软件相关 陈少华 2017-03-08 发表

VLAN TAG是在802.1Q中定义的标签,带VLAN TAG的报文头格式如下: 01 0c cd 01 00 01 00 01 7a 01 00 52 81 00 00 00 其中 81 00为TPID,即表明此数据包为带802.1Q/802.1P标签的数据包; 接下去的00 00为TCI(标签控制信息字段),表示为二进制共有16位,其中前3位为优先级,第4位为 CFI,通常为0,第5-16位为VLAN ID,VLAN ID为0用于识别帧优先级。 某一些网卡驱动默认会在接收数据包的时候过滤VLAN TAG,使得用wireshark等软件抓到的数据包中 不含VLAN TAG,此时需要通过修改注册表让驱动保留VLAN TAG。

一、组网拓扑

为了抓到HostA与HostB之间的报文,下面介绍几种WireShark组网。

1. 在线抓取

如果WireShark本身就是组网中的一部分,那么,很简单,直接抓取报文就行了。

Switched Media — Same Computer



Figure 1, Switched Media-Same Computer

1. 串联抓取

串联组网是在报文链路中间串联一个设备,利用这个中间设备来抓取报文。

这个中间设备可以是一个HUB,利用HUB会对域内报文进行广播的特性,接在HUB上的WireShark也能收到报文。



Figure 2, Switched Media -- "Hubbing Out"

若是WireShark有双网卡,正确设置网络转发,直接串接在链路上。



Figure 3, Machine-in-the-middle

也可以利用Tap分路器对来去的报文进行分路,把报文引到WireShark上。





串联组网的好处是报文都必须经过中间设备,所有包都能抓到。缺点是除非原本就已经规划好,不然 要把报文链路断开,插入一个中间设备,会中断流量,所以一般用于学习研究,不适用于实际业务网 并联组网是将现有流量通过现网设备本身的特性将流量引出来。若是网络本身通过HUB组网的,那么将WireShark连上HUB就可以。



Figure 5, Shared Media

若是交换机组网,那直接连上也能抓取广播报文。



Figure 6, Switch-MAC Flooding

当然,最常用的还是利用交换机的镜像功能来抓包。





并联组网的优点是不用破坏现有组网,适合有业务的在线网络。缺点是HUB组网已经不常见,而交换 机组网的设备开启镜像后,对性能有非常大的影响。

1. WireShark的安装

WireShark是免费开源软件,在网上可以很轻松获取到。

Windows版的WireShark分为32位而64位两个版本,根据系统的情况来决定安装哪一个版本,虽然64 位系统装32位软件也能使用,但装相应匹配的版本,兼容性及性能都会好一些。

在Windows下,WireShark的底层抓包工具是Winpcap,一般来说WireShark安装包内本身就包含了对应可用版本的Winpcap,在安装的时候注意钩选安装就可以。安装过程简单,不再赘述。

2. 更新网卡的最新驱动

早期网卡的驱动不会对VLAN TAG进行处理,而是直接送给上层处理,在这种环境下,WireShark可以正常抓到带VLAN TAG的报文。

而Intel, broadcom, marvell的网卡则会对报文进行处理, 去掉TAG后再送到上层处理, 所以WireShar k在这种情况下通常抓不到VLAN TAG。这时我们需要针对这些网卡做一些设置, WireShark才能够抓取带VLAN TAG的报文。

- 3. 按照以下说明修改注册表
- 1) Intel

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-080 02BE10318}\00xx (where xx is the instance of the network adapter that you need to see tags on.) PCI或者PCI-X网卡增加dword:MonitorModeEnabled,通常设置为1即可

0 - disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)

1 - enabled (Store bad packets. Store CRCs. Do not strip 802.1Q vlan tags)

PCI-Express网卡增加dword:MonitorMode,通常设置为1即可

0 - disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)

1 - enabled (Store bad packets. Store CRCs. Do not strip 802.1Q vlan btag)

2 - enabled strip vlan (Store bad packets. Store CRCs. Strip 802.1Q vlan tag as normal) Broadcom

在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet下搜索,找到"TxCoalescingTicks"并确认这 是唯一的,增加一个新的字符串值"PreserveVlanInfoInRxPacket",赋值1。

2) Marvell Yukon 88E8055 PCI-E 干兆网卡

"HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\00

0" (where 000 is the number of the folder for the Marvel ethernet controller)

增加DWORD: SkDisableVlanStrip: 1

4. 以Intel网卡为例,对网卡进行配置选择Intel网卡的本地连接,右键属性

 10	慧用(B)
	状态(U)
	诊新(1)
9	桥接(G)
	创建快捷方式(S)
9	删除(D)
*	重命名(M)
-	屬件(2)

Figure 8

点击"配置"按钮。



Figure 9

在VLAN选项卡中,加入任意一个VLAN,激活接口的VLAN TAG上送功能。此时可以把"本地连接"接口 看成是一个Trunk接口。

常規 链接	主席 高级 由语管理 分组
VLAN	# VLAN
(intel) di	L VLAN ID (D):
- Aller	10
同此适配器关联的	/L VLAN 名称 (N):
VLAN 名称	VLANIO
	□未标记的 VLAN (U)
	VLAN ID
新建 (8)	
允许为适配装配置	1 正在配置。请稍候…
₩ 推算:	
 初進 規封領 	24
• 如果一 VLAN	7
	••••

