实验：LAN 技术

HCIE 综合实验 - LAN 技术

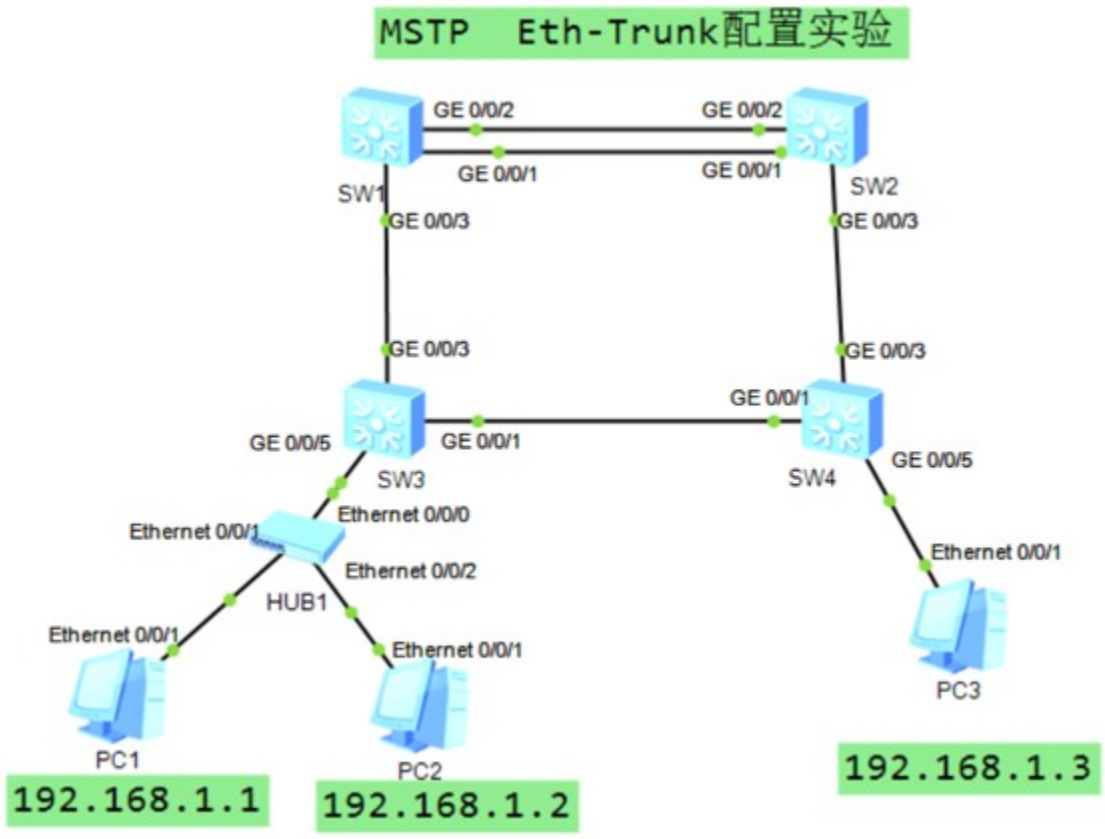
臧家林制作

LAN 技术 1： MSTP Eth-Trunk
LAN 技术 2： STP 选举
LAN 技术 3： RSTP 保护

= = = = = = = =

LAN 技术 1： MSTP Eth-Trunk

以太网是当今现有局域网 LAN（Local Area Network）采用的最通用的通信协议标准，以太网作为一种原理简单、便于实现同时又价格低廉的局域网技术已经成为业界的主流。
本实验主要介绍了 LAN 网络中的 Eth-Trunk 技术和 MSTP 技术。



==========

mac 地址

MAC 地址表记录了交换机学习到的其他设备的 MAC 地址与接口的对应关系，以及接口所属 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式在所属 VLAN 内除接收接口外的所有接口转发该报文。

mac 表的组成可以分为动态、静态和黑洞

动态表项

交换机刚启动时 mac-add 是空的，没有任何内容

```
[SW3]dis mac-add
[SW3]
```

两台 pc 相互 ping 一下

```
PC>ping 192.168.1.3

Ping 192.168.1.3: 32 data bytes, Press Ctrl_C to break
From 192.168.1.3: bytes=32 seq=1 ttl=128 time=63 ms
From 192.168.1.3: bytes=32 seq=2 ttl=128 time=62 ms
From 192.168.1.3: bytes=32 seq=3 ttl=128 time=63 ms
From 192.168.1.3: bytes=32 seq=4 ttl=128 time=78 ms
```

可以通信后，可以看到 mac-add 中有两台 PC 的 mac 地址

```
[SW3]dis mac-add
MAC address table of slot 0:
-------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port           Type
               VSI/SI
-------------------------------------------------------------------------
5489-9842-64f9 1           -      -      GE0/0/5        dynamic
5489-98f5-694b 1           -      -      GE0/0/1        dynamic
-------------------------------------------------------------------------
```

动态表项，默认老化时间 300 秒，也可以修改
mac-add aging-time 500

```
[SW3]dis mac-address aging-time

  Aging time: 300 seconds
```

静态表项

交换机默认所有接口都在 vlan 1 中
mac-address static aaaa-bbbb-cccc g0/0/5 vlan 1

```
[SW3]dis mac-add
MAC address table of slot 0:
-------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port           Type
               VSI/SI
-------------------------------------------------------------------------
aaaa-bbbb-cccc 1           -      -      GE0/0/5        static
-------------------------------------------------------------------------
```

