ระบบรักษาความปลอดภัย บริการ และความเร็ว

ภาค 1 : โครงสร้าง

เราเตอร์บริการเบ็ดเสร็จรุ่นใหม่จากซิสโก้ สามารถรองรับบริการข้อมูล เสียง และวิดีโอได้พร้อมๆ กัน โดยมีความเร็วระดับสายแถมยังปลอดภัยอีกด้วย

เมื่อเดือนสิงหาคมที่ผ่านมาซิสโก้เปิดตัวเราเตอร์รุ่นล่าสุดของตนเองออกมา เราเตอร์รุ่นนี้มีการออกแบบขึ้นมาใหม่หมดเพื่อสนองตอบต่อความต้องการของสาขา รวมทั้งธุรกิจขนาดเล็กและขนาดกลาง (SMB) ที่เพิ่มสูงขึ้นเรื่อยๆ เราเตอร์ Integrated Services Routers แบ่งออกเป็นรุ่น 1800, 2800 และ 3800 ได้รวมเอาระบบสื่อสารผ่านไอพี, เครือข่ายส่วนตัวเสมือน (virtual private network - VPN), ไฟร์วอลล์, ระบบป้องกันและแยกแยะการบุกรุก รวมทั้งบริหารอื่นๆ อีกมากไว้ในแพลตฟอร์มประสิทธิภาพสูงเพียงชุดเดียว การผสมผสานบริการต่างๆ อย่างกลมกลืน และยังมีการออกแบบที่มีเอกลักษณ์เฉพาะตัว ช่วยแบ่งเบาภาระการเข้ารหัสจากซีพียูไปยังชิปแยกต่างหากเพื่อช่วยให้การประมวลผลรวดเร็วยิ่งขึ้น ช่วยให้บริการต่างๆ ทำงานได้พร้อมกัน แถมยังมีช่องทางให้เติบโตต่อไปในอนาคตอีกด้วย แม้ว่ามีผู้เข้ามาใช้ระบบ WAN มากเกินกว่าที่กำหนดเอาไว้ก็ตาม โดยผู้ที่มีโอกาสทดสอบรายหนึ่งรายงานว่าใช้งานซีพียูแค่ร้อยละ 74 เท่านั้น

บริการที่ความเร็วสาย

ซิสโก้ได้ทำการสำรวจความเห็นของสาขาและลูกค้า SMB กว่า 300 ราย เพื่อแยกแยะความต้องการของตลาดสำหรับนำมาปรับปรุงเราเตอร์รุ่นใหม่ Mike Stallone ผู้จัดการสายผลิตภัณฑ์ของซิสโก้กล่าวว่า "เราถามลูกค้าว่าพวกเขาต้องการอะไร แล้วเราก็พัฒนาสินค้าออกมาตามนั้น" ซิสโก้ได้นำเอาบริการและคุณสมบัติต่างๆ มากกว่าครึ่งหนึ่งที่ลูกค้าต้องการมารวมอยู่ในเราเตอร์ แทนที่ลูกค้าจะต้องซื้ออุปกรณ์แยกจากกัน สิ่งที่ลูกค้าต้องการมากที่สุดก็คือคุณสมบัติเกี่ยวกับระบบรักษาความปลอดภัย เช่น ไฟร์วอลล์, VPN, ระบบป้องกันและแยกแยะการบุกรุก และซอฟต์แวร์ป้องกันไวรัสตามลำดับ ความต้องการอันดับต่อมาก็คือ ระบบโทรศัพท์ไอพี, ระบบบีบอัดข้อมูล ระบบกลั่นกรองเนื้อหาข้อมูล ระบบทำแคช คุณภาพของการให้บริการ (quality of service -QoS) ระบบสตรีมมิงและระบบมัลติคาสติง

