

# CCNA

640-802

**Layer 2 switching and Spanning Tree Protocol (STP):**







Revision no.: PPT/2K804/04

Revision no.: PPT/2K804/04



**What is Switching ?**

* It breaks the Collision Domain



* It takes the packet and forwards to destined port without any modification.
* Network still remains in one large Broadcast Domain.
* It increases bandwidth of the network.
* Multiple devices can be connected to each interface.



Revision no.: PPT/2K804/04



**Switches versus Bridges**

* Switches are nothing but bridges with more ports, with certain important differences:



* + Bridges are software based while Switches are hardware based. Using ASICs chip to make filtering decision.
  + Bridges can only have one Spanning-Tree Instance per bridge, while switches can have many.
  + Bridges can have only 16 ports, while switches can have hundreds
  + Bridges are self managed while switches are manageable.



Revision no.: PPT/2K804/04



**Switching Technology**

* To understand Switching Technology we need to understand the following :



* + Layer 2 Switching
  + Address Learning
  + Forward/Filtering Decisions
  + Loop Avoidance
  + Spanning-Tree Protocol
  + LAN Switch Types



Revision no.: PPT/2K804/04



**Layer 2 Switching**

* This is hardware based switching



* It uses MAC address to filter the network.
* To build Filter Table, it uses ASICs (Application-specific Integrated Circuits)
* It is like Multiport bridge.
* Layer 2 switches do not look at the Network layer header and hence faster.



Revision no.: PPT/2K804/04



**Layer 2 Switching (contd.)**

* Based on hardware address it decides whether to forward the packet or drop it.



* Layer 2 Switching provides the following:

###### Hardware-based bridging (MAC)

* + Wire speed
    - Layer 2 switch is considered faster because no modification in the packet.

###### Low Latency

* + - Because the switching is faster

###### Low cost



Revision no.: PPT/2K804/04



**Functions of Switch at Layer 2**

* There are three main functions at Layer2



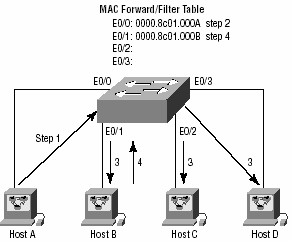
* + Address Learning
  + Forward / Filter Decisions
  + Loop Avoidance



Revision no.: PPT/2K804/04



**Address Learning**

* Switches and Bridges remember the source address of each frame received on an interface and enter this information into MAC database.



* + Whenever switch receives a packet it makes an entry of the source address and sends a broadcast for destination.
  + The destination machine then responds to broadcast and switch receives a packet from destination.
  + Switch again makes entry for the destination machine’s hardware address.
  + Using this method Switch maintains a table stating that which hardware address is available at which port.



Revision no.: PPT/2K804/04



**Forward / Filter Decisions**

* When a frame is received on an interface, the switch looks at the destination hardware address and finds the exit interface in the MAC database.



* + When a frame is reached to the switch the destination port is checked in MAC database to find out the exit interface.
  + If found the packet will be forwarded to the mentioned port
  + If not found the Broadcast / Multicast is sent on all the ports and the exit port for this particular address is determined.



Revision no.: PPT/2K804/04



**Broadcast /Multicast**

* When packets are sent to a specific machine that is called Unicast.



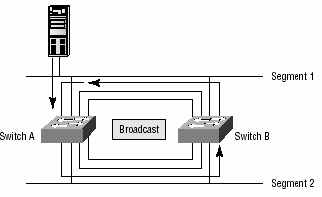
* It always knows the destination address.
* When packets are sent to few selected or a group of machines that is called Multicast.
* This does not know the destination no. but it knows the network no. (few 1s &0s and rest all 1s).
* When packets are sent to all that is called Broadcast.
* It the destination address will be all 1s.



Revision no.: PPT/2K804/04



**Loop Avoidance**

* + If multiple connections between switches are created for redundancy, network loops can occur.



* + - Most commonly networks are implemented with redundant links for fault tolerance purpose.
    - These multiple links may cause loops and broadcast storm
    - In a switched network some scheme should be implemented to avoid these loops.
    - The Spanning-Tree Protocol (STP) is used to stop network loops and allow redundancy.