黑洞表项
通过配置黑洞 MAC 地址表项，可以过滤掉非法用户。
配置黑洞 MAC 地址后，源 MAC 地址或目的 MAC 地址是该 MAC 的报文将会被丢弃。

mac-add blackhole aaaa-bbbb-1234

```
[SW3]dis mac-add
MAC address table of slot 0:
-------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port           Type
               VSI/SI
-------------------------------------------------------------------------
aaaa-bbbb-cccc 1           -      -      GE0/0/5        static
aaaa-bbbb-1234 -           -      -      -              blackhole
```

清除 MAC 地址表项和 ARP 表项
清除所有动态 MAC（系统视图）：undo mac-address dynam

ic
清除所有静态 MAC（系统视图）：undo mac-address static
删除一条静态 ARP 表项（系统视图）：undo arp static
删除多条 ARP 表项（用户视图）：reset arp all (所有)

==========
端口安全

端口安全（Port Security）通过将接口学习到的动态 MAC 地址转换为安全 MAC 地址（包括安全动态 MAC、安全静态 MAC 和 Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

配置端口安全功能，将接口学习到的 MAC 地址转换为安全 MAC 地址，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，只允许学习到 MAC 地址的设备通信。这样可以阻止其他非信任用户通过本接口和交换机通信，提高设备与网络的安全性。

启动端口安全后，一个接口只能学习一个 mac 地址

配置端口安全保护动作。 缺省情况下，端口安全保护动作为 restrict。
restrict :丢弃源 MAC 地址不存在的报文并上报告警。推荐使用 restrict 动作。
protect : 只丢弃源 MAC 地址不存在的报文，不上报告警。
shutdown : 接口状态被置为 error-down，并上报告警。

int g0/0/5

port-security enable

两台 PC 192.168.1.1 和 192.168.1.2 只能一个 PC 可以 ping 通 192.168.1.3，后 ping 的一台是不通的，因为启动端口安全后，一个接口只能学习一个 mac 地址，多了就违规，数据帧被丢弃

dis trapbuffer

```
#Dec 11 2019 13:53:25-08:00 SW3 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.2
5.191.3.1 configurations have been changed. The current change number is 6, the
change loop count is 0, and the maximum number of records is 4095.
#Dec 11 2019 13:51:32-08:00 SW3 L2IFPPI/4/PORTSEC_ACTION_ALARM:OID 1.3.6.1.4.1.2
011.5.25.42.2.1.7.6 The number of MAC address on interface (10/10) GigabitEthern
et0/0/5 reaches the limit, and the port status is 1. (1:restrict;2:protect;3:s
hutdown)
#Dec 11 2019 13:51:04-08:00 SW3 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.2
```

int g0/0/5
port-security max-mac-num 5
port-security protect-action protect
port-security mac-address sticky
port-security mac-address sticky aaaa-1234-cccc
vlan 1

==========

MAC 地址漂移

MAC 地址漂移是指设备上一个 VLAN 内有两个端口学习到同一个 MAC 地址，后学习到的 MAC 地址表项覆盖原 MAC 地址表项的现象。

MAC 地址漂移避免机制：

1.提高接口 MAC 地址学习优先级；
2.不允许相同优先级的接口发生；
3.MAC 地址表项覆盖。

缺省情况下，接口学习 MAC 地址的优先级为 0，数值越大优先级越高,最高为 3
不允许相同优先级的接口发生 MAC 地址表项覆盖，也可以防止 MAC 地址漂移，提高网络的安全性。
配置全局 MAC 地址漂移检测
配置 MAC 地址漂移检测功能

int g0/0/5
mac-learning priority 3

undo mac-learning priority 3 allow-flapping

mac-address flapping detection

vlan 1
loop-detect eth-loop block-time 100 retry-times 3

当检测到该 VLAN 内发生 MAC 地址漂移时，被检测到的物理接口将被阻塞 100S，100S 重新开放该物理接口，开放后如果在 20S 没有再次检测到 MAC 地址漂移，则该物理接口阻塞将被彻底解除；如果 20S 内再次检测到 MAC 地址漂移，则再次将该接口阻塞。重复以上操作 3 次，如果仍然能检测到该物理接口有 MAC 地址漂移现象发生，则永久阻塞该物理接口。

==========
配置 Eth-Trunk

Eth-Trunk 在逻辑上把多条物理链路捆绑等同于一条逻辑链路，对上层数据透明传输。所有 Eth-Trunk 中物理接口的参数必须一致，Eth-Trunk 链路两端要求一致的物理参数有：Eth-Trunk 链路两端相连的物理接口类型、物理接口数量、物理接口的速率、物理接口的双工方式以及物理接口的流控方式。

int Eth-Trunk 1
trunkport g0/0/1
或者
int eth-trunk 1
int g0/0/1
eth-trunk 1

SW1：
int Eth-Trunk 1
mode manual load-balance
int g0/0/1
eth-trunk 1
int g0/0/2
eth-trunk 1
q

SW2：
int Eth-Trunk 1
mode manual load-balance
int g0/0/1
eth-trunk 1
int g0/0/2
eth-trunk 1
q

