

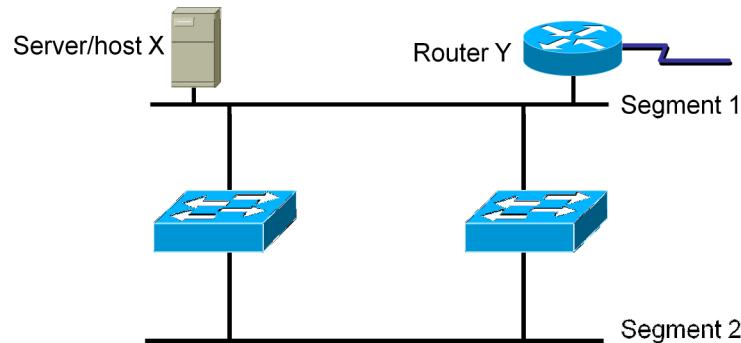
# Implementing Spanning Tree

## Chapter 3

Copyright 2012 CertificationKits LLC. All Rights Reserved.



# Redundant Topology



- Redundant topology eliminates single points of failure
- Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems

Copyright 2012 CertificationKits LLC All Rights Reserved



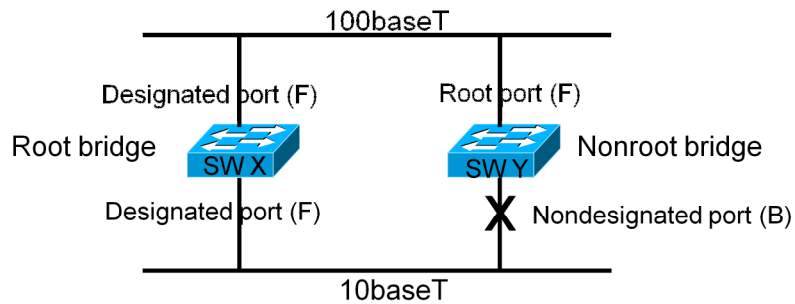
Spanning Tree Protocol is a bridge protocol that enables a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange Bridge Protocol Data Unit (BPDU) messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces.

Spanning Tree Protocol is a standardized technique for maintaining a network of multiple bridges or switches. When the topology changes, Spanning Tree Protocol transparently reconfigures bridges and switches to avoid the creation of loops by placing ports in a forwarding or blocking state. Each VLAN is treated as a separate bridge and a separate instance of Spanning Tree Protocol is applied to each. Spanning Tree Protocol parameters are set for each VLAN. For each spanning tree instance, you configure a set of global options with a set of port parameters. The port parameter list contains only ports that are members of a given VLAN. A maximum of 64 spanning tree instances are supported, one for each VLAN.

STP provides a loop free redundant network topology by placing certain ports in the blocking state. STP uses the Spanning Tree Algorithm (STA) to find redundant links and shut them down. STP's main task is to stop network loops from occurring on your layer-2 network (bridges or switches). It vigilantly monitors the network to find all links, making sure that no loops occur by shutting down any redundant ones.

# Spanning-Tree Operations

- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment

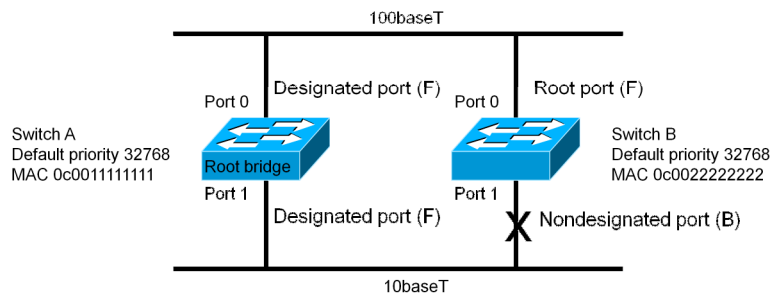


Copyright 2012 CertificationKits LLC All Rights Reserved



A switch performs spanning tree by default. The default settings will elect a root bridge and calculate the shortest path from every switch to the root

