มุ่งหน้าสู่ยุคของฮอตสปอต

บริษัทผู้ให้บริการจะติดตั้งเครือข่ายไร้สายสาธารณะ (Wireless Hotspot) ที่ทำกำไรได้อย่างไร

ระบบเครือข่ายไร้สาย: สิ่งที่ผู้ใช้อยากให้มีทุกหนแห่ง

เป้าหมายของบริษัทผู้ให้บริการ (Service Provider) ก็คือการติดตั้งเครือข่ายไร้สายสาธารณะ (public wireless networks-PWLANs) ทั่วโลก ระบบเครือข่ายเหล่านี้อิงอยู่กับมาตรฐาน IEEE 802.11 ที่เอาไว้เรียกใช้บริการออนไลน์ต่างๆ อย่างกว้างขวาง เช่น เว็บ อีเมล์ การเชื่อมต่อระบบเครือข่ายส่วนตัวเสมือน (virtual private networking - VPN) ไปยังระบบเครือข่ายขององค์กร เพลง วิงโทน และภาพยนตร์

ในปัจจุบันนักเดินทางใช้ PWLAN ในสนามบิน สถานีรถไฟ โรงแรม ศูนย์ประชุม ร้านหนังสือ และคอฟฟี่ชอบ ผู้เชี่ยวชาญคาดว่ามีการติดตั้งฮอตสปอตไร้สายมากกว่า 100,000 จุดในปี 2004 ที่ผ่านมา ด้วยเหตุนี้บริษัทผู้ให้บริการสื่อสารจึงพร้อมที่จะให้บริการในวงกว้างได้แล้ว ส่วนระบบที่มีการติดตั้งอยู่ในตอนนี้ก็คือระบบเครือข่ายไร้สายแบบเคลื่อนที่ ซึ่งเป็นการขยายการบริการไปยังเครื่องบิน รถไฟ และรถยนต์ด้วย

แล้วใครจะใช้?

ในอดีต ผู้คนมองว่าการให้บริการสื่อสารไร้สายสาธารณะเป็นบริการเพ้อฝันบวกกับโมเดลการทำธุรกิจที่ยังมีข้อสงสัยอยู่ ด้วยเหตุนี้จึงมีผู้ประกอบการรายเล็กๆ เท่านั้นที่เจาะตลาดโรงแรมและสนามบินอยู่ อย่างไรก็ตามเมื่อมีการติดตั้งฮอตสปอตกันมากขึ้น และมีผู้ใช้หันมาใช้ระบบสื่อสารไร้สายกันมากขึ้น การสื่อสารไร้สายในที่สาธารณะจึงกลายเป็นบริการซึ่งมีการยอมรับอย่างกว้างขวาง ซึ่งบริษัทผู้ให้บริการสื่อสารแต่ละรายสามารถนำมาดำเนินงานในหลายแง่มุมได้ บริษัทต่างๆ นำเอาแนวทางที่แตกต่างกัน 3 แบบมาทำให้การติดตั้ง PWLAN ได้ผลตอบแทนจากการลงทุนที่คุ้มค่า

โมเดลแบบแรกเกี่ยวข้องกับการให้บริการ PWLAN ที่ทำงานอิสระซึ่งทำกำไรได้ ถ้าหากพิจารณาจากข้อมูลทางการตลาดและผลลัพธ์จริงที่เกิดขึ้นแล้ว ปัจจัยหลักๆ ซึ่งทำให้ธุรกิจฮอตสปอตทำกำไรได้ประกอบด้วย

จับจองทำเลทอง: สนามบินและโรงแรมจัดเป็นจุดที่มีอัตราการใช้งานสูงสุดและกลายเป็นทำเลทองของผู้ประกอบการที่ประสบความสำเร็จส่วนใหญ่

การสร้างฮอตสปอตที่มีจุดให้บริการกว้างขวางครอบคลุม: นอกจากสนามบินและโรงแรมแล้ว โมเดลการทำธุรกิจ PWLAN ที่ประสบความสำเร็จมักขึ้นอยู่กับบริการบอกรับสมาชิกเป็นหลัก ซึ่งการที่จะขายสมาชิกได้ก็ต่อเมื่อสามารถให้บริการในสถานที่ต่างๆ อย่างกว้างขวางเท่านั้น ส่วนผู้ให้บริการสื่อสารหลายรายมักรวมตัวกันเพื่อที่จะให้บริการอย่างกว้างขวางครอบคลุมผ่านการเชื่อมโยงเครือข่ายร่วมกัน

ราคาที่เหมาะสม: ผู้ประกอบการหลายรายตั้งราคาการใช้ระบบ PWLAN ในรูปของบริการระดับพรีเมี่ยม ที่ตั้งราคาเอาไว้ที่ 25 ถึง 30 ดอลลาร์ต่อวัน แม้ว่านักเดินทางฐานะดีอาจยอมรับราคาระดับนี้ได้ แต่ผู้ใช้อื่นๆ กลับไม่ได้คิดแบบนั้น ผู้ประกอบการที่ประสบความสำเร็จให้บริการคิดเป็นรายชั่วโมงหรือรายวันในราคาประหยัด แถมยังมีการสมัครบริการรายเดือนโดยคิดค่าบริการ 10 ถึง 20 ดอลลาร์ต่อเดือนเท่านั้น

