VLAN 介绍及话机配置

版本：<1.1>

发布日期：<2018-5-13>

目录

1 修订历史

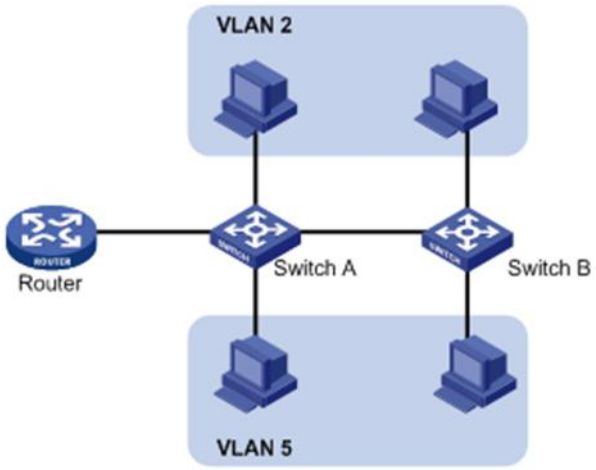
修订历史:

版本	作者	发布时间	说明
1.1	Wang Tian Liang	2018.5.13	初始版本

2 VLAN

2.1 Vlan 简介

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现 LAN 互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文被限制在一个 VLAN 内，如图 1-1 所示。



VLAN 的划分不受物理位置的限制：不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由设备。

VLAN 的优点如下：

1. 限制广播域。广播域被限制在一个 VLAN 内，需要的路由的流量减少，路由器增加的延时也会减少，节省了带宽，提高了网络处理能力。

2. 增强局域网的安全性。VLAN 间的二层报文是相互隔离的，即一个 VLAN 内的用户不能和其它 VLAN 内的用户直接通信，如果不同 VLAN 要进行通信，则需通过路由设备或三层交换机等三层设备。

3.灵活构建虚拟工作组。用 VLAN 可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，不需要安装新的网络电缆和重新配置集线器或路由器，网络构建和维护更方便灵活。

2.2 Vlan 原理

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。

IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案，对带有 VLAN 标识的报文结构进行了统一规定。

IEEE 802.1Q 是支持以太网中 vlan 的网络标准。该规范定义了一种标准方法，用于对带有 VLAN 成员信息的以太网数据包进行标记。VLAN 感知设备是理解 VLAN 成员和 VLAN 格式的设备。当来自话机的数据包进入网络的 VLAN 感知部分时，会添加一个标签来表示该话机的 VLAN 成员。每个包必须与一个 VLAN 内的完全不同。在不包含 VLAN 标记的网络中，VLAN 感知部分中的一个包被假定为在本机(或默认)VLAN 上流动。

802.1Q 在源 MAC 地址和以太网的以太网类型字段之间添加一个 4 字节的标签。两个字节用于标记协议标识符(TPID)，另两个字节用于标记控制信息(TCI)。TCI 字段进一步划分为 PCP(优先级代码点)、CFI(规范格式指示器)和 VID (VLAN ID)。

传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如图 1-2 所示。

图 1-2 传统以太网帧封装格式

其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

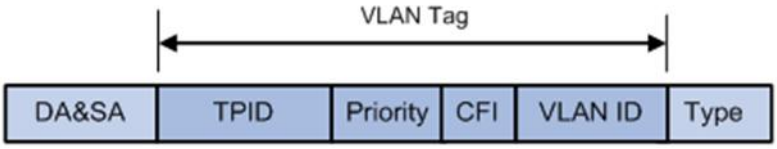


图 1-3 VLAN Tag 的组成字段

如图 1-3 所示，VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

1.TPID 用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。

2. Priority 表示报文的 802.1P 优先级，长度为 3bit，相关内容请参见“ACL 和 QoS 配置指导”中的“QoS”。

3.CFI 字段标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1bit，取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装，缺省取值为 0。

4.VLAN ID 标识该报文所属 VLAN 的编号，长度为 12bit，取值范围为 0～4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1～4094。

网络设备利用 VLAN ID 来识别报文所属的 VLAN，根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 值，来对报文进行处理。

说明： 对于多 VLAN Tag 报文，设备会根据其最外层 VLAN Tag 进行处理，而内层 VLAN Tag 会被视为报文的普通数据部分。

2.3 Vlan 应用

2.3.1 LLDP 介绍

LLDP (Link Layer Discovery Protocol)允许话机接收或是将与设备相关的信息发送到与网络上直接连接的设备上，这些设备也在使用该协议，并存储有关其他设备的信息。使用 LLDP 收集的信息存储在设备中作为管理信息数据库(MIB)，并且可以使用 RFC 2922 中指定的简单网络管理协议(SNMP)查询。

该协议把设备本端的诸如管理地址、设备能力、设备标识、接口标识等信息组织成不同的 TLV，每个信息组织成一个 TLV（Type/Length/Value，类型/长度/值），多个 TLV 构成 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元），LLDP 传输的信息称为 LLDP 数据单元(LLDPDUs)。LLDPDU 包含一组。类型长度值(TLV)元素，每一个元素都包含一个特定类型的关于设备或端口传输信息的信息。

每个 TLV 组件都有以下基本结构如下：

类型	长度	数值
7 bits	9 bits	0-511 字节

图 1-4 TLV 结构

LLDP 支持对以下 TLVs 进行通告：

1）强制 LLDP TLVs:底盘 ID、端口 ID 和生存时间(TTL)都包含在一个默认 LLDPDU。

2）可选择 LLDP TLVs：系统名称、系统描述等，话机将可选的 TLVs 和强制 TLVs 一起发送到 LLDPDU 中。

3）组织特定的 TLVs：MAC/PHY 配置/状态和端口 VLAN ID，分别在 IEEE 标准 802.3 和 802.1 中定义。

LLDP-MED(媒体端点发现)由电信行业协会(TIA)出版。它是在端点设备和网络连接设备之间运行的 LLDP 的扩展。即在以太网上部署了语音设备，通过配置该类中相应的 TLV 来获取这些语音设备的信息，LLDP-MED 专门为 IP (VoIP)应用程序提供支持，并提供以下功能：

1）发现性能：允许使用 LLDP-MED 端点来确定连接设备支持和启用的功能。它可以用来指示连接的设备是一个电话，一个开关，一个中继器等。

2）语音 VLAN 配置：提供了一种机制，用于将一个交换机通知一个 VLAN 使用的设

备，该设备支持“即插即用”的网络。

3）电源管理：提供与设备如何供电、电源优先级以及设备需要多少功率有关的信息。

4）库存管理：提供了一种管理设备的方法和设备的属性，如型号、序列号、软件修改等。

5）位置识别发现：在设置紧急呼叫时，提供从开关到设备的位置信息。

除了 LLDP 支持的 TLVs 外，LLDP- med 还支持以下 TLVs 的通告:

1）LLDP-MED 性能 TLV：允许 LLDP-MED 端点确定连接设备的性能支持，以及设备的可用性能。

2）网络策略 TLV：允许互联的网络设备和端点间相互通告的 VLAN 配置，以及端口上为特定应用关联的二层/三层属性。如，交换机可以通报一个 VLAN 号将用的电话。

3）电源管理 TLV：在两个 LLDP-MED 端点和互联的网络设备间启用高级电源管理。允许交换机和电话传送电源信息，如，有多少设备是开启电源的，电源功率分配的优先级，以及设备所需的电源功率。

4）清单管理 TLV：允许端点发送它自己的详细清单信息到交换机上，包括硬件版本信息、固件版本、软件版本、序列号、生产商名称、型号和资产 ID TLV。

5）位置 TLV：提供从交换机到端点的信息。

说明：LLDP 或 LLDP- MED，并不是同时可以在任何给定的时间在两个设备之间的接口上使用。

2、LLDP 在话机上的功能

LLDP 提供了特殊的互操作性好处，IP 电话故障排除，策略的自动部署和先进的 PoE(以太网的电源)。当 LLDP 功能在手机上启用时，手机会定期向直接连接的 LLDP 激活开关发布自己的信息。话机也可以接收来自连接开关的 LLDP 数据包。

当应用程序类型为“语音”时，话机决定是否更新从 LLDP 包获得的 VLAN 配置。当话机上的 VLAN 配置不同于由交换机发送的版本时，话机会执行更新和重新启动。这使得话机可以通过学习来获取交换机的 VLAN id，然后开始与呼叫控制通信。

3、LLDP 功能配置

以 x6 型号话机为例，下图为 LLDP 配置界面

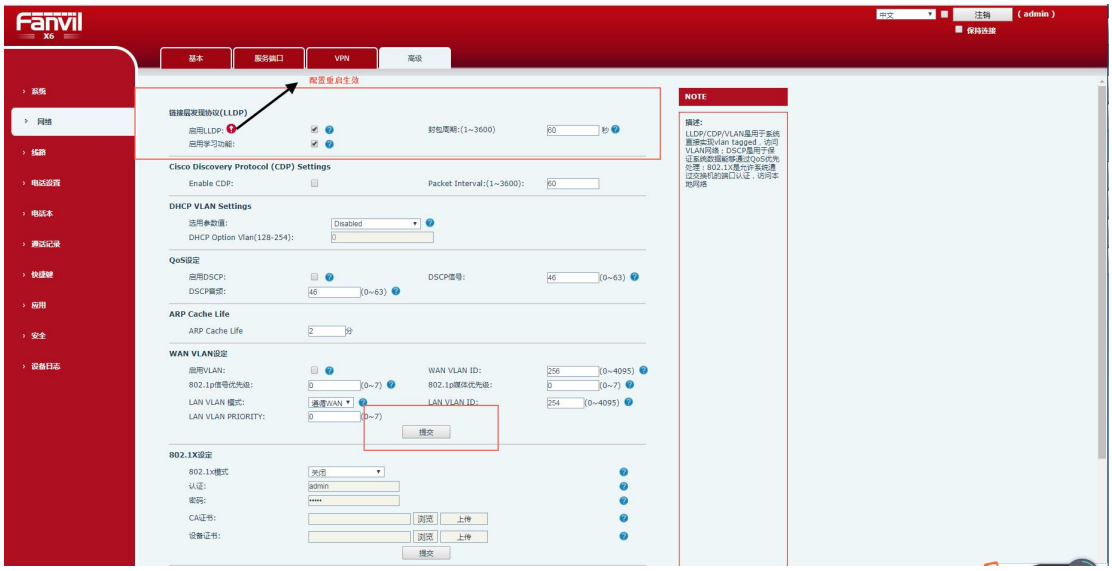


图 1-5 LLDP 配置界面

通过 web 用户界面配置 LLDP 步骤：

1）使用管理员凭证登录到 web 用户界面，默认管理员用户名和密码都是“admin”。

2）点击 Network->Advanced.