Revision no.: PPT/2K804/04



**Loop Occurring**

* In this scenario if no loop avoidance scheme is implemented the switch will generate a broadcast storm.



* A device can receive multiple copy of same frames.
* The MAC address table will be continuously updated and the table itself will be confused, because frames will be received from more than one link. This is called “thrashing” MAC Table.
* This is how loops within other loop will be generated and no switching will be performed in the network.
* Note : Spanning Tree Protocol is designed to solve this problem.



Revision no.: PPT/2K804/04



**Spanning-Tree Protocol**

* The main function of STP is to maintain a loop free network.



* Originally STP was created by DEC (Now Compaq)
* It was modified by IEEE and was published in 802.1d specification.
* DEC and IEEE 802.1d are not compatible
* All CISCO switches run on IEEE802.1d version of STP
* STP uses the spanning-tree algorithm (STA) to first create a topology database, then search out and destroy redundant links.







Revision no.: PPT/2K804/04

**Spanning Tree Terms**



Revision no.: PPT/2K804/04



**Spanning Tree Operations**

* Selecting the Root Bridge



* Selecting the Designated Port
* Spanning-Tree Port States
* Convergence



Revision no.: PPT/2K804/04



**Selecting Root Bridge**

* In one Broadcast Domain only one Bridge is designated as Root Bridge.



* All Ports on the Root Bridge are in Forwarding State and are called Designated Port
* All ports in forwarding state can send and receive traffic.
* Bridge ID is used to determine the Root Bridge and Root Port.
* Bridge ID includes the priority and the MAC Address of the device.



Revision no.: PPT/2K804/04



**Selecting the Designated Port**

* There will be only one Designated Port in one Segment.



* Designated Port is selected on the bridge that has the lowest cost path to Root Bridge.
* Designated Port is in the forwarding state.
* Responsible for forwarding traffic for the segmentation
  + Nondesignated Ports are normally in the blocking state to break the loop topology. That means the Spanning Tree is preventing it from forwarding traffic.



Revision no.: PPT/2K804/04



**Selecting the Designated Port (contd.)**

* Typical Costs of Different Ethernet Networks



|  |  |  |
| --- | --- | --- |
| **Speed** | **New IEEE Cost** | **Original IEEE Cost** |
| 10Gbps | 2 | 1 |
| 1Gbps | 4 | 1 |
| 100Mbps | 19 | 10 |
| 10Mbps | 100 | 100 |



Revision no.: PPT/2K804/04



**Spanning Tree Port State**

* There are four different states for ports on Switch / Bridge running STP.



* + **Blocking** : Won’t forward frames; listens to BPDUs. All ports are in blocking state by default when the switch is powered up.
  + **Listening** : Listens to BPDUs to make sure no loops occur on the network before passing data frames.
  + **Learning** : Learns MAC addresses and builds a filter table but does not forward frames.
  + **Forwarding** : Sends and receives all data on the bridged port.



Revision no.: PPT/2K804/04



**Convergence**

* Convergence occurs when bridges and switches have transitioned to either the forwarding or blocking states.



* No data is forwarded during this time.
* Convergence is important to make sure all devices have the same database.
  + Before data can be forwarded, all devices must be updated.
  + The problem with convergence is the time it takes for these devices to update.
  + It usually takes 50 seconds to got from Blocking to forwarding state.
  + Forward delay is the time it takes to transition a port from listening to learning state or from learning to forwarding state.



Revision no.: PPT/2K804/04



**Spanning Tree Timers**

|  |  |  |
| --- | --- | --- |
| Timer | Primary Function | Default Setting |
| Hello Time | Time between sending of configuration BPDUs by the root Bridge | 2 seconds |
| Forward Delay | Duration of listening and learning states | 30 seconds |
| Max Age | Time BPDU stored | 20 seconds |

* It is not recommended that you change the default STP Timers, but the timers can be adjusted if necessary.



