SỐ 4 • THÁNG 3–4/2013

TẦM NHÌN MẠNG

NETWORKS VISION

Bản tin của Công ty Nhân Sinh Phúc

BYOD
ẢNH HƯỞNG VÀ THÁCH THỨC

Trang 6

Lựa chọn tủ rack cho trung tâm dữ liệu

Trang 12

Tích hợp PoE vào hệ thống mạng

Trang 15

NSP® NETWORKS

SMARTER

DATA CENTER INFRASTRUCTURE

datacenteragility.com

TIẾT KIỆM THỜI GIAN, KHÔNG GIAN & NĂNG LƯỢNG với MRJ21 XG

PRE-TERMINATED, PLUG & PLAY 10GBE COPPER SYSTEM

Tiết kiệm thời gian: Các loại dây nhảy bấm sẵn và hộp cát-sét dạng mô-đun tiết kiệm thời gian lắp đặt và đảm bảo tính sẵn sàng cho những ứng dụng ảo hóa và đám mây.

Tiết kiệm không gian: Tiết kiệm không gian bên trong và ngoài tủ rack. Chỉ một sợi cáp mỏng cho mỗi đầu nối MRJ21 16 đôi.

Tiết kiệm năng lượng: Tiết kiệm không gian bên trong rack đồng nghĩa với việc các luồng không khí không bị cản trở. Tiết kiệm chi phí và nâng cao hiệu quả của giải pháp làm mát.

AMP NETCONNECT

ampnetconnect.eu/MRJ21_X G

EVERY CONNECTION COUNTS

TE connectivity

Kỷ niệm 14 năm thành lập công ty NSP

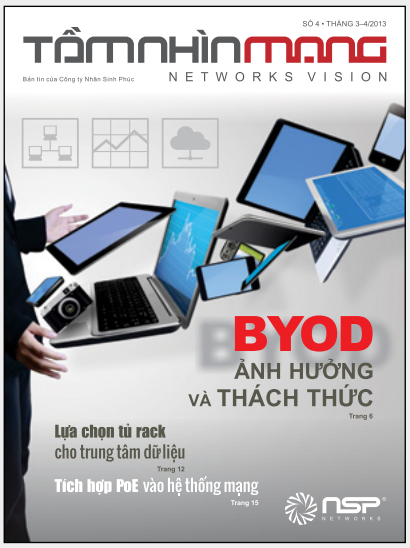
Bản tin *Tầm nhìn Mạng* số 4 (phát hành tháng 3/2013) bạn đang cầm trên tay đánh dấu 14 năm hình thành và phát triển của công ty TNHH TM–DV Tin học Nhân Sinh Phúc (gọi tắt là NSP). Chặng đường hơn một thập niên chưa hẳn là dài đối với lịch sử một công ty, tuy nhiên cũng đủ để NSP chứng tỏ quyết tâm của mình trong việc thực hiện sứ mệnh đã tuyên bố: làm cầu nối giúp khách hàng liên tục cập nhật, nắm bắt các tiêu chuẩn và công nghệ mới trên thế giới, thông qua việc tiếp cận và phổ biến kiến thức, cũng như cung cấp các sản phẩm, giải pháp ứng dụng những công nghệ tiên tiến. Nhân dịp này, bản tin *Tầm nhìn Mạng* cũng được tăng thêm bốn trang nhằm chuyển tải tốt hơn thông tin đến bạn đọc.

Bài viết chủ đề kỳ này liên quan đến chính sách BYOD–chấp nhận thiết bị di động cá nhân trong doanh nghiệp hoặc trong môi trường giáo dục. Chuyện tưởng chừng như đơn giản và hợp lý, như cho phép nhân viên sử dụng các thiết bị cá nhân như máy tính xách tay, máy tính bảng... phục vụ cho công việc, nhằm tăng năng suất và giảm chi phí đầu tư, lại trở thành thách thức cho các nhà quản lý CNTT, khi xét đến những nguy cơ có thể phát sinh từ các thiết bị này.

Không như các nước có ngành CNTT phát triển, ở Việt Nam, phản ứng của các nhà quản lý trước tình trạng nhân viên sử dụng thiết bị di động cá nhân trong tổ chức thường xảy ra theo hai chiều hướng khác nhau. Một số nhà quản lý ý thức được áp lực về băng thông lên cơ sở hạ tầng mạng, cũng như khả năng bị tấn công qua lỗ hổng bảo mật của thiết bị cá nhân, nhưng lại thiếu giải pháp ngăn ngừa dẫn đến việc cấm tiệt nhân viên sử dụng. Tuy nhiên, phổ biến hơn vẫn là việc các nhà quản lý cho nhân viên thoải mái sử dụng thiết bị cá nhân mà không quan tâm đến mối nguy tiềm tàng theo kiểu "điếc không sợ súng", hoặc cho rằng hệ thống ít quan trọng nên tin tặc không quan tâm. Bài viết sẽ bàn kỹ hơn về những thách thức, cũng như các biện pháp để triển khai BYOD một cách an toàn.

PHẠM TRUNG HIẾU
Phó Giám đốc NSP

TRONG SỐ NÀY



Tiêu điểm

Chuyên đề

TẦM NHÌN MẠNG
NETWORKS VISION

Đơn vị xuất bản
Công ty TNHH TM–DV Tin học
Nhân Sinh Phúc (NSP Co., Ltd.)
359 Võ Văn Tần, Phường 5, Quận 3,
Tp. Hồ Chí Minh
ĐT: +84 8 3834 2108 Fax: +84 8 3834 2109
Website: www.nsp.com.vn
E-mail: tamnhinmang@nsp.com.vn

Chịu trách nhiệm xuất bản
PHẠM TRUNG HIẾU

Ban biên tập
PHẠM TRUNG HIẾU
LƯU LÊ QUI NHƠN
NGUYỄN VĂN ĐÔNG MINH
VŨ QUANG MINH
TRẦN NGỌC THANH

Thư ký biên tập
NGUYỄN THANH TUẤN

Mỹ thuật
NGUYỄN TRẦN MINH

Phát hành
BÙI VĂN TIN

tamnhinmang.vn

In tại nhà in Lê Quang Lộc. GPXB số 22/QĐ-BT-STTTT, ngày 31/8/2012

IBM cung cấp nền tảng DCIM Trellis của Emerson

Sắp đến, Emerson Network Power (ENP) sẽ kết hợp sản phẩm DCIM Trellis của hãng với phần mềm quản lý dịch vụ CNTT (ITSM) của IBM. Nằm trong thỏa thuận hợp tác, IBM cũng sẽ cung cấp nền tảng Trellis của ENP như là một giải pháp DCIM của mình. Theo ENP, việc tích hợp phần mềm của IBM với nền tảng Trellis sẽ cung cấp khả năng hiển thị thời gian thực từ những ứng dụng CNTT, thông qua các thành phần cơ sở hạ tầng và mạng lưới điện, cho phép quản lý môi trường trung tâm dữ liệu một cách toàn diện. Thomas Jamie, Phó Chủ tịch chiến lược và phát triển Tivoli của IBM nhận định: "Sự kết hợp giải pháp DCIM hàng đầu thị trường của Emerson Network Power, nền tảng Trellis–cùng với các giải pháp của chúng tôi (IBM) cho việc quản lý dịch vụ và quản lý hệ thống CNTT, sẽ là một hướng đi lý tưởng và sáng tạo nhằm đáp ứng nhu cầu của các khách hàng hiện nay".

Fluke Networks ra mắt dòng sản phẩm Visual TruView™

Ngày 29/01/2013, Fluke Networks (FNET) chính thức giới thiệu dòng sản phẩm Visual TruView™–thiết bị hợp nhất các giải pháp giám sát hiệu suất và xử lý sự cố mạng. Theo một cuộc khảo sát gần đây của FNET, hơn 50% các chuyên gia mạng không có đầy đủ

những công cụ cần thiết để xác định một cách nhanh chóng và chính xác các sự cố liên quan đến VoIP, các tương tác của ứng dụng và các vấn đề về hiệu suất mạng khác. Visual TruView™ cung cấp một giải pháp duy nhất lấp đầy những nhu cầu cấp thiết này của thị trường.

NSP tổ chức kỷ niệm ngày thành lập công ty lần thứ 14

Ngày 23 tháng 3 năm 2013, công ty NSP tổ chức buổi lễ kỷ niệm ngày thành lập lần thứ 14 kết hợp với một buổi dã ngoại cho toàn thể cán bộ, nhân viên tại khu du lịch The BCR–quận 9. Đây là một trong những sự kiện thường niên của NSP nhằm đánh dấu các cột mốc quan trọng trong quá trình phát triển.

Năm nay, ngoài sự kiện chính, nhân viên công ty còn được tham gia những trò chơi team-building đặc sắc nhằm tạo một không gian vui vẻ, thoải mái sau giờ làm việc, đồng thời xây dựng và phát huy khả năng làm việc nhóm, tinh thần đồng đội trong công ty.

Thành lập ngày 20 tháng 3 năm 1999 với tên gọi đầy đủ là công ty TNHH TM-DV Tin học Nhân Sinh Phúc, NSP đã từng bước khẳng định mình để trở thành một trong những nhà phân phối thiết bị, giải pháp hàng đầu trong lĩnh vực hệ thống mạng máy tính tại thị trường Việt Nam. Cho đến nay, NSP là đối tác phân phối chính thức của những công ty/tập đoàn hàng đầu thế giới như TE Connectivity, Emerson Network Power, Eaton, Fluke Networks, HP, Brady, ACTi...

TE Connectivity nằm trong danh sách "Top 100 Global Innovators" năm 2012

Lần thứ hai liên tiếp, TE Connectivity nằm trong danh sách "Top 100 Global Innovators" do tổ chức Thomson Reuters bình chọn. Đây là danh sách tôn vinh những tổ chức, doanh nghiệp có được những thành tựu lớn trong việc đổi mới, cải tiến trên quy mô toàn cầu trong việc bảo vệ sáng kiến và trong việc thương mại hóa các phát minh của mình.

Phương thức lựa chọn "Top 100 Global Innovators" năm 2012 được phát triển bởi Thomson Reuters và được sự chấp nhận của nhiều tổ chức sở hữu trí tuệ hàng đầu trên thế giới. Phương thức này sử dụng một nền tảng phân tích tiên tiến của Thomson Reuters để tính toán, nghiên cứu và phân tích các chỉ số sau: Thomson Reuters Derwent World Patents Index® (DWPISM), Derwent Patents Citation Index™, Quadrilateral Patent Index™ và Thomson Innovation®. Các tiêu chí để đánh giá và tính toán các chỉ số này bao gồm: sự thành công, tính toàn cầu, tầm ảnh hưởng và số lượng các bằng sáng chế của tổ chức, doanh nghiệp.

Ngoài TE Connectivity, hai đối tác phân phối quan trọng khác của công ty NSP là Emerson và Eaton cũng góp mặt trong danh sách này.

NSP cùng Emerson Network Power tham gia sự kiện Connect VMware Solutions Symposium 2013

Ngày 5 & 7 tháng 3 năm 2013, VMware đã tổ chức sự kiện Connect VMware Solutions Symposium 2013 (Connect VSS 2013) tại Hà Nội và Tp. HCM. Đây là sự kiện lớn trong năm của VMware nhằm mang tới cho khách hàng kiến thức về những xu hướng và giải pháp mới nhất về hạ tầng ảo hóa và hạ tầng đám mây. Tham dự Connect VSS 2013, khách hàng có cơ hội tiếp cận với những chuyên gia công nghệ hàng đầu từ VMware và đối tác.

Tham gia sự kiện với vai trò là đối tác chiến lược của VMware trên thế giới, Emerson Network Power (ENP) cùng đối tác phân phối tại Việt Nam là công ty NSP đã mang tới cho khách hàng giải pháp quản trị hạ tầng trung tâm dữ liệu (DCIM) tiên tiến nhất của hãng. Giải pháp này cho phép mở rộng phạm vi tiếp cận bao gồm cả cơ sở hạ tầng công nghệ thông tin (máy chủ, thiết bị lưu trữ, hệ thống mạng...) lẫn cơ sở hạ tầng tiện nghi (hệ thống làm lạnh, thiết bị lưu điện, thanh phân phối nguồn...). Từ đó, DCIM cung cấp cho người sử dụng cái nhìn và khả năng quản lý toàn diện hơn về toàn bộ tài nguyên bên trong TTDL.

TE Connectivity đào tạo giải pháp kết nối hiệu suất cao

Ngày 25-28/2 vừa qua, TE Connectivity đã tổ chức đào tạo các giải pháp kết nối hiệu suất cao cho nhân viên kinh doanh đến từ những nhà phân phối ủy quyền tại Việt Nam với mục đích cập nhật những thông tin mới nhất từ hãng tới khách hàng một cách chính xác nhất.

