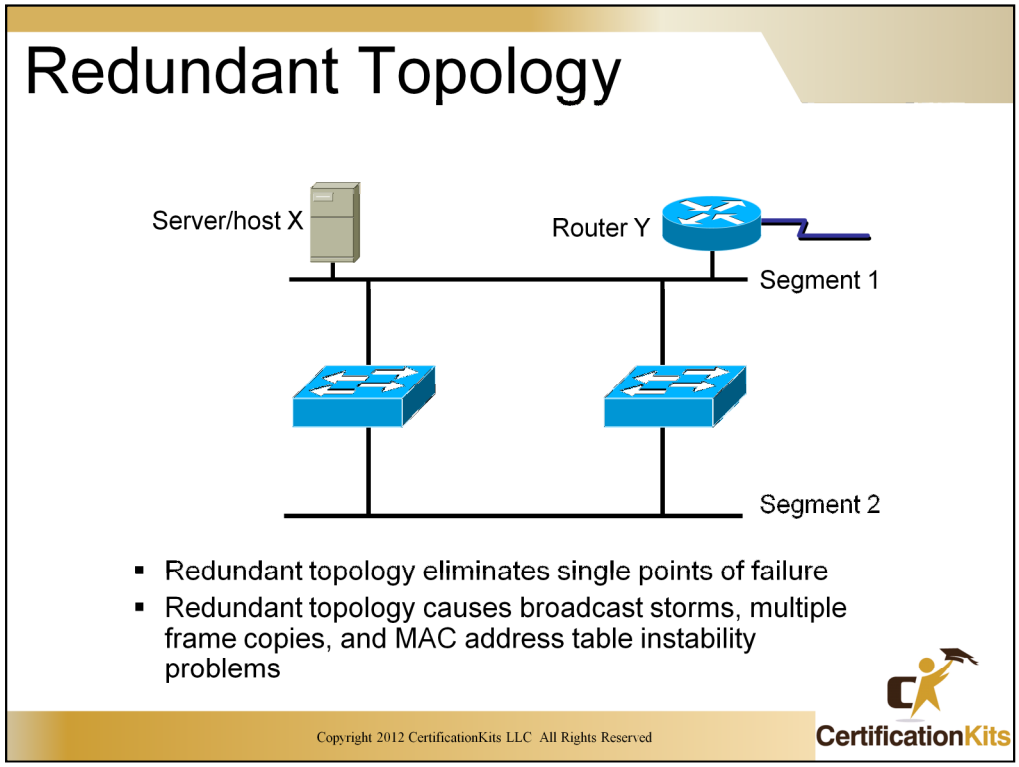
Implementing Spanning Tree

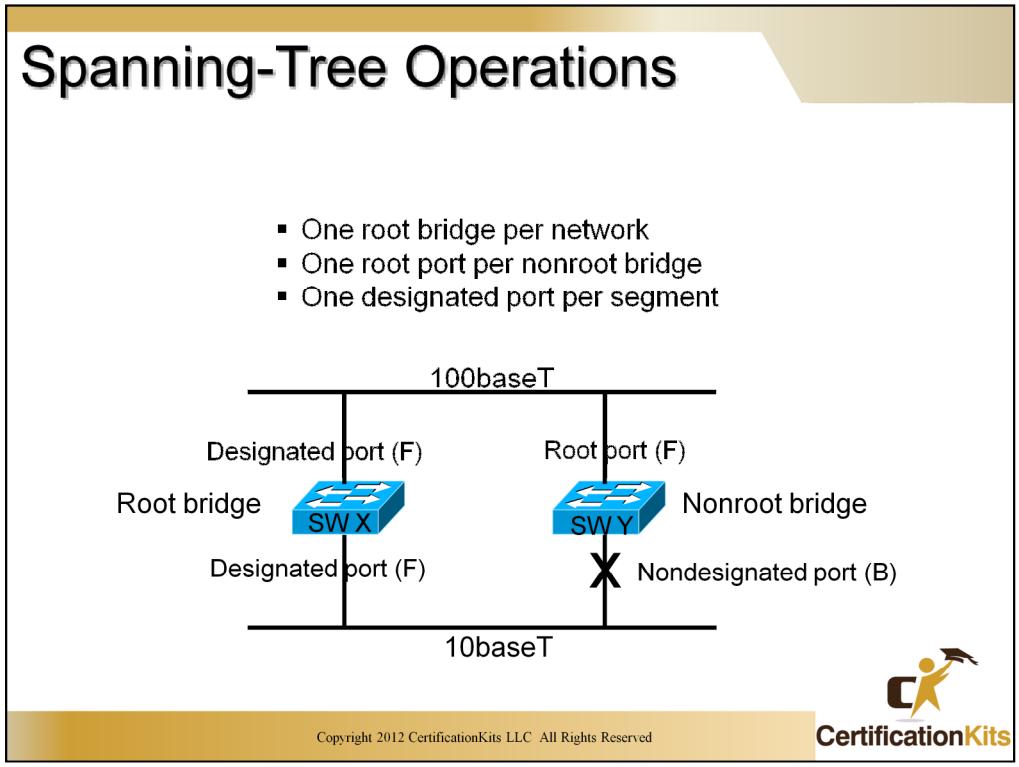
Chapter 3



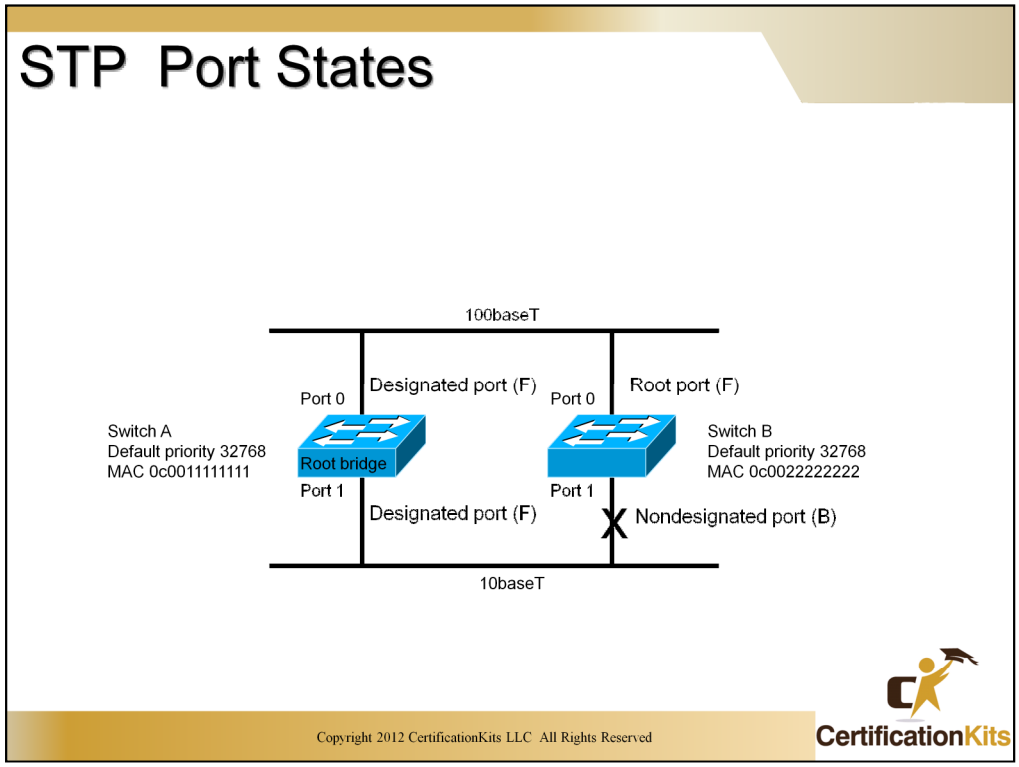
Spanning Tree Protocol is a bridge protocol that enables a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange Bridge Protocol Data Unit (BPDU) messages with other bridges to detect loops, and then remove the loops by shutting down selected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



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



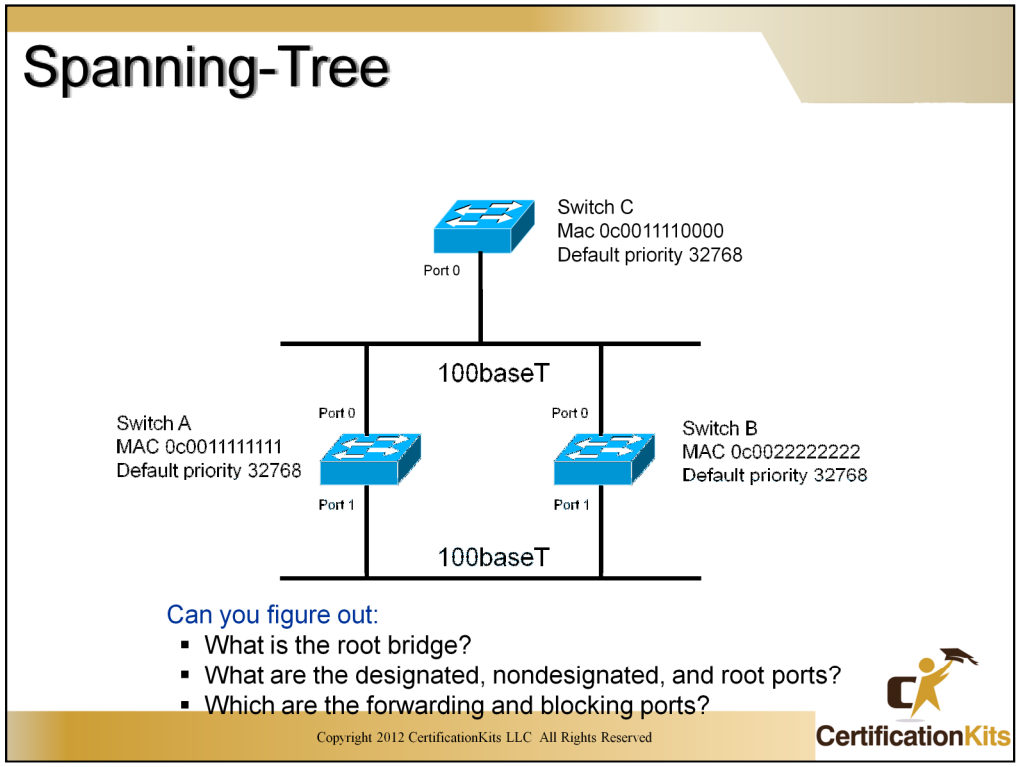
Active Ports will have the lowest combination of:

