

Chapter 4

Telecommunication Systems

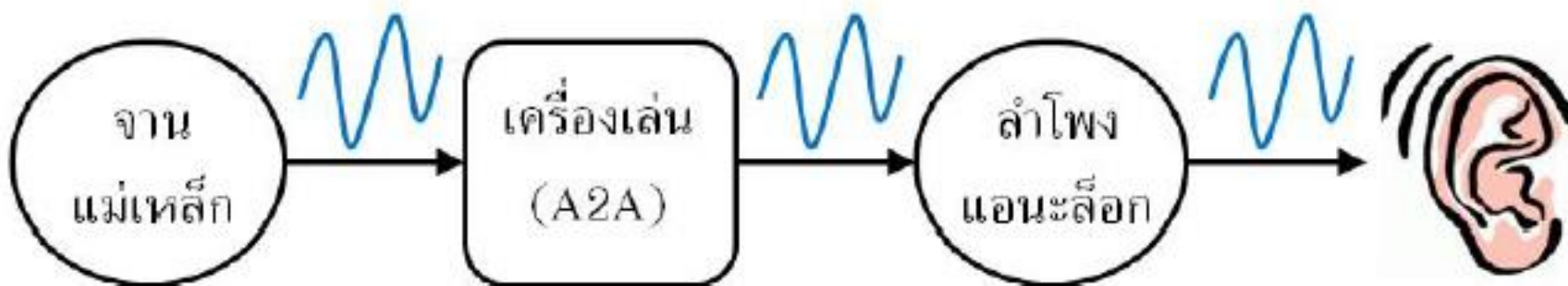
โทรคมนาคม (Telecommunications) 

โทรคมนาคม หมายถึงการสื่อสารระยะไกล โดยใช้เทคโนโลยีต่าง ๆ โดยเฉพาะอย่างยิ่งผ่านทางสัญญาณไฟฟ้า หรือคลื่นแม่เหล็กไฟฟ้า เนื่องจากเทคโนโลยีที่แตกต่างกันจำนวนมากที่เกี่ยวข้องกับคำนี้ จึงมักใช้ในรูปแบบพหูพจน์ เช่น Telecommunications [วิกิพีเดีย](#)

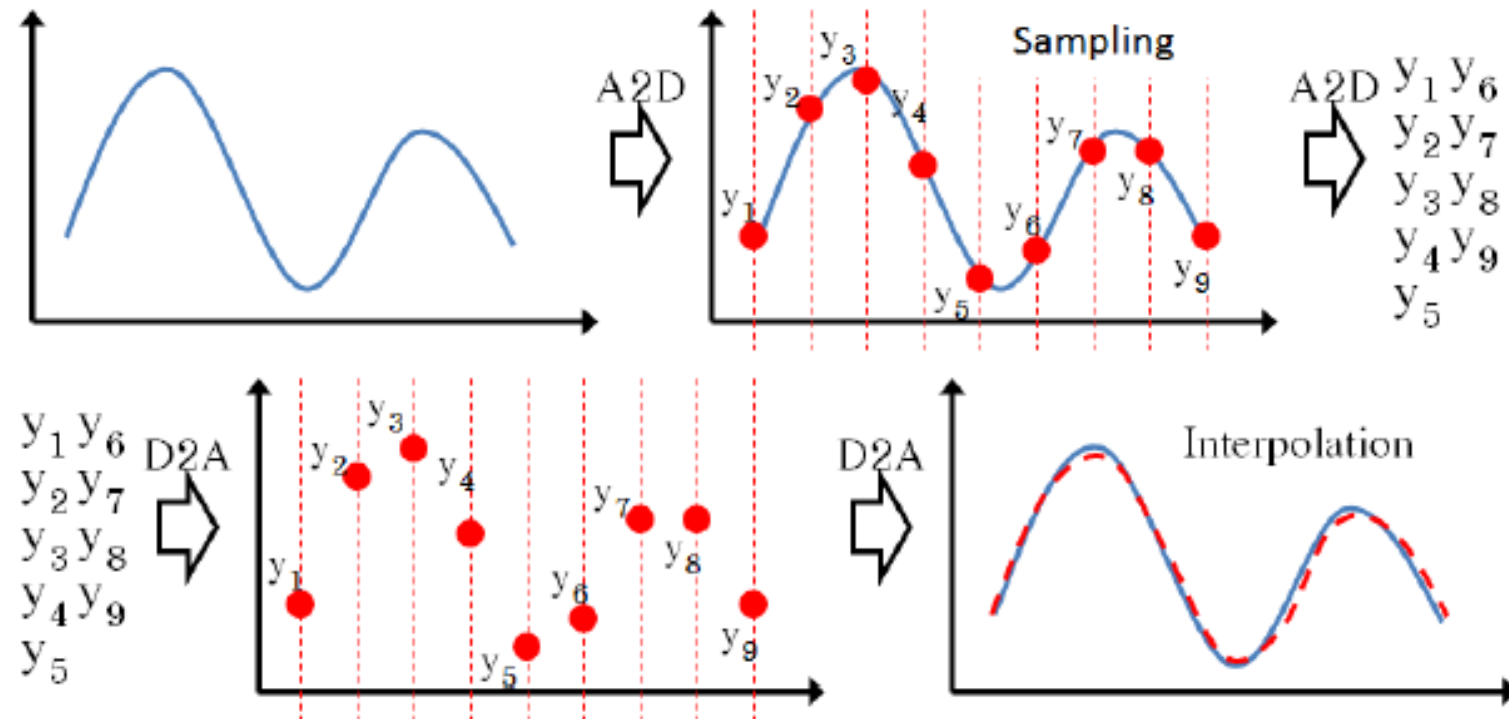
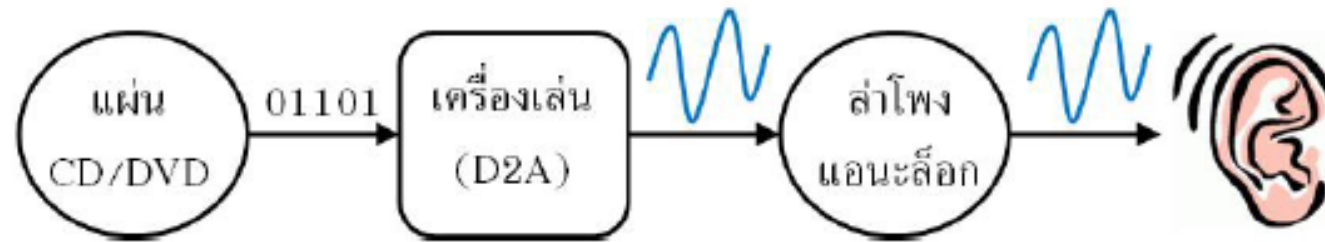
Analog vs. Digital



ข้อเสียคือมีการรบกวน ทำให้สัญญาณเพี้ยนไป
และเข้ารหัสข้อมูลไม่ได้



ข้อดีคือสัญญาณไม่เพี้ยนเลย
(ถ้าการรบกวนไม่มากเกินไป)
เข้ารหัสข้อมูลได้ง่าย ปลอดภัย

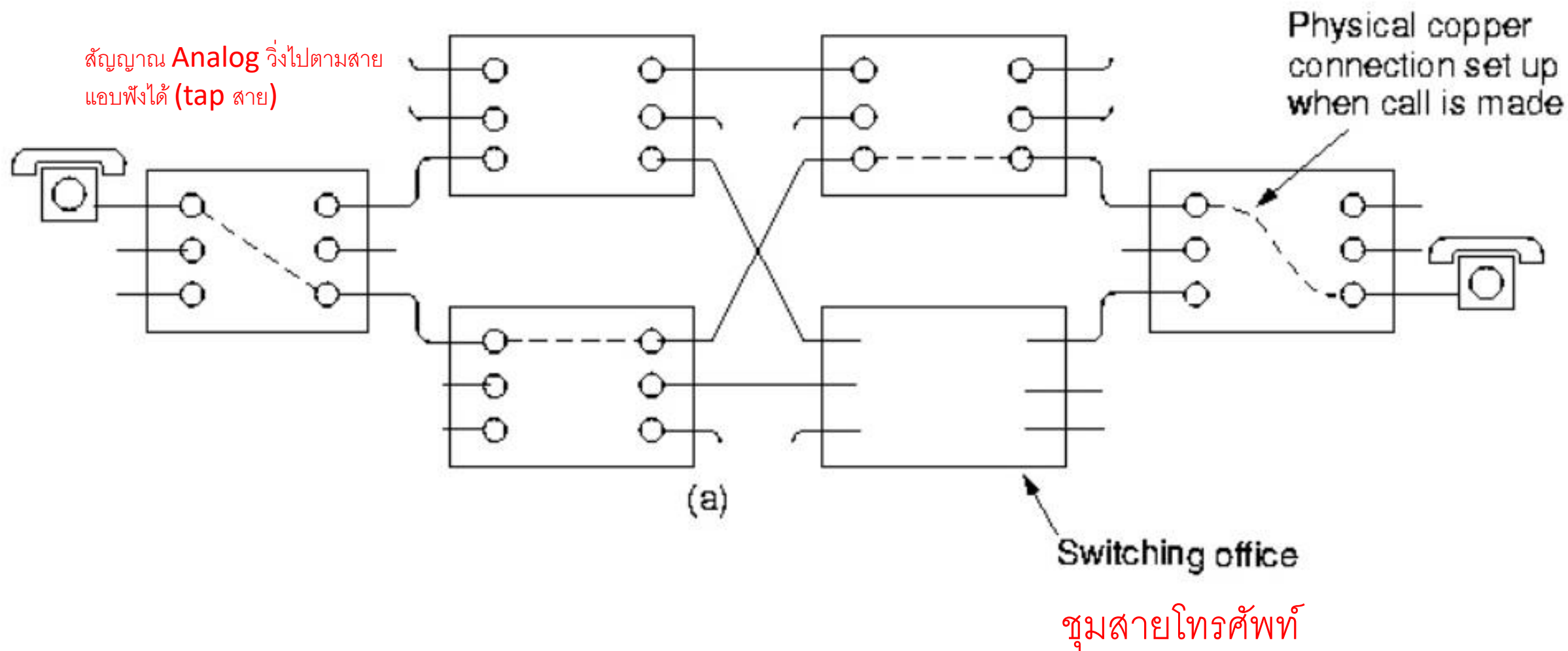


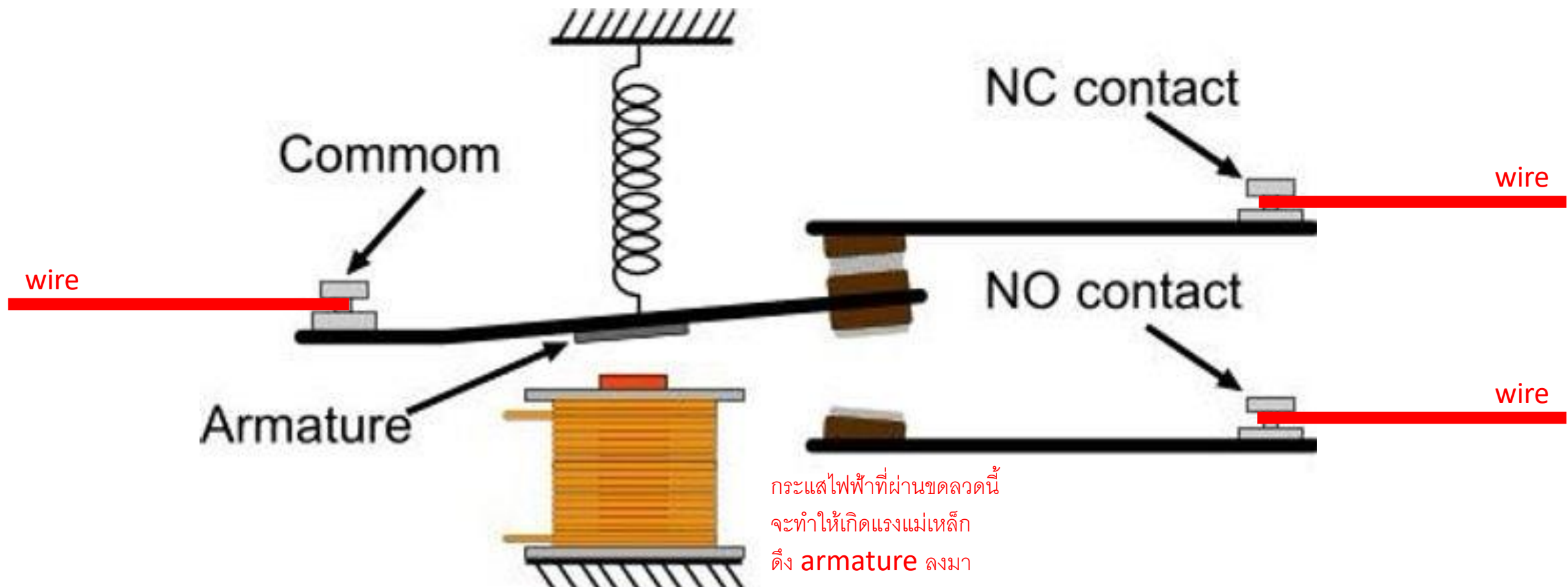
Public Switched Telephone Network (PSTN)

Plain Old Telephone Service (POTS)