# STP Port States



CertificationKits

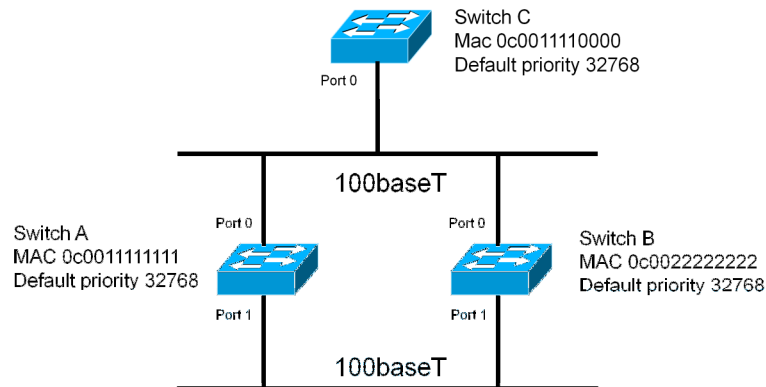
Copyright 2012 CertificationKits LLC All Rights Reserved

Active Ports will have the lowest combination of:

- Root Path Cost
- Bridge ID (of upstream bridge)
- Port ID

Path from any switch to the root will travel either directly to the root bridge or through a parent or “designated” switch. Blocked ports continue to send/receive BPDUs but NOT DATA.

# Spanning-Tree



Can you figure out:

- What is the root bridge?
- What are the designated, nondesignated, and root ports?
- Which are the forwarding and blocking ports?



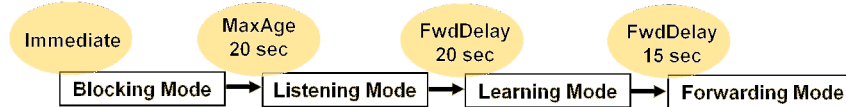
CertificationKits

Copyright 2012 CertificationKits LLC All Rights Reserved

Switch C will become the Root Bridge because it has the lowest Bridge ID. Port 0 on Switch A and Port 0 on Switch B will become the Root Port, Port 1 on switch A will become the designated port because the port has a lower port ID.

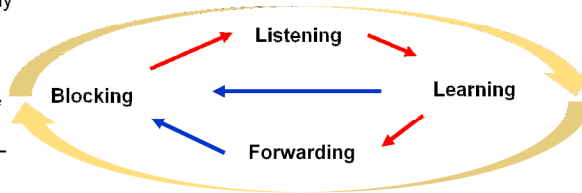
# STP State Transitions

## Port STP Timer Time Line



Ports can be disabled administratively or because of h/w failure or deletion of a ports native VLAN

During recalculation of spanning tree old/useless MAC entries will remain in the CAM table – Spanning Tree will Force an faster purge of these entries



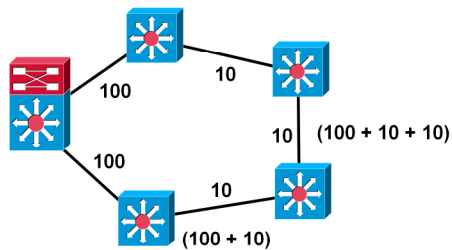
**CertificationKits**

Copyright 2012 CertificationKits LLC All Rights Reserved

- Disabled = Administratively Down
- Blocking = Receiving BPDUs
- Listening = Sending and Receiving BPDUs (building the topology)
- Learning = Populating CAM table
- Forwarding = Sending/Receiving User Data

# Calculating Root Path Cost

<u>Link Speed</u>	<u>Cost</u>
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100



Cost is calculated as  $1000/BW$  (in mbps) on older switches

New switches use a non-linear scale: 100mbps = 19  
1000mbps = 4



**CertificationKits**

Copyright 2012 CertificationKits LLC All Rights Reserved

Path cost is a function of bandwidth of each path. It can be changed using a switch port cost parameter. Is determined by the sum of port costs between source and destination.