Root Path Cost

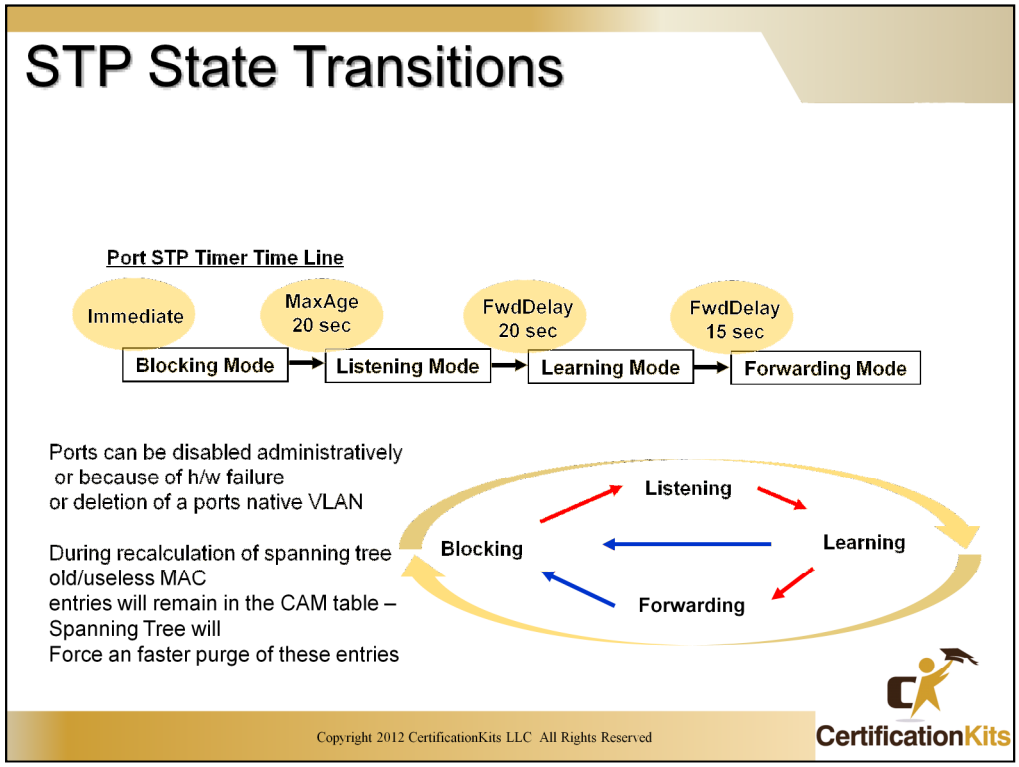
Bridge ID (of upstream bridge)

Port ID

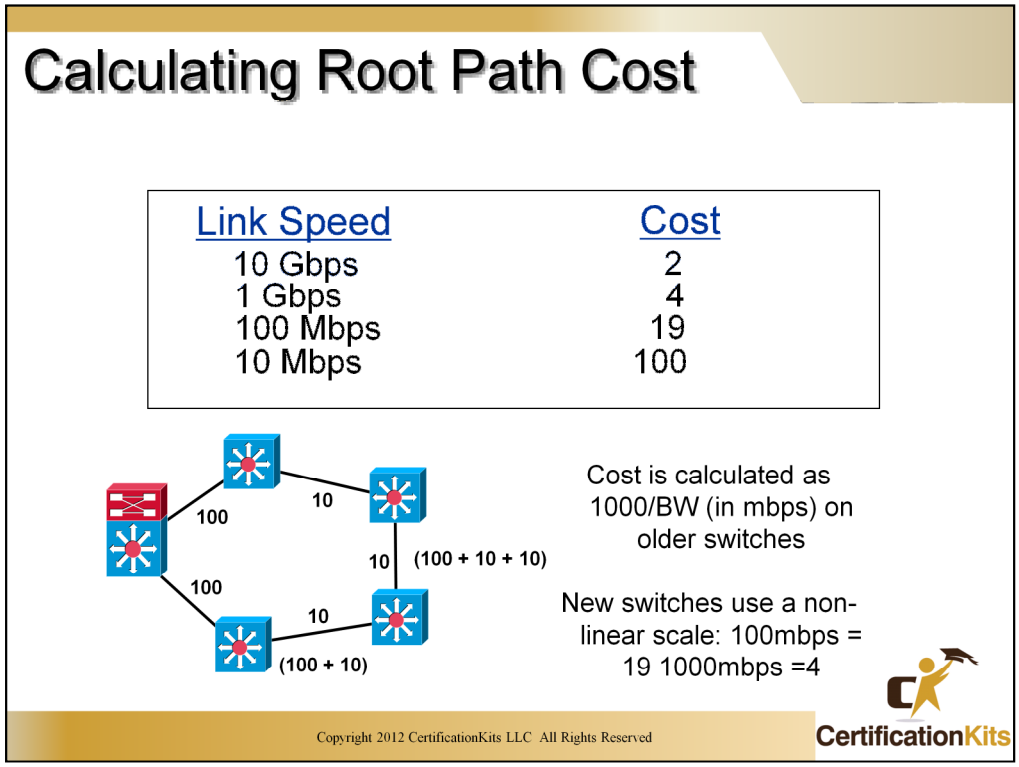
Path from any switch to the root will travel either directly to the root bridge or though a parent or "designated" switch. Blocked ports continue to send/receive BPDUs but NOT DATA.



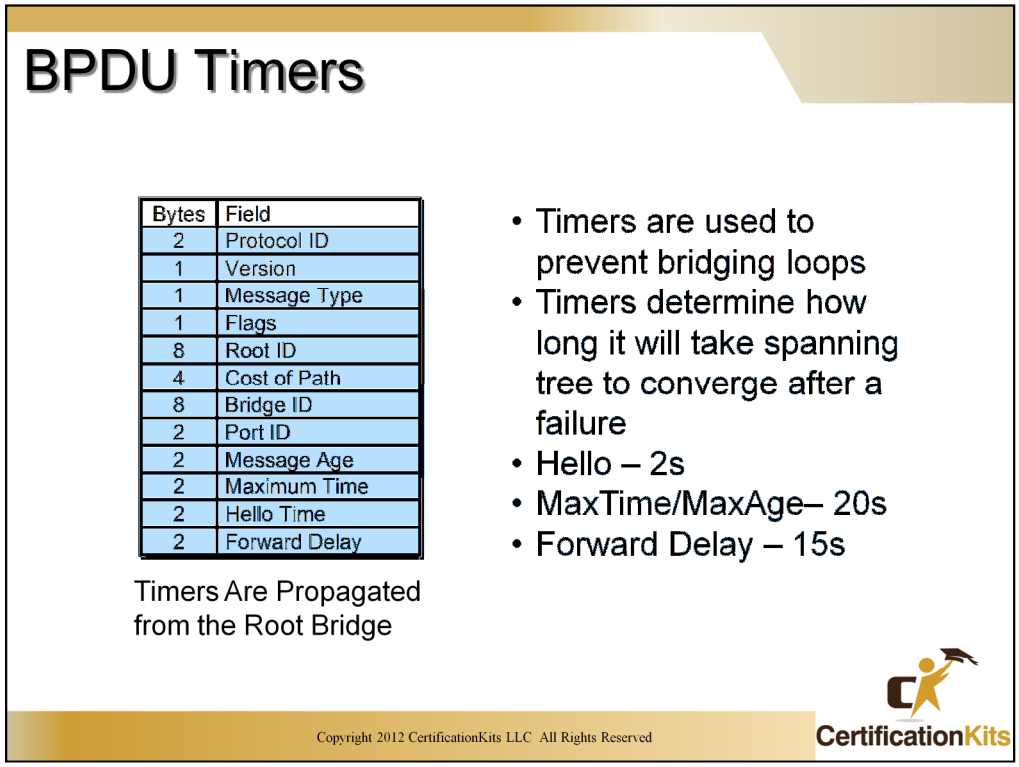
Switch C will become the Root Bridge because it has the lowest Bridge ID. Port 0 on Switch A and Port 0 on Switch B will become the Root Port, Port 1 on switch A will become the designated port because the port has a lower port ID.