Hộp đấu nối quang mật độ cao Q3000

Các giải pháp trên bao gồm: giải pháp MPOptimate, tủ phân phối quang mật độ cao OMX 600, hộp đấu nối cáp quang mật độ cao Q3000, giải pháp đấu nối cáp đồng bấm sẵn 10G SigmaLink XG và MRJ21 XG, hệ thống quản lý sợi quang mật độ cao NGF, hệ thống máng cáp Fiber Guild...

Việt Nam–Thị trường phát triển nhanh nhất Đông Nam Á trong lĩnh vực giám sát hình ảnh

Theo báo cáo mới nhất của hãng nghiên cứu thị trường IMS Research 2012, Việt Nam đã vượt qua các quốc gia khác như Singapore, Malaysia, Thailand, Philippines, Indonesia... để trở thành thị trường phát triển nhanh nhất trong lĩnh vực giám sát hình ảnh trong khu vực Đông Nam Á.

Theo báo cáo này, Singapore và Malaysia là một trong các thị trường tương đối phát triển trong khu vực, nhưng trong những thị trường mới nổi, Việt Nam dẫn đầu với tốc độ tăng trưởng dự đoán hàng năm là 22,3% (từ năm 2010 đến 2015).

Theo bà Cheryl Li, tác giả bài phân tích và báo cáo trên, kết quả này có được một phần do Việt Nam đã giảm thuế nhập khẩu các mặt hàng camera giám sát hình ảnh, từ đó dẫn đến việc thu hút nhiều thương hiệu từ Châu Âu và Mỹ tham gia thị trường. Ngoài ra, các dự án giám sát an ninh, đặc biệt là dự án nhà nước đang ngày càng phát triển cả về số lượng lẫn độ lớn.

Hội nghị Ethernet Technology Summit sắp được diễn ra

Ethernet Technology Summit–Hội nghị về công nghệ Ethernet năm nay được tổ chức vào ngày 02 đến ngày 4 tháng 4 tại khách sạn Santa Clara Marriott, thung lũng Silicon. Chủ đề chính của năm nay sẽ tập trung vào mạng hội tụ, công nghệ Ethernet 40/100/400 Gigabit, kiến trúc mạng dựa trên nền phần mềm, ảo hóa và mạng hiệu suất cao. Ông Claudio DeSanti (Cisco System)–chủ tịch hội thảo cho biết: "Ethernet vẫn đang phát triển, Ethernet Technology Summit năm nay tiếp tục là nơi để theo dõi các diễn biến trong ngành. Năm nay, hội thảo sẽ dành ra hai ngày để tập trung vào hai chủ đề chính là kiến trúc mạng trên nền phần mềm, và OpenFlow…". Các diễn giả trong hội thảo năm nay đến từ các công ty công nghệ hàng đầu như Cisco, Broadcom, Dell, IBM, HP, Spirent, Brocade, Big Switch Networks, Orange France Telecom…

Fluke Networks tổ chức hội nghị Sales Kick-Off cho khu vực Châu Á Thái Bình Dương

Tháng 2/2013 vừa qua, Fluke Networks (FNET) đã tổ chức hội nghị thường niên Sales Kick-Off cho khu vực Châu Á Thái Bình Dương (APAC) nhằm tổng kết tình hình kinh doanh trên toàn khu vực, đưa ra các mục tiêu cho năm 2013 và lộ trình phát triển các sản phẩm mới.

Năm 2012 đánh dấu sự phát triển vượt bậc về doanh số và tốc độ tăng trưởng của thị trường APAC, đặc biệt ở các quốc gia phát triển như Singapore, Trung Quốc, Nhật Bản, Malaysia… Với tốc độ phát triển hiện nay, FNET dự đoán thị trường APAC sẽ tăng trưởng khoảng 100% trong vòng 3 năm tới, từ năm 2013 đến 2015.

BYOD–Ảnh hưởng và thách thức

Theo nghiên cứu của Gartner, có hơn 821 triệu thiết bị thông minh (điện thoại thông minh và máy tính bảng) được mua trên toàn thế giới trong năm 2012, chiếm hơn 70% số lượng thiết bị IT được bán ra. Sự bùng nổ này cho thấy BYOD thực sự là một biển báo chỉ đường cho xu hướng công nghệ tương lai.

Cách đây không lâu, máy tính bàn và laptop vẫn là những thiết bị điện tử hữu hiệu để nhân viên sử dụng tại nơi làm việc. Hiện tại, phần lớn nhân viên đều sở hữu và luôn mang theo bên mình các thiết bị điện tử mới hiện đại và hiệu quả hơn. Đó là nhờ sự bùng nổ thị trường tiêu dùng công nghệ cao với những thiết bị như điện thoại thông minh và máy tính bảng.

Khi mới xuất hiện, các thiết bị này được dùng cho mục đích cá nhân, nhưng với những tiện ích đa dạng, chúng dần được sử dụng nhiều hơn cho mục đích công việc và kinh doanh. Việc gia tăng các phần mềm trên nền web cũng góp phần thúc đẩy các sản phẩm công nghệ này phát triển. Kết quả là chiếc tàu lượn siêu tốc mang tên BYOD tiếp tục tăng tốc và chưa có dấu hiệu chậm lại trong tương lai gần.

Điều hiển nhiên, không có xu hướng công nghệ nào lại không đi kèm với sự đánh đổi về chi phí. Trong trường hợp của BYOD, đó chính là chi phí về bảo mật và hiệu suất WLAN, cùng với những ảnh hưởng về công việc của các chuyên viên mạng.

Một số nhà quản trị mạng đang sẵn sàng đón nhận mô hình BYOD một cách nhiệt tình. Họ đã tiến hành các bước nhằm tối thiểu hóa ảnh hưởng của việc kết nối các thiết bị cá nhân vào hệ thống mạng, đồng thời vẫn đảm bảo cung cấp môi trường hoạt động tốt nhất cho các thiết bị này.

Tuy nhiên, có một số câu hỏi quan trọng đặt ra đối với doanh nghiệp và các nhà quản trị đang sẵn sàng đón nhận và cung cấp BYOD: Làm thế nào để giữ vững tính bảo mật trong khi các máy trạm của người dùng không bị hạn chế? Có thể quản lý được quan hệ khá hỗn loạn của các thiết bị với số lượng không cố định? Làm sao để duy trì tốc độ kết nối với hàng loạt thiết bị và hệ điều hành khác nhau?

Đó mới chỉ là ở phần cứng. Phía sau mỗi thiết bị còn kèm theo vô số các ứng dụng. Khi mỗi ứng dụng được sản xuất từ một nhà phát triển phần mềm riêng, với một tác giả riêng, sẽ có những đòi hỏi truy cập tài nguyên mạng khác nhau. So với đặc điểm là chặn tất cả các ứng dụng "lạ" của môi trường mạng truyền thống, BYOD thực sự là một thế giới hoàn toàn khác.

Những thách thức đối với chuyên viên mạng

Thách thức dễ nhận thấy nhất từ BYOD chính là số lượng truy cập mạng. Dù không phải tất cả, nhưng hầu hết các hệ thống WLAN của doanh nghiệp đều được hoạch định, phân bổ phù hợp với nhu cầu về công suất và băng thông dựa trên tài sản sẵn có của doanh nghiệp (như số lượng laptop và điện thoại IP). Tuy nhiên, với tốc độ phát triển không kiểm soát của các thiết bị cá nhân do nhân viên mang đến nơi làm việc, hoạch định hệ thống Wi-Fi ban đầu xem như sụp đổ. Theo báo cáo từ tổ chức Gartner, các thiết bị di động cá nhân không chỉ tranh giành tín hiệu và băng thông mạng Wi-Fi, mà còn ngốn tài nguyên mạng nhiều hơn các laptop thông thường, vì các mô-đun của chúng yếu hơn và ít đáp ứng tiêu chuẩn hơn (mạng Wi-Fi hoạt động trên cơ chế mạng chia sẻ, nếu trong hệ thống có một thiết bị tham gia mạng với tốc độ thấp, sẽ kéo theo toàn bộ hệ thống hoạt động với tốc độ thấp).

Những hành xử không mong muốn của các thiết bị cá nhân có thể gây ảnh hưởng lớn đến hệ thống WLAN. Với những thiết bị thuộc tài sản công ty, tình trạng này sẽ không xảy ra, hoặc nếu

Thuật ngữ BYOD được viết tắt từ "Bring your own device", được sử dụng lần đầu tiên vào năm 2009 bởi Intel, nhưng đến năm 2011 nó mới thực sự nổi bật khi được Unisys, VMware và Citrix System giới thiệu đến giới công nghệ.

BYOD được biết đến như là một chính sách chấp nhận nhân viên đem các thiết bị di động cá nhân (như laptop, máy tính bảng, điện thoại thông minh) vào nơi làm việc và sử dụng chúng để truy cập các thông tin hay ứng dụng quan trọng của công ty. Thuật ngữ này cũng được sử dụng để diễn tả việc chấp nhận sinh viên sử dụng các thiết bị cá nhân trong môi trường giáo dục.

BYOD xâm nhập đáng kể trong thế giới kinh doanh, với khoảng 60% nhân viên đã sử dụng các thiết bị công nghệ cá nhân (mặc dù bị hạn chế) tại nơi làm việc. Trong hầu hết trường hợp, các doanh nghiệp không thể ngăn chặn xu hướng này. Nhiều người tin rằng BYOD sẽ giúp các nhân viên nâng cao năng suất làm việc. Những người khác nói rằng BYOD sẽ làm tăng sự tiện lợi và tinh thần làm việc của nhân viên bằng cách sử dụng chính thiết bị của họ, đồng thời làm cho công ty trông như một người sử dụng lao động linh hoạt và có sức hút.

có, chúng đã được tính đến từ trước và không gây gián đoạn mạng của người dùng khác. Ngược lại, các thiết bị cá nhân thường cố tranh giành tài nguyên mạng và hạn chế truy cập của những người dùng khác.

Khi hệ thống WLAN và BYOD ngày càng trở nên thiết yếu trong hoạt động kinh doanh và điều khiển một lượng ngày càng nhiều dữ liệu quan trọng, vấn đề sống còn đối với các chuyên viên mạng là phải có phản ứng nhanh để kịp thời giải quyết các vấn đề về hiệu suất mạng. Thực tế, nhiều kỹ sư phụ trách hệ thống WLAN hiện nay vẫn chưa được trang bị đầy đủ kỹ năng về mạng không dây. Trong trường hợp này, các công cụ phần mềm thông minh cung cấp khả năng hiển thị chi tiết và hướng dẫn xử lý sự cố là giải pháp vô giá trong việc duy trì kết nối và hiệu suất mạng.

Bảo mật

Những tác động ngẫu nhiên về bảo mật là nguy cơ ít được nhìn thấy nhưng có hậu quả thật sự nghiêm trọng. Chúng thường tiềm ẩn khi các thiết bị cá nhân kết nối vào hệ thống WLAN và truy cập vào các ứng dụng mạng hay dữ liệu. Có hai mặt của vấn đề cần được quan tâm:

Đầu tiên, là việc truy cập mạng. Người sở hữu máy tính bảng hoặc điện thoại thông minh có thể thiếu thông tin để đăng nhập vào hệ thống WLAN an toàn và đáng tin cậy. Do đó, họ có thể truy cập một hệ thống WLAN không an toàn bên ngoài. Điều này đồng nghĩa với việc mở một "cổng sau" cho các xâm nhập trái phép từ một bên thứ ba vào hệ thống mạng doanh nghiệp, một tác động nguy hiểm mà có thể sẽ không bao giờ được phát hiện.

Khía cạnh thứ hai, là với các thiết bị đã được áp dụng chế độ bảo mật, được chấp thuận và đăng ký quyền truy cập đã chứng thực, kết nối được mã hóa. Vấn đề là khả năng rò rỉ thông tin– các thông tin, tài liệu mật hoặc các dữ liệu khác có thể bị chuyển ra ngoài. Điều này có thể thực hiện thông qua việc lưu trữ các dữ liệu trên bộ nhớ của chính các thiết bị cá nhân hoặc thông qua các giải pháp lưu trữ đám mây như Dropbox.

Quản lý

Được xem như thiết bị tiêu dùng, máy tính bảng và điện thoại thông minh không được các nhà cung cấp giải pháp quan tâm nhiều trong việc thiết kế công cụ quản lý. Bên cạnh đó, các dòng sản phẩm thường xuyên ra đời với số lượng lớn, kèm theo một loạt các phần mềm (firmware) và hệ điều hành được nâng cấp liên tục, gây đau đầu cho các nhân viên quản lý CNTT. Thách thức này còn khó khăn gấp bội khi đối mặt với yêu cầu vừa phải quản lý các BYOD, vừa chịu áp lực từ việc cắt giảm nguồn nhân lực.