เมื่ออัตราการใช้ PWLAN เพิ่มสูงขึ้น และลูกค้าตระหนักถึงความสำคัญของบริการแบบนี้เพิ่มขึ้น ดังนั้นบริษัทผู้ให้บริการสื่อสารจึงพยายามสร้างความแตกต่างให้เกิดขึ้นแก่บริการมีสายและไร้สายของตนเอง โมเดลแบบที่สองที่จะช่วยให้คืนทุนจาก PWLAN ก็คือการแถมบริการไร้สายไปกับบริการที่มีอยู่เดิม เพื่อทำให้บริการของตนได้ผลตอบแทนเฉลี่ยสูงขึ้น บริษัทผู้ให้บริการสื่อสารทั่วโลก เช่น Portugal Telecom, Comcast และ Singtel ใช้นโยบายแบบนี้ ส่วนเมื่อไม่นานมานี้ SBC ประกาศว่าจะให้บริการ PWLAN แก่สมาชิก DSL ปัจจุบันของตนผ่านทางฮอตสปอต 3,500 จุด (เพิ่มขึ้นเป็น 20,000 จุดภายในปี 2006) โดยคิดค่าบริการแค่ 1.99 ดอลลาร์ต่อเดือนเท่านั้น

ท้ายสุด บางทีวิธีคืนทุนที่ได้ผลกับ PWLAN มากที่สุดก็คือการผสานมันกับเทคโนโลยีอื่นๆ เพื่อให้บริการข้อมูลแบบโมไบล์อย่างครบวงจร บริษัท Swisscom ได้ติดตั้งบริการ Packet Radio Services (GPRS) Universal Mobile Telecommunications System (UMTS) ซึ่งให้บริการเชื่อมต่ออย่างกว้างขวางแก่สมาชิกของตนเอง โดยผู้ใช้จ่ายค่าบริการตามอัตราการใช้งานจริง การใช้โมเดลชนิดนี้สามารถควบคุมการติดต่อของลูกค้าจากเครือข่ายไร้สายที่แตกต่างกันได้ผ่านทางโมไบล์ไอพี และลูกค้าไม่จำเป็นต้องรู้ว่าพวกเขาติดต่อกับระบบเครือข่ายใดอยู่ รวมทั้งไม่จำเป็นต้องรู้ว่าต้องทำอะไรบ้างจึงจะเชื่อมต่อได้ โดยนอกจากใช้ง่ายแล้ว บริการนี้ยังมีระบบรักษาความปลอดภัยระบบสื่อสารไร้สายที่แข็งแกร่งที่สุดผ่านทางระบบตรวจสอบสิทธิและระบบเข้ารหัส 802.1X/EAP อีกด้วย

สถาปัตยกรรม

ถ้าหากต้องการให้บริการอย่างกว้างขวางในตลาดได้ บริษัทผู้ให้บริการสื่อสารไร้สายจำเป็นต้องติดตั้งโครงสร้างที่คล่องตัวที่รองรับบริการจำนวนมากที่มีอยู่ในปัจจุบันได้ รวมทั้งปรับตัวเข้าหาบริการที่กำลังอยู่ในระหว่างการพัฒนาได้ด้วย ถ้าหากพูดถึงระบบเครือข่ายแล้ว เรื่องนี้หมายถึงโครงสร้างที่คล่องตัวที่ผู้ใช้สามารถติดต่อและใช้งานได้โดยง่าย ระบบต้องรองรับการสื่อสารจากอุปกรณ์ไคลเอ็นต์ชนิดใดก็ได้ โดยไม่จำเป็นต้องใช้ซอฟต์แวร์ไคลเอ็นต์หรือการปรับแต่งคอนฟิกกูเรชันพิเศษ โครงสร้าง PWLAN ในลักษณะนี้ขยายระบบได้ เพื่อรองรับการควบคุมการให้บริการแก้ไซต์หลายพันแห่ง ซึ่งกระจายกันอยู่ตามจุดต่างๆ ได้

โครงสร้าง PWLAN ระดับบริษัทสื่อสารช่วยให้ติดตั้งฮอตสปอตขนาดเล็กจำนวนมากตามร้านกาแฟหรือร้านหนังสือได้ รวมทั้งฮอตสปอตขนาดใหญ่ตามสนามบินและศูนย์การประชุม เป็นต้น (ดูภาพประกอบ) (บทความนี้ไม่ได้พูดถึง PWLAN สำหรับส่วนตัว ซึ่งทำการติดตั้งภายในสำนักงานซึ่งอยู่ภายใต้ระบบเครือข่ายซึ่งมีการดูแลส่วนตัวให้บริการไร้สายเพื่อติดต่อกับอินเทอร์เน็ตเท่านั้น) ฮอตสปอตทั้งหมดสามารถบริหารจากศูนย์กลางเพื่อปรับแต่งคอนฟิกกูเรชัน แก้ปัญหา และรายละเอียดของอุปกรณ์ทั้งหมด (Inventory) ของใช้ฮอตสปอตขนาดใหญ่ซึ่งมีจุดเชื่อมต่อรวมกันนับสิบจุดจำเป็นต้องมีการปรับแต่งทางวิศวกรรมคล้ายคลึงกับการติดตั้งภายในองค์กรต่างๆ เช่น ต้องมีการสำรวจสถานที่และมีการปรับแต่งคลื่นวิทยุระหว่างจุดติดต่อด้วย

