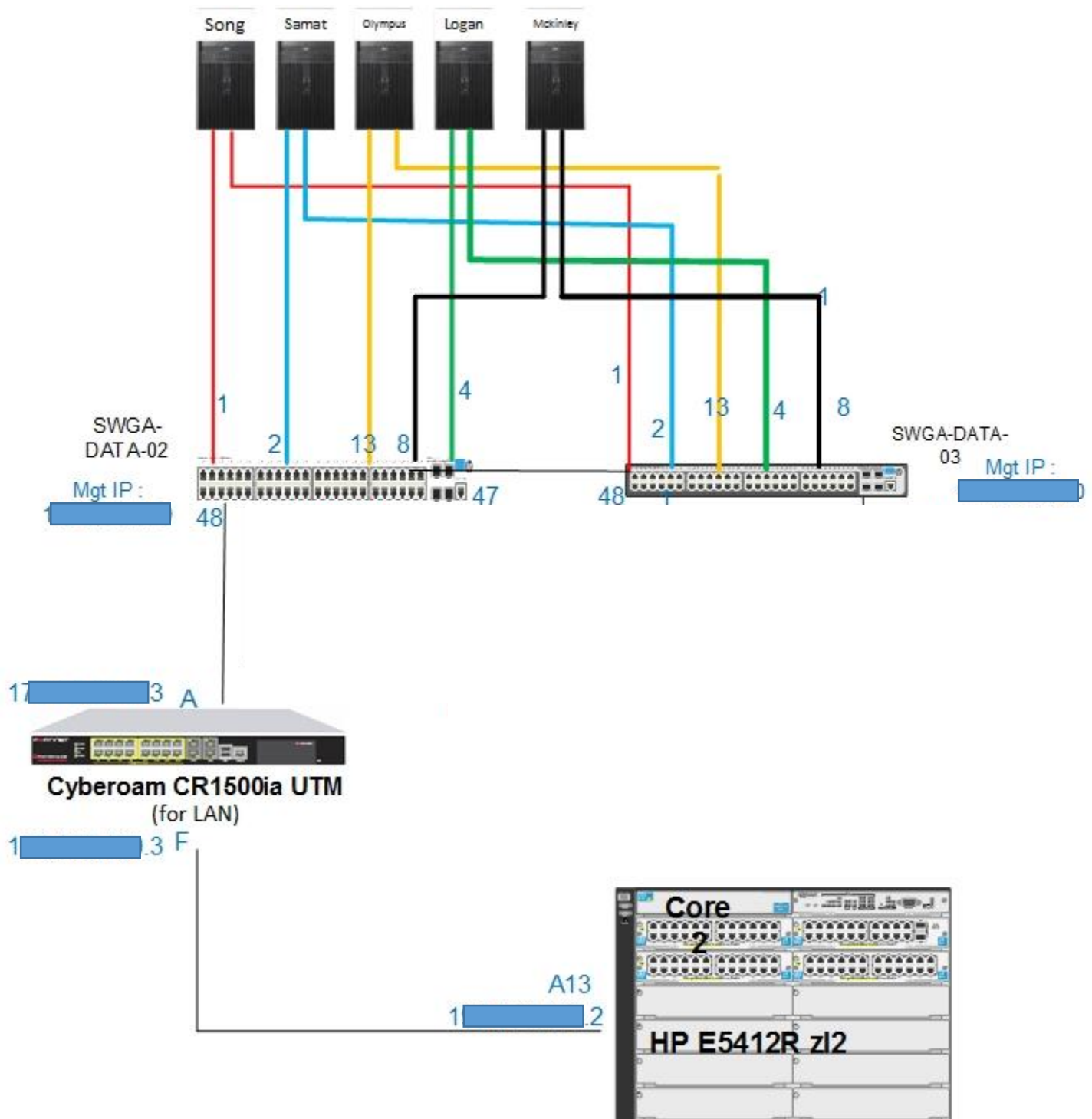


Strange Intermittent Network Connectivity

Problem Description:

1. Random PCs intermittently loose connectivity to the server while the rest of the PCs on the LAN are fine and continue to access the server just fine. When the issue occurs the random PC cannot ping the server. While the rest of the LAN can still ping the server just fine.
2. When the issue occurs, it only lasts for several seconds to 2 minutes at the most.
3. The issue started last week of March.



Troubleshooting Steps Performed:

1. Installed a network monitoring system from Solarwinds. The application was able to detect excessive CRC broadcast but we decided to adjust the threshold because it seems that the switches are just too sensitive when it comes to CRC.
2. The NMS did not detect any CPU utilization issue on the switches.
3. Installed Savious Omnippeek.