3）在 LLDP 界面设置下，通过勾选对应配置，选择是否 enable LLDP。

4）在分组间隔(1~3600s)字段中输入所需时间(以秒为单位)。

5）单击 Apply 确认配置更改。

6）需要重启话机来使配置生效。

5、配置验证

启用 LLDP 功能后，话机执行以下操作:

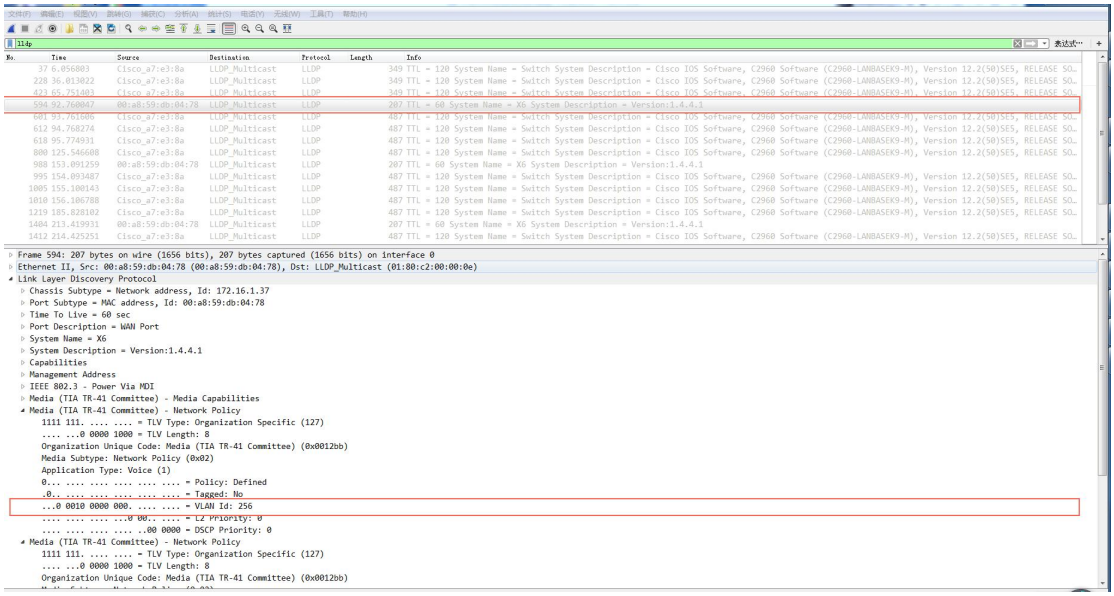
1）定期将话机的信息(例如，硬件修改、固件修订、序列号)发送到网络上的多播地址。

2）允许 LLDP 数据包收到网络(广域网)端口或无线局域网端口。

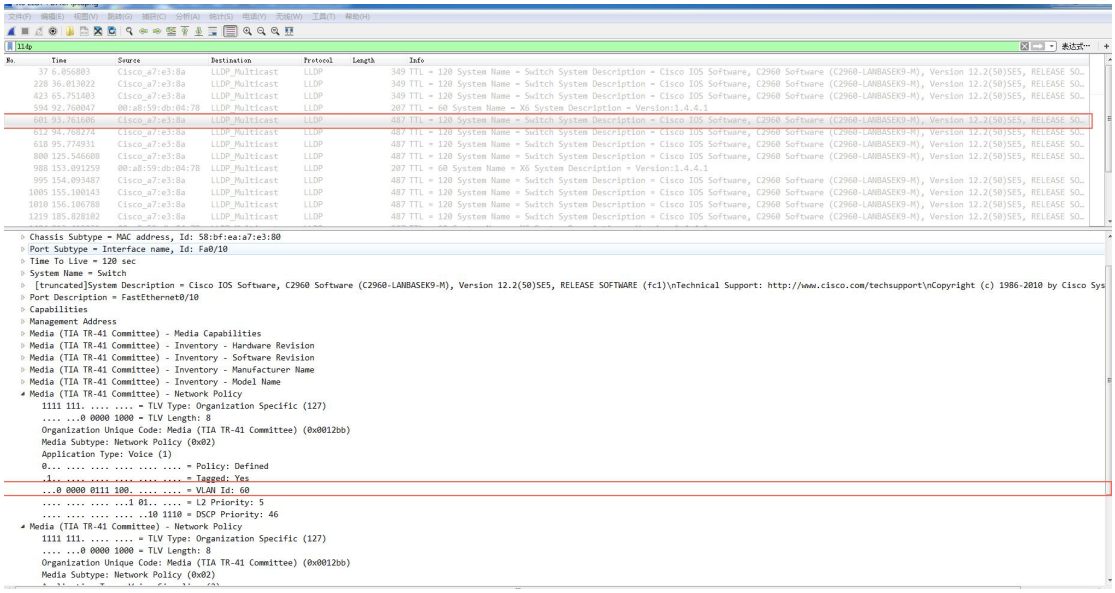
3）支持 MAC / PHY 配置(例如,速率、双工模式)。

4）从网络策略获取 VLAN 信息，它优先于手动设置。

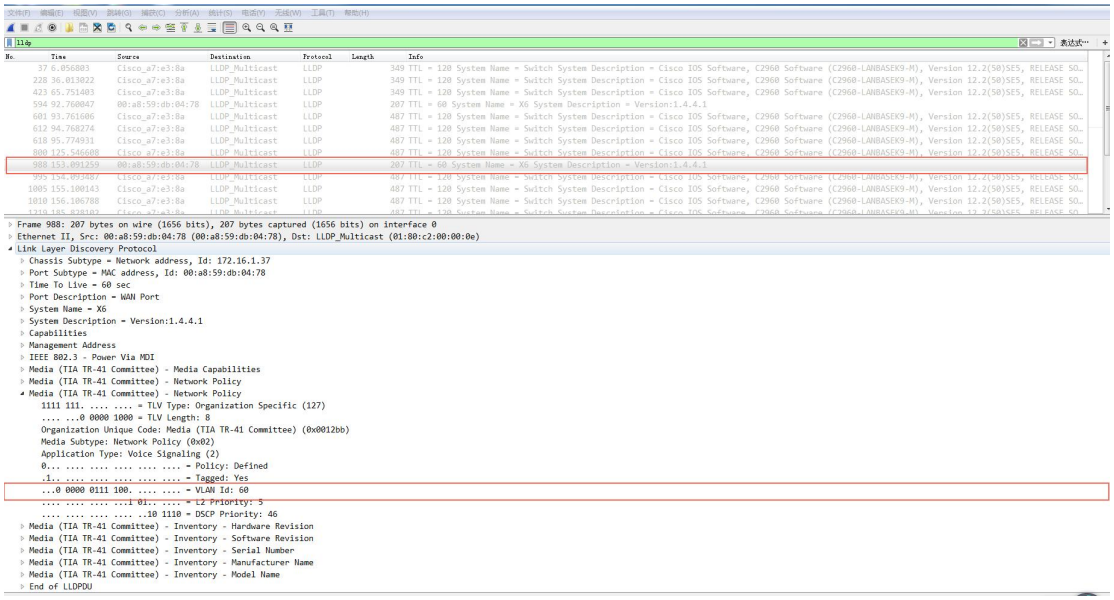
下图显示了由电话发送的 LLDP 包，数据包包含多个 TLVs(在获取 VLAN ID 之前)。



下图显示了通过电话接收的 LLDP 数据包，数据包包含多个 TLVs(由交换机发送)。



下图显示了通过电话发送的 LLDP 包，数据包包含多个 TLVs(在获得 VLAN ID 之后)。



2.3.2 CDP 介绍

CDP (Cisco Discovery Protocol)允许话机接收并将与设备相关的信息从网络上直接连接到其他设备上，并存储其他设备的信息。

2、CDP 在话机上的功能应用

当 CDP 功能在话机上启用时，话机会定期向直接连接的 CDP 激活开关发布自己的信息。话机也可以接收来自连接开关的 CDP 数据包。当话机上的 VLAN 配置不同于由交换机发送的版本时，话机会执行更新和重新启动。这使得话机可以通过学习来获取交换机的 VLAN id，然后开始与呼叫控制通信。

3、CDP 功能配置

以 x6 型号话机为例，下图为 CDP 配置界面

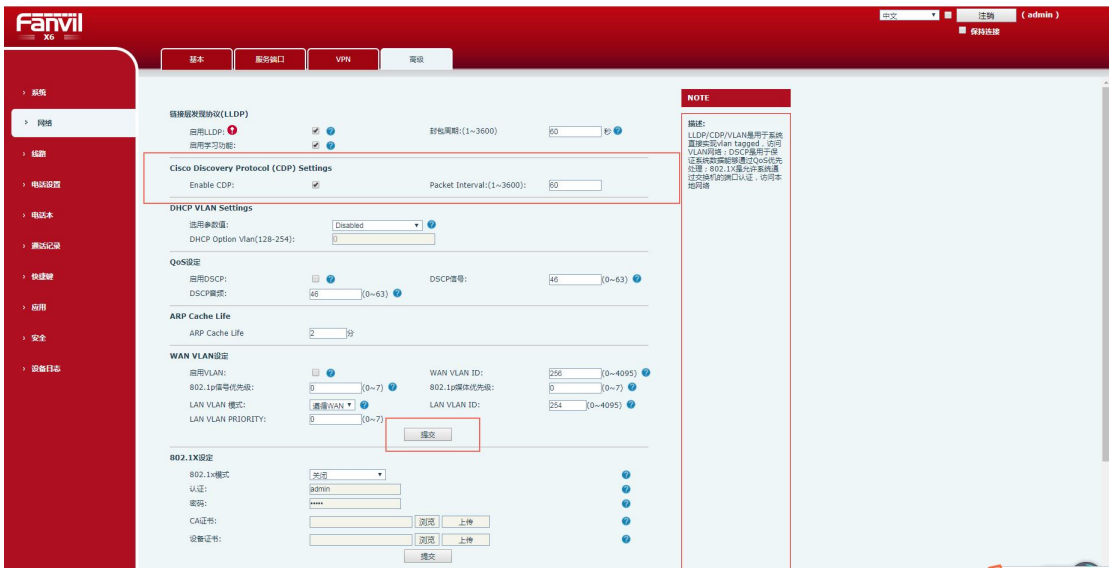


图 1-6 CDP 配置界面

1）使用管理员凭证登录到 web 用户界面，默认管理员用户名和密码都是“admin”。

2）点击 Network->Advanced.

