บทที่

11

การเข้าถึงแบบจุดต่อจุด (Point–to–Point Access)

Point–to–Point protocols define the access to the media where there exists one dedicated link between two communicating nodes.

Point–to–Point Access นิยามการเข้าใช้ตัวกลาง (Media) ของอุปกรณ์การสื่อสาร ในรูปแบบหนึ่ง โดย อุปกรณ์คู่สายเข้าใช้การเชื่อมต่อที่สงวนไว้สำหรับอุปกรณ์คู่นั้น โดยเฉพาะ (Dedicated Link) ตลอดช่วงการสื่อสาร ดังรูป

FIGURE 11.1 แนวคิดการเชื่อมต่อที่สงวนไว้สำหรับอุปกรณ์ 1 คู่ โดยเฉพาะซึ่งเป็นพื้นฐานของ Point to Point Access Protocol

การเข้าถึงตัวกลางอีกรูปแบบหนึ่งที่เทียบเคียงกันได้แก่ Multiple Access

Multiple Access Protocol นิยามการเข้าใช้ตัวกลาง ของอุปกรณ์การสื่อสาร ในทางตรงข้ามกับ Point–to–Point Protocol (PPP) กล่าวคือ มีการจัดสรรการเชื่อมต่อ ไว้สำหรับให้อุปกรณ์ทุกตัวในระบบ *เข้าใช้ร่วมกัน* (Shared Link)

ข้อกำหนดของการสื่อสารแบบจุดต่อจุด

Point-to-Point Protocol (PPP) นิยมใช้กันแพร่หลาย (แต่ไม่จำกัดอยู่เพียงแค่นี้เท่านั้น) โดยผู้ใช้ Internet สำหรับเชื่อมต่อ Computer กับผู้ให้บริการ Internet (ISP) ผ่านทางสื่อหลายทาง อาทิเช่น MODEM ธรรมดา DSL MODEM และ Cable MODEM เป็นต้น

PPP ระบุข้อกำหนดในการสื่อสาร ในหัวข้อต่อไปนี้

- นิยามรูปแบบของกรอบข้อมูล (Frame Format) สำหรับการแลกเปลี่ยนระหว่างอุปกรณ์

- นิยาม ข้อตกลง (Negotiate) ระหว่างอุปกรณ์ในการริเริ่มการเชื่อมต่อ (Establishing the Link)
- นิยาม การจำกัดการเข้าถึงข้อมูล (Encapsulate) จาก Network Layer ใน Data Link Frame
- นิยาม วิธีการตรวจสอบ (Authenticate) ซึ่งกันและกันระหว่างอุปกรณ์

รูปแบบของกรอบข้อมูล
รูปแบบของกรอบข้อมูล (Frame Format) ใน PPP ใช้รูปแบบเดียวกับ HDLC ดังรูป

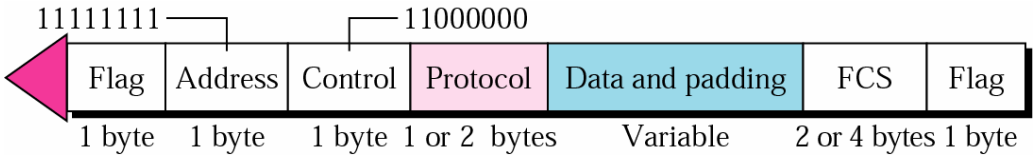


FIGURE 11.2 แผนผังแสดง Frame Format สำหรับ PPP

สำหรับแต่ละ Field ภายใน PPP Frame มีข้อกำหนดดังต่อไปนี้

- **Flag** ทำหน้าที่ระบุขอบเขตของ PPP Frame (เป็นค่าคงที่ 0111 1110)
- **Address** เป็นการสื่อสารระหว่างจุด จึงไม่ต้องระบุ (เป็นค่าคงที่ 1111 1111)
- **Control (U-frame)** ระบุว่าใน Frame นั้นไม่มี Sequence Number และ ไม่มี Flow หรือ Error Control (เป็นค่าคงที่ 1100 0000)
- **Protocol** ระบุชนิดของข้อมูลใน Frame นั้น
- **Data and Padding** บรรจุตัวข้อมูล หรือข่าวสารต่างๆ
- **Frame Check Sequence** (FCS) ได้แก่ CRC ขนาด 2 หรือ 4 Bytes