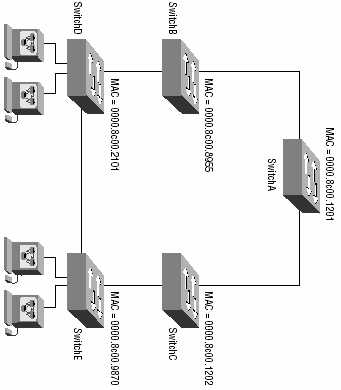






Revision no.: PPT/2K804/04

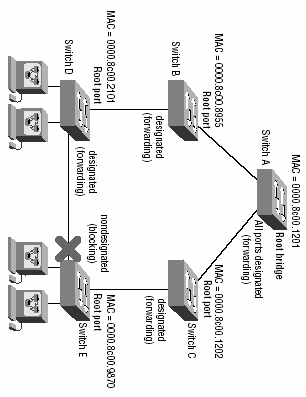
**Spanning Tree Example**







Revision no.: PPT/2K804/04



**Spanning Tree Example (contd.)**

Revision no.: PPT/2K804/04



**Spanning Tree PortFast**

* If you have a server or other devices connected into your switch that you’re totally sure won’t create a switching loop if STP is disabled, you can use something called portfast on these ports. If the portfast is enabled the port won’t spend the usual 50 seconds to come up into forwarding mode while STP is converging.



* Switch(config-if)#**spanning-tree portfast ?**

#### disable Disable portfast for this interface

* trunk Enable portfast on the interface even in trunk mode<cr>



Revision no.: PPT/2K804/04



* Switch(config-if)#**spanning-tree portfast**

#### %Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.

* Use with CAUTION
* %Portfast has been configured on FastEthernet0/1 but will only have effect when the interface is in a non-trunking mode.
* Switch(config-if)#



Revision no.: PPT/2K804/04



* The range command, you can use on switches to help you configure multiple ports at the same time.
* Switch(config)#**int range fastEthernet 0/1 - 12**
* Switch(config-if-range)#**spanning-tree portfast**

#### The preceding range command allows me to set all 12 of my switch ports into portfast mode by typing in one command and then simply pressing the Enter key.

* **Note:** I also want you to know that the interface range command can be used in conjunction with any command.



Revision no.: PPT/2K804/04



**Spanning Tree UplinkFast**

* UplinkFast is a Cisco-specific feature that improves the convergence time of STP in case of a link failure. The UplinkFast feature is designed to run in a switched environment when the switch has at least one alternate/backup root port (a port in blocking state).



* UplinkFast allows a switch to find alternate paths to the root bridge before the primary link fails. This means that if the primary link fails, the secondary link would come up more quickly—the port wouldn’t wait for the normal STP convergence time of 50 seconds



Revision no.: PPT/2K804/04



**Spanning Tree BackboneFast**

* BackboneFast is used for speeding up convergence.



* BackboneFast should be enabled on all Catalyst switches to allow for detection of indirect link failures.
* Enabling BackboneFast is also beneficial because it starts the spanning tree reconfiguration more quickly—it can save 20 seconds on the default 50-second STP convergence time.



Revision no.: PPT/2K804/04



**Rapid Spanning Tree Protocol (RSTP) 802.1w**

* Cisco created PortFast, UplinkFast, and BackboneFast to “fix” the holes and liabilities the IEEE 802.1d standard presented.



* The drawbacks to these enhancements are only that they are Cisco proprietary and need additional configuration.
* But the new 802.1w standard (RSTP) addresses all these issues.



Revision no.: PPT/2K804/04



**EtherChannel**

* Instead of having redundant links and allowing STP to put one of the links in BLK (blocked) mode, we can bundle the links and create a logical aggregation so that our multiple links will then appear as a single one. Since doing this would still provide the same redundancy as STP.



* There are two versions of EtherChannel there’s the Cisco version of EtherChannel and the IEEE version : Cisco’s version is called Port Aggregation Protocol (PAgP) and the IEEE 802.3ad standard is called Link Aggregation Control Protocol (LACP).
* Both versions work equally as well, but how you configure each is different



Revision no.: PPT/2K804/04

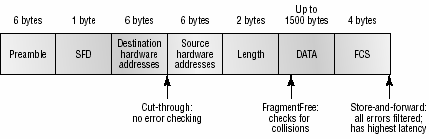


**LAN Switch Types**

* Switching type basically effects the Latency and the reliability of your network.