Do các công ty không thể cung cấp chuyên gia về WLAN tại mỗi văn phòng chi nhánh, họ thường áp dụng các giải pháp quản lý và giám sát từ xa. Với trường hợp BYOD, điều này trở thành một trở ngại lớn vì không phải thiết bị nào cũng cung cấp giao diện phân tích phù hợp với hệ thống của bạn. Ví dụ: các thiết bị của Apple với hệ điều hành iOS hiện nay vốn không có bất cứ tác nhân hỗ trợ quản trị và phân tích nào. Một số thiết bị Android có cung cấp các tính năng mở rộng để phân tích và ghi log sự kiện, nhưng hầu hết chỉ giới hạn một số hàm API và không hỗ trợ tính năng xử lý sự cố từ xa. Những hạn chế này đặc biệt gây khó khăn cho bộ phận IT vì họ không thể hỗ trợ cho từng người với từng thiết bị, kéo theo đó là các thiết bị cá nhân có thể hoạt động với hiệu suất không tốt, gây trì trệ cả hệ thống WLAN.

Những tác động đến việc kinh doanh

Theo các phân tích về ảnh hưởng của BYOD như trên, những rủi ro có thể xảy ra là giảm hiệu quả hoạt động kinh doanh, tăng chi phí hoạt động và ảnh hưởng đến chính sách an ninh, bảo mật. Nhưng thay vào đó, ta có thể sử dụng BYOD một cách hợp lý như một tài sản phục vụ cho việc kinh doanh.

Để tích hợp BYOD thành công

Kế hoạch, dự đoán và thiết kế

Để tích hợp thành công BYOD vào hệ thống WLAN của doanh nghiệp, việc hoạch định và thiết kế rất cần được chú ý. Điểm mấu chốt là phải hiểu rõ độ bao phủ và hiệu suất của hệ thống Wi-Fi

hiện tại: vị trí của các AP (Access Point); vị trí tường, cửa và các kết cấu kim loại; xác định các vị trí mật độ truy cập cao như phòng họp, khu vực tiếp tân, phòng chờ (là những phòng phần lớn sử dụng truy cập không dây).

Hạ tầng cáp mạng hỗ trợ cho AP cũng nên được quan tâm đúng mức. Với chuẩn 802.11n, tốc độ truyền dữ liệu lên đến 300 Mbit/s, các AP phải được kết nối bằng Cat. 6 với tốc độ 1 Gbps.

Cần lưu ý các kiểu thiết bị BYOD. Ví dụ: hầu hết các thiết bị bỏ túi đều được tối ưu hóa mức tiêu thụ điện năng và kích thước nhỏ. Điều này gây hạn chế về hiệu suất RF (Radio Frequency) và ăng-ten, khiến tốc độ truyền dữ liệu của các thiết bị này thấp hơn laptop hay máy in qua mạng. Ngoài ra, do những thiết bị lỗi thời thường không hỗ trợ băng tần 5 Ghz hay chế độ ghép kênh nên dễ dẫn đến việc tranh giành ở băng tần 2,4 Ghz, gây xung đột hệ thống mạng.

Ứng dụng cũng là yếu tố cần cân nhắc. Băng thông phải được ưu tiên cho các ứng dụng thời gian thực như VoIP và hội nghị trực tuyến. Tác động từ hệ thống mạng đến chất lượng cuộc gọi qua mạng phải được kiểm tra kỹ càng, đảm bảo tính thông suốt và chất lượng cuộc gọi, đặc biệt ở những vùng giao thoa giữa các AP.

Một loạt các công cụ thiết kế mạng đã cách mạng hóa phương pháp triển khai và thiết kế mạng wireless. Sử dụng những thông tin về bố trí mặt bằng, cơ sở hạ tầng mạng hiện có, môi trường sóng wireless xung quanh khu vực, số lượng và mức độ sử dụng, các công cụ này có thể dự đoán và tính toán hiệu suất cũng như độ bao phủ của hệ thống WLAN. Thiết kế có thể được điều chỉnh, thêm hay di chuyển các thiết bị cho phù hợp với sự phát triển của BYOD hoặc khi cần thay đổi bố trí văn phòng.

Từ mô hình do các công cụ thiết kế cung cấp, ta sẽ có được danh sách mua sắm thiết bị cụ thể, bao gồm từ những bảng so sánh thông số kỹ thuật của các AP cụ thể, của các nhà cung cấp cho đến giản đồ sóng của các loại ăng-ten. Tất cả những bước chuẩn bị này sẽ giúp tiết kiệm thời gian cho quá trình triển khai trong hiện tại và tương lai.

Khảo sát, thẩm định và triển khai

Với bất kỳ hệ thống wireless nào, điều quan trọng cần xác định là phải xem thực tế có đúng như các phần mềm hoạch định đưa ra hay không (vì không thể chắc chắn tín hiệu sóng sẽ bị ảnh hưởng như thế nào). Chúng ta sử dụng phần mềm hoạch định như một cơ sở lý thuyết để đặt các AP, sau đó cần tiến hành kiểm tra và cải thiện thiết kế. Quá trình này nên được tiến hành lặp đi lặp lại nhiều lần đến khi có kết quả tối ưu. Tuy nhiên, trong quá trình chỉnh sửa vị trí, phải xem xét đến cơ sở hạ tầng có sẵn như nguồn điện, kết nối mạng cho AP.

Smart Device List

Display Name (32)	ACL	OS	Model
HTC:E8:D2:D0	U	Android/Windows	HTC
APPLE:3F:6B:33	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:81:4E:F8	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:6D:C...	U	Android/Windows	Samsung
APPLE:CE:79:CE	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:A6:66:ED	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:1F:42:7E	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:18:C3:75	U	iOS	iPhone 5/iPad 4/iPad Mini
SAMSUNG:4A:8...	U	Android/Windows	Samsung
SAMSUNG:21:5...	U	Android/Windows	Nexus
APPLE:81:E4:91	U	iOS	iPhone 4/iPhone 4s/iPad
APPLE:2D:B4:08	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:C1:0...	U	Android/Windows	Samsung
ASUSTEK:CC:A...	U	Android/Windows	Nexus 7
APPLE:0D:86:96	U	iOS	iPhone 4/iPhone 4s/iPad
SAMSUNG:0D:B...	U	Android/Windows	Samsung
APPLE:4C:73:7C	U	iOS	iPhone 5/iPad 4/iPad Mini

Hình minh họa: Giải pháp quản lý các thiết bị di động trong hệ thống mạng

Phát hiện và loại bỏ nhiễu

Hệ thống wireless phát triển khiến các nguồn nhiễu cũng phát triển theo. Với trường hợp này, các công cụ phần mềm có thể liên tục giám sát để cảnh báo cho kỹ sư mạng ngay khi có sự cố về nhiễu. Trong các sự cố về nhiễu, dễ khắc phục nhất là nhiễu từ các thiết bị Wi-Fi khác, chỉ cần thay đổi kênh của các thiết bị trong vùng bị ảnh hưởng. Tuy nhiên, đây lại trở thành vấn đề với BYOD. Rất nhiều thiết bị bật cả tính năng Bluetooth và Wi-Fi, dẫn đến bão hòa hiệu năng của băng tần 2,4 GHz. Điều này vẫn xảy ra khi ta không tiếp nhận các thiết bị BYOD, chúng vẫn sẽ lặp đi lặp lại quá trình tìm kiếm AP và cố gắng kết nối vào mạng.

Nhiễu cũng có thể đến từ những nguồn khác, không chỉ Bluetooth và Wi-Fi mà còn bao gồm điện thoại bàn không dây và lò vi sóng, do cả hai thiết bị này dùng cùng băng tần với hệ thống Wi-Fi. Theo một khảo sát gần đây, 82% người cho biết đã từng có kinh nghiệm về sự cố hiệu suất WLAN gây ra bởi nhiễu từ các thiết bị không thuộc hệ thống WLAN. Khi gặp phải loại nhiễu này, việc cần làm là di chuyển chỗ đặt thiết bị hoặc thêm các phụ kiện lọc nhiễu.

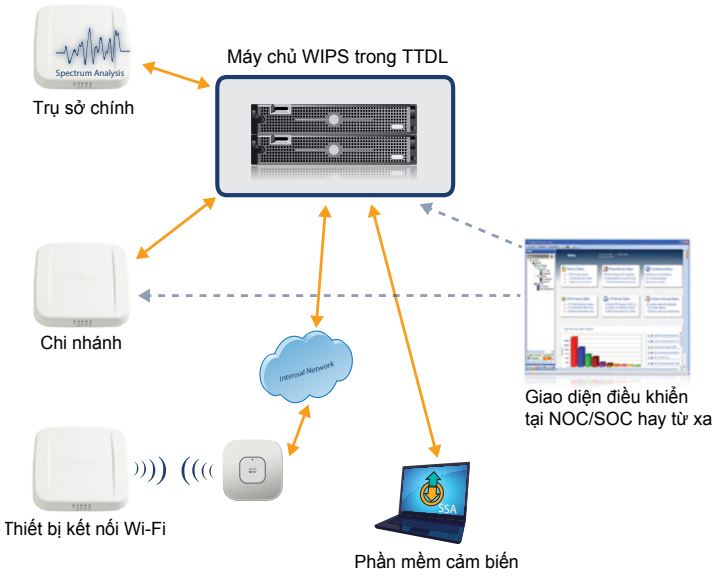
Duy trì bảo mật

Một phần quan trọng của chiến lược BYOD là duy trì bảo mật trong môi trường wireless. Trong khi nhà cung cấp phần cứng có thể cung cấp các công cụ bảo mật thô sơ, chỉ có hệ thống phòng chống xâm nhập wireless chuyên dụng (WIPS) mới có thể duy trì bảo mật một cách đầy đủ và mạnh mẽ.

Hệ thống WIPS hoạt động dựa trên hai phương thức bao gồm giám sát sóng phổ nhằm phát hiện các thiết bị wireless trái phép và tự động ngăn chặn truy cập vào hệ thống WLAN. Với các tổ chức lớn, nguy cơ đặc biệt cần đề phòng đến từ các điểm truy cập giả, là loại sự cố mở ra thêm một đường cho bất cứ ai cũng có thể xâm nhập vào hệ thống mạng. Hệ thống WIPS sẽ phát hiện bằng cách sử dụng bộ lọc địa chỉ MAC, chống giả mạo MAC bằng cách kết hợp các thông số đặc trưng của thiết bị. Hệ thống WIPS cũng phát hiện và cảnh báo những trường hợp có hoạt động cố gắng tấn công mạng wireless.

Các công cụ WIPS hiện nay thường liên quan đến ba yếu tố sau: cảm biến thông minh có thể quét sóng phổ và bắt gói dữ liệu; kế đến là một hoặc nhiều server để thu thập thông tin từ cảm biến và phân tích dữ liệu bắt gói; cuối cùng là một bộ quản trị và báo cáo tập trung.

Các mô hình này cho phép triển khai cảm biến trên nhiều chi nhánh, cung cấp



Mô hình các thành phần cơ bản trong hệ thống WIPS

khả năng giám sát và phát hiện 24/7. WIPS sẽ cảnh báo cho các kỹ sư mạng và những người chịu trách nhiệm về bảo mật khi có bất kì sự cố hay nguy cơ tấn công nào.

Sự tăng trưởng của BYOD và wireless cũng kéo theo khả năng phát triển các lỗ hổng và nguy cơ bảo mật. Do đó, một yếu tố quan trọng khác phải chú ý là luôn cập nhật và đề phòng các nguy cơ mới. Trong khi các nhà cung cấp thiết bị đưa ra các bản cập nhật không thường xuyên (bao gồm cập nhật về các lỗ hổng bảo mật), hệ thống WIPS sẽ giúp ta tập trung quản lý cập nhật từ xa và không cần phải có mỗi chuyên gia tại từng chi nhánh.

Quản lý

Để có thể cung cấp BYOD trong doanh nghiệp, các thiết bị phải cam kết không ảnh hưởng đến những người dùng khác. Tuy nhiên, việc đạt được một môi trường hòa hợp giữa các thiết bị wireless truyền thống và các thiết bị cá nhân của nhân viên vẫn còn vấp phải những rào cản nhất định.

Cần nhớ rằng, tốc độ của người dùng mạng Wi-Fi không chỉ được xác định bởi hiệu suất của mạng không dây. Những kết nối mạng có dây, cung cấp kết nối cho AP cũng như tốc độ đáp ứng của máy chủ, dữ liệu hay các dịch vụ đám mây cũng góp phần quan trọng. Vì vậy, điều cần thiết là phải giám sát end-to-end thực sự, xác định và đo lường toàn bộ đường đi từ người dùng đến thiết bị đầu cuối cung cấp dịch vụ.