ไม่ว่าจะมีขนาดเล็กหรือขนาดใหญ่ก็ตาม แต่ฮอตสปอตทั้งหมดสามารถให้บริการหลายชนิดผ่านโครงสร้างพื้นฐานเพียงชุดเดียวได้ สถานที่ใช้งานปกติมักจะมีจุดติดต่อกับระบบเครือข่ายแบบมีสายและไร้สาย โดยที่ระบบไร้สายใช้สำหรับลูกค้าและพนักงานที่ต้องเดินทาง และระบบมีสายใช้สำหรับการทำรายการจากพีซี การออกแบบที่มีประสิทธิภาพใช้ VLAN ไร้สายจำนวนมากเพื่อแยกผู้ใช้ออกเป็นกลุ่มและใช้ควบคุมสัญญาณของระบบ ควบคู่ไปกับกลไกควบคุมคุณภาพของการให้บริการ (quality of service -QoS) และสอดคล้องกับมาตรฐาน IEEE 802.1Q นอกจากนั้นการทำงานกับเทคโนโลยีการสร้างช่องทางสำหรับการติดต่อ (tunneling) นี้ยังอิงกับ IP Security (IPSec) หรือ Generic Routing Encapsulation (GRE) ช่วยให้การติดต่อมีความปลอดภัยยิ่งขึ้น การติดตั้งฮอตสปอตเป็นจำนวนมากช่วยให้จุดใช้งานขนาดใหญ่ให้บริการที่มีแบนด์วิดธ์สูงๆ เช่น ภาพยนตร์ออนไลน์และให้บริการอุปกรณ์ชนิดต่างๆ ได้หลากหลายมากขึ้น เช่นโทรศัพท์ไอพีแบบมีสายและไร้สาย โทรศัพท์วิดีโอ และโทรศัพท์ Global System for Mobile Communications (GSM)/802.11 โหมดคู่ได้ด้วย

ส่วนประกอบในระบบ PWLAN ของซิสโก้

โซลูชัน Cisco PWLAN ซึ่งทำงานได้อย่างครบวงจรประกอบด้วยส่วนประกอบต่างๆ เพื่อใช้กับฮอตสปอตและศูนย์ข้อมูลกลาง ฮอตสปอตประกอบด้วยจุดให้บริการ เช่น Cisco Aironet 1100, 1200 หรือ 1300 ซึ่งเชื่อมต่อกับ Cisco Access Zone Router (AZR) สำหรับระบบ WAN หรือเชื่อมต่อผ่านอินเทอร์เน็ตไปยังศูนย์ข้อมูลก็ได้ Cisco IOS Software ใน Cisco AZR มีคุณสมบัติเฉพาะเกี่ยวกับ PWLAN เช่น ระบบป้องกันการปลอมแปลงค่าไอพี (IP Spoofing) ระบบตรวจสถานะการใช้งานของผู้ใช้ (L2 user detection & Session termination) ระบบระบุตำแหน่งพอร์ตสวิตช์ และบริการ client static IP เป็นต้น ส่วนคุณสมบัติมาตรฐานเพื่อใช้ติดตั้งระบบ PWLAN ประกอบด้วยระบบเชื่อมต่อ WAN, IETF 802.1Q VLAN, dynamic address assignment, กลไก QoS และความสามารถในการเลือกเส้นทางการส่งข้อมูล (Policy based roting) เป็นต้น การแยกสัญญาณของ VLAN และ QoS จัดเป็นเรื่องที่มีประโยชน์อย่างมาก โดยที่ผู้ค้าหลายรายอาจจะใช้ระบบเครือข่ายชุดเดียวกัน นอกเหนือจากระบบเครือข่ายสาธารณะแล้ว ตัวอย่างเช่น ถ้าหากเป็นการใช้งานที่สนามบิน ผู้ใช้อาจประกอบด้วยหน่วยงานขนถ่ายกระเป๋า ร้านขายอาหาร ศูนย์ควบคุมภาคพื้นดิน และอื่นๆ อีกมาก

โซลูชัน Cisco Mobile Exchange ซึ่งใช้งานในศูนย์ข้อมูล (หรือจุดกระจายสัญญาณในหน่วยงานขนาดใหญ่) ใช้ควบคุมการติดต่อของผู้ใช้ การจัดสรรบริการ ระบบบริหาร ระบบรักษาความปลอดภัย และระบบคิดค่าใช้จ่าย เป็นต้น โซลูชันที่ประกอบด้วย Cisco Services Selection Gateway (SSG) ซึ่งทำงานร่วมกับ Cisco Subscriber Edge Service Manage (SESM) เพื่อให้บริการแก่สมาชิกและดูแลบริการอื่นๆ ระบบดังกล่าวใช้ในการตรวจสอบสิทธิของผู้ใช้ จัดสรรพอร์ทัลของผู้ค้าแต่ละราย รวบรวมและส่งข้อมูลการคิดค่าบริการ และบันทึกกิจกรรมต่างๆ เพื่อใช้เรียกเก็บเงิน รักษาความปลอดภัย และการบริหาร โดยที่ Cisco Access Registrar จัดเป็นเซิร์ฟเวอร์ RADIUS ซึ่งทำงานได้อย่างยืดหยุ่น โดยมีบริการตรวจสอบสิทธิ์ ให้สิทธิ์ และการคิดบัญชี รองรับระบบตรวจสอบสิทธิ์จำนวนมาก เช่น ระบบ Extensible Authentication Protocol (EAP) แบบต่างๆ

