GNS3 模拟环境中使用 Wireshark 抓 STP 协议报文

Oct. 23, 2024

1. 在 GNS3 中配置 wireshark [2, 3]

2. STP 协议报文的抓包解析 [1]

在 GNS3 环境中搭建了如下网络:

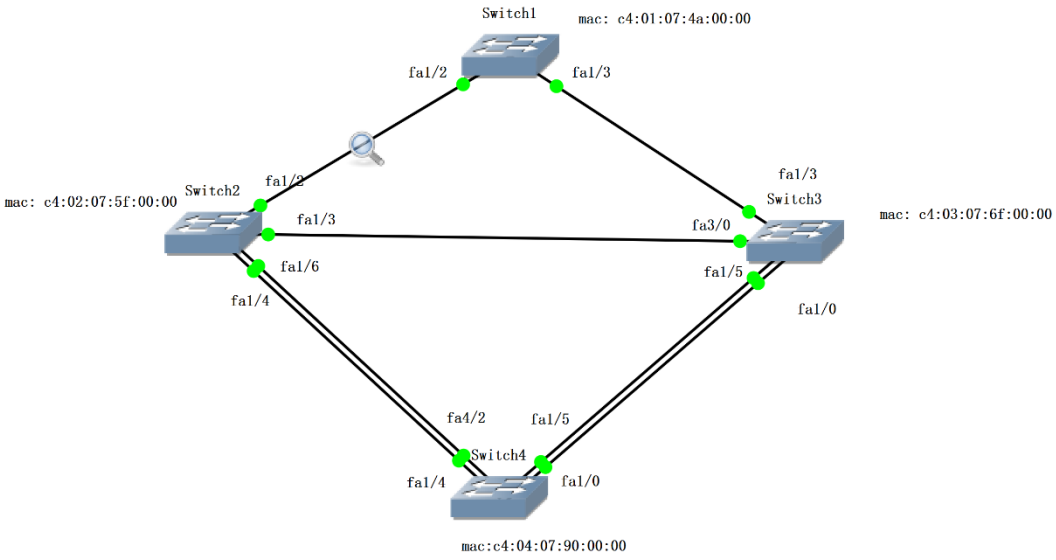


图 1、GNS3 模拟环境中网络架构

步骤：

1) 先按照[4]将 GNS3 中路由器配置成交换机，交换机间先不要连线，分别把 4 个路由器配置成交换机。
2) 把各个交换机连接起来，然后启动交换机，就会看到各个接口颜色显示为绿色。
3) 点击任何一个交换机就可以对交换机进行配置，就像在实体机上一样。可以用”show mac-address”查看交换机的 MAC 地址了。
4) 将鼠标移到连接 Switch 1 和 Switch 2 之间的连线上，右键鼠标选择”start wireshark”，就可以抓包了。
5) 交换机上可以采用”show spanning-tree”来展示网络中 spanning-tree 的一些重要信息。

