

## Network 常識-802\_1Q 與 802\_1P 簡介(Issue 01)

這篇文章主要介紹了 802.1Q VLAN 協議在乙太網路交換集線器中的實行方式，以及 802.1p 協議的一些基本內容，在 IP Phone 中，這兩個協議是最重要也最常見的，除了 PHILIPS 的 Call@Net 話機型錄中有關 QoS 的部分也特別提到這兩種協議外，其他像 AVAYA、NORTEL、ALCATEL、CISCO 的規格中也都有提到此兩種協議，為此這別將這兩個協議做一個簡介，期望能對各位同事有所幫助。

### 一、802.1Q 協議

802.1Q 協議，即 Virtual Bridged Local Area Networks 協議，主要規定了 VLAN 的實行，下面我們首先講述一下有關 VLAN 的基本觀念。

Virtual LANs 目前發展很快，世界上主要的大網絡廠商在他們的 Switch 設備中都使用了 VLAN 協議，顧名思義，VLAN 就是虛擬區域網路，比如對於 HP2626Switch 來說，可以將它的 24 個 100M 乙太網路埠劃分為幾個組，比如協議組，ATM 組，測試組等，這樣，組內的各個用戶就像在同一個區域網路內(可能協議組的用戶位於很多的 Switch 上，而非一個 Switch)一樣，同時，不是本組的用戶也無法訪問本組的成員。

實際上，VLAN 成員的定義可以分為 4 種：

#### 根據網路埠劃分 VLAN

這種劃分 VLAN 的方法是根據乙太網路交換集線器的網路埠來劃分，比如 SWITCH 的 1~4 網路埠為 VLAN A，5~17 為 VLAN B，18~24 為 VLAN C，當然，這些屬於同一 VLAN 的網路埠可以不連續，如何配置，由管理員決定，如果有多個 Switch 的話，例如，可以指定 Switch 1 的 1~6 網路埠和 Switch 2 的 1~4 網路埠為同一 VLAN，即同一 VLAN 可以跨越數個乙太網路交換集線器，根據網路埠劃分是目前定義 VLAN 的最常用的方法，IEEE 802.1Q 協議規定的就是如何根據 Switch 的網路埠來劃分 VLAN。這種劃分的方法的優點是定義 VLAN 成員時非常簡單，只要將所有的網路埠都指定義一下就可以了。它的缺點是如果 VLAN A 的用戶離開了原來的網路埠，到了一個新的 Switch 的某個網路埠，那麼就必須重新定義。

#### 根據 MAC 地址劃分 VLAN

這種劃分 VLAN 的方法是根據每個主機 MAC 地址來劃分，即對每個 MAC 地址的主機都配置他屬於哪個組。這種劃分 VLAN 的方法的最大優點就是當用戶物理位置移動時，即從一個 Switch 換到其他的 Switch 時，VLAN 不用重新配置，

所以，可以認為這種根據 MAC 地址的劃分方法是基於用戶的 VLAN，這種方法的缺點是初始化時，所有的用戶都必須進行配置，如果有幾百個甚至上千個用戶的話，配置是非常累的。而且這種劃分的方法也導致了 Switch 執行效率的降低，因為在每一個 Switch 的網路埠都可能存在很多個 VLAN 組的成員，這樣就無法限制廣播包了。另外，對於使用筆記型電腦的用戶來說，他們的網卡可能經常更換，這樣，VLAN 就必須不停的配置。

#### 根據網路層劃分 VLAN

這種劃分 VLAN 的方法是根據每個主機的網路層地址或協議類型(如果支持多協議)劃分的，雖然這種劃分方法可能是根據網路地址，比如 IP 地址，但它不是路由，不要與網路層的路由混淆。它雖然查看每個封包的 IP 地址，但由於不是路由，所以，沒有 RIP，OSPF 等路由協議，而是根據生成樹算法進行橋交換

這種方法的優點是用戶的物理位置改變了，不需要重新配置他所屬的 VLAN，而且可以根據協議類型來劃分 VLAN，這對網路管理者來說很重要，還有，這種方法不需要附加的旗標來識別 VLAN，這樣可以減少網路的通信量。