* There are three Switching Types:
  + Store and Forward
  + Cut-through
  + FragmentFree



Revision no.: PPT/2K804/04



**Store and Forward**

* It is default in Routers & Bridges



* In this method the entire data is first stored, processed for errors, if it is found error free, it is forwarded otherwise returned.
* Uses CRC for error checking.
* Latency is high in this case but it is extremely reliable.
  + Latency : Time involved in sending the data from one node to another

Revision no.: PPT/2K804/04



**Cut-Through (Real Time)**

* Cut-Through switching is the fastest one, because it does not check for errors.



* It does not store data and process for error.
* It just reads the destination address and forwards it.
* It begins to forward the frame as soon as it reads the destination address and determines the outgoing interface.
* It has Lowest Latency and not reliable.
* Hence it is also called Wire Speed Switching.



Revision no.: PPT/2K804/04



**FragmentFree (Modified Cut-Through)**

* It provides us both Low latency as well as Speed.



* It is a modified form of Cut Through switching.
* It reads the first 64 bytes and then forwards.
  + It checks 64 bytes because most of the errors occur in these bytes only. If first 64 bytes are error free FragmentFree Switching considers entire data error free.
* If there is any error in first 64 bytes the packet will be dropped or else forwarded.
* It provides better reliability than the Cut-through with almost same Latency as in Cut through.



Revision no.: PPT/2K804/04



**Configuring the Catalyst 1900 and 2950 Switches**

* This Section covers the following:
  + Setting the passwords



* + Setting the hostname
  + Configuring the IP address and subnet mask
  + Setting a description on the interfaces
  + Erasing the switch configurations
  + Configuring VLANs
  + Adding VLAN memberships to switch ports
  + Creating a VTP domain
  + Configuring trunking



Revision no.: PPT/2K804/04



**1900 and 2950 Switch Startup**

* The Catalyst 1900 Switch



* 1 user(s) now active on Management Console.
* User Interface Menu
* [M] Menus
* [K] Command Line
* [I] IP Configuration
* Enter Selection: K
* CLI session with the switch is open.
* To end the CLI session, enter [Exit].
* >



Revision no.: PPT/2K804/04



**1900 and 2950 Switch Startup (contd.)**

## The Catalyst 2950 Switch



* --- System Configuration Dialog ---
* Would you like to enter the initial configuration dialog? [yes/no]: no
* Press RETURN to get started!
* 00:04:53: %LINK-5-CHANGED: Interface Vlan1, changed state to
* administratively down
* 00:04:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
* changed state to down
* Switch>



Revision no.: PPT/2K804/04



**Setting the Passwords**

* Understanding Passwords



* Passwords are not case sensitive.
* Passwords cannot be less than 4 character and more than 8 characters.
* You need to set passwords separately for :
  + User Mode
  + Privilege Mode.



Revision no.: PPT/2K804/04



**Setting the User Mode and Enable Mode Passwords for 1900 catalyst switch**



* Use level 1 for User Mode
* Use level 15 for Enable Mode
* >enable
* #config t
* Enter configuration commands, one per line. End with CNTL/Z.
* (config)#enable password level 1 todd
* (config)#enable password level 15 todd1
* (config)#exit
* #exit



Revision no.: PPT/2K804/04



**Setting the User Mode and Enable Mode Passwords for 2950 catalyst switch**



Switch>**enable** Switch#**config t**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#**line vty 0 15** Switch(config-line)#**login** Switch(config-line)#**password telnet** Switch(config-line)#**line con 0** Switch(config-line)#**login** Switch(config-line)#**password todd** Switch(config-line)#**exit** Switch(config)#**exit**

##### Switch#



Revision no.: PPT/2K804/04



**Setting the Enable Secret Password**

* The enable secret password is a more secure password and it supersedes the enable password if it is set .