HDLC (High-Level Data Link Control) เป็นการข้อกำหนดของการสื่อสารข้อมูลชนิด Bit-oriented Synchronous พัฒนาโดย ISO ซึ่งมีการนิยามโครงสร้างของ กรอบข้อมูล (Frame Format) องค์ประกอบของกระบวนการ (Elements of Procedure) และ ลำดับชั้นของกระบวนการ ทั้งแบบสมดุล และไม่สมดุล (Balanced and Unbalanced Classes of Procedure) ในปัจจุบันนิยมใช้สำหรับเชื่อมต่อระหว่างอุปกรณ์สื่อสาร 2 ตัว

สถานะของการเปลี่ยนแปลง
การสื่อสารแบบ PPP มีการดำเนินไปเป็นลำดับสถานะ (Phases) แสดงดังแผนผัง ซึ่งประกอบด้วย 5 สถานะได้แก่

- **สถานะว่าง** (Idle) สถานะนี้ไม่มีการใช้ช่องสัญญาณ และไม่มีสัญญาณพาหะ

- **สถานะริเริ่มการเชื่อมต่อ** (Establishing Link) PPP จะเข้าสู่สถานะนี้ เมื่ออุปกรณ์ด้านหนึ่ง ร้องขอการเชื่อมต่อ ในขั้นตอนนี้จะมีการตกลง เงื่อนไขระหว่างอุปกรณ์ทั้งสองฝั่ง ซึ่งถ้าสำเร็จ ขั้นตอนต่อไป จะเป็นได้ 2 กรณี กล่าวคือ
    - ไปยังสถานะ Authentication *หรือ*
    - ผ่านไปยังสถานะ Network โดยตรง (ไม่ต้องมีการตรวจสอบสิทธิ์)
- **สถานะตรวจสอบสิทธิ์** (Authentication) สถานะนี้ เป็นการตรวจสอบสมบัติของอุปกรณ์ทั้งสองฝั่ง เพื่อตัดสินว่าจะดำเนินการต่อไปหรือไม่ ในขั้นนี้จะเป็นการแลกเปลี่ยน Authentication Packet ระหว่างกัน
- **สถานะแลกเปลี่ยนข้อมูล** (Networking: Exchanging Data and Controls) สถานะนี้เป็นสถานะหลักของ PPP ซึ่งประกอบด้วยการแลกเปลี่ยน Control Packet และ Data Packet ระหว่างอุปกรณ์ทั้งสองฝั่ง
- **สถานะยุติการเชื่อมต่อ** (Terminating Link) สถานะนี้เป็นสถานะที่มีการแลกเปลี่ยน Packet ที่ใช้สำหรับการยกเลิกการเชื่อมต่อ

