Spanning Tree Protocol

Jan 2024

Introduction

This is a much simplified introduction to Spanning Tree Protocol on Cisco switches. In general, with our AQB solution, we would have two data switches with a single link, and so would not see the issues listed here. However it is useful to understand Spanning Tree Protocol (STP) to be able to identify issues if some switches have been mis-configured.

Spanning Tree Protocol essentially stops packet loops (where the same packet transports around your switches constantly) which causes broadcast storms and thus grinds the network to a complete halt.

Spanning Tree is a Layer 2 Protocol.

Types of Spanning Tree Prototol

```
STP / 802.1D - The Original STP. (on a Cisco Switch you might see this: Spanning tree enabled protocol
ieee.
PVST+ - Cisco improvement of STP adding a Per VLAN feature.
RSTP / 802.1w - (Rapid STP) Improved STP with much faster Convergence.
Rapid PVST+ - Cisco improvement of RSTP adding Per VLAN feature.
```

Convergence is where Switch ports can change state much faster than the older STP. This is very important because without RSTP it can take around a minute for a switch convergence change, which is a very long time.

Switch Layout

Spanning Tree Protocol is designed to block multiple routes where the same packet (frames) can get to any destination using multiple routes, look at the diagram below.

This switch configuration, while required for redundancy within the network, without Spanning Tree Protocol causes the following issues.

Broadcast Storm

This is important to understand:

When a switch receives a broadcast message, that switch will forward that message out of every interface on that switch, except the one it was received on.

So all interfaces on switch B will forward the message, so Switch A and Switch C get that message, then Switches A and C broadcast that message again, and it comes back to Switch B, rinse and repeat and you have a Broadcast Storm or what some refer to as a Packet Storm.

The reason this occurs is because a Loop has been formed.

Unstable MAC Address Tables

When a switch receives a frame, the switch adds the MAC address and Port number the frame came in on to what is called a Mac Address Table. This issue when you have a Loop due to the same frame coming in to different interfaces is that the switch has to keep updating its Mac Address Table.

In the Broadcast Storm scenario, the switch will keep receiving the same message in different Interfaces, so all the Switches will be constantly updating their MAC Address Tables.

This causes Unstable MAC Address Tables.

Duplicate Frames

Looking at the two Devices, if Device A sends a message to Device B, assuming Switch B does not know where Device B is, then Switch B will broadcast out of all of its interfaces, that message. Then Switch A and Switch C will receive that message, Switch C will then forward the message to Device B, that's good.

However, Switch A has also forwarded the packet to Switch C, which in turn forwards it to Device B, Device B is confused because it now has duplicate frame. So in this scenario, we have lots of Duplicate Frames going to devices.

Solution

It should be obvious from this article that using Spanning Tree Protocol is the answer, but what essentially does Spanning Tree Protocol do? Before talking about some of the processes behind Spanning Tree Protocol, let us look at the basic thing Spanning Tree Protocol does to resolve our issue.

Spanning Tree Protocol is able to detect Loops and deal with them by putting an interface in to Blocking Mode. The Blocked interface still receives the data, it just ignores it, thus resolving the Loop issue.

Once an interface is blocked, there are not Broadcast Storms, Unstable MAC Addresses and no Duplicate Frames.

What Spanning Tree Protocol really does is, via a strict process, Spanning Tree Protocol choses which Interface to put in to Blocking Mode on which Switch.

Spanning Tree Protocol Process

This is a high level explanation, I am sure there is much more to STP, but this should suffice for what we require.

There are several Steps that Spanning Tree Protocol follows, and they are:

```
1. Elect a Root Bridge.
2. Place Root Bridge Interfaces in to Forwarding State.
3. Each Non-Root switch choses its Root Port. This is the best route to the bridge (based on cost etc).
4. Remaining Links choose a Designated Port.
5. All other ports are placed in to a Blocking State.
```

We can visualise this using the diagram below:

Cisco has several modes for Spanning Tree Protocol. What we have looked at above is the standard Spanning Tree Protocol, but Cisco also has PVST, Per Vlan Spanning Tree.

PVST means that you can have Spanning Tree Protocol running on Multiple VLANs, where each VLAN has a different Root Bridge. PVST is the default mode for Cisco Switches when using Spanning Tree Protocol.

Port Roles

Roles define the function of each port.

```
Root Ports - The best port on a switch to reach the Root Bridge.
Designated Port - The Port with the best route to the Root Bridge on a link. Based on the best (lowest)
```

```
Cost.
Non-Designated Port - All other ports that are in a Blocking State.
```

Port States

States define the state of each port. Ports can change state while moving from one role to another.

```
Disabled - A port that is Shutdown.
Blocking - A port that is Blocking traffic.
Listening - Not Forwarding traffic and not Learning MAC Addresses.
Learning - Not Forwarding traffic but learning MAC Addresses.
Forwarding - Sending and Receiving traffic as normal.
```

Listening and Learning are 'Transitional' States, ports will enter these states while changing from one role to another.