บางประเทศกำหนดให้ผู้ให้บริการ PWLAN ต้องให้บริการระบบเครือข่ายโฮสต์ที่เป็นกลาง ซึ่งให้บริการผู้ใช้ได้อย่างเท่าเทียมกัน ดังนั้นผู้ให้บริการแต่ละรายจึงจำเป็นต้องมีระบบเชื่อมต่อไปยังเครือข่ายและบริการของผู้ให้บริการรายอื่นๆ จากฮอตสปอตสาธารณะได้ด้วย ระบบเครือข่ายที่มีระบบควบคุมการใช้งานแบบโลคอลสามารถโอนถ่ายสัญญาณของผู้ใช้ไปยังผู้ให้บริการจำนวนมากได้ขึ้นอยู่กับการเลือกของผู้ใช้

ประสบการณ์ของผู้ใช้

สิ่งที่ผู้ใช้จะต้องทำมีแค่เรื่องง่ายๆ ดังต่อไปนี้

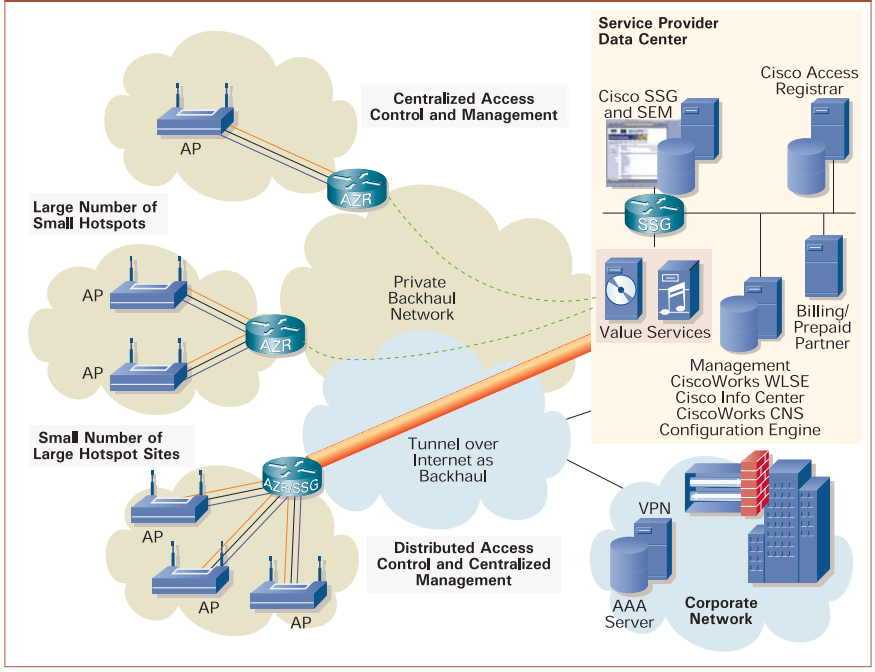
1. ผู้ใช้เชื่อมต่อกับ WLAN และเรียกเว็บบราวเซอร์ขึ้นมา
2. ผู้ใช้จะเข้าสู่หน้าจอล็อกอินโดยอัตโนมัติ (พอร์ทัลของผู้ให้บริการ)
3. ผู้ใช้สามารถเลือกใช้บริการตัวอย่างที่ฟรีได้ แต่ถ้าจะใช้ตามปกติต้องล็อกอินต่อไป
4. ผู้ใช้ล็อกอินและสามารถเรียกใช้บริการพรีเมี่ยม เช่น อีเมล์ หรือ VPN องค์กรได้
5. ระบบคิดค่าใช้จ่ายการใช้งานจนกว่าผู้ใช้จะเลิกใช้บริการ

PWLAN ซึ่งได้รับการออกแบบมาเป็นอย่างดีจะทำให้การใช้งานง่ายขึ้นในหลายรูปแบบ การเชื่อมต่อที่ง่ายดายผ่านทางจุดเชื่อมต่อไร้สายแบบเปิดที่ไม่มี WEP แล้วส่งสัญญาณ Service Set Identifiers (SSIDs) ซึ่งเกี่ยวข้องกับ VLAN สาธารณะออกไป จากนั้นอุปกรณ์ไคลเอ็นต์มองเห็นระบบเครือข่ายและสามารถเชื่อมต่อได้โดยที่ไม่ต้องกรอก SSID ลงไป