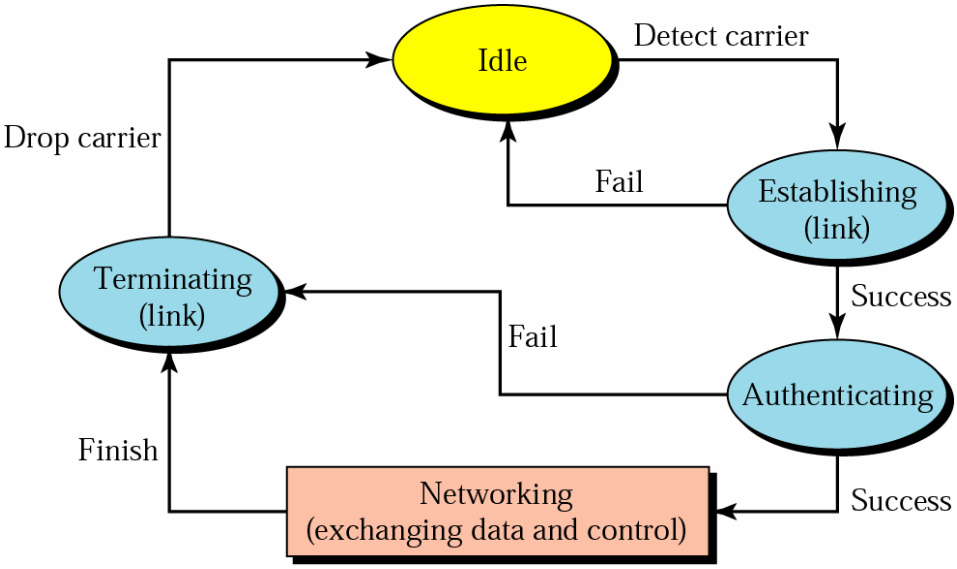


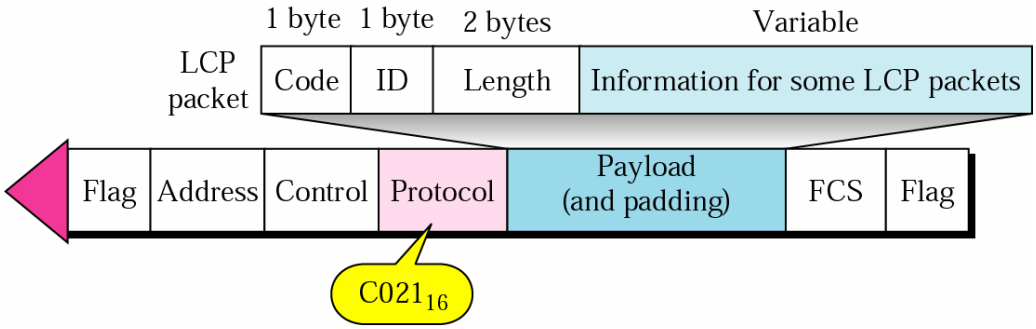
FIGURE 11.3 แผนผังแสดงความสำคัญความสัมพันธ์ต่อเนื่องของแต่ละสถานะใน PPP

PPP Stack ถึงแม้ว่า PPP จะจัดอยู่ใน Data Link Layer แต่ PPP ได้มีการเรียกใช้ ลำดับขั้นของ Protocol อีก 3 ชนิด เพื่อเพิ่มประสิทธิภาพในการทำงาน โดยระบุค่าใน Protocol Field ได้แก่

1. Link Control Protocol (LCP)
2. Authentication Protocol และ
3. Network Control Protocol (NCP)

Link Control Protocol (LCP)

LCP มีหน้าที่รับผิดชอบเฉพาะเรื่องที่เกี่ยวกับการเชื่อมต่อ (เฉพาะสถานะ Establishing/Terminating Link เท่านั้น) ได้แก่ ริเริ่มการเชื่อมต่อ (Establishing Link) ปรับแต่งการเชื่อมต่อ (Configuring Link) เจรจาเงื่อนไขข้อตกลงในการริเริ่มการเชื่อมต่อ (Negotiating Link) ดูแลรักษาการเชื่อมต่อ (Maintaining Link) และ ยกเลิกการเชื่อมต่อ (Terminating Link) สำหรับ Protocol นี้จะไม่มีการแลกเปลี่ยน User Data ดังรูป หมายเลขระบุ LCP เป็นค่าคงที่ $C021_{16}$



ข้อมูลในแต่ละตำแหน่งของ LCP Packet อธิบายได้ดังนี้

- **Code** ระบุชนิดของ LCP Packet ซึ่งขึ้นกับ Function ในขณะนั้น
- **ID** หมายเลขของ LCP ซึ่งจะต้องตรงกัน ทั้งด้านรับ (Request Packet) และด้านส่ง (Reply Packet)
- **Lengths** ระบุความยาวของ LCP Packet
- **Information** บรรจุข่าวสารพิเศษที่จำเป็นต่อ LCP Packet บางชนิด