3）在 CDP 界面设置下，通过勾选对应配置，选择是否 enable CDP。

4）在分组间隔(1~3600s)字段中输入所需时间(以秒为单位)。

5）单击 Apply 确认配置更改。

4、配置验证

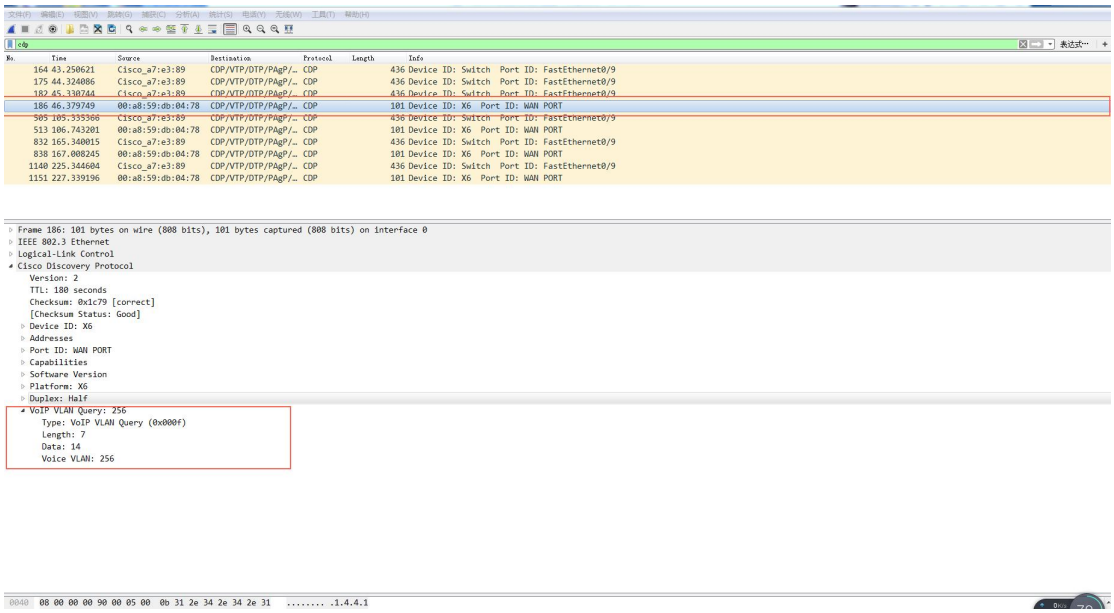
启用 CDP 功能后，话机执行以下操作:

1）定期将话机的信息(如软件修改、设备 ID、功耗)发送到网络上的多播地址上。

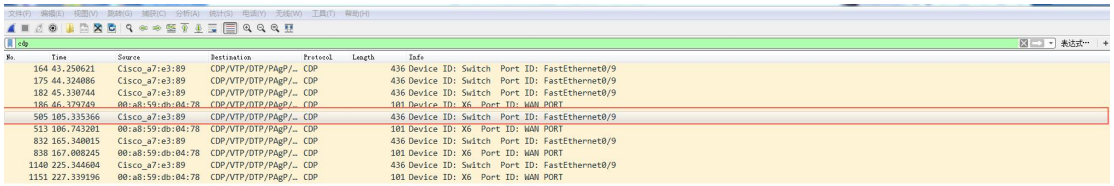
2）允许将 CDP 数据包收到网络(广域网)端口或无线局域网端口。

3）获得连接端口的 VLAN ID。

下图显示了通过电话发送的CDP数据包(在学习到交换机VLAN id和VLAN查询字段之前)

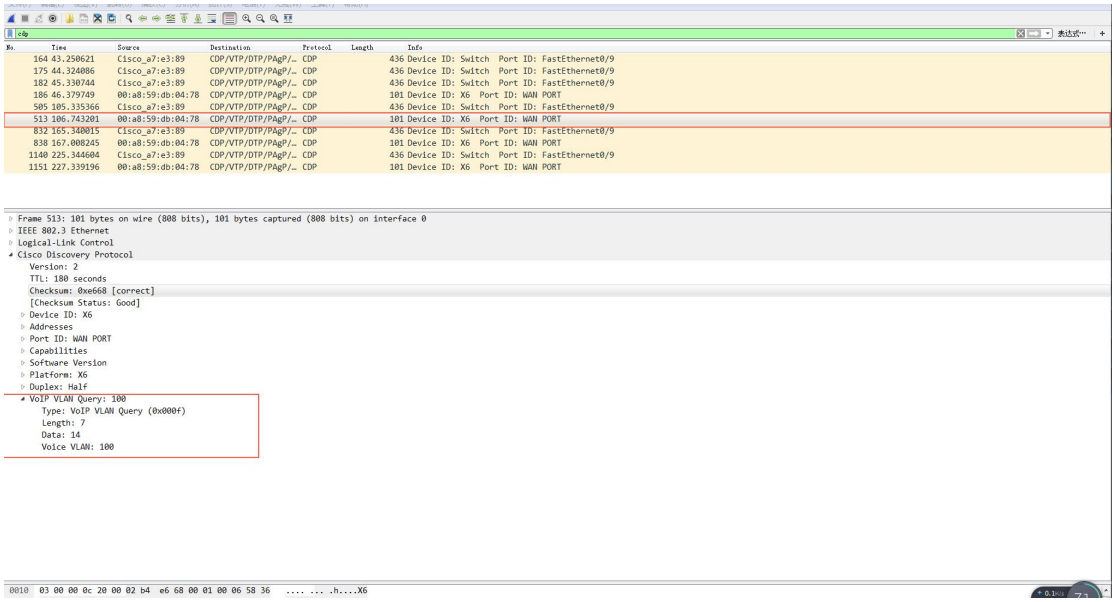


下图显示了电话接收的 CDP 数据包(使用 VLAN 应答字段，由交换机发送)。



下图显示了通过电话发送的 CDP 数据包(在学习到交换机的 VLAN id 后，可以看到 VLAN

查询字段)。



2.3.3 DHCP 介绍

1、DHCP VLAN 介绍

话机支持通过 DHCP 发现 VLAN。当 VLAN 发现方法被设置为 DHCP 时，话机将检测到一个有效的 VLAN ID 的 DHCP 选项，默认情况下，使用预定义的选项 132 来提供 VLAN ID。用户可以定制用于检测 VLAN ID 的 DHCP 选项。

2、DHCP VLAN 功能配置

以 x6 型号话机为例，下图为 DHCP VLAN 配置界面

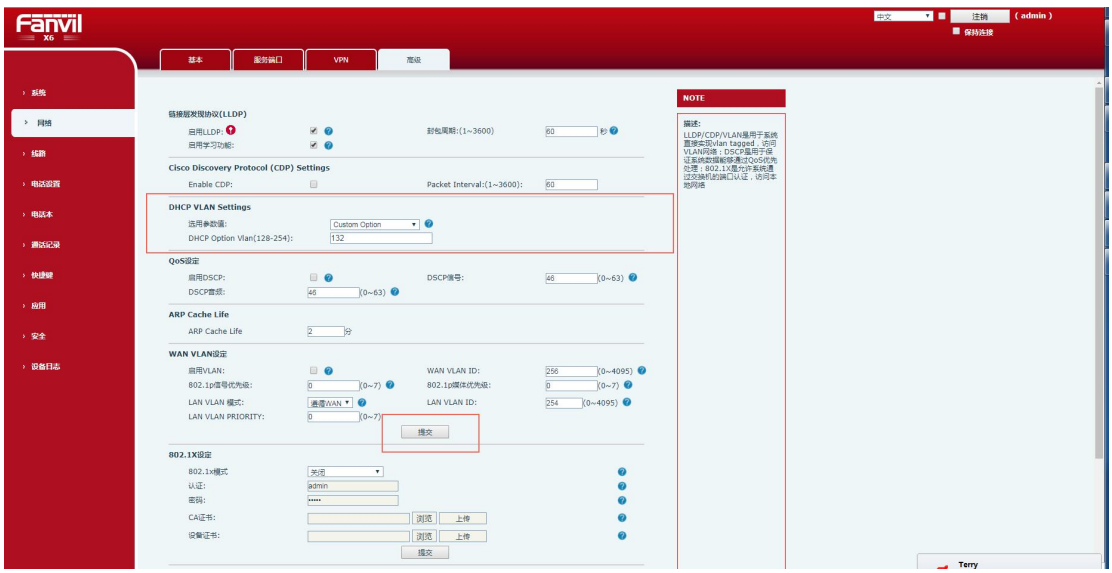


图 1-7 DHCP VLAN 配置界面

1）使用管理员凭证登录到 web 用户界面，默认管理员用户名和密码都是“admin”。

2）点击 Network->Advanced.

3）在 VLAN 块中，从 DHCP VLAN 激活的下拉列表中选择所需的值。

4）在选项字段中输入所需要的值，用户可以通过逗号指定最多的 5 个选项和单独的选项。

5）单击 Apply 确认配置更改。

3、配置验证

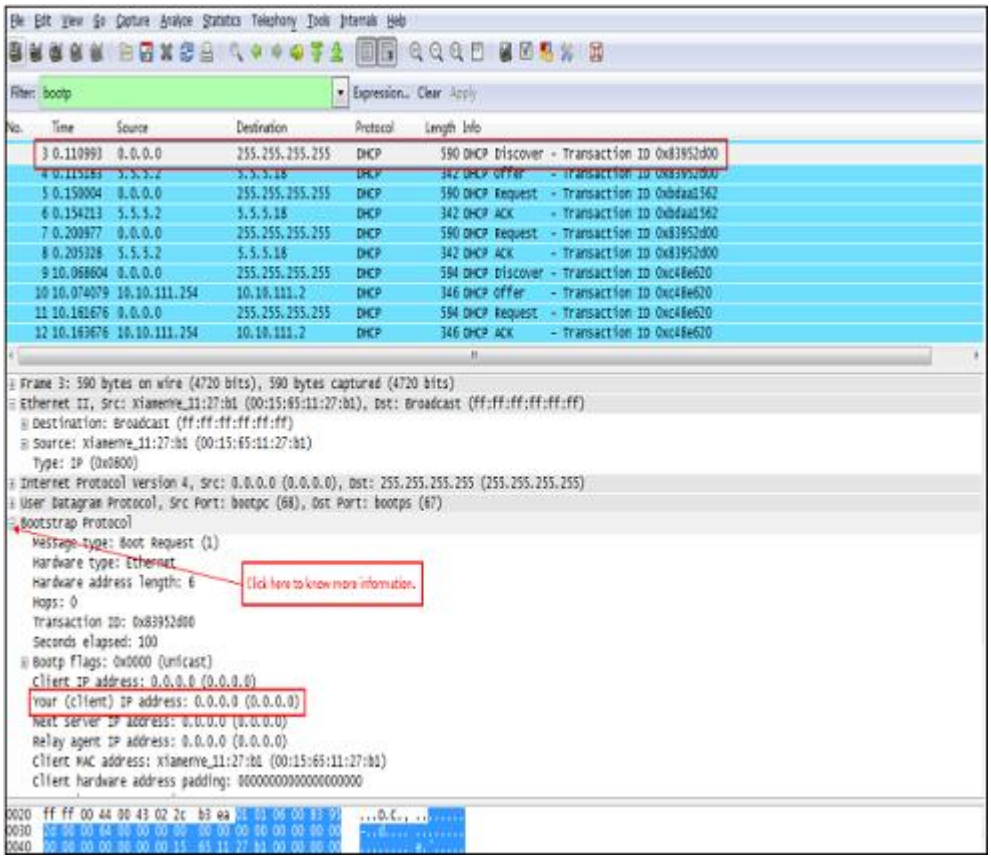
当将话机配置为使用 DHCP 进行 VLAN 发现时，DHCP 选项设置为 132，话机执行以下操作:

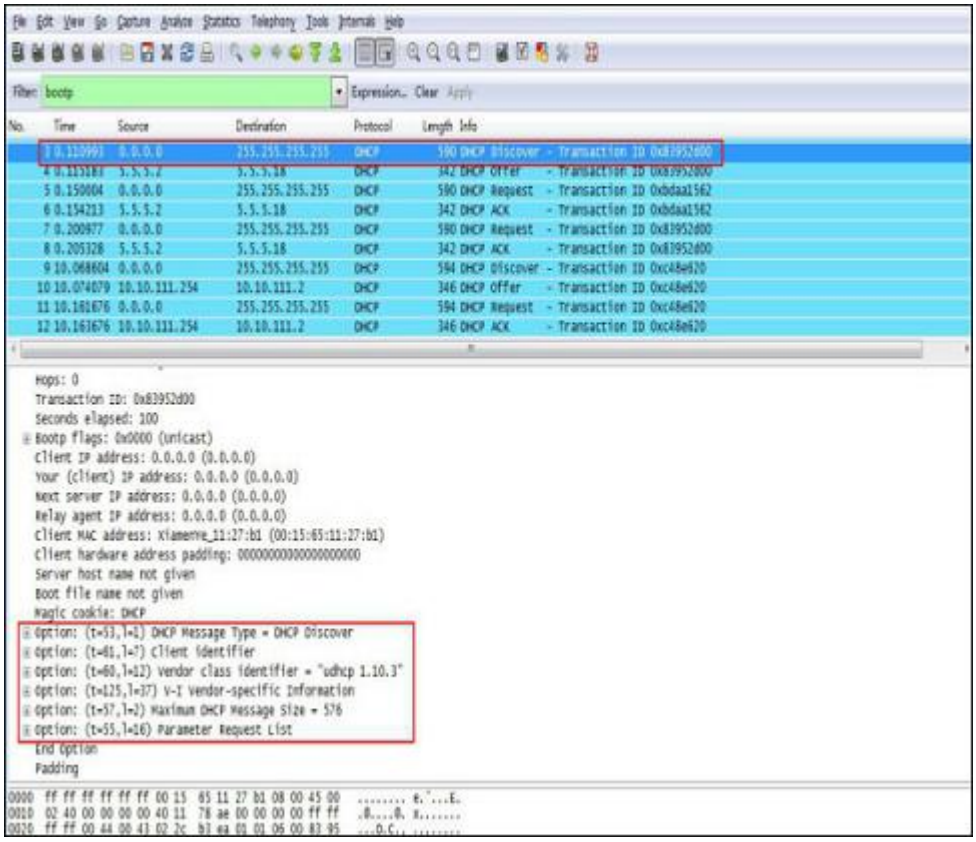
1）话机广播一个 DHCP 发现消息，以检查是否有一个 DHCP 服务器可用。

2）如果 DHCP 服务器发送带有选项 132 的 DHCP 消息，话机将接收消息，发送 DHCP 请求，并保存 DHCP 服务器在 DHCP 选项 132 中提供的 VLAN ID。

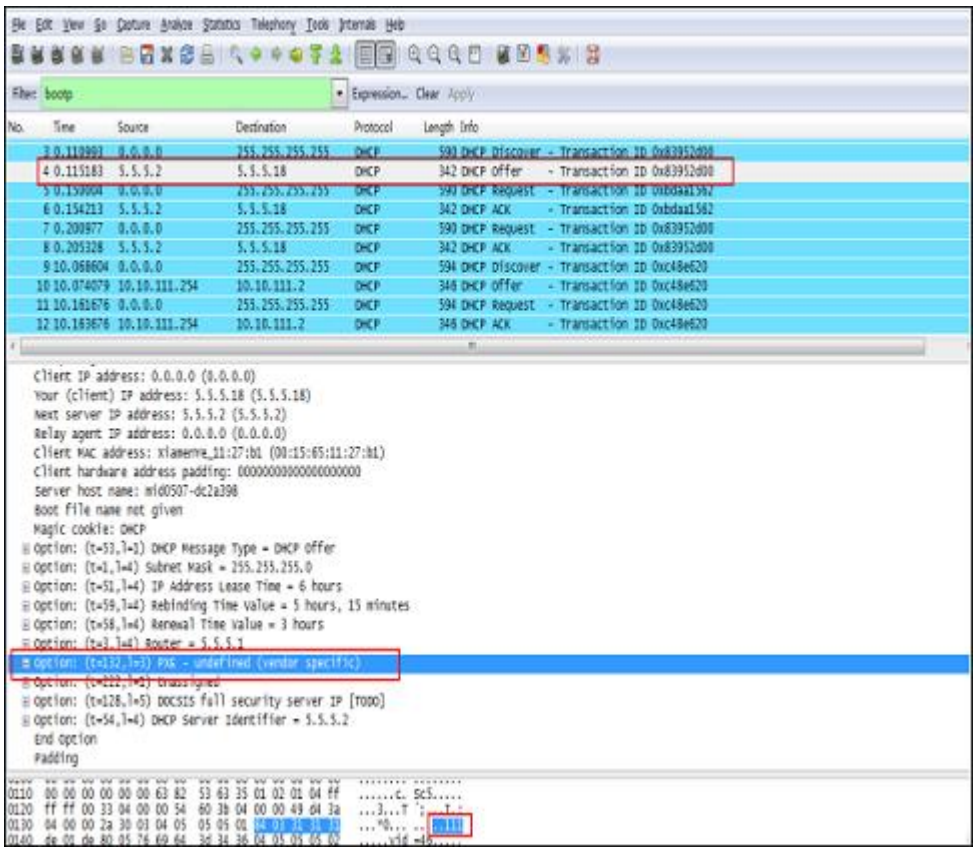
3）从 DHCP 服务器获取 VLAN ID 后，话机将释放所租用的 IP 地址，并启动一个新的 DHCP 发现周期，并使用现在已知的语音 VLAN ID 标记。在此过程之后，话机将通过 DHCP 选项 132 中从 DHCP 服务器获得的 VLAN ID 发送所有数据包。

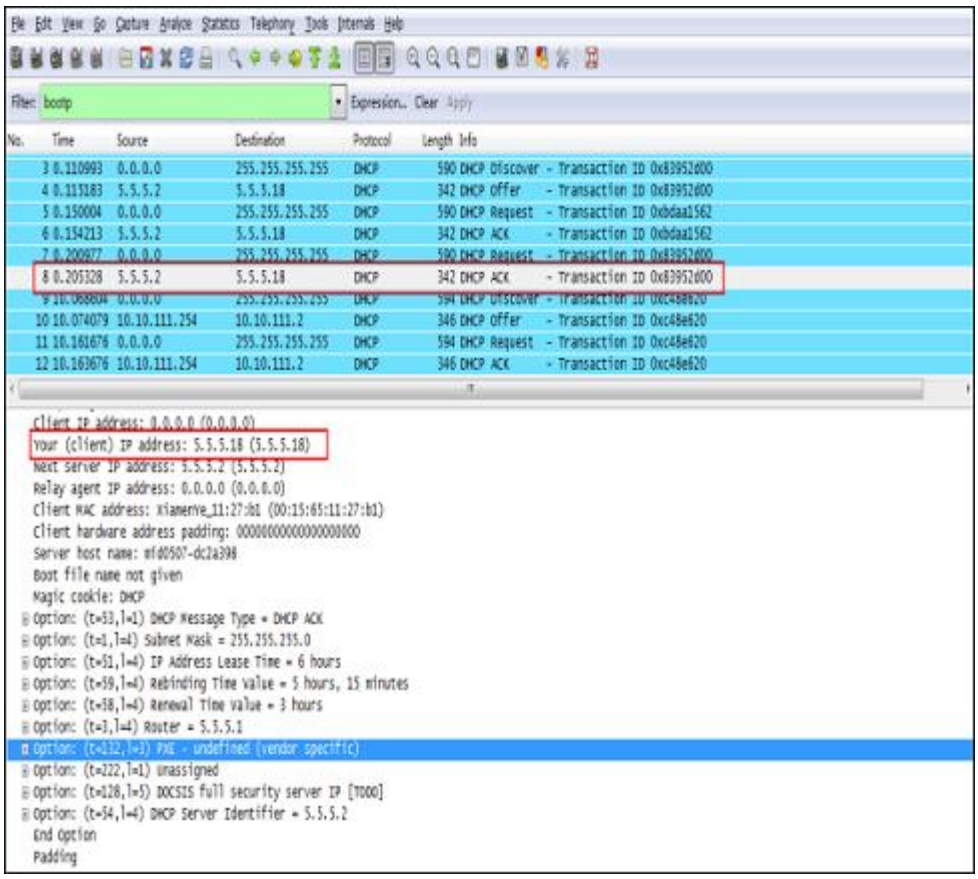
下图显示了通过电话发送的 DHCP 发现消息(在获取 VLAN ID 之前):