配置完成后，查看 Eth-Trunk 1 接口状态 ，可以看到工作

模式为 normal（手工负载分担方式），g0/0/1 和 g0/0/2 接口已经添加到 Eth-Trunk 1 中，并且处于 UP 状态
<SW1>display eth-trunk 1

```
[SW1]dis eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------
PortName                      Status      Weight
GigabitEthernet0/0/1          Up          1
GigabitEthernet0/0/2          Up          1
```

可以看到目前该接口的总带宽，是 g0/0/1 和 g0/0/2 接口带宽之和
<SW1>display interface Eth-Trunk 1

```
[SW1]display int Eth-Trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:
Switch Port, PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,M
 2G, Current BW: 2G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-
Current system time: 2018-05-04 21:31:47-08:00
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
GigabitEthernet0/0/1          UP          1
GigabitEthernet0/0/2          UP          1
```

查看 SW1 接口的生成树状态，可以看到 SW1 的两个接口被捆绑成为一个 Eth-Trunk 接口，并且该接口处于转发状态。

<SW1>display stp brief

```
[SW1]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/5        DESI  FORWARDING      NONE
   0    Eth-Trunk1                  DESI  FORWARDING      NONE
```

当链路故障发生时，链路可以进行切换，并且只要物理链路有一条是正常的，Eth-Trunk 接口就不会断开，仍然可以保证数据的转发。

配置 Eth-Trunk 实现链路聚合（静态 LACP 模式）

在 SW1 SW2 之间再连接一个 g0/0/5 接口

现网络管理员为公司再部署一条链路作为备份链路，并采用静态 LACP 模式配置 Eth-Trunk 实现两条链同时转发，一条链路备份，当其中一条转发链路出现问题时，备份链路可立即进行数据转发。
需要将先前已经加入到 Eth-Trunk 接口下的物理接口先删除，之后在 SW1 SW2 上的 Eth-Trunk 接口下，将工作模式改为静态 LACP 模式

SW1：
```
int g0/0/1
undo eth-trunk
int g0/0/2
undo eth-trunk
q
int Eth-Trunk 1
mode lacp-static
int g0/0/1
eth-trunk 1
int g0/0/2
eth-trunk 1
int g0/0/5
eth-trunk 1
q
```

SW2：
```
int g0/0/1
undo eth-trunk
int g0/0/2
```

```
undo eth-trunk
q
int Eth-Trunk 1
mode lacp-static
int g0/0/1
eth-trunk 1
int g0/0/2
eth-trunk 1
int g0/0/5
eth-trunk 1
q
```

配置完成后，查看 SW1 的 Eth-Trunk 1 的接口状态 ，可以看到 3 个接口默认都处于活动状态（Selected）

```
<SW1>display eth-trunk 1
```

```
[SW1]dis eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768      System ID: 4c1f-cc8d-3d21
Least Active-linknumber: 1  Max Active-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
ActorPortName         Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1  Selected 1GE      32768   2      305     10111100  1
GigabitEthernet0/0/2  Selected 1GE      32768   3      305     10111100  1
GigabitEthernet0/0/5  Selected 1GE      32768   6      305     10111100  1
```

将 SW1 的系统优先级从默认的 32768 改为 100，使其成为主动端口（值越低优先级越高），并按照主动端口的接口来选

择活动接口。两端设备选出主动端后，两端都会以主动端的接口优先级来选择活动端口。两端选择了一致的活动接口，活动链路组便可以建立起来，设置这些活动链路以负载分担的方式转发数据。

SW1 系统优先级为 100，活动接口上限阈值为 2，设置 g0/0/1 、g0/0/5 接口优先级为 100

SW1：

lacp priority 100

int eth-trunk 1
max active-linknumber 2
int g0/0/1
lacp priority 100
int g0/0/5
lacp priority 100
q

配置完成后，可以看到 g0/0/5 没有被选择，因为默认是不抢占的
优先级低，但没有开启抢占，所以没有被选择

```
[SW1]dis eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc8d-3d21
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName         Status   PortType PortPri PortNo PortKey PortState Wei
GigabitEthernet0/0/1  Selected 1GE      100     2      305     10111100  1
GigabitEthernet0/0/2  Selected 1GE      32768   3      305     10111100  1
GigabitEthernet0/0/5  Unselect 1GE      100     6      305     10100000  1

==========
```

改变抢占方式

在 lacp 模式下，默认是不抢占的，
开启抢占后，默认的抢占延时为 30s

```
int eth-Trunk 1
lacp preempt enable
lacp preempt delay 10
```

配置完成后，查看一下 <SW1>display eth-trunk 1

```
[SW1]dis eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc8d-3d21
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName         Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1  Selected 1GE      100     2      305     10111100  1
GigabitEthernet0/0/2  Unselect 1GE      32768   3      305     10100000  1
GigabitEthernet0/0/5  Selected 1GE      100     6      305     10111100  1
```

==========

改变负载分担模式

默认是基于源目 IP 地址进行负载分担，可以根据需要进行改变

```
[SW1]dis eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: STATIC
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc8d-3d21
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
```

SW1：
int eth-trunk 1
load-balance dst-ip

==========

配置 Eth-Trunk 接口的散列依据

缺省情况下，当 Eth-Trunk 接口根据 IP 进行散列

int eth-trunk 1
load-balance packet

说明：

基于 IP 的散列算法能保证包顺序，但不能保证带宽利用率。

基于包的散列算法能保证带宽利用率，但不能保证包的顺序。

配置 Eth-Trunk 成员接口的负载分担权重

int g0/0/1
distribute-weight 2

缺省情况下，成员接口的负载分担权重为 1

==========

创建 VLAN，并将相应接口加入 VLAN

SW1：
vlan batch 2 to 20
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
int Eth-Trunk 1
trunkport g0/0/1
trunkport g0/0/2

```
port link-type trunk
port trunk allow-pass vlan 2 to 20
q
```