這種方法的缺點是效率，因為檢查每一個封包的網路層地址是很費時的(相對於前面兩種方法)，一般的 Switch 晶片都可以自動檢查網路上封包的乙太網路旗標，但要讓晶片能檢查 IP 旗標，需要更高的技術，同時也更費時。當然，這也跟各個廠商的實作方法有關。

#### IP 多址廣播作為 VLAN

IP 多址廣播實際上也是一種 VLAN 的定義，即認為一個多址廣播組就是一個 VLAN，這種劃分的方法將 VLAN 擴大到了廣域網，因此這種方法具有更大的靈活性，而且也很容易通過路由器進行擴展，當然這種方法不適合區域網路，主要是效率不高，對於區域網路的多址廣播，有二層多址廣播協議 GMRP。

通過上面可以看出，各種不同的 VLAN 定義方法有各自的優缺點，所以，很多廠商的 Switch 都實行了不只一種方法，這樣，網路管理者可以根據自己的實際需要進行選擇，另外，許多廠商在實行 VLAN 的時候，考慮到 VLAN 配置的複雜性，還提供了一定程度的自動配置和方便的網路管理工具。

以前，各個廠商都聲稱他們的 Switch 實行了 VLAN，但各個廠商實行的方法都不相同，所以彼此是無法互連，這樣，用戶一旦買了某個廠商的 Switch，就沒法買其他廠商的了。而現在，VLAN 的標準是 IEEE 提出的 802.1Q 協議，只有支持相同的開放標準才能保證網路的互連互通，以及保護網路設備投資。

下面講述一下 VLAN 的優點:

減少移動和改變的代價，即所說的動態管理網路，也就是當一個用戶從一個位置移動到另一個位置是，他的網路屬性不需要重新配置，而是動態的完成，這種動態管理網路給網路管理者和使用者都帶來了極大的好處，一個用戶，無論他到哪裡，他都能不做任何修改地接入網路，這種前景是非常美好的。當然，並不是

所有的 VLAN 定義方法都能做到這一點。

虛擬工作組，VLAN 的最具雄心的目標就是建立虛擬工作組模型，例如，在校園網中，同一個系的就好像在同一個 LAN 上一樣，很容易的互相訪問，交流信息，同時，所有的廣播包也都限制在該虛擬 LAN 上，而不影響其他 VLAN 的人，一個人如果從一個辦公地點換到另外一個地點，而他仍然在該系，那麼，他的配置無須改變，同時，如果一個人雖然辦公地點沒有變，但他換了一個系，那麼，只需網絡管理者那配置一下就行了。這個功能的目標就是建立一個動態的組織環境，當然，這只是一個遠大的目標，要實行它，還需要一些其他包括管理等方面的支持。

限制廣播包，按照 802.1D 透明網橋的算法，如果一個封包找不到路由，那麼 Switch 就會將該封包向所有的其他網路埠發送，這就是橋的廣播方式的轉發，這樣的結果，毫無疑問極大的浪費了頻寬，如果配置了 VLAN，那麼，當一個封包沒有路由時，Switch 只會將此封包發送到所有屬於該 VLAN 的其他網路埠，而不是所有的 Switch 的網路埠，這樣，就將封包限制到了一個 VLAN 內。在一定程度上可以節省頻寬。

安全性，由於配置了 VLAN 後，一個 VLAN 的封包不會發送到另一個 VLAN，這樣，其他 VLAN 的用戶的網絡上是收不到任何該 VLAN 的封包，從而就確保了該 VLAN 的信息不會被其他 VLAN 的人竊聽，從而實行了訊息的保密。

理論上，VLAN 可以擴展到 WAN 上，但是，這是不明智的做法，因為 VLAN 允許廣播包發送出去，而且它沒有很好的路由算法，經常是以廣播的形式轉發封包，這樣，毫無疑問，極大地浪費了 WAN 的寶貴的頻寬，所以說，將基於網路埠的，MAC 地址和網絡地址的 VLAN 擴展到 WAN，是不合理的，而基於多播的 VLAN 概念則可以靈活有效的擴展到 WAN。一般的乙太網路交換集線器實行的都是基於網路埠的 VLAN，個別的會實行基於 MAC 地址和網絡層地址的 VLAN，而路由器中可以通過 IGMP 多播協議實行所謂的多址廣播形式的 VLAN。