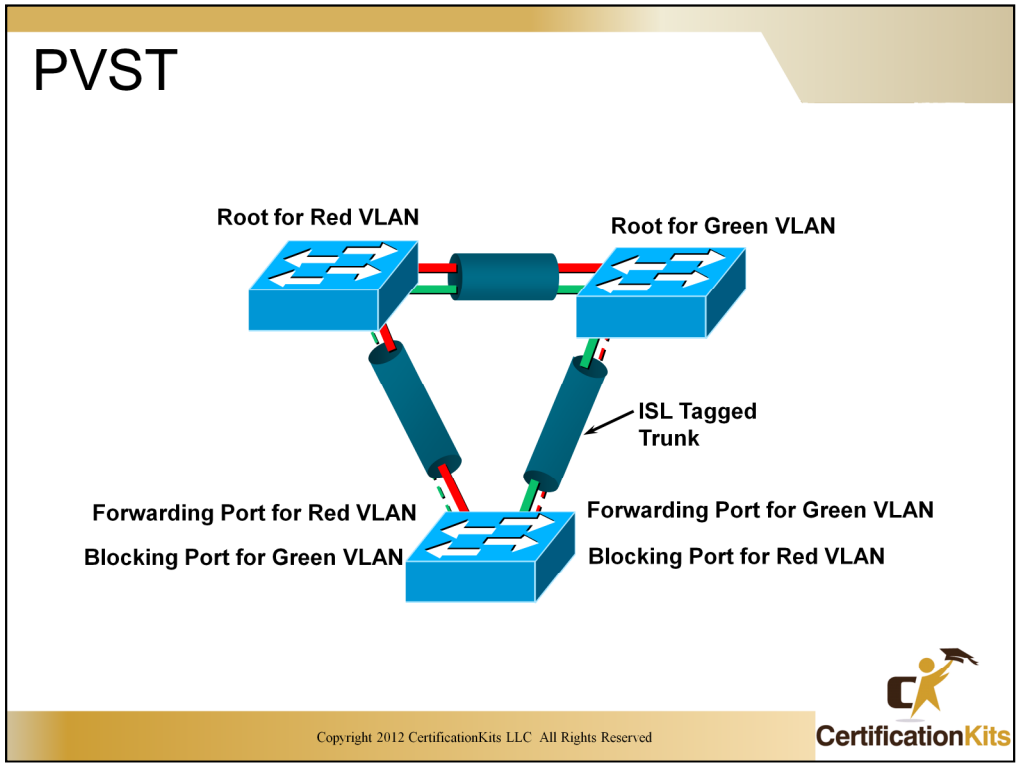
Disabled	=	Administratively Down
Blocking	=	Receiving BPDUs
Listening	=	Sending and Receiving BPDUs (building the topology)
Learning	=	Populating CAM table
Forwarding	=	Sending/Receiving User Data



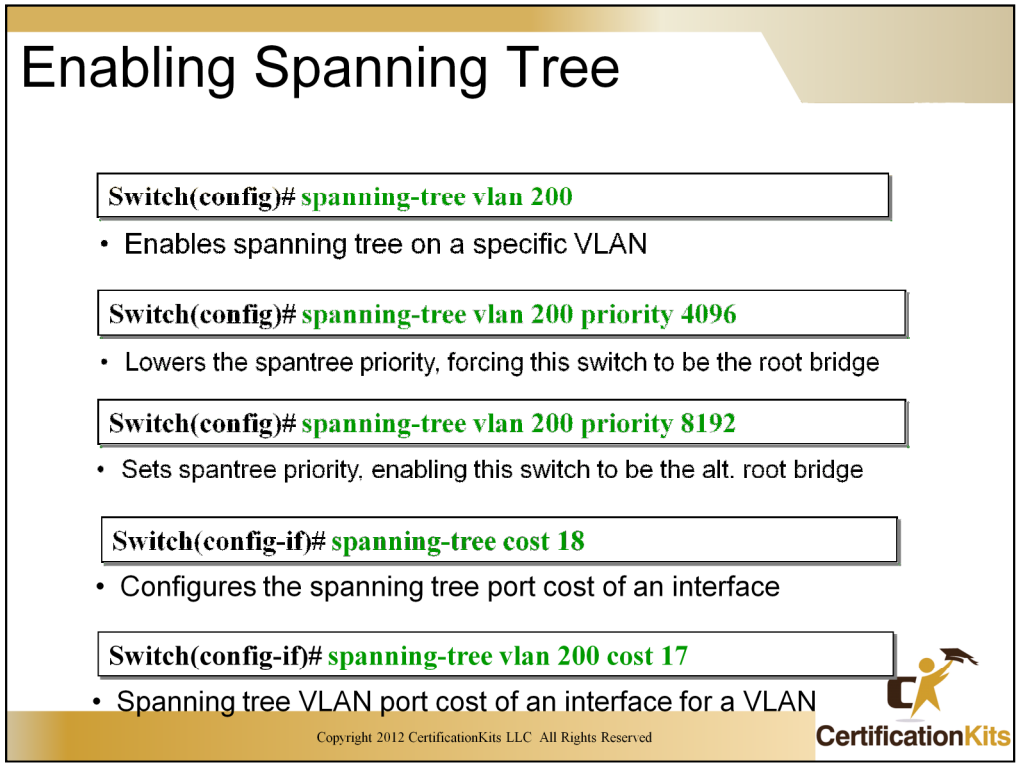
Path cost is a function of bandwidth of each path. It can be changed using a switch port cost parameter. Is determined by the sum of port costs between source and destination.



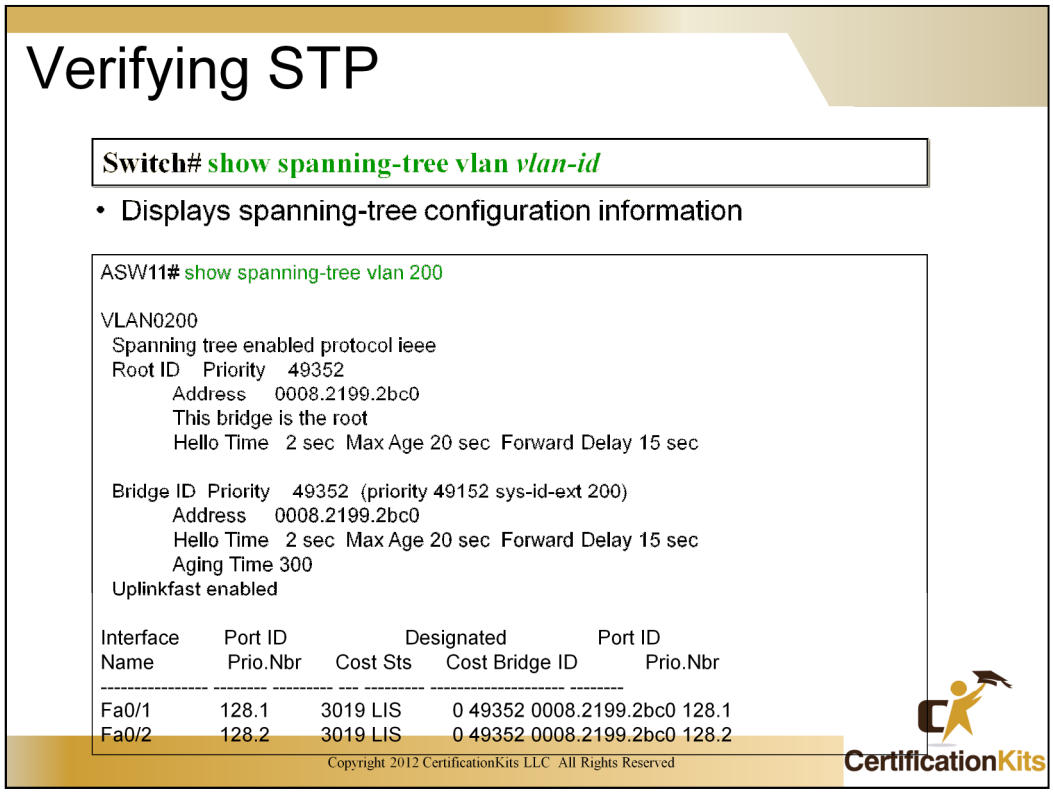
BPDU timers are set by the Root bridge. By default the hello interval is set to once every 2 seconds. Why so often? To avoid loops!



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.



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.



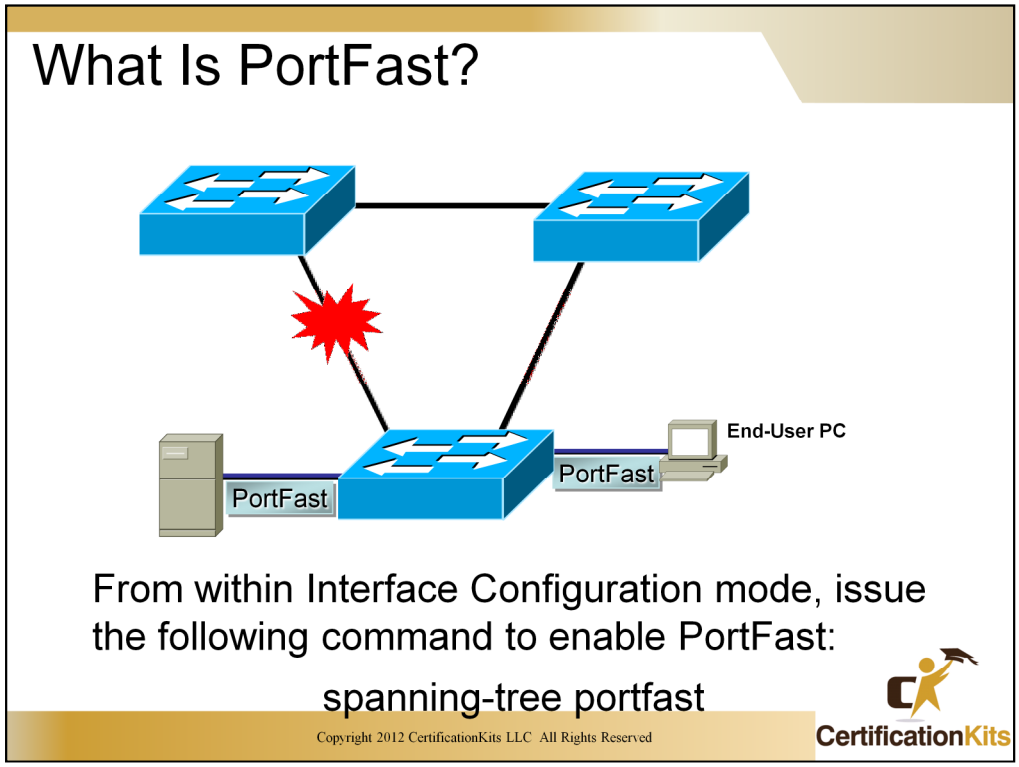
To display information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

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.