SW2 :

```
vlan batch 2 to 20
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
int Eth-Trunk 1
trunkport   g0/0/1
trunkport   g0/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 20
q
```

SW3 :

```
un ter mo
sys
sysname SW3
vlan batch 2 to 20
int g0/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 20
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
int g0/0/5
port link-type access
port default vlan 2
q
```

SW4 :

```
un ter mo
```

```
sys
sysname SW4
vlan batch 2 to 20
int g0/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 20
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
int g0/0/5
port link-type access
port default vlan 2
q
```

配置 MSTP

SW1 :

```
stp pathcost-standard legacy
stp instance 0 priority 0
stp instance 1 root primary
stp instance 2 root secondary

stp region-configuration
region-name hcie
revision-level 1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
active region-configuration
q
```

SW2 :

```
stp pathcost-standard legacy
stp instance 1 root secondary
stp instance 2 root   primary
```

```
stp region-configuration
region-name hcie
revision-level 1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
active region-configuration
q
```

SW3 :

```
stp pathcost-standard legacy
int g0/0/1
stp instance 2 cost   40

stp region-configuration
region-name hcie
revision-level 1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
active region-configuration
q
```

SW4 :

```
stp pathcost-standard legacy
int g0/0/1
stp instance 1 cost   40

stp region-configuration
region-name hcie
revision-level 1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
active region-configuration
q
```

配置 STP 保护功能

指定端口配置根保护功能，边缘端口配置 BPDU 保护

SW1：

```
int g0/0/3
stp root-protection
```

SW2：

```
int g0/0/3
stp root-protection
```

SW3：

```
stp bpdu-protection
int g0/0/5
stp edged-port enable
```

SW4：

```
stp bpdu-protection
int g0/0/5
stp edged-port enable
```

验证配置结果

SW1 dis stp brief

在 MSTI1 中，由于 Switch 1 是根桥，Switch 1 的端口 Eth-Trunk1 和 g0/0/3 成为指定端口。在 MSTI2 中，Switch 1 的端口 g0/0/3 成为指定端口，端口 Eth-Trunk1 成为根端口。

```
[SW1]dis stp brief
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/3
DESI    FORWARDING             ROOT
      0        Eth-Trunk1
```

```
DESI    FORWARDING              NONE
      1         GigabitEthernet0/0/3
DESI    FORWARDING              ROOT
      1         Eth-Trunk1
DESI    FORWARDING              NONE
      2         GigabitEthernet0/0/3
DESI    FORWARDING              ROOT
      2         Eth-Trunk1
ROOT    FORWARDING              NONE
```

在 MSTI2 中，由于 Switch 2 是根桥，Switch 2 的端口 Eth-Trunk1 和 g0/0/3 成为指定端口。在 MSTI1 中，Switch 2 的端口 g0/0/3 成为指定端口，端口 Eth-Trunk1 成为根端口。

```
[SW2]dis stp brief
 MSTID    Port
Role    STP State           Protection
      0         GigabitEthernet0/0/3
DESI    FORWARDING              ROOT
      0         Eth-Trunk1
ROOT    FORWARDING              NONE
      1         GigabitEthernet0/0/3
DESI    FORWARDING              ROOT
      1         Eth-Trunk1
ROOT    FORWARDING              NONE
      2         GigabitEthernet0/0/3
DESI    FORWARDING              ROOT
      2         Eth-Trunk1
DESI    FORWARDING              NONE
```

dis stp int g0/0/3 brief
Switch 3 的端口 g0/0/3 在 MSTI1 和 MSTI2 中为根端口。Switch 3 的另一个端口 g0/0/1，在 MSTI2 中被阻塞，在 MSTI1 中被计算为指定端口。

```
[SW3]dis stp int g0/0/3 brief
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/3
ROOT    FORWARDING            NONE
      1        GigabitEthernet0/0/3
ROOT    FORWARDING            NONE
      2        GigabitEthernet0/0/3
ROOT    FORWARDING            NONE

[SW3]dis stp int g0/0/1 brief
 MSTID    Port
Role    STP State           Protection
      0        GigabitEthernet0/0/1
DESI    FORWARDING            NONE
      1        GigabitEthernet0/0/1
DESI    FORWARDING            NONE
      2        GigabitEthernet0/0/1
ALTE    DISCARDING            NONE
```

