

ระบบบันทึกและจัดการข้อมูลผู้ใช้เครือข่าย

Network Users Logging and Management System

โดย

นายจักรภูมิ มณีรัตน์

รหัสนักศึกษา 5410110069

อาจารย์ที่ปรึกษาโครงงาน

อาจารย์ที่ปรึกษา อาจารย์รัชชัย เอ็งฉ้วน

หัวข้อที่จะพูดในวันนี้

ภาพรวม

สิ่งที่ได้ดำเนินการไปแล้ว

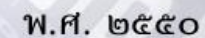
สิ่งที่จะทำต่อไป

สรุป

ภาพรวม

- ที่มาและความสำคัญ
- ความรู้และเครื่องมือที่จะใช้
- แนวคิด

ความสำคัญและที่มาของโครงการ



A close-up photograph of a hand typing on a black computer keyboard. The background is a dark, textured surface featuring a pattern of white binary code (0s and 1s). The word "PASSWORD" is prominently displayed in a bright red, sans-serif font, appearing as if it's a digital overlay or a sticker on the keyboard. The lighting is dramatic, with the hand and the red text being the primary focal points against the dark, patterned background.

ความสำคัญและที่มาของโครงการ

- ระบบและเครื่องมือในส่วนของการระบุตัวตนในปัจจุบันส่วนใหญ่รองรับการทำงานในระบบ IPv4 แต่ยังไม่รองรับระบบ IPv6



ความสำคัญและที่มาของโครงการ

Virtual System	Source User	Source address	Source Host Name	Risk	Bytes	Sessions
vsys1	5[REDACTED]	172.22.[REDACTED]	172.22.1[REDACTED]	5	575.35 M	214
vsys1	5[REDACTED]	172.24.[REDACTED]	172.24.1[REDACTED]	4	570.62 M	55
vsys1	5[REDACTED]	172.24.[REDACTED]	172.24.3[REDACTED]	4	562.59 M	546
vsys1	5[REDACTED]	172.24.[REDACTED]	172.24.2[REDACTED]	4	557.45 M	60
vsys1	5[REDACTED]	172.21.[REDACTED]	172.21.1[REDACTED]	4	553.60 M	323
vsys1	5[REDACTED]	172.24.[REDACTED]	172.24.5[REDACTED]	4	552.52 M	23
vsys1	5[REDACTED]	172.22.[REDACTED]	172.22.1[REDACTED]	4	542.35 M	98
vsys1	5[REDACTED]	172.19.[REDACTED]	172.19.1[REDACTED]	4	532.77 M	50
vsys1	5[REDACTED]	172.18.[REDACTED]	172.18.4[REDACTED]	4	515.05 M	83
vsys1		2001:3c8:9009:51c:a461[REDACTED]	2001:3c8:9009[REDACTED]	4	509.76 M	42

ภาพแสดงข้อมูลบางส่วนจากรางงานสถิติการใช้งาน ของ firewall ของมหาวิทยาลัยสงขลานครินทร์
ในส่วนของ Risky Users ประจำวันที่ 26 กันยายน พ.ศ.2557