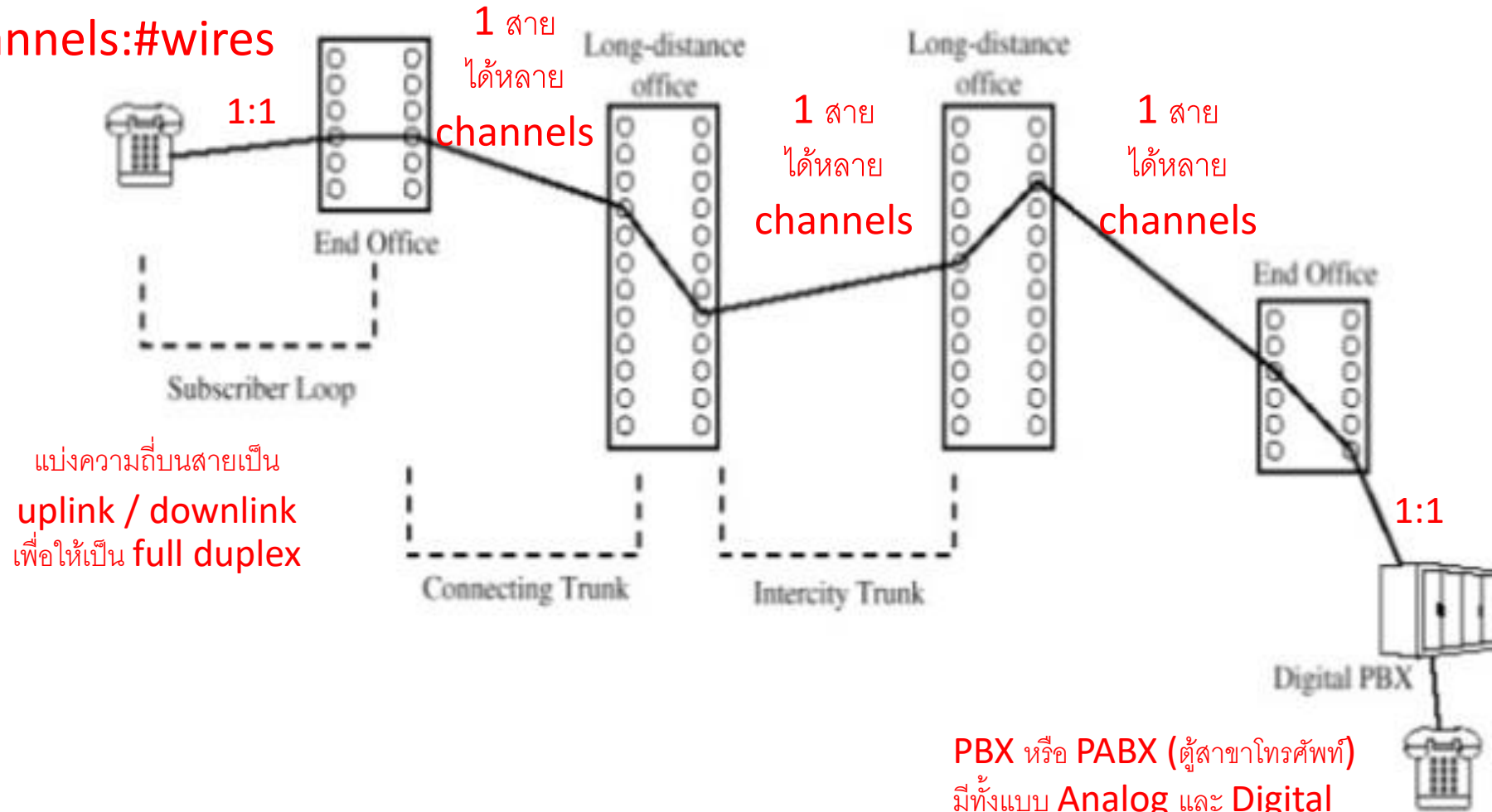
Circuit switched vs. Packet switched





อัตราส่วน

#channels:#wires

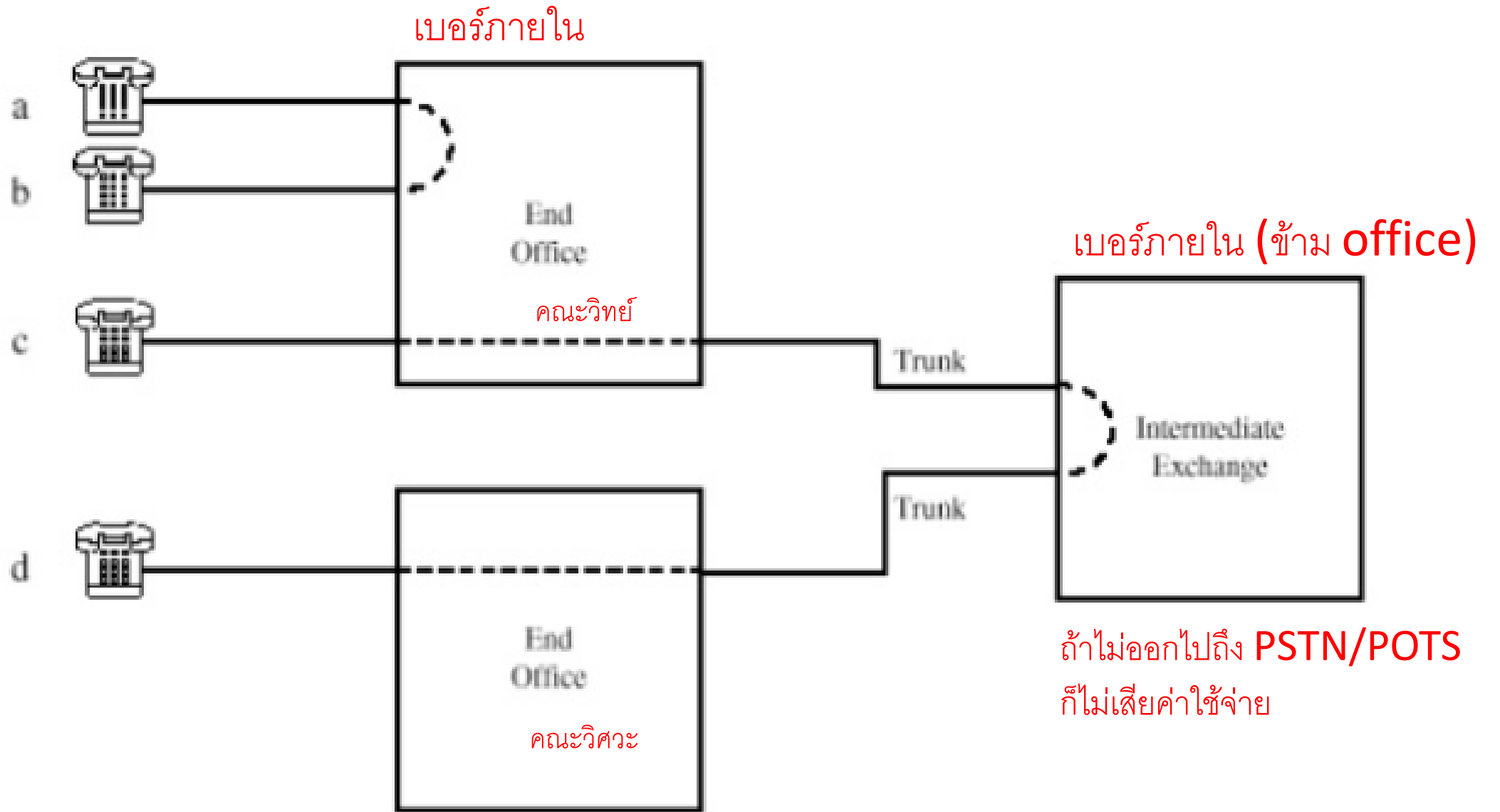


แบ่งความถี่บนสายเป็น
uplink / downlink
เพื่อให้เป็น full duplex

PBX หรือ PABX (ตู้สาขาโทรศัพท์)

มีทั้งแบบ Analog และ Digital

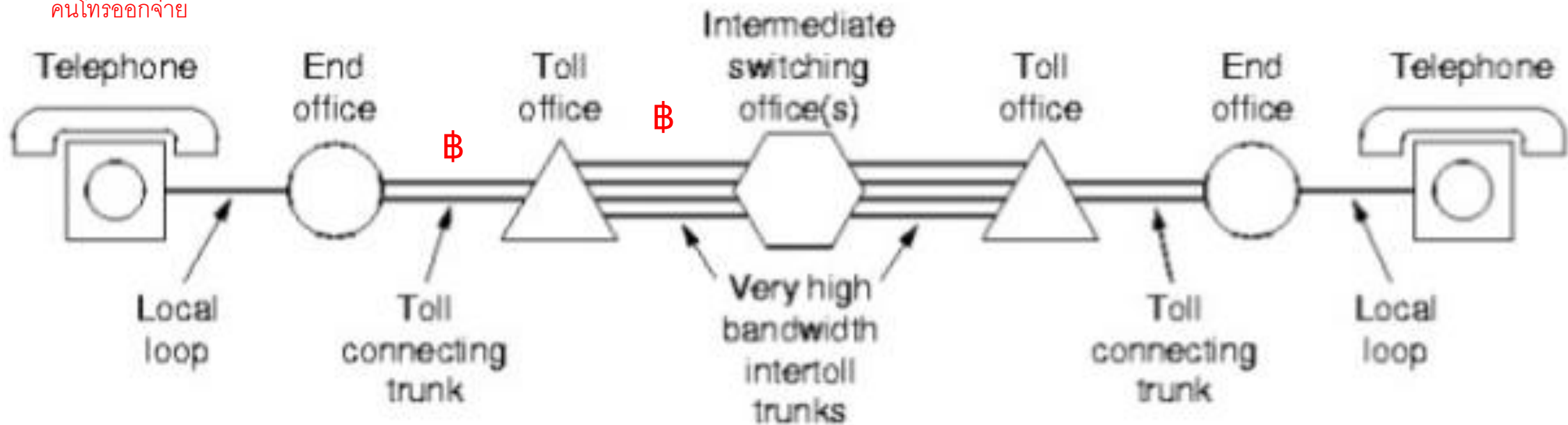
ทำให้โทรภายในได้ และทำให้มีโทรศัพท์
มากกว่าจำนวนสาย (เส้นทาง) ได้ แต่โทร
ออกพร้อมกันทุกเครื่องไม่ได้

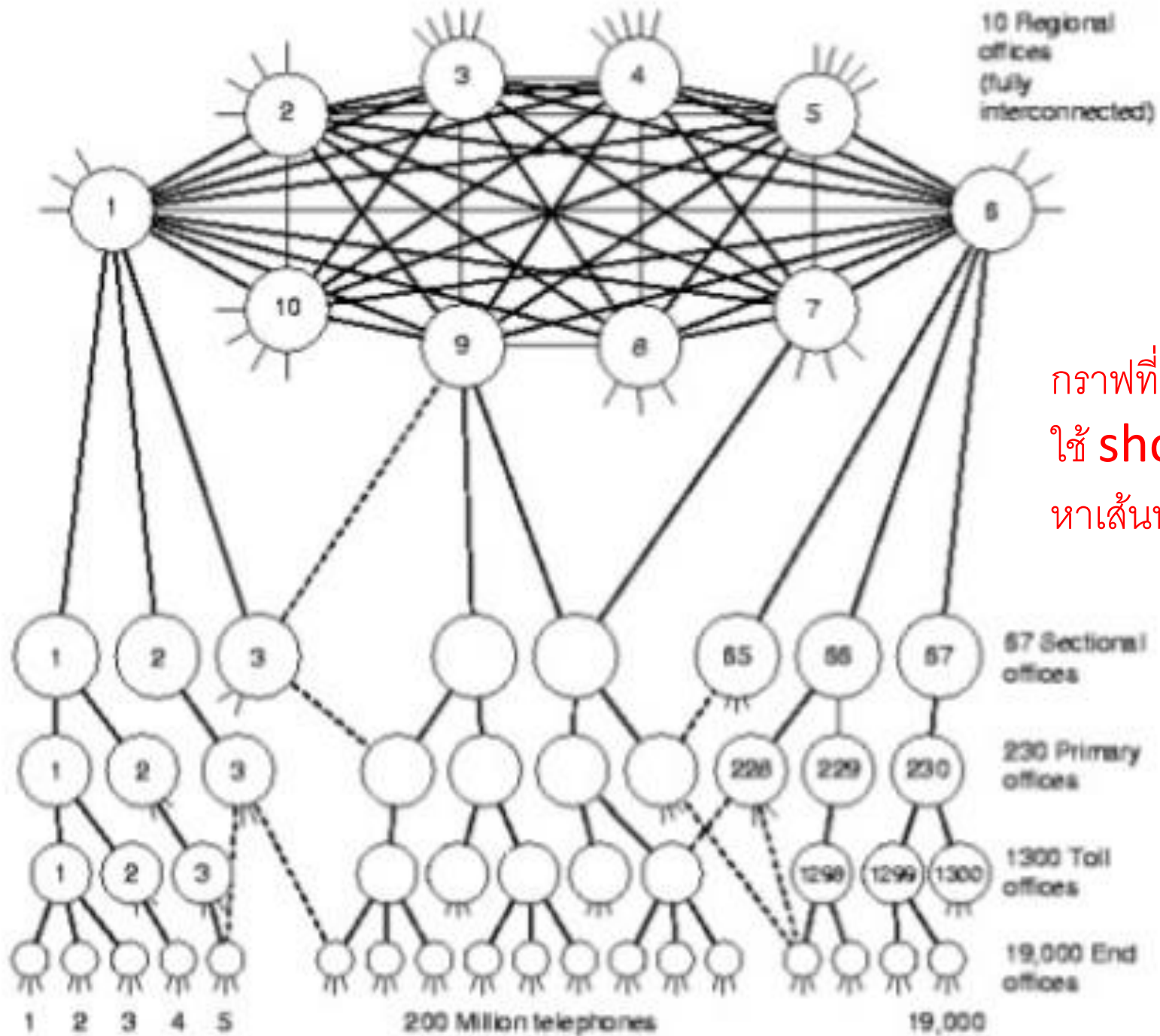


ข้ามจังหวัด/ประเทศ
นาทีละ 10/100 บาท

ในจังหวัดครั้งละ 3 บาท

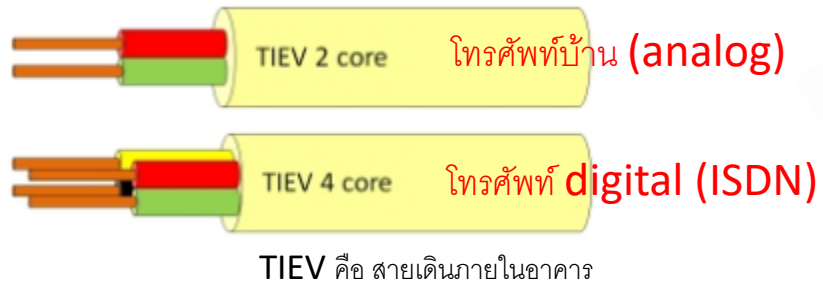
คนโทรออกจ่าย



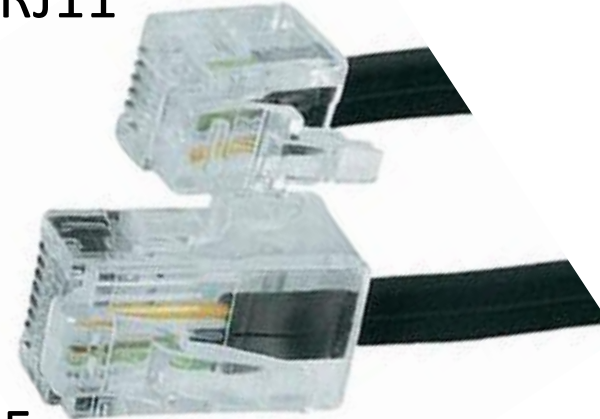


กราฟที่แต่ละเส้นเชื่อมมี **weight (cost)**
ใช้ **shortest path algorithm**
หาเส้นทางที่มีค่าใช้จ่ายน้อยที่สุด

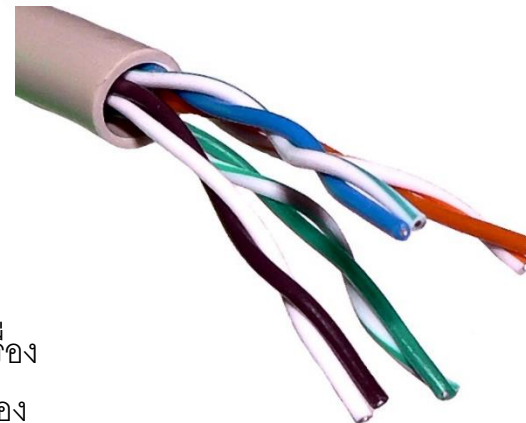
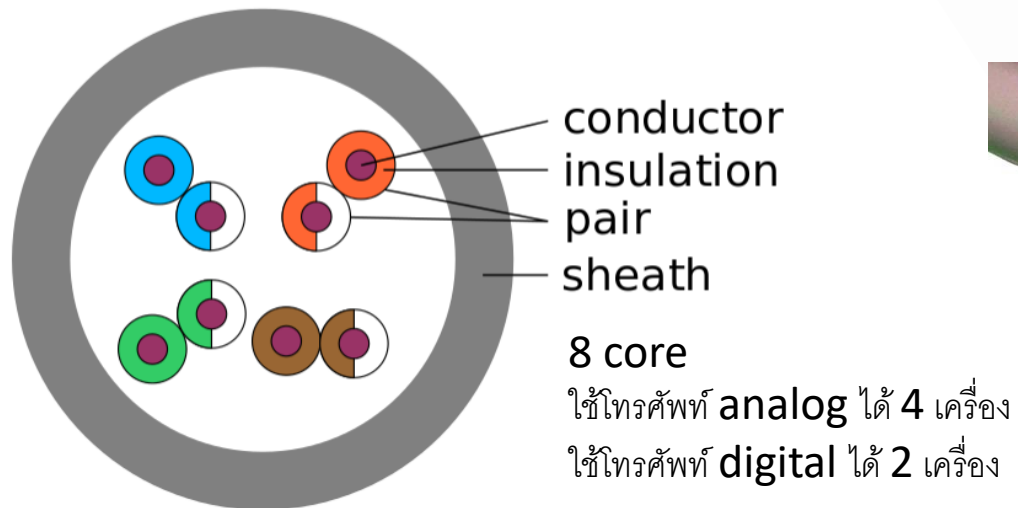
สาย Unshielded Twisted Pair (UTP)