# BPDU Timers

Bytes	Field
2	Protocol ID
1	Version
1	Message Type
1	Flags
8	Root ID
4	Cost of Path
8	Bridge ID
2	Port ID
2	Message Age
2	Maximum Time
2	Hello Time
2	Forward Delay

Timers Are Propagated  
from the Root Bridge

- Timers are used to prevent bridging loops
- Timers determine how long it will take spanning tree to converge after a failure
- Hello – 2s
- MaxTime/MaxAge– 20s
- Forward Delay – 15s



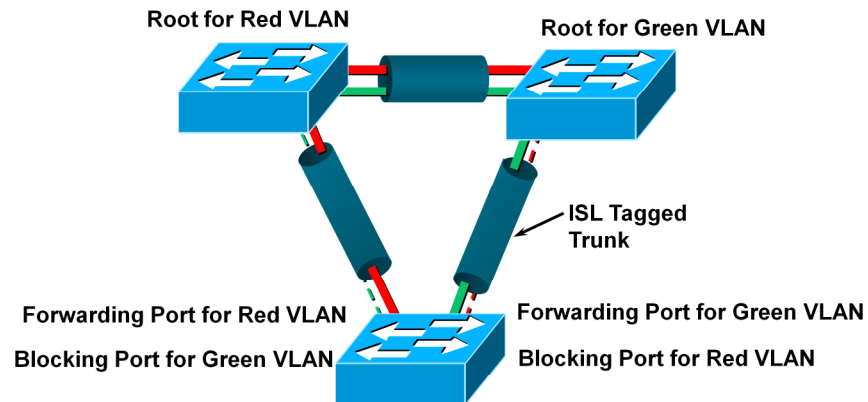
CertificationKits

Copyright 2012 CertificationKits LLC All Rights Reserved

BPDU timers are set by the Root bridge. By default the hello interval is set to once every 2 seconds. Why so often? To avoid loops!



# PVST



Copyright 2012 CertificationKits LLC All Rights Reserved



Per VLAN Spanning Tree allows the network administrator to control the forwarding paths on per vlan basis. It also creates a flexible design tool for traffic management that will give you the capability to provide layer 2 redundancy.

# Enabling Spanning Tree

```
Switch(config)# spanning-tree vlan 200
```

- Enables spanning tree on a specific VLAN

```
Switch(config)# spanning-tree vlan 200 priority 4096
```

- Lowers the spantree priority, forcing this switch to be the root bridge

```
Switch(config)# spanning-tree vlan 200 priority 8192
```

- Sets spantree priority, enabling this switch to be the alt. root bridge

```
Switch(config-if)# spanning-tree cost 18
```

- Configures the spanning tree port cost of an interface

```
Switch(config-if)# spanning-tree vlan 200 cost 17
```

- Spanning tree VLAN port cost of an interface for a VLAN

Copyright 2012 CertificationKits LLC All Rights Reserved



Wow, the whole enchilada. We placed a bullet point under each of the commands to help you digest what is going on in these examples. All of the above is not necessary to configure spanning-tree, but it shows the flexibility in dictating which switch will become the root bridge.

# Verifying STP

```
Switch# show spanning-tree vlan vlan-id
```

- Displays spanning-tree configuration information

```
ASW11# show spanning-tree vlan 200
```

VLAN0200

Spanning tree enabled protocol ieee

Root ID Priority 49352

Address 0008.2199.2bc0

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 49352 (priority 49152 sys-id-ext 200)

Address 0008.2199.2bc0

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Uplinkfast enabled

Interface Name	Port ID Prio.Nbr	Designated Cost Sts	Port ID Cost Bridge ID	Port ID Prio.Nbr
Fa0/1	128.1	3019 LIS	0 49352 0008.2199.2bc0	128.1
Fa0/2	128.2	3019 LIS	0 49352 0008.2199.2bc0	128.2

Copyright 2012 CertificationKits LLC All Rights Reserved



To display information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

The keywords and arguments that are available with the **show spanning-tree** command will vary depending on the platform you are using and the network modules that are installed and operational. The example on the slide shows the “vlan” argument being utilized.

