VLAN 划分

一、什么是 VLAN

虚拟局域网

二、VLAN 的优势

广播控制
安全性
带宽利用
延迟

三、VLAN 的种类

1、静态 VLAN
基于端口划分静态 VLAN
2、动态 VLAN
基于 MAC 地址划分动态 VLAN

四、VLAN 的配置

1、全局配置模式创建 VLAN
全局：VLAN 2 创建 VLAN 2
Name 名字（给 vlan2 命名）
2、vlan 数据库配置模式
特权：vlan database
Vlan 2 name caiwu(创建 vlan 并命名为 caiwu)
3、删除 vlan
进入 vlan 数据库或全局模式：no vlan 2
4、接口加入 vlan
- 进入将要加入 vlan 的接口然后输入
  Switchport access vlan 3
- 同时将多个接口加入 vlan
  全局：interface range f 0/1-10
  Switchport access vlan 2 将 1-10 口同时加入 vlan2

5、查看 vlan 信息
特权：show vlan brief
6、description 添加 vlan 描述信息
No description 删除 vlan 描述信息

五、trunk 中继链接

1、作用：实现跨交换机之间的 vlan 通信

2、链路类型：

- 接入链路：
- 中继链路：可以承载多个 vlan

3、vlan 的表示

- Isl（cisco 私有的标记方法）
  ISL 外部封装头部 26 个字节，尾部 4 个字节共 30 字节
- IEEE802.1Q （公有的标记方法）
  内部封装在标准以太网帧内插入了 4 个字节，其中 12 位 vlan 标识。

4、ISL 和 802.1Q 的异同

相同点：都是显示了 vlan 的信息

不同点：IEEE802.1Q 是公有的标记方式，ISL 是 cisco 私有的，ISL 采用外部标记的方法，802.1Q 采用内部标记的方法，ISL 标记的长度为 30 字节，802.1Q 标记的长度为 4 字节。

5、trunk 的模式和协商

- Trunk 模式
  接入（access）
  干道（trunk）
  动态期望（desirable）主动
  动态自动（auto）被动
- Trunk 模式协商结果

SW1 端口模式	SW2 端口模式	结果
trunk	auto	trunk
trunk	desirable	trunk
auto	auto	access
auto	desirable	trunk
desirable	desirable	trunk

6、trunk 的配置（中继链路）

接口模式：Switchport mode trunk（直接配置为 trunk）

7、在 trunk 链路上移除某 vlan

进入 trunk 接口：switchport trunk allowed vlan remove 3 中继链路不允许传送 vlan3 的数据。

8、在 trunk 链路上添加某 vlan

进入 trunk 接口：switchport trunk allowed vlan add 3

9、查看接口模式

特权：show interface f0/5 switchport

10、trunk 的动态模式配置

接口模式：switchport mode dynamic desirable(配置为动态期望)
dynamic auto(动态自动)

六、EthernetChannel(以太通道)

1、功能：
多条线路负载均衡，带宽提高
容错，当一条线路失效时，其他线路通信，不会丢包。
2、以太网通道的配置：
全局：interface range f0/6-8
Switchport mode trunk
Channel-group 1 mode on （开启 group/组模式）
3、查看以太网通道的配置：
特权：show etherchannel summary
4、以太网道必须遵循以下一些规则：
- 参与捆绑的端口必须属于同一个 vlan，如果是在中继模式下，要求所有参加捆绑的端口配置成相同的中继模式。
- 所有参与捆绑的端口的物理参数设置必须相同，应该有同样的速度和全/半双工模式设置。

七、在路由器上配置 DHCP 服务

1、全局:IP dhcp pool 名字（定义地址池）
2、network 192.168.1.0 255.255.255.0(动态分配 IP 地址段)
3、default-router 192.168.1.254 (动态分配的网关地址)
4、dns-server 202.106.0.20（动态分配的 dns 服务器地址）此命令后可以跟多个备用的 DNS 地址。
5、全局：ip dhcp excluded-addres 192.168.1.1(预留已静态分配的 IP 地址)