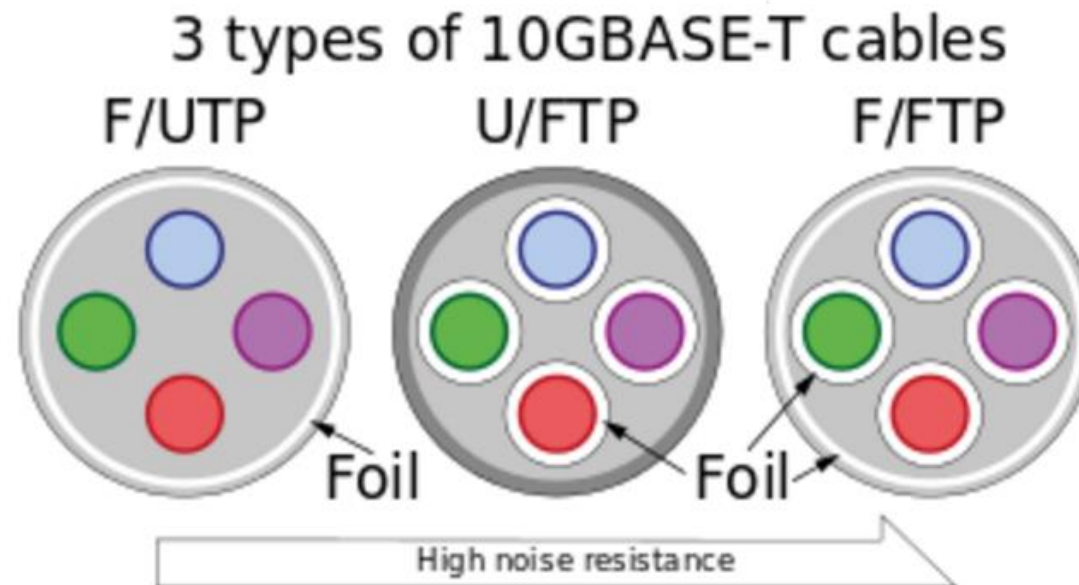
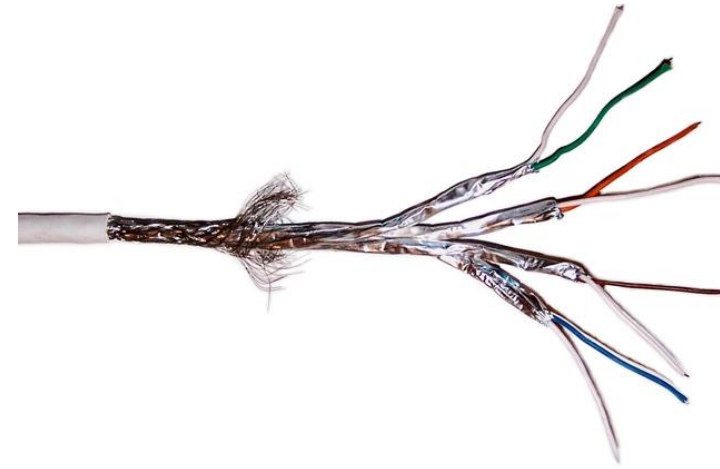
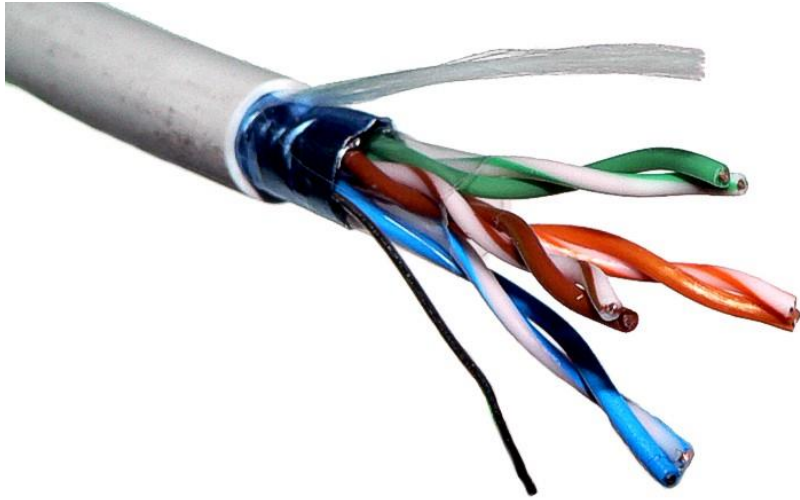
RJ11



RJ45



สาย Foiled UTP และ Shielded UTP



Modem

ใช้โทรศัพท์พร้อมกับโมเด็มไม่ได้
ปัจจุบันเน็ตบ้านก็ใช้สายโทรศัพท์
แต่ใช้ความถี่ที่สูงกว่า
ไม่ชนกับเสียงพูด

สายโทรศัพท์บ้าน
(RJ11)

ต้องโทรออกหา ISP ก่อน
ครั้งละ 3 บาท สายหลุดก็
ต่อใหม่ เสียอีก 3 บาท

ส่งสัญญาณ digital ผ่านช่องสัญญาณ analog (เสียงพูด)
ที่มี bandwidth แคบ ($< 4 \text{ KHz}$)



Serial Port
(สมัยนั้นไม่มี USB)

PC



ได้ data rate สูงสุด
ประมาณ 56K bit/s



Integrated Services Digital Network (ISDN)

Abbreviation of integrated services digital network, an international communications standard for sending voice, video, and data over digital telephone lines. ISDN requires special metal wires and supports data transfer rates of 64 Kbps (64,000 bits per second). Most ISDN lines offered by telephone companies give you two lines at once, called B channels. You can use one line for voice and the other for data, or you can use both lines for data to give you data rates of 128 Kbps, four or five times the data rate provided by today's fastest modems. 17

ต้องใช้สายพิเศษ (4c)

ใช้สายโทรศัพท์เดิม (2c) ไม่ได้

The original version of ISDN employs baseband transmission. Another version, called B-ISDN, uses broadband transmission and is able to support transmission rates of 1.5 million bits per second and higher. B-ISDN requires fiber optic cables and is not widely available.

	B channel	D channel
Basic Rate Interface (BRI)	2 x 64 kbit/s	1 x 16 kbit/s
Primary Rate Interface (PRI)	23 x 64 kbit/s	1 x 16 kbit/s (US, T1)
	30 x 64 kbit/s	1 x 16 kbit/s (AUS, E1)
Narrowband ISDN (N-ISDN)	64 kbit/s (ออกมาตราฐานต่ำ ออกมาก็ล้าสมัย data rate น้อย)	
Broadband ISDN (B-ISDN)	> 1.5 - 2 Mbit/s (primary rate) ถูกกลืนด้วย tech อื่นๆ เช่น DSL	

ISDN ออกแบบมาเพื่อ circuit-switched network (ต้องโทรออกก่อน ไม่เหมาะกับ internet)

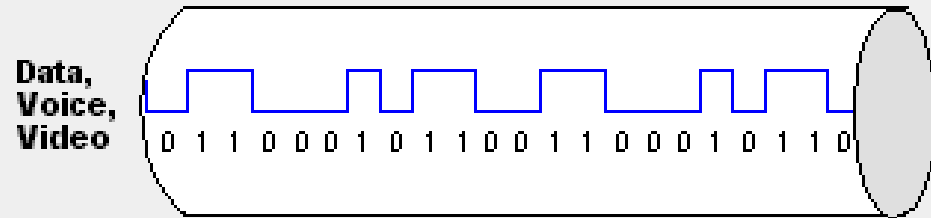
Digital Subscriber Line (DSL) ออกแบบมาเพื่อ packet-switched network

ISDN vs. DSL อ่าน <http://www.tech-faq.com/difference-between-isdn-and-dsl.html>

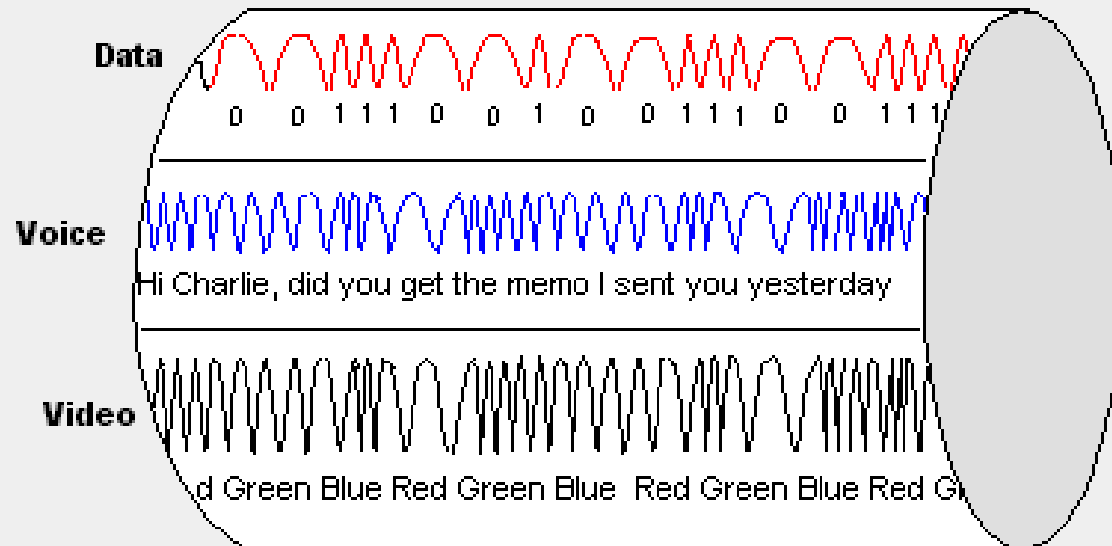
Baseband vs. Broadband

BASEBAND & BROADBAND (TDM & FDM)

BASEBAND (TDM, interleaves digital signals)



BROADBAND (FDM, true simultaneous)



เช่น Cable TV, Internet, Telephone, Radio มาในสายเดียวกัน

In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. Baseband communication is bi-directional, which means that the same channel can be used to send and receive signals. In Baseband, frequency-division multiplexing is not possible.

Broadband sends information in the form of an analog signal. Each transmission is assigned to a portion of the bandwidth, hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible.

<http://www.omnisecu.com>

ในความหมายทั่ว ๆ ไป

broadband = high-speed internet

Table 8.6 Comparison of xDSL Alternatives**DSL ใช้สายโทรศัพท์ที่มีอยู่แล้วได้ (2c) ไม่ต้องใช้สายใหม่ (4c)**

	ADSL	HDSL	SDSL	VDSL
Data Rate	1.5–9 Mbps downstream 16–640 kbps upstream	1.544 or 2.048 Mbps	1.544 or 2.048 Mbps	13–52 Mbps downstream 1.5–2.3 Mbps upstream
Mode	Asymmetric	Symmetric	Symmetric	Asymmetric
Copper Pairs	1	2	1	1
Range (24-Gauge UTP)	3.7–5.5 km	3.7 km	3.0 km	1.4 km
Signaling	Analog	Digital	Digital	Analog
Line Code	CAP/DMT	2B1Q	2B1Q	DMT
Frequency	1–5 MHz	196 kHz	196 kHz	≥10 MHz
Bits/Cycle	Varies	4	4	Varies

UTP = unshielded twisted pair

3BB VDSL
BROADBAND
Very High Speed Digital Subscriber Line

50/10 Mb

ราคา 700 บาท

Powered by JAS

โทร. 1530
www.3bb.co.th

สมัครได้ที่ศูนย์บริการทั่วประเทศ

รับส่วนลด

50/10 หมายถึง downstream/upstream
ไม่สมมาตร เพราะโดยทั่วไปใช้ downstream มากกว่า

ใน กทม Fiber เป็น norm ไปแล้ว



ติดตั้ง 3BB Fiber
รับสิทธิ์
Fiber Router ฟรี
Dual Band WiFi มูลค่า 2,200 บาท



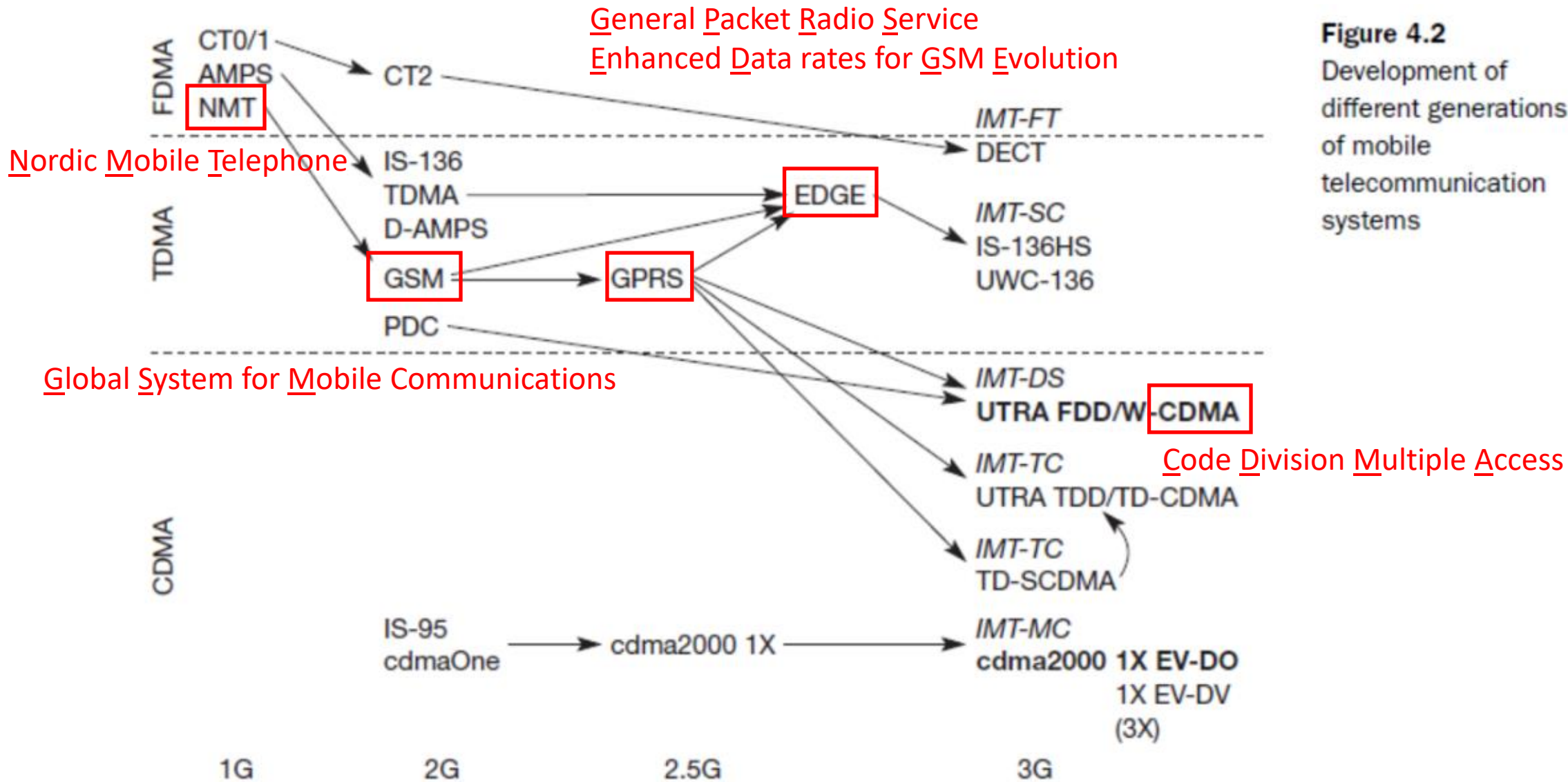
ถึง 30 ก.ย. 61 นี้

Powered by **JAS**

สอบถามโทร. **1530**
สมัครได้ที่ สามบีบีช้อปป หรือตัวแทนขายทั่วประเทศ

*สำหรับแพ็คเกจ 3BB Fiber 50/20Mbps เป็นต้นไป

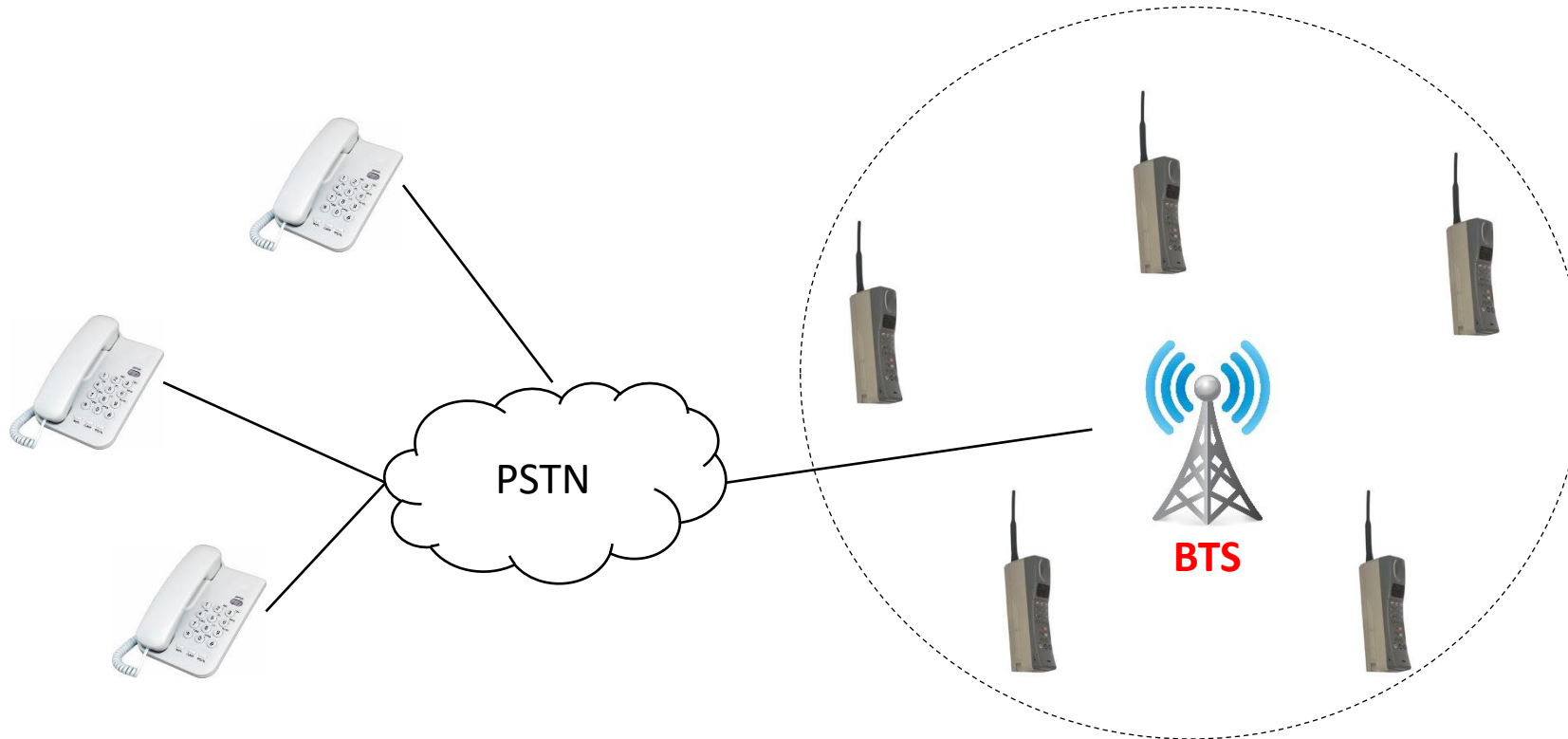
Development of 1G to 3G



1G

A **transceiver** is an electronic device which is a combination of a radio transmitter and a receiver, hence the name.