ตารางด้านล่างแสดง Code ประเภท และคำอธิบายของ LCP Packet แต่ละชนิด

Code	Packet Type	Description
01_{16}	Configure-request	Contains the list of proposed options and their values
02_{16}	Configure-ack	Accepts all options proposed
03_{16}	Configure-nak	Announces that some options are not acceptable
04_{16}	Configure-reject	Announces that some options are not recognized
05_{16}	Terminate-request	Requests to shut down the line
06_{16}	Terminate-ack	Accepts the shut down request
07_{16}	Code-reject	Announces an unknown code
08_{16}	Protocol-reject	Announces an unknown protocol
09_{16}	Echo-request	A type of hello message to check if the other end is alive
$0A_{16}$	Echo-reply	The response to the echo-request message
$0B_{16}$	Discard-request	A request to discard the packet

**ACK และ NAK หมายถึง Positive และ Negative Acknowledgement ตามลำดับ*

จากตารางสังเกตว่า LCP Packet สามารถแบ่งออกได้เป็น 3 กลุ่ม ดังนี้

Configuration Packets ใช้ในการเจรจาต่อรอง (Negotiate) เงื่อนไขระหว่างอุปกรณ์ ประกอบด้วยข่าวสาร 4 ชนิด ได้แก่

- Configure-request $(\mathbf{01})_{16}$ อุปกรณ์ผู้ริเริ่มการเชื่อมต่อ ส่งข่าวสารนี้พร้อมกับชุดของ **เงื่อนไข** (Options) ไปยังอุปกรณ์อีกด้านหนึ่ง (ทุก Options จะส่งถูกไปในภายข่าวสารเดียว)

- Configure-ack $(\mathbf{02})_{16}$ เมื่ออุปกรณ์ปลายทางยอมรับเงื่อนไขที่ร้องขอ จะส่งข่าวสารนี้กลับไปยังต้นทาง พร้อมกับยืนยัน Options ดังกล่าว

- Configure-nak $(\mathbf{03})_{16}$ ถ้าอุปกรณ์ปลายทางพิจารณาแล้วพบว่า จำเป็นต้องยกเว้น/ปรับปรุงบางเงื่อนไข จะส่งข่าวสารนี้กลับไปยังต้นทาง เพื่อให้ส่งเงื่อนไขมาใหม่

- Configure-reject $(\mathbf{04})_{16}$ อุปกรณ์ปลายทางจะโต้ตอบกลับด้วยข่าวสาร นี้หากไม่รู้จักเงื่อนไขที่ระบุ และต้นทางต้องทบทวน/ปรับเปลี่ยน เงื่อนไข และทำการส่งใหม่

Link Termination Packets เป็น Packets ที่ใช้สำหรับแจ้ง ยกเลิกการสื่อสาร และการเชื่อมต่อระหว่างอุปกรณ์ทั้งสองฝั่ง ประกอบด้วยข่าวสาร 2 ชนิด ได้แก่

- Terminate-request $(\mathbf{05})_{16}$ อุปกรณ์ด้านใดด้านหนึ่ง สามารถที่จะแจ้งยกเลิกการสื่อสารก็ได้ โดยส่ง Packet ด้วยข่าวสารนี้

- Terminate-ack $(\mathbf{06})_{16}$ อุปกรณ์ปลายทางซึ่งเป็นผู้รับ Terminate-request จะต้องตอบรับด้วยข่าวสารนี้

Link Monitoring and Debugging Packets เป็น Packets ที่ใช้สำหรับเฝ้าดูและตรวจสอบข้อผิดพลาด ประกอบด้วยข่าวสาร 5 ชนิด ได้แก่

- Code-reject $(\mathbf{07})_{16}$ เมื่ออุปกรณ์ด้านสั่งไม่รู้จัก Code ใน Packet ที่ได้รับ