# Spanning Tree Protocol (STP)

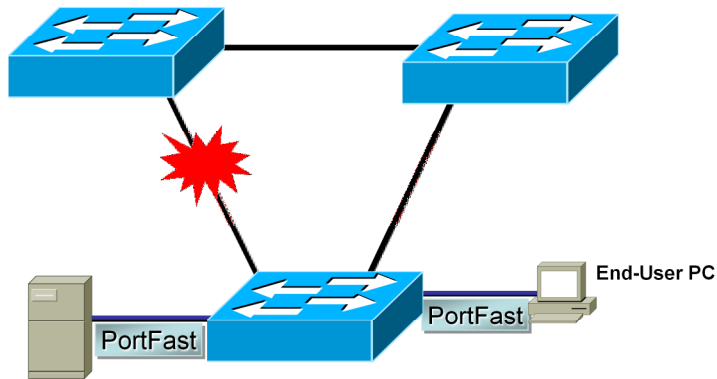
## Speeding up STP



**CertificationKits**

Copyright 2012 CertificationKits LLC. All Rights Reserved.

# What Is PortFast?



From within Interface Configuration mode, issue the following command to enable PortFast:

**spanning-tree portfast**

Copyright 2012 CertificationKits LLC All Rights Reserved



Portfast is used to minimize server or workstation downtime. Portfast is configured on a port to port basis. Be careful to only enable Portfast on ports that are connected directly to end hosts (i.e. servers or PCs), not to other switches.

# Enabling and Verifying PortFast

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

- Enables PortFast on an interface

```
Switch# show running-config interface {{fastethernet|  
gigabitethernet} slot/port}|{port-channel pc_number}
```

- Displays PortFast interface configuration information

```
Switch# show running-config interface fastethernet 5/8  
Building configuration..  
Current configuration:  
  
interface FastEthernet5/8  
no ip address  
switchport  
switchport access vlan 200  
switchport mode access  
spanning-tree portfast  
end
```



CertificationKits

Copyright 2012 CertificationKits LLC All Rights Reserved

Note: You should use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops.

## Protecting STP w/Portfast Enabled

- BPDU Guard
  - Receiving BPDUs puts the port in “error disable” state
- BPDU Filtering
  - Receiving BPDUs turns off Portfast and resumes normal STP operation.
- Root Guard
  - Moves ports that receive superior BPDUs to the “root inconsistent” state.