- ใช้สัญญาณ **Analog** โดรบกวนมาก ไม่ปลอดภัย เข้ารหัสไม่ได้ ใช้ **voice** เท่านั้น ยังไม่มี **data**
- มี **Base Transceiver Station (BTS)** ตัวเดียว นำโทรศัพท์มือถือ (**MS**) ถี้ออกนอกพื้นที่ (**cell**) ไม่ได้
- โทรศัพท์มือถือทุกเครื่องส่งสัญญาณผ่าน **BTS**, **BTS** ทำหน้าที่เป็นตัวกลางระหว่าง **MS** และโทรศัพท์บ้าน
- ใช้ **Frequency Division Multiple Access (FDMA)**
- ระบบ **AMPS (US)**, **TACS (UK)**, **NMT (Nordic countries)**, **C-Netz (Germany)**
- **AMPS** ใช้ความถี่ 824 - 849 MHz (Uplink) และ 869 - 894 MHz (Downlink) ช่องละ 30 KHz (833 channels)



กลุ่มนอร์ดิก

ภูมิภาค



กลุ่มประเทศนอร์ดิก หรือรวมเรียกเป็นภูมิภาคนอร์ดิก หมายถึงภูมิภาคในยุโรปเหนือ ประกอบด้วย เดนมาร์ก ฟินแลนด์ ไอซ์แลนด์ นอร์เวย์ และสวีเดน และดินแดนปกครองตนเองในสังกัดประเทศเหล่านั้นสามแห่ง ได้แก่ กรีนแลนด์ หมู่เกาะแฟโร และหมู่เกาะโอลันด์ ประเทศในกลุ่มนอร์ดิกมีประวัติศาสตร์ร่วมกันมายาวนาน และมีสิ่งต่าง ๆ ... [วิกิพีเดีย](#)



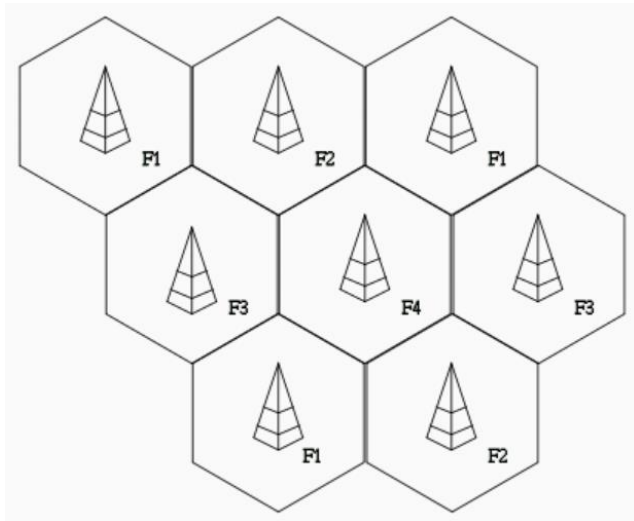
Hotline Ericsson ใช้ระบบ NMT 450 MHz
(ซ้าย) ติดรถยนต์ (ขวา) ถือติดตัวไปได้ น้ำหนัก 5 kg
ราคา 1 แสนบาท (พ.ศ. 2532)



Ericsson is a Swedish company. Nokia is in Finland.

2G

- ใช้สัญญาณ **Digital** เสียงคมชัด เข้ารหัสข้อมูล ยังเน้นการใช้งาน **voice** เป็นหลัก แต่ก็เริ่มใช้ **data** บ้าง เช่น **SMS** เป็นต้น
- คิดค่าบริการตามเวลาโทร และจำนวนครั้งที่ส่ง **SMS**
- ใช้ **cells** จำนวนมากเพื่อคลุมพื้นที่ให้บริการ เกิด **Cellular Network** นำ **MS** เคลื่อนที่ไปได้ ทำ **handover**
- ใช้ **FDMA + TDMA** เพื่อสร้าง **channels**
- ระบบ **GSM (EU), D-AMPS (US)**
- ยังใช้ **network** แบบ **circuit-switching**



Cell รูป 6 เหลี่ยม (อุดมคติ) ของจริงไม่เป็นรูปทรงเรขาคณิต ขึ้นอยู่กับสิ่งกีดขวาง และการรบกวนในธรรมชาติ F1, F2, F3, ... คือ ย่านความถี่ที่ไม่ทับซ้อนกัน เพื่อไม่ให้แต่ละ **cell** รบกวนกัน

GSM Architecture

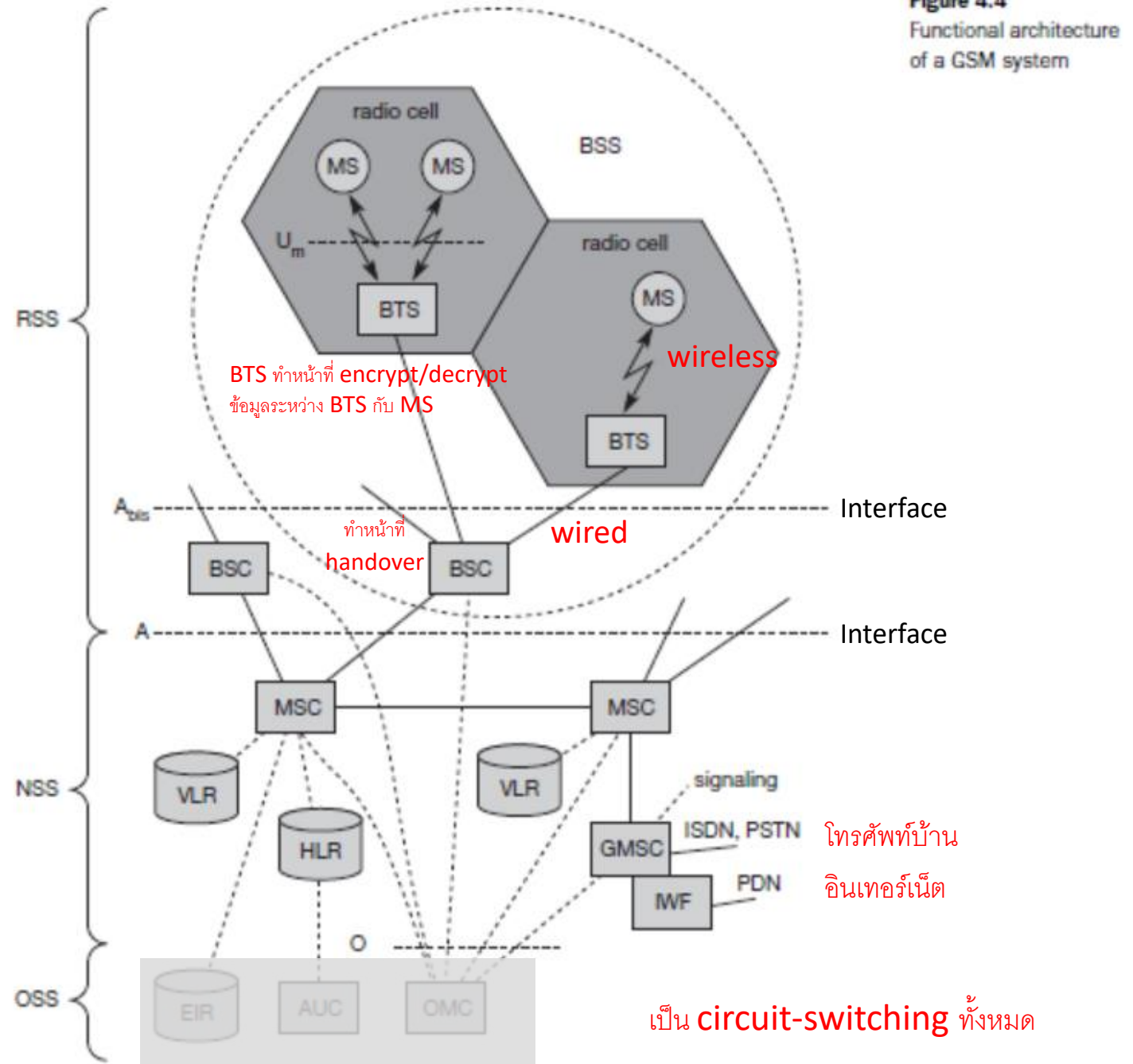
ประกอบด้วย 3 ส่วนคือ

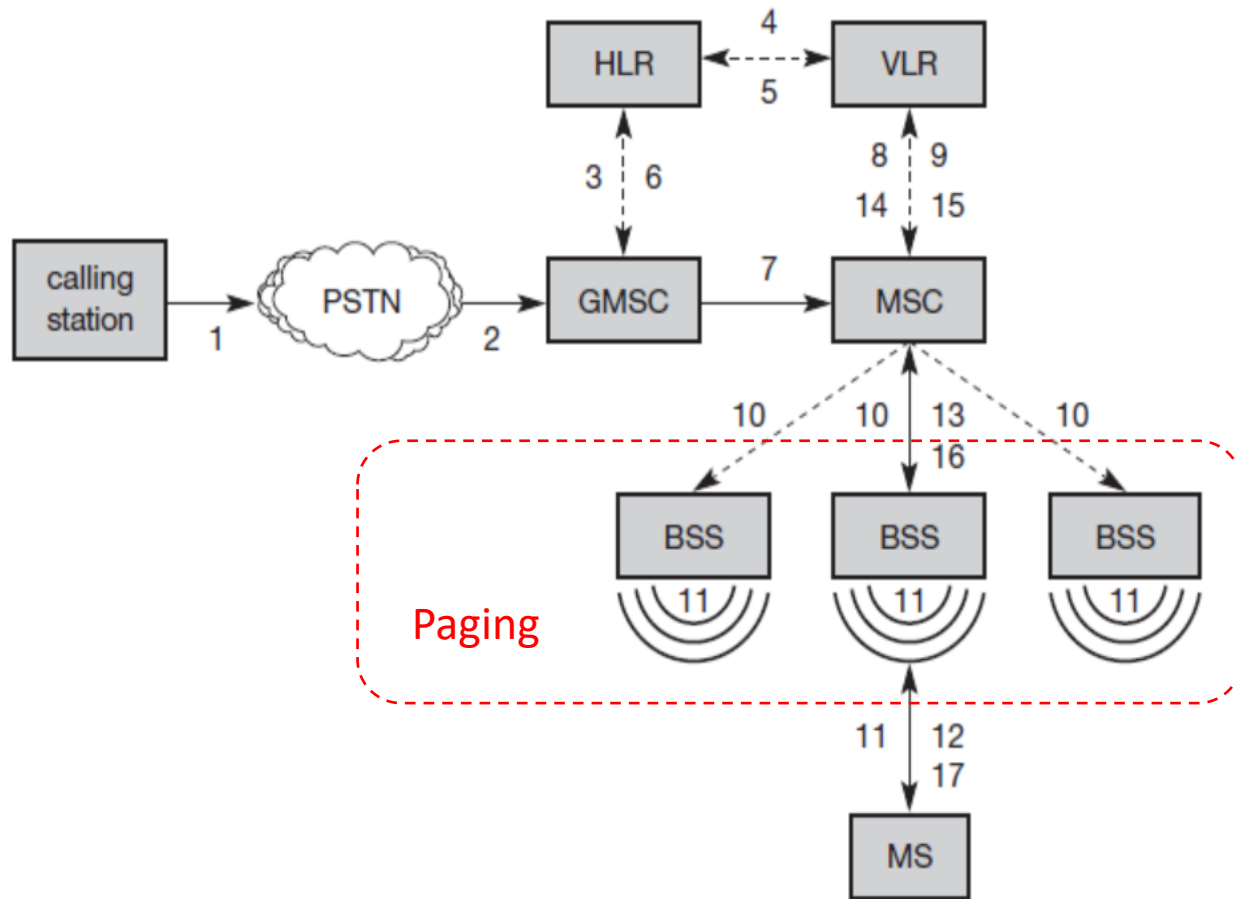
radio subsystem (RSS)

network and switching subsystem (NSS)

operation subsystem (OSS)

BSS	Base Station Subsystem
MS	Mobile Station
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Services Switching Center
VLR	Visitor Location Register
HLR	Home Location Register
EIR	Equipment Identity Register
AUC	Authentication Center
OMC	Operation and Maintenance Center
GMSC	Gateway MSC
IWF	Interworking Functions





โทรศัพท์บ้านโทรเข้ามือถือ

1. กดเบอร์โทรใน GSM เช่น ที่ขึ้นต้นด้วย 081
2. ส่งไป Gateway MSC (GMSC)
3. HLR เช็คว่ามีเบอร์นี้อยู่ในระบบ และมีสิทธิใช้งาน
4. HLR ขอ location จาก VLR (น่าจะขอจาก VLR ทุกตัว)*
5. VLR ส่ง location มาให้
6. HLR รู้ location แล้วว่าต้องไปที่ MSC ไหน จึง forward ไปยัง GMSC
7. GMSC ก็ forward ต่อไปยัง MSC
8. MSC ขอ status ของ MS จาก VLR ถ้า busy ก็จบ สายไม่ว่าง
9. VLR ส่ง status กลับมา
10. MSC ทำ paging ในทุก ๆ cell ที่ MSC นั้นดูแลอยู่
11. MS ตอบกลับไปยัง BSS
12. BSS ตอบกลับไปยัง MSC
13. ทำ security check (authen) และเริ่มการเข้ารหัส
14. 15. 16. 17. VLR ส่งสัญญาณให้ MSC setup connection (สร้าง data channel) กับ MS

*Once a subscriber moves to an MSC's location area, there is a record update in the VLR.

It automatically informs the subscriber's HLR of the change (<https://tektelic.com/what-it-is/visitor-location-register>).