Các xu hướng về truyền thông đa phương tiện như hội nghị từ xa, hội nghị trực tuyến hay các cuộc gọi hình ảnh có thể làm tăng yêu cầu về truyền dữ liệu trong một số thời điểm nhất định. Tuy nhiên, cần phải có các cảm biến thu thập thông tin tức thời để cảnh báo khi sự cố diễn ra nhằm có được những phương pháp đề phòng trong tương lai.

Với các thử nghiệm về tính liên tục của hệ thống wireless nhằm phát hiện các điểm tắt nghẽn, tỉ lệ lỗi cao, suy giảm tốc độ truyền dữ liệu và những vấn đề khác..., các nhà quản trị đã có đầy đủ thông tin cần thiết để có thể chủ động đối phó sự cố. Thay vì đuổi theo các vấn đề đã xảy ra, tốt hơn hết các nhà quản trị nên ngăn ngừa các sự cố có thể xảy ra ngay từ đầu.

Tiết kiệm chi phí

BYOD không được nhìn nhận thực sự trong hệ thống mạng doanh nghiệp vì dường như chúng làm tăng chi phí hoạt động. Thêm thiết bị đồng nghĩa với việc tăng khối lượng cơ sở hạ tầng, kéo theo yêu cầu bổ sung các công cụ quản lý mới, thành lập các quy trình mới, thêm việc cho nhà quản trị và có thể thêm cả chi phí. Tuy nhiên trên thực tế, lượng công việc các nhà quản trị mạng phải gánh không quá nhiều so với khi không có BYOD. Các công cụ hỗ trợ quản lý hiệu suất và bảo mật hiện đại là trợ thủ đắc lực giúp giảm nhẹ công việc của nhà quản trị. Việc tự động hóa thông qua các cảm biến và phần mềm quản lý thông minh cũng giúp đảm bảo hiệu quả quản trị, duy trì chính sách bảo mật, đồng thời không cần tăng quy mô đội ngũ IT.

BYOD đã thúc đẩy các công cụ quản trị mạng phải phát triển hơn, tinh vi hơn, đồng thời mang lại lợi ích hỗ trợ cho người dùng mạng có dây. Cả mạng có dây và không dây đều được giám sát và quản lý cùng nhau trên môi trường mạng, không cần phải tách biệt thành hai môi trường riêng biệt, tạo cơ hội để tiết kiệm chi phí.

Bên cạnh đó, có những bằng chứng cho thấy sử dụng BYOD, các nhân viên có thể làm việc nhiều hơn, dễ dàng và thuận lợi hơn ở bất kỳ nơi đâu có mạng wireless, bù đắp lại khoản chi phí quản lý và hỗ trợ cho các thiết bị này. Hơn nữa, các công ty hiện nay cũng có xu hướng tăng các ứng dụng ảo hóa và điện toán đám mây, đồng nghĩa với việc tăng tiềm năng tiết kiệm chi phí hoạt động từ BYOD vì nhân viên có thể làm việc tại bất cứ nơi đâu có thể truy cập Internet.

Xu hướng mạng di động

Từ trước đến nay, BYOD chỉ được xem xét về khía cạnh WLAN. Hiện tại, sự phát triển xu hướng mạng di động 3G và 4G/LTE đang được tính đến bởi các nhà khai thác mạng di động. Với chiếc điện thoại di động của mình, các nhân viên có thể làm việc được cả ở những nơi không có mạng wireless.

Trong trường hợp này, gánh nặng thường thuộc về các nhà khai thác mạng di động. Tuy nhiên, các công ty lớn với nhiều không gian công cộng đã chuyển qua các công nghệ như Femtocell, Picocell, Microcell và hệ thống phân phối ăng-ten để cung cấp mạng di động trong doanh nghiệp.

Kết luận

Dù vẫn tồn tại những rủi ro có thể ảnh hưởng đến hiệu quả hoạt động kinh doanh, chi phí và chính sách an ninh, bảo mật... nhưng với nhiều tiện ích đa dạng của mình, BYOD ngày càng được sử dụng nhiều cho mục đích công việc. Bằng cách tích hợp thành công BYOD vào hệ thống mạng sẵn có, doanh nghiệp có thể sử dụng BYOD hợp lý như một tài sản phục vụ hiệu quả trong kinh doanh.

Vũ Quang Minh
Theo Fluke Networks

Lựa chọn STP hay UTP cho hệ thống giám sát?

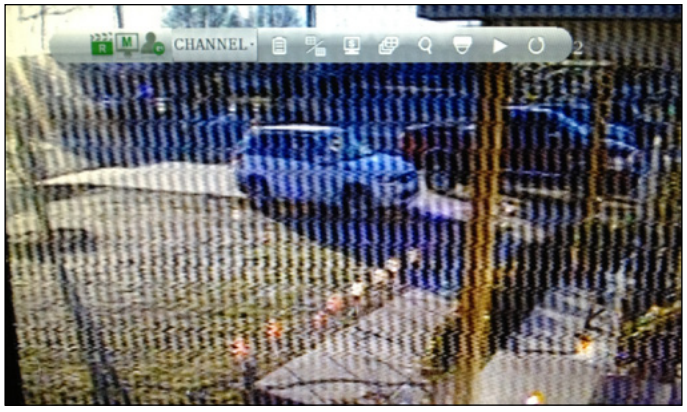
Nhiễu điện trong hệ thống cáp là một trong những nguyên nhân gây ra các sự cố về hình ảnh trong lĩnh vực giám sát an ninh. Việc sử dụng cáp có lớp bọc chống nhiễu sẽ là "vũ khí" lợi hại nhằm loại bỏ vấn đề này.

Khi triển khai hệ thống camera giám sát, phần lớn các nhà tích hợp hệ thống ít chú ý đến việc nên chọn loại cáp mạng nào, họ chỉ quan tâm đến giá cả và thường quyết định theo phương châm: "rẻ là được". Tuy nhiên trong lĩnh vực giám sát an ninh, việc lựa chọn loại cáp để sử dụng không chỉ có ý nghĩa rất quan trọng mà còn ảnh hưởng trực tiếp đến chất lượng hình ảnh. Bài viết này sẽ trình bày về loại cáp có lớp bọc chống nhiễu (shielded), tìm hiểu cơ chế mà loại cáp này ngăn chặn các vấn đề gây ảnh hưởng đến chất lượng hình ảnh, và so sánh chúng với loại không có lớp bọc chống nhiễu (unshielded).

Nhiễu điện–"sát thủ" hình ảnh

Trong lĩnh vực giám sát an ninh, các nhà tích hợp thường chú trọng các thiết bị như camera và NVRs (Network Video Recorders), họ ít quan tâm đến hệ thống cáp truyền dẫn. Khi chất lượng hình ảnh gặp vấn đề, các nhà tích hợp thường truy tìm nguyên nhân trên camera và cố gắng tùy chỉnh các thông số để giải quyết sự cố, sau đó đau đầu vì chẳng thể giải quyết được gì. Tuy nhiên, nếu họ quan tâm đúng mức vào hệ thống cáp, vấn đề có thể sẽ được giải quyết nhanh chóng. Ví dụ như trong hình minh họa bên dưới.

Nhiễu điện trong hệ thống cáp chính là nguyên nhân gây ra sự cố như trong hình. Hệ thống cáp không chỉ truyền tải luồng dữ liệu hình ảnh, mà còn "hút" và truyền tải kèm theo cả yếu tố "nhiễu" không mong muốn. Lúc này, sử dụng cáp có lớp bọc chống nhiễu sẽ là "vũ khí" lợi hại để loại bỏ các vấn đề tương tự.



Hình minh họa: Camera bị tác động bởi nhiễu

Bên cạnh đó, việc chọn và sử dụng cáp mạng có chất lượng kém sẽ ảnh hưởng trực tiếp đến hiệu suất của các camera và đầu ghi hình. Trong phần dưới đây, hãy cùng tìm hiểu và so sánh sự khác biệt giữa hai loại cáp: cáp đôi xoắn có lớp bọc chống nhiễu (STP–Shielded Twisted Pair) và cáp đôi xoắn không có lớp bọc chống nhiễu (UTP–Unshielded Twisted Pair).

Tổng quan

Nhìn bằng mắt thường, có thể thấy khác biệt chủ yếu giữa STP và UTP là về cấu tạo vật lý. Hình ảnh bên dưới cho thấy so với UTP, cáp STP có thêm một lớp vỏ làm bằng nhôm được bọc bên ngoài các đôi xoắn.

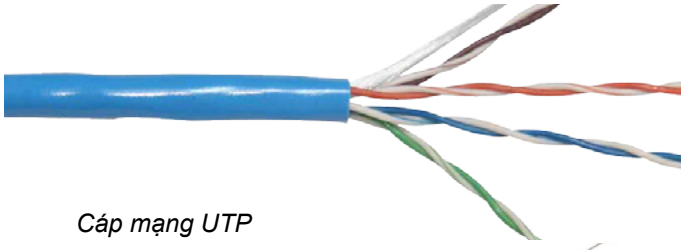
Khi nhận dạng cáp, không nên nhầm lẫn loại "Shielding" với "Screening". "Screening" là loại cáp có một lớp lá kim loại hoặc lưới bao phủ toàn bộ sợi cáp. Trên thực tế, việc bọc từng đôi riêng trong "Shielding" so với bọc gộp toàn bộ sợi cáp trong "Screening" đều nhằm mang lại một số lợi ích tương tự về mặt chống nhiễu. Tuy nhiên, khả năng chống nhiễu của chúng không tương đương và hiệu suất mỗi loại cũng khác nhau.

STP là tên viết tắt thường dùng của cáp đôi xoắn có lớp bọc chống nhiễu, đôi khi còn được viết là "U/FTP" (Unscreened/Foil-shielded twisted pair). Khi các tiêu chuẩn dành cho hệ thống cáp được phát triển và tinh lọc theo thời gian, các sản phẩm cáp chuyên dùng cho các ứng dụng cao cấp trong trung tâm dữ liệu ra đời đã làm thay đổi ý nghĩa của thuật ngữ trên. Tuy nhiên, với hầu hết các ứng dụng giám sát an ninh, "STP" vẫn là tên gọi phổ biến nhất.

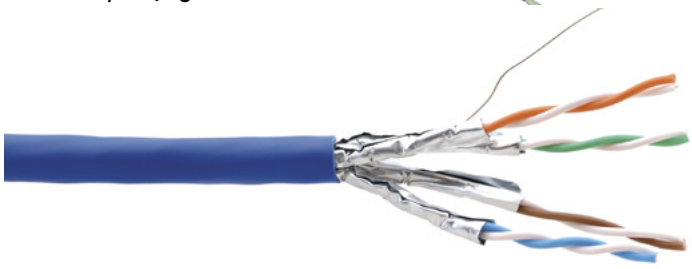
Khác biệt về cấu tạo vật lý: Liệt kê những khác biệt hữu hình giữa STP với UTP

- ***Lá kim loại bảo vệ:*** STP có một lớp lá kim loại mỏng, thường làm bằng nhôm, bao quanh từng cặp dây xoắn. Lớp này thường được gọi là "drain". Việc thiếu các giải pháp triệt tiêu nhiễu, các "drain" có thể gây khuếch đại những vấn đề mà STP cố gắng giảm thiểu.
- ***Vỏ dày:*** Việc bổ sung thêm các lớp lá nhôm sẽ làm tăng trọng lượng cũng như đường kính sợi cáp STP. Vì vậy, cần thiết phải sử dụng một loại vỏ nhựa dày cách điện để tăng độ bền. Nhìn chung, cáp STP nặng và dày hơn so với cáp UTP, đồng nghĩa với việc khó khăn hơn trong quá trình thi công lắp đặt.
- ***Lõi nhựa, dây hỗ trợ tước vỏ (Pull Strips), và dây tiếp đất:*** Tùy thuộc vào nhà sản xuất và thương hiệu, cáp STP có thêm vài đặc điểm không thể tìm thấy trong cáp UTP. Những đặc điểm này bao gồm lõi nhựa cứng nằm bên trong cáp để tách riêng các cặp dây, dây hỗ trợ tước vỏ và có thêm dây điện nối đất.

Khác biệt về chức năng: Những chức năng vật lý cộng thêm của STP mà UTP không sở hữu:



Cáp mạng UTP



Cáp mạng STP

• ***Trở kháng EMI:*** Ưu điểm chính của lớp lá kim loại (drain) bảo vệ STP tránh được nhiễu điện từ trường (electromagnetic interference) từ môi trường, hay còn gọi là EMI. Nhờ mỗi cặp dây xoắn được bọc riêng, khả năng nhiễu từ môi trường xung quanh vào cáp được giảm thiểu đáng kể hoặc loại bỏ hoàn toàn.