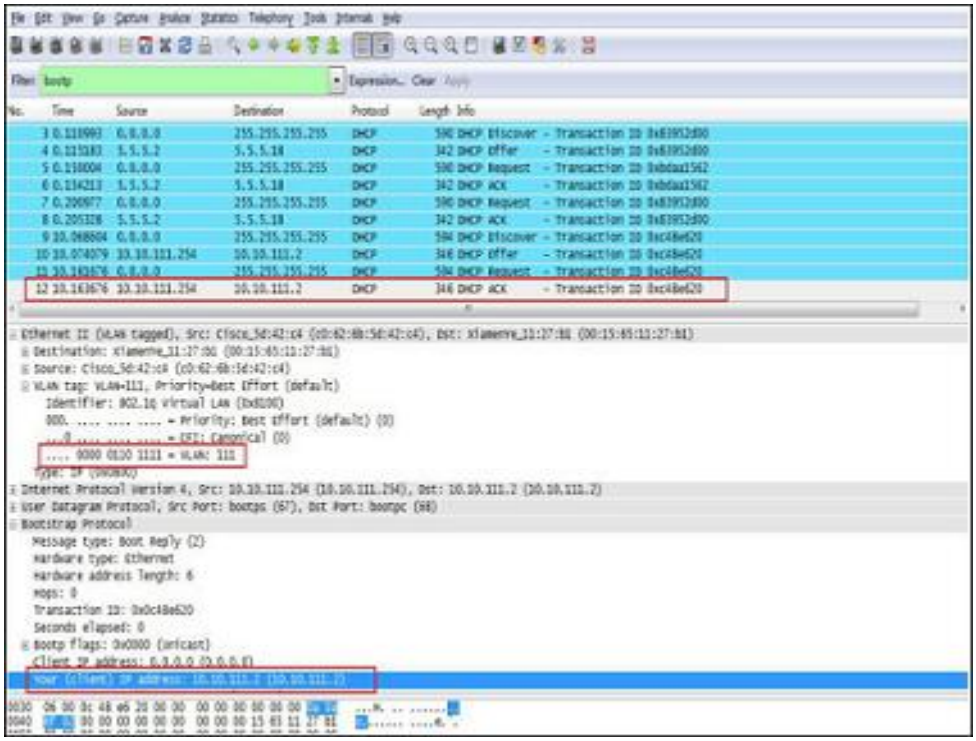
下图显示了由电话接收的 DHCP 提供的消息(DHCP 服务器发送了一个 DHCP 提供了选项 132):





下图显示了通过电话接收的 DHCP 消息(DHCP 服务器将 ACK 消息发送到话机):

从 DHCP 服务器获取 VLAN ID 后，话机将释放所租用的 IP 地址(5.5.5.18)，并使用 VLAN-tag 111 启动一个新的 DHCP 发现消息。下图显示了话机收到的 DHCP 消息:



在此过程之后，话机从 VLAN 111 中的 DHCP 服务器获得了一个 IP 地址(10.10.111.2)。

2.3.4 VLAN

1、VLAN 介绍

默认情况下，VLAN 在话机上是禁用的。用户可以通过 web 用户界面或话机用户界面或使用配置文件配置 VLAN。在通过话机配置 VLAN 之前，用户需要从网络管理员获得 VLAN ID。当用户配置 VLAN 特性时，最重要的问题是在交换机上确认连接端口(访问、主干和混合端口)的类型。这确保了从话机中(标记/未标记)的信息可以正常传输。VLAN 特性可能会影响到话机在网络中的功能。在配置之前，请联系网络管理员了解更多信息。

2、VLAN 功能配置

用户可以启用或禁用 VLAN，并分别为 Internet (WAN)端口和 PC（LAN）端口设置特定的 VLAN id 和优先级

通过 web 用户界面为 Internet (WAN)端口配置 VLAN：

以 x6 型号话机为例，下图为 VLAN 配置界面

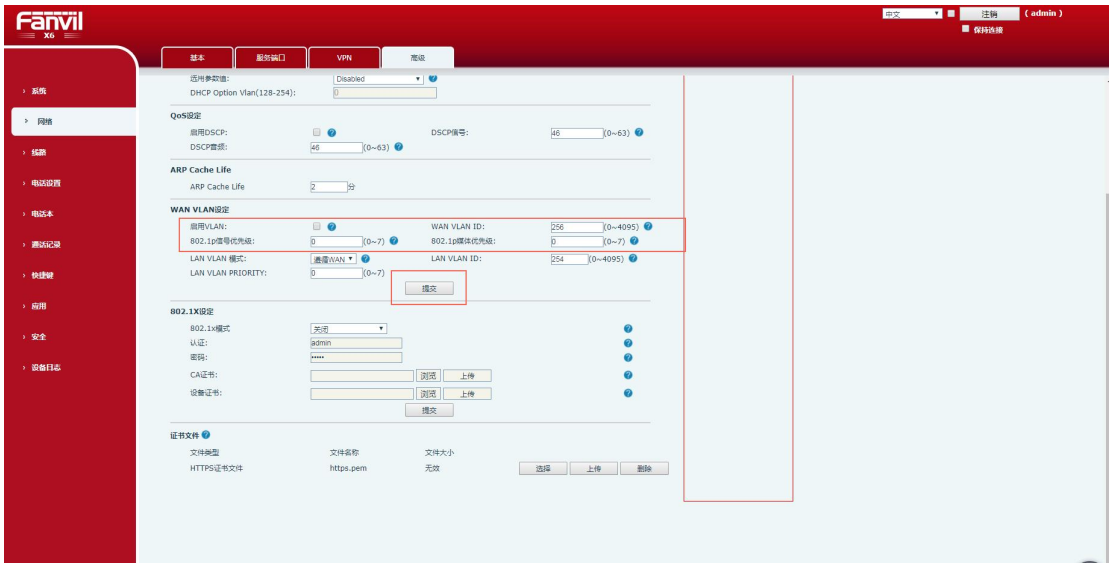


图 1-8 WAN VLAN 配置界面

1）使用管理员凭证登录到 web 用户界面，默认管理员用户名和密码都是“admin”。

2）点击 Network->Advanced.

3）在 VLAN 块中，通过勾选的方式选择是否使能开启 VLAN。

4) 从 WAN VLAN ID(1-4094)字段中输入 VLAN ID。

5）在优先级的设置字段中输入所需的值(0-7)。7 是最高优先级。

6）单击 Apply 确认配置更改。

通过 web 用户界面为 PC 端口配置 VLAN:：

以 x6 型号话机为例，下图为 VLAN 配置界面

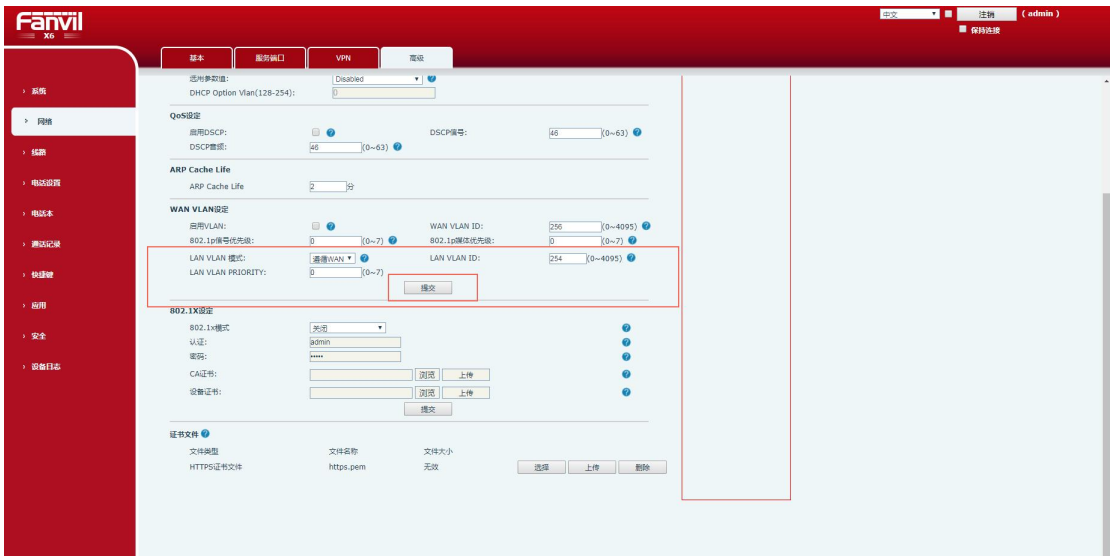


图 1-9 LAN VLAN 配置界面

1）使用管理员凭证登录到 web 用户界面，默认管理员用户名和密码都是“admin”。

2）点击 Network->Advanced.

3）在 VLAN 设置块中，从 LAN VLAN 端口的 MODE 下拉列表中选择所需的值。

4) 从 LAN VLAN ID(1-4094)字段中输入 VLAN ID。

5）在优先级的设置字段中输入所需的值(0-7)。7 是最高优先级。

通过话机用户界面配置 VLAN (WAN)端口信息:

以 x6 型号话机为例，下图为 VLAN 配置界面

图 2-1 WAN VLAN 配置界面

1）Menu->Advanced(Enter Password:123)->Network->QoS&Vlan->WAN VLAN。

2) 通过话机上的 left/right 选择按键，或者 softkey 的 left/right 选择按键，选择是否开启 WAN WLAN。

3) 从 WAN VLAN ID(1-4094)字段中输入 VLAN ID。

4) 在优先级的设置字段中输入所需的值(0-7)。7 是最高优先级

5) 按下 OK 按键保存配置修改。

通过话机用户界面配置 VLAN (WAN)端口信息:

以 x6 型号话机为例，下图为 VLAN 配置界面

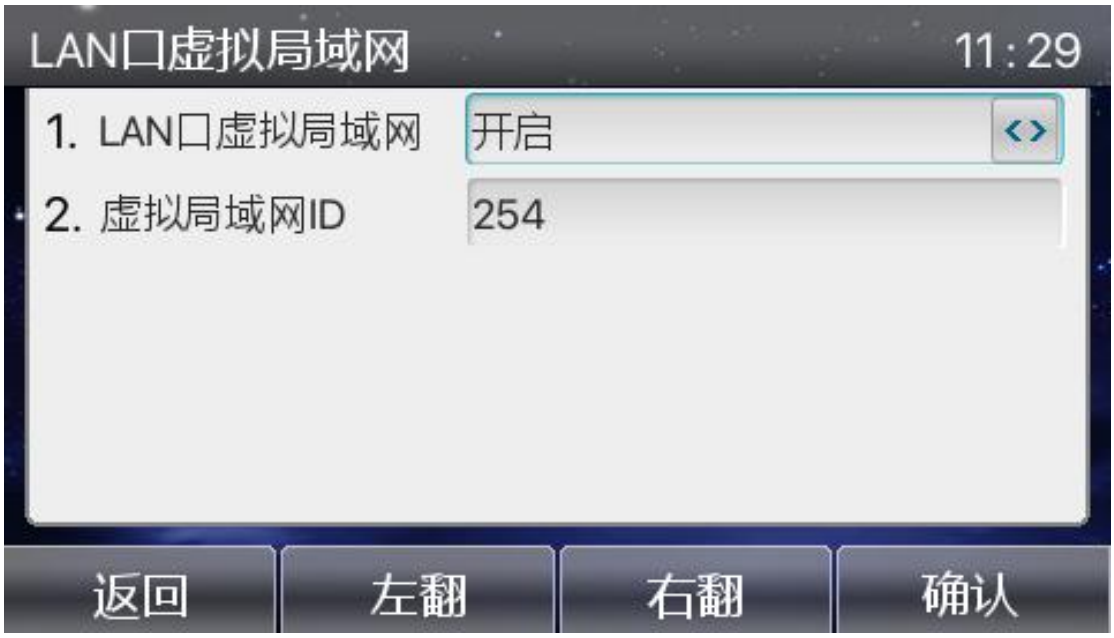


图 2-2 LAN VLAN 配置界面

1）Menu->Advanced(Enter Password:123)->Network->QoS&Vlan->LAN VLAN。

2）通过话机上的 left/right 选择按键，或者 softkey 的 left/right 选择按键，选择 LAN WLAN 的值。

3）从 LAN VLAN ID(1-4094)字段中输入 VLAN ID。

4）在优先级的设置字段中输入所需的值(0-7)。7 是最高优先级

5）按下 OK 按键保存配置修改。

3、配置验证

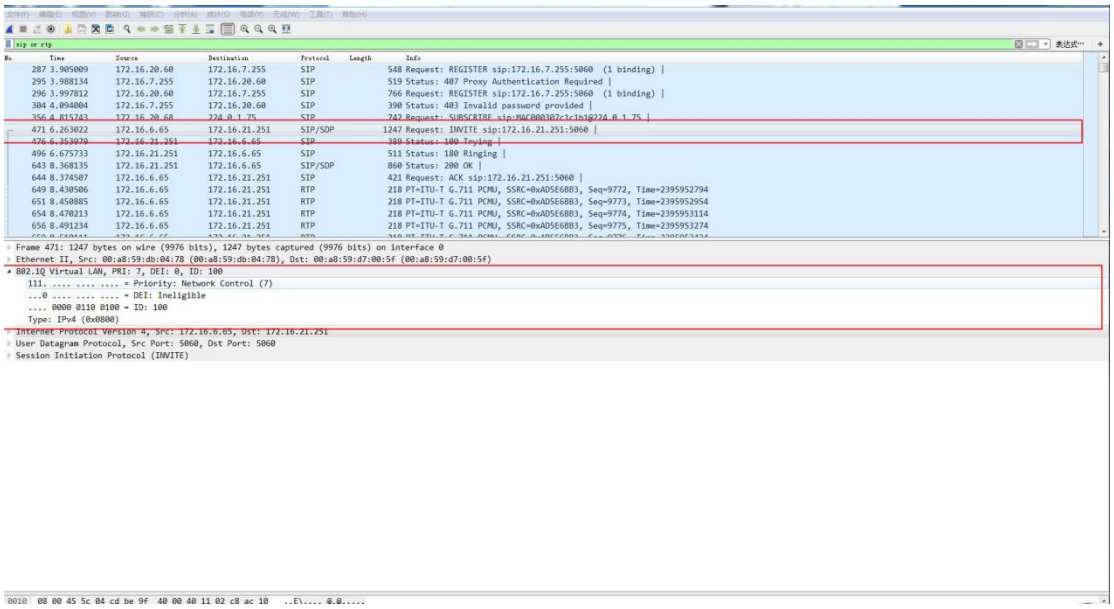
检查 802.1P 的 Audio 和 signal 设置是否正确，话机执行以下操作：

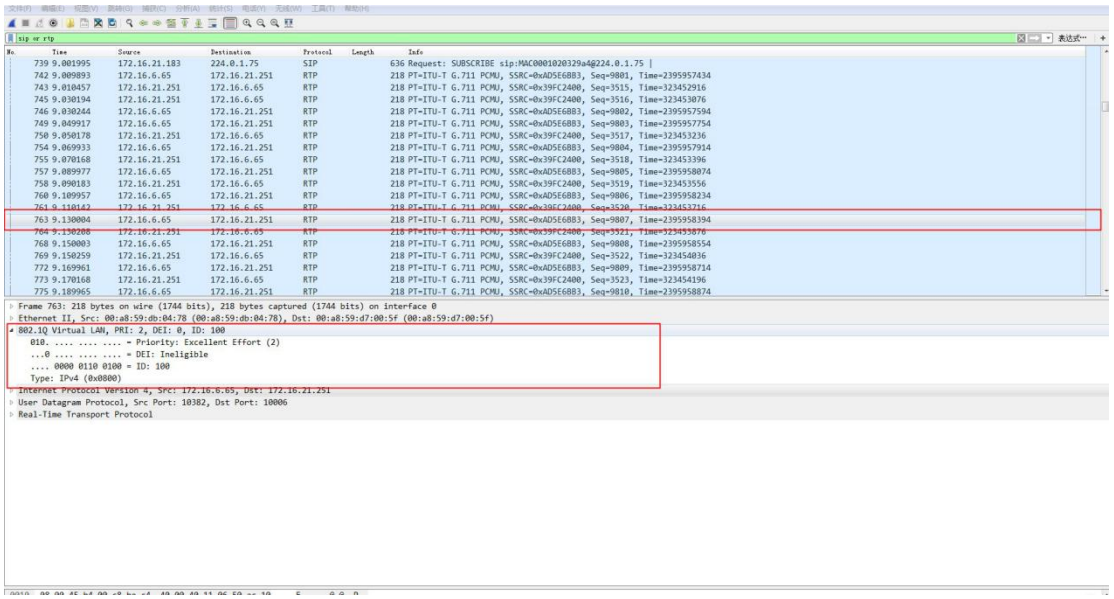
1）测试话机设置静态 ip，网页上或者话机上设置开启 VLAN，设置 VLAN ID 的值为 100，并开启 DSCP，设置 Audio DSCP、Signal DSCP 的值为不同的值；

2）802.1p Signal Priority 的值为 0-7 之间的一个任意值，例如 7，802.1p Media Priority 的值为 0-7 之间的任意一个值，例如 2；

3）抓包过滤 sip or rtp，用测试话机 ip 直拨另一个话机，抓包查看通话过程。通过 SIP 包（sip/sdp）的链路层可以看见 VLAN Tag 字段，其中可看见 VLAN ID，并且 Priority 字段的值即为 802.1p Signal Priority 的值，Signal DSCP 的值为测试话机设置的值。通过 rtp 包的链路层可以看见 VLAN Tag 字段，其中可看见 VLAN ID 为测试话机设置的 VLAN ID，Priority 字段的值即为 802.1p Media Priority 的值，Audio DSCP 为测试话机设置的值。