ซิสโก้ได้นำเอาเราเตอร์ Integrated Services Router รุ่นก่อนหน้านี้ซึ่งประกอบด้วยรุ่น 1700, 2600 และ 3700 มาปรับปรุงเป็นเราเตอร์รุ่นใหม่ที่ Stallone เรียกว่า "การเข้ารหัสที่ความเร็วสาย" งานการเข้ารหัสและถอดรหัสจะถูกย้ายจากโพรเซสเซอร์กลางไปสู่ชิปแบบผนวกที่ออกแบบมาเฉพาะสำหรับแอพพลิเคชัน (ASICs) ในเราเตอร์รุ่น Cisco 2800 และ 3800 และย้ายไปสู่ field-programmable gate array (FPGA) ในเราเตอร์รุ่น Cisco 1800 ซึ่งถือเป็นการย้ายการทำงานจากซอฟต์แวร์ไปสู่ฮาร์ดแวร์โดยตรง การที่เข้ารหัสและถอดรหัสเป็นสิ่งที่สิ้นเปลืองประสิทธิภาพในการประมวลผลอย่างมาก ดังนั้นวิธีการนี้จึงช่วยให้ประสิทธิภาพของซีพียูดีขึ้นอย่างมาก รวมทั้งช่วยให้ผู้ใช้ใช้บริการต่างๆ ได้พร้อมกันอย่างที่ไม่เคยทำได้มาก่อนอีกด้วย

Chris Fairbanks หัวหน้าสถาปนิกระบบเครือข่ายของบริษัท ePlus และลูกค้าที่ใช้ Cisco 3825 Router

ถ้าหากวัดประสิทธิภาพของการเข้ารหัสแล้ว เราจะพบว่า Cisco 1841 Router สามารถรองรับช่องทางการเชื่อมต่อผ่าน VPN ได้ถึง 800 ช่องทาง ส่วนเราเตอร์ Cisco 2800 รับได้ 1,500 ช่องทาง และเราเตอร์ Cisco 3845 รับได้ 2,500 ช่องทาง

Mike Wood ผู้จัดการสายผลิตภัณฑ์ Integrated Services Routers ของซิสโก้กล่าวว่า ASIC และ FPGA ยังมีสวิตซ์ที่สามารถส่งสตรีมสัญญาณเสียงไปยังส่วนประกอบต่างๆ ในแผงวงจรหลักได้ หรือส่งไปยังโมดูลที่เสียบต่อในสล็อตของเราเตอร์ก็ได้ นอกจากนั้นชิปพิเศษเหล่านี้ยังช่วยให้มีการเรียกใช้หน่วยความจำโดยตรงระหว่างชิปประมวลผลสัญญาณดิจิตอล (digital signal processors - DSP) และหน่วยความจำของตัวเครื่อง ซึ่งเท่ากับเป็นการแบ่งเบาภาระของซีพียูเพิ่มขึ้นไปอีก

การผสานบริการเพื่อสนองความต้องการในอนาคต

แม้ว่าเราเตอร์รุ่นใหม่เหล่านี้มีประสิทธิภาพที่ดีขึ้นก็ตาม แต่จุดเด่นที่แท้จริงก็คือการผสานบริการต่างๆ เข้าด้วยกันมากกว่า เราเตอร์ Cisco 1800 และ 2800 ใช้ระบบปฏิบัติการ Cisco IOS Software Release 12.3(8)T ส่วนเราเตอร์ Cisco 3800 ใช้ระบบปฏิบัติการ IOS Release 12.3(11)T มีการนำเอาคุณสมบัติด้านการรักษาความปลอดภัยจำนวนมากมาใส่เอาไว้ในแผงวงจร

หลัก เช่น Network Admission Control (NAC) เพื่อใช้ป้องกันไวรัสและป้องกันการบุกรุก เป็นต้น