• ***Cách ly luồng nhiễu:*** Đối với loại cáp không có lớp bọc chống nhiễu, nhiễu được xem như là "con đường hai chiều". Một là chính các đôi cáp hay sợi cáp sẽ gây nhiễu lên nhau. Hai là do chính bản thân hệ thống cáp Ethernet phát ra nhiễu không mong muốn và ảnh hưởng đến một số ứng dụng khác, đặc biệt trong lĩnh vực sản xuất hoặc y khoa. Chính vì vậy, việc bổ sung lớp bọc chống nhiễu cho các cặp dây sẽ giảm thiểu hoặc loại bỏ vấn đề này.

• ***Tốc độ truyền dẫn cao hơn:*** Một số nghiên cứu cho thấy hệ thống cáp có lớp bọc bảo vệ không chỉ giúp giảm nhiễu mà còn có thể nâng cao tốc độ băng thông. Tuy nhiên, những tuyên bố này cần được xem xét một cách thận trọng.

Khác biệt về chi phí

Việc sử dụng cáp STP sẽ gia tăng chi phí từ 20-40 USD cho mỗi camera so với cáp UTP. Giả định khoảng cách kéo cáp là 150 feet (~ 46 m), chi phí sử dụng cáp STP sẽ nhiều hơn khoảng 40% so với UTP, ngoài ra còn phát sinh thêm các chi phí nguyên vật liệu cần thiết cho việc kéo cáp STP cũng như nhân công.

Nên sử dụng STP ở đâu?

Câu trả lời rất đơn giản: ở bất cứ nơi nào có thể gặp vấn đề về nhiễu. Dưới đây là một số nguồn có "nguy cơ cao" trong việc phát sinh ra nhiễu gây ảnh hưởng đến hình ảnh:

• ***Gần đường điện cao áp:*** Đường điện có thể ảnh hưởng trực tiếp tới hệ thống cáp truyền tải dữ liệu khi chúng đi song song với nhau. Hiện tượng nhiễu có thể xảy ra, và trường hợp này nên sử dụng cáp STP.

• ***Gần các nguồn cảm điện:*** các thiết bị điện như động cơ điện, máy biến áp điện, cuộn dây từ tính... có thể tạo ra sự can thiệp lên cáp truyền dữ liệu đặt gần nó đủ để làm suy giảm chất lượng hình ảnh.

Ngoài ra còn có các nguồn khác có thể gây ảnh hưởng đến hình ảnh như thiết bị GSM/máy bộ đàm, thiết bị với ánh sáng huỳnh quang (một trong các nguồn lớn nhất của EMI)… Sử dụng cáp STP để đảm bảo chất lượng hình ảnh trong trường hợp này là cần thiết.

Có nhất thiết phải dùng STP cho hệ thống giám sát an ninh?

Theo kết quả khảo sát, phần lớn các nhà tích hợp đều trả lời là "hiếm khi" hoặc "chưa bao giờ" sử dụng cáp STP cho hệ thống giám sát an ninh. Thực tế, hầu như tất cả các hệ thống cáp Ethernet sử dụng cho giám sát hình ảnh hiện nay đều đang sử dụng cáp UTP.

Hiện nay, cáp STP vẫn chưa được sử dụng phổ biến cho hệ thống giám sát an ninh. Tuy nhiên, tùy theo nhu cầu và môi trường ứng dụng cụ thể, doanh nghiệp có thể cân nhắc để chọn lựa loại cáp STP hay UTP cho phù hợp. Cách sử dụng STP thông minh nhất là dùng cho cáp Ethernet chạy trong những khu vực có "nguy cơ cao" như đã đề cập trong bài và một số trường hợp khác...

Trần Ngọc Thanh
Theo IP Video Market

Lựa chọn tủ rack cho trung tâm dữ liệu

Khi được thiết kế và lắp đặt đúng cách, hệ thống tủ chứa thiết bị chính là nền tảng giúp tăng cường hiệu suất và tính sẵn sàng cao cho hệ thống CNTT; một tài sản mang tính chiến lược trong việc đảm bảo độ tin cậy của TTDL.

Trước đây, hệ thống tủ chứa thiết bị (tủ rack) trong trung tâm dữ liệu (TTDL) chỉ được xem như một sản phẩm đơn giản để sắp xếp và tổ chức các thiết bị khác như máy chủ và thiết bị CNTT... Ngay cả hiện nay, khi nhu cầu thẩm mỹ và tính hiện đại của TTDL ngày càng được chú trọng, một số nhà quản trị vẫn nghĩ tủ rack chỉ là vật trang trí bên trong TTDL. Trên thực tế, tủ rack là một sản phẩm được thiết kế với công nghệ hiện đại, giúp nâng cao hiệu quả của các thiết bị được chứa bên trong và cải thiện đáng kể năng suất làm việc của các nhân sự trong TTDL.

Hệ thống tủ chứa thiết bị là một tài sản chiến lược, một thành phần đóng vai trò quan trọng trong mọi TTDL. Nếu được thiết kế và lắp đặt hợp lý, tủ rack sẽ hỗ trợ việc lắp đặt/thay đổi các thiết bị trong hạ tầng vật lý của hệ thống được nhanh chóng và linh hoạt hơn, đồng thời tăng cường khả năng giám sát và quản lý môi trường hoạt động của thiết bị.

Vấn đề hiện tại

Hiện nay, nhiệm vụ chủ yếu của các nhà quản trị là phải đảm bảo TTDL có thể hoạt động được liên tục 24/7/365. Ngoài ra, dung lượng lưu trữ và hiệu suất của TTDL cũng là những vấn đề đang được quan tâm.

Sự ra đời của các thế hệ máy chủ và thiết bị mạng mật độ cao mới đã làm tăng nhanh số lượng/mật độ thiết bị bên trong tủ rack và mức tiêu thụ năng lượng tổng thể của hệ thống. Mật độ năng lượng trong từng tủ rack đã tăng từ 6 kW trong năm 2006 lên đến 8 kW trong năm 2012 và được dự đoán sẽ tăng lên 12 kW trong năm 2014 (theo *Data Center Users Group*).

Các nhà quản trị TTDL ngày càng quan tâm đến những hệ thống tủ rack cao hơn, sâu hơn, rộng hơn nhằm cung cấp nhiều không gian tổ chức và quản lý thiết bị, thích ứng tốt với những hệ thống CNTT mật độ cao. Ngoài ra, các giải pháp phân phối nguồn và quản lý nhiệt độ cũng được xem xét nhằm nâng cao hiệu suất sử dụng điện của thiết bị bên trong các hệ thống mật độ cao.

Số lượng thiết bị tăng thêm trong các hệ thống mật độ cao gây phát sinh rất nhiều dây nguồn và cáp mạng bên trong tủ. Nếu số lượng lớn thiết bị, dây nguồn và cáp mạng này không được tổ chức tốt, sẽ hạn chế khả năng thao tác và quản lý hệ thống của các nhà quản trị. Ngoài ra, do không có đủ không gian trống bên trong, các luồng khí nóng sẽ không thể

thoát ra ngoài dẫn đến tình trạng quá tải nhiệt độ trên thiết bị.

Độ ẩm và nhiệt độ cao bên trong tủ rack dễ dàng gây ra những sự cố đối với thiết bị trong TTDL. Theo một phân tích của *Ponemon Institute*, một phút TTDL không vận hành gây thiệt hại chi phí xấp xỉ 5.600 USD cho doanh nghiệp. Theo đó, nếu hệ thống gặp một sự cố và không thể vận hành trong 90 phút, chi phí trung bình sẽ lên tới 504.000 USD. Thiệt hại gây ra bởi những sự cố này buộc các nhà quản trị phải tìm ra những phương thức giúp hệ thống có thể vận hành một cách liên tục. Việc tổ chức tốt hạ tầng vật lý, tối ưu hóa khả năng lưu chuyển các luồng không khí nóng/lạnh và giám sát môi trường thông qua màn hình cảm biến được tích hợp ở mặt trước tủ là một trong những giải pháp cần được nhà quản trị cân nhắc.

An ninh cũng là một trong những vấn đề được quan tâm hàng đầu trong TTDL. An ninh ở đây không chỉ là an ninh về mặt thông tin trong hệ thống mạng, mà còn là việc bảo vệ thiết bị khỏi những rủi ro và hư hỏng về mặt vật lý. Chính vì thế, hệ thống khóa bảo vệ ở cửa trước/sau và cửa hông tủ rack đã trở thành một trong những tiêu chuẩn không thể thiếu khi lựa chọn hệ thống tủ chứa thiết bị trong TTDL.

Xu hướng tương lai

Nhu cầu nâng cao hiệu suất hoạt động và bảo đảm độ tin cậy của hệ thống chứa thiết bị trong TTDL đã và đang thúc đẩy sự phát triển của ngành công nghiệp sản xuất sản phẩm này. Các tủ rack được thiết kế ngày càng tiện dụng nhằm hỗ trợ cho việc lắp đặt thiết bị được dễ dàng và nhanh chóng hơn. Hiện tại, việc lắp đặt/tháo gỡ các thiết bị bên trong tủ rack không đòi hỏi nhân sự thực hiện phải có bất kỳ kỹ năng đặc biệt nào, cũng không cần bất kỳ thiết bị chuyên môn nào hỗ trợ. Ưu điểm này giúp việc lắp đặt hoặc thay đổi thiết bị trong các TTDL hiện nay được tiến hành nhanh chóng và dễ dàng hơn bao giờ hết.

Do sự gia tăng về số lượng của các thiết bị hoạt động bên trong TTDL, các loại tủ rack kích thước lớn với chiều cao từ 42U trở lên (1U = 44,45 mm) ngày càng được sử dụng nhiều hơn và đang trở nên phổ biến trong các TTDL trên toàn thế giới.

Các loại thiết bị rack-mount cũng được sản xuất với chiều sâu ngày càng lớn hơn. Nếu như trước đây, các loại máy chủ rack-mount có thể dễ dàng lắp được vào các tủ rack sâu 1.000 mm thì đến hiện tại, việc lắp đặt các loại máy chủ phiến (blade server) đòi hỏi chiều sâu của tủ rack phải là 1.200 mm.

Sự ra đời của các loại thiết bị tản nhiệt bên hông cũng yêu cầu những nhà sản xuất tủ rack phải thay đổi kích thước sản phẩm cho phù hợp. Các loại tủ rack với chiều ngang lên đến 1.000 mm đã xuất hiện và ngày càng trở nên phổ biến trên thị trường. Những loại tủ này hỗ trợ nhiều khoảng không hơn ở hai bên hông thiết bị, giúp các luồng không khí nóng/lạnh có thể di chuyển ra/vào thiết bị dễ dàng hơn. Tuy nhiên, trong những trường hợp này, việc lắp đặt thêm một vài phụ kiện đặc biệt bên trong tủ để bảo đảm các luồng không khí nóng/lạnh có thể di chuyển đúng hướng là cần thiết.

Tủ rack được sắp xếp theo mô hình lối lưu thông không khí nóng/lạnh giúp đảm bảo hiệu suất và tuổi thọ cho các thiết bị bên trong. Đây là mô hình phổ biến và hiệu quả nhất hiện nay, tạo ra những lối lưu thông riêng biệt cho các luồng khí nóng/lạnh trong TTDL. Theo mô hình này, hệ thống tủ rack trong TTDL sẽ được sắp xếp thành những dãy song song sao cho mặt trước và mặt sau của các dãy tủ lần lượt nằm đối diện nhau, hình thành lối lưu thông không khí lạnh (ở giữa hai dãy có mặt trước đối diện nhau) và lối lưu thông không khí nóng (ở giữa hai dãy có mặt sau đối diện nhau). Nhờ đó, luồng không khí nóng thoát ra và luồng không khí lạnh đi vào thiết bị không bị trộn lẫn vào nhau, từ đó nâng cao hiệu suất của giải pháp tản nhiệt, đồng thời tiết kiệm năng lượng tiêu thụ từ các thiết bị làm lạnh.