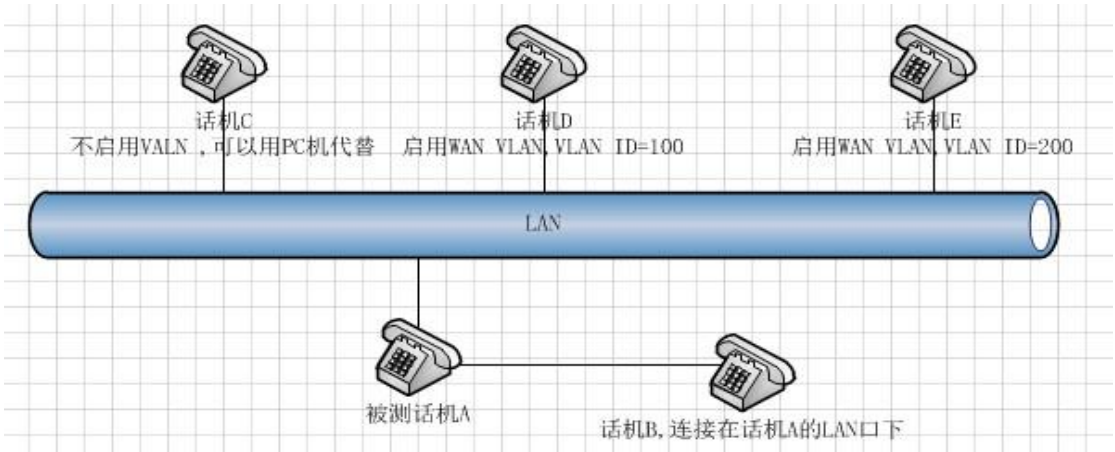
以下为对应测试的抓包截图：





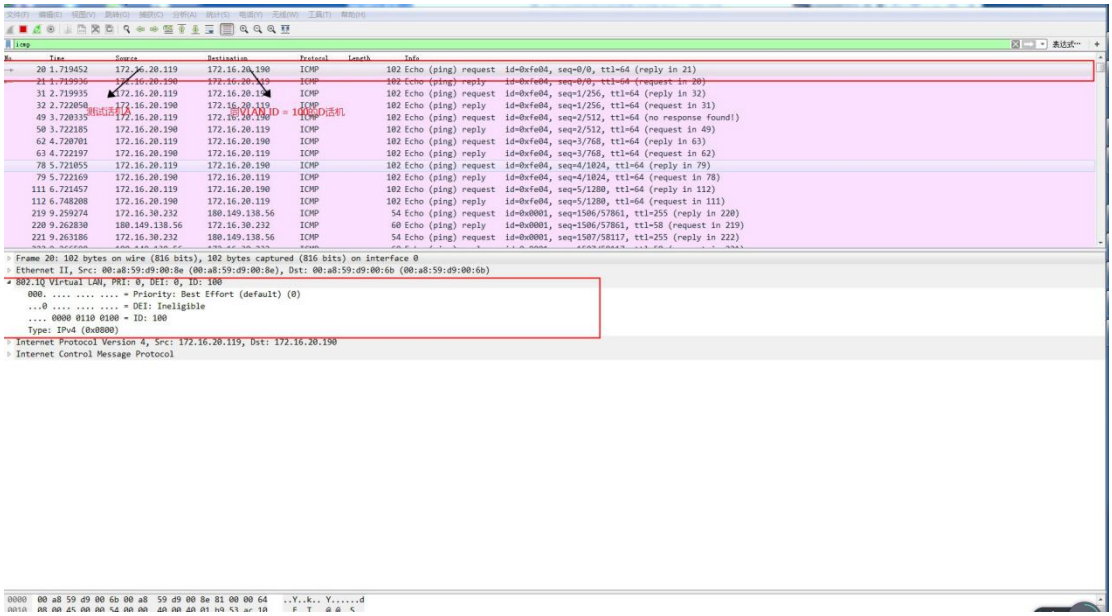
开启 wan vlan，同 tag 的设置可以互通，话机执行以下操作：

测试环境：被测话机 A 与辅助测试话机 C、D、E 连接在同一个 hub 或者交换机下，辅助测试话机 B 连接在 A 的 LAN 口下，如下图所示：

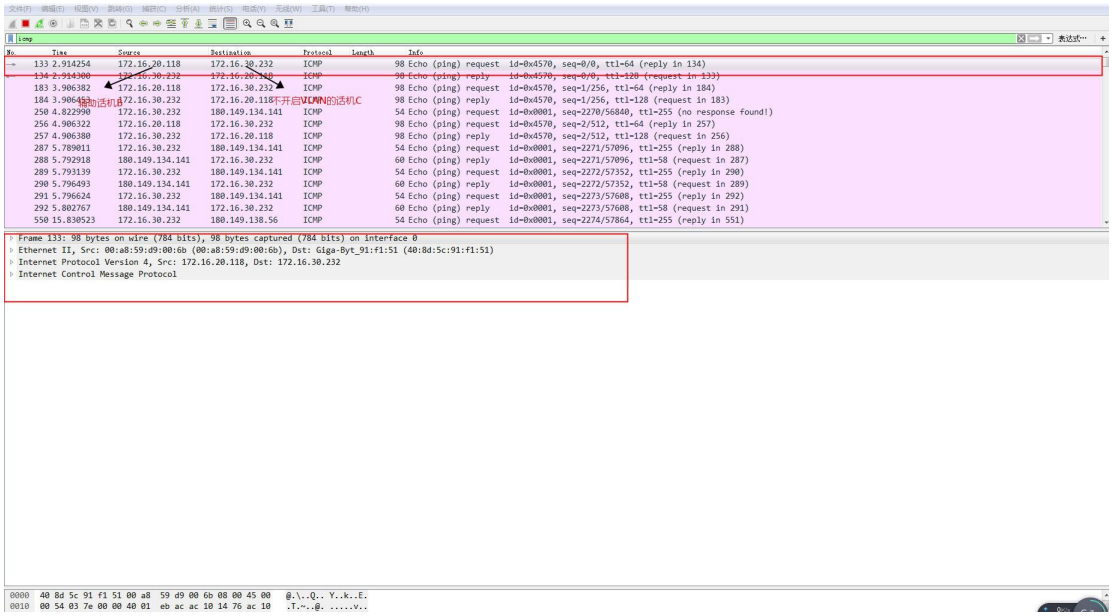


1）登录网页，修改配置为此（如果此前已经启用了 VLAN，pc 无法访问 web 时，可以先从 LCD 中将 VLAN disable），WLAN ID = 100，LAN VLAN 为 disable，并设置保存成功；

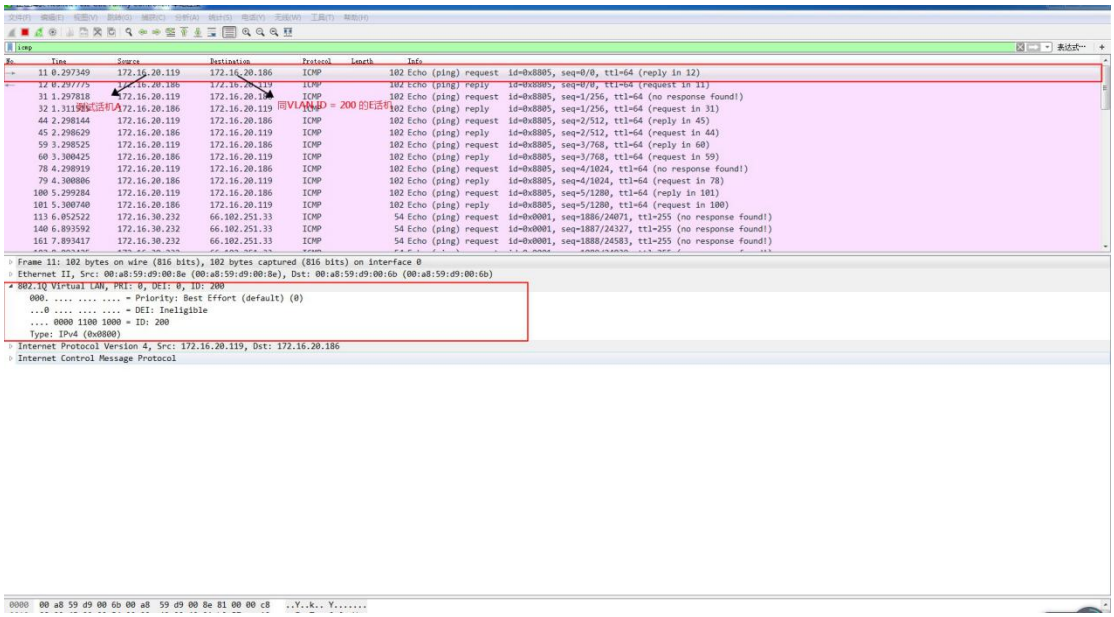
2）分别用话机 A 去 ping 话机 B、C、D、E，可以看到话机 A 可以 ping 通话机 D，不能 ping 通 B、C、E，抓包可以看到 A 发出的包带 tag 100，抓包如下：



3）分别用话机 B 去 ping 话机 A、C、D、E，可以看到话机 B 可以 ping 通话机 C，不能 ping 通 A、D、E，抓包确认话机 B 发出的包不带 tag，抓包如下：



4）修改 WAN port VLAN ID 为 200，重复测试步骤 2、3，可以看到话机 A,可以 ping 通话机 E，不能 ping 通 B、C、D，抓包确认话机 A 发出的包带 tag 200；话机 B，可以 ping 通话机 C，不能 ping 通 A、D、E，抓包确认话机 B 发出的包不带 tag。


icmp
No. Time Source Destination Protocol Length Info
11 0.297349 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=0/0, ttl=64 (reply in 12)
12 0.297775 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=0/0, ttl=64 (request in 11)
31 1.297818 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=1/256, ttl=64 (no response found!)
32 1.311 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=1/256, ttl=64 (request in 31)
44 2.298144 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=2/512, ttl=64 (reply in 45)
45 2.298629 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=2/512, ttl=64 (request in 44)
59 3.298525 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=3/768, ttl=64 (reply in 60)
60 3.300425 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=3/768, ttl=64 (request in 59)
78 4.298919 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=4/1024, ttl=64 (no response found!)
79 4.300806 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=4/1024, ttl=64 (request in 78)
100 5.299284 172.16.20.119 172.16.20.186 ICMP 102 Echo (ping) request id=0x8805, seq=5/1280, ttl=64 (reply in 101)
101 5.300740 172.16.20.186 172.16.20.119 ICMP 102 Echo (ping) reply id=0x8805, seq=5/1280, ttl=64 (request in 100)
113 6.052522 172.16.30.232 66.102.251.33 ICMP 54 Echo (ping) request id=0x0001, seq=1886/24071, ttl=255 (no response found!)
140 6.893592 172.16.30.232 66.102.251.33 ICMP 54 Echo (ping) request id=0x0001, seq=1887/24327, ttl=255 (no response found!)
161 7.893417 172.16.30.232 66.102.251.33 ICMP 54 Echo (ping) request id=0x0001, seq=1888/24583, ttl=255 (no response found!)
测试活机A
同VLAN ID = 200 的E活机
Frame 11: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: 00:a8:59:d9:00:8e (00:a8:59:d9:00:8e), Dst: 00:a8:59:d9:00:6b (00:a8:59:d9:00:6b)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 200
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
.... 0000 1100 1000 = ID: 200
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.20.119, Dst: 172.16.20.186
Internet Control Message Protocol
0000 00 a8 59 d9 00 6b 00 a8 59 d9 00 8e 81 00 00 c8 ..Y..k.. Y.....

3 交换机 Vlan

3.1 Trunk 的精解，分析 tagged 和 untagged

以太网端口有三种链路类型：Access、Hybrid 和 Trunk。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口；Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。端口接收数据时： 如果端口是 tagged 方式，当数据包本身不包含 VLAN 的话，输入的数据包就加上该缺省 vlan；如果数据包本身已经包含了 VLAN，那么就不再添加。 如果是 untagged 方式，输入的数据包全部都要加上该缺省 vlan。不管输入的数据包是否已经有 VLAN 标记。 端口发送数据时： 如果端口是 tagged 方式，如果端口缺省 VLAN 等于发送的数据包所含的 VLAN，那么就会将 VLAN 标记从发送的数据包中去掉；如果不相等，则数据包将带着 VLAN 发送出去，实现 VLAN 的透传。 如果是 untagged 方式，则不管端口缺省 VLAN 为多少，是否等于要输出的数据包的 VLAN，都会将 VLAN ID 从数据包中去掉。

以太网端口有三种链路类型：Access、Hybrid 和 Trunk。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口；Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。这里的 trunk 并不是端口干路的概念，即端口汇聚或者链路聚合，而是允许 vlan 透传的一个概念。

需要注意的是：

1) 在一台以太网交换机上，Trunk 端口和 Hybrid 端口不能同时被设置。

2) 如果某端口被指定为镜像端口，则不能再被设置为 Trunk 端口，反之亦然。

3) 缺省情况下，端口为 Access 端口。 Access 端口只属于 1 个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，不用设置；

4) Hybrid 端口和 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID。如果设置了端口的缺省 VLAN ID，当端口接收到不带 VLAN Tag 的报文后，则将报文转发到属于缺省 VLAN 的端口；当端口发送带有 VLAN Tag 的报文时，如果该报文的 VLAN ID 与端口缺省的 VLAN ID 相同，则系统将去掉报文的 VLAN Tag，然后再发送该报文。

需要注意的是：

1) Trunk 端口不能和 isolate-user-vlan 同时配置；

2) Hybrid 端口可以和 isolate-user-vlan 同时配置。但如果缺省 VLAN 是在 isolate-user-vlan

中建立了映射的 VLAN，则不允许修改缺省 VLAN ID，只有在解除映射后才能进行修改。

3) 本 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 和相连的对端交换机的 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能正确传输。

4) 缺省情况下，Hybrid 端口和 Trunk 端口的缺省 VLAN 为 VLAN 1，Access 端口的缺省 VLAN 是本身所属于的 VLAN。

由于每一台桌面交换机上连接有分别属于 VLAN1 和 VLAN2 的工作站，而上连端口只有一个，因此，我们需要在交换机和交换机的连接端口上设置为"加标签"（Tagged）。而服务器和工作站的连接端口是不识别标签的，因此连接端口应该设置为"取消标签"（Untagged）。

1) Trunk 端口不能和 isolate-user-vlan 同时配置；Hybrid 端口可以和 isolate-user-vlan 同时配置。但如果缺省 VLAN 是在 isolate-user-vlan 中建立了映射的 VLAN，则不允许修改缺省 VLAN ID，只有在解除映射后才能进行修改。

2) 本 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 和相连的对端交换机的 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 必须一致，否则报文将不能正确传输。

交换机接口出入数据处理过程：

tag 就是普通的 ethernet 报文，报文结构的变化是在源 mac 地址和目的 mac 地址之后，加上了 4bytes 的 vlan 信息，也就是 vlan tag 头；untag 就是普通的 ethernet 报文，比 tag 报文少了 4 bytes 字节。