Scenario 1:

The server of Omnippeek was connected to Sw1. Thru port mirroring, we were able to monitor the packets coming in and out of the servers. During the time that the issue happened, the following data had the most number of results:

- a. High DNS error
- b. Kerberos Traffic

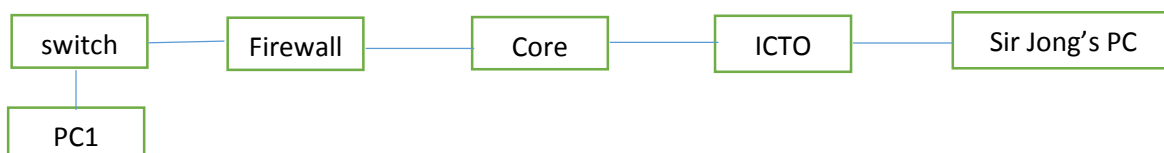
What we did:

- ➔ Temporarily removed the 172.27.35.225 DNS server and just used 172.27.35.218.
- ➔ Adjusted the Maxtoken size registry of Kerberos

Scenario 2:

The server of Omnippeek was connected to the firewall but we did not find any unusual activity which can possibly resolve the ongoing issue.

4. Replaced the cable connecting SWGA-DATA-02 to Firewall and the cable connecting the firewall to the core switch.
5. Power cycle the firewall and the core switch.
6. Replaced the 3 switches at the ICT Office (SWGA-ICTO-01, SWGA-ICTO-02, SWGA-ICTO-03)
7. Connected a computer to the switch where the servers are also connected (same VLAN too) and based on our observation, the computer did not experience any issue with the connection during the entire monitoring process. Thus, we were able to conclude that there is no issue with the connection from the firewall going to the servers.
8. Configured the ports on SWGA-DATA-02 to negotiate via full-duplex and the speed of each port was also changed to 1000.
9. Configured the port on the core switch and the port on the firewall to negotiate on full duplex.
10. Tried continuous ping from the firewall to the servers and the firewall did not encounter request timed out.
11. Connected the firewall to core2 last April 23rd then after one day of monitoring the connection, we decided to return it to its original connection which is core1 to firewall because no improvement happened.
12. We contacted Sophos and so far, they did not find any virus on the network/devices
13. Clear the arp table of the core.
14. Identified the top IPs when it comes to data usage.
15. Removed core1 from the network's infra.
16. Connected all cables back to core1
17. Reboot switches.
18. Reboot Ruckus.
19. Tried the topology below:



During the issue, we got the following results:

- a) PC 1 to Sir Jong's PC --- continuous ping/no drop
- b) Sir Jong's PC to PC1 – timed out

20. It was suggested that the teaming of the servers be removed in the meantime and just use one switch instead because a possible loop might be happening based on the topology on the part of the server switch.

21. Bypassed firewall and connected the core switch directly to the 172.27.100.29 switch of the server farm. We also disconnected almost all of the connections coming from the core switch then reconnect each cable every after 45 mins while monitoring the connection. We did not encounter any issue when we used that setup however, we've done the test late night when no one was using the network. Lastly, when we brought back the network to its original setup (firewall included), the logs indicated that the connection from sir Jhong's workstation experienced packet loss around 3:30am.

I hope someone will take time to help us. We are not actually using Cisco switches. Ours are from HP but I just want to try my luck here. We've been experiencing connection problem for almost 2 months now. When the issue happens, random PC loose connection to the to the server but it doesn't last long. Most of the time the issue happens for several seconds to 2 minutes at the most.

Here are the different scenarios that we encounter:

Scenario 1:

Workstation 1 -----> server 1 == continuous ping
Workstation 1 ----->server 2 === continuous ping
Workstation 2 ----->server 1 === continuous ping
Workstation 2 ----->server 2 === request timed out

Scenario 2:

Workstation 1 -----> server 1 == request timed out
Workstation 1 ----->server 2 === continuous ping
Workstation 2 ----->server 1 === continuous ping
Workstation 2 ----->server 2 === request timed out

Scenario 3:

Server 1 -----> Workstation 1 == no packet loss
Server 1 -----> Workstation 2 == no packet loss
Server 2 -----> Workstation 1 == no packet loss
Server 2 -----> Workstation 2 == no packet loss

Note: I also attached the detailed topology of our network and the troubleshooting steps that weve done. Thank you so much in advance.