เราเตอร์ Cisco 2800 และ 3800 ยังสามารถทำงานเป็น PBX หรือคีย์ซิสเต็มส์ขนาดเล็ก เพื่อรองรับระบบข่าวสารเสียงได้โดยใช้ Cisco CallManager Express (แอพพลิเคชัน IOS ชนิดหนึ่ง) และ Cisco Unity Express เราเตอร์เหล่านี้ยังจัดเป็นเราเตอร์รุ่นแรกที่ผสานสล็อต DSP ลงไปในเราเตอร์โดยตรงอีกด้วย สล็อต DSP สามารถเปิดการทำงานได้โดยใช้ packet voice/fax DSP modules (PVDMs) เพื่อรองรับการทำงานของคุณสมบัติเรื่องการประชุมร่วมกัน, transcoding และระบบรักษาความปลอดภัย

เราสามารถผสานบริการต่างๆ เพิ่มขึ้นได้โดยการเพิ่มโมดูลอื่นๆ ซึ่งมีคุณสมบัติต่างออกไป อาทิ advanced integration modules (AIMs), โมดูลระบบเครือข่าย หรือ enhanced network modules (NMEs) และการ์ดเชื่อมต่อเครือข่าย WAN ความเร็วสูง (high-speed WAN interface cards - HWICs) เป็นต้น นอกจากนั้นเราเตอร์ Cisco 2821 และ 2851 ยังมีสล็อตพิเศษสำหรับใส่ extension voice modules (EVMs) เพื่อรองรับระบบสื่อสารเสียงอะนาล็อกและ BRI ได้โดยที่ไม่ต้องสละสล็อตโมดูลระบบเครือข่าย นอกจากนั้น EVM ยังทำงานในสล็อต NME ใดๆ ของเราเตอร์ 3800 ได้ด้วย เราเตอร์เหล่านี้ยังมีพอร์ตฟาสต์อีเทอร์เน็ต และ/หรือกิกะบิตอีเทอร์เน็ต รวมทั้งพอร์ต USB ในตัวอีกด้วย

Brian Ryder ผู้จัดการสายผลิตภัณฑ์และสถาปนิก Integrated Services Router กล่าวว่า "ความต้องการของลูกค้าเพิ่มขึ้นอยู่ตลอดเวลา ในช่วงแรกๆ ผู้ใช้ส่วนใหญ่ต้องการแค่ระบบรักษาความปลอดภัยและระบบเสียงไอพีเท่านั้น แต่ในตอนนี้พวกเขาต้องการระบบรักษาความปลอดภัย (ระบบป้องกันการบุกรุก, VPN ที่เข้ารหัส, Network Admission Control) รวมทั้งยังต้องการระบบแจกจ่ายซอฟต์แวร์ ระบบจัดการข่าวสาร ระบบทำแคชข้อมูลโลคอลและอื่นๆ อีกมาก การเตรียมสล็อตเหล่านี้เอาไว้ช่วยให้ลูกค้าได้รับบริการทั้งหมดที่พวกเขาต้องการได้"

Ryder ยังบอกอีกว่า "คุณสมบัติแต่ละชนิดทำงานประสานกับคุณสมบัติอื่นๆ ในเราเตอร์ แต่ถ้าหากเป็นสภาพแวดล้อมในการใช้อุปกรณ์เป็นชิ้นๆ แล้ว คุณสมบัติเหล่านี้อาจไม่รู้จักกันก็ได้ ตัวอย่างเช่น ถ้าหากไม่มีการผสานฟังก์ชันเหล่านี้เข้าด้วยกันแล้ว ฟังก์ชันที่ใช้เซตอัพ VPN อาจไม่รู้จัก QoS ก็ได้ ดังนั้นมันจึงไม่อาจจัดสรรแพ็กเก็ตอย่างที่กำหนดเอาไว้ก่อนได้ คุณสามารถทำสิ่งต่างๆ เหล่านี้ได้โดยใช้แพลตฟอร์มแบบเบ็ดเสร็จ แต่การใช้อุปกรณ์แยกจากกันไม่อาจทำงานแบบนี้ได้"