Figure 10

配置完VLAN后,如果发现系统禁用了"本地连接"接口,则只要启用它,会看到网络连接中会出现一个新的子接口"本地连接2"。



在WireShark上查看抓取"本地连接"接口的报文。

Device	Description	p	Packets	Packets/s	
🔲 🛃 VMware Network Adapter VMnet8	VMware Virtual Ethemet Adapter	fe80::6577:a55b:94a6:1e90	0	0	Retails
🔲 🛃 VMware Network Adapter VMnet1	VMware Virtual Ethemet Adapter	fe80::e4b7:256a:821e:282a	0	0	Details
🔲 🛃 无线网络连接 2	Microsoft	fe80::94a0:f15:cdf:e82e	0	0	Details
 	Intel(R) 82579LM Gigabit Network Connection	none	369	9	Details
🔲 🔝 无线网络连接	Microsoft	fe80::84ef:df00:f482:847	3407	86	Details

Figure 12

可以看到已经可以抓到有VLAN TAG的报文了。

Filte	NT.			- Expressio	n Clear Apply Save
No.	Time	Source	Destination	Protocol	Length Info
	25 2.66639	100 198.19.1.2	198.19.1.1	IPv4	124 any 0-hop protocol (114)
	26 2.77718	800 198, 19, 1, 2	198, 19, 1, 1	IPv4	124 any 0-hop protocol (114)
	27 2.88829	500 198.19.1.2	198.19.1.1	IPW4	124 any 0-hop protocol (114)
	28 2.99946	600 198.19.1.2	198.19.1.1	IPWE	124 any 0-hop protocol (114)
	29 3.11090	000198.19.1.2	198.19.1.1	IPU4	124 any 0-hop protocol (114)
	30 3.22169	500 198, 19, 1, 2	198,19,1,1	1.014	124 any 0-hop protocol (114)
	31 3.33279	800 198.19.1.2	198.19.1.1	IPV4	124 any 0-hop protocol (114)
	32 3.44380	600198.19.1.2	198.19.1.1	IPVA	124 any 0-hop protocol (114)
	13 3.55496	100198.19.1.2	198,19,1.1	IPV4	124 any 0-hop protocol (114)
	34 3,66609	800198.19.1.2	198.19.1.1	IPV4	124 any 0-hop protocol (114)
4					. W
E F	rame 25: 12- thernet II, 02.10 Virtu 000 0 0000 (Type: IP ()	4 bytes on wire (Src: 00:00:00_00 al LAN, PRI: 0, Cl = Prior = CFI: 6 0001 0011 = ID: 1 0x08001	992 bits), 124 bytes :00:39 (00:00:00:00: FI: 0, ID: 19 ity: Best Effort (de Canonical (0) 9	captured (9 00:39), Dst: fault) (0)	192 bits) on interface 0 Broadcast (ff:ff:ff:ff:ff:ff;ff

Figure 13

由于此时的子接口都是有VLAN属性的,所以无法当成正常的网卡来用。如果想要在抓VLAN包的同时,还能够与网络正常通信,只要再新建一个末标记的VLAN就行。



Figure 14

这时,会生成一个对应的子接口"本地连接3",在这个接口上正确配置网络参数数,就可以正常通信了



示例

Wireshark抓到的带802.1Q的包象下图这样:

	6 0.455058	10.40.108.29	10.40.108.16	ICMP	Echo ((ping)	requ	est		
	7 0.456012	10.40.108.16	10.40.108.29	ICMP	Echo ((ping)	repl	V		
	8 0.509960	192.200.1.2	192.200.1.254	TCP	0 > 0	RST	Seq=	1 Win=C) Len=	
	9 0.554383	Microsof_28:f6:c9	Broadcast	ARP	Who ha	as 192	. 200.	112.177	? Te	
	10 0.595324	Zhongxin 19:1a:98	Broadcast	ARP	Who ha	as 192	.200.	112,129	? Te	
	11 0.610086	192.200.1.2	192.200.1.254	TCP	0 > 0	RST	Seq=	1 Win=C) Len=	
	12 0.709929	192.200.1.2	192.200.1.254	TCP	0 > 0	RST,	CWR	Seq=1	Win=0	
	13 0.809938	192.200.1.2	192.200.1.254	TCP	0 > 0	RST,	CWR	Seq=1	Win=0	
	14 0,909929	192,200,1,2	192,200,1,254	тср	0 > 0	TRST.	CWR	Seg=1	Win=0	
	15 1.004892	Zhongxin 19:1a:98	Broadcast	ARP	who ha	as 192	.200.	112,667	Tel	
	16 1.009697	Zhongxin 19:5f:dc	Broadcast	ARP	who ha	as 192	.200.	1.130?	Tell	
	17 1 009745	Zhonoxin 19:5f.dc	Broadcast	ARP	who ha	s 197	200	1 1317	Tell	~
	<								>	
										2
	■ Frame 9 (64 bytes on wir	e, 64 bytes captured)								
Ethernet II Src: Microsof 28:f6:c0 (00:02:ff:28:f6:c0) Det: Broadcast (ff:ff:ff:ff:ff:ff)										
			5), 55er 5roudeus.							
	⊞ 802.1Q V1rtual LAN, PRI:	0, CFI: 0, ID: 200								
	Address Resolution Proto	ocol (request)								
										_

Figure 16

PRI: 0 优先级 ID: 200 VLAN ID