Post 4

Thursday, January 24, 2019 11:19 PM

LAN REDUNDANCY P3

Config/Verify the BID: 2 Diff methods to config bridge priority value on Catalyst switch:
Way 1: To ensure switch has lowest bridge priority use:
S3(config)# spanning-tree vlan <*vlan-id*> root primary [*global config*]

- Priority for switch set to predefined value 24,576
- Or highest multiple of 4,096 less than lowest bridge priority detected on network

If alternate RB desired:
S3(config)# spanning-tree vlan <*vlan-id*> root secondary [*global config*]

- Sets priority for the switch to predefined value of 28,672
- Ensures alternate switch becomes RB if primary RB fails
- Assumes rest of switches have default 32,768 priority value

Way 2:
S3(config)# spanning-tree vlan <*vlan-id*> priority value [*global config*]

- Gives more granular control over bridge priority value
- Priority value is config in increments of 4,096 between 0-61,440.

Verify bridge priority of switch:
S3# show spanning-tree
PortFast/BPDU Guard

PortFast	**Cisco feature for PVST+ envs** **When switch port is config w/PortFast** • Port transitions from blocking to fwding immediately • Bypassing usual 802.1D STP transition states (listening/learning) • Can use on access ports to allow devices to connect to network immed **Access ports:** Ports connected to a single workstation/server **PortFast: Useful for DHCP** Without it: A PC can send a DHCP req before port is in fwding state • This would deny the host from getting a usable IP/info • PortFast immediately changes state to fwding: PC always gets usable IP
BPDU Guard	**In valid config: BPDUs should never be received:** • That would indicate another bridge/switch is connected to the port ○ Could cause a spanning tree loop **BPDU Guard:** Puts port in an error-disabled state on receipt of BPDU • Will effectively shut down port • Provides secure response to invalid configs

To config PortFast on port:
S3(config-if)# spanning-tree portfast [int config]: Each int to be enabled on
S3(config)# spanning-tree portfast default [global config]: Enables on all nontrunking ints
To configure BPDU guard on L2 access port:
S3(config-if)# spanning-tree bpduguard enable [int config]
S3(config)# spanning-tree portfast bpduguard default [global config]

- Enables on all PortFast-enabled ports

PVST+ Load Balancing

1. Select switches you want for primary/2dary RB's for each VLAN
2. Config switch to be primary bridge for VLAN:

spanning-tree vlan <*number*> root primary

1. Config switch to be 2ndary bridge for VLAN:

spanning-tree vlan <*number*> root secondary
show spanning-tree active Displays spanning tree config details for active ints only
show spanning-tree
Spanning Tree Mode Rapid PVST+: Cisco implementation of RSTP

- Supports RSTP on per-VLAN basis

Config Rapid PVST+ on Cisco switch
S1# conf t
S1(config)# spanning-tree mode rapid-pvst Config Rapid PVST+ spanning tree-mode
S1(config)# int fa0/1
S1(config-if)# spanning-tree link-type point-to-point Specify link type
S1(config-if)# end
S1# clear spanning-tree detected-protocols

Analyzing the STP Topology

1. Discover L2 topology: Network docs if exist: **show cdp neighbors**
2. Use STP knowledge to determine expected L2 path: Know which switch is RB
3. **show spanning-tree vlan** To determine which switch is RB
4. **show spanning-tree vlan** All switches to find which ports in blocking/fwding state /confirm expected L2 path

Expected vs Actual Topology
show spanning-tree

- Provides a quick overview of the status of STP for all VLANs defined on switch
- Specify VLAN to limit scope of cmd

show spanning-tree vlan vlan_id

- Get STP info for a particular VLAN.
- Get info about role/status of each port on switch [FWD/BLK/etc..]
- Also gives info about BID of local switch/root ID: The BID of RB

Spanning Tree Failure Consequences
2 types of failure

1. Similar to OSPF issue; STP might block ports that should have gone into fwding state
2. STP erroneously moves 1/more ports into fwding state

Ethernet frame headers don't include TTL fields:

- Any frame that enters a bridging loop continues to be fwded by switches indefinitely
- Only exceptions: Frames that have dest address recorded in MAC table of switches
- Frames are simply fwded to port associated w/MAC and don't enter loop
    - Any frame that is flooded by switch enters loop
    - Includes: Broadcasts/multicasts/unicasts w/globally unknown dest MAC

Consequences/Symptoms of STP failure:

- Load on all links in switched LAN quickly starts increasing as more and more frames enter loop
- Not limited to links from loop: Also affects any other links in switched domain b/c frames are flooded on all links
- When spanning tree failure is limited to single VLAN only links in that VLAN affected
- Switches/trunks that don't carry that VLAN operate normally

If spanning tree failure created a bridging loop: Traffic increases exponentially

- Switches will flood the broadcasts out multiple ports
- Creates copies of frames every time switches fwd them

When control plane traffic starts entering loop (OSPF/EIGRP Hellos): Devices running protocols quickly get overloaded

- CPUs approach 100% utilization while trying to process ever-increasing load of control plane traffic

Earliest indication: Routers or L3 switches reporting control plane failures/running at high CPU load

- Switches exp frequent MAC table changes

If loop exists:

- Switch may see frame w/certain source MAC coming on 1 port/another frame w/same source coming in on diff port sec later
- Will cause switch to update MAC address table twice for same MAC

Default Gateway Limitations
STP's enable physical redundancy in switched network

- Host at access layer of hierarchical network also benefits from alternate default GW's
- If a router or router int (that serves as default GW) fails: Hosts config'd w/default GW are isolated from outside networks
- Mechanism needed to provide alt default GW's in switched networks where 2/more routers connected to same VLANs

End devices: Typically config w/single IP for default GW:

- This address doesn't change when topology does: If default GW IP can't be reached:
- Local device is unable to send packets off local network segment: Disconnecting it from the rest of

networ

Router Redundancy

Prevent single point of failure at GW: Implement virtual router

- Multiple routers are config'd to work together to present the illusion of a single router to hosts on LAN
- By sharing an IP/MAC 2/more routers can act as single virtual

IP of virtual router is config as default GW for workstations on specific IP segment

- When frames are sent from host devices to GW: Hosts use ARP to resolve MAC that is associated w/IP of default GW
- ARP resolution returns MAC of virtual router
- Frames sent to MAC of virtual router can then be physically processed by currently active router w/in virtual router group
- Protocol is used to ID 2/more routers as devices responsible for processing frames sent to the MAC/IP of single virtual router
- Host devices send traffic to address of virtual router
- Physical router fwds this traffic is transparent to host devices
- Redundancy protocol provides mechanism for determining which router should take active role in fwding traffic
    - Also determines when fwding role must be taken over by standby router
    - Transition from 1 fwding router to another is transparent to end devices

First-hop redundancy: Ability of network to dynamically recover from failure of a device acting as a default GW

Steps for Router Failover

When the active router fails: Redundancy protocol transitions standby router to new active router role

These steps take place when active router fails:

1. Standby router stops seeing Hello msgs from fwding router
2. Standby router assumes role of fwding router
3. B/C the new fwding router assumes both IP/MAC of virtual router: Hosts sees no disruption in service

First Hop Redundancy Protocols

FHRP: First Hop Redundancy Protocols:

HSRP	**Hot Standby Router Protocol:** • Cisco-proprietary FHRP designed to allow transparent failover of 1st-hop IPv4 device • Provides high network availability by providing 1st-hop routing redundancy for IPv4 hosts • On networks config w/IPv4 default GW • Used in group of routers for selecting an active/standby device **In group of device ints:** • Active device is one used for routing packets • Standby is device that takes over when active fails/pre-set conditions met **Function of HSRP standby:** • Monitor operational status of HSRP group/quickly assume packet-fwding responsibility if active router fails
HSRP for IPv6	**Cisco: HSRP IPv6 group has virtual MAC address derived from:** • HSRP group #/virtual IPv6 link-local address derived from HSRP virtual MAC address • Periodic router adverts (RAs) sent for HSRP virtual IPv6 link-local address when HSRP group active • When group becomes inactive these RAs stop after final RA is sent
VRRPv2	**Virtual Router Redundancy Protocol version 2:** • Non-proprietary election protocol • Dynamically assigns responsibility for 1/more virtual routers to VRRP routers on IPv4 LAN • Allows 7 routers on multiaccess link to use same virtual IPv4 address • Config'd to run VRRP protocol in conjunction with 1/more other routers attached to LAN **In a VRRP config:** • 1 router elected as virtual router master • Other routers act as backups in case virtual router master fails
VRRPv3	**Supports IPv4/IPv6 addresses:** • Works in multi-vendor envs/More scalable than VRRPv2

GLBP	**Gateway Load Balancing Protocol:** • Cisco-proprietary FHRP that protects data traffic from failed router/circuit (like HSRP/VRRP) • Also allows load balancing bet group of redundant routers
GLBP for IPv6	**Same functionality of GLBP for IPv6:** • Provides auto router backup for IPv6 hosts config'd w/single default GW on a LAN • Multiple 1st-hop routers on LAN combine to offer single virtual 1st-hop IPv6 router • While sharing IPv6 packet fwding load
IRDP	**ICMP Router Discovery Protocol:** • RFC 1256: Legacy FHRP solution • Allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks

HSRP

HSRP Verification:	○ Responds to default GW's ARP requests w/virtual router's MAC ○ Assumes active fwding of packets for virtual router ○ Sends Hello msgs ○ Knows virtual router IP
HSRP standby router	○ Listens for periodic Hello msgs ○ Assumes active fwding of packets if it doesn't hear from active router ○ **show standby** to verify HSRP state

GLBP Verification

Only active router in HSRP/VRRP groups fwds traffic for virtual MAC's

- Resources associated w/standby router are not fully utilized
- Can accomplish some load balancing w/these protocols by creating multiple groups/assigning multiple default GW's
- Burden

GLBP	**Cisco solution:** • Allows auto selection/simultaneous use of multiple available GW's in addition to auto failover bet them • Multiple routers share load of frames that are sent to a single default GW address **Has following:** • Allows full use of resources on all devices w/out burden of creating multiple groups • Provides single virtual IP/multiple virtual MAC's • Routes traffic to single GW distributed across routers • Auto rerouting in event of failure **show glbp** To verify GLBP status