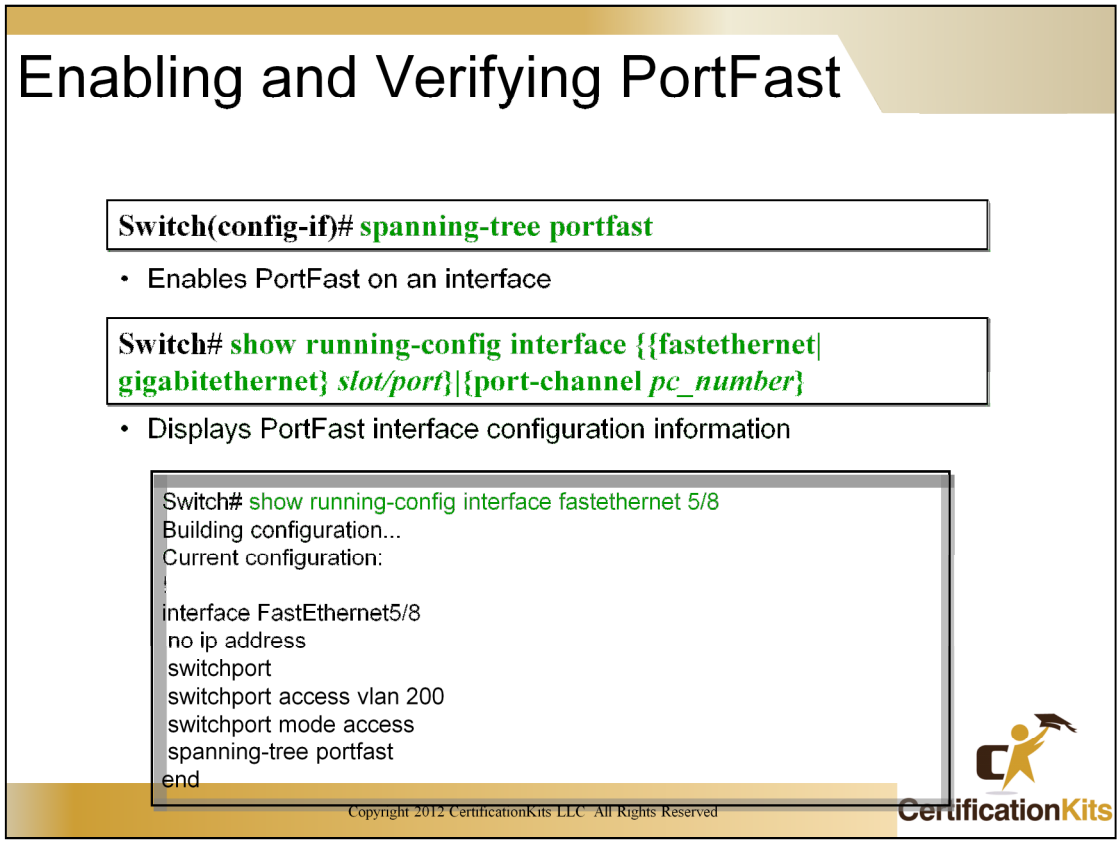
Spanning Tree Protocol (STP)

Speeding up STP

CertificationKits



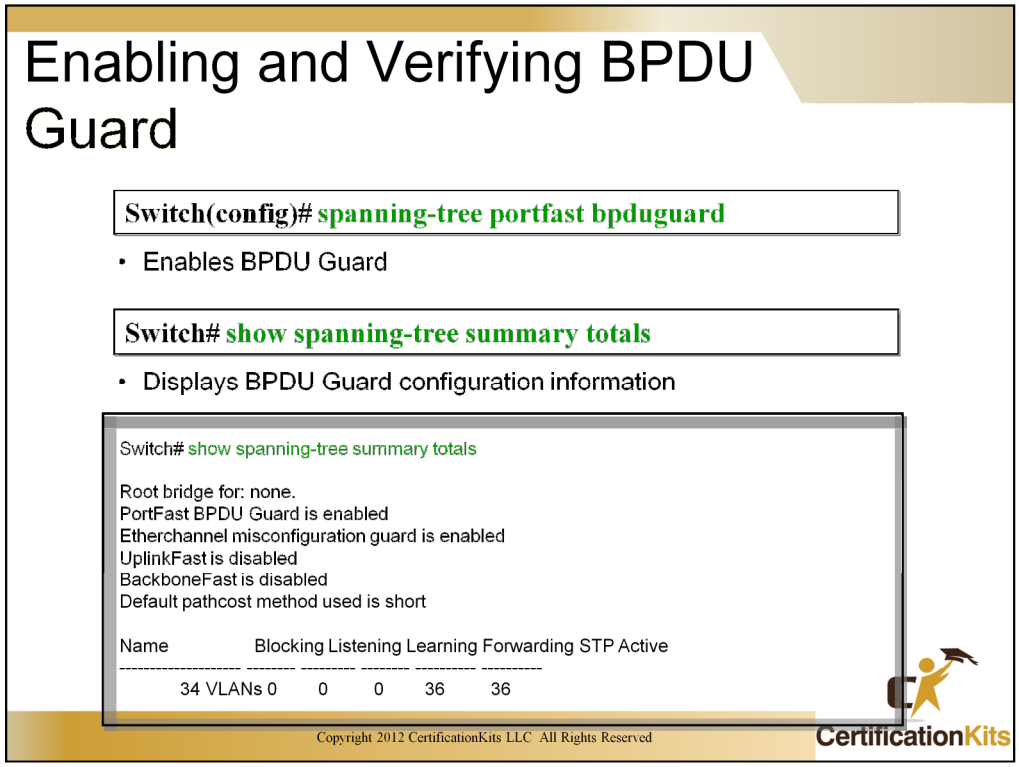
Portfast is used to minimize server or workstation downtime. Portfast is configured on a port to port basis. Be careful to only enable Portfast on ports that are connected directly to end hosts (i.e. servers or PCs), not to other siwtches.



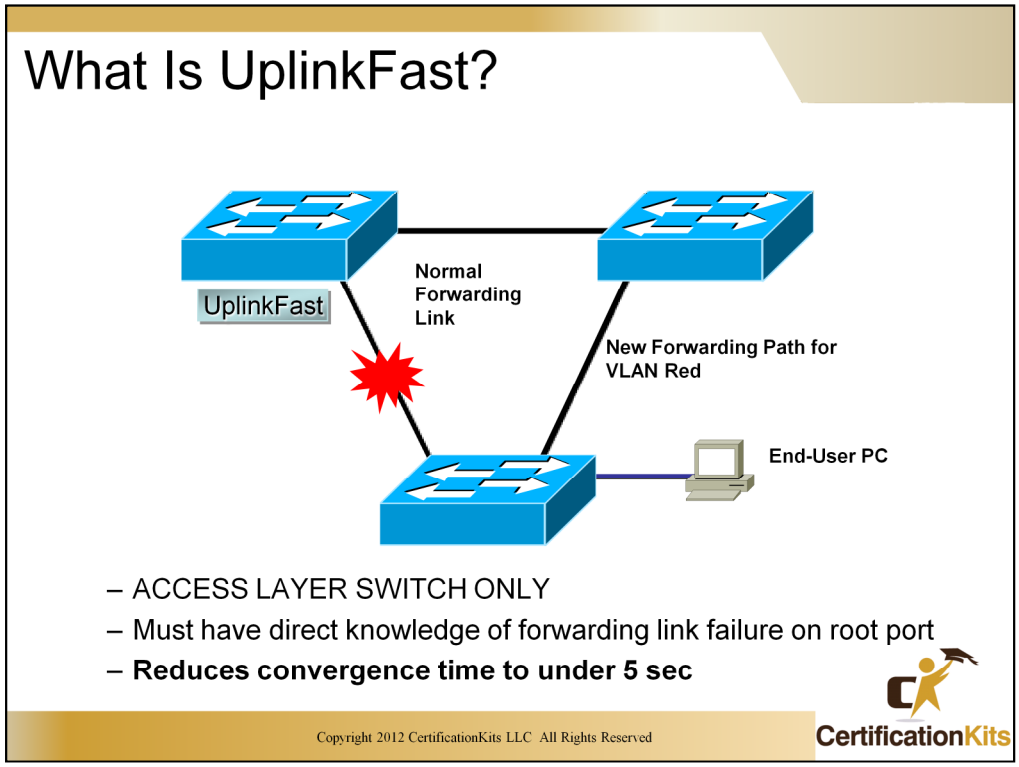
Note: You should use PortFast to connect a single end station or a switch port to a switch port. If you enable PortFast on a port that is connected to another Layer 2 device, such as a switch, you might create network loops.