802.1Q 協議定義了基於網路埠的 VLAN 模型，這是使用得最多的一種方式。下面我們重點講述一下 Switch 晶片是如何實行 VLAN 的，如果想瞭解更細節的內容，可以參考 802.1Q 協議，由於協議文本講的非常抽象，所以，我們以 TI 公司的交換晶片為例來講述，更便於理解。例子中的 TNETX4090 提供了 8 個 100M 乙太網路埠和 1 個 1G 乙太網路埠。

如圖 1 所示，每一個支持 802.1Q 協議的主機，在發送封包時，都在原來的乙太網路旗標中的源地址後增加了一個 4 字節的 802.1Q 旗標，之後接原來乙太網的長度或類型域，關於乙太網路旗標的封裝格式，參見乙太網方面的培訓教材。

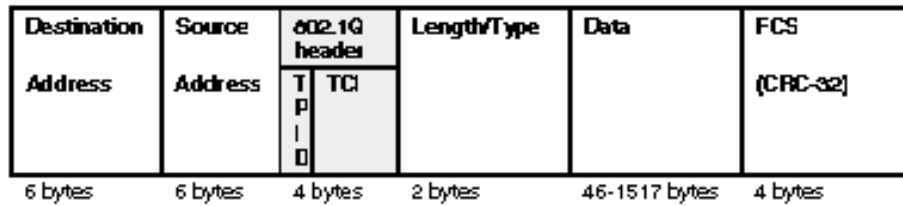


圖 1 帶有 802.1Q 標籤頭的乙太網封包

這 4 個字節的 802.1Q 標籤頭包含了 2 個字節的標籤協議標識 (TPID--Tag Protocol Identifier, 它的值是 8100), 和兩個字節的標籤控制訊息 (TCI--Tag Control Information), TPID 是 IEEE 定義的新的類型, 表明這是一個加了 802.1Q 標籤的本文, 圖 2 顯示了 802.1Q 標籤頭的詳細內容。

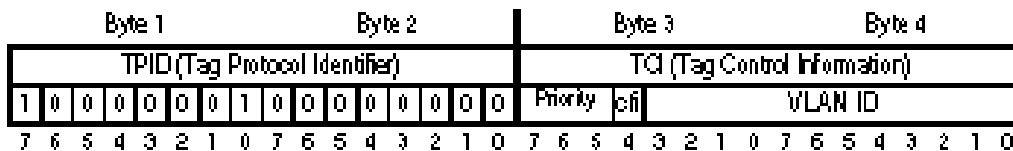


圖 2 802.1Q 標籤頭

該標籤頭中的訊息解釋如下：

LAN Identified (VLAN ID): 這是一個 12 位的域, 指明 VLAN 的 ID, 一共 4096 個, 每個支持 802.1Q 協議的主機發送出來的封包都會包含這個域, 以指明自己屬於哪一個 VLAN, 目前 TNETX 3270 只支持 32 個 VLAN。

Canonical Format Indicator (cfi): 這一位主要用於總線型的乙太網與 FDDI、令牌環網交換數據時的棧格式, TNETX 3270 忽略此位。

Priority: 這 3 位指明封包的優先級。一共有 8 種優先級, 主要用於當 Switch 阻塞時, 優先發送哪個封包。TNETX 3270 和 TNETX 4090 只支持一種優先級, 所以這一位也沒有用,

不難看出, 802.1Q 標籤頭的 4 個字節是新增加的, 目前我們使用的計算機並不支持 802.1Q, 即我們計算機發送出去的封包的乙太網路標頭還不包含這 4 個字節, 同時也無法識別這 4 個字節, 將來會有軟體和硬體支持 802.1Q 協議的。對於 Switch 來說, 如果它所連接的乙太網段的所有主機都能識別和發送這種帶 802.1Q 標籤頭的封包, 那麼我們把這種網路埠稱為 Tag Aware 網路埠; 相反, 如果該 Switch 網路埠說連接的乙太網段有只要有一台主機不支持這種乙太網路旗標, 那麼 Switch 的這個網路埠我們稱為 Access 網路埠, 從目前的情況可以看出, 所有的 Switch 的網路埠都屬於後一種。