ถ้าหากต้องการให้ระบบสามารถรองรับผู้ใช้งานได้มากที่สุดไม่ว่าจะด้วย configuration แบบไหน อุปกรณ์ระบบเครือข่ายจำเป็นต้องเป็นแบบเสียบต่อแล้วใช้งานได้เลย ไคลเอ็นต์ซึ่งมีไอพีตายตัว Network Address Translation (NAT) ตายตัว และตั้งตัวแปรเว็บพร็อกซีเอาไว้สามารถเชื่อมต่อได้โดยที่ไม่ต้องแก้ไขอะไร ส่วนบริษัทผู้ให้บริการสื่อสารสามารถปรับแต่ง NAT ที่ AZR เพื่อรองรับการทำงานของไคลเอ็นต์ที่มีไอพีตายตัว ส่วนไคลเอนต์ที่มีการ ตั้งค่า DNS ส่วนตัวอยู่แล้ว ผู้ให้บริการจะทำการโอนย้ายผู้ใช้ไปยังเซิร์ฟเวอร์ DNS แบบโลคอล ซึ่งมีการแบ่งกลุ่ม DNS ต่อบริการแต่ละชนิด ในรูปของคุณลักษณะของบริการที่อิงกับช่วงไอพีแอดเดรสที่กำหนดเอาไว้

การตั้งตัวแปรเว็บพร็อกซีจะโอนย้ายผู้ใช้ไปยังโลคอลเว็บพร็อกซีที่มีระบบตรวจสอบสิทธิ์และไม่มีระบบตรวจสอบสิทธิ์ ส่วนบริษัทผู้ให้บริการสื่อสารจำเป็นต้องล็อกการติดต่อไปยังบริการเว็บพร็อกซีและพอร์ตที่มีสิทธิ์ถูกต้องเท่านั้น

บริษัทผู้ให้บริการสื่อสารที่ใช้โครงสร้างของซิสโก้



ระบบเครือข่ายชนิดเดียวที่ให้บริการหลายชนิด: โมเดลการทำธุรกิจ PWLAN ที่ทำกำไรได้ เริ่มต้นจากโครงสร้างระบบเครือข่ายที่มีระบบบริหารที่ศูนย์กลาง ซึ่งจัดสรรบริการที่คิดค่าธรรมเนียมไปยังฮอตสปอตนับพันๆ จุดได้

เพื่อป้องกันผู้ที่พยายามติดต่อเข้ามาในระบบโดยไม่ได้เสียค่าบริการ ถ้าหากไม่ต้องการให้มีคำสั่งล็อกอินที่มีรายละเอียดมากเกินไป Cisco SSG จะโอนผู้ใช้ไปยังเว็บอินเทอร์เฟซหรือพอร์ทัลเพื่อขอให้ผู้ใช้กรอกชื่อและรหัสผ่านลงไปเท่านั้น หรือบอกให้ผู้ใช้ใหม่ทำการลงทะเบียนเพื่อใช้บริการใหม่ก็ได้

PWLAN ใช้ไอพีแอดเดรสของไคลเอ็นต์เพื่อค้นหาผู้ใช้และแสดงผลพอร์ทัลและบริการที่เหมาะสม ถ้าหากเป็นการทำงานของไซต์เพียงแห่งเดียว มักจะแยกแยะผู้ใช้โดยดูจากช่วงของไอพีแอดเดรสที่กำหนดเอาไว้ก่อน ถ้าหากเป็นการทำงานของไซต์ขนาดใหญ่ที่มีจุดติดต่อเป็นจำนวนมาก เราสามารถใช้ Cisco AZR เพื่อแยกแยะตำแหน่งของผู้ใช้ถึงระดับจุดติดต่อแต่ละจุดใด โดยใช้ตัวระบุตำแหน่งสวิตช์ของพอร์ตผ่านทาง Dynamic Host Control Protocol (DHCP) Option 82 การระบุตำแหน่งจัดเป็นคุณสมบัติสำคัญชนิดหนึ่งใน PWLAN เพื่อช่วยให้สามารถให้บริการร่วมกันหลายๆ ผู้ให้บริการในจุดใช้งานขนาดใหญ่ เช่น สนามบิน หรือเครือข่ายร้านค้าขนาดใหญ่ เช่น โรงแรม และ ร้านกาแฟ เป็นต้น ซึ่ง Cisco SESM สามารถแยกแยะจากไอพีแอดเดรสว่าต้องแสดงผลพอร์ทัลชนิดใดต่อผู้ใช้

เมื่อผู้ใช้เลิกการใช้งานแต่ไม่ได้ล็อกเอาต์ ระบบตรวจสถานะการใช้งานของผู้ใช้ (L2 user detection & Session termination) ใน Cisco AZR จะปิดการทำงานเซสชันนั้นให้ วิธีการนี้จะปิดการคิดค่าบริการโดยดูจากเวลาที่ใช้งานจริง และช่วยปกป้องผู้ใช้ไม่ให้โดนเข้ามาขโมยเซสชันที่ใช้อยู่ด้วย

สิ่งที่สำคัญที่สุดก็คือ บริษัทผู้ให้บริการสื่อสารต้องยอมรับรูปแบบการชำระเงินแบบต่างๆ ไม่ว่าจะเป็นแบบล่วงหน้าหรือภายหลัง (Prepaid and Postpaid) ที่อยู่ในรูปของการเสียค่าบริการเพียงครั้งเดียวหรือค่าสมาชิกและยอมรับการชำระเงินผ่านเครดิตการ์ดหรือเดบิตการ์ดก็ได้ เนื่องจาก PWLAN เป็นตลาดที่เพิ่งเริ่มต้นเท่านั้น วิธีการชำระเงินที่พบมากที่สุดในปัจจุบันก็คือการชำระเงินโดยเครดิตหรือเดบิตชนิดหรือบัตรเติมเงิน ซึ่งให้สิทธิ์ใช้ระบบเครือข่ายได้ภายในเวลาที่จำกัด ถ้าหากตลาดเติบโตมากขึ้น ผู้ใช้ก็จะเปลี่ยนไปใช้ระบบชำระเงินผ่านสมาชิก ที่คล้ายคลึงกับการจ่ายค่าน้ำ ค่าไฟ หรือค่าโทรศัพท์