Protecting STP w/Portfast Enabled

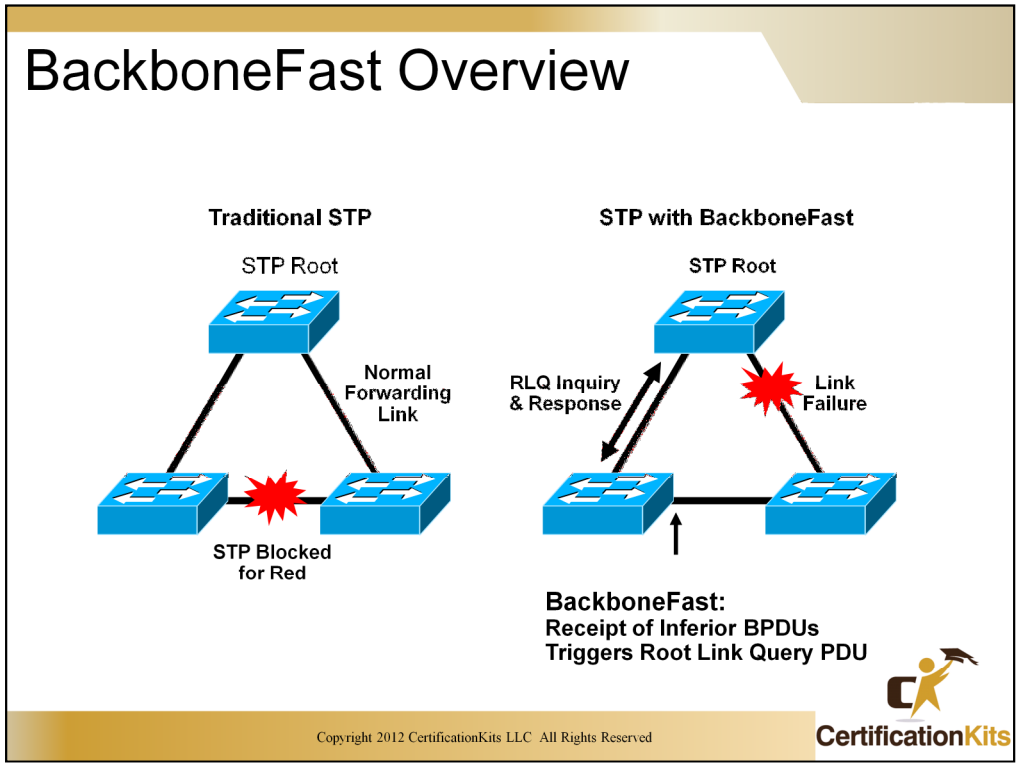
- BPDU Guard
  - Receiving BPDUs puts the port in "error disable" state
- BPDU Filtering
  - Receiving BPDUs turns off Portfast and resumes normal STP operation.
- Root Guard
  - Moves ports that receive superior BPDUs to the "root inconsistent" state.



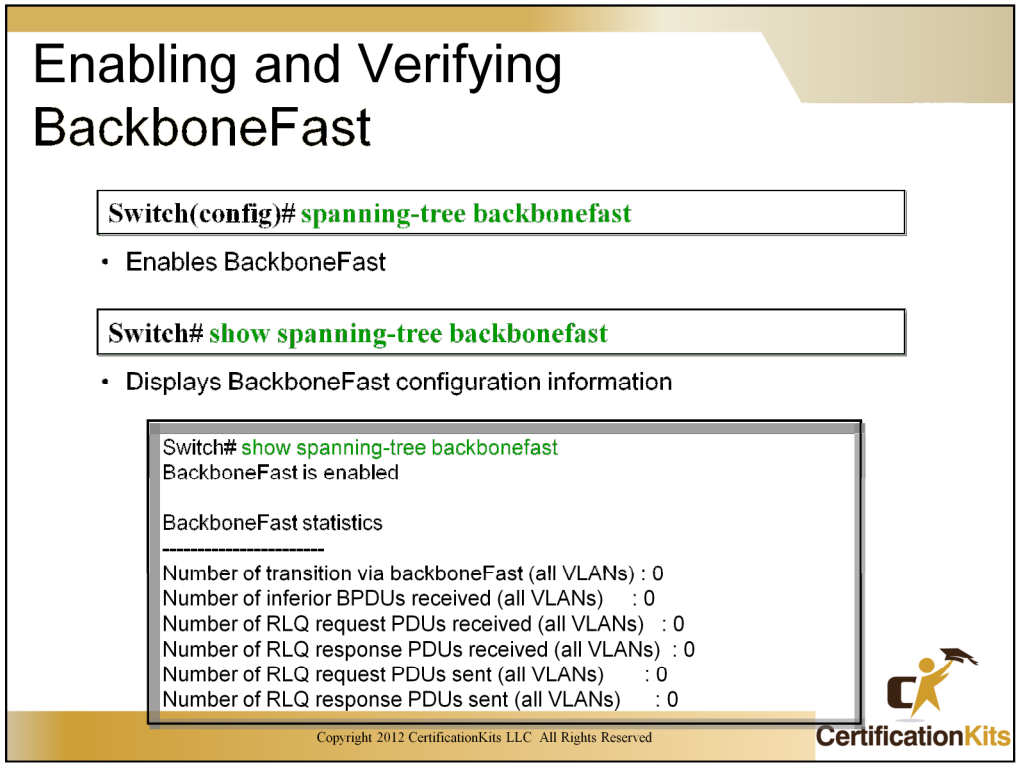
If a port with bpduguard enabled receives a BPDU, the port with be placed in errordisable state.



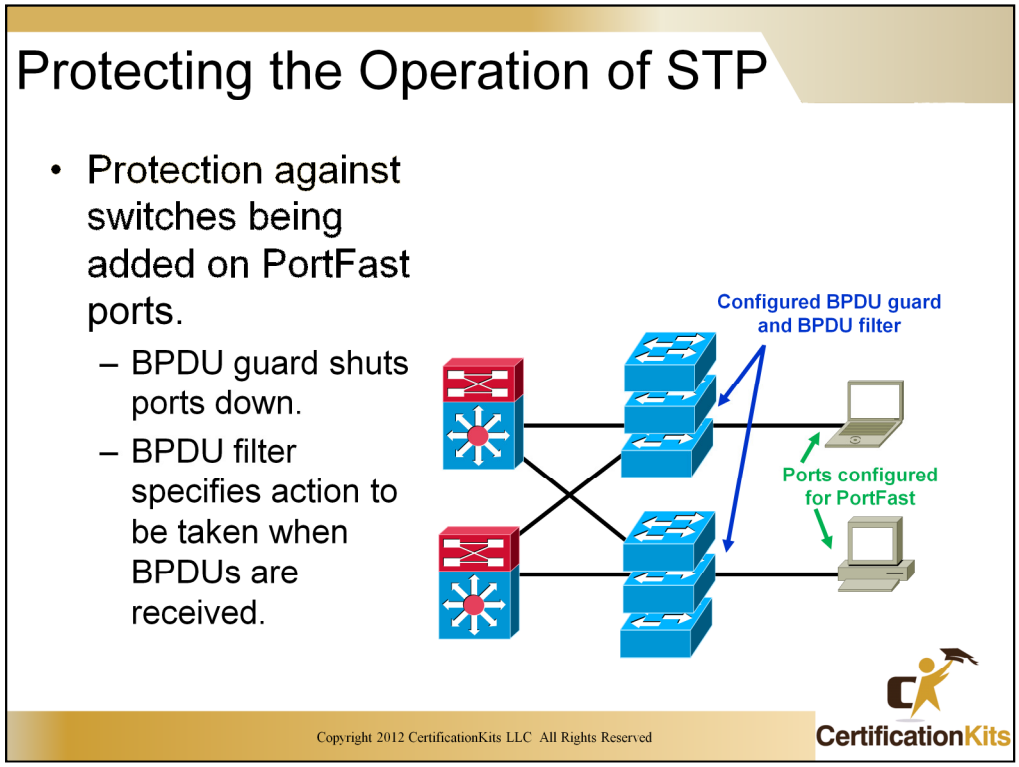
UplinkFast is a means for speeding up network convergence. It minimizes network downtime from about 50sec. to somewhere less than 5sec. Uplink fast is configured on a switch to switch basis and should only be configured on Access Layer Switches.



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.