下图就是捕获的 STP 报文了。

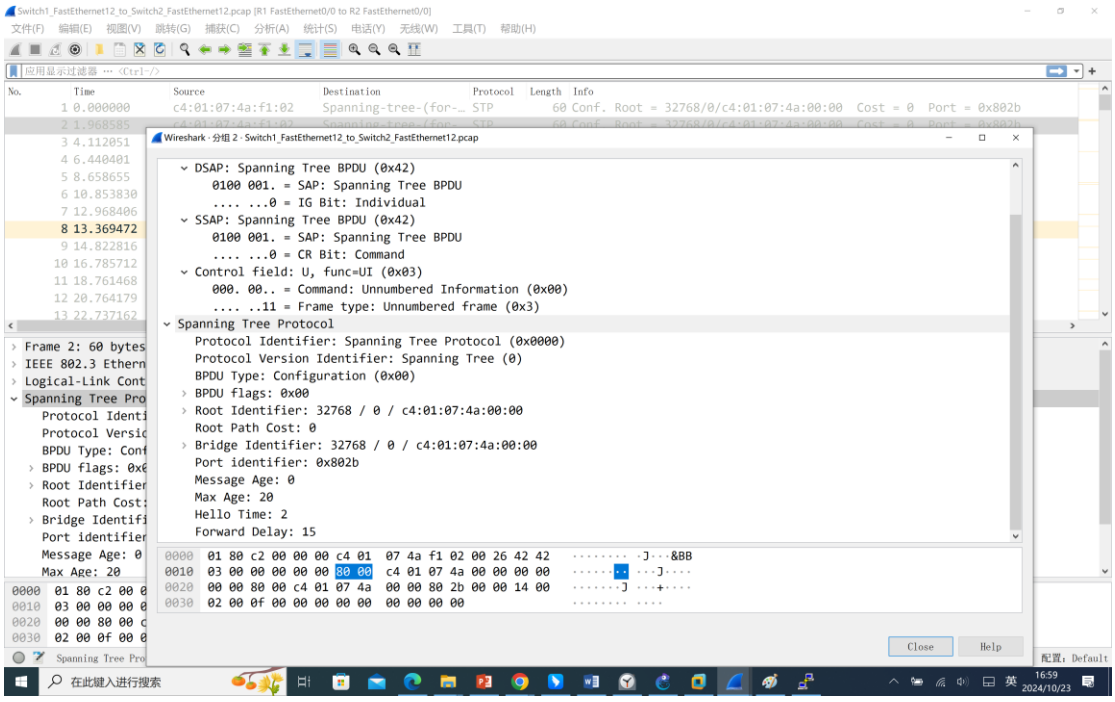


图 2、在 Switch 1 和 Switch 2 之间的连线上捕获的 STP 报文

STP 帧格式

字段内容	说明
Protocol Identifier	Spanning Tree Protocol (0x0000)
Protocol Version Identifier	Spanning Tree (0)
BPDU Type	Configuration (0x00)
BPDU flags	0x00
Root Identify	根桥的桥 ID。网桥 ID 都是 8 个字节——前两个字节是网桥优先级，后 6 个字节是网桥 MAC 地址。
Root Path Cost	根路径开销，本端口累计到根桥的开销。
Bridge Identify	本交换机的桥 ID。
Port identifier	发送该 BPDU 的端口 ID
Message Age	BPDU 在网络中传播的生存期
Max Age	BPDU 在设备中能够保存的最大生存期
Hello Time	两个相邻交换机发送 BPDU 的时间间隔
Forward Delay	端口状态迁移的延时

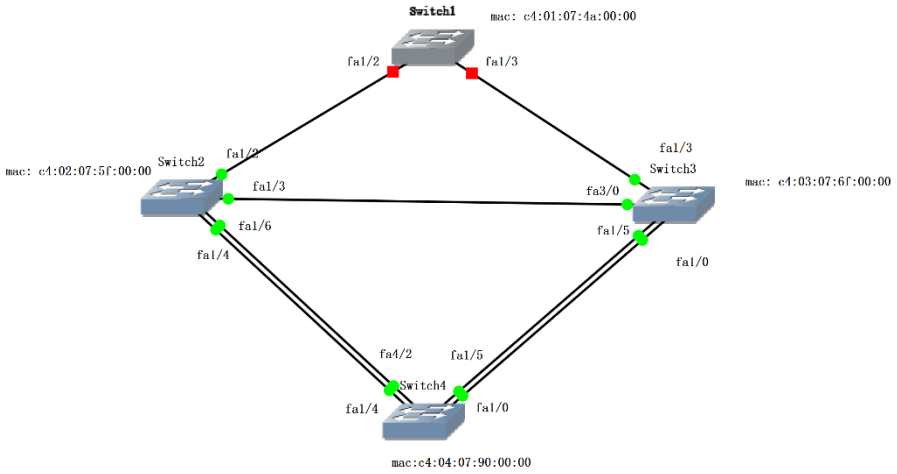
STP 协议中一些重要的时间参数：

1) **Hello Time**: 交换机每隔 Hello Time 时间会向周围的交换机发送配置 BPDU 报文，以确认链路是否存在故障。当网络拓扑稳定后，该值只有在根桥上修改才有效。默认的 Hello Time 的值是 2 秒。
2) **Message Age**: 如果配置 BPDU 是根桥发出的，则 Message Age 为 0。否则，Message Age 是从根桥发送到当前桥接收到 BPDU 的总时间，包括传输延时等。实际实现中，配置 BPDU 报文每经过一个交换机，Message Age 增加 1。
3) **Max Age**: 注意在网络中任何数据包都有它们自己的生存期。是指 BPDU 报文的最长生存时间，可在根桥上通过命令人为改动这个值。Max Age 通过配置 BPDU 报文的传递，可以保证 Max Age 在整网中一致。非根桥设备收到配置 BPDU 报文后，会将报文中的 Message Age 和 Max Age 进行比较：如果 Message Age 小于等于 Max Age，则该非根桥设备会继续转发配置 BPDU 报文。如果 Message Age 大于 Max Age，则该配置 BPDU 报文已经过了生存期，该非根桥设备将直接丢弃该配置 BPDU。默认的 Max Age 值是 20 秒。
4) **Forward Delay**: 当拓扑发生变化，新的配置消息要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，一般指从 listening 状态到 learning 状态，或是从 leaning 状态到 Forwarding 状态所需要的时间，协议默认的 Forward Delay 值是 15 秒。

STP 协议通过在交换机之间传递配置 BPDU 来选举根交换机,以及确定每个交换机端口的角色和状态。在初始化过程中，每个桥都主动发送配置 BPDU。在网络拓扑稳定以后，只有根桥主动发送配置 BPDU，其他交换机在收到上游传来的配置 BPDU 后，才会发送自己的配置 BPDU。