八、配置技巧

1、全局：no ip domain-lookup 禁用 DNS 域名解析
2、配置输出日志同步
全局：line console 0
Logging synchronous
3、配置控制台会话时间
全局：line console 0
Exec-timeout 0 0（第一个 0 代表分钟，第二个 0 代表秒 0 0 代表永不超时）
4、操作技巧
？查询
Table 补全
命令简写

单臂路由

一、单臂路由

1、作用：

实现不同 vlan 间通信

2、子接口

路由器的物理接口可以被划分成多个逻辑接口，每个子接口对应一个 vlan 网段的网关。

3、vlan 标签的封装结构

全局：interface f0/0.1

Encapsulation dot1Q 2

4、单臂路由的缺陷

单臂容易形成网络瓶颈，子接口依托于物理接口，应用不灵活，vlan 间转发需要查看路由表，严重浪费设备资源。

二、三层交换技术

1、作用

使用三层交换技术实现 vlan 间通信

三层交换=二层交换+三层转发

2、基于 CEF 的快速转发

主要包含两个转发用的信息表：

- 转发信息库（FIB）：FIB 类似于路由表，包含路由表中转发信息的镜像。当网络的拓扑发生变化时，路由表将被更新，而 FIB 也将随之变化，这些信息是根据路由表中的信息得到的。
- 邻接关系表：每个 FIB 条目，邻接关系表中都包含相应的第 2 层地址。

3、虚拟接口

三层交换机上配置的 vlan 接口为虚接口

4、三层交换机的配置

- 在三层交换机启用路由功能

全局：ip routing

- 配置虚拟接口的 IP 地址

全局：interface vlan 2

Ip address 192.168.2.1 255.255.255.0

No shutdown

- 在三层交换机上配置 trunk 并指定接口封装为 802.1Q

接口模式：switchport trunk encapsulation dot1Q

Switchport mode trunk

- 配置路由接口

进入接口： no switchport

三、动态路由

1、动态路由特点

减少了管理任务

占用了网络带宽

2、按照路由执行的算法动态路由协议的分类

- 距离矢量路由协议

依据从源网络到目标网络所经过的路由器的个数选择路由，RIP 、IGRP

- 链路状态路由协议

综合考虑从源网络到目标网络的各条路径的情况选择路由 OSPF、IS-IS

3、RIP 路由协议

- RIP 是距离-矢量路由选择协议
- RIP 度量值为跳数，最大跳数为 15 跳，16 跳为不可达。
- RIP 更新时间，每隔 30S 发送路由更新消息，UDP520 端口。
- RIP 路由更新消息，发送整个路由表消息。

4、RIP V1 与 RIP V2 的区别

RIP v1	RIP v2
有类路由协议	无类路由协议
广播更新 (255.255.255.255)	组播更新（224.0.0.9）
不支持 VLSM	支持 VLSM
自动路由汇总，不可关闭	自动汇总可关闭，可手工汇总
更新的过程中不携带子网信息	更新的过程中携带子网信息

5、RIP V2 的配置

全局：router rip

Version 2

No auto-summary(关闭路由汇总)

Network 主网络 ID

default-information originate **将默认路由添加到 rip 中**

生成树

一、STP（生成树协议）

1、STP 简介

逻辑上断开环路，防止广播风暴的产生

当线路故障，阻塞接口被激活，恢复通信，起备份线路的作用。

2、生成树的算法

每个广播域一个根网桥

每个非根网桥的一个根端口

每个网段上一个指定端口

非指定端口，非根端口被阻塞

3、生成树算法分为 3 个步骤：

➢ 选择根网桥

选择交换网络中网桥 ID 最小的交换机成为根网桥，网络 ID 是一个八字的字段，前两个字节十进制数为网桥优先级，后六个字是网络的 MAC 地址，优先级小的被选择为根网桥，如优先级相同则 MAC 地址小的为根网桥。