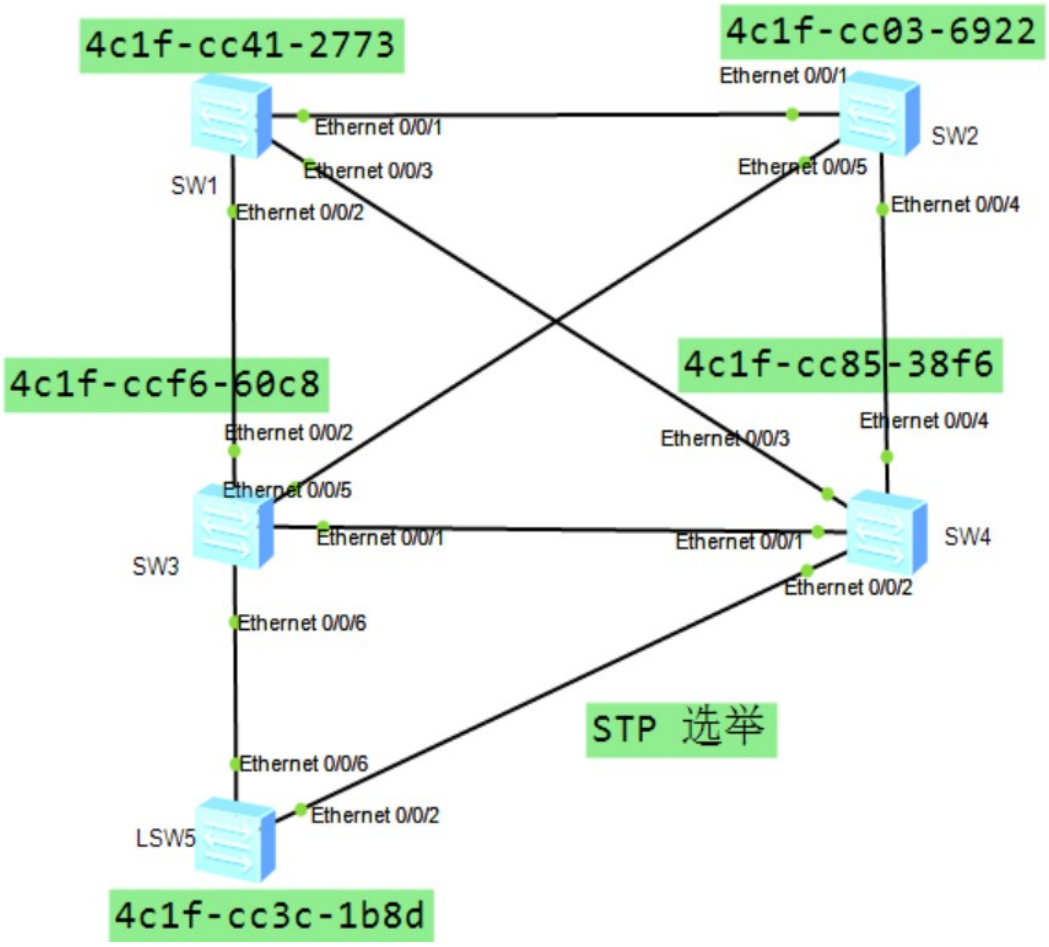
Switch 4 的端口 g0/0/3 在 MSTI1 和 MSTI2 中为根端口。Switch 4 的另一个端口 g0/0/1，在 MSTI1 中被阻塞，在 MSTI2 中被计算为指定端口。

```
[SW4]dis stp int g0/0/3 brief
 MSTID    Port
```

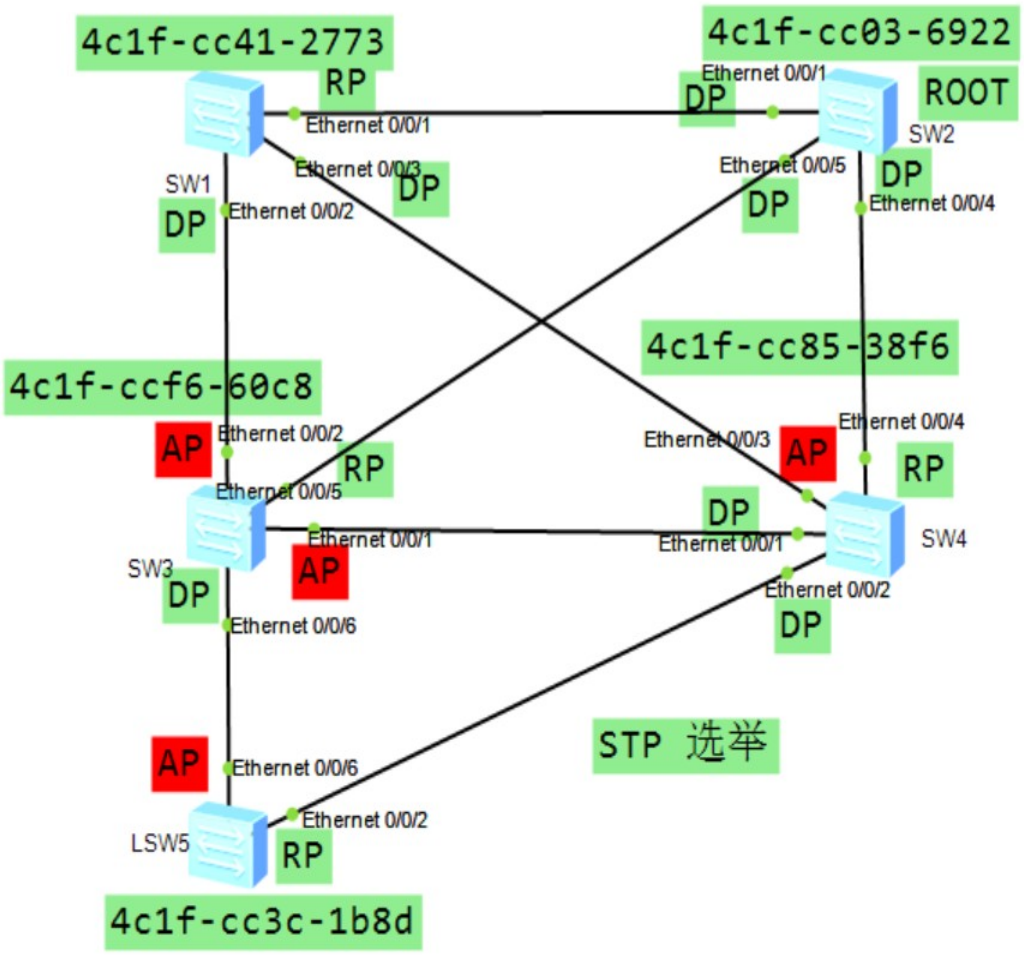
```
Role    STP State           Protection
      0         GigabitEthernet0/0/3
ROOT    FORWARDING              NONE
      1         GigabitEthernet0/0/3
ROOT    FORWARDING              NONE
      2         GigabitEthernet0/0/3
ROOT    FORWARDING              NONE

[SW4]dis stp int g0/0/1 brief
 MSTID    Port
Role    STP State           Protection
      0         GigabitEthernet0/0/1
ALTE    DISCARDING              NONE
      1         GigabitEthernet0/0/1
ALTE    DISCARDING              NONE
      2         GigabitEthernet0/0/1
DESI    FORWARDING              NONE

==========
```