- Protocol-reject $(\mathbf{08})_{16}$ เมื่ออุปกรณ์ด้านสั่งไม่รู้จัก Protocol ใน Packet ที่ได้รับ

- Echo-request $(\mathbf{09})_{16}$ ใช้สำหรับเฝ้าดู/ตรวจสอบการทำงานของ Link ว่าเป็นปรกติหรือไม่ ถ้าปกติ อุปกรณ์ด้านรับจะต้องได้รับ Packet สะท้อนกลับมา (Echo-reply)

- Echo-reply $(\mathbf{0A})_{16}$ อุปกรณ์ปลายทางจะตอบด้วยข่าวสารนี้ กลับไปยังผู้ส่งเมื่อได้รับ Echo-request โดยข้อมูลในส่วน Information จะคัดลอกมาจากข่าวสารที่ได้รับ

- Discard-request $(\mathbf{0B})_{16}$ ใช้สำหรับอุปกรณ์ด้านส่งตรวจสอบการทำงานตัวเอง ด้านรับไม่สนใจข่าวสารนี้

Authentication Protocol

Authentication Protocol เป็น Protocol ที่มีความสำคัญมากสำหรับ PPP ที่ได้ออกแบบมาเพื่อการเชื่อมต่อ โดยการหมุนหมายเลข (Dialup) ซึ่งต้องมีการตรวจสอบ Identity (ID) ของผู้ใช้บริการ ซึ่งจะไม่มีการแลกเปลี่ยน User Data โดยมีการกำหนด Authentication Protocol ไว้ 2 ลักษณะ ได้แก่

1. Password Authentication Protocol (PAP)

PAP เป็นการตรวจสอบความถูกต้องของ Identification (ID) ของผู้ใช้บริการกับรหัสผ่าน (Password) ที่ผู้ใช้ระบุ ซึ่งมีขั้นตอนในการตรวจสอบดังนี้

1) ผู้ใช้ป้อน ID (Login) พร้อมกับรหัสผ่าน (Password) ส่งไปบน PAP Packet

2) ด้านรับตรวจสอบความถูกต้อง แล้วพิจารณา ตอบรับ หรือปฏิเสธ

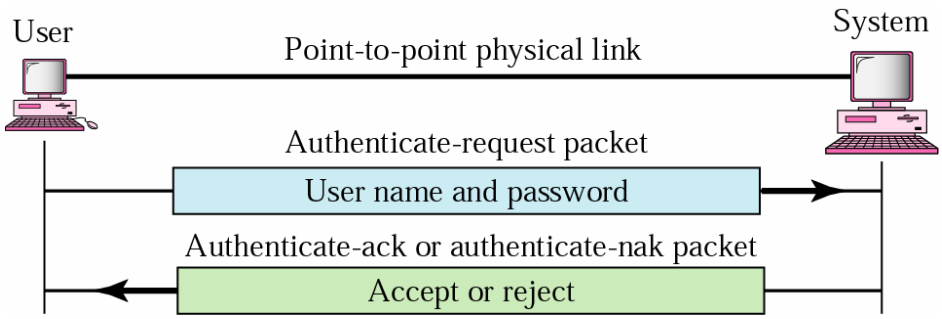
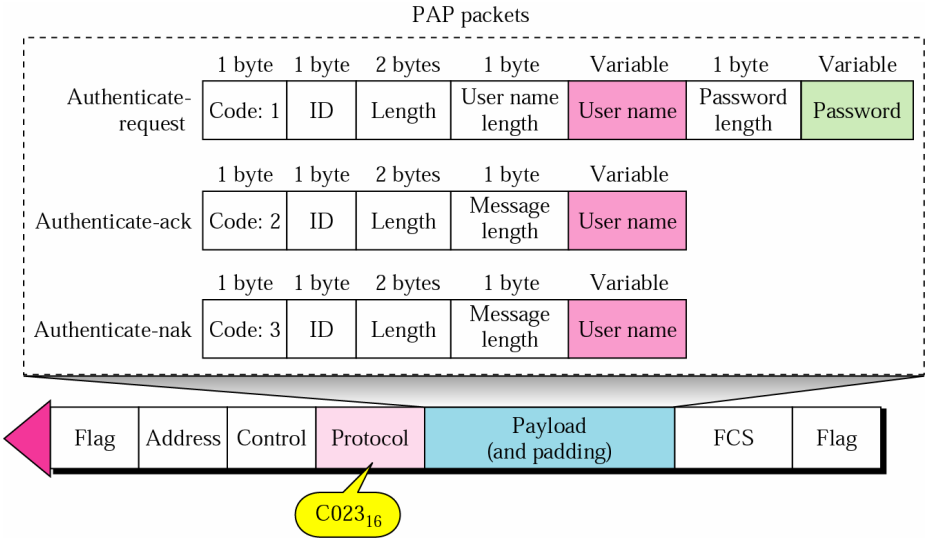