那麼, 在現在的情況下, Switch 是如何支持 VLAN 的呢? 是這樣的, 比如

Switch 的 1~4 網路埠屬於同一個 VLAN，那麼當 1 網路埠進來一個封包是，Switch 看到該封包沒有 802.1Q 標籤頭，那麼，它會根據 1 號網路埠所屬的 VLAN 組，自動給該封包添加一個該 VLAN 的標籤頭，然後再將封包交給資料庫查詢模塊，資料庫查詢模塊會根據封包的目的地址和所屬的 VLAN 進行路由，之後交給轉發模塊，轉發模塊看到這是一個包含標籤頭的封包，而實際上發送的網路埠所連的乙太網段的計算機不能識別這種封包，所以，它會再將封包進來是 Switch 給添加的標籤頭再去掉。如果計算機支持這種標籤頭，那麼就不需要 Switch 添加或刪除標籤頭了，至於到底是添加還是刪除要看 Switch 所連的乙太網段的主機是否識別這種封包，即該 Switch 的網路埠是哪種類型的網路埠。當然，對於兩個 Switch 互連的網路埠一般都是 Tag Aware 網路埠，這樣，Switch 和 Switch 之間交換封包時是無須去掉標籤頭的。

一般 Switch 的連接方式如圖 3 所示

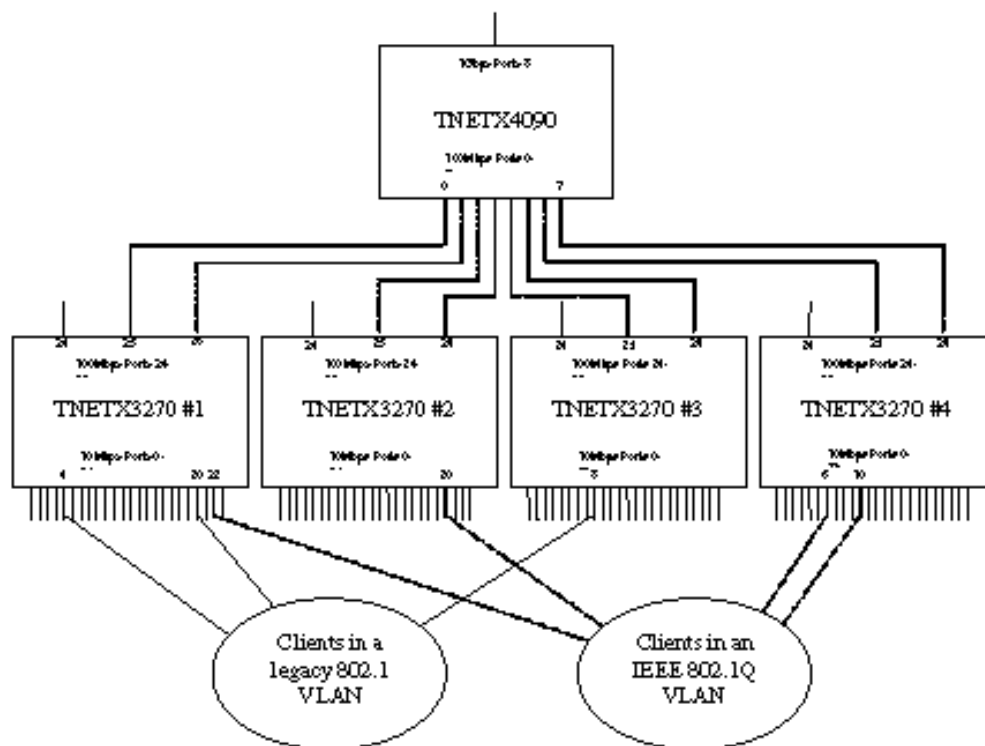


圖 3 多個 Switch 的組網圖

圖中虛線是 Tag Aware 網路埠，實線是 Access 網路埠。

乙太網路交換集線器處理封包的流程如圖 4 所示。

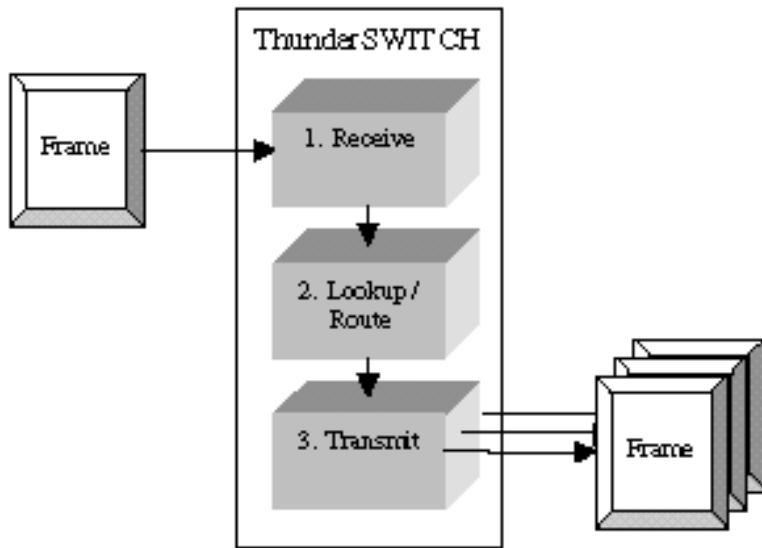


圖 4 封包處理流程

處理流程包括 3 個步驟：