Root Bridge Election

This covers the way a Root Bridge is elected 'automatically'

The way switches elect a Root Bridge is using a BPDU. The BPDU contains:

```
The Root Cost
The Root BID
The Local BID
```

A BID or Bridge ID is a key factor to choosing a Root Bridge.

Root Cost:0
Local BID: 32769aaaa:aaaa:aaaa
Root BID: 32769aaaa:aaaa:aaaa

The BID is made up of:

STP Priority + MAC Address
STP Priority default value is 32768 + VLAN ID (VLAN 1 in this example)

The switch with the lowest overall BID will become the Root Bridge.

On start up, all switches will assume they are the Root Bride and list themselves in the BPDU as the Root Bridge. The Switches then share BPDUs with each other. Once the two switches that do not have the lowest BID work this out, they will change their BPDU to list the switch with the lowest BID as the BPDU.

Once this process is complete:

All Ports on the Root Bridge enter a Forwarding State. While this will not be discussed here in any detail, all the other port decisions (Root Ports, Designated Port etc) are all based on Port Cost.

Check Spanning Tree Status

To check the status of Spanning Tree, Telnet in to the switch and use the following: (This command was performed on a Cisco Switch that had been factory reset, it is an older Cisco and on any newer units you might see a different result).

```
sh span
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0006.f680.1f80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     1cde.a755.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p
```

There is a lot of information here.

```
Spanning tree enabled -  Good, Spanning Tree is enabled on this switch (by default Cisco Switches enable
STP)
protocol -               ieee (this is the 802.1D standard, or the 'original' Spanning Tree Protcol)
Priority 32778 -         This is the 32768 default value plus the VLAN (100).
Address 0006.f680.1f80 - The MAC address of the Switch.
Cost 19 -                The Cost
Port 1 (FastEthernet0/1) The Interface being used for STP
```

Set/Change Spanning Tree Mode

If we want to change the Spanning Tree mode, then we can use a very simple set of commands:

Using the Switch Telnet Interface:

```
en
conf t
spanning-tree mode ?

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

(we want rapid-pvst)

spanning-tree mode rapid-pvst
```

You will not see out output from using this command (unless you get an error) but by using the sh span again you will see that the mode has changed.

```
end (back to top level of Cisco Telnet)

sh span

sh span

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     0006.f680.1f80
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     1cde.a755.6980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 19        128.1    P2p Peer(STP)
```

Now it can be seen that the protocol is listed as rstp (Rapid Spanning Tree Protocol)

Spanning Tree and Portfast

Part of the Spanning Tree Protocol is where a port has to change role, say when a device is plugged in to the switch, the switch may have to transition from Blocking mode to Forwarding mode. PortFast is a Cisco proprietary protocol.

A quick reminder of port modes:

```
Blocking - A port that is Blocking traffic.
Listening - Not Forwarding traffic and not Learning MAC Addresses.
Learning - Not Forwarding traffic but learning MAC Addresses.
Forwarding - Sending and Receiving traffic as normal.
```

A Blocking Port cannot move to a Forwarding port directly (normally) the Blocking Port has to transition as follows:

```
Blocking

  Listening - 15s

  Learning - 15s

Forwarding
```

Any device connected to a port can only connect to the network after transitioning through all of those states. This can take around 30 seconds (or longer if switch is busy). This is why when you plug a device in to a Cisco, it can take 30 seconds before the interface goes green.

During this 30 seconds, no user data is available on this port.

Spanning Tree Portfast allows a port to transition to the forwarding state immediately, bypassing the Listening and Learning states.

Spanning Tree Portfast should be configured on edge ports where you can expect client PCs, Servers, Printers etc. Basically any port that is not part of a STP loop that expects STP messages or BPDUs.

Having said that, Portfast will not stop STP operation, if that port receives any STP or BPDU messages, it will revert back to 'normal' mode and participate in Listening and Learning modes.

Two Switches with Single Link

For what we do with our systems, there are generally two data switches between devices, with a link between them (per VLAN) which looks like this diagram below:

In this example, we can see just a single link from Switch A to Switch B. This means that there cannot be any Loops, so STP would not be required here (although it is worth remember that STP in some form runs on a Cisco be default).

Remember this Statement regarding STP - ***When a switch receives a broadcast message, that switch will forward that message out of every interface on that switch, except the one it was received on.***

Having STP running is not going to cause any issues, and in fact as a safety measure is still quite good (who knows who might bridge the switches with a second cable).