David Willis นักวิเคราะห์อาวุโสของบริษัทวิจัย เมต้า กรุ๊ป กล่าวว่า คุณสมบัติที่บริการต่างๆ รู้จักกันไม่เพียงแต่มีประโยชน์เท่านั้น แต่ยังมีความสำคัญอย่างมาก เขากล่าวว่า "Cisco Integrated Services Routers มีระบบอัจฉริยะที่ใช้แยกแยะและสั่งงานแอพพลิเคชันบางอย่างได้อย่างเต็มประสิทธิภาพได้ ตัวอย่างเช่น ระบบสามารถแยกแยะได้ว่าแอพพลิเคชันจำเป็นต้องใช้การจัดลำดับความสำคัญ QoS หรือไม่ จากนั้นก็จัดสรรเทคโนโลยีบางอย่างเข้าไปเพื่อสร้างความมั่นใจว่าสามารถเรียกใช้ระบบเครือข่ายในระดับที่ต้องการได้ แถมระบบยังใส่ขั้นตอนการบีบอัดข้อมูลให้แก่สัญญาณของแอพพลิเคชันบางอย่างได้ด้วย"

ระบบรักษาความปลอดภัยแบบเบ็ดเสร็จ

สิ่งที่ผู้ตอบแบบสอบถามให้ความสำคัญสูงสุดก็คือเรื่องของระบบรักษาความปลอดภัย ดังนั้นเราเตอร์รุ่นใหม่จึงเน้นไปที่การรักษาความปลอดภัยของการสื่อสาร การป้องกันภัย การรักษาความลับและตัวตนของผู้ใช้ และการปกป้องโครงสร้างพื้นฐานของระบบเครือข่าย การรักษาความปลอดภัยของระบบสื่อสารกระทำผ่านช่องทาง VPN และการเข้ารหัส, dynamic multipoint VPN (DMVPN), Easy VPN, voice, video and data VPN (V3PN) และคุณสมบัติ multi-VPN Routing and Forwarding (multi-VRF)

Willis กล่าวว่า DMVPN จัดเป็นคุณสมบัติที่น่าสนใจอย่างยิ่ง "วิธีการนี้ทำให้ผู้ใช้ต้องเปลี่ยนมุมมองเกี่ยวกับ VPN เสียใหม่ ในอดีต ถ้าหากเราใช้ VPN ผ่านอินเทอร์เน็ต การบริหารจัดการเป็นเรื่องที่เสียเวลาและยุ่งยากอย่างมาก องค์กรขนาดใหญ่มักจะใช้โซลูชันส่วนตัว เช่น MPLS หรือระบบเครือข่ายเฟรมรีเลย์ แต่ DMVPN ช่วยให้ VPN ผ่านอินเทอร์เน็ตทำงานได้ดีขึ้น การเซตอัพ และการปิดการทำงานจะเป็นไปแบบอัตโนมัติ ซึ่งช่วยให้องค์กรขนาดใหญ่สามารถใช้อินเทอร์เน็ตได้ แถมยังช่วยประหยัดค่าใช้จ่ายอีกด้วย"

ส่วนระบบป้องกันภัยจะอยู่ในชุดคุณสมบัติรักษาความปลอดภัยของ Cisco IOS Software ซึ่งประกอบด้วย Cisco IOS firewall, transparent firewall ชนิดใหม่, ระบบป้องกันการบุกรุก, ระบบป้องกันไวรัสผ่าน NAC ระบบกลั่นกรอง URL และระบบรักษาความปลอดภัยเนื้อหาข้อมูล โดยที่ IOS firewall เป็นโปรแกรมตรวจสอบแบบ stateful ซึ่งประกอบด้วยระบบป้องกันการโจมตีเพื่อทำให้ระบบปฏิเสธการให้บริการ แยกแยะแอพพลิเคชัน สัญญาณ และผู้ใช้ได้ดีขึ้น มีระบบตรวจสอบโพรโตคอลที่ทันสมัยเพื่อใช้กับแอพพลิเคชันเสียง วิดีโอ และอื่นๆ และการกำหนดนโยบายรักษาความปลอดภัยต่อผู้ใช้ อินเทอร์เฟซหรืออินเทอร์เฟซย่อย ส่วน transparent firewall ช่วยทำให้ Integrated Services Routers มีระบบป้องกันเลยอร์ 3 สำหรับการสื่อสารเลเยอร์ 2 ได้

