

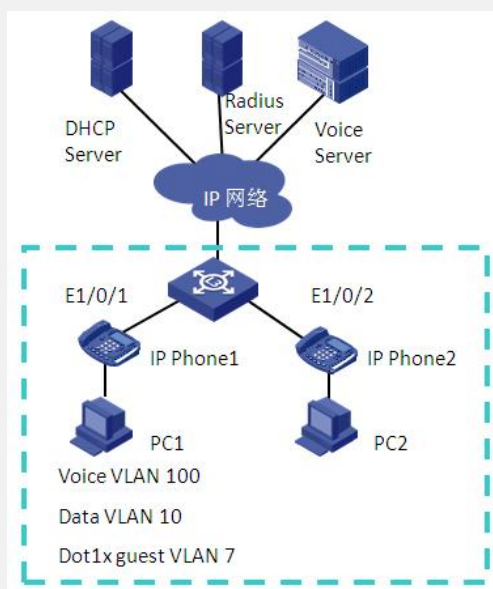
S3600系列交换机voice vlan采用LLDP自动识别OUI 功能的典型配置

一、组网需求:

用户通过H3C S3600系列交换机作为各楼层接入交换机，每个接入交换机端口下连接1台IP Phone和1个PC上网用户。PC用户采用端口安全认证，如果通过接入认证，则接入业务VLAN，可以访问业务网中相应资源。如果未能通过认证，则接入缺省guest VLAN，访问受限资源。每个业务端口下仅能允许1个通过认证用户存在，该端口下其他用户将不能与通过认证用户并存。

原来S3600的版本上，必须配置IP Phone的OUI来使得IP Phone加入voice VLAN，且每台设备最多添加16个OUI段，这样就给实际部署带来了不便，不仅仅需要统计各个IP Phone的OUI，还要规划每台设备的OUI不能超过16个。为了使得部署voice VLAN的工作更加简单方便，我们可以采用LLDP自动识别OUI来加入Voice VLAN的特性。采用此特性部署voice VLAN时要求下挂的IP Phone 支持LLDP协议。

二、组网图:



IP Phone 和PC连接在同一个端口;

IP Phone的voice VLAN 是100;

PC 所在的Data VLAN 是10;

PC 做dot1x认证的Guest VLAN是7;

Radius Server采用IAS服务器: 主备IP分别是10.1.1.91、10.1.1.92

设备NAS-IP10.2.2.10

PC认证客户端采用windows自带客户端。

三、配置步骤:

1. VLAN 配置

```
#
vlan 7
name data_guest
#
vlan 10
name data_users
#
```

```
vlan 100
  name Voice
2、全局Voice VLAN功能配置;
  undo voice vlan security enable
  voice vlan 100 enable
3、全局配置LLDP;
  # 全局使能LLDP。
  LLDP enable
4、PC进行认证的相关功能配置;
  #全局使能端口安全
  port-security enable
  #使能dot1x的DHCP报文触发认证
  dot1x dhcp-launch
  #配置dot1x的认证方式
  dot1x authentication-method eap
  #关闭dot1x的握手功能
  undo dot1x handshake enable
  #配置设备NAS-IP
  radius nas-ip 10.2.2.10
  #配置Radius scheme
  radius scheme IAS
  server-type extended
  primary authentication 10.1.1.91
  primary accounting 10.1.1.91
  secondary authentication 10.1.1.92
  secondary accounting 10.1.1.92
  accounting optional
  key authentication h3c
  key accounting h3c
  user-name-format without-domain
  # 配置domain
  domain h3c
  scheme radius-scheme IAS
  vlan-assignment-mode string
  accounting optional
  #配置默认domain
  domain default enable h3c
5、业务端口配置;
  # 配置业务口E1/0/1
  interface Ethernet1/0/1
    stp edged-port enable
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 7 10 100
    port trunk pvid vlan 7
    multicast-suppression 10
```

```
undo voice vlan mode auto //Voice Vlan 手工方式端口配置
voice vlan enable //Voice Vlan 端口配置
voice vlan lldp //此命令用来开启LLDP识别OUI特性
port-security port-mode userlogin-secure-or-mac //端口安全配置
port-security guest-vlan 7 //端口安全Guest VLAN配置
```

6、验证配置结果

可以使用下面命令来验证结果：

display connection 查看认证用户是否上线

display lldp neighbor-information brief 查看LLDP邻居信息

display mac-address 查看PC和IP Phone MAC地址学习是否正确

四、配置关键点：

- 1、 这里采用端口安全的主要目的是为了满足不同端口只允许一个经过认证的dot1x用户的需求。
- 2、 S3600系列交换机从R1702P23版本开始支持LLDP自动识别OUI特性。
- 3、 IP话机也要支持LLDP功能。
- 4、 本文中略掉了相关server侧的配置，以及实现路由互通的其他配置，实际部署时要添加对应的配置。
- 5、 端口下注意不要开启命令“lldp compliance admin-status cdp txrx”在测试中发现开启此命令的情况下，CISCO话机会随机出现不发送LLDP报文的情况，导致话机和设备之间无法建立LLDP邻居关系。