FIGURE 11.4 แผนผังแสดงขั้นตอนของ Password Authentication Protocol (PAP)

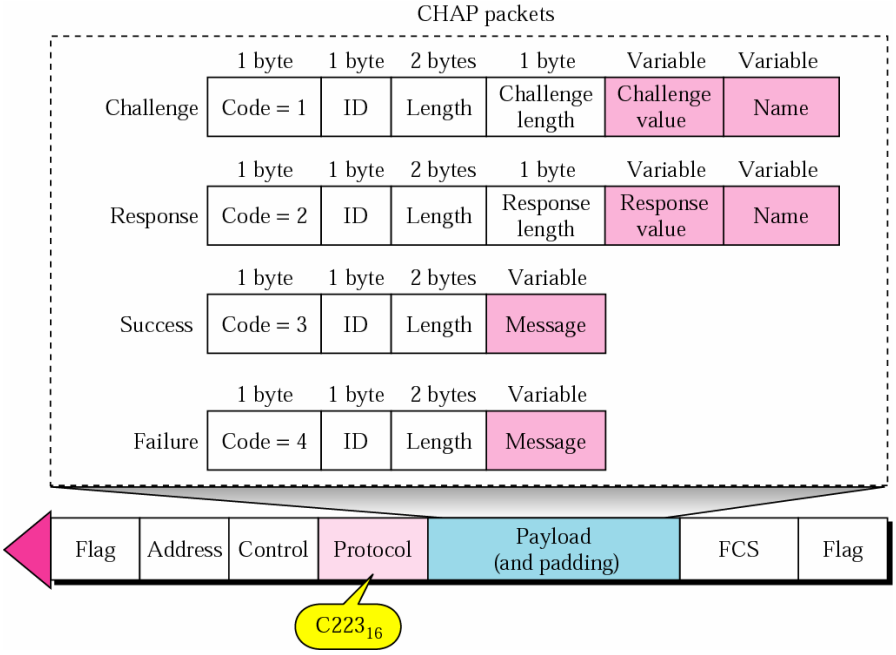
PAP (Code = $C023_{16}$) ประกอบด้วย Packet 3 ชนิดได้แก่ Authenticate-request Authenticate-ack และ Authenticate-nak ดังแผนภาพ



2. Challenge Handshake Authentication Protocol (CHAP)

CHAP เป็นการตรวจสอบความถูกต้องของรหัสผ่านแบบโต้ตอบ โดยอุปกรณ์ที่ให้บริการ (Server) จะถาม "**คำถาม**" เพื่อให้อุปกรณ์ที่ขอใช้บริการ (Client) "**ตอบ**" ซึ่งจะมีกี่ชุดคำถามก็ได้ ซึ่งหากผู้ขอใช้บริการตอบได้สอดคล้องกับข้อตกลงที่ได้ระบุไว้ ทุกชุดคำถาม จึงจะสามารถมีสิทธิ์เข้าใช้ระบบของผู้ให้บริการ