接收過程：該過程負責接收封包，封包可以是帶標籤頭的，也可以不帶標籤頭，如果不帶，Switch 會知道根據該網路埠所屬的 VLAN 添加上相應的標籤頭。

查找/路由過程：該過程根據封包的目的 MAC 地址、VLAN 標識已經資料庫中註冊的訊息決定把封包發送到哪個網路埠。

發送過程：將封包發送到乙太網段上，如果該網段的主機不能識別 802.1Q 標籤頭，那麼就將該標籤頭去掉，如果是與其他 Switch 互連的網路埠，一般不去掉。

具體的接收、查詢和發送過程可以參考 TNETX 3270 的相關資料，下面是一個無標籤頭的封包的接收到發送的過程。

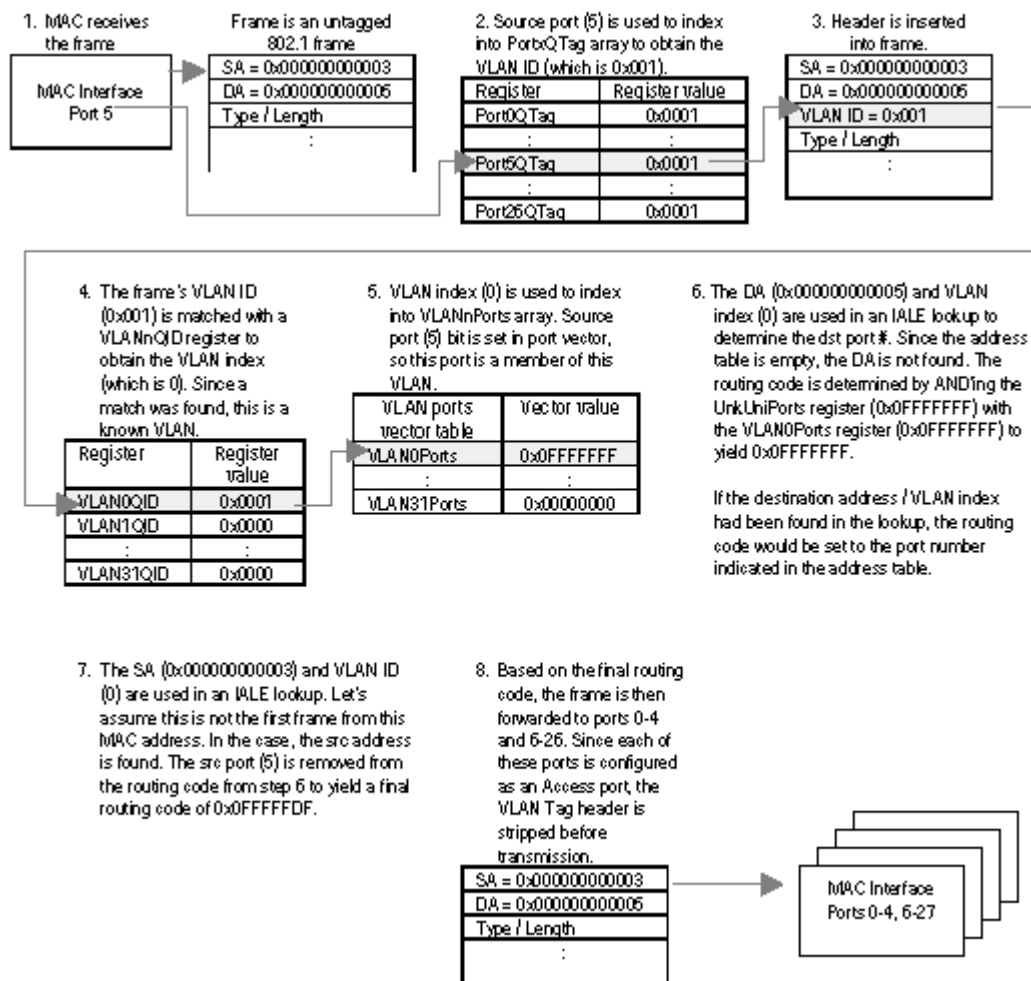
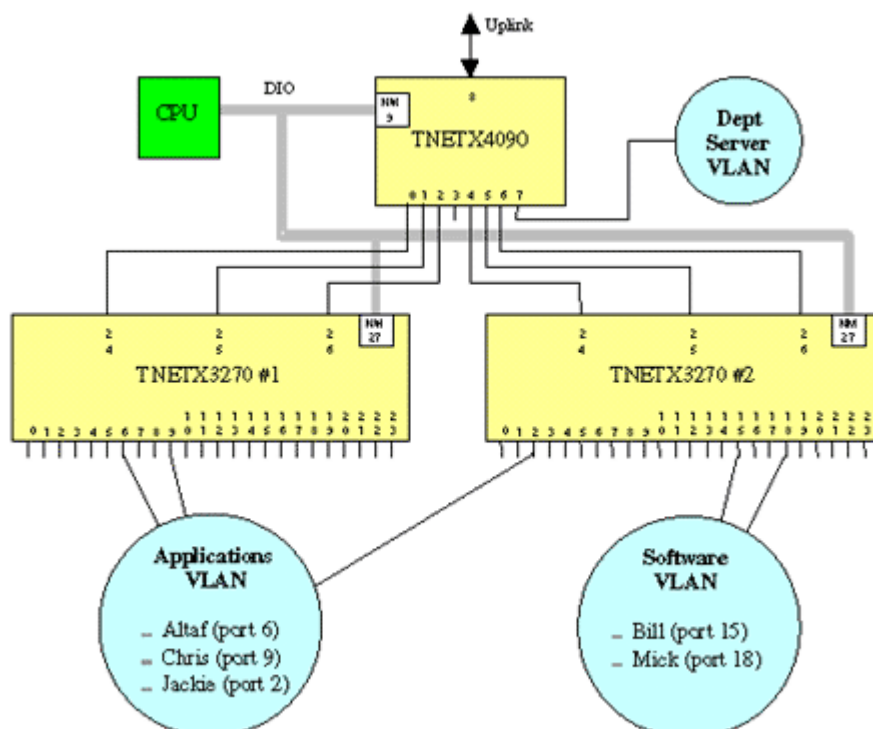