ความสำคัญและที่มาของโครงการ

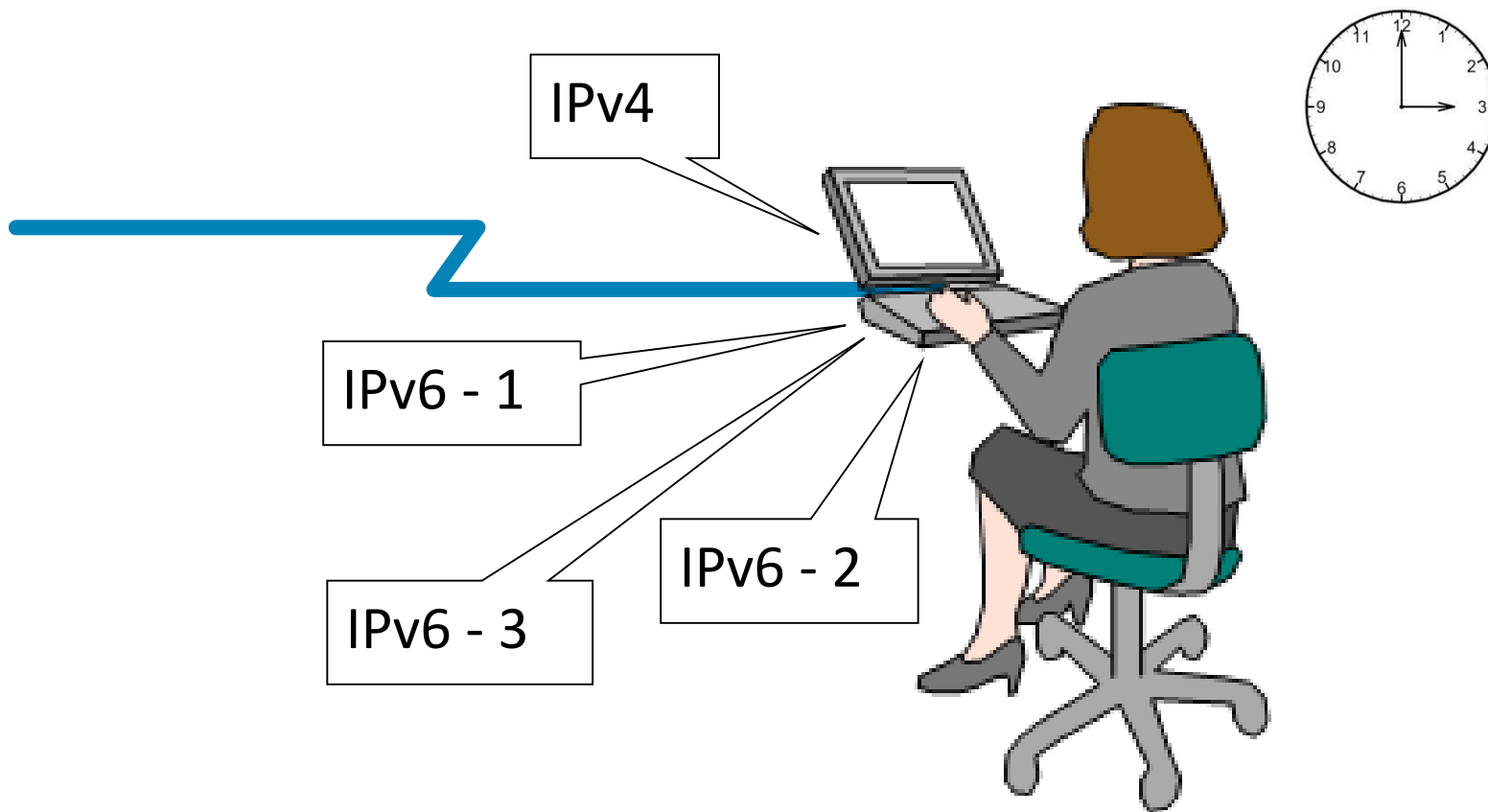
```
tua@tua-OptiPlex-380:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr b8:ac:6f:4e:cd:10
          inet addr:172.30.232.224  Bcast:172.30.232.255  Mask:255.255.255.0
          inet6 addr: 2001:3c8:9009:1e8:dd16:1299:6ee0:fd09/128 Scope:Global
          inet6 addr: 2001:3c8:9009:1e8:fd5c:52e6:b109:4f9e/64 Scope:Global
          inet6 addr: 2001:3c8:9009:1e8:11f5:a7a4:2563:b33a/128 Scope:Global
          inet6 addr: 2001:3c8:9009:1e8:baac:6fff:fe4e:cd10/64 Scope:Global
          inet6 addr: fe80::baac:6fff:fe4e:cd10/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4739906 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1697362 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2030955308 (2.0 GB)  TX bytes:210415007 (210.4 MB)
          Interrupt:16
```