网桥优先级的取值范围 0-65535 默认值为 32768

➢ 选择根端口（root ports）

在非根网桥上选择根端口，每个非根网桥只能选择一个根端口。

依据：

✧ 到根网桥最低的根路径成本。

带宽越大，传输数据的成本也就越低。

带宽与路径成本的关系：

链路带宽（Mbps）	路径成本
10	100
16	62
45	39
100	19
155	14
622	6
1000	4

✧ 直连的网桥 ID 最小

当路径成本相同时候，比较连接的交换的网桥 ID 值，选择网桥 ID 值小的作为根端口。

✧ 端口 ID 最小

当网桥 ID 相同的时候，比较端口 ID 值（比较的是对端口的端口 ID 值）选择较小的作为根端口。

➢ 选择指定端口（Designated ports）

根桥上的端口全是指定端口

在每个网段上，选择 1 个指定端口

非根桥上的指定端口，选择顺序：

- 根路径成本较低
- 所在的交换机的网桥 ID 的值较小
- 端口 ID 的值较小（与选择根端口不同的是在比较端口 ID 值时，比较的是自身的端口 ID 值）

4、BPDU（桥协议数据单元）

➢ 使用组播发送 BPDU

➢ 2 种类型：

配置 BPDU

拓扑变更通告 BPDU

- BPDU 报文字段

主要关键字段：

根网桥 ID：

根路径成本：

发送网桥 ID：

端口 ID：

5、STP 的收敛

交换机端口的 5 种 STP 状态

状　　态	用　　途
转发（Forwarding）	发送/接收用户数据
学习（Learning）	构建网桥表
侦听（Listening）	构建“活动”拓扑
阻塞（Blocking）	只接收 BPDU
禁用（Disabled）	强制关闭

6、STP 的 3 种计时器

HELLO 时间：网桥发送配置 BPDU 报文之间的时间间隔，默认 2 秒。

转发延迟：一个端口在侦听到学习状态所花费的时间间隔，默认 15 秒。

最大老化时间：交换机在丢弃 BPDU 报文之前储存它的最大时间，默认 20 秒。

二、VLAN 与 STP（生成树）之间的关系：

PVST+　：（增强的每 VLAN 生成树）

PVST+　配置的意义

配置网络中比较稳定的交换机为根网桥

利用 PVST+ 实现网络的负载分担

三、PVST+的配置命令

1、启用生成树命令

全局：spanning-tree vlan 2

2、指定根网桥

- 改优先级

全局：spanning-tree vlan 2 priority 优先级的值

注意：优先级的值是 4096 的倍数

- 直接指定

全局：spanning-tree vlan 2 root primary

Secondary

注：配置 primary,优先级是 24576

配置 secondary，优先级是 28672

3、查看生成树的配置

特权：show spanning-tree vlan 1

4、速端口

使连接终端的端口快速进入到转发状态，该端口不经过侦听和学习状态，直接进入转发状态，节省 30 秒的转发延迟。速端口只能配置在连接终端的接口上。

5、配置速端口

接口模式：spanning-tree portfast

6、查看某个 vlan 的生成树详细信息

特权：show spanning-tree vlan 2 detail

热备份路由选择协议（HSRP）

1、作用

CISCO 私有协议，确保了当网络边缘设备或接入链路出现故障时，用户通信能迅速并透明的恢复，以此为 IP 网络提供冗余性。通过使用同一个虚拟 IP 地址和虚拟 MAC 地址，LAN 网段上的两台或多台路由器可以作为一台虚拟路由器对外提供服务。HSRP 使组内的 cisco 路由器能互相监视对方的运动状态。