LAN 技术 2：STP 选举

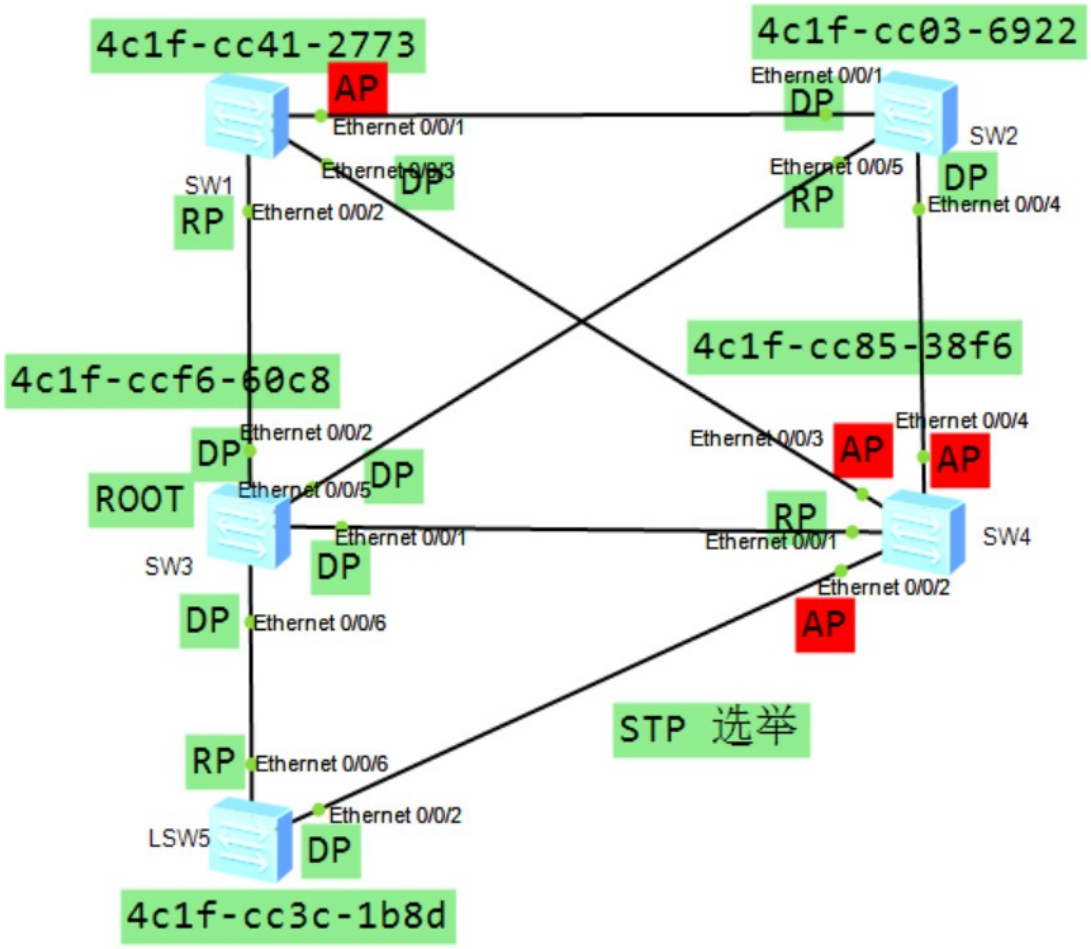
每个网络只有一个根桥
每个非根桥都要选出一个根端口
每个 Segment 只有一个指定端口
非指定端口将被堵塞