* Enable password for 1900 (config)#enable secret todd2
* Enable password for 2950 Switch(config)#enable secret todd1



Revision no.: PPT/2K804/04



**Setting the Hostname**

* Setting hostname in 1900 switch



* #config t
* Enter configuration commands, one per line. End with CNTL/Z
* config)#hostname Todd1900
* Todd1900(config)#
* Setting hostname in 2950 switch
* Switch(config)#hostname Todd2950
* Todd2950(config)#



Revision no.: PPT/2K804/04



**Setting IP Information**

* Setting ip information for 1900 switch



* Todd1900#config t
* Enter configuration commands, one per line. End with CNTL/Z
* Todd1900(config)#ip address 172.16.10.16 255.255.255.0
* Todd1900(config)#ip default-gateway 172.16.10.1
* Todd1900(config)#



Revision no.: PPT/2K804/04



**Setting IP Information (contd.) …**

## Setting ip information for 2950 switch



###### Todd2950#config t

Enter configuration commands, one per line. End with CNTL/Z. Todd2950(config)#int vlan1

Todd2950(config-if)#ip address 172.16.10.17 255.255.255.0 Todd2950(config-if)#no shut

Todd2950(config-if)#exit

00:22:01: %LINK-3-UPDOWN: Interface Vlan1, changed state to up

00:22:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Todd2950(config)#ip default-gateway 172.16.10.1 Todd2950(config)#

* Ip address is actually configure under the VLAN1 interface, Every port on every switch is a member of VLAN1 by default.
* An IP address is set “for” the switch so you can manage the thing inband (through the network).



Revision no.: PPT/2K804/04



**Configuring Interface Descriptions**

* Setting Interface Descriptions in 1900 switchTodd1900



#**config t**

###### Enter configuration commands, one per line. End with CNTL/Z Todd1900(config)#**int e0/1**

Todd1900(config-if)#**description Finance\_VLAN**

Todd1900(config-if)#**int f0/26**

Todd1900(config-if)#**description trunk\_to\_Building\_4**

###### Todd1900(config-if)#



Revision no.: PPT/2K804/04



**Configuring Interface Descriptions (contd.)**

* Setting Interface Descriptions in 2950 switch



Todd2950(config)#**int fastEthernet 0/?**

<0-12> FastEthernet interface number Todd2950(config)#**int fastEthernet 0/1** Todd2950(config-if)#**description Sales Printer** Todd2950(config-if)#**int f0/12**

Todd2950(config-if)#**description Connection to backbone**

###### Todd2950(config-if)#**^Z** Todd2950#



Revision no.: PPT/2K804/04



**Erasing the Switch Configuration**

* Switch configuration is stored in NVRAM



* ***Startup-config*** stored in NVRAM cannot be viewed.
* Contents modified in ***running-config*** is automatically stored in NVRAM.
* In routers you need to ***copy running-config*** to ***startup****-* ***config*** whereas in switches not.

## Use “delete nvram” command from global configuration mode to erase switch configuration.

* But the 2950 switch has a ***running****-****config*** and a ***startup****-* ***config***. You save the configuration with the ***copy run start*** command, and you can erase the contents of NVRAM with the erase startup-config command.



Revision no.: PPT/2K804/04



**Erasing the Switch Configuration (contd.)**

* To delete the contents of NVRAM to the factory default settings.



Todd1900#**delete ?**

nvram NVRAM configuration

vtp Reset VTP configuration to defaults Todd1900#**delete nvram**

This command resets the switch with factory defaults. All system

parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

Reset system with factory defaults, [Y]es or [N]o? **Yes**

* Notice the message the 1900 gave me when I used the delete nvram command—once you say yes, the configuration is gone!



Revision no.: PPT/2K804/04



**Erasing the Switch Configuration (contd.)**

* + To delete the 2950, you just type **erase startup-config**



## from the privileged mode prompt like this:

Todd2950#**erase startup-config**

###### Erasing the nvram filesystem will remove all files! Continue? [confirm] **(enter)**

[OK]

Erase of nvram: complete Todd2950#

* + Unlike the 1900, when you erase the configuration on the 2950, you have to reload the switch before the running- config will actually be deleted.



Revision no.: PPT/2K804/04



**Configuring Catalyst Switches**

**Port Security**



* By using port security, you can limit the number of MAC addresses that can be assigned dynamically to a port.
* A secured switch port can associate anywhere from 1 to 8,192 MAC addresses, but the ’50 series can support only 192.
* You can choose to allow the switch to learn these values dynamically, or you can set a static address for each port using the switchport port-security mac-address *mac-address* command.