2、HSRP 组成员

活跃路由器

备份路由器

虚拟路由器（即该 lan 上的网关）

其他路由器

3、HSRP 虚拟 MAC 地址格式

0000.0c07.ac2f

厂商编码

HSRP 虚拟 MAC 地址，HSRP 编码总是 07.ac

HSRP 组号

4、HSRP 消息

HSRP 中的所有路由器都发送或接收 HSRP 消息

使用用户数据报协议（UDP）端口号 1985

使用组播发送 HSRP 消息，组播地址 224.0.0.2　　生存时间 TTL=1

5、HSRP 状态

- 初始状态：
- 学习状态：
- 监听状态：
- 发言状态：
- 备份状态：
- 活跃状态：

6、HSRP 计时器

Hello 间隔（默认 3s）

保持时间（默认 10s）

五、HSRP 的配置

1、配置为 HSRP 的成员

进入路由器的网关接口

Standby 2 ip 虚拟网关 IP

2、配置 HSRP 的优先级

接口 Standby 2 priority 优先级

优先级范围 0-255，默认为 100

3、HSRP 占先权

接口 Standby 2 preempt

4、HSRP 端口跟踪

接口 Standby 2 track f0/0 150

5、查看 HSRP 的状态

- 查看 HSRP 摘要信息

特权：show standby brief

访问控制列表

一、访问控制列表概述

1、 访问控制列表（ACL）

- 读取第三层、第四层包头信息
- 根据预先定义好的规则对包进行过滤

2、访问控制列表的处理过程

- 如果匹配第一条规则，则不再往下检查，路由器将决定该数据包允许通过或拒绝通过。
- 如果不匹配第一条规则，则依次往下检查，直到有任何一条规则匹配。
- 如果最后没有任何一条规则匹配，则路由器根据默认的规则将丢弃该数据包。

3、访问控制列表的类型：

- 标准访问控制列表

基于源 IP 地址过滤数据包

列表号是 1-99

- 扩展访问控制列表

基于源 IP 地址、目的 IP 地址、指定协议、端口等来过滤数据包

列表号是 100-199

- 命名访问控制列表

命名访问控制列表允许在标准和扩展访问控制列表中使用名称代替表号

二、标准访问控制列表

1、标准访问控制列表的创建

全局：access-list 1 permit 192.168.1.0 0.0.0.255（允许）

全局：access-list 1 deny 192.168.1.1 0.0.0.0（拒绝）

通配符掩码：也叫做反码。用二进制数 0 和 1 表示，如果某位为 1，表明这一位不需要进行匹配操作，如果为 0 表明需要严格匹配。

例：192.168.1.0/24 子网掩码是 255.255.255.0，其反码可以通过 255.255.255.255 减去 255.255.255.0 得到 0.0.0.255

隐含拒绝语句：

Access-list 1 deny 0.0.0.0 255.255.255.255

2、将 ACL 应用于接口

接口模式：ip access-group 列表号 in 或 out

注：access-list 1 deny 192.168.1.1 0.0.0.0 或写为 access-list 1 deny host 192.168.1.1

Access-list 1 deny 0.0.0.0 255.255.255.255 或写为 access-list 1 deny any

3、删除已建立的访问控制列表

全局：no access-list 列表号

4、接口上取消 ACL

接口模式：no ip access-group 列表号 in （入口）或 out（出口）

5、查看访问控制列表

特权：show access-lists

三、扩展访问控制列表

1、作用

可以根据源 IP 地址，目的 IP 地址，指定协议，端口等过滤数据包。

2、扩展访问控制列表号：100-199

3、eq 等于、lt 小于、gt 大于、neq 不等于

4、扩展访问控制列表案例：

例 1　全局：access-list 101 permit ip 192.168.1.0 0.0.0.255　192.168.2.0 0.0.0.255 (允许 192.168.1.0 网络访问 192.168.2.0 网络的所有服务)

全局：access-list 101 deny ip any any (拒绝所有)

例 2　全局：access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 21（拒绝 192.168.1.0 网段访问 192.168.2.2 的 TCP 的 21 端口）

例 3　全局：access-list 101 deny icmp 192.168.1.0 0.0.0.255 host 192.168.2.2 echo(拒绝 192.168.1.0 ping 192.168.2.2)

5、删除扩展 ACL

全局： no access-list 列表号

注：扩展与标准 ACL 不能删除单条 ACL 语句，只能删除整个 ACL。

6、扩展 ACL 应该应用在离源地址最近的路由器上。

四、命名访问控制列表

1、命名访问控制列表可以配置标准命名也可配置扩展命名。

2、命名访问控制列表的 ACL 语句默认第一条为 10，第二条为 20，依此类推。

3、命名 ACL 可以删除单条 ACL 语句，而不必删除整个 ACL。并且命名 ACL 语句可以有选择的插入到列表中的某个位置，使得 ACL 配置更加方便灵活。

4、标准命名 ACL 的配置

- 全局：ip access-list standard 名字
  Permit host 192.168.1.1
  Deny any
- 命名 ACL 应用于接口
  接口模式：ip access-group 名字 in 或 out