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



BPDU Guard

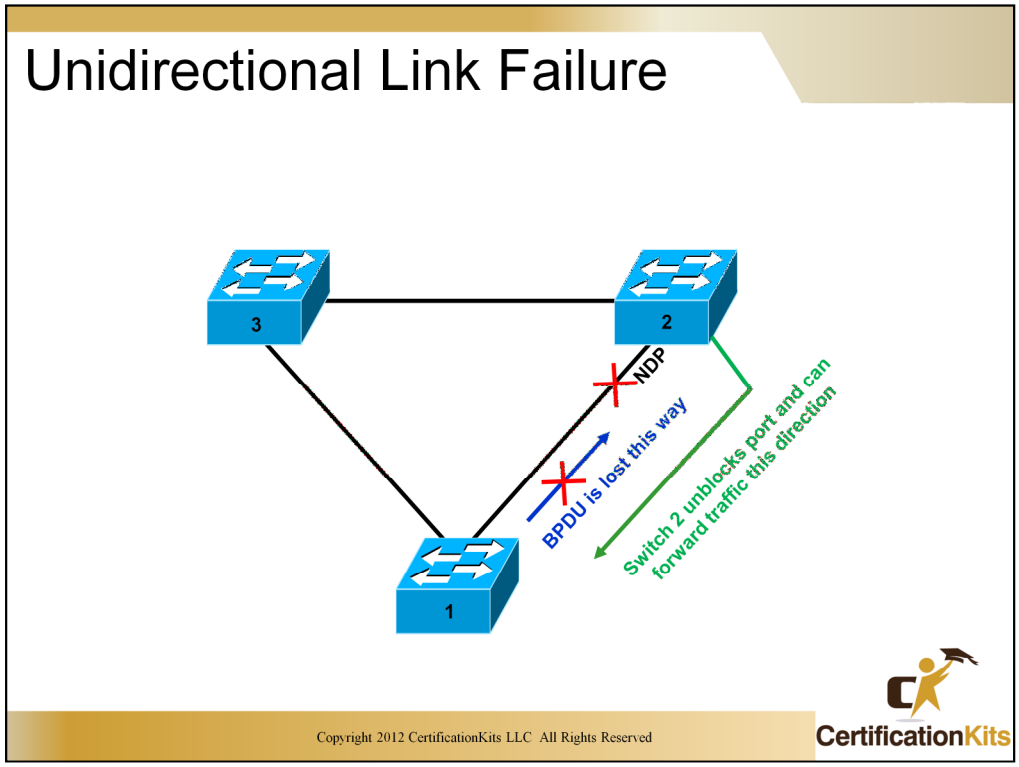
BPDU guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network.

BPDU Filtering

PortFast BPDU 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.

BPDU Root Guard

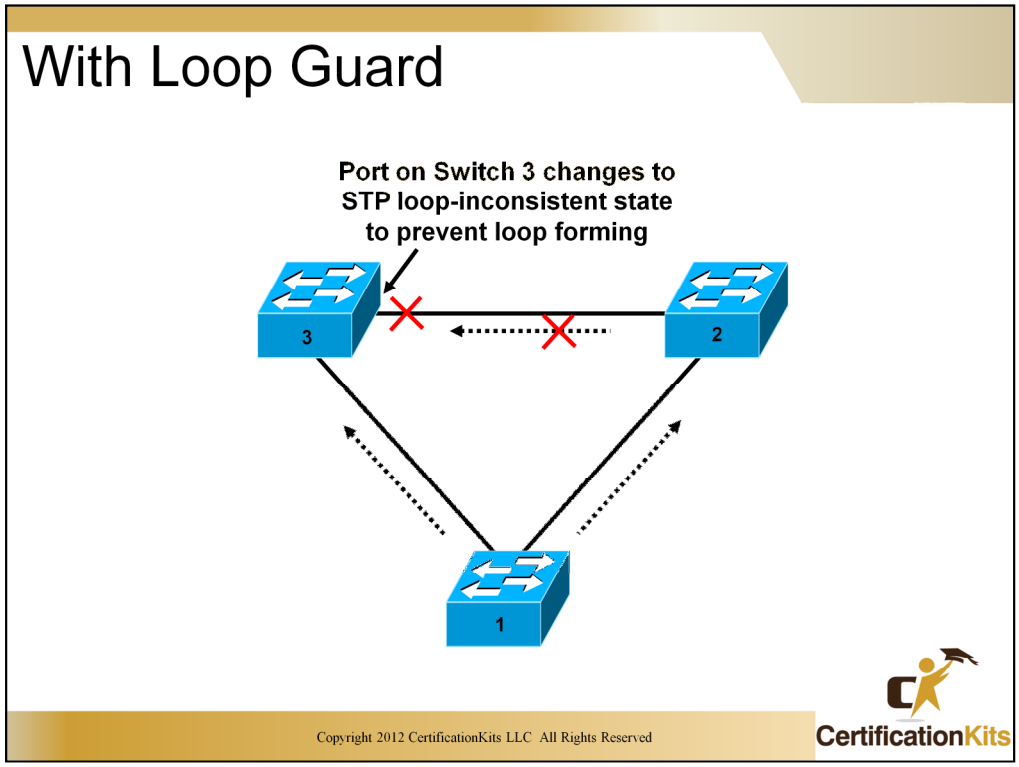
BPDU root guard protects against a switch outside the designated network attempting to become the root bridge by blocking its access until the receipt of its BPDUs ceases.



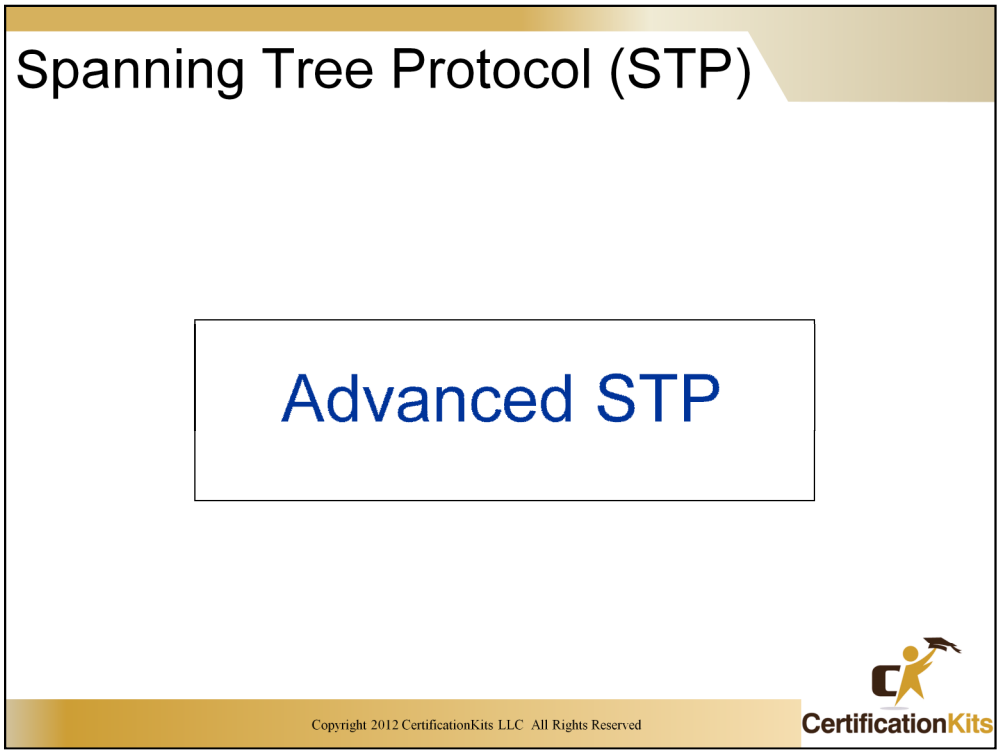
A unidirectional link occurs when traffic is transmitted between neighbors in one direction only. Unidirectional links can cause spanning tree topology loops. UDLD allows devices to detect when a unidirectional link exists and also to shut down the affected interface.

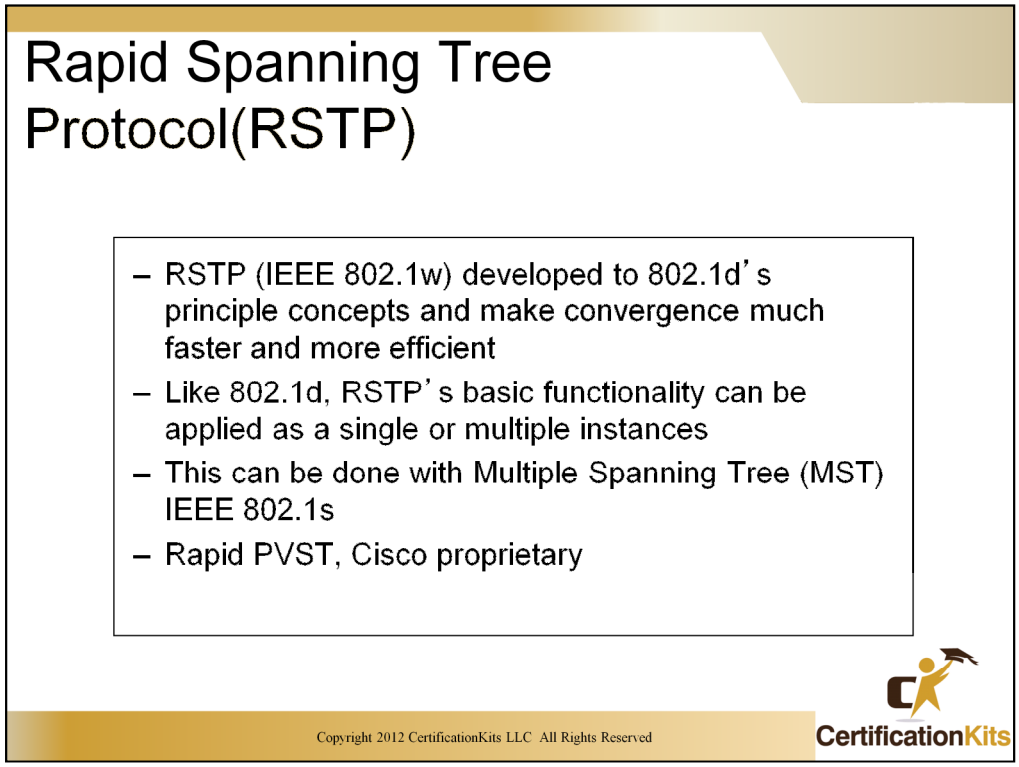
UDLD is a Layer 2 protocol that works with the Layer 1 mechanisms to determine the physical status of a link. If one fiber strand in a pair is disconnected, autonegotiation would not allow the link to become active or stay up. If both fiber strands are operant from a Layer 1 perspective, UDLD determines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