情况列举 Switch 收发 Switch 对标记的处理 remark

Access (接收) Tagged = PVID 不接收 注：部分高端产品可能接收。

Access (接收) Tagged =/ PVID 不接收 注：部分高端产品可能接收。

Access (接收) Untagged 接收 增加 tag＝PVID 从 PC

Access (发送) Tagged = PVID 转发 删除 tag

Access (发送) Tagged =/ PVID 不转发 不处理

Access (发送) Untagged 无此情况 无此情况 无此情况

Trunk (接收) Tagged = PVID 接收 不修改 tag

Trunk (接收) Tagged =/ PVID 接收 不修改 tag

Trunk (接收) Untagged 接收 增加 tag＝PVID

Trunk (发送) Tagged = PVID If Passing then 转发 删除 tag

Trunk (发送) Tagged =/ PVID If Passing then 转发 不修改 tag

Trunk (发送) Untagged 无此情况 无此情况 无此情况（注）

Hybrid (接收) Tagged = PVID 接收 不修改 tag 对端是 trunk

Hybrid (接收) Tagged =/ PVID 接收 不修改 tag 对端是 trunk

Hybrid (接收) Untagged 接收 增加 tag＝PVID 类 Trunk

Hybrid (发送) Tagged = PVID Tag 和 untag 中列出的 vlan 可以 passing 看 Tag 项和 untag 项

Hybrid (发送) Tagged =/ PVID Tag 和 untag 中列出的 vlan 可以 passing 看 Tag 项和 untag 项

Hybrid (发送) Untagged 无此情况 无此情况 无此情况（注）

收报文：

Acess 端口

收到一个报文,判断是否有 VLAN 信息：如果没有则打上端口的 PVID，并进行交换转发,如果有则直接丢弃（缺省）

发报文：

Acess 端口：

将报文的 VLAN 信息剥离，直接发送出去

收报文：

trunk 端口：

收到一个报文，判断是否有 VLAN 信息：如果没有则打上端口的 PVID，并进行交换转发，如果有判断该 trunk 端口是否允许该 VLAN 的数据进入：如果可以则转发，否则丢弃

发报文：

trunk 端口：

比较端口的 PVID 和将要发送报文的 VLAN 信息，如果两者相等则剥离 VLAN 信息，再发送，如果不相等则直接发送

收报文：

hybrid 端口：

1 收到一个报文

2 判断是否有 VLAN 信息：如果没有则打上端口的 PVID，并进行交换转发，如果有则判断该 hybrid 端口是否允许该 VLAN 的数据进入：如果可以则转发，否则丢弃

发报文：

hybrid 端口：

1 判断该 VLAN 在本端口的属性（disp interface 即可看到该端口对哪些 VLAN 是 untag，哪些 VLAN 是 tag）

2 如果是 untag 则剥离 VLAN 信息，再发送，如果是 tag 则直接发送

3.2 不同链路类型端口收发报文的差异

<table>
<tr><th rowspan="2">端口类型</th><th colspan="2">对接收报文的处理</th><th rowspan="2">对发送报文的处理</th></tr>
<tr><th>当接收到的报文不带 Tag 时</th><th>当接收到的报文带有 Tag 时</th></tr>
<tr><td>Access 端口</td><td>为报文打上缺省 VLAN 的 Tag</td><td>当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文
当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文</td><td>由于 VLAN ID 就是缺省 VLAN ID，去掉 Tag，发送该报文</td></tr>
<tr><td>Trunk 端口</td><td rowspan="2">当缺省 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文，给报文打上缺省 VLAN 的 Tag
当缺省 VLAN ID 不在端口允许通过的 VLAN ID 列表里时，丢弃该报文</td><td rowspan="2">当 VLAN ID 在端口允许通过的 VLAN ID 列表里时，接收该报文
当 VLAN ID 是该端口不允许通过的 VLAN ID 时，丢弃该报文</td><td>当 VLAN ID 与缺省 VLAN ID 相同，且是该端口允许通过的 VLAN ID 时：去掉 Tag，发送该报文
当 VLAN ID 与缺省 VLAN ID 不同，且是该端口允许通过的 VLAN ID 时：保持原有 Tag，发送该报文</td></tr>
<tr><td>Hybrid 端口</td><td>当报文中携带的 VLAN ID 是该端口允许通过的 VLAN ID 时，发送该报文</td></tr>
</table>

4 Cisco2960 系列交换机 VLAN 配置

4.1 以太网 VLAN 的默认值

以太网 VLAN 的默认值和范围

参数	默认	范围
VLAN ID	1	1～4094。 **注意** 扩展范围的 VLAN（VLAN ID 的范围是 1006 至 4094）没有被保存在 vlan 的数据库。
VLAN 名称	*VLANxxxx*，其中 *XXXX* 代表四个数字（包括前导零）等于 VLAN ID 号	没有范围
IEEE 802.10 SAID	100001（100000 加 t VLAN ID）	1 到 4294967294
MTU 大小	1500	1500 到 18190
Translational bridge 1	0	0 至 1005
Translational bridge 2	0	0 至 1005
VLAN 状态	活跃	活跃，暂停

4.2 创建或修改以太网 vlan

vlan 数据库中的每个以太网 vlan 都有属于 1 到 1001 中的唯一的四位数字的 ID，VLAN IDs 1002 到 1005 是为 Token Ring 和 FDDI VLANs 保留的。创建一个新的 vlan 被加入到 vlan 数据库里，为 vlan 分配一个 id 和名字。

在特权模式下，用以下命令来创建和修改 vlan。

	命令	目的
Step 1	**configure terminal**	进入全局配置模式。

Step 2	**vlan** *vlan-id*	输入 VLAN ID。输入新的 VLAN ID 来创建一个 VLAN，或者输入现有 VLAN ID 修改该 VLAN。 **注意** 此命令可用的 VLAN ID 范围是 1～4094。
Step 3	**name** *vlan-name*	（可选）输入该 VLAN 的名称。如果没有输入的 VLAN 名称，默认是 *vlan 附加*带有前导 0 的四位数字。例如，VLAN0004 是 vlan 4 的默认名称。
Step 4	**mtu** *mtu-size*	（可选）更改 MTU 大小（或其他 VLAN 特性）。
Step 5	**remote-span**	（可选）配置 vlan 为远程 SPAN 会话的 RSPAN VLAN。 **注意** 交换机必须运行使用 LAN 基本镜像 RSPAN。
Step 6	**end**	返回特权模式。
Step 7	**show vlan**{**name** *vlan-name* | **id** *vlan-id*}	确认您的输入。
Step 8	**copy running-config startup config**	（可选）保存交换机配置。

4.3 删除 vlan

不能删除不同介质类型的默认 vlan：以太网 VLAN 1 和 FDDI 或 Token Ring VLANs 1002 至 1005。

注意 ： 当你删除一个 VLAN，任何分配给该 VLAN 的端口变得无效。他们仍然是与 VLAN 相关的（因而是无效的），直到您将它们分配到一个新的 VLAN。

在特权模式下，按照以下步骤删除 vlan：

	命令	目的
Step 1	**configure terminal**	进入全局配置模式。
Step 2	**no vlan** *vlan-id*	通过输入 vlan 的 ID 删除 valn。
Step 3	**end**	返回特权模式。
Step 4	**show vlan brief**	确认 vlan 已经被删除。
Step 5	**copy running-config startup**	（可选）保存交换机配置

	config	

4.4 分配静态端口的 vlan

注意： 如果你指定接口的 VLAN 不存在，创建新的 VLAN。

在特权模式下，按照以下步骤进行配置：

	Command	**Purpose**
Step 1	**configure terminal**	进入全局配置模式。
Step 2	**interface** *interface-id*	输入的接口加入 VLAN。
Step 3	**switchport mode access**	为端口定义 vlan 的成员模式（二层接入端口）。
Step 4	**switchport access vlan** *vlan-id*	将端口分配到一个 vlan 下。有效的 VLAN ID 是 1～4094。
Step 5	**end**	返回特权模式
Step 6	**show running-config interface***interface-id*	验证接口的成员模式。
Step 7	**copy running-config startup-config**	（可选）保存配置。

4.5 配置 valn 中继端口（trunk 端口）

特权模式下，根据下面步骤配置一个 trunk 端口：

	命令	**目的**
Step 1	**configure terminal**	进入全局配置模式。
Step 2	**interface** *interface-id*	指定端口被配置为集群，并进入接口配置模式。
Step 3	**switchport mode trunk**	配置接口为二层 Trunk（要求该接口是一个二层接入端口或指定中继模式）。
Step 4	**switchport access vlan***vlan-id*	（可选）指定缺省 VLAN，如果接口停止中继。
Step 5	**switchport trunk native vlan** *vlan-id*	为 802.1Q 中继指定本地 VLAN。
Step 6	**end**	返回特权模式。
Step 7	**show interfaces***interface-id* **switchport**	显示交换机端口的配置。
Step 8	**show interfaces***interface-id* **trunk**	显示交换机端口 trunk 配置。

Step 9	**copy running-config startup-config**	（可选）保存配置。

将端口恢复默认值，用命令 **default interface** *interface-id*；要重置所有默认中继接口中继特性，使用命令 **no switchport trunk**。

配置中继口上允许的 vlan：

在特权模式下，根据下面步骤配置修改中继口上的 vlan 列表

	命令	**目的**
Step 1	**configure terminal**	进入全局配置模式。
Step 2	**interface** *interface-id*	指定的端口进行配置，并进入接口配置模式。
Step 3	**switchport mode trunk**	配置端口为 VLAN 中继端口。
Step 4	**switchport trunk allowed vlan** {**add** |**all** | **except** |**remove**} *vlan-list*	(可选) 配置修改中继口上的 vlan 列表。 *vlan-list* 可以是一个数字或者由两个数字组成一个范围，必须使用连字符。（数字的范围 1~4096） 默认情况下，允许所有 VLAN 都被允许。
Step 5	**end**	返回特权模式。
Step 6	**show interfaces***interface-id***switchport**	确认 vlan 列表配置。
Step 7	**copy running-config startup-config**	（可选）保存配置。

4.6 配置 Native VLAN 无标记流量

配置 IEEE 802.1Q 标记的 Trunk 端口可以收到标记和非标记的流量。默认情况下，交换机在本地 VLAN 配置的端口转发无标记流量。本地 VLAN 是默认 VLAN 1。

在特权模式下，根据下面步骤配置 802.1Q 中继本地 vlan：

	Command	**Purpose**
Step 1	**configure terminal**	进入特权模式。

Step 2	**interface** *interface-id*	定义被配置为 IEEE 802.1Q 中继的接口，并进入接口配置模式。
Step 3	**switchport trunk native vlan** *vlan-id*	配置 VLAN Trunk 端口上发送和接收无标记流量。 对于 *vlan-id* 的范围是 1～4094。
Step 4	**end**	返回特权 EXEC 模式。
Step 5	**show interfaces** *interface-id* **switchport**	验证配置。
Step 6	**copy running-config startup-config**	（可选）保存配置。

要恢复默认本地 vlan 配置，用端口配置命令 **no switchport trunk native vlan** 。

5 适用范围

思科 2960 系列交换机

6 参考资料

<http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/swvlan.html>