เราเตอร์รุ่นนี้ยังเป็นเราเตอร์รุ่นแรกที่มีระบบป้องกันการบุกรุกแบบอินไลน์อีกด้วย ระบบ Intrusion Prevention System (IPS) ซึ่งเป็นส่วนหนึ่งของ Cisco IOS Software จัดเป็นบริการตรวจสอบแพ็กเก็ตเชิงลึกแบบอินไทม์ที่สามารถหยุดยั้งผู้บุกรุกก่อนที่จะเรียกใช้ระบบเครือข่ายได้ IPS นำเอาเทคโนโลยีในอุปกรณ์ Intrusion Detection System Sensor ของซิสโก้มาใช้ ดังนั้นมันจึงมีร่องรอยของไวรัสและเวิร์มพื้นฐานเก็บไว้เป็นจำนวนมาก รวมทั้งยังยอมให้ผู้ใช้เรียกระบบที่เหมาะสมกับอุปกรณ์และระบบปฏิบัติการที่ใช้อยู่อีกด้วย

ถ้าหากต้องการรักษาความปลอดภัยช่องทางสื่อสารที่เข้ามาให้ดีขึ้น ผู้ใช้อาจจำเป็นต้องติดตั้งระบบ Intrusion Prevention System และ/หรือ content engine network module เพื่อรักษาความปลอดภัยของข้อมูล ระบบชนิดที่สองนี้ยังมีระบบกลั่นกรอง URL เป้าหมายอีกด้วย Stallone กล่าวว่า "ระบบรักษาความปลอดภัยมีอยู่สองส่วนก็คือ การป้องกันสัญญาณที่เข้ามาและการปกป้องความลับของข้อมูลที่ออกไป"

การปกป้องความลับและตัวตนของผู้ใช้ตรงกับคุณสมบัติที่มีอยู่ใน IOS เช่น NAC ที่ใช้ป้องกันไวรัสและระบบตรวจสอบตัวตน ระบบตรวจสอบสิทธิ์ในการใช้งาน และบัญชี (authentication, authorization and accounting - AAA) รวมทั้งการให้สิทธิ์ที่ยกเลิกได้ของ NAC ช่วยให้สาขาหรือบริษัท SMB มั่นใจได้ว่าจุดปลายทุกจุด (แม้แต่อุปกรณ์โมไบล์หรือพีซีที่ใช้ในบ้าน) ตรงกับนโยบายรักษาความปลอดภัยที่กำหนดเอาไว้แล้ว

Willis กล่าวว่า "คุณสมบัติดังกล่าวจัดว่ามีค่าอย่างมากเนื่องจากตัวระบบเครือข่ายเองเข้าใจโฮสต์และผู้ใช้มากขึ้น วิธีการนี้จะช่วยให้บริษัทจำนวนมากมั่นใจว่าเมื่อพวกเขาเปิดช่องทางการสื่อสารขึ้นมา พวกเขาจะยังคงควบคุมผู้ใช้และสัญญาณที่วิ่งผ่านไปมาได้อยู่"