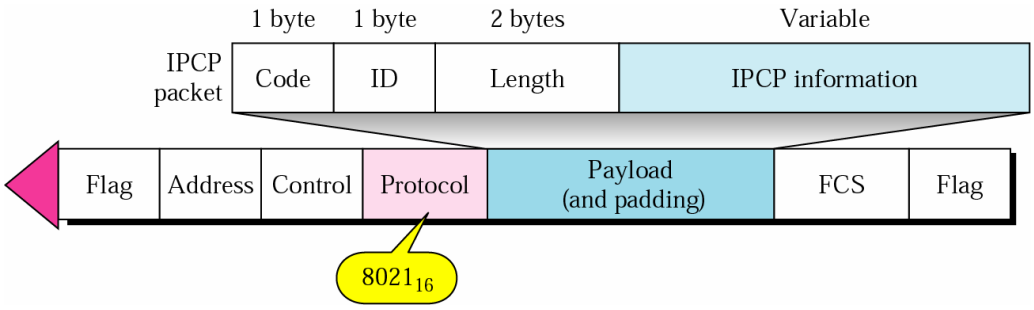
CHAP (Code = $C223_{16}$) ประกอบด้วย Packet 4 ชนิดได้แก่ Challenge Response Success และ Failure ดังแผนภาพ



Network Control Protocol (NCP)

เมื่อการเชื่อมต่อได้ถูกริเริ่ม (Established) แล้วการสื่อสารจะเริ่มเข้าสู่สถานะของ Network เพื่อแลกเปลี่ยนข้อมูล และคำสั่งควบคุม (Data and Controls) ซึ่ง PPP จะใช้ Network Control Protocol (NCP) ซึ่งทำหน้าที่เรียบเรียง และบรรจุข้อมูลจาก Network Layer ลงสู่ Packet ของ PPP Frame

IPCP (Inter-network Protocol Control Protocol) ทำหน้าที่ในการริเริ่มการเชื่อมต่อใน Network Layer ก่อนจะมีการเชื่อมต่อใน Data Link Layer (ดังแผนผังในรูปที่ 11.4)



การนิยามชนิดของ IPCP Packet ทำได้โดยระบุรหัสดังตาราง ตัวอย่างเช่น คู่การสื่อสาร (Party) ใช้ Code 01 (Configure-request) ในการตกลงตัวเลือกเช่นชุดของ IP Address เมื่อได้ข้อตกลงร่วมกันแล้ว รหัสของ Protocol จะเปลี่ยนเป็น 0021_{16} เพื่อแสดงว่า Packet เป็นของ IP (Layer 3) ไม่ใช่ IPCP (Layer 2) เมื่อการสื่อสารสิ้นสุด ใช้ Code 05 (Terminate-request) เพื่อยุติการเชื่อมต่อ

Code	IPCP Packet
01	Configure-request
02	Configure-ack
03	Configure-nak
04	Configure-reject
05	Terminate-request
06	Terminate-ack
07	Code-reject

กระบวนการสำหรับกรณีทั่วไป และตัวอย่าง
การบวนการสำหรับกรณีทั่วไปของ PPP สามารถสรุปได้ดังแผนผังต่อไปนี้

