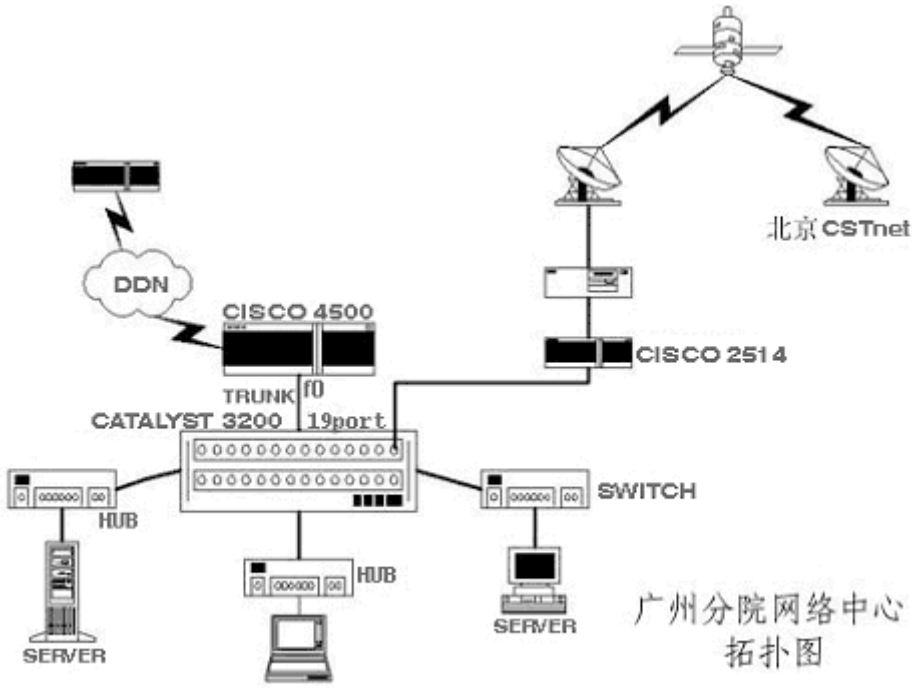
# VLAN 在網路管理中的應用

一、前言

廣州分院電腦網是中科院"百所聯網"二期工程的一部分，網路中心設備於 1998 年初安裝運行，隨著用戶接入和網路應用的開展，在運行、管理中碰到不少問題。雖然已逐漸完善網路中心設備及伺服器的配置和建立了相應的管理制度，一些問題也得以解決和控制，但對防止一些不守法用戶經常採用未授權 IP 上網問題，仍不能得到解決，網管人員爲此花費不少精力。當時曾想在邊界路由器上做 IP-MAC 綁定，但由於 CSTNET 從網路整體安全考慮，邊界路由器管理權由院網路中心控制，對二級節點的廣州分院網來說,如把 IP-MAC 綁定在邊界路由器上，將不利於網路監控及管理,對可能發生的一些事件無法做出快速反應，因此實際是不可行的。解決問題只能在廣州分院網路中心設備上入手。

二、網路結構配置及解決方案




由於 4500 只配高速口 f0，其餘爲非同步接口，使得邊界路由 Cisco 2514 只能接入 Catalyst3200，和所有局域網形成"平構式"結構，對防止 IP 盜用問題造成先天不足。

從分析 Catalyst 3200 虛網功能上可見，除了虛網功能本身的優點外，Catalyst 3200 交換機與 Cisco 4500 路由器的高速口支持 ISL(InterSwitch Link)及 VTP（VLAN TRUNK PROTOCOL），這對強化網路管理提供有力的技術保證。通過對 Catalyst 3200 的埠進行虛網設置，再跟據網路用戶所在的物理位置、工作性質、網路通信負載儘量均衡原則，把所有網路用戶納入不同虛擬子網,各子網經 Catalyst 3200 與 Cisco 4500 的高速口連接--路由，再把 IP-MAC 綁定在 Cisco 4500 上就可能達到預期目的。

三、虛擬子網 VLAN 的配置

1).Catalyst 3200 交換機上 VLAN 及 VTP 的配置 經超級終端進入 Catalyst 3200 控台

a).設置 VLAN 管理域 進入"SET VTP AND…· ",選"VTP ADMINISTRATION CONFIGURATION" 設置 VALN 管理功能變數名稱"GIETNET"；VTP 方式爲"SERVER"。

b).設置 VLAN 及 TRUNK： 將所有子網的交換機、HUB 上連至 Catalyst 3200 的 10MB 或 100MB 口，並按上述原則分配 VLAN，將這些埠進行虛網劃分如下：

| 子网号 | 子网IP及路由口 | 3200端口 | 子网名 |
|---|---|---|---|
| 2 | 192.168.111.0<br>192.168.111.1 | 1, 17, 15 | VLAN1 |
| 3 | 192.168.111.64<br>192.168.111.65 | 6, 7, 8 | VLAN2 |
| 4 | 192.168.111.128<br>192.168.111.129 | 9, 11, 3 | VLAN3 |
| Catalyst 3200的19口(100MB)被指定为TRUNK口与Cisco 4500的f0连接 | | | |