มือถือโทรเข้าโทรศัพท์บ้าน

1. MS ร้องขอไปยัง BSS ว่าต้องการโทรออก
2. BSS ส่งต่อ request นี้ไปยัง MSC
3. MSC เช็คว่า VLR ว่าผู้ใช้งานนี้สามารถใช้บริการนี้ได้ และมีทรัพยากรพอ (มี channel ว่าง)
4. VLR ตอบกลับมา
5. 6. 7. 8. 9. 10. MSC setup connection (สร้าง channel ระหว่าง MS กับโทรศัพท์บ้าน)

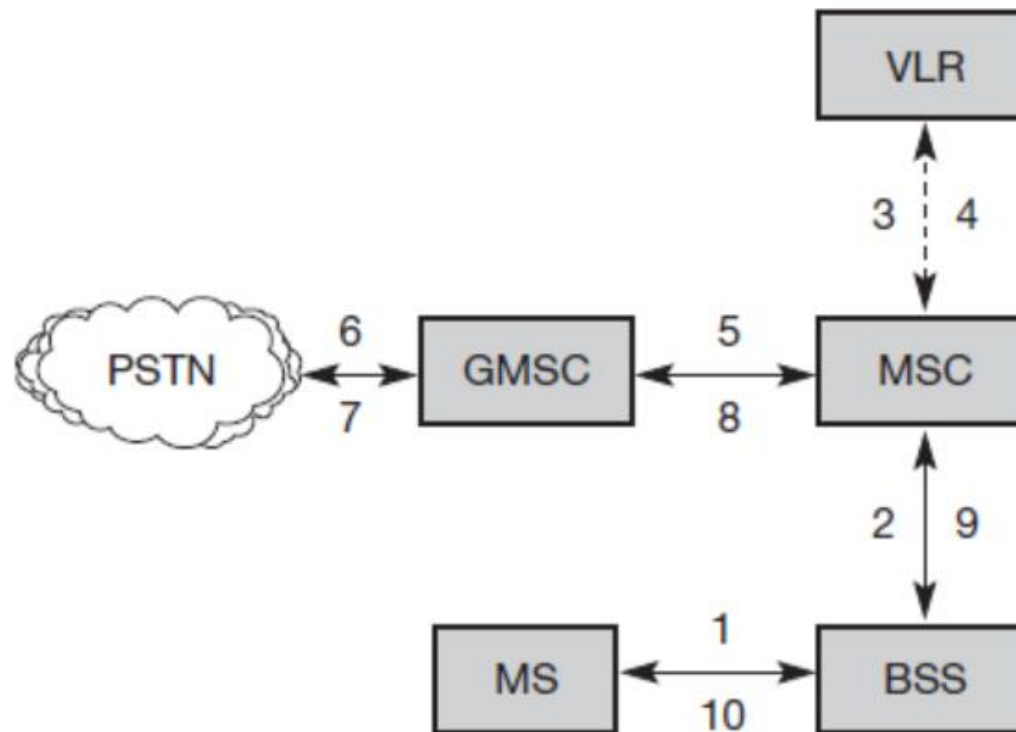


Figure 4.9
Mobile originated
call (MOC)

Handover

(2) ต้อง retransmit data ผ่าน BSC

(3) ต้อง retransmit data ผ่าน MSC₁

(4) ต้อง retransmit data ผ่าน MSC₁ และ MSC₂

ต้องลบเรคคอร์ดใน VLR เก่า และเพิ่มเรคคอร์ดใน VLR ใหม่

Figure 4.11
Types of handover
in GSM

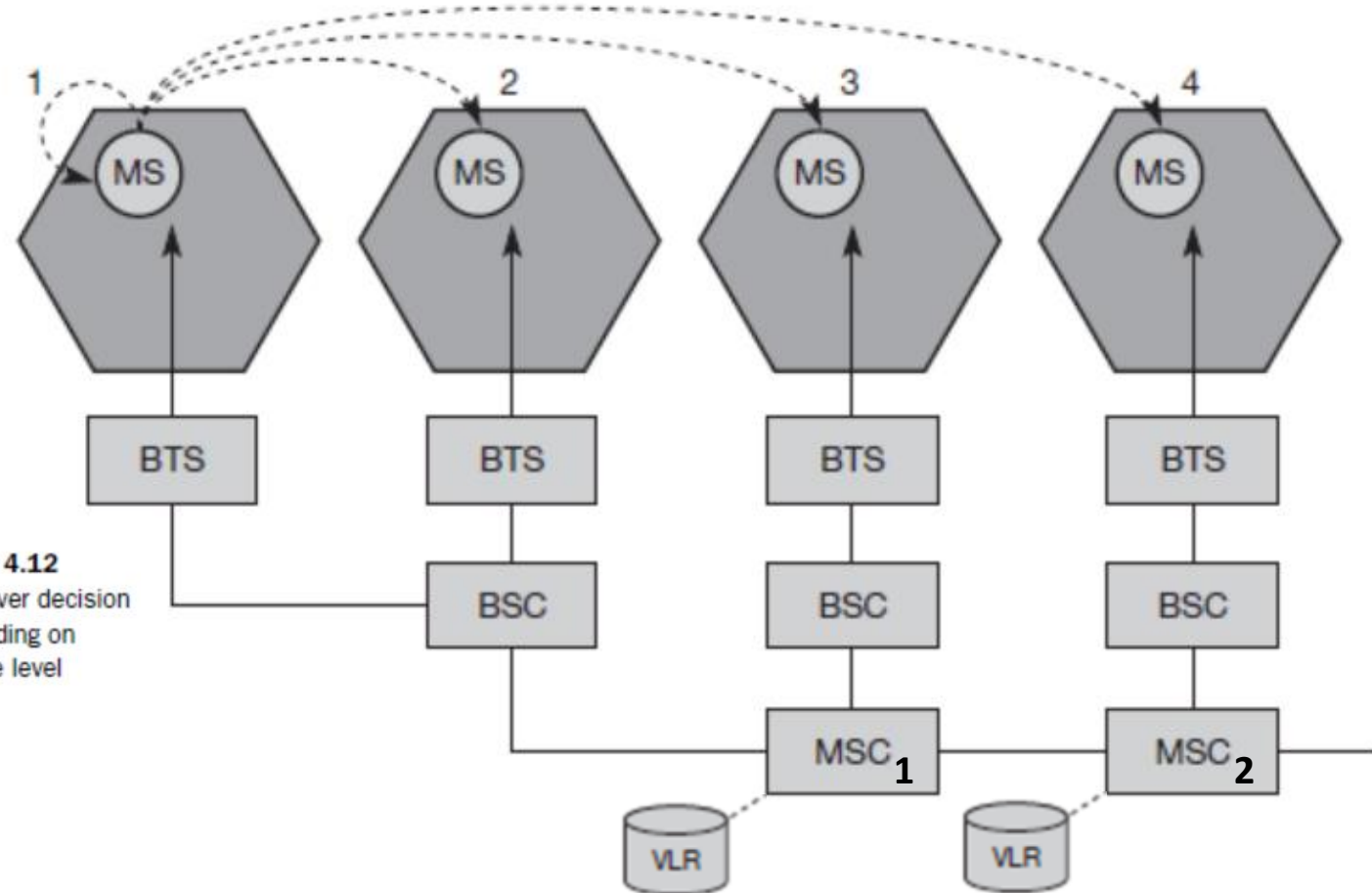
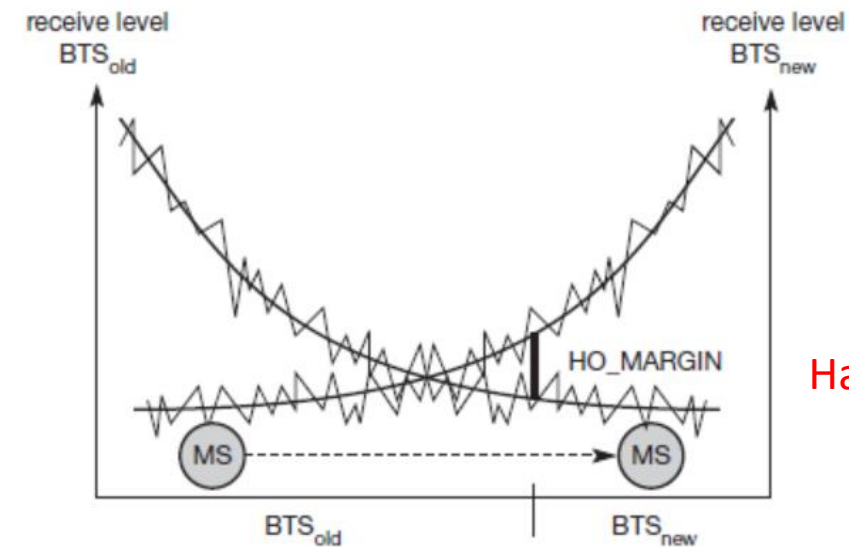


Figure 4.12
Handover decision
depending on
receive level

Hand-over margin



2.5G

- General Packet Radio Service (GPRS)
- ใช้ network แบบ packet-switching (เหมือน internet)
- คิดเงินตามปริมาณข้อมูล (MB/GB) ไม่ได้คิดเงินตามเวลา
- การใช้งานเริ่มเปลี่ยนจาก voice เป็น data มากขึ้น
- ดูเว็บไซต์ทั่ว ๆ ไปได้ แต่ยังทำ video streaming ไม่ได้



1 time slot = 1 voice channel

เอา time slot ที่ว่างของ TDMA มาใช้ทำ GPRS

เพื่อขาย data (internet) คิดค่าบริการเป็นรายเดือน

จะได้ data rate เท่าใด ขึ้นกับปริมาณการใช้งานในขณะนั้น

แพ็คเกจตามปริมาณการใช้งาน

แพ็คเกจเหมาจ่ายแบบรายเดือนต่อเนื่อง	อัตราค่าบริการ
แพ็คเกจ EDGE/GPRS 100 MB + Wi-Fi 5 ชม.	129 บาท
แพ็คเกจ EDGE/GPRS 500 MB + Wi-Fi 10 ชม.	399 บาท
แพ็คเกจ EDGE/GPRS 1 GB + Wi-Fi ใช้งานได้ไม่อื่น	699 บาท

• WiFi ความเร็ว 1 Mbps

• ค่าบริการส่วนเกินจากแพ็คเกจ 0.12 บาท/กิโลไบต์ (ส่วนเกินของกิโลไบต์ นับเป็น 1 กิโลไบต์)

สิทธิในการทดลองใช้บริการ 3G

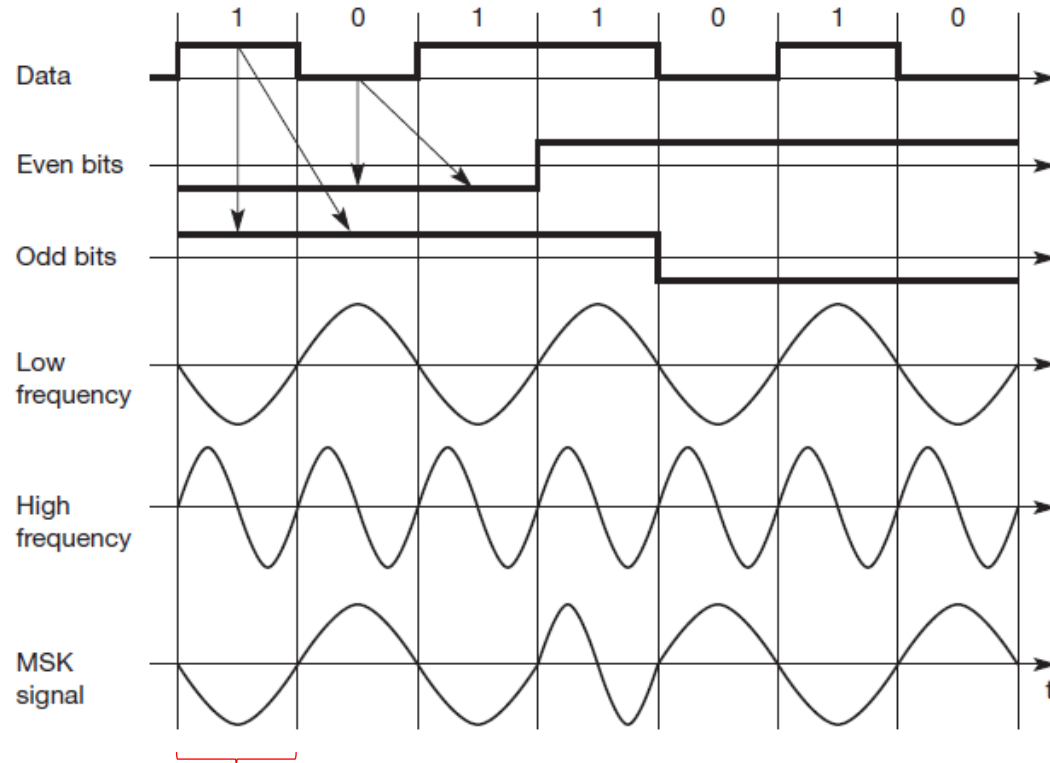
100 MB

500 MB

1 GB

2.75G

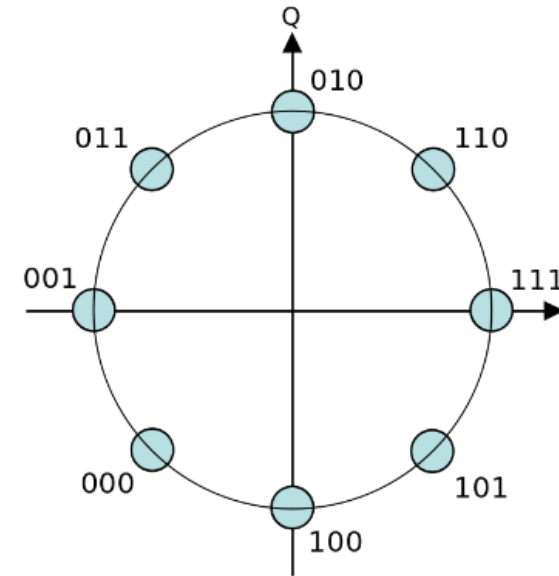
- Enhanced Data Rates for GSM Evolution (EDGE)
- เปลี่ยนวิธี modulation ทำให้ส่งข้อมูลได้เร็วขึ้น 3 เท่า



ส่งได้ 1 บิต แต่ถ้าใช้ PSK ส่งได้ 3 บิต

Gaussian Minimum Shift Keying (GMSK)

ใช้ใน GSM Standard



Phase Shift Keying (PSK)

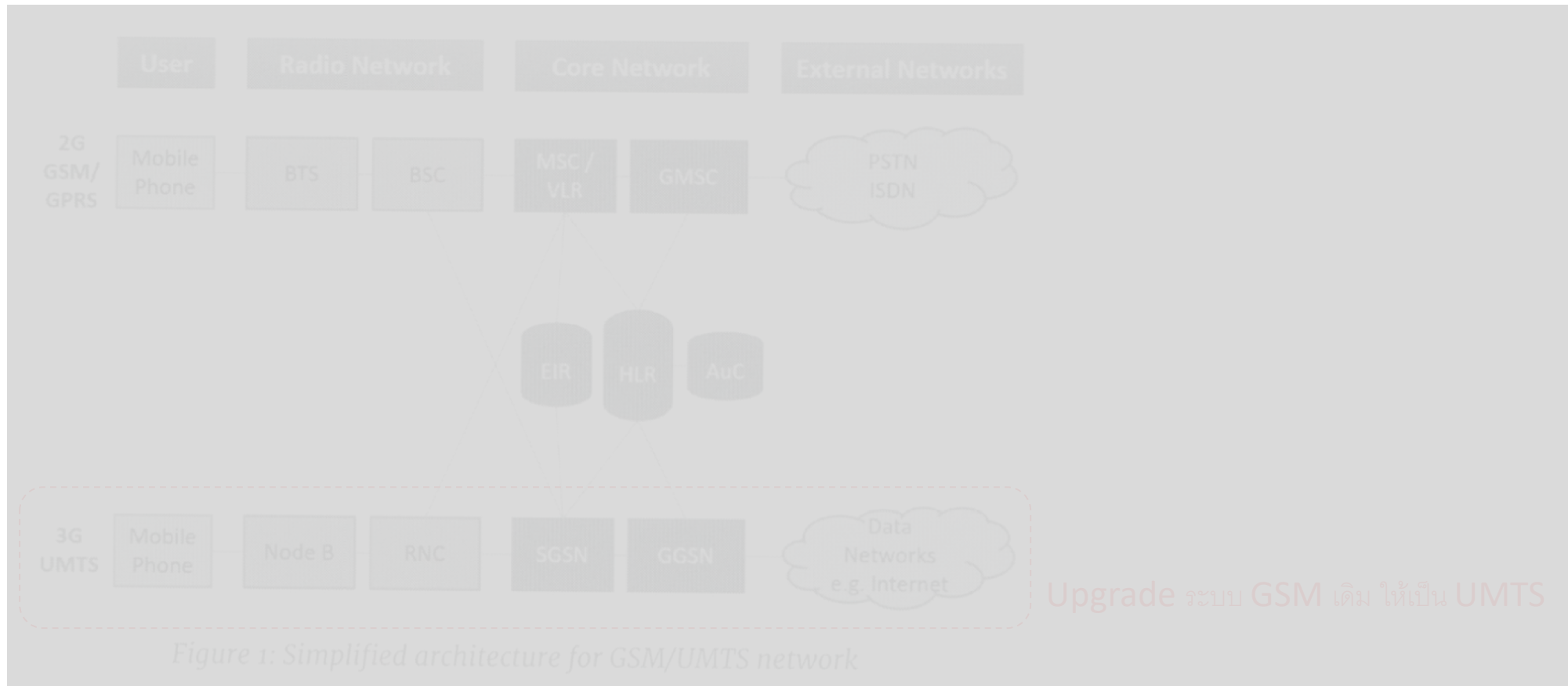
ใช้ 8 เฟสที่แตกต่างกัน

ส่งทีละ 3 บิต เร็วขึ้น 3 เท่า

เร็วกว่า GMSK 3 เท่า

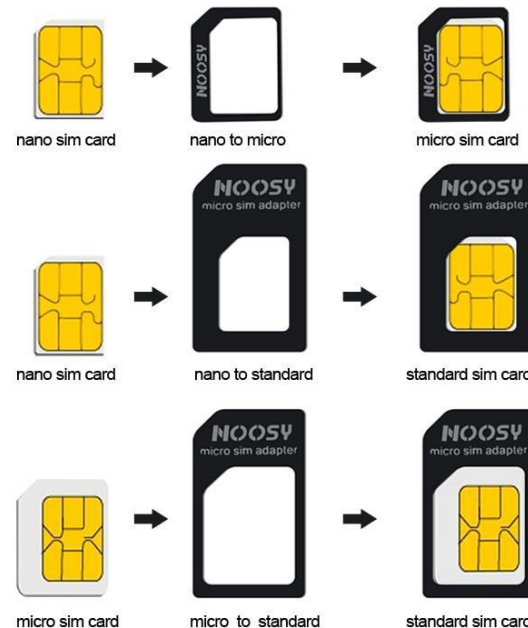
3G

- ใช้ CDMA (2G ใช้ FDMA + TDMA)
- ได้ data rate สูงพอที่จะทำ video streaming ได้ (แต่ถ้ามี users ใน cell จำนวนมาก data rate ก็ลดลง)
- แบบที่ 1 อัปเกรดระบบเดิม GSM -> UMTS
- แบบที่ 2 อัปเกรดระบบเดิม IS-95 (cdmaOne) -> CDMA2000