CertificationKits

Copyright 2012 CertificationKits LLC All Rights Reserved

# Enabling and Verifying BPDU Guard

```
Switch(config)# spanning-tree portfast bpduguard
```

- Enables BPDU Guard

```
Switch# show spanning-tree summary totals
```

- Displays BPDU Guard configuration information

```
Switch# show spanning-tree summary totals
```

```
Root bridge for: none.  
PortFast BPDU Guard is enabled  
Etherchannel misconfiguration guard is enabled  
UplinkFast is disabled  
BackboneFast is disabled  
Default pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
34 VLANs	0	0	0	36	36

Copyright 2012 CertificationKits LLC All Rights Reserved

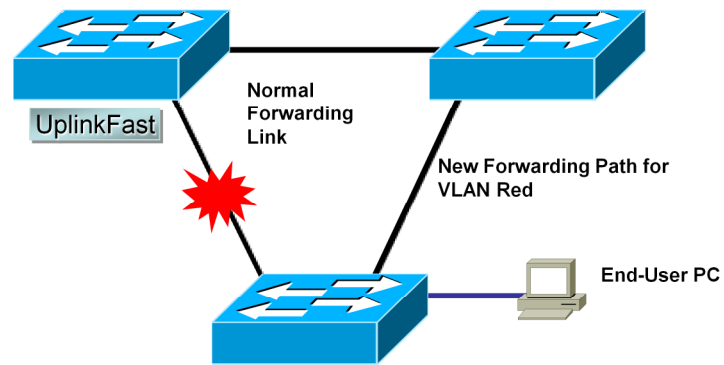


CertificationKits

If a port with bpduguard enabled receives a BPDU, the port will be placed in errordisable state.



## What Is UplinkFast?



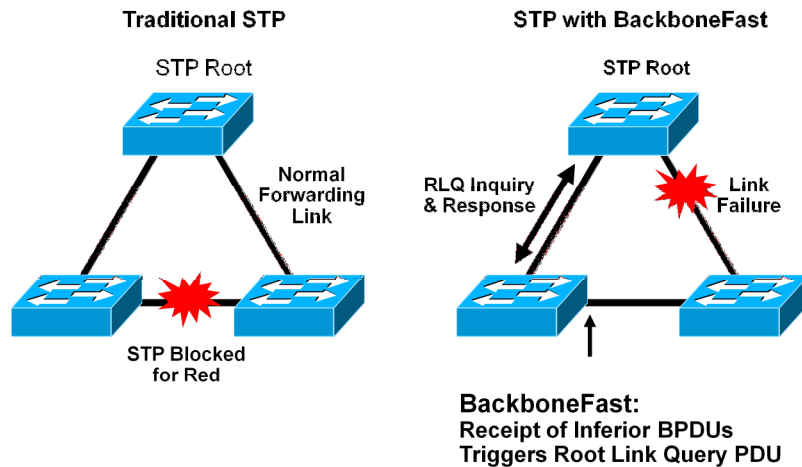
- ACCESS LAYER SWITCH ONLY
- Must have direct knowledge of forwarding link failure on root port
- **Reduces convergence time to under 5 sec**

Copyright 2012 CertificationKits LLC All Rights Reserved



UplinkFast is a means for speeding up network convergence. It minimizes network downtime from about 50sec. to somewhere less than 5sec. Uplink fast is configured on a switch to switch basis and should only be configured on Access Layer Switches.

# BackboneFast Overview



Copyright 2012 CertificationKits LLC All Rights Reserved



Backbone fast is configured on EVERY switch in the switching fabric. Backbone fast uses Root Link Queries (RLQ). Here is the scenario, a switches Root Port fails and it now thinks that it is the new Root Bridge. It promotes itself and starts sending BPDUs, but switches in the network do not recognize the switch as being the Root so they send a RLQ to the real root bridge to see if it is still alive. If the real Root Bridge answers, then the switch send a correction to the switch who lost his old Root Port and it now creates a new Root Port.

# Enabling and Verifying BackboneFast

```
Switch(config)# spanning-tree backbonefast
```

- Enables BackboneFast

```
Switch# show spanning-tree backbonefast
```

- Displays BackboneFast configuration information

