Spanning tree best practices cisco

The distinctive characteristic is highlighted as an improved internal statement routing internal routing protocol (EIGRP) is an internal gateway protocol suitable for many different topology and media. In a well-designed network, EIGRP scales well provides very fast convergence... View more hello we have 2 data centers with a direct connection to AWS Run BGP. The US DC announces that it/19 your domain and DC CA declares /12, the problem is that /19 falls within the /12 range. Is there a way to prevent DC from CA ... View more hi-guys, I have two questions about eIGRP behavior when we have multiple EIGRP methods: 1- I tried to appear on some router eIGRP paths acquired for the X.X.X track by typing command: show ip eigrp topology X.X.X. X. on output there w... View more goal network management to provide a solution to quickly set up a router in a remote location that supports Wi-Fi and provides instant access to the Internet using LTE as a means of transportation while deploying with Cisco SD-WAN. Remote factor connecting the router to power sou... View more of the highlights! Can you share what will be configuracion of SVI with a stretch tree please? Thank you. Distinguished by the distinctive distinctive distinctive distinctive highlighted enhanced by the Internal Gateway Guidance Protocol (EIGRP), it is an internal gateway protocol that fits many different media topology. In a well-designed network, EIGRP scales well provides very fast convergence... View more hello we have 2 data centers with a direct connection to AWS Run BGP. The US DC announces that it/19 your domain and DC CA declares /12, the problem is that /19 falls within the /12 range. Is there a way to prevent DC from CA ... View more hi-guys, I have two questions about eIGRP behavior when we have multiple EIGRP methods: 1- I tried to appear on some router eIGRP paths acquired for the X.X.X track by typing command: show ip eigrp topology X.X.X. X. on output there w... View more goal network management to provide a solution to quickly set up a router in a remote location that supports Wi-Fi and provides instant access to the Internet using LTE as a means of transportation while deploying with Cisco SD-WAN. Remote factor connecting the router to power sou... View the most prominent highlights can you please help me to find out why, as I want to connect the trunk link again. Thank you, Abhisar, highlighted by the enhanced highlight of the Internal Gateway Steering Protocol (EIGRP), an internal portal protocol suitable for many different media topology. In a well-designed network, EIGRP scales well provides extremely fast View more hello we have 2 data centers with a direct connection to AWS Run BGP. The US DC announces that it/19 your domain and DC CA declares /12, the problem is that /19 falls within the /12 range. Is there a way to prevent DC from CA ... View more hi-guys, I have two questions about eIGRP behavior when we have multiple EIGRP methods: 1- I tried to appear on some router eIGRP paths acquired for the X.X.X track by typing command: show ip eigrp topology X.X.X. X. on output there w... View more goal network management to provide a solution to quickly set up a router in a remote location that supports Wi-Fi and provides instant access to the Internet using LTE as a means of transportation while deploying with Cisco SD-WAN. Remote factor connecting the router to power sou... View more let me start by saying that stretching a tree is a good thing. It provides you with loops, which will completely close down the grid. But it must be configured correctly to work properly. I can't count how many times I have had a client contact me, desperate with a terribly broken network, and I've responded, it looks like a stretching tree problem. There are many ways in which things can go wrong with a stretching tree. In this article I've collected a few recurring topics. As I said, stretching a tree is a good thing. But for some reason, a lot of switch vendors disable it by default. So outside the box, you may have to enable the protocol. Sometimes people deliberately disable the stretch ing tree. The most common reason for blocking a stretch ing tree is that the original 802.1D Stretch Tree Protocol (STP) goes through a fairly long waiting period of time it becomes an electrically active outlet to when it starts to pass traffic. This waiting period, usually 45 seconds, is long enough that DHCP can give up trying to get an IP address for this new device. One solution to the problem is simply disabling the stretching tree on the switch. This is the wrong solution. The correct solution is to configure a feature called PortFast on Cisco keys. (Most switch sellers have a similar feature.) The portfast tree configuration extends to all ports connected to end-of-end devices such as workstations. The waiting period is then automatically exceeded and the DHCP works correctly. It is only important to configure this command on ports that connect to peripherals. Ports connected to other switches need to share run tree information. Allowing the grid to choose the root bridge as the name suggests, the range tree solves the loops in the grid by creating a logical tree structure between the switches. The switch becomes one tree root, called root bridge. All the other keys then find out the best path to get to the root bridge. If there are multiple paths, then on each switch, the tree stretch determines the best path and puts all the other ports in blocking In this way, there is one path between any two devices on the grid, although it may not be circular. Each key involved in a stretching tree has a bridge priority. The lower priority switch becomes root bridge. If there is a draw, then switch with the lowest bridge ID number wins. The ID number is usually derived from the MAC address on the switch. The problem is that each switch by default has the same priority value (32768). So if you don't manually configure the best (lower) priority value bridge on a particular key, the grid will simply select the root for you. Then the Murphy Act applies. The resulting root bridge can have some small edge switch with slow ascending links and limited rear resources. To make things worse, the bad choice of root bridge can make the grid less stable. If there is a communication problem that takes any random switch off the grid, stretching the tree heals fairly quickly. But if the root bridge goes down, or if the failure means that some keys no longer have a path to the root bridge, this constitutes a major topology change. A new root bridge must be selected. The entire network will be frozen during this time and no packages can be redirected. I always recommend making a basic root bridge switch. I also like to select root bridge backup. If there are redundant double basic keys, then one is root bridge and the