如图所示根据规则，选举如下



如果修改 SW3 的优先级 4096 ，让 SW3 为根，则各交换机的端口角色将发生变化

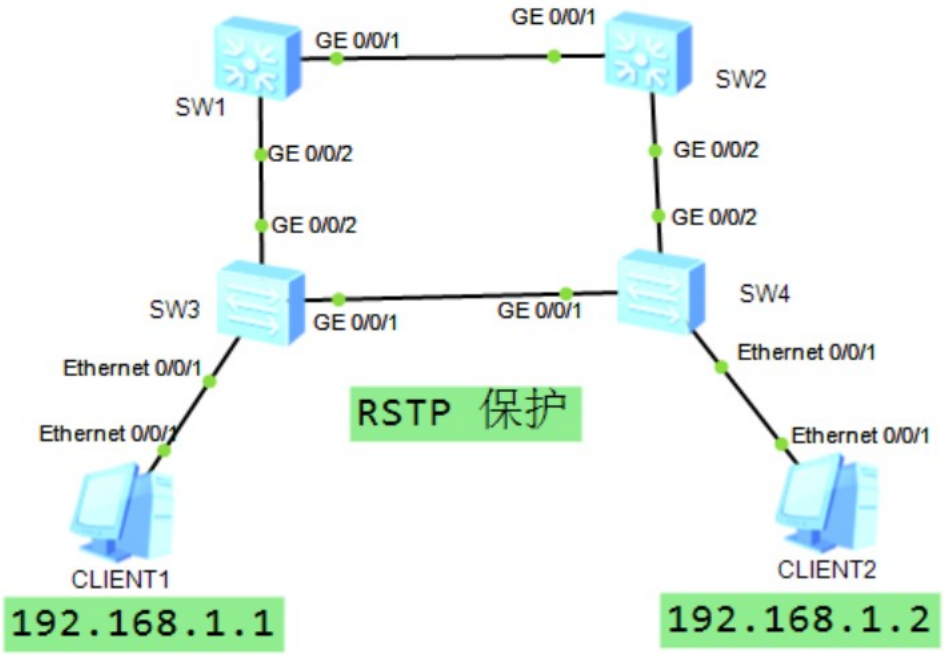


==========

LAN 技术 3：RSTP 保护

在 RSTP 交换网络中，为了防止恶意或临时环路的产生，可配置保护功能来增强网络的健壮性和安全性。

1 BPDU 保护
2 根保护
3 环路保护
4 TC-BPDU 保护



基本配置

SW1:
undo ter mo
sy
sys SW1
stp mode rstp
stp priority 4096

SW2:
undo ter mo
sy
sys SW2
stp mode rstp
stp priority 8192

SW3:
undo ter mo
sy

```
sys SW3
stp mode rstp
int e0/0/1
stp edged-port enable
```

```
SW4:
undo ter mo
sy
sys SW4
stp mode rstp
int e0/0/1
stp edged-port enable
```

配置 BPDU 保护

BPDU 保护：保护边缘端口在收到了 BPDU 以后，会将该端口 error-down，同时通知网管。
只能针对与边缘端口保护
配置：stp bpdu-protection //在系统视图下

为防止边缘端口收到不合法的 BPDU 后网络重新收敛，在 SW3 SW4 上配置 BPDU 保护功能。
在系统视图下使用命令 stp bpdu-protection 启用交换机边缘端口的 BPDU 保护功能。默认交换机的 BPDU 保护功能处于禁用状态

```
[SW3]dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge         :32768.4c1f-cc0b-6f81
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :4096 .4c1f-cc13-66cd / 20000
CIST RegRoot/IRPC   :32768.4c1f-cc0b-6f81 / 0
CIST RootPortId     :128.24
BPDU-Protection     :Disabled
TC or TCN received  :18
```

SW3:
stp bpdu-protection
SW4:
stp bpdu-protection

配置之后，就是 Enable 状态

为了演示边缘端口收到 BPDU 的效果，把 SW3 的 g0/0/2 端口配置为边缘端口
SW3:
int g0/0/2
stp edged-port enable

```
[SW3-GigabitEthernet0/0/2]
May 10 2018 20:06:46-08:00 SW3 %%01MSTP/4/BPDU_PROTECTION(l)[1]:This edged-port
GigabitEthernet0/0/2 that enabled BPDU-Protection will be shutdown, because it r
eceived BPDU packet!
[SW3-GigabitEthernet0/0/2]
```

g0/0/2 端口收到交换机的 BPDU 后被关闭，并弹出日志提示设置自动恢复为 up 延时为 30 s。当端口被关闭后，删掉 g0/0/2 端口的边缘端口配置，30 s 后端口会自动 up 并弹出日志提示
SW3:
int g0/0/2
undo stp edged-port
undo shut
q
error-down auto-recovery cause bpdu-protection interval 30

如果 SW3 上还是边缘端口，
int g0/0/2
stp edged-port

端口一直处于 up 和 down 的状态切换。撤消端口下的边缘端口配置
int g0/0/2
undo stp edged-port

```
[SW3]
May 10 2018 20:09:57-08:00 SW3 %%01ERRDOWN/4/ERRDOWN_DOWNRECOVER(l)[12]:Notify i
nterface to recover state from error-down. (InterfaceName=GigabitEthernet0/0/2)
May 10 2018 20:09:57-08:00 SW3 ERRDOWN/4/ErrordownRecover:OID 1.3.6.1.4.1.2011.5
.25.257.2.2 Error-down recovered. (Ifindex=29, Ifname=GigabitEthernet0/0/2, Caus
e=bpdu-protection, RecoverType=auto recovery)
May 10 2018 20:09:59-08:00 SW3 %%01PHY/1/PHY(l)[13]:    GigabitEthernet0/0/2: ch
ange status to up
May 10 2018 20:09:59-08:00 SW3 ERRDOWN/4/ErrordownOccur:OID 1.3.6.1.4.1.2011.5.2
5.257.2.1 Error-down occured. (Ifindex=29, Ifname=GigabitEthernet0/0/2, Cause=bp
du-protection)
May 10 2018 20:09:59-08:00 SW3 %%01MSTP/4/BPDU_PROTECTION(l)[14]:This edged-port
 GigabitEthernet0/0/2 that enabled BPDU-Protection will be shutdown, because it
received BPDU packet!
```

