e-zone Vol 534
Nov 6, 2008

text - photo/陳振豐 edit/莫西城 art/Bo

本地不少大專院校，近年擴展校內網絡設備，以應付網絡頻寬需求日增的趨勢。事實上，由於院校內的人流相對較多，故此除了對寬頻速度有要求外，院校近年開始着重終端登入的資訊保安。為確保登入校內網絡的每台終端電腦均符合校方要求，近期部署的邊緣網絡交換機（edge switch）皆順應市場要求，新增終端保安功能。香港教育學院便是其中一個例子。

香港教育學院在這兩年間擴展網絡基建，除了增加寬頻外，亦為了提升網絡端口保安效能的緣故。

邊緣伺服器 教院強化端口保安

香港教育學院資訊科技服務處處長鄭弼亮表示，部署高效的網絡環境，可配合院校的新教學需求。學生可在校內透過網絡，遠程存取各項教學資訊，並可登入互聯網瀏覽各項資訊，故該校早在 10 年前已部署網絡設備基建，並採用不同網絡商的路由器及交換機。隨着頻寬要求日益提高，同時為配合未來的統一通訊策略，加上優化網絡保安的大前提下，教院於 2006 年部署 78 台華三通訊（H3C）的邊緣網絡交換機，擴展網絡基建效能。

優化終端保安

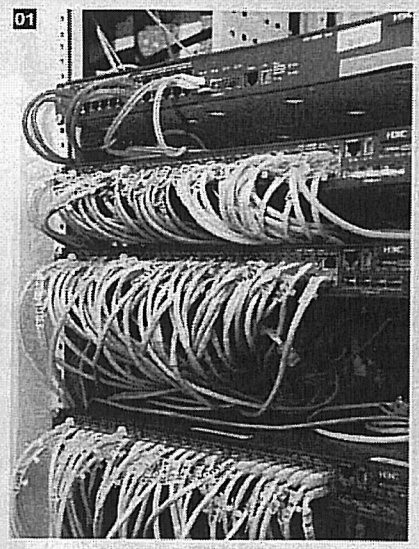
鄭弼亮強調，院校讓學生上網的原意，主要讓學生能涉獵更多資訊，瀏覽過程要以自由為前提，這一點跟企業禁止員工瀏覽跟業務無關的網站，出發點可謂大相逕庭。但自由歸自由，院校仍要確實做妥網絡保安管理，故此在今年部署新的邊緣交換機的要求上，便十分重視端口網絡保安效能，確保資訊人員能立即檢視哪部電腦出現問題，並立即修正。

傳統來說，要實踐終端的資訊保安，多數以防火牆網關作為對終端偵察的方式。不過，後者相對只專注於檢測網絡交通狀況，遇上不尋常的網絡交通，雖可作出攔截，卻難以檢視從哪一部終端電腦引起。另外，院校可事先登錄每部終端電腦內獨有的 MAC 位址，之後才容許學生在校內上網；惟遇上學生更換電腦上網，往往要重新登錄電腦，過程繁瑣。事實上，院校上網人數眾多，這兩種傳統的網絡保安方式，難以實踐有效率的保安管理。

有見及此，該院校近年引入的終端邊緣交換機，必須能夠提供較靈活的端口的網絡保安管理。H3C 的邊緣交換器 S3600 系列，具備位址解析協定（Address Resolution Protocol；ARP）偵察功能，以阻隔 ARP 偽裝（ARP Spoofing）及中間人的攻擊。