AAA ช่วยให้ผู้ดูแลระบบกำหนดและดูแลการควบคุมการใช้ระบบได้อย่างคล่องตัว โดยขึ้นอยู่กับสายสัญญาณหรือขึ้นกับผู้ใช้ก็ได้ ส่วนพอร์ต USB ที่มีอยู่ในเราเตอร์ Cisco 1800, 2800 และ 3800 สามารถปรับแต่งให้ทำงานกับ USB token ที่ซื้อแยกต่างหาก เพื่อรักษาความปลอดภัยของการแจกจ่ายตัวแปรและระบบจัดเก็บข้อมูลสิทธิ์ VPN นอกแพลตฟอร์ม การทำงานแยกกันแบบนี้ช่วยให้ผู้ดูแลระบบสามารถส่งเราเตอร์และ token แยกจากกันได้ เพื่อทำให้ระบบมีความปลอดภัยมากขึ้น (คุณสมบัติ USB จะคลอดในไตรมาสแรกของปี 2005) อุปกรณ์ระบบเครือข่ายแต่ละชนิดและระบบเครือข่ายโดยรวมจะได้รับการปกป้องโดยคุณสมบัติอย่าง Network-based Application Recognition (NBAR), Secure Shell Version 2 (SSHv2), Simple Network Management Protocol เวอร์ชัน 3 (SNMPv3) และ role based Command-line Interface

การปกป้องโครงสร้างพื้นฐานของระบบเครือข่ายทำได้โดยใช้ Cisco Router and Security Device Manager (SDM) ซึ่งเป็นเครื่องมือบริหารผ่านเว็บที่ใช้ง่าย สำหรับเราเตอร์ที่ใช้ระบบปฏิบัติการ Cisco IOS Software โดยเฉพาะ Ranjan Goel ผู้จัดการผลิตภัณฑ์ของซิสโก้กล่าวว่า เครื่องมือ SDM เวอร์ชัน 1.0 มีให้ในแพ็กเก็ตเราเตอร์บางชนิดแล้ว ซึ่งทำให้ SDM มีการใช้งานอย่างกว้างขวาง ส่วน SDM เวอร์ชัน 2.0 จะให้มาพร้อมกับ Integrated Services Routes

Goel กล่าวว่าการปรับแต่งระบบรักษาความปลอดภัยเริ่มมีความซับซ้อนมากขึ้น และส่วนใหญ่เริ่มมีความสัมพันธ์กัน เช่น การเซตอัพระบบรักษาความปลอดภัยของระบบแลนและ WAN หรือ Network Address Translation และไฟร์วอลล์ เป็นต้น นอกจากนั้นผู้ดูแลระบบยังต้องติดตั้งระบบรักษาความปลอดภัยให้แก่เครือข่ายอย่างครอบคลุมอีกด้วย การใช้ SDM ช่วยให้ผู้ดูแลระบบสามารถปรับแต่งเราเตอร์ สวิตช์, QoS และบริการอื่นๆ ได้ง่าย รวมทั้งยังคอยดูแลประสิทธิภาพของเครือข่ายได้อีกด้วย

Goel กล่าวว่า SDM เป็นการนำเอา "ความรู้" ที่ได้รับมาจากศูนย์ให้ความช่วยเหลือทางด้านเทคนิค หรือ TAC (Technical Assistance Center) ของซิสโก้มาใช้ในรูปของโปรแกรมช่วยเหลืออัจฉริยะที่ช่วยลดความผิดพลาดของการปรับแต่งตัวแปรต่างๆ ถ้าหากมีข้อผิดพลาดเกิดขึ้น โปรแกรมช่วยเหลือจะชี้ให้เห็นว่าจุดใดที่ผิดพลาดและแนะนำวิธีการแก้ไขให้ นอกจากนั้นการคลิ้กเม้าส์เพียงครั้งเดียวยังทำให้โปรแกรมช่วยเหลือตรวจสอบระบบรักษาความปลอดภัยเริ่มทำการตรวจว่ามีการปฏิบัติตามคำแนะนำทั้งหมดเกี่ยวกับการรักษาความปลอดภัยเราเตอร์แล้วหรือยัง ถ้าหากเป็นการทำงานที่แบบเก่าแล้วต้องเสียเวลาทำหลายชั่วโมง