配置根保护

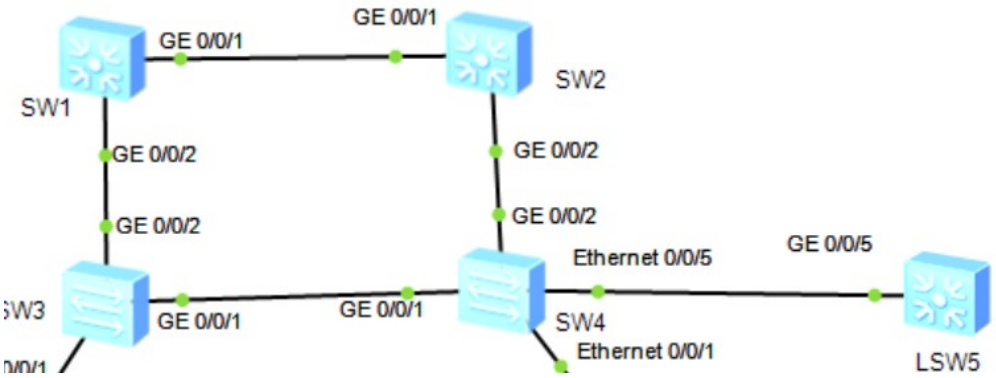
根保护是指定端口上的特性。当端口角色是指定端口时，配置根保护功能才能生效。若在其他类型的端口上配置根保护功能，根保护功能不会生效。

根保护：当该端口收到更优的 RST BPDU 后，端口进入 Discarding 状态，不再转发报文。若一段时间内端口未收到更优的 RST BPDU，则会自动恢复到正常的 Forwarding 状态

只能在指定端口上保护

配置：stp root-protection //在接口试图下

新接入一台交换机



如果没有配置根保护，将 SW5 的优先级改为 0 ，SW5 立即抢占为根，SW4 的 e0/0/5 为 RP

如果在 SW4 的 DP e0/0/5 配置了根保护， SW5 不会为根

SW4 的 e0/0/5 为 DP ，但状态为 DISCARDING

```
MSTID    Port
Role     STP State           Protection
      0        Ethernet0/0/1
DESI     LEARNING                  NONE
      0        Ethernet0/0/5
DESI     DISCARDING                ROOT
      0        GigabitEthernet0/0/1
ALTE     DISCARDING               NONE
      0        GigabitEthernet0/0/2
ROOT     FORWARDING                NONE
```

配置环路保护

如果由于链路拥塞或者单向链路故障导致根端口收不到来自上游设备的 BPDU，交换机会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中环路的产生。

环路保护 loop-protection．在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上游设备的 BPDU 报文，则向网管发出通知信息（此时根端口会进入 Discarding 状态，角色切换为指定端口），而 Alternate 端口则会一直保持在阻塞状态（角色也会切换为指定端口），不转发报文，从而不会在网络中形成环路。
只在根端口或 Alternate 端口上生效
配置：stp loop-protection //在接口试图下

在 SW2 的 g0/0/2 端口下配置
SW2:
int g0/0/2
stp bpdu-filter enable

这样一来，SW4 由于收不到来自上游的 BPDU，就重新选择根端口，观察所有交换机的端口信息
没有接口阻塞，网络上有环

恢复 SW2 的 g0/0/2 端口，在 SW4 的 g0/0/1 和 g0/0/2 端口配置环路防护功能
SW2:
int g0/0/2
undo stp bpdu-filter

SW4:
int g0/0/1
stp loop-protection
int g0/0/2
stp loop-protection

```
[SW4]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet0/0/1               DESI  FORWARDING      BPDU
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      LOOP
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      LOOP
```

在 SW2 上配置 BPDU 过滤

SW2:

int g0/0/2

stp bpdu-filter enable

在 SW4 上查看 STP 的状态信息

```
[SW4]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet0/0/1               DESI  FORWARDING      BPDU
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      LOOP
   0    GigabitEthernet0/0/2        DESI  DISCARDING      LOOP
```

可以看到 SW4 的 g0/0/1 端口成为了根端口，g0/0/2 端口虽然成为了指定端口，但是处于 Discarding 状态，不转发数据，这样就避免了环路。

没有了环路，两台 PC 之间是可以 ping 通的

```
PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time=62 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time=94 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=141 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=140 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=157 ms
```

配置 TC-BPDU 保护

启用了 TC-BPDU 保护功能后，可以配置交换机处理 TC 类型 BPDU 报文的最大速度，以避免频繁地删除 MAC 地址表项和 ARP 表项，从而达到保护交换机的目的。默认情况交换机的 TC 保护功能是处于关闭状态。
TC-BPDU 泛洪保护：当设备收到 TC-BPDU 以后，在单位时间内会有一个限制的次数。
配置：stp tc-protection threshold 在系统视图下+可处理的报文数量

SW1:
stp tc-protection
stp tc-protection threshold 2

配置的含义是：交换机在单位时间内，允许在收到 TC-BPDU 报文后立即进行地址表项删除操作的最大次数为两次，默认为 1 次