Subscriber identity module (SIM)

- SIM เป็นสิ่งที่กำหนดว่าจะให้บริการอะไรบ้าง voice, data, package/promotion ฯลฯ
- ไม่ใช่เบอร์โทรศัพท์ เนื่องจากเบอร์เดิม เปลี่ยน SIM ได้ เช่น เปลี่ยน package/promotion
- หรือเบอร์เดียวมีหลาย SIM เช่น SIM หลักใช้ voice + data, SIM อื่น ๆ ใช้ data ได้อย่างเดียว
- ในระบบ GSM ถ้าไม่มี SIM จะโทรเบอร์ฉุกเฉินได้เท่านั้น เช่น 191 เป็นต้น
- Personal Identity Number (PIN) ใช้ activate SIM ยืนยันสิทธิ์การใช้งาน ถ้าใส่ผิด 3 ครั้งจะ lock
- Personal Unblocking Key (PUK) ใช้ unlock SIM



Authentication

ใน SIM ประกอบด้วย

- Individual authentication key, K_i
- Algorithm for authentication, A_3

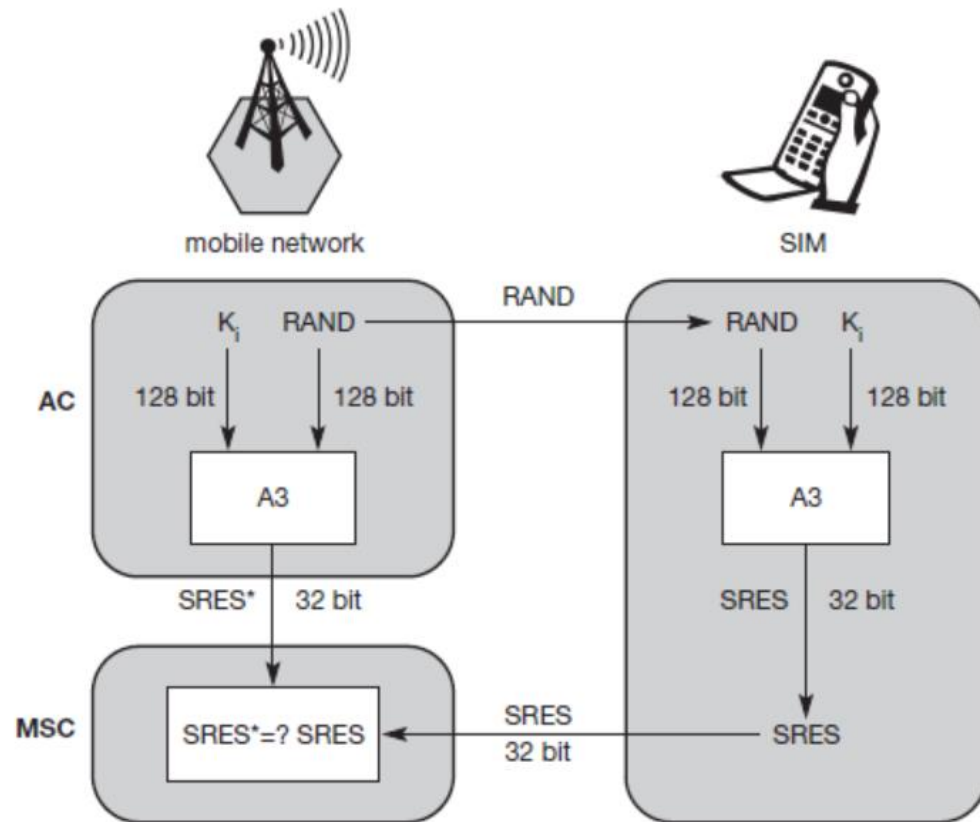


Figure 4.14
Subscriber
authentication

Assume

ผู้ร้ายไม่มี K_i (แต่อาจจะมี A_3 ก็ได้)

$RAND$ มีไว้ป้องกันผู้ร้ายได้ยิน $SRES$ เนื่องจากเป็น wireless

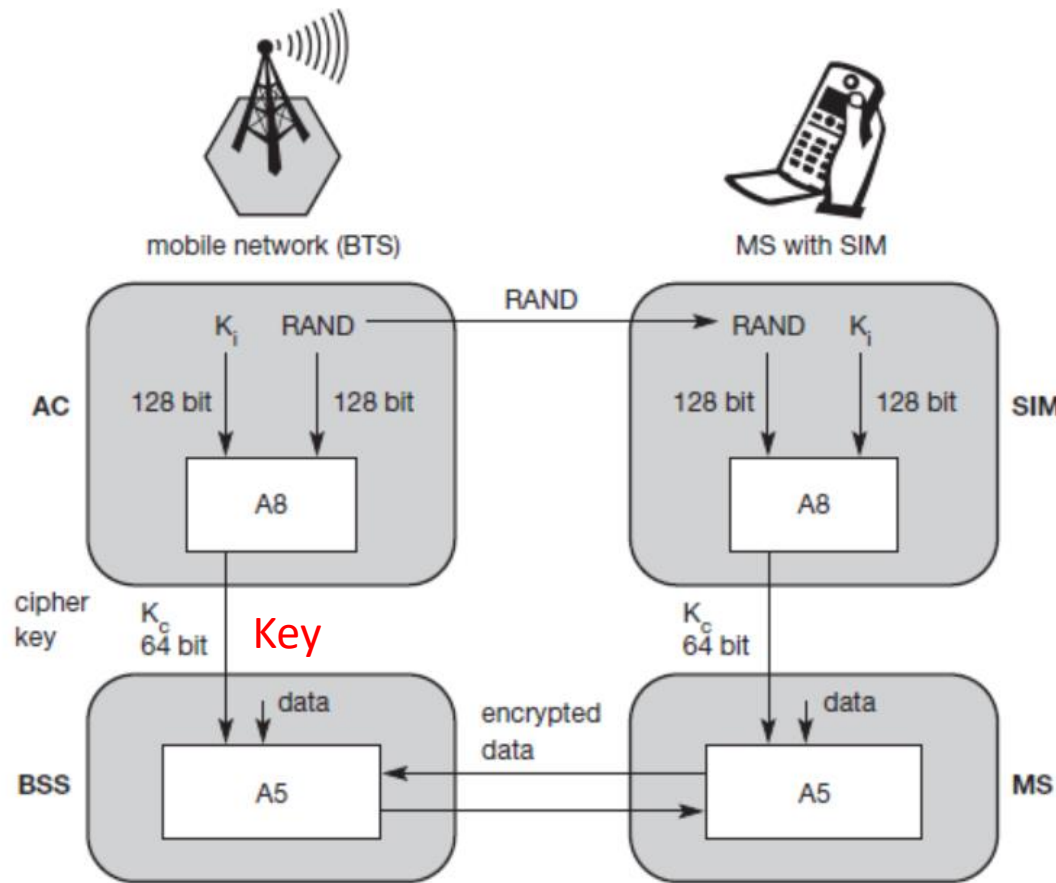
พอผู้ใช้ส่ง $SRES$ ออกมา ทุกคนก็ได้รับข้อมูล $SRES$ ไปด้วย

ต้องสร้าง $SRES$ ได้ตรงกัน ($SRES$ = Signed Response) ใครขโมย $SRES$ ไปได้ก็ไม่มีประโยชน์ เพราะทุกครั้งใช้ $RAND$ ใหม่

Encryption

Algorithm A5, A8 ใน SIM ใช้ random number ผสมกับ K_i เพื่อสร้าง cipher key K_c สำหรับเข้ารหัสข้อมูล (ถ้าใช้ K_i บ่อยๆ เดี่ยวคนจับได้ ต้องผสม random number ลงไปด้วย connect ใหม่รอบหน้าก็เปลี่ยน random number อีก)

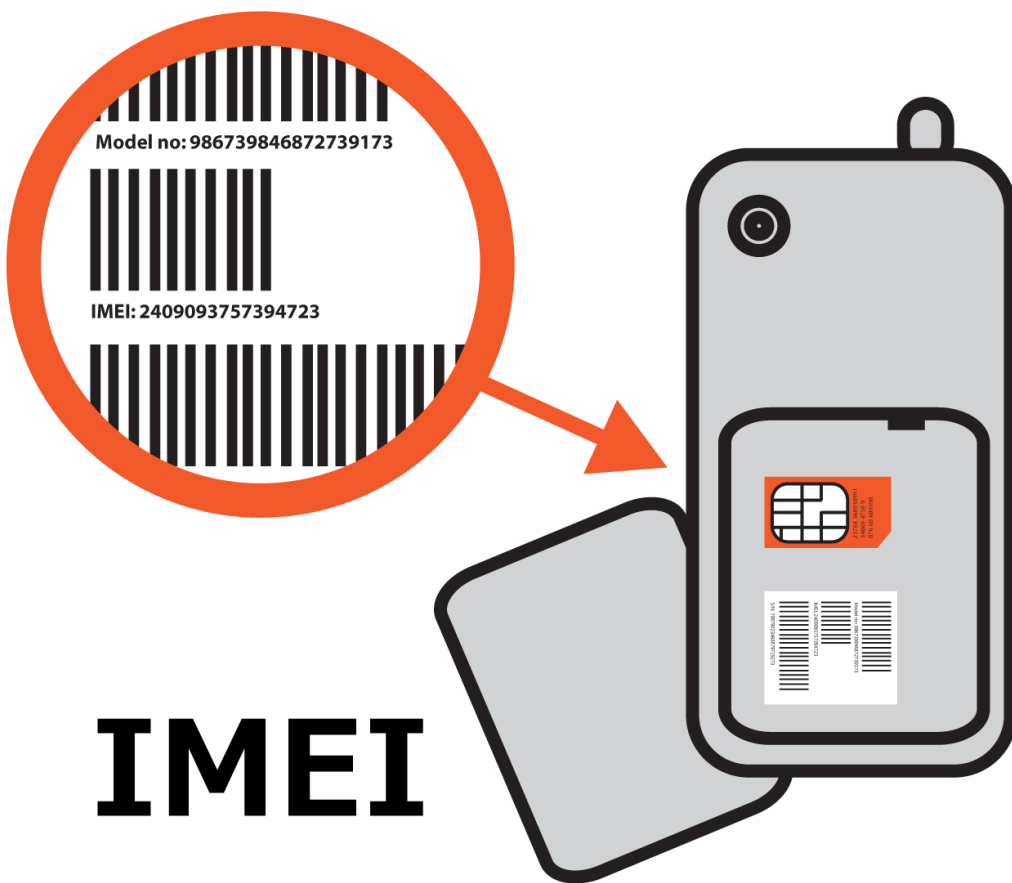
Figure 4.15
Data encryption



Assume
ผู้ร้ายไม่มี K_i (แต่อาจจะมี A8 ก็ได้)

International Mobile Equipment Identity (IMEI)

- IMEI เป็นหมายเลขเครื่อง ใช้ป้องกันการโจรกรรม
- เมื่อโทรศัพท์ถูกขโมยจะต้องแจ้ง IMEI กับผู้ให้บริการ เช่น AIS, DTAC, TRUE (แชร์ฐานข้อมูลเดียวกัน) เพื่อระงับการให้บริการ



Mobile station international subscriber number (MSISDN) อ่านว่า misden

- MSISDN = CC + NDC + SN
- CC = Country Code
- NDC = National Destination Code **0xx** คือ มือถือ เช่น **081**
- Subscriber Number
- MSISDN อยู่ในฐานะข้อมูลของผู้ให้บริการ Cellular Network

MSISDN แทน ผู้ใช้ (user) บ้าน หรือ มือถือ
(ไม่ได้บอกว่ายู่ใน cellular network ไດ)

Country Code

พื้นที่ 6 แปซิฟิกใต้และโอเชียเนีย [แก้ว]

- 60 —  มาเลเซีย
- 61 —  ออสเตรเลีย และใช้在地แดนภายนอกคือ  เกาะคริสต์มาส และ  หมู่เกาะโคโคส
- 62 —  อินโดนีเซีย
- 63 —  ฟิฟิลปินส์
- 64 —  นิวซีแลนด์
- 65 —  สิงคโปร์
- 66 —  ไทย

National Destination Code

ภาคกลาง

กรุงเทพฯ	02
กาญจนบุรี	034
ชัยนาท	056
นครปฐม	034
นครนายก	037
นนทบุรี	02
ปทุมธานี	02
ประจวบคีรีขันธ์	032
พระนครศรีอยุธยา	035
ราชบุรี	032
ลพบุรี	036
สระบุรี	036
สมุทรปราการ	02
สมุทรสงคราม	034
สมุทรสาคร	034
สิงห์บุรี	036
สุพรรณบุรี	035
อ่างทอง	035
เพชรบุรี	032

International mobile subscriber identity (IMSI) อ่านว่า imzee

- $IMSI = MCC + MNC + MSIN$ IMSI จะบุผู้ใช้งานใน cellular network
- $MCC = \text{Mobile country code } ()$ ของไทยคือ 520
- $MNC = \text{Mobile network code (MNC)}$ AIS ใช้ 03, TRUE ใช้ 04, DTAC ใช้ 05
- $MSIN = \text{Mobile subscriber identification number (MSIN)}$
- $MSIN$ เป็นเลข 10 หลัก เช่น 1234567890
- $IMSI$ อยู่ในซิมไม่สามารถแก้ไขได้
- การเอาเบอร์เดิมย้ายค่ายคือ ไปรับซิม ($IMSI$) ของค่ายใหม่ และแก้ฐานข้อมูลเพื่อผูก $MSISDN$ กับ $IMSI$ ใหม่
- เมื่อโทรออก แต่ละค่ายรู้ว่า $MSISDN$ นี้อยู่ในค่ายตัวเองหรือไม่ หรืออยู่ข้างนอก
- ซิมเดียวมี 2 $IMSI$ ได้ สำหรับผู้ให้บริการ 2 ราย เช่น ในไทยและในญี่ปุ่น
จะได้เชื่อมต่อกับเครือข่ายของผู้ให้บริการในไทยและในญี่ปุ่นได้ทั้งสองที่

$IMSI$ 1 น่าจะเป็นผู้ให้บริการในไทย (TRUE, AIS, DTAC)

$IMSI$ 2 น่าจะเป็นผู้ให้บริการในญี่ปุ่น

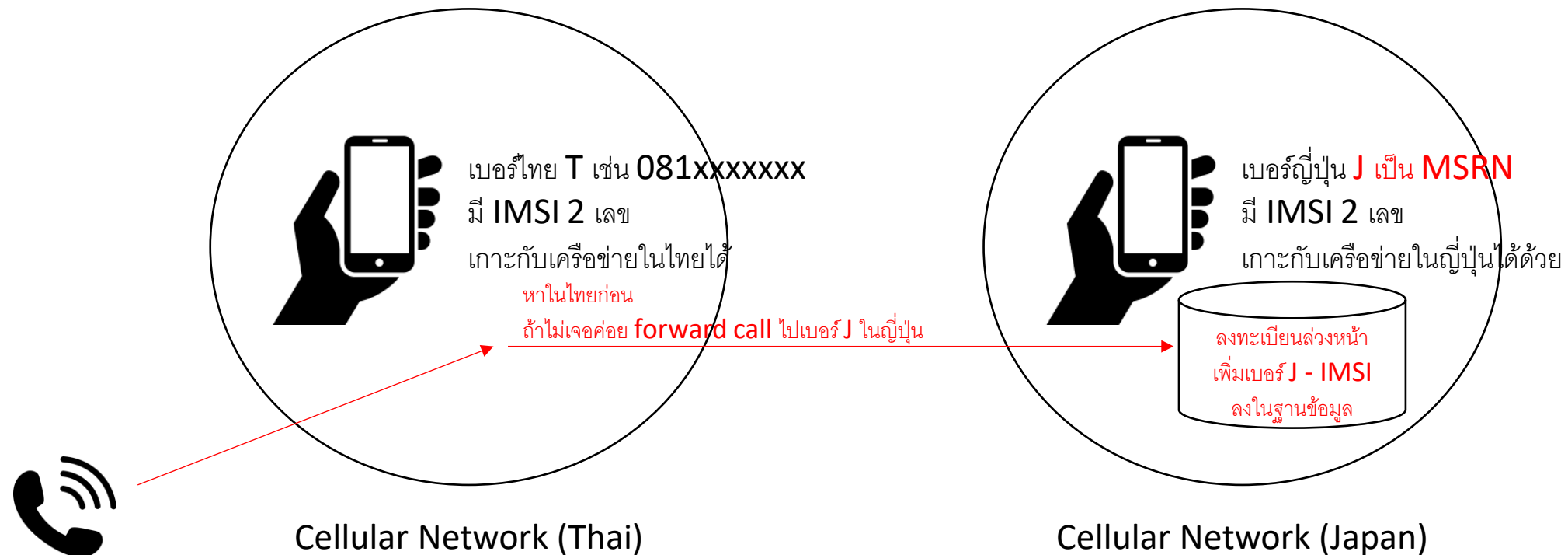
Temporary mobile subscriber identity (TMSI)