鄭弼亮表示，透過新增 H3C 邊緣交換器，將進一步擴展統一通訊網絡，當中不僅針對話音通訊，同時整合電郵等通訊工具，加強師生之間的連通訊。

01



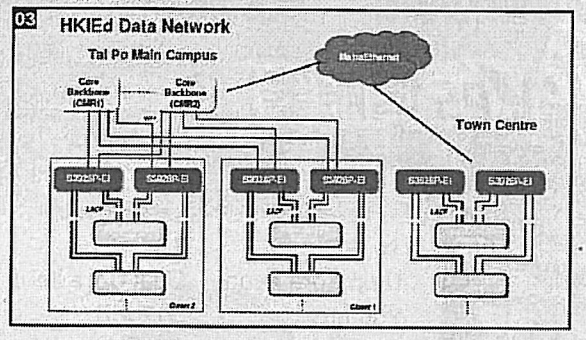
02

01 擴建邊緣交換器數目後，教院的大埔校舍可應付約 4,000 個終端端口保安。

02 教院方面表示，採用 H3C 邊緣交換機，主要因為該設備兼備 ARP 偵察功能及 802.1x 保安的雙重認證功能，減低非授權用戶登入校內網絡的風險。

03 教育的網絡基建架構圖，其中部署 S3600 系列的邊緣交換機，是該校新部署的項目。

03



MIND MAP

教育網絡基建布局

香港教育學院主要有兩間校舍，分別位於大埔及大角咀。該院自 1998 開始建立網絡基建，並自 2006 年開始全面為兩間院校升級。目前，該院校的大埔校舍共有 39 組配綫櫃（wiring closet），當中建立約 78 台的 H3C 的 S3928-EI 邊緣交換機，透過光纖連接到 2 間中央機房（各置 2 台 S7506-E 核心交換機），之間的連綫速度為 1Gb/s。

到了 2007 年，大埔院校繼續更新網絡設備，一共安裝了 120 台 S3600-52P-SI 及 S3600-52P-PWR 邊緣交換機，作為管理全校約 4,000 個端口連接埠的數據網絡基建。至於大角咀校舍，則設 2 台配綫櫃，當中以 2 台 S3928-EI 交換機作為骨幹網絡。兩家校舍今年更進一步把傳統的電話系統 TDM PABX 升級為 IP PABX 系統，進一步建立統一通訊網絡。

杜絕不明登入

所謂 ARP 偵察功能，是指在交換機內置動態主機設定協定窺探（DHCP Snoofing）功能。學生利用電腦在校內連綫上網時，校內的 DHCP 伺服器會記錄並識別他們的 MAC 位址，然後會分發 IP 位址給該部電腦；學生日後上網時，電腦發出的 ARP 封包會被交換機識別，交換機內存的 DHCP 表單，會窺探出該部電腦的 MAC 位址記錄，是否跟該個 IP 位址是一致，無問題的話便可順利連綫上網。

即使學生換了新的電腦，校方亦會再另行分發新的 IP 位址給他使用，務求交換機內所識別的 ARP 封包，必定屬於該名用戶；倘若其他人的電腦透過該組 IP 位址在校內連綫上網，交換機便會偵察出該部電腦的 MAC 位址跟原本的不同，便會封鎖該部電腦上網，杜絕登入連綫，防止黑客阻斷網絡服務，甚至盜取校內各項保密資訊。

另外，該系列的交換機支援 802.1x 保安認證，以輸入用戶名稱及密碼的認證方式，作為登入校內內聯網的憑證，配合 ARP 偵察功能，實踐雙重端口認證，確保登入者為授權的用戶。

伸延統一通訊

教院部署新的邊緣伺服器，除了提高端口保安外，亦作為該校擴展統一通訊網絡的主要設備之一。鄭弼亮表示，該校為提升教學質素，例如學生在海外實習期間，都能夠在遠程環境跟教師作實時通訊，於是自今年起進一步把大埔及大角咀兩間院校的 TDM PABX 電話，轉為 IP PABX 系統，透過 IP 電話或配置在電腦上的《Softphone》軟件等統一通訊設備，讓雙方通話，並透過協作平台分享教學資訊。

他表示，為提高通訊網絡流量，教院目前所建立的 VoIP 網絡中，除了 VoIP 網關採用北電網絡（Nortel Networks）的設備外，各層級的網絡設備均採用 H3C，包括兩組 S7506 E 交換機作骨幹網絡，以及用作連接校內各部 IP 電話的 S3600-28P-SI 邊緣伺服器。鄭弼亮補充，該設備能夠提供 QoS 及冗餘功能，確保話音質素，並減低話音中斷機會。