

STP, RSTP, MSTP

Essentials: Adjusting timer values for STP, RSTP, MSTP

Agenda

- Finish Ch 3 – STP slide decks
- Start Ch 6 – L2 Security

Assignments and Lab prep

- Next Cisco online quiz: Ch 3 during lab on Wed Feb 15
eg. 10:30am or 1pm depending on your lab section
- Read **Chapter 6** of the course textbook this week
- Lab 6 **post-lab** is due **before** the beginning your lab period this week
- Lab 7 **pre-lab** is due **before** the beginning your lab period this week
- Lab work: Lab07 posted on course web site; L2 security, especially portfast & BPDU guard; very relevant to NET3007.

STP: *Many Options*

Remember: *Loops are deadly to a network.* [1]

On tuning STP (802.1D) parameters:

“You can use this document to help you solve your networking issues, but only if you are familiar with the process or if someone who is familiar with the process has directed you. If you are unfamiliar with STP, changes that you make can cause any of these occurrences:

- Instabilities
- Application slowups
- CPU spikes
- LAN meltdown” [2]

. . .

”These values can seem quite conservative in a modern network, in which you are not likely to lose three BPDUs or to have 1 sec of latency for a frame through a switch. However, remember that these values exist in order to prevent STP loops that can occur in stress conditions, such as:

- Very high CPU utilization
- An overloaded port

Therefore, you must **consider these parameters as fixed values.**”
[emphasis added] [2]

On RSTP

“RSTP (IEEE 802.1w) natively includes most of the Cisco proprietary enhancements to the 802.1D spanning tree, such as **BackboneFast**, **UplinkFast**, and **PortFast**. RSTP can achieve much faster convergence in a properly configured network, sometimes in the order of a **few hundred milliseconds**. Classic 802.1D timers, such as forward delay and max_age, are only used as a backup and should not be necessary if point-to-point links and edge ports are properly identified and set by the administrator. Also, the timers should not be necessary if there is no interaction with legacy bridges.” [What about **hello??**] [3]

“In most cases, RSTP performs better than proprietary extensions of Cisco without any additional configuration.” [3]

Tuning Timers

CST or RSTP: `spanning-tree vlan {range} hello-time {1-10}`
`spanning-tree vlan {range} max-age {6-40}`
`spanning-tree vlan {range} forward-time {4-30}`

MSTP: `spanning-tree mst hello-time {1-10}`
`spanning-tree mst max-age {6-40}`
`spanning-tree mst forward-time {4-30}`

Be warned! *“However, until recently, redundant switched networks had to rely on the relatively sluggish 802.1d STP to achieve those goals. This often turned out to be the network administrator's most challenging task. The only way to get a few seconds off the protocol was to **tune the protocol timers**, but often at the **detriment of the network's health.**”* [4]

References (Note: **STA** = Spanning Tree Algorithm)

1. 802.1D: Understanding & Configuring Spanning Tree Protocol (STP)
www.cisco.com/en/US/tech/tk389/tk621/technologies_configuration_example09186a008009467c.shtml
2. Understanding and Tuning Spanning Tree Protocol Timers
www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094954.shtml
3. 802.1w: **Understanding Rapid Spanning Tree Protocol** [Best Reference]
www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml
4. 802.1s: Understanding Multiple Spanning Tree Protocol
www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml
5. Migrating to RSTP
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b0670.shtml
6. Migrating to MSTP
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b075f.shtml

L2 Security

How to digest Ch 6: textbook & slide deck:

#	Attack Name	Text pg	PPT pg	Purpose and Description	Severity	Counter-measures	Commands

Simplified list

1. MAC flooding attack – eavesdrop on traffic
1 What's allowed? **2** What do we do if rules are broken? **3** Prove it
Can limit MAC addresses, or use port authentication
2. VLAN hopping attack – double tagging
access mode; VACLs; pVLANs
3. Spoofing attacks: DHCP or ARP spoofing
DHCP snooping; IP source guard; Dynamic ARP Inspection (DAI)
4. Using switch info to gain access (CDP, telnet)
Disable both; use SSH