Yếu tố cần quan tâm

Vấn đề cần được quan tâm nhất khi triển khai hệ thống tủ chứa thiết bị trong TTDL chính là tính linh hoạt và khả năng thích ứng cao. Nhu cầu của khách hàng ngày càng phát triển và đa dạng, ngành công nghiệp tủ rack cũng vì thế mà phát triển theo. Tính linh hoạt và khả năng thích ứng cao của hệ thống tủ chứa thiết bị giúp các nhà quản trị nhanh chóng và dễ dàng phản ứng với những thay đổi trong hạ tầng và ứng dụng trong TTDL. Sau đây là một vài yếu tố cần được xem xét khi triển khai hệ thống tủ chứa thiết bị trong TTDL:

- ***Tải trọng:*** Tải trọng là yếu tố cần được quan tâm đầu tiên khi lựa chọn tủ rack. Dựa vào số lượng máy chủ, thiết bị, phụ kiện, hệ thống cáp mạng và nguồn thường được sử dụng ở mỗi tủ rack trong TTDL, các nhà quản trị nên cân nhắc lựa chọn các loại tủ có tải trọng tối thiểu 1000 kg hoặc 1350 kg với những tủ chứa các thiết bị nặng.
- ***Thanh treo thiết bị 19":*** Hệ thống thanh treo phải dễ dàng điều chỉnh để tương thích với chiều sâu của thiết bị. Các thanh treo phải được thiết kế linh hoạt bảo đảm lắp đặt được hệ thống cáp cho các thiết bị mạng bên trong.
- ***Hệ thống cửa:*** Hệ thống cửa yêu cầu có khóa bảo vệ và được đột lỗ cho độ thông thoáng 64% hoặc cao hơn để cung cấp đủ lượng không khí đi vào và đi ra thiết bị bên trong tủ. Hệ thống cửa trước/sau cũng nên có khả năng đổi chỗ cho nhau nhằm giúp người sử dụng linh hoạt hơn trong việc triển khai lắp đặt hệ thống tủ, đặc biệt là trong các không gian chật hẹp. Các tùy chọn về khóa bảo vệ bằng chìa, mật mã hoặc điện tử cũng nên được cân nhắc kỹ lưỡng.
- ***Cửa hông:*** Nên sử dụng các loại cửa hông có thiết kế hai phần trên/dưới, giúp

dễ dàng lắp đặt và thao tác hơn các loại cửa hông một tấm cồng kềnh trước đây. Hệ thống cửa hông này cũng nên được lắp đặt khóa bảo vệ giống như cửa trước và sau.

• ***Nóc tủ:*** Cần sử dụng những loại tủ có thiết kế các đường cáp vào ở nóc. Các đường cáp vào này phải cung cấp đủ không gian cho tối thiểu 1.500 sợi cáp Cat. 5 hoặc thậm chí là 2.500 sợi đối với các loại tủ chuyên dụng. Những tấm che trên nóc tủ cũng cần được quan tâm nhằm hạn chế bụi và tăng hiệu quả của các giải pháp tản nhiệt trong tủ. Ngoài ra, các nhà quản trị cũng cần quan tâm tới việc lắp đặt hệ thống thang/máng cáp vào nóc tủ sao cho dễ dàng và hiệu quả.

• ***Tính an toàn:*** Nên sử dụng các giải pháp như kết nối tủ với nhau, cố định tủ xuống sàn hoặc lắp đặt thiết bị chống nghiêng để bảo đảm khả năng an toàn của hệ thống trước những nguy cơ vật lý. Yếu tố này đặc biệt quan trọng ở các khu vực có khả năng xảy ra địa chấn cao, hệ thống tủ phải thật vững chắc trước những trận động đất có thể xảy ra.

• ***Phụ kiện:*** Để hệ thống tủ chứa thiết bị trong TTDL phát huy được hết hiệu quả và tính năng của mình, các loại phụ kiện cần được các nhà quản trị quan tâm và sử dụng. Hiện tại trên thị trường các nhà sản xuất tủ rack cung cấp phụ kiện với đầy đủ kích thước và đa dạng về chủng loại. Tuy nhiên chúng ta có thể phân loại chúng thành ba loại phụ kiện chính: phụ kiện hỗ trợ lắp đặt thiết bị (khay cố định, khay trượt...); phụ kiện hỗ trợ quản lý cáp (thanh quản lý cáp ngang, thanh quản lý cáp đứng...); phụ kiện hỗ trợ định hướng không khí (quạt tản nhiệt, thanh lắp khoảng trống...).

Kết luận

Khi được thiết kế và lắp đặt đúng cách, hệ thống tủ chứa thiết bị chính là nền tảng giúp tăng cường hiệu suất và tính sẵn sàng cao cho hệ thống CNTT; một tài sản mang tính chiến lược trong việc đảm bảo độ tin cậy của TTDL. Khi triển khai hệ thống tủ rack, các nhà quản trị TTDL nên lựa chọn những nhà sản xuất có cung cấp đầy đủ những giải pháp toàn diện như: hệ thống quản lý cáp và nhiệt độ, hệ thống hỗ trợ lắp đặt… để bảo đảm hệ thống tủ rack có thể mang lại giá trị cao nhất cho TTDL.

Các nhà quản trị cũng cần thận trọng trong việc cân nhắc kích thước tủ rack, vì các thiết bị CNTT đang được sản xuất với kích thước ngày càng lớn hơn trước. Việc lựa chọn kích thước tủ rack cần dựa trên tính linh động và khả năng tương thích với các thiết bị trong hệ thống, bảo đảm độ tin cậy và chi phí đầu tư thấp nhất, bao gồm cả những chi phí có khả năng phát sinh trong tương lai như xử lý sự cố, thiệt hại... Điều này giúp các nhà quản trị TTDL yên tâm rằng một khi được triển khai, hệ thống tủ rack mới sẽ không chỉ đáp ứng được đầy đủ các yêu cầu ở thời điểm hiện tại mà còn cho cả trong tương lai.

Nguyễn Thanh Tuấn
Theo Emerson Network Power

Tích hợp PoE vào hệ thống mạng

Công nghệ PoE tạo ra một nền tảng đơn giản hỗ trợ cung cấp điện năng và kiểm soát các thiết bị mạng như điện thoại sử dụng IP (VoIP), thiết bị hội nghị truyền hình trực tuyến, điểm truy cập không dây (WAP), camera an ninh…

Hiện nay, Ethernet là một trong những công nghệ được sử dụng phổ biến để kết nối mạng trên toàn thế giới. Công nghệ này sử dụng bốn đôi dây đồng xoắn lại với nhau (cáp Ethernet) để truyền dữ liệu cho nhiều ứng dụng khác nhau, từ Internet băng thông rộng dùng trong gia đình đến các trung tâm dữ liệu (TTDL) của những công ty công nghệ lớn. Đồng thời, cáp Ethernet còn có khả năng truyền tải điện với điện áp thấp an toàn (SELV), giúp tăng cường khả năng kết nối mạng cho cáp Ethernet. Phương pháp truyền tải kết hợp điện năng và dữ liệu (còn được gọi là PoE) mang lại cho người dùng nhiều lợi ích đáng kể so với phương pháp truyền dữ liệu và cung cấp điện năng theo cách thông thường.

Vì sao nên chọn PoE?

Công nghệ PoE tạo ra một nền tảng đơn giản hỗ trợ cung cấp điện năng và kiểm soát các thiết bị mạng như điện thoại sử dụng IP (VoIP), thiết bị hội nghị truyền hình trực tuyến, điểm truy cập không dây (WAP), camera an ninh… Khả năng kết hợp truyền tải dữ liệu và điện năng trên cùng một sợi cáp của PoE đặc biệt hữu dụng để bố trí cho những thiết bị cần cả kết nối mạng và sử dụng điện năng, giúp người dùng khắc phục được hạn chế về mặt kiến trúc thông qua việc loại bỏ bớt dây dẫn điện và các bộ chuyển đổi dòng điện xoay chiều (AC).

Khi mở rộng hệ thống mạng, nhu cầu kéo lại đường dây điện thường gây tốn kém rất nhiều thời gian và chi phí. Do đó, nếu tận dụng khả năng của PoE để loại bỏ bớt nhu cầu sử dụng ổ điện cho từng thiết bị mạng, việc lắp đặt và mở rộng hệ thống mạng sẽ trở nên rất nhanh chóng, dễ dàng, an toàn và hiệu quả hơn rất nhiều, đặc biệt về chi phí.

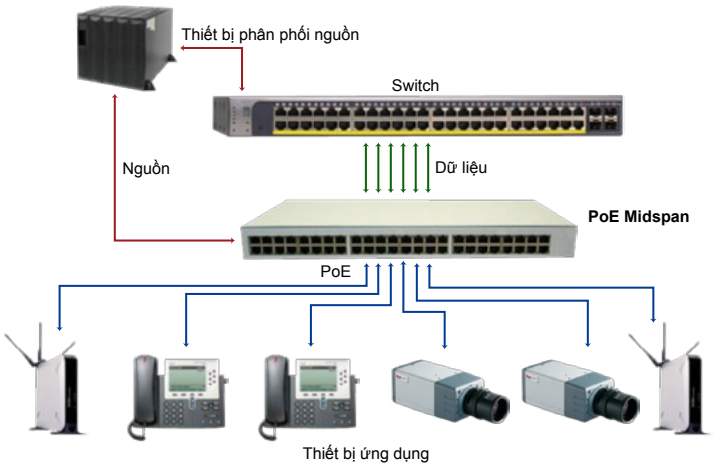
Ngoài ra, PoE còn cung cấp cho người dùng một quy trình xử lý sự cố đơn giản, an toàn và hiệu quả. Ví dụ: với khả năng kiểm soát và truy cập thiết bị từ xa của một camera an ninh có hỗ trợ PoE được lắp đặt ở trên cao, người dùng có thể thao tác hoặc tắt mở nguồn của camera thông qua một máy tính có kết nối mạng. Với những camera thông thường không hỗ trợ tính năng PoE, việc này sẽ phải thực hiện thủ công, gây tổn thất về mặt thời gian và nhân lực và đôi khi là bất khả thi.

Phương pháp tích hợp PoE vào hệ thống mạng

Switch PoE cho phép các nhà quản trị mạng toàn quyền kiểm soát trên mỗi cổng mạng, đồng thời hỗ trợ việc xác định và giải quyết các vấn đề về mạng theo cách đơn giản và dễ dàng hơn, giúp xử lý sự cố nhanh hơn. Tuy nhiên, các switch PoE thường chia sẻ điện năng một cách ngẫu nhiên hơn là thông qua các chỉ số được định trước cho ngõ ra của mỗi cổng. Điều này có thể dẫn đến nguy cơ mất điện nếu có quá nhiều thiết bị đòi hỏi cung cấp đủ điện cùng một lúc. Ngoài ra, các switch PoE thường đắt hơn so với switch truyền thống và không phù hợp cho người dùng chỉ cần một vài cổng PoE.

Phương pháp để tích hợp PoE vào một hệ thống mạng sẵn có là sử dụng thiết bị *midspan* đặt ở giữa các kết nối của switch và thiết bị mạng cần cấp nguồn. Thiết bị trung gian này sẽ cung cấp điện cho các thiết bị mạng trên cáp Ethernet mà không làm gián đoạn các kết nối dữ liệu. Dù được lắp đặt ở giữa switch và thiết bị mạng để bổ sung điện năng cho các kết nối mạng, nhưng *midspan* vẫn duy trì việc truyền tải dữ liệu như thể đang truyền trên một sợi cáp đơn liền mạch (xem hình 1). *Midspan* được thiết kế sẵn với nhiều loại đa dạng để phù hợp với những hệ thống mạng khác nhau từ cá nhân cho đến doanh nghiệp, giúp người dùng không cần thiết kế lại hệ thống mạng của mình mà vẫn có thể sử dụng được công nghệ PoE. Hơn nữa, *midspan* còn xác định cụ thể chỉ số điện năng cho mỗi cổng ở ngõ ra, giúp giảm bớt những sự cố liên quan đến việc chia sẻ nguồn điện khi sử dụng switch PoE.

PoE injector cũng là một giải pháp cấp nguồn PoE. Tuy nhiên, *PoE injector* chỉ tốt hơn so với kiểu cung cấp điện truyền thống do chúng cần được cung cấp nguồn và không có chức năng tự động điều chỉnh điện áp ngõ ra. Do đó, dù *PoE injector* rẻ hơn so với hầu hết các switch PoE và *midspan*, nhưng chúng chỉ được sử dụng trong một số trường hợp đặc biệt khi có nhu cầu kết nối chuyên dụng dành riêng cho thiết bị mạng có hỗ trợ PoE.