圖 5 一個無標籤頭的封包的處理流程

其中具體的路由過程參考 TNETX 3270 資料。圖 6 是另外的一個例子。



## 圖 6 一個互連的例子

以圖 6 為例，假如 Chris 發送一個封包給 Jackie，那麼，處理的過程如下：

Chris 發送一個封包給 Jackie。

封包到達 Switch1 的網路埠 9，這是一個無標籤頭的包，所以 Switch1 給該封包添加一個 VLAN ID。

根據目的 MAC 地址和 VLAN ID，查詢資料庫，知道該封包需要發送到 24（或 25、26 號網路埠，這 3 個網路埠被捆綁到一起，對上層來說，這 3 個網路埠就好像一個網路埠，實際上 Switch 會根據 3 個網路埠的流量來決定是從哪個網路埠往外發送）。如果不知道，則該封包還會被發送到網路埠 6，當然，在發送到網路埠 6 的乙太網段時，會先將標籤頭去掉，Altaf 收到後會丟棄這個封包，因為目的地址不是它。由於網路埠 24 是 Tag Aware 網路埠，所以，發送到 24 好網路埠的封包的標籤頭不去掉。

TNETX 4090Switch 收到這個封包後，根據 VLANID 和目的 MAC 地址在它的資料庫中查找路由，最後，它知道該封包應該發送到網路埠 4（5 或 6），標籤頭仍然不去掉。

Switch2 收到後，根據 VLAN ID 和目的 MAC 地址，在它的資料庫中查找路由，知道該封包需要發送到網路埠 2。於是將該封包發送出去。注意，發送出去的封包需要去掉標籤頭。

以上我們討論了 VLAN 收發封包的過程，它的具體實行已經由乙太網路交換集線器的交換晶片實行了，有興趣者可參考交換晶片的技術資料。

## 二、802.1P 協議

802.1p 協議定義了優先級的概念，對於那些實時性要求很高的封包，主機在發送時就在前面提到 MAC 旗標增加的 3 位優先級中指明該封包優先級高，這樣，當乙太網路交換集線器數據流量比較多時，它就會考慮優先轉發這些優先級高的封包。

目前部分乙太網路交換集線器所採用的交換晶片只支持 2 種優先級，也有一些能支持 4 個優先級。

802.1p 協議還定義了 GARP--Generic Attribute Registration Protocol。這裡的 Attribute 是指多址廣播 MAC 地址、網路埠過濾模式和 VLAN 等屬性，GARP 協議實際上可以定義很多 Switch 應該具有的特性，目前，它定義了 GMRP--GARP Multicast Registration Protocol 和 GVRP--GARP VLAN Registration Protocol 兩個協議，以後會根據網絡發展的需要定義其他的特性。GARP 定義了乙太網路交換



集線器之間交換這些特性訊息的方法，如何發送封包，接收的封包如何處理等等。

GMRP 協議是一個動態二層多址廣播註冊協議，它的很多方面跟 IGMP（三層多址廣播協議）類似，對於 IP 地址來說，D 類 IP 地址是多址廣播地址，實際上，對於每一個 IP 多址廣播地址，都有一個多址廣播 MAC 地址跟它對應，802.1p 協議就是根據多址廣播 MAC 地址來在乙太網路交換集線器上註冊和取消多址廣播成員身份的，而 IGMP 是根據多址廣播 IP 來管理的。當然，如果乙太網路交換集線器沒有實行 GMRP 協議，那麼就只能通過靜態配置來實行多址廣播了。

關於為什麼需要二層多址廣播協議？我們再詳細討論一下。與協議 IGMP 一樣，如果我們在自己的區域網路內成立一個多址廣播組，可能我們的區域網路包含了很多 Switch，如果這些 Switch 沒有實行二層多址廣播協議的話，那麼，某個組員給其他組員發送封包時，Switch 就會將該封包向所有的網路埠廣播，因為 Switch 不知道哪個網路埠有人加入了該多址廣播組，唯一的解決辦法就是管理員配置 Switch，這樣，才能將這種廣播轉發封包的發送方式限制住，而多址廣播本身是動態的，所以，通過這種靠管理員的配置來實行多址廣播的方式是不現實的。因此，就需要有一個二層多址廣播協議來動態管理組員。這就是為什麼需要二層多址廣播協議的原因，目前，許多高檔的 Switch 都把實行 802.1p 和 802.1Q 協議作為一個主要的性能指標。

GVRP 是 VLAN 協議，由於它與 GMRP 都是基於 GARP 之上的，所以它們之間的關係很緊密，它們都要對 Switch 的資料庫進行操作，這個協議的具體定義在 802.1Q 中。