- เป็น random number ที่ออกให้โดย VLR ในพื้นที่นั้น
- เมื่อย้ายไป VLR ใหม่ก็ออกเลขใหม่ให้ หรือออกเลขใหม่เมื่อเลขเดิมหมดอายุการใช้งาน
- การอ้างถึง MS จะใช้ TMSI ไม่ใช่ IMSI เพื่อซ่อนตัวตนของผู้ใช้บริการ
- VLR จะเก็บคู่ IMSI - TMSI ไว้ในฐานข้อมูล

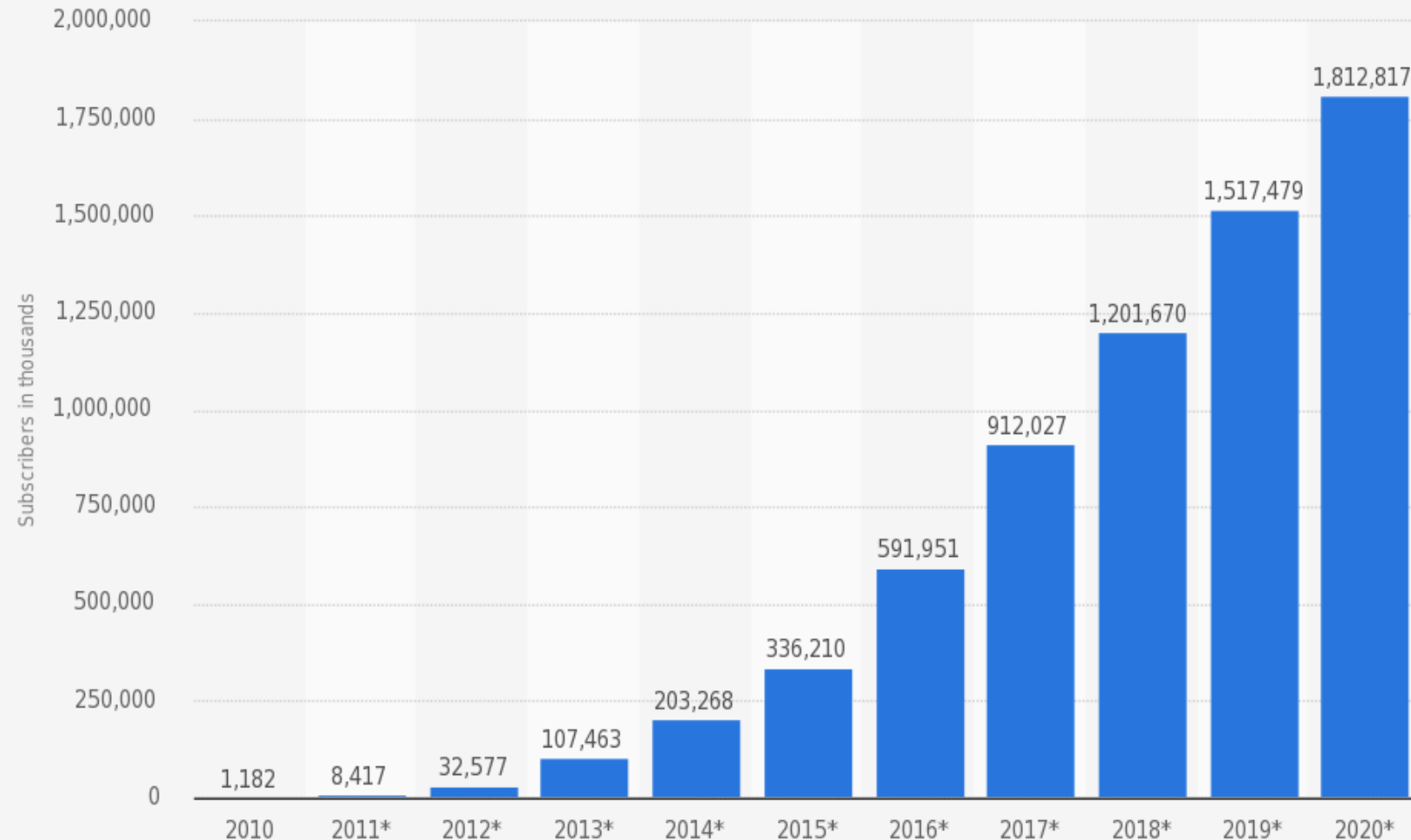
พนักงานที่ทำงานอยู่กับระบบหลังบ้านจะมองไม่เห็น IMSI ของลูกค้า เช่น ไม่รู้ว่า นาย ก โทรหานาย ข เป็นต้น

Mobile Station Roaming Number (MSRN)

- The Mobile Station Roaming Number (MSRN) is a temporarily telephone number assigned to a mobile station which roams into another numbering area. (This is usually another country). This number is needed by the home network to forward incoming calls for the mobile station to the network it visits.
- เช่น เบอร์ไทย T เปิด **roaming** ไปญี่ปุ่น ก็จะได้เบอร์โทรที่ญี่ปุ่นด้วยเป็น J เมื่อมีคนโทรเข้าเบอร์ T ที่ไทย ก็จะค้นหาในไทยก่อน เมื่อไม่เจอจะ **forward call** ไปเบอร์ J ที่ญี่ปุ่น



Number of 4G mobile subscribers worldwide from 2010 to 2020 (in 1,000)



Source:
Jefferies & Company
© Statista 2016

Additional Information:
Worldwide; Jefferies & Company; 2010

statista

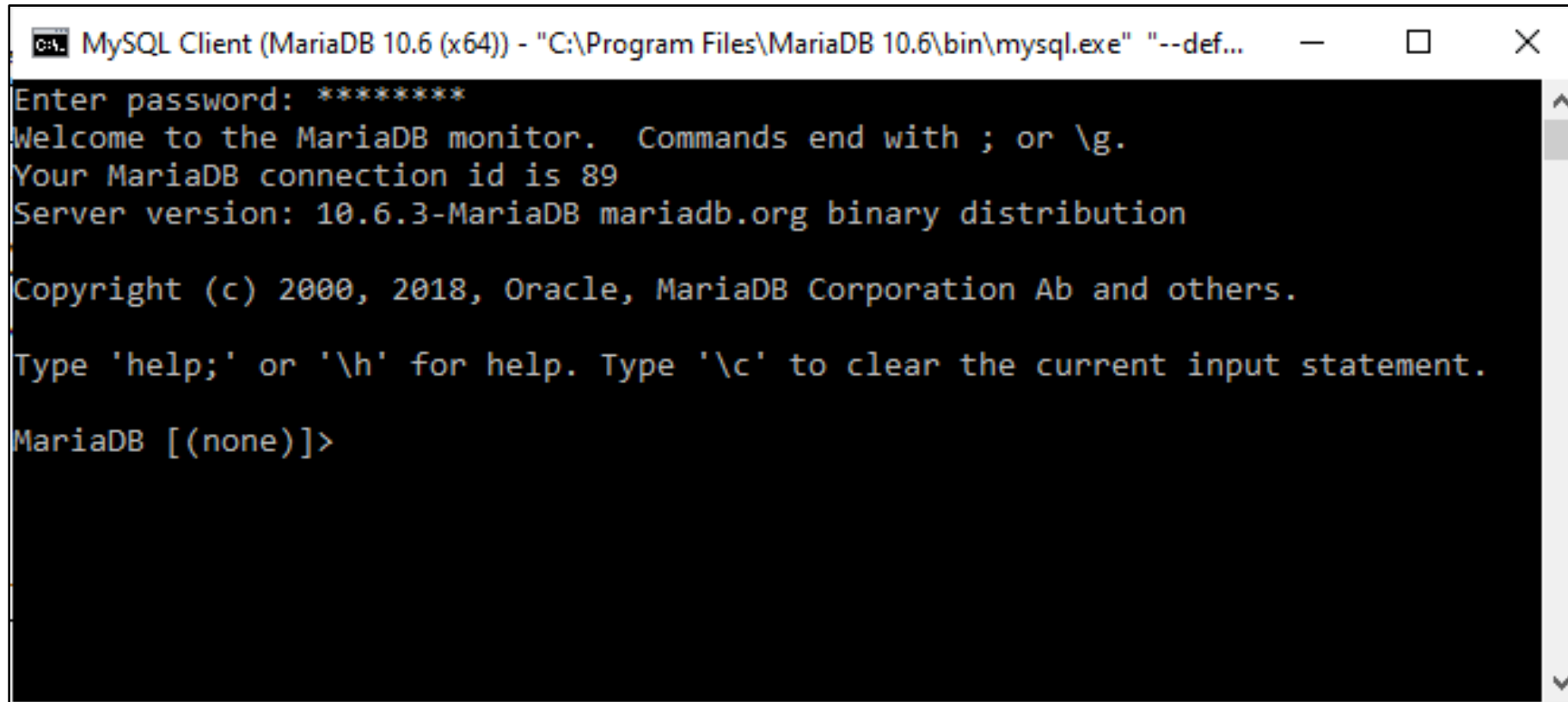
ทุก 4 - 5 คน
จะมีมือถือ 1 คน

ในประเทศร่ำรวย
1 คนจะมีมือถือหลายเครื่อง

แต่ในประเทศยากจน
ใน 100 คนจะมีมือถือเครื่องเดียว

ในอนาคตทุกคนน่าจะมีมือถือหมด
อย่างน้อยคนละ 1 เครื่อง

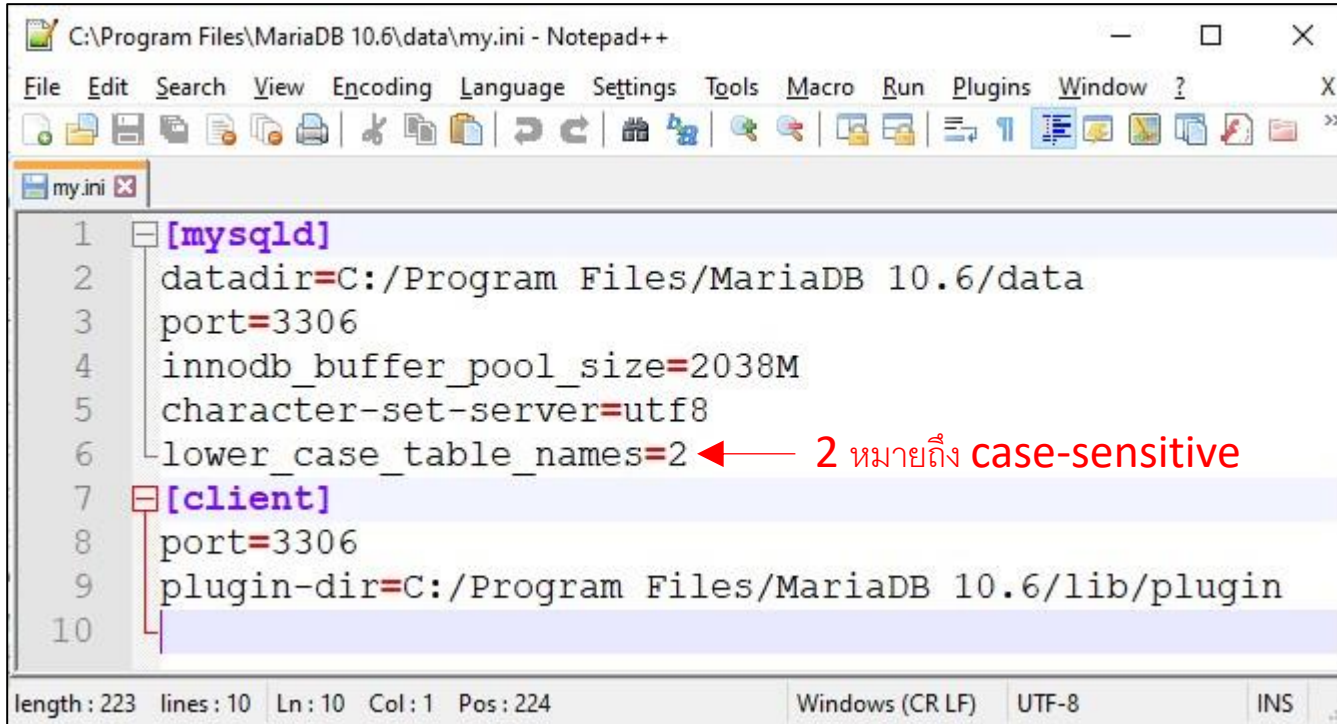
ติดตั้งฐานข้อมูล MariaDB จาก <https://mariadb.org>



```
MySQL Client (MariaDB 10.6 (x64)) - "C:\Program Files\MariaDB 10.6\bin\mysql.exe" "--def...  
Enter password: *****  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 89  
Server version: 10.6.3-MariaDB mariadb.org binary distribution  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]>
```

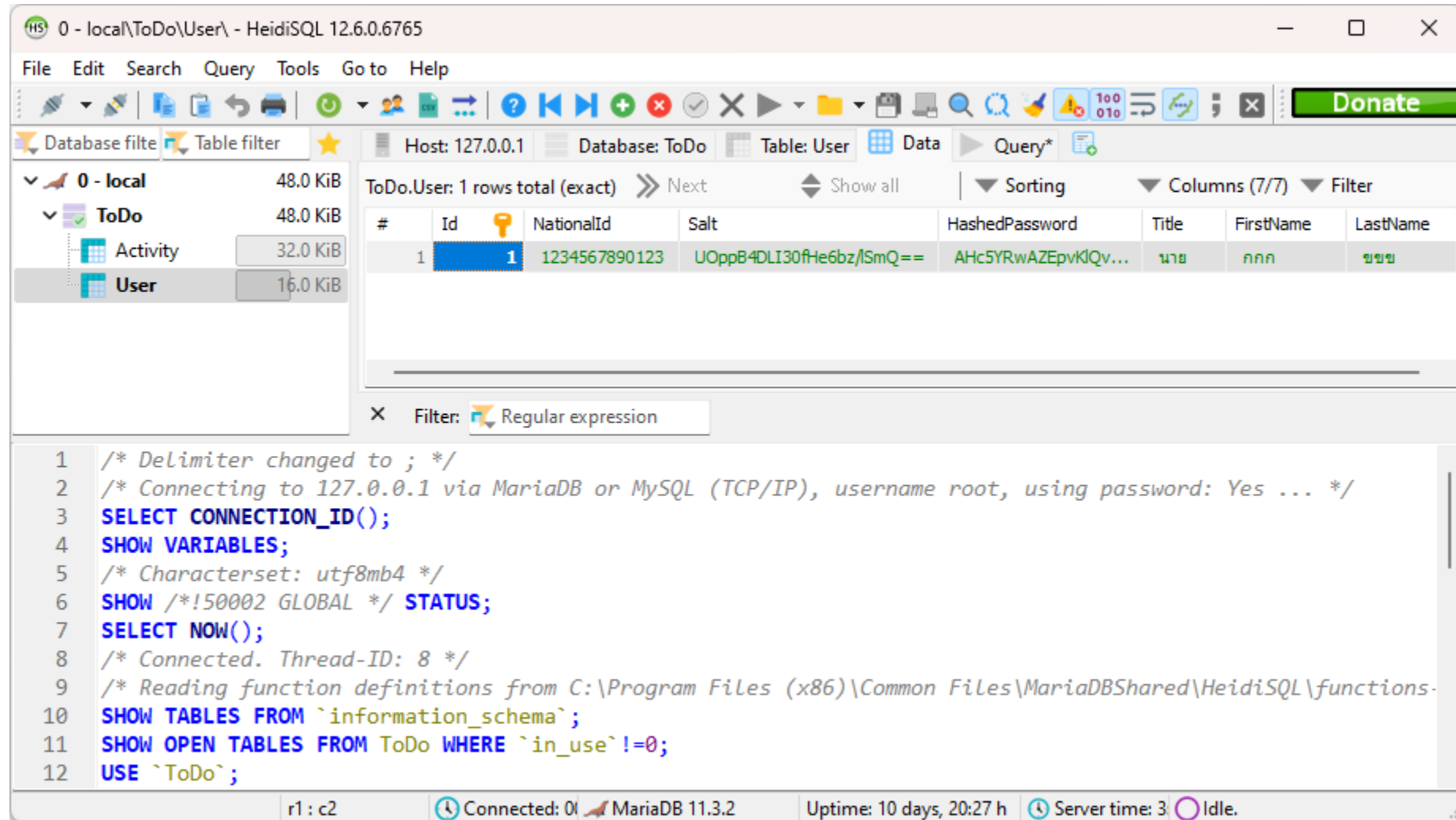
Configuration ของ MariaDB บน Windows

C:\Program Files\MariaDB 10.6\data\my.ini



```
C:\Program Files\MariaDB 10.6\data\my.ini - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
my.ini
1 [mysqld]
2   datadir=C:/Program Files/MariaDB 10.6/data
3   port=3306
4   innodb_buffer_pool_size=2038M
5   character-set-server=utf8
6   lower_case_table_names=2 ← 2 หมายถึง case-sensitive
7 [client]
8   port=3306
9   plugin-dir=C:/Program Files/MariaDB 10.6/lib/plugin
10
length: 223 lines: 10 Ln: 10 Col: 1 Pos: 224 Windows (CR LF) UTF-8 INS
```