Revision no.: PPT/2K804/04



S1#**config t**

Enter configuration commands, one per line. End with CNTL/Z. S1(config)#**int range fa0/3 - 4**

S1(config-if-range)#**switchport port-security maximum ?**

###### <1-8192> Maximum addresses

S1(config-if-range)#**switchport port-security maximum 1** S1(config-if-range)#**switchport port-security mac-address sticky** S1(config-if-range)#**switchport port-security violation ?**

###### protect Security violation protect mode restrict Security violation restrict mode shutdown Security violation shutdown mode

S1(config-if-range)#**switchport port-security violation shutdown**

###### S1(config-if-range)#**exit**

****

Revision no.: PPT/2K804/04



**PortFast**

S1#**config t**

S1(config)#**int range f0/3-4**

S1(config-if-range)#**spanning-tree portfast ?**

disable Disable portfast for this interface

trunk Enable portfast on the interface even in trunk mode <cr>



Revision no.: PPT/2K804/04



S1(config-if-range)#**spanning-tree portfast**

#### %Warning: portfast should only be enabled on ports connected to a single host.

* Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.
* Use with CAUTION
* %Portfast has been configured on FastEthernet0/2 but will only have effect when the interface is in a non-trunking mode.
* S1(config-if-range)#



Revision no.: PPT/2K804/04



**UplinkFast**

Here’s how to configure UplinkFast on our Access layer switches (S1 and S2): S1#**config t**

S1(config)#**spanning-tree uplinkfast**

S2#**config t**

S2(config)#**spanning-tree uplinkfast** S1(config)#**do show spanning-tree uplinkfast** UplinkFast is enabled

Station update rate set to 150 packets/sec. UplinkFast statistics



Revision no.: PPT/2K804/04



* Number of transitions via uplinkFast (all VLANs) : 1
* Number of proxy multicast addresses transmitted (all VLANs) : 8
* Name Interface List
* VLAN0001 Fa0/1(fwd), Fa0/2
* S1(config)#
* The uplinkfast command is a global command and it’s enabled on every port



Revision no.: PPT/2K804/04



**RSTP (802.1w)**

Core#**config t**



Core(config)#**spanning-tree mode ?**

#### mst Multiple spanning tree mode

pvst Per-Vlan spanning tree mode rapid-pvst Per-Vlan rapid spanning tree mode



Revision no.: PPT/2K804/04



* Core(config)#**spanning-tree mode rapid-pvst**

#### Core(config)#

* 1d02h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
* 1d02h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up



Revision no.: PPT/2K804/04



* The Core switch is now running the 802.1w STP. verify it by this command.

.

* Core(config)#**do show spanning-tree**

#### VLAN0001

* Spanning tree enabled protocol rstp
* Root ID Priority 32769
* Address 000d.29bd.4b80



Revision no.: PPT/2K804/04



This bridge is the root

* Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
* Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
* Address 000d.29bd.4b80
* Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
* Aging Time 300
* Interface Role Sts Cost Prio.Nbr Type



Revision no.: PPT/2K804/04



Fa0/5 Desg FWD 19 128.5 P2p Peer(STP) Fa0/6 Desg FWD 19 128.6 P2p Peer(STP) Fa0/7 Desg FWD 19 128.7 P2p Peer(STP) Fa0/8 Desg FWD 19 128.8 P2p Peer(STP)



Revision no.: PPT/2K804/04



**Verifying Cisco Catalyst Switches**

* To verify the IP address set on a switch, we can use the show interface command.
* S1#**sh int vlan 1**
* It displays the forward filter table, also called a content addressable memory (CAM) table.
* S1#**sh mac address-table**

****

Revision no.: PPT/2K804/04



**Assigning Static MAC Addresses**

* S1#**config t**
* S1(config)#**mac-address-table static aaaa.bbbb.cccc vlan 1 int fa0/5**
* S1(config)#**do show mac address-table**
* *With* ***show spanning-tree***, you can see who the root bridge is and what our priorities are set to for each VLAN.

### S1#sh spanning-tree

****

Revision no.: PPT/2K804/04



**Cisco Network Assistant**

* The Cisco Network Assistant (CNA) can make configuring your switches a breeze, which, as with the SDM, is both good and bad.



* It’s good in that it makes it easier for us to create much harder configs, and it’s bad because it makes it easier for everyone else to do that as well.
* But still, it can be a little tricky at first, so download it and get familiar with the CAN as much as possible



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:**