ภาพแสดง หมายเลข IP Address ที่เครื่องตัวอย่างได้รับ

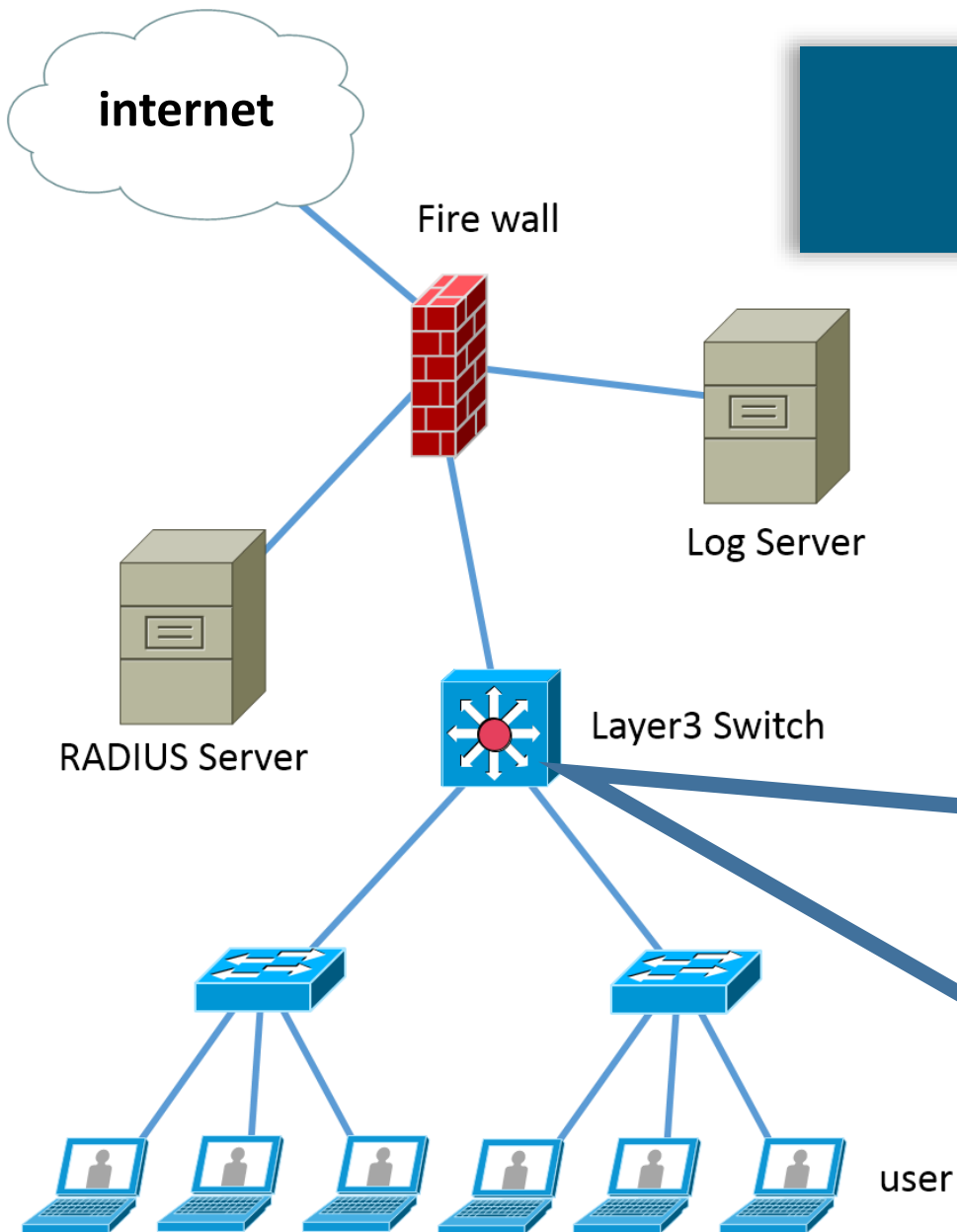
ความรู้และเครื่องมือที่จะใช้

- **ARP**
- **IPv6**
- **ND**
- **SNMP**
- **Layer3 switch**
- **Apache**
- **PHP**
- **MySQL**
- **Perl**
- **RADIUS**

แนวคิด



ภาพหลักการของโครงงาน



แนวคิด

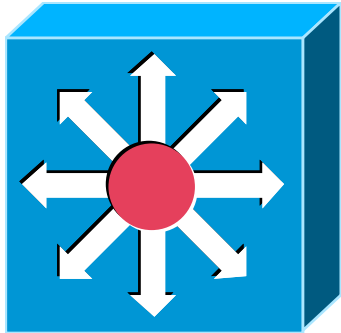
Layer3 switch

ARP table

ND table

ภาพ ระบบเครือข่าย

Layer3 switch



ARP table
(IPv4)

แนวคิด

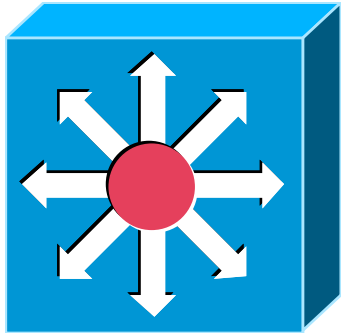
IPv4

Mac
Address

IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.69	=	STRING:	0:12:7f:17:a3:80
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.73	=	STRING:	0:19:e7:e8:2:41
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.75	=	STRING:	c:85:25:c9:25:c1
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.77	=	STRING:	c:85:25:a3:fb:c1
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.79	=	STRING:	a4:56:30:54:bd:c1
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.80	=	STRING:	0:12:43:bd:92:40
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.84	=	STRING:	0:15:63:6:8e:40
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.85	=	STRING:	0:19:e8:6c:40:42
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.88	=	STRING:	a4:56:30:56:68:41
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.89	=	STRING:	c:85:25:eb:e0:c1
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.100	=	STRING:	34:62:88:77:c4:f2
IP-MIB::ipNetToMediaPhysAddress.202	172.30.254.201	=	STRING:	0:c0:b7:d3:95:e8

ภาพ ผลลัพธ์จากการใช้คำสั่งใน SNMP เพื่อเรียกข้อมูลจาก ARP table
ของอุปกรณ์ Layer3 Switch

Layer3 switch



ND table
(IPv6)