ติดตั้งโปรแกรม HeidiSQL จาก <https://www.heidisql.com>



0 - local\ToDo\User\ - HeidiSQL 12.6.0.6765

File Edit Search Query Tools Go to Help

Database filter Table filter Host: 127.0.0.1 Database: ToDo Table: User Data Query*

0 - local 48.0 KiB
ToDo 48.0 KiB
Activity 32.0 KiB
User 16.0 KiB

ToDo.User: 1 rows total (exact) Next Show all Sorting Columns (7/7) Filter

#	Id	NationalId	Salt	HashedPassword	Title	FirstName	LastName
1	1	1234567890123	UOppB4DLI30fHe6bz/IsMQ==	AHc5YRwAZEpvKIQv...	นาง	กนก	ขนิษฐ

X Filter: Regular expression

```
1 /* Delimiter changed to ; */
2 /* Connecting to 127.0.0.1 via MariaDB or MySQL (TCP/IP), username root, using password: Yes ... */
3 SELECT CONNECTION_ID();
4 SHOW VARIABLES;
5 /* Characterset: utf8mb4 */
6 SHOW /*!50002 GLOBAL */ STATUS;
7 SELECT NOW();
8 /* Connected. Thread-ID: 8 */
9 /* Reading function definitions from C:\Program Files (x86)\Common Files\MariaDBShared\HeidiSQL\functions-
10 SHOW TABLES FROM `information_schema`;
11 SHOW OPEN TABLES FROM ToDo WHERE `in_use`!=0;
12 USE `ToDo`;
```

r1 : c2 Connected: 0 MariaDB 11.3.2 Uptime: 10 days, 20:27 h Server time: 3 Idle.

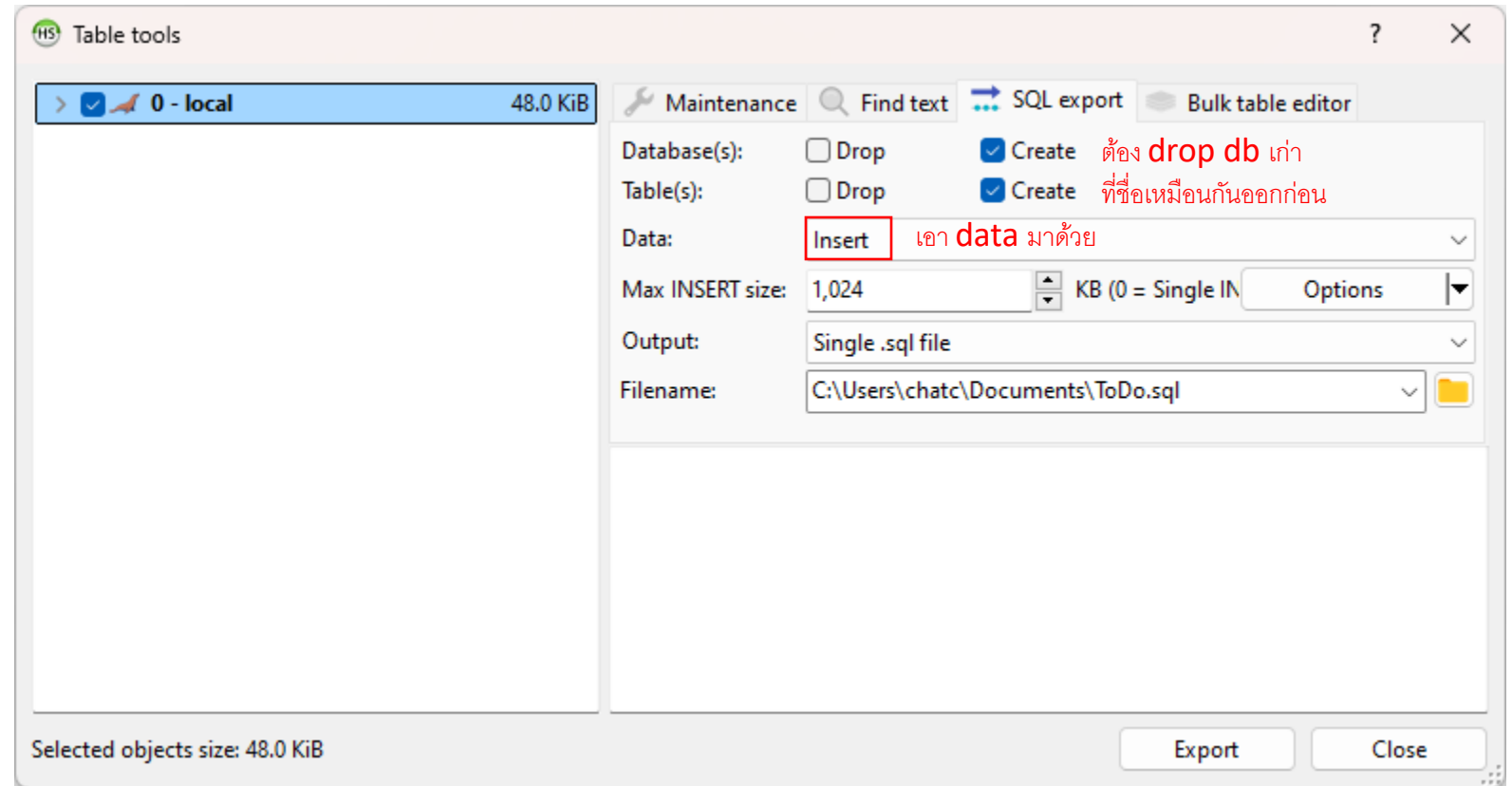
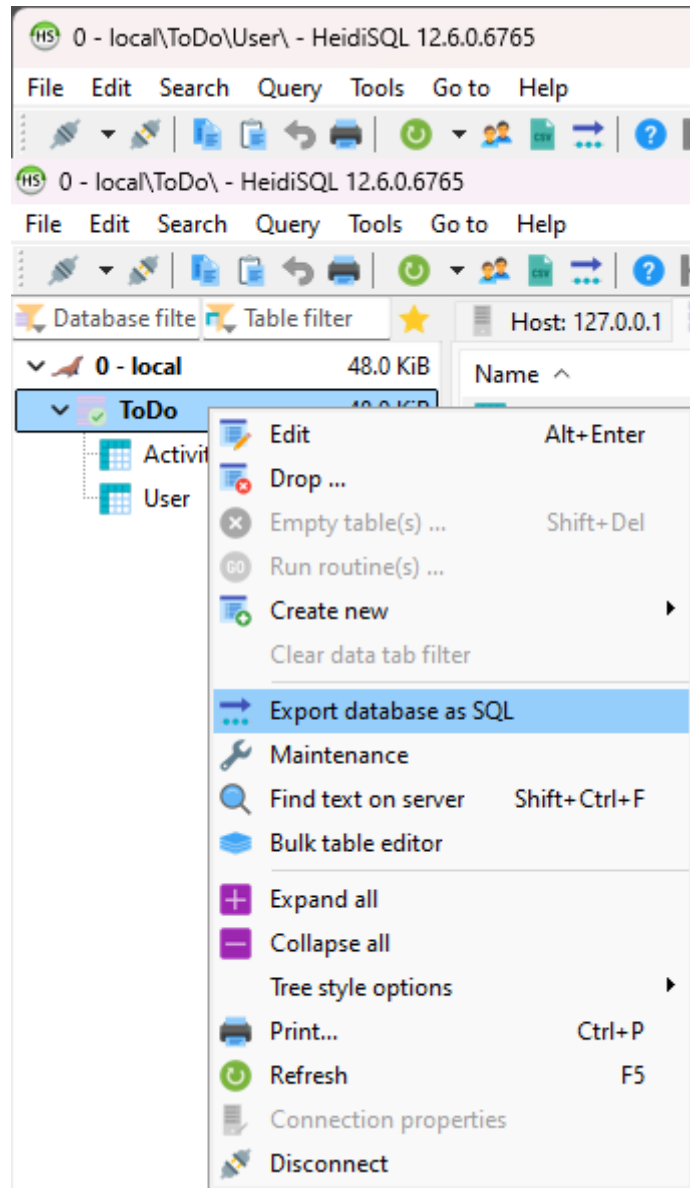
ตาราง User

Columns: + Add × Remove ▲ Up ▼ Down											
#	Name	Datatype	Length/Set	Unsign...	Allow N...	Zerofill	Default	Comment	Collation	Expression	Virtuality
 1	Id	INT	10	☒	☐	☐	AUTO_INCREMENT				
2	NationalId	CHAR	13	☐	☐	☐	No default		utf8mb4_thai_520_w2		
3	Salt	CHAR	24	☐	☐	☐	No default		utf8mb4_thai_520_w2		
4	HashedPassword	CHAR	44	☐	☐	☐	No default		utf8mb4_thai_520_w2		
5	Title	VARCHAR	100	☐	☐	☐	No default		utf8mb4_thai_520_w2		
6	FirstName	VARCHAR	100	☐	☐	☐	No default		utf8mb4_thai_520_w2		
7	LastName	VARCHAR	100	☐	☐	☐	No default		utf8mb4_thai_520_w2		

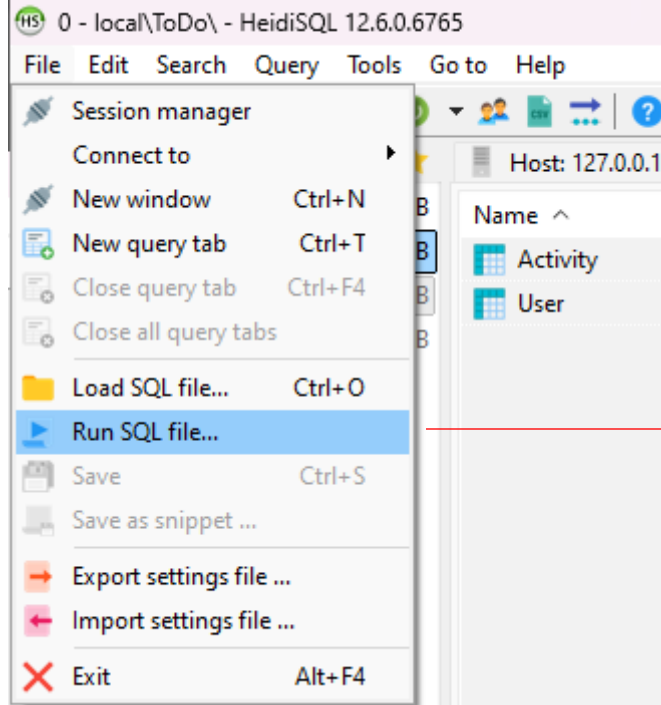
ตาราง Activity

Columns: + Add × Remove ▲ Up ▼ Down											
#	Name	Datatype	Length/Set	Unsign...	Allow N...	Zerofill	Default	Comment	Collation	Expression	Virtuality
 1	Id	INT	10	☒	☐	☐	AUTO_INCREMENT				
 2	UserId	INT	10	☒	☐	☐	No default				
3	Name	VARCHAR	100	☐	☐	☐	No default		utf8mb4_thai_520_w2		
4	When	DATETIME		☐	☐	☐	No default				

Export DB



Import DB



CAUsers\chat\Documents\99 - Temp\ToDo.sql - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

ToDo.sql

```
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
```

-- Host: 127.0.0.1
-- Server version: 11.3.2-MariaDB - mariadb.org binary distribution
-- Server OS: Win64
-- HeidiSQL Version: 12.6.0.6765

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET NAMES utf8 */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

-- Dumping database structure for ToDo
CREATE DATABASE IF NOT EXISTS `ToDo` /*!40100 DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_thai_520_w2 */;
USE `ToDo`;

-- Dumping structure for table ToDo.Activity
CREATE TABLE IF NOT EXISTS `Activity` (
 `Id` int(10) unsigned NOT NULL AUTO_INCREMENT,
 `UserId` int(10) unsigned NOT NULL,
 `Name` varchar(100) NOT NULL,
 `When` datetime NOT NULL,
 PRIMARY KEY (`Id`),
 KEY `FK1\_Activity\_User` (`UserId`),
 CONSTRAINT `FK1\_Activity\_User` FOREIGN KEY (`UserId`) REFERENCES `User` (`Id`)
) ENGINE=InnoDB AUTO_INCREMENT=3 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_thai_520_w2;

-- Dumping data for table ToDo.Activity: ~2 rows (approximately)
INSERT INTO `Activity` (`Id`, `UserId`, `Name`, `When`) VALUES
 (1, 1, 'เมื่อวาน', '2025-01-31 09:00:00'),
 (2, 1, 'เมื่อคืน', '2025-02-01 13:00:00');

-- Dumping structure for table ToDo.User
CREATE TABLE IF NOT EXISTS `User` (
 `Id` int(10) unsigned NOT NULL AUTO_INCREMENT,
 `NationalId` char(13) NOT NULL,
 `Salt` char(24) NOT NULL,
 `HashedPassword` char(44) NOT NULL,
 `Title` varchar(100) NOT NULL,
 `FirstName` varchar(100) NOT NULL,
 `LastName` varchar(100) NOT NULL,
 PRIMARY KEY (`Id`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_thai_520_w2;

-- Dumping data for table ToDo.User: ~1 rows (approximately)
INSERT INTO `User` (`Id`, `NationalId`, `Salt`, `HashedPassword`, `Title`, `FirstName`, `LastName`) VALUES
 (1, '1234567890123', 'UOppB4DLI30fHe6bz/1SmQ==', 'AHc5YRwAZEpvK1QvYyOQEnuPfulPoUY2R+KJZxAEY7M=', 'นาง', 'กนก', 'สม');

/*!40103 SET TIME_ZONE=IFNULL(@OLD_TIME_ZONE, 'system') */;
/*!40101 SET SQL_MODE=IFNULL(@OLD_SQL_MODE, '') */;
/*!40014 SET FOREIGN_KEY_CHECKS=IFNULL(@OLD_FOREIGN_KEY_CHECKS, 1) */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40111 SET SQL_NOTES=IFNULL(@OLD_SQL_NOTES, 1) */;

การสร้าง salt และ hashed password

```
C# Program.cs
1  using Microsoft.AspNetCore.Authentication.JwtBearer;
2  using System.Security.Cryptography;
3  using Microsoft.AspNetCore.Cryptography.KeyDerivation;
4  using Microsoft.IdentityModel.Tokens;
5
6  string pwd = "12345678";
7
8  // fixed salt
9  //byte[] s = Convert.FromBase64String("U0ppB4DLI30fHe6bz/lSmQ==");
10
11 // random salt
12 byte[] s = new byte[16];
13 RandomNumberGenerator.Create().GetBytes(s);
14
15 string hash = Convert.ToBase64String(KeyDerivation.Pbkdf2(
16     password: pwd,
17     salt: s,
18     prf: KeyDerivationPrf.HMACSHA1,
19     iterationCount: 10000,
20     numBytesRequested: 32));
21
22 Console.WriteLine("password = " + pwd);
23 Console.WriteLine("salt = " + Convert.ToBase64String(s));
24 Console.WriteLine("hashed password = " + hash);
```

password = 12345678

salt = GV5DJH0Gila9c983f5n6Pw==

hashed password = jldVak/4378qr1Ndvi9bGlcXLmpZ0cMoH2SafLte+Ew=

ต้อง random salt ใหม่ทุกครั้ง salt ของผู้ใช้แต่ละคนไม่ควรซ้ำกัน
เก็บเฉพาะ salt และ hashed password ลงฐานข้อมูล