mls qos global configuration command.
* We added two access VLANs to the same port, you can only do this if u have one for a data VLAN and another one for a voice VLAN.

**Note**: We can use CNA to Configure VLANs and Inter-VLAN Routing



Revision no.: PPT/2K804/04

permission.

prior the

without

emailed or

stored d,

reproduce be

may

material

this of

part No

reserved.

rights All

.

**2004**

**INSTITUTE, CMS**

**©**



**Design & Published by:**