ระบบรักษาความปลอดภัย

ในฐานะของระบบเครือข่ายแบบเปิด PWLAN มีความเสี่ยงเรื่องระบบรักษาความปลอดภัยคือ โครงสร้างพื้นฐานของบริษัทผู้ให้บริการสื่อสารและผู้ใช้มากพอๆ กัน การรักษาความปลอดภัยระบบเครือข่ายสาธารณะแตกต่างจากการรักษาความปลอดภัยของระบบเครือข่ายในองค์กร โดยระบบเครือข่ายในองค์กรมักจะควบคุมประเภทและ configuration ของอุปกรณ์และผู้ใช้ที่ยอมให้เข้ามาในระบบเครือข่ายได้ แต่ PWLAN แบบเปิดจำเป็นต้องไม่ผูกติดกับอุปกรณ์ไคลเอ็นต์ชนิดใดชนิดหนึ่ง เพื่อกระตุ้นให้มีการใช้งานอย่างกว้างขวาง ผู้ให้บริการสื่อสารต้องการให้ทุกคนเข้ามาใช้ระบบ WLAN ได้ แต่เมื่อผู้ใช้สื่อสารได้แล้ว พวกเขาต้องเสียค่าบริการไม่ว่ารูปแบบใดก็รูปแบบหนึ่ง

ในปัจจุบันระบบรักษาความปลอดภัยของ PWLAN แบบเปิดสามารถแก้ปัญหาภัยคุกคามที่มีต่อผู้ใช้ได้ 4 ประการก็คือ

- **ระบบตรวจสอบสิทธิ์ของผู้ใช้:** การที่พอร์ทัลเป็นเว็บเพจ ดังนั้นโซลูชันมาตรฐานในปัจจุบันจึงใช้ระบบเข้ารหัสแบบ HTTP over Secure Sockets Layer (HTTPS/SSL)

- **air link sniffing:** สามารถทำได้โดยง่ายเนื่องจากไม่มีระบบเข้ารหัส air link ดังนั้นผู้ให้บริการสื่อสารไร้สายสามารถให้บริการ VPN สำหรับผู้ใช้ที่ไม่มี VPN องค์กร

- **local direct peer attack:** การโจมตีแบบนี้สามารถป้องกันได้โดยง่ายโดยใช้คุณสมบัติ Publicly Secure Packet Forwarding (PSPF) ในจุดติดต่อ Cisco Aironet และคุณสมบัติ Policy-Based Routing (PBR) ใน Cicso AZR

- **Session hijacking:** แฮกเกอร์พยายามใช้บริการฟรีโดยการพ่วงใช้บริการกับผู้ใช้คนอื่นๆ ซึ่งเสียค่าบริการไปแล้ว บริษัทผู้ให้บริการสื่อสารสามารถบรรเทาปัญหา hijacking ได้ที่ใช้ไอพีแอดเดรสปลอมได้ โดยการล็อก MAC address ของผู้ใช้ที่ถูกต้องไปยังไอพีแอดเดรส รวมทั้งปิดการทำงานของเซสชันเมื่อผู้ใช้ลืมล็อกออฟ โซลูชันแบบนี้ไม่สามารถป้องกันได้ร้อยเปอร์เซ็นต์ เนื่องจากแฮกเกอร์ยังคงสามารถใช้ MAC address ปลอมเพื่อเข้ามาใช้บริการได้อยู่ดี แต่บริษัทผู้ให้บริการกำลังทำงานเพื่อแก้ปัญหานี้โดยใช้ระบบตรวจสอบสิทธิ์ตามมาตรฐาน IEEE 802.1X อยู่

การปรับปรุงระบบรักษาความปลอดภัย

การป้องกันการแอบเข้ามาใช้ PWLAN จัดเป็นงานที่มีความท้าทายอย่างมาก ดังนั้นบริษัทผู้ให้บริการสื่อสารจึงพยายามนำเอาเทคโนโลยีระบบรักษาความปลอดภัยระดับองค์กรมาใช้กับระบบเครือข่ายสาธารณะด้วย อุปสรรคอย่างหนึ่งก็คือระบบตรวจสอบสิทธิ์ของผู้ใช้การปลอมแปลงชื่อ และรหัสผ่านเป็นสิ่งที่ทำได้ง่ายมากและผู้ใช้มักจะลืมรหัสผ่านของตนเป็นประจำ ในขณะที่ one-time passwords (OTPs) เป็นเรื่องที่เสียค่าใช้จ่ายสูงและจำเป็นต้องมีการฝึกอบรมผู้ใช้ ส่วนระบบตรวจสอบสิทธิ์ IPSec ส่ง MAC address โดยไม่มีการเข้ารหัสใดๆ ไปก่อนที่จะมีการเข้ารหัส ในขณะที่จุดติดต่อแปลกปลอม (Rogue AP)โดยเฉพาะอย่างๆ บริเวณใกล้ๆ กับหน่วยงานเล็กๆ อาจจะก่อให้เกิดปัญหาได้ ดังนั้นผู้ใช้จึงต้องการหลักประกันว่าพวกเขาล็อกออนและมอบข้อมูลการชำระเงินให้แก่ระบบเครือข่ายที่ถูกต้องแล้ว