รวมบริการหลายๆ ชนิดเข้าด้วยกัน

โมดูลแต่ละชนิดหรือการ์ดสล็อตแต่ละช่องในเราเตอร์สามารถรองรับการทำงานได้มากกว่าหนึ่งชนิดขึ้นไป ดังนั้นผู้ใช้สามารถผสมผสานบริการหลายๆ ชนิดที่คิดว่าเหมาะสมกับตนมากที่สุดได้ลงไปได้ ตัวอย่างเช่น โมดูลระบบเครือข่าย หรือโมดูลระบบเครือข่ายรุ่นพิเศษสามารถใช้รองรับการทำงานของระบบข่าวสารเสียงและระบบตอบรับอัตโนมัติโดยใช้ Cisco Unity Express ได้ (มีความเร็วสูงถึง 1.2 กิกะบิตต่อวินาทีในเราเตอร์ Cisco 3800 Series) หรือใช้กลั่นกรอง URL, power over Ethernet, เพิ่มความจุให้แก่การโทรอะนาล็อกโดยใช้ extension voice module (EVM) และฟังก์ชันอื่นๆ อีกมาก นอกจากนั้นบริษัทต่างๆ ยังสามารถใช้ advanced integration modules (AIMs) เพื่อรองรับการทำงานของระบบจัดการข่าวสารเสียงและระบบตอบรับอัตโนมัติได้ (ผ่านทาง Cisco Unity Express) หรือใช้เร่งความเร็วของ VPN เพิ่มคุณสมบัติรักษาความปลอดภัยอื่นๆ เพิ่มระบบเข้ารหัสอื่นๆ การบีบอัดสัญญาณ การแบ่งและรวมเซ็กเมนต์ ATM รวมทั้งคุณสมบัติอื่นๆ ด้วย

ผู้ใช้สามารถใส่การ์ดลงไปในสล็อตสำหรับ HWIC ซึ่งทำให้การสื่อสารมีความเร็วระดับสาย หรือใส่การ์ดเชื่อมต่อ WAN (WAN interface cards - WICs) อื่นๆ ที่มีความเร็วต่ำกว่าก็ได้ โดย WIC จากเราเตอร์รุ่นก่อนหน้านี้ก็สามารถนำมาใช้ได้เช่นกัน ซึ่งช่วยในการร่วมกันย้อนหลังได้เป็นอย่างดี นอกจากนั้นสล็อต HWIC ยังใส่การ์ดเชื่อมต่อระบบเสียง (Voice Interface Cards - VICs) เพื่อรองรับการทำงานของ PRI, PSTN, เสียงบนเฟรมรีเลย์, เสียงบนเอทีเอ็ม และเสียงบนไอพี บวกกับ power over Ethernet ได้ด้วย ส่วน packet voice/fax DSP modules (PVDM) ยังรองรับการทำงานของเสียง แฟกซ์ วิดีโอ ระบบประชุมร่วม และ transcoding ได้ด้วย พอร์ตอีเทอร์เน็ตรองรับการทำงานของระบบแลนฟาสต์อีเทอร์เน็ตที่ความเร็ว 10 หรือ 100 เมกะบิตต่อวินาทีในระบบขนาดเล็ก หรือใช้ระบบแลนฟาสต์ หรือกิกะบิตอีเทอร์เน็ตในระบบขนาดใหญ่ก็ได้ สล็อต EVM เฉพาะในเราเตอร์ 2821 และ 2851 สามารถใส่โมดูลเพื่อเพิ่มจำนวนสายโทรศัพท์อะนาล็อก และช่องทางเสียงอะนาล็อก /DRI ได้ด้วย