5、扩展命名 ACL 的配置

全局：ip access-list extended 名字

Deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 80 （拒绝 1.0 网段访问 2.2 的 web 服务）

Permit ip any any

NAT 地址转换

一、NAT（网络地址转换）

1、作用：通过将内部网络的私有 IP 地址翻译成全球唯一的公网 IP 地址，使内部网络可以连接到互联网等外部网络上。

2、优点：

节省公有合法 IP 地址

处理地址重叠

增强灵活性

安全性

3、 NAT 的缺点

延迟增大

配置和维护的复杂性

不支持某些应用，可以通过静态 NAT 映射来避免

4、NAT 实现方式

- 静态转换

IP 地址的对应关系是一对一，而且是不变的，借助静态转换，能实现外部网络对内部网络中某些特设定服务器的访问。

静态 NAT 配置：

配置接口 IP 及路由

全局：ip nat inside source static 192.168.100.2 61.159.62.130

在内外接口上启用 NAT：

进入出口配置 ip nat outside

进入入口配置：ip nat inside

- 动态转换

IP 地址的对应关系是不确定的，而是随机的，所有被授权访问互联网的私有地址可随机转换为任何指定的合法的外部 IP 地址。(内部网络同时访问 internet 的主机数少于配置的合法地址中的 IP 个数时适用)

动态 NAT 配置

全局：access-list 1 permit 192.168.100.0 0.0.0.255

全局：ip nat pool nsd 61.159.62.131 61.159.62.133 netmask 255.255.255.248(定义地址池名称为 nsd，地址池 IP 范围 61.159.62.131 到 61.159.62.132)

全局：ip nat inside source list 1 pool nsd

- 端口多路复用（PAT）

通过改变外出数据包的源 IP 地址和源端口并进行端口转换，内部网络的所有主机均可共享一个合法 IP 地址实现互联网的访问，节约 IP。

PAT 的配置：

全局：ip nat inside source list 1 interface f0/1 overload

5、NAT 三种实现方式的区别

静态转换的对应关系一对一且不变，并且没有节约公用 IP，只隐藏了主机的真实地址。

动态转换虽然在一定情况下节约了公用 IP，但当内部网络同时访问 internet 的主机数大于合法地址池中的 IP 数量时就不适用了。

端口多路复用可以使所有内部网络主机共享一个合法的外部 IP 地址，从而最大限度的节约 IP 地址资源。

二、查看 NAT 转换条目

特权：show ip nat translations 显示当前存在的转换

特权：show ip nat translations verbose 显示详细的 NAT 转换条目信息

三、清除 NAT 转移条目

1、特权：clear ip nat translation *清除 NAT 转换条目中的所有条目

注：静态 NAT 条目不会被清除

特权：clear ip nat translation inside local-ip global-ip 清除包含一个内部转换的一个简单转换条目

特权：Clear ip nat translation outside local-I global-io 清除包含一个外部转换的一个简单转换条目

四、NAT 常见问题

ACL 阻止转换后的流量
进行地质转换的 ACL 不全
Overload 参数漏配
不对称路由问题
动态地址池 IP 地址范围配置错误
动态地址池与静态转换地址重叠
Inside 和 outside 接口配置错误

五、显示每个转换的数据包

特权：debug ip nat
S 表示源地址
D 表示目的地址
192.168.1.2->61.159.62.130 表示将 192.168.1.2 转换为 61.159.62.130

TFTP 协议

定义

- TFTP（Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。端口号为 69。
- 它基于 UDP 协议而实现，此协议设计的时候是进行小文件传输的。

TFTP 作用

- 利用 tftp 服务器，备份 Cisco 路由器与交换机的 IOS 系统
- IOS 系统：网际操作系统，可以等同的认为它就是路由器的操作系统，像我们常用的 XP 一样。

路由器 组成

- CPU
- 存储
- 接口
- 控制台端口

CPU

路由器的处理器负责执行处理数据包所需的工作，比如维护路由，作出路由决定等等。路由器处理数据包的速度在很大程度上取决于处理器的类型。

存储

1、只读内存(ROM)。

2、随机存取内存 (RAM)。

3、闪存。

4、非易失性 RAM(NVRAM)

只读内存(ROM)