BPDU 有两种类型：配置 BPDU 和 TCN BPDU。配置 BPDU 描述本设备的配置信息，包含了桥 ID、路径开销和端口 ID 等参数。TCN BPDU 是指下游交换机感知到拓扑发生变化时向上游发送的拓扑变化通知。

模拟出故障情形一：当我把 Switch1 停止时，根网桥重新选举 Switch 2 因为 MAC 地址最小被推举为新的根网桥。



下图是在 Switch 2 上显示 spanning tree 的相关信息。我查看了一下所有交换机的优先级都为 32768。所以选举根网桥主要就是根据交换机的 MAC 地址，谁的 MAC 地址最小，谁就是根网桥。

```
% Ambiguous command:  "dis stp"
Switch2#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c402.075f.0000
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag set, detected flag set
  Number of topology changes 2 last change occurred 00:00:05 ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 31, notification 0, aging 300

 Port 43 (FastEthernet1/2) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.43.
   Designated root has priority 32768, address c402.075f.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.43, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 4, received 2162

 Port 44 (FastEthernet1/3) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.44.
   Designated root has priority 32768, address c402.075f.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.44, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 2160, received 0

 Port 45 (FastEthernet1/4) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.45.
   Designated root has priority 32768, address c402.075f.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.45, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 2171, received 3

 Port 47 (FastEthernet1/6) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.47.
   Designated root has priority 32768, address c402.075f.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.47, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 2171, received 4

Switch2#
```

当我重新启动交换机 Switch 1 后，查看 Switch 4 上 spanning tree 信息如下图，可以看出 Switch 4 上除了接口 Fa1/4 之外，其余三个接口 Fa1/0，Fa1/5，Fa4/2 都被阻塞了，这样就不会形成回路。可以采用"show mac-address-table"查看交换机上 MAC 地址表。

```
Switch4#
Switch4#show spanning-tree

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address c404.0790.0000
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address c401.074a.0000
  Root port is 45 (FastEthernet1/4), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 3 last change occurred 00:05:46 ago
          from FastEthernet1/5
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 41 (FastEthernet1/0) of VLAN1 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.41.
   Designated root has priority 32768, address c401.074a.0000
   Designated bridge has priority 32768, address c403.076f.0000
   Designated port id is 128.41, designated path cost 19
   Timers: message age 4, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 2231, received 2215

 Port 45 (FastEthernet1/4) of VLAN1 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.45.
   Designated root has priority 32768, address c401.074a.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.45, designated path cost 19
   Timers: message age 7, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 6, received 4473

 Port 46 (FastEthernet1/5) of VLAN1 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.46.
   Designated root has priority 32768, address c401.074a.0000
   Designated bridge has priority 32768, address c403.076f.0000
   Designated port id is 128.46, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 2231, received 2250

 Port 163 (FastEthernet4/2) of VLAN1 is blocking
   Port path cost 19, Port priority 128, Port Identifier 128.163.
   Designated root has priority 32768, address c401.074a.0000
   Designated bridge has priority 32768, address c402.075f.0000
   Designated port id is 128.47, designated path cost 19
   Timers: message age 7, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   BPDU: sent 6, received 4475
```

模拟出故障情形二：当我把 Switch2 停止时，根网桥不变，还是 Switch1，因为 MAC 地址最小。这时我查看 Switch4 上的 spanning tree 信息，一开始接口 Fa1/0 的状态是 listening，接口 fa1/4 的状态还是 forwarding，接口 fa1/5 的状态还是 blocking，接口 Fa4/2 的状态是 learning。过一会儿，Switch4 上的除了 fa1/5 的状态是 blocking 意外，其余三个全是 forwarding。可以在每条链路上用 wireshark 抓包。抓包过程还发现 CDP 数据包，CDP 是 Cisco Discovery Protocol 的缩写，

它是由思科公司推出的一种私有的二层网络协议，它能够运行在大部分的思科设备上面。通过运行 CDP 协议，思科设备能够在与它们直连的设备之间分享有关操作系统软件版本，以及 IP 地址，硬件平台等相关信息。Wireshark 捕获的数据包可以在你设置 GNS 实验 project 名称目录下的\project-files\captures 子目录中找到，比如我所捕获的数据，就在 E:\ComputerNetworks\2024\Slides\4_MACLayer\实验\STP\project-files\captures 目录下。

参考链接

[1] https://www.cnblogs.com/zylSec/p/14627690.html (STP 协议报文的抓包解析)

[2] https://blog.csdn.net/qq_20388417/article/details/105024425 (4 步教你如何在 GNS3 中使用 wireshark 抓包)

[3] https://blog.csdn.net/explorer9607/article/details/82750521 (在 GNS3 中 Wireshark 抓不到包的缘故)

[4] https://blog.csdn.net/weixin_45726050/article/details/102592953 (GNS3 中交换机建立与接口配置)