บริษัทผู้ให้บริการสื่อสารพยายามจำลองการทำงานระดับองค์กร เพื่อแก้ปัญหาเหล่านี้โดยใช้ระบบตรวจสอบสิทธิ์ IEEE 802.1X และ EAP บางชนิด ซึ่งโซลูชัน Cisco PWLAN ใส่เทคโนโลยีเหล่านี้ลงไปด้วยแล้ว มาตรฐาน 802.1X/EAP ซึ่งอิงอยู่กับ RFC 2284 จะสร้างคีย์เข้ารหัสต่อเซสชันที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา เพื่อป้องกันไม่ให้แฮกเกอร์เข้ามาแอบดูข้อมูล นอกจากนั้นการเข้ารหัสยังช่วยป้องกัน session hijacking ได้อีกด้วย ส่วนระบบตรวจสอบสิทธิ์ร่วมกันระหว่างผู้ใช้และระบบเครือข่ายจะช่วยแก้ปัญหาเรื่องการล็อกออนเข้าไปในระบบเครือข่ายปลอม ส่วน Wi-Fi Protected Access (WPA) จัดเป็นเซตย่อยของมาตรฐาน IEEE 802.11i ซึ่งประกอบด้วย 802.1X, EAP, Temporal Key Integrity Protocol (TKIP) และ Message Integrity Check (MIC)

อย่างไรก็ตามทั้ง 802.1X และ EAP จำเป็นต้องมีซอฟต์แวร์ไคลเอ็นต์ด้วย ถ้าหากต้องการให้บริการตลาดในวงกว้างได้แล้ว บริษัทผู้ให้บริการสื่อสารการที่ต้องระบุให้ไคลเอ็นต์ต้องหาซอร์ฟแวร์พิเศษคงไม่ดีแน่ วิธีการแก้ปัญหาก็คือการใส่ 802.1X และ EAP ลงไปในระบบปฏิบัติการของตัวอุปกรณ์เลย ในปัจจุบันมีเพียงวินโดวส์เอ็กซ์พีเท่านั้นมีเทคโนโลยีเหล่านี้อยู่แล้ว แต่คงต้องใช้เวลาอีกหลายปีกว่าที่เทคโนโลยีดังกล่าวจะถูกแปลงไปไว้ในระบบปฏิบัติการและแพลตฟอร์มทุกชนิดได้ ความท้าทายอีกอย่างหนึ่งก็คือมี EAP อยู่หลายชนิด และการที่ไม่มีมาตรฐานอุตสาหกรรมก่อให้เกิดความกังวลว่าอาจจะเกิดปัญหาการทำงานร่วมกันได้เมื่อผู้ใช้ย้ายจุดติดต่อจุดหนึ่งไปสู่อีกจุดหนึ่ง

ระบบบริหารระบบเครือข่าย

ถ้าหากระบบเครือข่ายยังคงให้บริการได้นั่นหมายถึงระบบเครือข่ายจะทำรายได้ให้ต่อไป การบริหารระบบเครือข่ายที่ศูนย์กลางอย่างมีประสิทธิภาพถือเป็นสิ่งที่จำเป็นเพื่อปกป้องรายได้ ควบคุมค่าใช้จ่ายในการดำเนินงาน และแก้ปัญหาได้อย่างรวดเร็ว ซิสโก้มีโซลูชันบริหารซึ่งจัดสรรและดูแลระบบเครือข่ายแบบมีสายและไร้สายได้โดยอัตโนมัติ โดยมีอุปกรณ์ควบคุมที่ศูนย์กลางซึ่งสามารถคอยดูแลฮอตสปอตหลายพันจุดได้ ส่วนเรื่องของการบริหารอุปกรณ์เรามี CiscoWorks LAN Management Solution (LMS) ซึ่งมีเครื่องมือสำหรับการบริหาร configuration อุปกรณ์สำรอง และองค์ประกอบในระบบด้วย ส่วน Cisco CNS Configuration Engine ช่วยให้ปรับแต่ง configuration ของ Cisco AXR ได้โดยไม่ต้องไปสัมผัสกับตัวเครื่องโดยตรง เนื่องจากสามารถส่ง configuration ที่เหมาะสมไปยัง Cisco AZR ทั่วทั้งระบบเครือข่ายมีการติดตั้งในจุดที่มีการใช้ฮอตสปอตได้ ในขณะที่ Cisco Wireless LAN Solution Engine (WLSE) ซึ่งเป็นส่วนหนึ่งของโซลูชัน Cisco SWAN จะทำการบริหารและปรับแต่งตัวแปรจุดติดต่อ Cisco Aironet ที่มีสิทธิ์โดยอัตโนมัติ เมื่อมีการล็อกออนเข้ามาในระบบเครือข่ายจากหน่วยงานที่อยู่ในระยะไกล นอกจากนั้นระบบยังมีคุณสมบัติบริหารคลื่นวิทยุอย่างเต็มรูปแบบ รวมทั้งความสามารถในการคำนวณว่าฮอตสปอตให้บริการครอบคลุมพื้นที่ขนาดไหน รวมทั้งแยกแยะคลื่นรบกวนจากจุดติดต่อข้างเคียง หรืออุปกรณ์บางชนิดได้ด้วย