other becomes my backup. Set the priority of the bridge on the primary root bridge to the best possible value —4096- and the backup root bridge to the next best value -8192. Why are these funny numbers? Well, that's a longer story we don't have space here, but less prioritized bits have another goal, so they're not available for use as priorities. Stretch Tree saves you from loops/photos: A dark day on Flickr using the old 802.1D is called the first open standard for a tree stretching 802.1D. It is one of the oldest standards in the IEEE 802 series of standards that includes specifications for each type of Ethernet and Wi-Fi as well as a range of other protocols. It works well despite its age, and you'll find this kind of tree extending on almost every key. Any 802.1D switch that does not support is only useful in small isolated environments, and should not be connected to any other switches. But there have been many important developments for the tree stretching since 802.1D. These improvements allow for sub-second convergence after the link fails, as well as the ability to scale to larger grids, the ability to obtain different distributed tree topology and different root bridges for different VLAN networks. So it makes sense to use it. Cisco switches the most modern virtual to a protocol called PER-VLAN RSTP. This symbolizes the protocol of a rapid stretch ing tree. It automatically works separately The tree area with a separate root bridge on each local local network. In practice, it is common to make the same root bridge switch on all or most vlaNs, though. The quick feature or RSTP is what you'll find perhaps the most useful. This allows the network to recover from most failures at times on an order of 1 to 2 seconds. A multi-instance tree extension or MST, similar to RSTP. The main difference is that you can set groups of VLAN that are all part of the same tree structure with a single common root bridge. However, I recommend using all-VLAN RSTP in most cases because it is easier to configure. Also, I've encountered some interoperabilty problems with MSTP among the various switch vendors. Mixing tree types that stretch should be very clear from the descriptions of 802.1D, RSTP, and MST in the previous section that mixing them can get messy. RSTP and MST protocols have rules for how to handle this mixing, and in general they involve creating separate areas within the grid for groups of keys running different flavors of a stretch tree. This is rarely the result of the most efficient paths that are identified between devices. The only really valid reason for mixing tree-stretching species is to allow the inclusion of old equipment that does not support more modern protocols. Over time, there should be fewer and fewer of these older devices, and the number of places where it makes sense to mix protocols should be smaller. I recommend choosing one, preferably RSTP or MST, and just use it in a consistent way across all your keys. Photo: the svensson on Flickr using MST with trim trunks because MST allows one stretching structure tree that supports multiple VLANs, you need to be very careful about the trunks switching between your. I once had a large complex network client involving many keys and many VLANs networks. They ran MST. For simplicity, they had appointed one MST instance, meaning that all VLANs were controlled by the root bridge itself. The problem for this client arose when they decided that they should only be present on certain switches for security reasons. Everything is perfectly reasonable. So they removed the VLAN network of the main inter-switch trunks, and added only new special trunks to these safe VLANS. Everything broke mst all the VLAN was considered to be part of the same tree and has chosen any trunks to prevent which will be redirected based on this assumption. But in this case, because some VLAN carriers were only present on some trunks and other VLANs were present on other trunks, preventing the trunk only meant passing some of vlaNs. Blocking the other trunk only means passing another set of VLANs. For the banned VLANs, there was simply no track to the root bridge at all. So, if you're going to use MST, you either need to make sure that all VLANs are passed on to all Or you need to carefully and manually create different MST instances for each set of VLANs with special topological requirements. In other words, you have to do accurate analysis and design the network correctly. Or you could take an easy way out and run all-VLAN RSTP. The conflicting root bridge and HSRP/VRRP are another common problem with stretching tree networks that sometimes interact in terms of layer 2 and 3 repetition mechanisms. Let's say I have a grid core consisting of two layer 3 switches. On each piece I want these basic keys to serve as redundant virtual portals. And I want to connect all of the extra estuary keys to all of the basic keys and make stretch tree remove loops. In this scenario, the tree root bridge may be stretching to a particular VLAN on one of these primary switches and hSRP/VRRP main default statement on the other switch. Then the Ethernet window that arises on one of the transducers of information-oriented information to the default statement will need to take an additional leap, first to the root bridge, then to the secondary primary switch that currently owns the default ferry IP. Normally this is not a problem, but imagine that I pass the packets between two VLANs, both with the Basic A switch as a root bridge and b basic switch as a virtual gateway. Each package must rise to switch A, cross the spine link to get routed on Core Switch B. Then the spinal link must be crossed back to return to switch A to be delivered to its destination. All back-link packets must also cross the spine twice. This creates a huge burden on the traffic on the spine link where each package must cross in both directions twice. It also causes a late-time penalty as each package needs to be sequenced and sent twice. Even on 10Gbps links, this usually costs a couple of microseconds in both directions, which can add up to particularly sensitive applications. Suppose instead that the default statement was on the same switch as the root bridge. Now the package goes up to the root bridge, switch core A, and gets steered between the VLANs and immediately turned into a device for the recipients of the information. The spine does not cross at all in either direction. Stretching tree is a wonderfully important protocol. Allows us to build redundancy in switch-between connections. It saves us from catastrophic episodes when someone accidentally connects things they shouldn't. It is true that the stretch tree can be misprepared with bad consequences, but this possibility should not dissuade you from using it. The solution is to be careful and thoughtful about network design. Design.