本項設置從控制臺的 CONFIGURATION 選定"LOCAL VLAN PROT CONFIGURATION"，進行 VLAN 及 TRUNK 口的指定，並把所有的 3 個 VLAN 填入 TRUNK 口的配置單中，最後顯示如下

| Prot | Mode | VLAN NAME |
|---|---|---|
| 1 | Static | VLAN1 |
| 2 | Static | Default (未用) |
| 3 | Static | VLAN3 |
| • | • | • |
| • | • | • |
| 7 | Static | VLAN2 |
| 8 | Static | VLAN2 |
| 9 | Static | VLAN3 |
| 10 | Static | Default (未用) |
| 11 | Static | VLAN3 |
| • | • | • |
| • | • | • |
| 19 | Trunk | Default VLAN1 VLAN2 VLAN3 |

2).Cisco 4500 路由器的設置

把 Cisco 4500 的 f0 口按子網數"分割"成相應的"子口"， 根據其設置的 ISL（InterSwitch Link）號,與相應子網進行邏輯連接。在本例中，f0 被分割爲 f0.1、f0.2、f0.3 與 VLAN1、VLAN2、VLAN3 連接，其配置命令如下：

router#config t

router(config)#int f0.1

router(config-subif)#Description VLAN1_GIET

router(config-subif)#ip address 192.168.111.1 255.255.255.192

router(config-subif)#encapsulation isl 2

. .

router(config)#int f0.2

router(config-subif)#Description VLAN2_gzbnic

router(config-subif)#ip addess 192.168.111.65 255.255.255.192

router(config-subif)#encapsulation isl 3

. .

Ctl Z

wr

設置完畢,再請北京網路中心把邊界路由器中有關子網路由項全部指向 Cisco 4500,用戶的閘道按其子網路由器地址設定。

3).在 Cisco 4500 路由器上建立 ARP 表

爲強化網路管理防止 IP 盜用，在 Cisco 4500 路由器上建立 ARP 表，將所有子網的 IP 與相應的網卡 MAC 位址進行綁定，對於未用的 IP 也進行綁定，如：

ARP 192.168.111.130 0800.3c5d.419f ARPA (已分配的 IP 有網卡位址)

.

ARP 192.168.111.169 0000.0000.0000 ARPA (未分配的 IP 無網卡位址)

當註冊網路用戶需更換網卡時，需得到網管人員的確認、同意，對企圖非法盜用者將無法進行（參見下述）；另外可按具體情況設置訪問控制列表等安全管理措施。

四、系統特點

經過虛網設置和 IP-MAC 綁定結合, 網路系統的特點：

1).發揮 VLAN 優勢

合理分配網路資源，均衡網路負載，有效降低網上廣播資訊,方便對用戶的分組管理。

2).增強網路安全

由於網路各子網相互隔離，網路通訊限制在子網內；子網間的交通或出境的通訊全部通過其相應的路由埠,加強了 Cisco 4500 對全網的控制能力,並由 4500 上的 ARP 表進行用戶 IP 的合法性核查。

3).強化網路管理、合理記費

如 2)所述，由於虛網的配置加上 Cisco 4500 的 IP-MAC 的匹配檢查，使得 IP 盜用比一般的位址綁定更爲困難，理由是這種配置結構下，即使想盜用，其通訊也只限於本子網內(活動範圍大大減少,被當場抓獲可能性加大) ；Cisco 4500 上的 IP-MAC 的匹配核查，使得有計費的 IP 盜用無法進行(盜用變得無意義)，從而達到合理記費和有效提高網路管理、控制能力。

本工作於去年完成，運行穩定，滿足要求。華教公司的田戈先生對方案提供寶貴意見，在此表示感謝。

名詞解釋：

1).VLAN TRUNK PROTOCOL（VTP）：用 VTP 設置和管理整個域內的 VLAN，在管理域內 VTP 自動發佈配置資訊,其範圍包括所有 TRUNK 連接,如交換互連( ISL )、802.10 和 ATMLAN（LANE）當交換機加電時,它會週期性地送出 VTP 配置請求,直至接到近鄰的配置( summary )廣播資訊，從而進行結構配置必要的更新。 交換機的 VTP 配置有三種模式：伺服器、客戶和透明模式。

2).ISLTRUNK ISL 中繼不同的 VLAN 多路包,包頭帶有"ISL VLAN 數"標誌( VTP VLAN ID )。