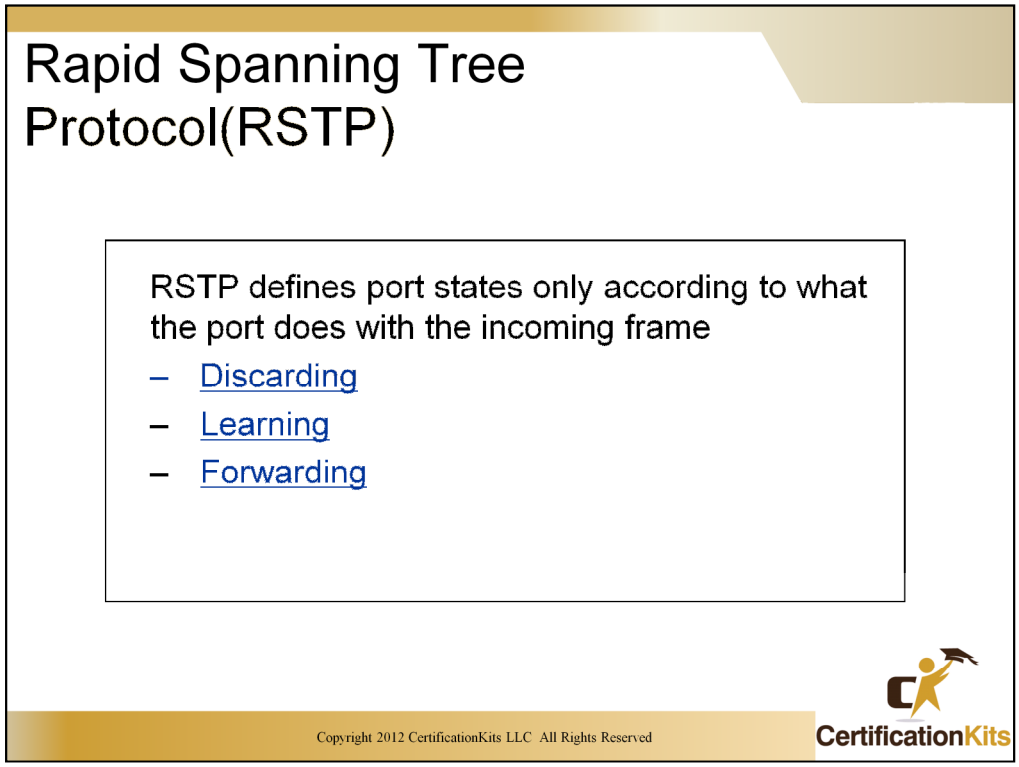
Root Bridge in RSTP is elected just like 802.1d. After all switches agree on the Root, the following port roles are determined

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 that the path the Root Port takes.

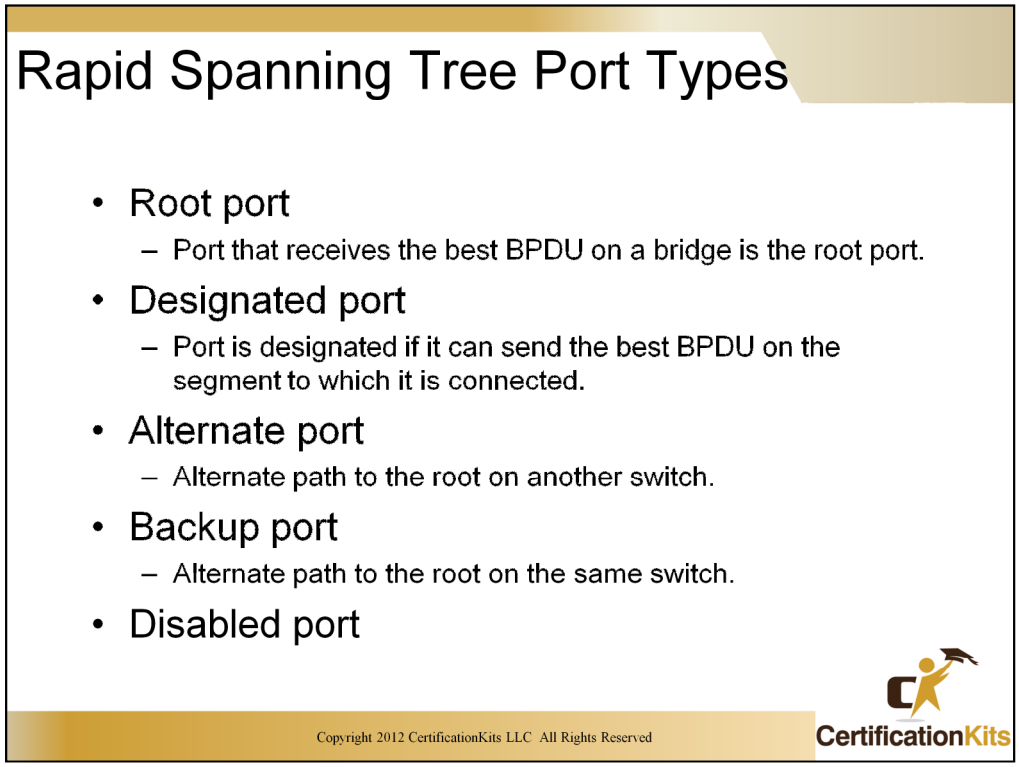
4. Backup Port – Port that provides a redundant (but less desirable) connection to a segment where another switch port connects. If that common segment is lost, the switch may or may not have a path back to the root



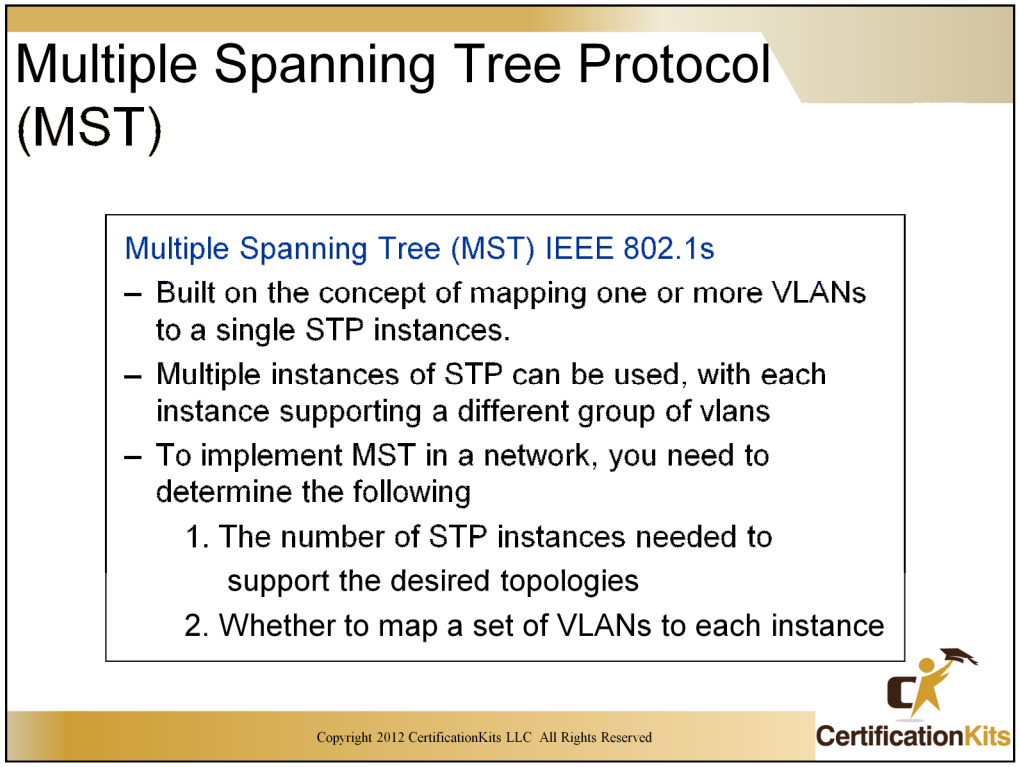
Discarding – Incoming frames are simply dropped, no MAC addresses are learned

Learning – Incoming frames are dropped, but MAC addresses are learned

Forwarding – Incoming frames are forwarded according to MAC addresses that have been learned



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.