มองไปในอนาคต

เทคโนโลยีระบบเครือข่ายไร้สายมีความสมบูรณ์แบบเพียงพอที่จะนำไปใช้งานในวงกว้างได้แล้ว ในขณะที่ตัวผู้ค้าเองก็พยายามแก้ปัญหาเกี่ยวกับการให้บริการต่างๆ เช่น การให้บริการข้ามเครือข่ายทั่วโลก เป็นต้น ตัวอย่างเช่น พนักงานของบริษัทที่กำลังอยู่ในระหว่างการเดินทางและต้องการล็อกออนไปยัง VPN ขององค์กรผ่านทาง PWLAN ของศูนย์ประชุมซึ่งอยู่ภายใต้การดูแลของบริษัทสื่อสารที่แตกต่างออกไป ดังนั้นโซลูชันจำเป็นต้องช่วยให้ผู้ใช้ใช้งานได้อย่างสะดวก เทคโนโลยีต้องช่วยให้ผู้ใช้ติดต่อกับเครือข่ายที่ต้องการได้ โดยมีข้อตกลงเรื่องการชำระค่าบริการพ่วงมาด้วย เราอาจจำเป็นต้องมีบริษัทคนกลางที่เอาไว้คอยเคลียร์บัญชี เพื่อสร้างความมั่นใจว่าบริษัทสื่อสารที่ถูกยืมบริการจะได้รับเงินค่าบริการ ส่วนบริษัทสื่อสารต้นตอจะออกใบเรียกเก็บเงินอย่างถูกต้อง องค์ประกอบหลายส่วนของระบบชนิดนี้ยังไม่มีมาตรฐาน เช่น ระบบระบุตัวตนของผู้ใช้เพื่อเรียกเก็บเงินในภายหลัง และการระบุตำแหน่งใช้งานเป็นต้น ในขณะที่บริษัทผู้ให้บริการสื่อสารยังให้บริการในวงกว้างที่มีคุณสมบัติเชื่อมโยงเครือข่ายที่จำกัดอยู่

องค์ประกอบส่วนอื่นๆ ที่กำลังอยู่ในระหว่างการติดตั้งก็คือการเชื่อมโยงเครือข่ายระหว่างเทคโนโลยีและผู้ให้บริการที่แตกต่างกัน รวมทั้งเครือข่ายข้อมูลโมไบล์ที่อิงกับมาตรฐาน 3G อีกด้วย ในขณะที่เทคโนโลยีโมไบล์ไอพีที่ซิสโก้เป็นผู้บุกเบิกมีโซลูชันมาตรฐานที่ช่วยรองรับการเชื่อมโยงเครือข่ายเข้าด้วยกันได้แล้ว

อีกเรื่องหนึ่งที่น่าสนใจก็คือระบบเสียงผ่าน 802.11 ผู้ค้าบางรายเปิดตัวโทรศัพท์โหมดคู่ออกมาแล้ว ซึ่งทำงานกับระบบ GSM และโครงสร้างพื้นฐานไร้สายแบบ 802.11 ได้ โทรศัพท์โหมดคู่จะช่วยให้ผู้ใช้ PWLAN ประหยัดค่าโทรศัพท์ได้ ตัวอย่างเช่น เจ้าหน้าที่รักษาความปลอดภัยของสนามบินอาจจะใช้เครือข่าย 802.11 เพื่อรองรับการสื่อสารเสียงภายในตัวอาคาร และเปลี่ยนไปใช้เครือข่าย GSM เมื่อพวกเขาเดินออกไปนอกตัวอาคาร เป็นต้น

ท้ายสุด ผู้ให้บริการบางรายมีการติดตั้งอุปกรณ์ 802.11 ภายนอกอาคารแล้ว ซึ่งจะช่วยให้มีการติดต่อสื่อสารอย่างกว้างขวางจากร้านกาแฟข้างถนนและสถานที่สาธารณะกลางแจ้ง เช่น สวนสาธารณะและโรงละครเป็นต้น ซิสโก้พยายามตอบสนองความต้องการดังกล่าวโดยใช้โซลูชัน Metropolitan Mobile Network ซึ่งช่วยให้รัฐบาลท้องถิ่นและหน่วยงานซึ่งดูแลการคมนาคมมีเครือข่ายบรอดแบนด์ที่ปลอดภัยใช้งานทั่วเมือง ซึ่งจะช่วยให้เกิดแอพพลิเคชันใหม่ๆ ตามมา โดยการขยายบริการจากโครงสร้างพื้นฐานที่มีสายไปสู่เครือข่ายไอพีไร้สายได้ โซลูชันเหล่านี้เสนอวิธีการใหม่ๆ สำหรับหน่วยงานสาธารณะที่จะจัดการการสื่อสารและบริการต่างๆ ไปยังพนักงานและประชาชนของตนให้รวดเร็วขึ้น ■