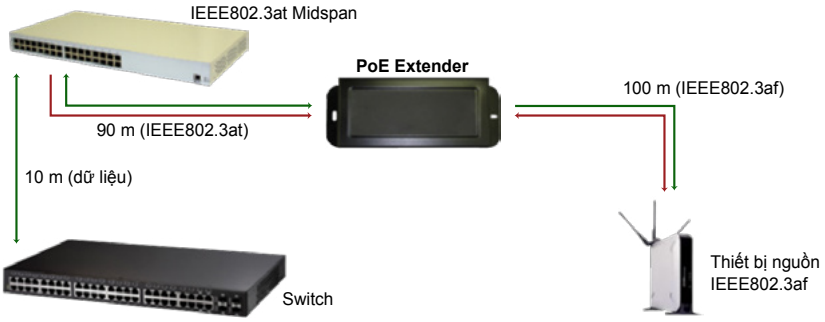


Hình 1: Mô hình kết nối thiết bị PoE Midspan

Các tiêu chuẩn

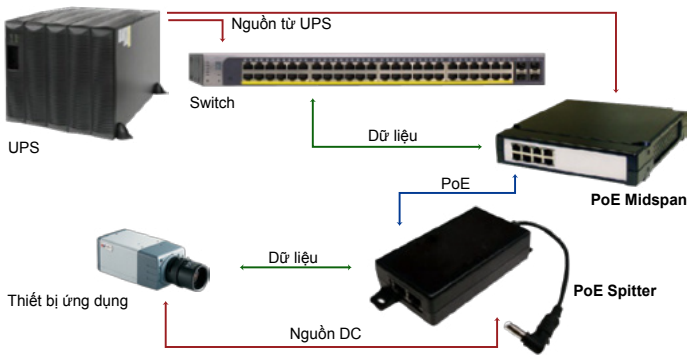
802.3af là chuẩn PoE đầu tiên được phát triển để đáp ứng các vấn đề an toàn liên quan đến việc phát nhiệt trong dây dẫn. Được phê chuẩn vào năm 2003 bởi tổ chức *IEEE*, 802.3af cung cấp cho ngành một tiêu chuẩn PoE chính thức, phù hợp với các ứng dụng đòi hỏi nguồn lên đến 12,95 Watt (W). Trong tiêu chuẩn này, IEEE quy định các ngõ ra của PoE nên là 15,4 W để đảm bảo suy hao trong suốt chiều dài của dây dẫn. Đồng thời, chuẩn cũng quy định độ dài tối đa để truyền được PoE là 100 m (330 feet) hoặc ít hơn theo giới hạn về chiều dài của cáp Ethernet nhằm đảm bảo hiệu quả truyền dữ liệu và điện năng cho thiết bị.

Trong năm 2009, IEEE phê chuẩn tiêu chuẩn 802.3at. Tiêu chuẩn mới này vẫn duy trì các yêu cầu liên quan đến việc phát hiện và kết nối của tiêu chuẩn 802.3af, nhưng mở rộng hơn khả năng của PoE bằng cách nâng mức điện năng cung cấp cho các ứng dụng mạng lên đến 25,95 W. Để đảm bảo khả năng tương thích ngược với các ứng dụng mạng hiện có, IEEE cũng bắt buộc các thiết bị *midspan* và switch PoE được sản xuất theo 802.3at phải có khả năng phát hiện tải của 802.3af và phải tự động giảm lượng điện năng của các ứng dụng về mức thích hợp.



Hình 3: PoE Extender giúp tăng khoảng cách truyền PoE và dữ liệu

Gần đây, một số nhà sản xuất đã cho ra mắt thiết bị *midspan* và switch PoE có khả năng cung cấp điện năng ngõ ra cao hơn so với tiêu chuẩn của IEEE, nhưng các bổ sung khác cho tiêu chuẩn hiện hành vẫn chưa được soạn thảo. Một số sản phẩm này đã được thiết kế để tương thích với tiêu chuẩn 802.3 hiện hành liên quan đến việc dò tìm, kết nối và quy định về điện năng, nhưng một số thiết bị khác lại không làm được điều này. Do đó, những ai đang có ý định triển khai thiết bị *midspan* hoặc switch PoE để cung cấp điện hơn 25,95 W cho mỗi ổ cắm nên làm việc trực tiếp với nhà sản xuất thiết bị nhằm xác định xem những thiết bị này có thích hợp với các ứng dụng mà mình dự định triển khai hay không.



Hình 2: PoE Splitter tách biệt đường truyền PoE và dữ liệu

Khả năng phát hiện và kết nối

Một ưu điểm khác nữa của PoE là xử lý an toàn. Cả hai tiêu chuẩn 802.3af và 802.3at đều yêu cầu hệ thống PoE có trở kháng bên trong là 25 kilo-ohm, giúp phát hiện mức điện năng của các ứng dụng mạng là bao nhiêu, sau đó điều chỉnh cho phù hợp. Trước khi cấp nguồn cho các thiết bị mạng, bộ nguồn của thiết bị PoE sẽ phát hiện và xác định mức trở kháng, phân loại các thiết bị mạng dựa trên lượng điện năng yêu cầu để xem xét và xác định tải thích hợp. Ví dụ: một *midspan* có khả năng cung cấp 15,4 W cho mỗi cổng, trong thực tế thiết bị mạng chỉ cần sử dụng 8 W là hoạt động tốt, *midspan* sẽ tự động giảm mức điện năng ở ngõ ra của cổng đó về mức điện năng phù hợp với thiết bị để bù vào sự suy hao dọc theo chiều dài của cáp. Việc "bắt tay" này đảm bảo cho kết nối được chắc chắn đúng và an toàn. Nếu bất kỳ yếu tố nào của quá trình này bị gián đoạn hoặc có bất kỳ lỗi nào xảy ra, bộ cấp nguồn tuân thủ theo chuẩn 802.3 sẽ không thực hiện việc cung cấp điện năng cho các thiết bị mạng.

Kết nối với thiết bị không tích hợp PoE

Một số thiết bị trong hệ thống mạng của cá nhân và doanh nghiệp không được thiết kế để nhận dữ liệu và nguồn điện trên cùng một cổng. Những thiết bị này mặc dù không nhất thiết phải tuân theo PoE, nhưng đôi khi vẫn có thể tích hợp chúng chung với hệ thống mạng PoE mới thiết lập hoặc hệ thống mạng PoE hiện có thông qua các *splitter*. Các *splitter* này sẽ chia tách nguồn điện và dữ liệu được truyền tải trên cáp Ethernet, và thực hiện việc cấp nguồn cho các thiết bị này thông qua hai kết nối riêng biệt–một cáp Ethernet dành cho ngõ ra theo chuẩn của dữ liệu và một dây DC (direct current) được bấm vào đầu nối chuẩn (xem hình 2). *Splitter* cũng có thể phát hiện và giảm điện áp cho các thiết bị mạng không yêu cầu đầu ra 44 đến 57 DC (mức điện áp thường được yêu cầu bởi các thiết bị có hỗ trợ PoE).

Có rất nhiều các *splitter* tương thích với chuẩn 802.3af và có thể sử dụng chúng với bất kỳ thiết bị *midspan* hoặc switch nào (xem hình 2). Tuy nhiên, khi kết hợp các *splitter* vào hệ thống mạng đang hoạt động ở mức điện năng cao hơn tiêu chuẩn 802.3at, các chuyên gia khuyên người dùng nên mua các *splitter* từ cùng một nhà sản xuất với thiết bị *midspan* của họ. Tiêu chuẩn cho các thiết bị có giao tiếp với nhau theo nhiều cách, do đó các thiết bị được

sản xuất bởi các nhà sản xuất khác nhau có thể giao tiếp với nhau không đúng cách. Ví dụ, nếu một *splitter* được lắp đặt trong hệ thống mạng theo chuẩn 802.3at sử dụng phương thức phát hiện và kết nối khác so với phương thức của thiết bị switch PoE hoặc *midspan*, cụ thể như phương thức phát hiện dựa trên phần mềm sẽ khác với phương thức phát hiện dựa trên phần cứng. Kết quả là bộ cấp nguồn PoE sẽ không truyền tải điện năng đến các thiết bị mạng hoặc không chấp nhận chuẩn 802.3at, đồng thời thực hiện việc cấp nguồn cho ngõ ra theo chuẩn 802.3af (do khả năng tương thích ngược), điều này sẽ dẫn đến tình trạng không cung cấp đủ điện năng để cho cả hai thiết bị đầu cuối và *splitter* cùng hoạt động.

Các *splitter* thế hệ mới đã được thiết kế với ngõ ra kép cung cấp cho người dùng khả năng cấp nguồn cho nhiều thiết bị từ một sợi cáp Ethernet duy nhất tại một vị trí nào đó, điều này sẽ rất thuận tiện cho các ứng dụng như camera an ninh.

Mở rộng hệ thống mạng

Hạn chế chính của công nghệ PoE và kết nối mạng sử dụng cáp Ethernet là không thể mở rộng xa hơn 100 m (330 feet) tính từ switch (như tiêu chuẩn IEEE 802.3 đã quy định nhằm giảm thiểu việc mất dữ liệu). Giải pháp để cung cấp điện năng cho các thiết bị mạng vượt quá khoảng cách đã quy định là phải di chuyển switch PoE hiện có đến điểm tập trung thiết bị mạng hoặc mua thêm switch phụ để phục vụ cho phần mở rộng, nhưng cả hai giải pháp này đều là những lựa chọn tốn kém.

Trên thị trường hiện nay đã có một sản phẩm mới–*PoE extender* có khả năng cung cấp cho người dùng giải pháp để mở rộng phạm vi hoạt động của một mạng PoE. *PoE extender* là thiết bị có khả năng truyền tải điện năng và dữ liệu đáng tin cậy trên cáp Ethernet, giúp tăng độ dài tối đa lên gấp đôi mà không cần phải di chuyển hoặc bổ sung thiết bị *midspan* hoặc switch PoE vào hệ thống mạng (xem hình 3). *PoE extender* hoạt động theo cách thức tương tự như thiết bị switch PoE nhưng có chi phí thấp hơn, do chúng có sẵn nhiều tùy chọn từ một cổng đến nhiều cổng, có thể hoạt động mà không cần bộ chuyển đổi bên ngoài và không yêu cầu thêm hệ thống quản lý hoặc phần mềm phức tạp. Khi hợp nhất thành một mạng PoE, thiết bị này có thể tái tạo và truyền tải điện năng, dữ liệu đến các thiết bị mạng với khoảng cách xa lên đến 200 m (660 feet) tính từ thiết bị switch.

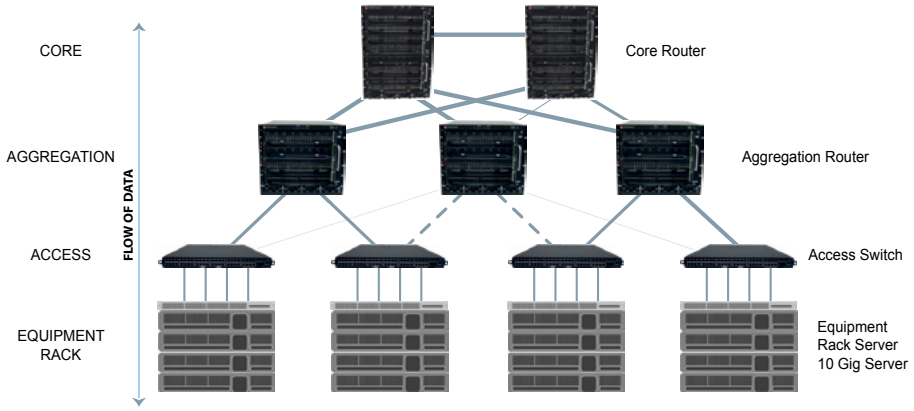
Kết luận

Công nghệ PoE cung cấp cho người dùng phương pháp lắp đặt và mở rộng hệ thống mạng một cách dễ dàng, an toàn, hiệu quả chi phí trong việc truyền tải điện năng và dữ liệu cho một loạt các thiết bị mạng. Đây là một sự lựa chọn tuyệt vời cho cả hai hệ thống mạng PoE mới hoàn toàn và hệ thống mạng PoE sẵn có của các cá nhân, gia đình và doanh nghiệp.

Đông Minh
Nguồn BICSI

Tổ chức trung tâm dữ liệu hiệu quả với kiến trúc VToR

Với những ưu điểm: độ trễ thấp, độ sẵn sàng cao, chi phí thấp và hỗ trợ nhu cầu mở rộng cơ sở hạ tầng, Ethernet fabric và kiến trúc VToR là những giải pháp thông minh giúp nâng cao hiệu quả tổ chức TTDL



Hình 1: Phương thức truyền dữ liệu trong kiến trúc mạng ba tầng truyền thống

Một trung tâm dữ liệu (TTDL) được tổ chức tốt phải có độ sẵn sàng cao nhằm thỏa mãn những yêu cầu lưu trữ linh hoạt, các ứng dụng mới, đồng thời đáp ứng nhu cầu chuyển đổi của doanh nghiệp và khách hàng của họ. Hiệu suất sử dụng không gian, độ trễ thấp và quản lý năng lượng hiệu quả là những yếu tố đảm bảo một TTDL được tổ chức tốt. Trong bài viết này, chúng tôi sẽ đề cập về khái niệm *Ethernet fabric* và vai trò của kiến trúc VToR (Virtual Top-of-Rack) trong việc nâng cao hiệu quả tổ chức TTDL.

Fabric Ethernet

Mạng Ethernet thông thường bao gồm một hệ thống phân cấp nhiều tầng, thường bị quá tải băng thông tại mỗi tầng. Mô hình này thường được dùng để thiết kế mạng Fast Ethernet, client-server tốc độ 1 Gbps, nơi thường sử dụng thiết bị switch Ethernet tốc độ 10 Gbps.