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:

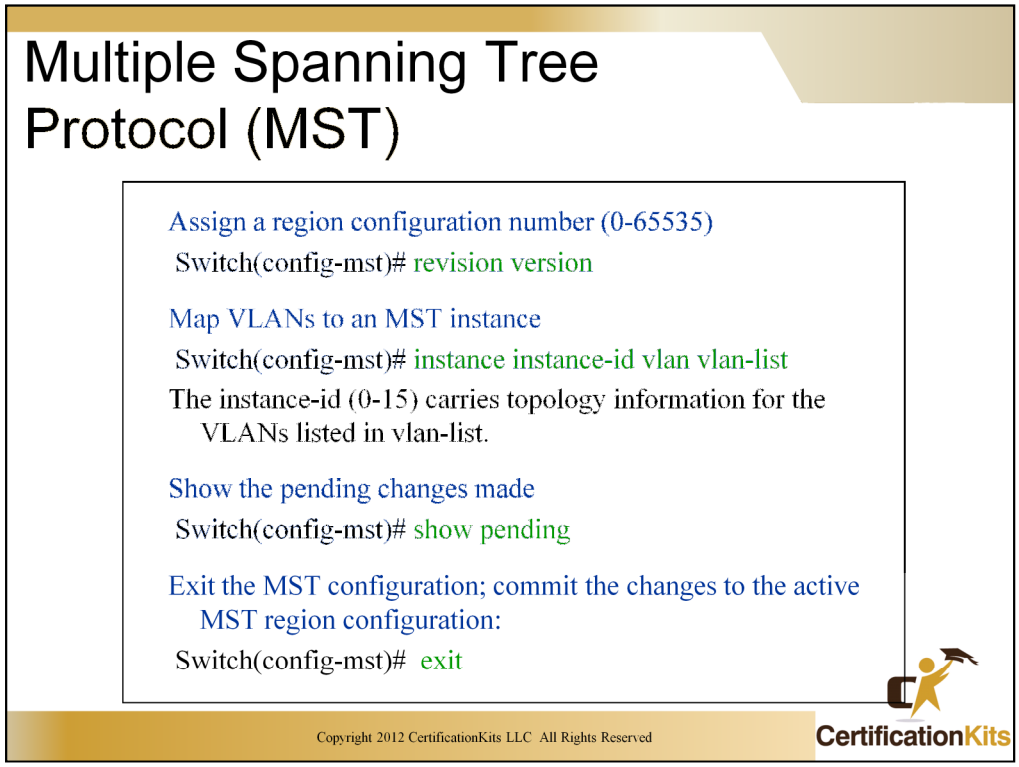
Switch(config)# spanning-tree mode set

Enter the MST configuration:

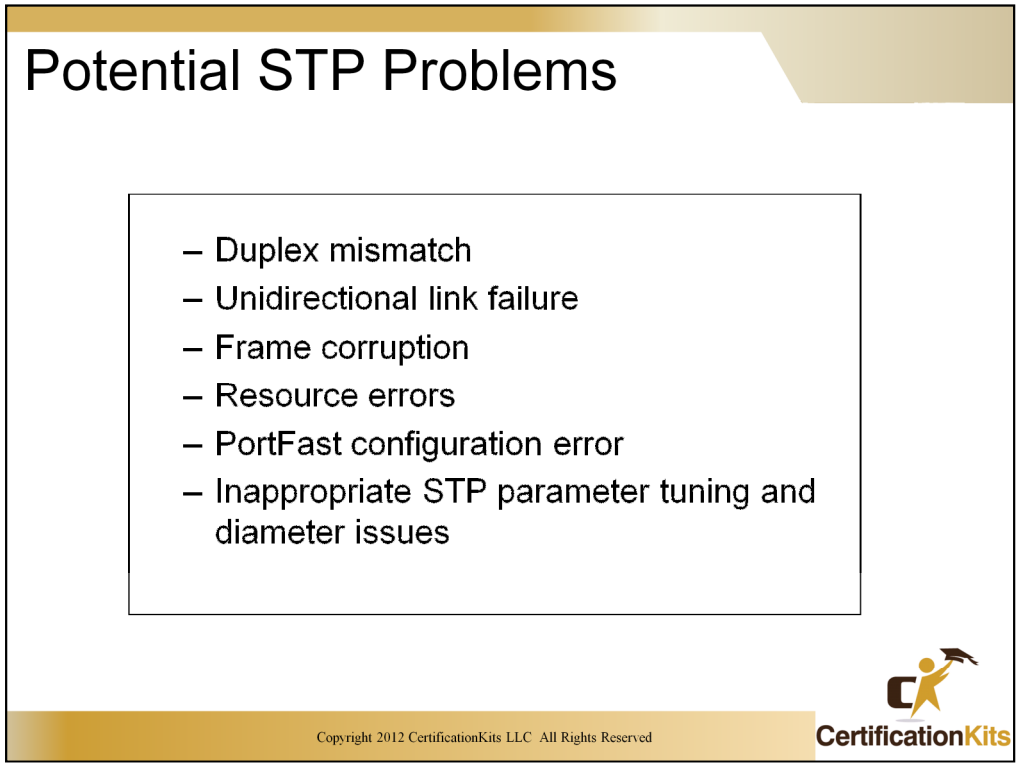
Switch(config)# spanning-tree mst configuration

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

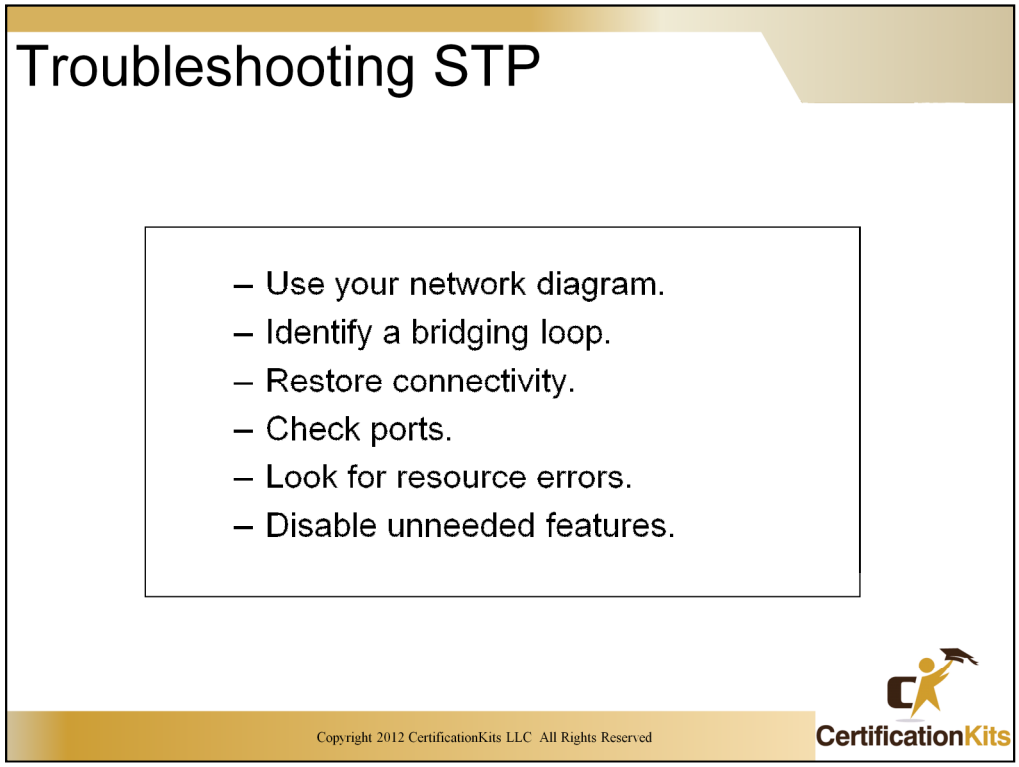
Switch(config)# name *name*



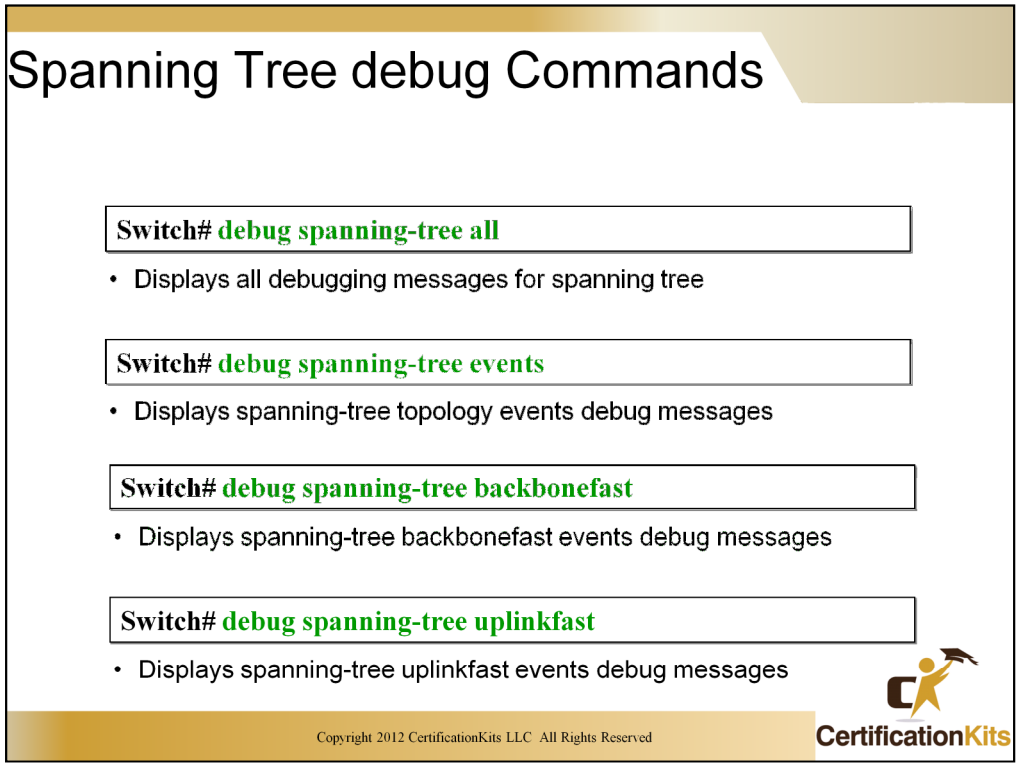
Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (802.1D standard) and provides for faster spanning tree convergence after a topology change. The standard also includes features equivalent to Cisco PortFast, UplinkFast and BackboneFast for faster network reconvergence. 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.



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



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.



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