- ROM 保存着路由器的引导(启动)软件。这是路由器运行的第一个软件，负责让路由器进入正常工作状态。ROM 中的硬件检测程序，检测各组件能否正常工作

闪存（Flash）

- 闪存（Flash）是可读可写的存储器，在系统重新启动或关机之后仍能保存数据。Flash 中存放着当前使用中的 IOS

随机存取内(RAM)

- RAM 也是可读可写的存储器，但它存储的内容在系统重启或关机后将被清除。和计算机中的 RAM 一样，RAM 的存取速度优于其它 3 种内存的存取速度。 运行期间，RAM 中包含路由表项目、ARP 缓冲项目、日志项目和队列中排队等待发送的分组。除此之外，还包括运行配置文件(Running-config)、正在执行的代码、IOS 操作系统程序和一些临时数据信息。

非易失性（NVROM)

- 非易失性 RAM(Nonvolatile RAM)是可读可写的存储器，在系统重新启动或关机之后仍能保存数据。保存 Startup-Config 文件。

路由器的加电过程

- 1.系统硬件加电自检。运行 ROM 中的硬件检测程序，检测各组件能否正常工作。完成硬件检测后，开始软件初始化工作
- 2.软件初始化过程。运行 ROM 中的 BootStrap 程序，进行初步引导工作
- 3.寻找并载入 flash 中 IOS 系统文件。
- 4.IOS 装载完毕，系统在 NVRAM 中搜索保存的 Startup-Config 文件，进行系统的配置

备份 IOS 系统

1、搭建 TFTP 服务器
2、配置 ip 地址
3、特权模式下：Router#dir flash:

```
                              Directory of flash:/
                              3   -rw-     5571584         <no date>  c2600-i-mz.122-28.bin
```

4、Router#copy flash: tftp:　　#拷贝 flash 到 tftp

```
Source filename []? c2600-i-mz.122-28.bin                 #拷贝源文件名
Address or name of remote host []? 192.168.1.254     #目标 tftp 服务器 ip
Destination filename [c2600-i-mz.122-28.bin]?    #上传到目的地址文件名
Writing
c2600-i-mz.12228.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
[OK - 5571584 bytes]
5571584 bytes copied in 0.132 secs (42208000 bytes/sec)
```

IOS 丢失后的修复

1、配置 ip 地址：

```
                        rommon 2 > IP_ADDRESS=192.168.1.1
                        rommon 3 > IP_SUBNET_MASK=255.255.255.0
```

2、配置网关： DEFAULT_GATEWAY: 192.168.1.254
3、服务器 IP：TFTP_SERVER: 192.168.1.254
4、下载 IOS：TFTP_FILE: c2600-i-mz.122-28.bin
5、确认：rommon 10 > TFTPDNLD　　#根据以上参数寻找 TFTP 服务器

```
          IP_ADDRESS: 192.168.1.1
          IP_SUBNET_MASK: 255.255.255.0
          DEFAULT_GATEWAY: 192.168.1.254
```

TFTP_SERVER: 192.168.1.254
TFTP_FILE: c2600-i-mz.122-28.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y

密码恢复

1、配置密码,改名并保存
2、重新加电，ctrl+break
进入 ROM 状态（灾难恢复状态）
3、rommon1> confreg 0x2142
#用命令 confreg 设置参数值 0x2142 跳过配置文件
4、启动后，路由器就不再读取 startup-config
5、进入到特权模式后
Router# copy startup-config running-config
6、改密码
7、修改配置寄存器的值
R1(config)# config-register 0x2102
8、重启验证

TELNET 协议

- Internet 远程登陆服务的标准协议和主要方式。必须输入用户名和密码来登录服务器，采用明文传输方式。端口号是 TCP 的 23.

作用

- 主要用于远程登陆服务

Telnet 管理服务器
实验思路
1、准备两台虚拟机，win7 与 server 2008
2、win7 作为客户端，控制面板 -----打开或关闭 windows 功能------telnet 客户端
3、2008 服务器
安装 telnet 组件：控制面板------打开或关闭 windows 功能----功能------添加功能------telnet 服务器端
开启 telnet 端口及服务：管理工具------服务-----telnet----右击属性------启用模式（手动）-------应用-------启用