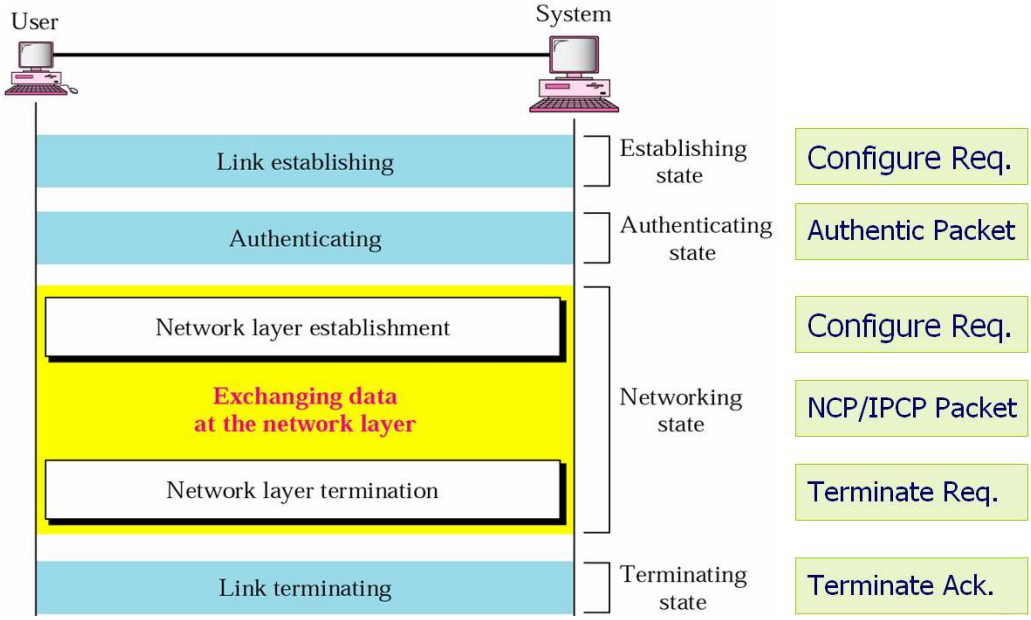


FIGURE 11.4 แผนผังแสดงขั้นตอนกรณีทั่วไปของการเชื่อมต่อด้วย PPP (ซ้าย) พร้อมกับชนิดของ Packet ที่เกี่ยวข้อง (ขวา)

สำหรับตัวอย่างการประยุกต์ใช้งาน PPP อันหนึ่งได้แก่ Dialup Internet Connection ซึ่งประกอบด้วยขั้นตอนดังต่อไปนี้

- จากสถานะ Idle เมื่อผู้ใช้คลิกเลือกการ เชื่อมต่อ PPP จะเริ่มทำงาน (Establishing Link)
- ผู้ใช้ระบุ Login และ Password ในการเข้าใช้ระบบ
- ระบบเข้าสู่กระบวนการ Authentication เพื่อตรวจสอบ Account ของผู้ใช้
- ถ้าการตรวจสอบครบถ้วนสมบูรณ์ผู้ใช้จึงสามารถเชื่อมต่อกับระบบได้ พร้อมทำการแลกเปลี่ยนข้อมูลใน Network Layer ต่อไป จนกว่าฝ่ายใดฝ่ายหนึ่งจะร้องขอให้ยุติการเชื่อมต่อ (Terminating Link)

แบบฝึกหัด

1. อธิบายหลักการของ Point to Point Access มาพอสังเขป
2. ศึกษา และอภิปราย รูปแบบต่างๆ ในการเชื่อมต่อ Internet ของผู้ใช้ทั่วไปผ่าน PPP
3. Protocol ของ Point to Point Access ได้มีการระบุข้อกำหนดการสื่อสารในประเด็นใดบ้าง
4. อธิบายความหมาย และหน้าที่ของ Field ต่างๆ ใน PPP Frame
5. อธิบายขั้นตอนการทำงานของ PPP จากแผนผังการเปลี่ยนสถานะ (Transition State)
6. จากแผนผังการเปลี่ยนสถานะของ PPP ถ้าหากขั้นตอนริเริ่มการเชื่อมต่อ (Link Establishing) ล้มเหลวแล้วระบบจะอยู่ในสถานะใด
7. อธิบายความแตกต่างของหน้าที่ ระหว่าง LCP Authentication Protocol และ NCP ใน PPP Stacks
8. LCP สามารถจำแนก Packet ออกได้เป็นกี่ชนิด และแต่ละชนิดมีหน้าที่รับผิดชอบอย่างไรบ้าง
9. อภิปรายเปรียบเทียบข้อดี และข้อเสียระหว่าง PAP และ CHAP ในขั้นตอน Authentication
10. ยกตัวอย่าง Protocol ที่อ้างอิง หรือคล้ายคลึงกับ PPP มา 1 ตัวอย่าง