การมีโมดูลและการ์ดสล็อตให้เลือกใช้หลายชนิดช่วยให้ผู้จัดการระบบเครือข่ายติดตั้งบริการหลายชนิดที่ปรับแต่งมาเพื่อสนองตอบต่อความต้องการเฉพาะของแต่ละสาขาหรือ SMB ได้ ตัวอย่างเช่น ลูกค้าที่ใช้เราเตอร์ Cisco 2821 สามารถใช้โมดูล EVM ของระบบเพื่อเพิ่มจำนวนสายเสียงได้ วิธีการนี้จะช่วยประหยัดสล็อตโมดูลระบบเครือข่าย เพื่อช่วยเพิ่มความเร็วหรือเพิ่มวิดีโอสตรีมมิงได้ ส่วนสล็อต PVDM สามารถจัดการกับ IP voice termination ได้ ส่วนสล็อต AIM ในตัวยังสามารถใช้เพื่อรองรับการเร่งความเร็ว VPN, บีบอัดข้อมูล หรือระบบจัดการข่าวสารเสียงและระบบตอบรับอัตโนมัติผ่านทาง Cisco Unity Express ได้ด้วย

ผู้ที่เลือกใช้เราเตอร์ Cisco 3845 รุ่นสูงสุดจะได้รับบริหารและความยืดหยุ่นมากที่สุด สล็อตโมดูลระบบเครือข่ายจำนวน 4 ช่องของเราเตอร์สามารถรองรับบริการต่างๆ ได้เป็นจำนวนมาก เช่น อีเทอร์เน็ตสวิตชิง ซึ่งทำงานกับระบบจ่ายไฟผ่านอีเทอร์เน็ต, ระบบจัดการข่าวสารเสียง (มากถึง 100 เมล์บ็อกซ์) บวกกับระบบตอบรับอัตโนมัติ ระบบสร้างแคชข้อมูล และระบบวิเคราะห์เครือข่ายด้วย ส่วนแหล่งจ่ายพลังงาน 2 ชุดตามมาตรฐาน 802.3af ใช้เป็นระบบสำรองและอินไลน์เพาเวอร์ได้ ส่วนผู้ที่ใช้ Cisco 1841 สามารถเลือกใช้ WIC มากกว่า 30 ชนิดเพื่อรองรับการสื่อสารข้อมูลของตนเอง หรือบางทีอาจเลือกใช้บริการข้อมูล T1 ร่วมกับสล็อต HWIC บวกกับเลือกใช้ระบบสื่อสารที่ช้ากว่าไปยังเครือข่ายเฟรมรีเลย์ก็ได้ ในขณะที่สลอต AIM ใช้รองรับการเร่งความเร็วของ VPN เป็นหลัก

Jennifer Lin ผู้จัดการสายผลิตภัณฑ์ของซิสโก้กล่าวว่าทางบริษัทมีโมดูลและการ์ดมากกว่า 90 ชนิดที่ติดตั้งลงไปในสล็อตต่างๆ ได้ ความคล่องตัวดังกล่าวช่วยให้ผู้ใช้ขยายขอบเขตการทำงานของแอพพลิเคชันในเราเตอร์รุ่นใหม่ได้ แถมยังได้รับจุดเด่นในเรื่องการบริหารระบบโดยง่าย ค่าใช้จ่ายที่ลดลง และการติดตั้งระบบที่ทำได้อย่างรวดเร็วอีกด้วย โมดูลระบบเครือข่ายส่วนใหญ่มีโพรเซสเซอร์และฮาร์ดไดรฟ์อยู่ในตัวเรียบร้อยแล้ว ดังนั้นโมดูลเหล่านี้จะทำงานได้อย่างอิสระโดยไม่ต้องพึ่งซีพียูของเราเตอร์ จากนั้นซีพียูของเราเตอร์ก็จะทำงานน้อยลง แถมผู้ใช้ยังสามารถบริหารโมดูลเหล่านี้ผ่านทางอินเทอร์เฟซชุดเดียวกันอีกด้วย Lin กล่าวว่า "ลูกค้ามีอิสระในการเลือกใช้เครื่องมือบริหารผ่านเว็บบราวเซอร์หรือบรรทัดคำสั่ง (command-line interface - CLI) ที่เหมาะกับความต้องการของตนได้" ■