```
Switch# show spanning-tree backbonefast
BackboneFast is enabled

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)   : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs): 0
Number of RLQ request PDUs sent (all VLANs)    : 0
Number of RLQ response PDUs sent (all VLANs)   : 0
```



CertificationKits

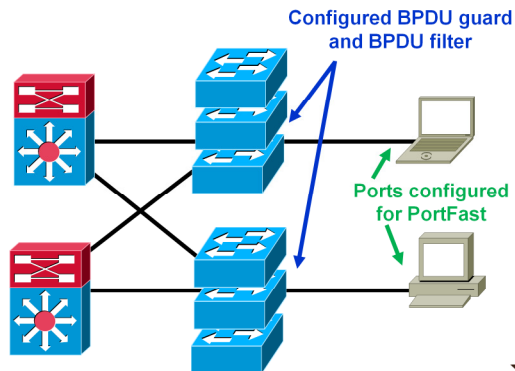
Copyright 2012 CertificationKits LLC All Rights Reserved

For BackboneFast to work, you must enable it on all switches in the network.  
BackboneFast is not supported on Token Ring VLANs.

# Protecting the Operation of STP

- Protection against switches being added on PortFast ports.

- BPDUs guard shuts ports down.
- BPDUs filter specifies action to be taken when BPDUs are received.



Copyright 2012 CertificationKits LLC All Rights Reserved



## BPDUs Guard

BPDUs guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network.

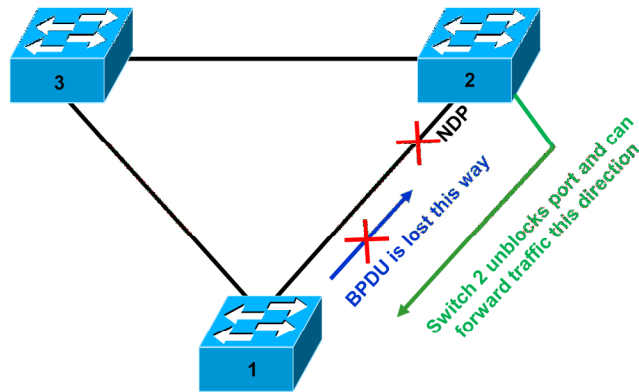
## BPDUs Filtering

PortFast BPDUs filtering affects how the switch acknowledges BPDUs seen on PortFast-configured ports. Its functionality differs if it is configured globally or on a per-port basis. This difference will be explained elsewhere in this course.

## BPDUs Root Guard

BPDUs root guard protects against a switch outside the designated network attempting to become the root bridge by blocking its access until the receipt of its BPDUs ceases.

# Unidirectional Link Failure



Copyright 2012 CertificationKits LLC All Rights Reserved

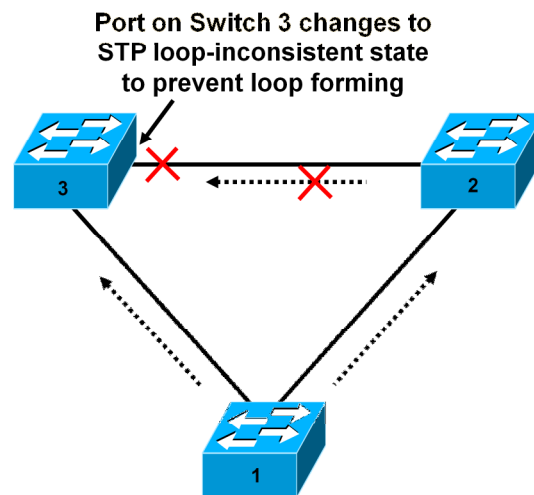


A unidirectional link occurs when traffic is transmitted between neighbors in one direction only. Unidirectional links can cause spanning tree topology loops. UDLD allows devices to detect when a unidirectional link exists and also to shut down the affected interface.

UDLD is a Layer 2 protocol that works with the Layer 1 mechanisms to determine the physical status of a link. If one fiber strand in a pair is disconnected, autonegotiation would not allow the link to become active or stay up. If both fiber strands are operant from a Layer 1 perspective, UDLD determines if traffic is flowing bidirectionally between the correct neighbors.

The switch periodically transmits UDLD packets on an interface with UDLD enabled. If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional, and the interface is shut down. Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable unidirectional links.

## With Loop Guard



CertificationKits

Copyright 2012 CertificationKits LLC All Rights Reserved

With loop guard enabled, the blocking port on switch 3 will transition into the STP loop-inconsistent state upon expiration of the max age timer. Because a port in the STP loop-inconsistent state will not pass user traffic, no loop is created. The loop-inconsistent state is effectively equal to the blocking state.

# Spanning Tree Protocol (STP)

## Advanced STP

Copyright 2012 CertificationKits LLC. All Rights Reserved.



# Rapid Spanning Tree Protocol(RSTP)

- RSTP (IEEE 802.1w) developed to 802.1d's principle concepts and make convergence much faster and more efficient
- Like 802.1d, RSTP's basic functionality can be applied as a single or multiple instances
- This can be done with Multiple Spanning Tree (MST) IEEE 802.1s
- Rapid PVST, Cisco proprietary



Copyright 2012 CertificationKits LLC All Rights Reserved

CertificationKits

Root Bridge in RSTP is elected just like 802.1d. After all switches agree on the Root, the following port roles are determined

1. **Root Port** – The one switch port on each switch that has the best root path cost to the root
2. **Designated Port** – The port on a network segment that has the best root path cost to the root
3. **Alternate Port** – Port that has an alternate path to the Root, different than the path the Root Port takes.
4. **Backup Port** – Port that provides a redundant (but less desirable) connection to a segment where another switch port connects. If that common segment is lost, the switch may or may not have a path back to the root



# Rapid Spanning Tree Protocol(RSTP)

RSTP defines port states only according to what the port does with the incoming frame

- [Discarding](#)
- [Learning](#)
- [Forwarding](#)



Copyright 2012 CertificationKits LLC All Rights Reserved

**CertificationKits**

- [Discarding](#) – Incoming frames are simply dropped, no MAC addresses are learned
- [Learning](#) – Incoming frames are dropped, but MAC addresses are learned
- [Forwarding](#) – Incoming frames are forwarded according to MAC addresses that have been learned

## Rapid Spanning Tree Port Types

- **Root port**
  - Port that receives the best BPDU on a bridge is the root port.
- **Designated port**
  - Port is designated if it can send the best BPDU on the segment to which it is connected.
- **Alternate port**
  - Alternate path to the root on another switch.
- **Backup port**
  - Alternate path to the root on the same switch.
- **Disabled port**



**CertificationKits**

Copyright 2012 CertificationKits LLC All Rights Reserved

There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

# Multiple Spanning Tree Protocol (MST)

## Multiple Spanning Tree (MST) IEEE 802.1s

- Built on the concept of mapping one or more VLANs to a single STP instances.
- Multiple instances of STP can be used, with each instance supporting a different group of vlans
- To implement MST in a network, you need to determine the following
  1. The number of STP instances needed to support the desired topologies
  2. Whether to map a set of VLANs to each instance



Copyright 2012 CertificationKits LLC All Rights Reserved

CertificationKits

MST can be implemented where having PVST running causes too much load on the resources of the switch. It allow you to group vlans together so you can have fewer instances of spanning tree running on the switch.

MST configuration is manual as there no current method to propagate this info as in VTP.

**The following must be done in order:**

Enable MST on the switch by defining the region:

```
Switch(config)# spanning-tree mode set
```

Enter the MST configuration:

```
Switch(config)# spanning-tree mst configuration
```

Assign a region configuration name (up to 32 char):

```
Switch(config)# name name
```

# Multiple Spanning Tree Protocol (MST)

Assign a region configuration number (0-65535)

Switch(config-mst)# **revision version**

Map VLANs to an MST instance

Switch(config-mst)# **instance instance-id vlan vlan-list**

The instance-id (0-15) carries topology information for the VLANs listed in vlan-list.

Show the pending changes made

Switch(config-mst)# **show pending**

Exit the MST configuration; commit the changes to the active MST region configuration:

Switch(config-mst)# **exit**



Copyright 2012 CertificationKits LLC All Rights Reserved

**CertificationKits**

Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster spanning tree convergence after a topology change. The standard also includes features equivalent to Cisco PortFast, UplinkFast and BackboneFast for faster network reconvergence. The configuration revision number give you a means to track changes to the MST region. Each time you make changes, you should increment the revision accordingly on each router with the same number.

# Potential STP Problems

- Duplex mismatch
- Unidirectional link failure
- Frame corruption
- Resource errors
- PortFast configuration error
- Inappropriate STP parameter tuning and diameter issues



**CertificationKits**

Copyright 2012 CertificationKits LLC All Rights Reserved

Listed on the slide are potential Spanning Tree Problems. The problems can be a result of problems are with layer 1 or 2 of the OSI reference model.

# Troubleshooting STP

- Use your network diagram.
- Identify a bridging loop.
- Restore connectivity.
- Check ports.
- Look for resource errors.
- Disable unneeded features.



Copyright 2012 CertificationKits LLC All Rights Reserved

**CertificationKits**

Network documentation is crucial in troubleshooting STP problems. When a bridge loop occurs, CPU utilization on associate switch will most likely hit 100% utilization as all available CPU resources will be utilized.

# Spanning Tree debug Commands

Switch# **debug spanning-tree all**

- Displays all debugging messages for spanning tree

Switch# **debug spanning-tree events**

- Displays spanning-tree topology events debug messages

Switch# **debug spanning-tree backbonefast**

- Displays spanning-tree backbonefast events debug messages

Switch# **debug spanning-tree uplinkfast**

- Displays spanning-tree uplinkfast events debug messages



Copyright 2012 CertificationKits LLC All Rights Reserved

**CertificationKits**

Always utilize Cisco debug commands with caution as most are CPU intensive and could bring down an operational network