Phương thức truyền dữ liệu trong kiến trúc mạng ba tầng truyền thống làm tăng độ trễ kết nối từ *server* đến *server*, cản trở sự di chuyển của các máy ảo trong mạng và đòi hỏi việc quản lý hệ thống mạng phức tạp hơn. Trong khi đó, *Ethernet fabric* tạo nên một tài nguyên mạng linh động, dễ dàng đáp ứng nhu cầu di chuyển của các máy ảo và lượng băng thông lớn trong môi trường TTDL ảo hóa.

Thuật ngữ *"Ethernet fabric"* đề cập đến sự phát triển của mạng Ethernet từ mô hình mạng ba tầng truyền thống đến kiến trúc mạng *mesh* ngang hàng *layer 2*. Với mô hình ba tầng truyền thống trong trung tâm dữ liệu (TTDL) không sử dụng công nghệ ảo hóa, hầu hết các luồng dữ liệu được truyền từ *"trên xuống dưới"*–nghĩa là từ server đến người dùng, hoặc từ *server* đến *storage* bằng cách sử dụng các *router*. Trong môi trường TTDL ảo hóa mật độ cao, các luồng dữ liệu rất lớn được truyền ngang hàng từ *"bên này sang bên kia"*–truyền từ *server* đến *server* thông qua đường trục rút ngắn.

Ethernet fabric có giá thành thấp, tốc độ cao, độ trễ thấp, ít thất thoát dữ liệu hơn và hỗ trợ khả năng mở rộng cơ sở hạ tầng mạng. *Ethernet fabric* có thể cung cấp một kết nối 1 Gbps hoặc 10 Gbps, cho phép các *server* có thể tính toán và lưu trữ dữ liệu nhằm tối đa hóa năng lực tích hợp với chi phí hiệu quả nhất.

Ethernet fabric là một thiết kế mạng thông minh cho phép các thiết bị *router* hoặc *switch layer 3* có thể giao tiếp với nhau nhằm xác định đường đi ngắn nhất trong hệ thống mạng; chúng còn có khả năng mở rộng khi cần tăng số lượng *server*. Ứng dụng này cung cấp độ tin cậy tuyệt đối và băng thông sẵn sàng để người dùng có thể sử dụng bất cứ thời điểm nào.

Kiến trúc Virtual Top of Rack

Virtual Top of Rack (VToR) là một kiến trúc TTDL được thiết kế nhằm cung cấp kiến trúc *Ethernet fabric* ngang hàng, với độ trễ thấp, chi phí thấp và ít tiêu hao điện năng.

Chi phí thấp, tiết kiệm điện năng

Trong kiến trúc này, các *switch ToR (Top of Rack)* truyền thống tại mỗi tủ rack được thay thế bằng một *patch panel (phiến đấu nối)* và kết nối thẳng đến *core router*. Thiết kế này tiết kiệm chi phí cho hệ thống làm mát, giảm tiêu hao điện năng và chi phí mua sắm thiết bị *switch* tại mỗi tủ rack so với kiến trúc ToR thông thường.

Độ sẵn sàng cao

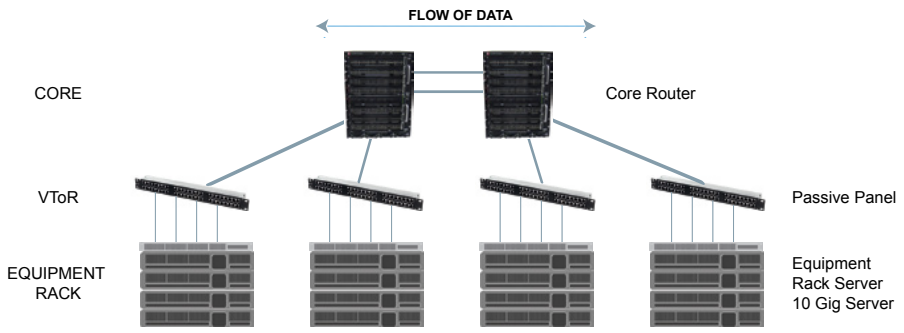
Bên cạnh đó, việc loại bỏ những thiết bị *switch* tại mỗi tủ rack cũng giúp loại bỏ các lỗi tiềm tàng do những *switch* này gây ra (như quá tải nguồn điện, lỗi phần cứng), giúp tăng cường độ sẵn sàng cho TTDL và đơn giản hóa kiến trúc kết nối ngang hàng.

Độ trễ thấp

Khả năng giảm độ trễ truyền dẫn dữ liệu cũng là một ưu thế lớn của kiến trúc VToR. Thông thường trước khi dữ liệu được truyền đi, các thiết bị định tuyến sẽ kiểm tra và xác định đường đi cho gói tin. Quá trình này chính là nguyên nhân làm tăng độ trễ đường truyền. Kiến trúc VToR thực hiện việc chuyển mạch và định tuyến trong cùng một *chassis* tại tầng *core*, giúp loại bỏ quá trình tính toán và định tuyến đường đi giữa hai thiết bị định tuyến, đồng thời loại bỏ khoảng cách giữa các *switch* và nhờ đó, giảm thiểu tối đa độ trễ đường truyền.

Công nghệ đa kết nối

Nhiều giải pháp VToR trên thị trường hiện nay thường hướng đến việc dùng cáp đồng thay vì cáp quang. Thực tế,



Hình 2: Phương thức truyền dữ liệu trong kiến trúc VToR

công nghệ cáp quang hỗ trợ tối ưu cho những ứng dụng yêu cầu tốc độ cực cao và độ trễ tối thiểu trên một khoảng cách đáng kể. Nhưng trong TTDL, cáp đồng vẫn được sử dụng phổ biến để kết nối các *switch*, công nghệ cáp đồng *MRJ21 XG* cung cấp tốc độ lên đến 10 Gbps cùng với mật độ kết nối cao giữa các tủ rack chứa *server* và tủ rack chứa thiết bị mạng.

Cáp trục *MRJ21 XG* được bấm sẵn tại nhà máy giúp giảm 37% không gian trong tủ rack so với cáp đôi xoắn truyền thống. Cáp trục được gắn lên phiến *MRJ21 XG* trên mỗi tủ rack, cung cấp các cổng cắm giao diện RJ45, hỗ trợ sử dụng dễ dàng với các dây đấu nối Cat. 6A. Lợi ích của công nghệ *MRJ21 XG* còn được nhận thấy ở kết nối 10 Gbps với khoảng cách lên đến 30 m giữa tủ rack chứa *server* và tủ rack chứa core *router/switch*.

Việc triển khai MRJ21 1 Gbps dạng phiến trong mô hình VToR giúp tăng mật độ cổng trong một kết nối lên 24 cổng, gấp sáu lần đầu nối RJ45 thông thường. Mỗi *router blade* có thể chứa đến 8 phiến MRJ21 1 Gbps, tương đương 48 cổng trên một *blade*, nghĩa là sẽ có tối đa 1.536 cổng trên một *router* 32 slot. Sử dụng công nghệ MRJ21 1 Gbps cũng giúp giảm đáng kể lượng cáp ngang (một sợi cáp trục *MRJ21 XG* có thể sử dụng cho 24 kết nối RJ45), giúp tăng cường độ thông thoáng, giảm chi phí cho hệ thống làm mát trong tủ rack cũng như trong TTDL.

Kết luận

Với những ưu điểm: độ trễ thấp, độ sẵn sàng cao, chi phí thấp và hỗ trợ nhu cầu mở rộng cơ sở hạ tầng, *Ethernet fabric* và kiến trúc VToR là những giải pháp thông minh giúp nâng cao hiệu quả tổ chức TTDL. Đồng thời, việc triển khai công nghệ đa kết nối trong kiến trúc VToR sẽ giúp tăng mật độ cổng kết nối, giảm thiểu không gian sử dụng, tăng cường độ thông thoáng, giảm chi phí làm mát và nâng cao hiệu quả TTDL.

Lưu Lê Qui Nhơn
Theo TE Connectivity

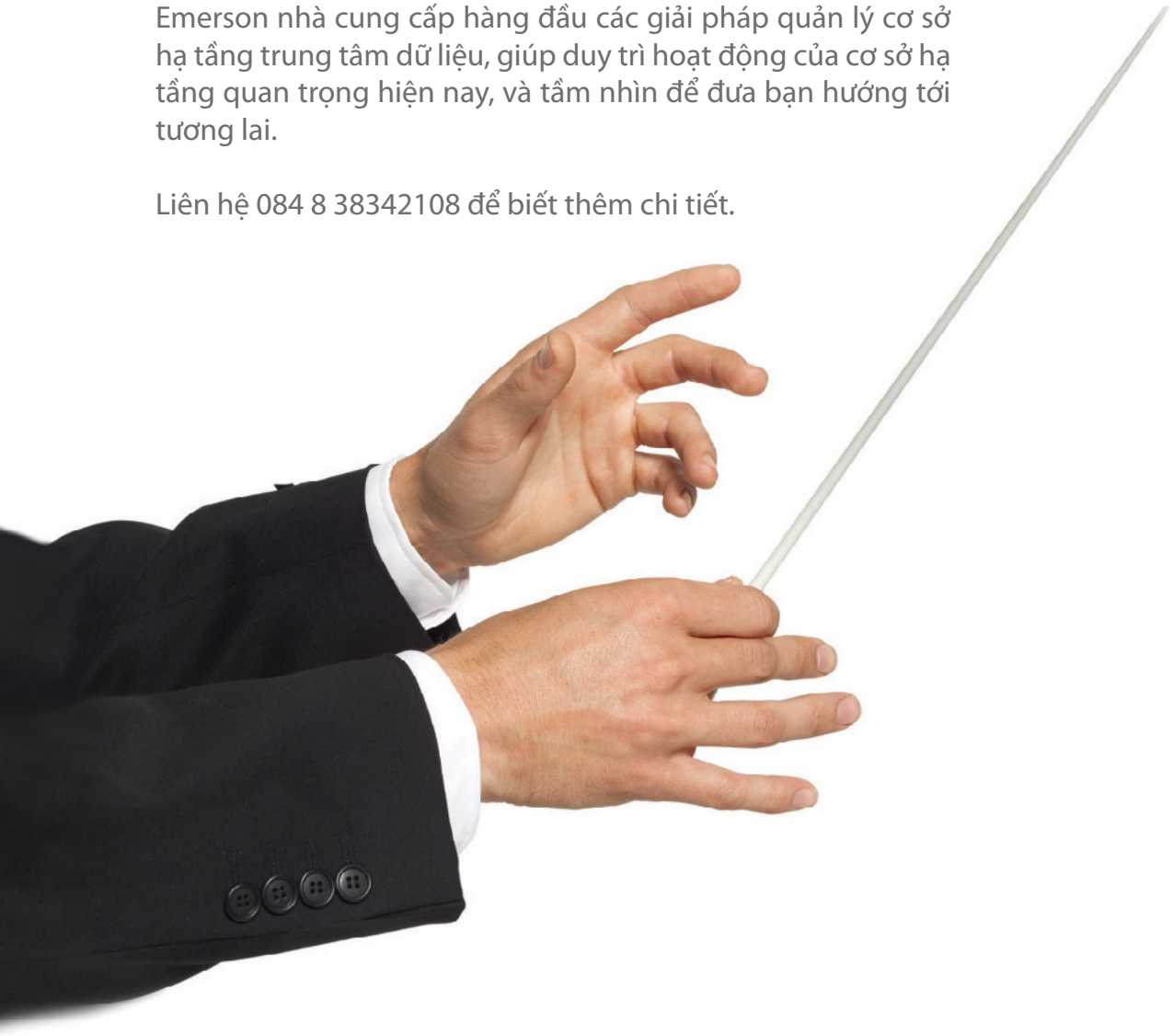
EMERSON
Network Power

NẮM QUYỀN KIỂM SOÁT TRUNG TÂM DỮ LIỆU NĂNG ĐỘNG...
HAY ĐỂ TRUNG TÂM DỮ LIỆU KIỂM SOÁT BẠN.

ĐÓ LÀ SỰ KHÁC BIỆT SỐNG CÒN.

Emerson nhà cung cấp hàng đầu các giải pháp quản lý cơ sở hạ tầng trung tâm dữ liệu, giúp duy trì hoạt động của cơ sở hạ tầng quan trọng hiện nay, và tầm nhìn để đưa bạn hướng tới tương lai.

Liên hệ 084 8 38342108 để biết thêm chi tiết.



www.EmersonNetworkPower.Asia
www.nsp.com.vn/Avocent

ẤN PHẨM TẶNG, KHÔNG DÙNG CHO MỤC ĐÍCH THƯƠNG MẠI

EMERSON. CONSIDER IT SOLVED.™