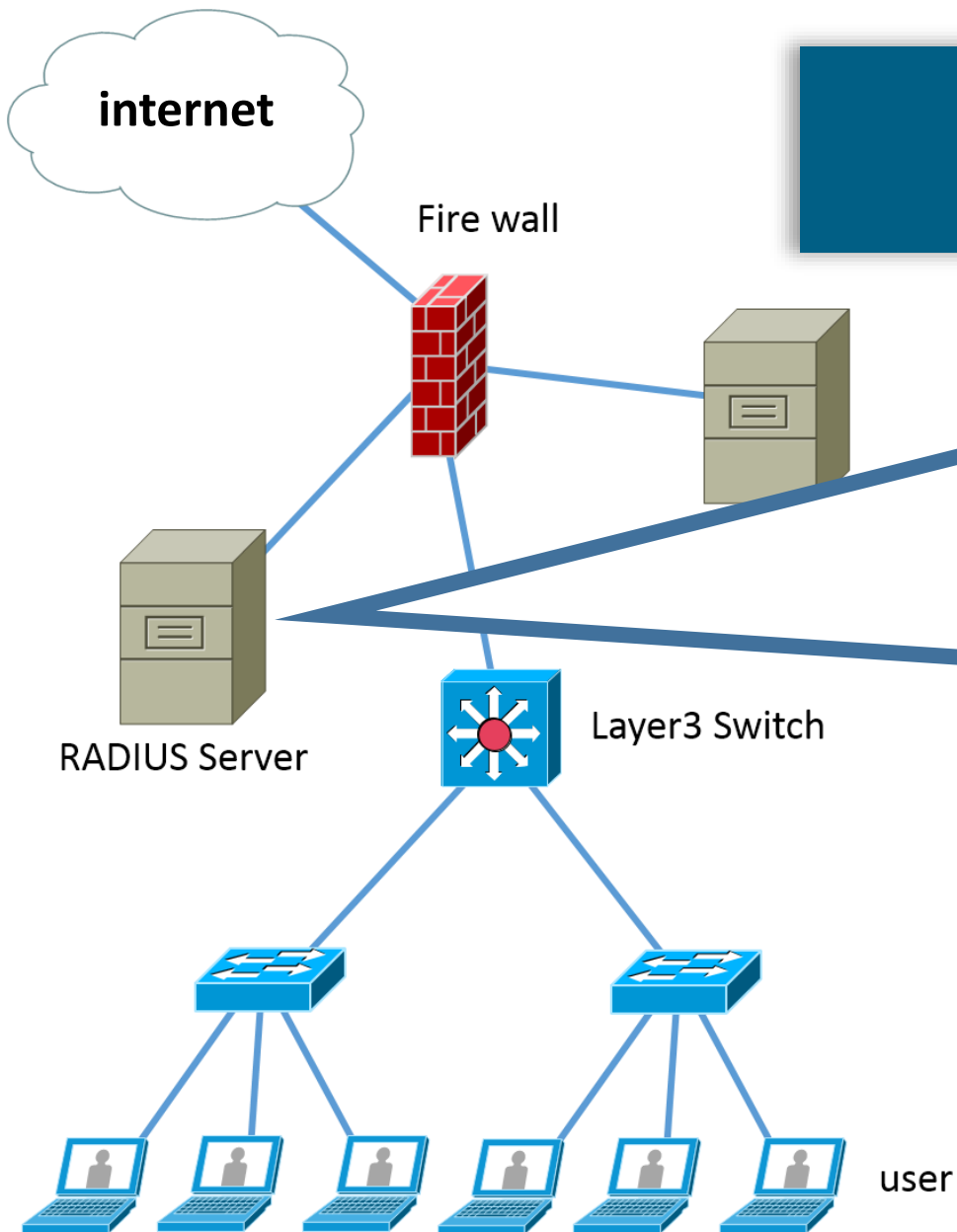
แนวคิด

IPv6

Mac
Address

IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"20:01:03:c8:90:09:01:f3:6d:0c:33:df:5c:53:3a:53"	=	STRING:	20:89:84:89:ff:7d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"20:01:03:c8:90:09:01:f3:a9:5f:ec:70:da:e1:50:86"	=	STRING:	14:da:e9:61:b0:1d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"20:01:03:c8:90:09:01:f3:cc:0c:d9:4a:6d:e9:ba:ac"	=	STRING:	44:8a:5b:a0:83:e6
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"20:01:03:c8:90:09:01:f3:cc:49:8e:8d:4a:4e:29:cd"	=	STRING:	e0:db:55:f7:69:fe
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"20:01:03:c8:90:09:01:f3:f1:c6:b0:42:ff:a8:3a:d5"	=	STRING:	10:78:d2:47:f5:66
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"fe:80:00:00:00:00:00:00:08:7f:c6:9a:1e:fe:4b:c7"	=	STRING:	20:89:84:89:ff:7d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"fe:80:00:00:00:00:00:00:71:35:0a:9d:c0:51:d2:63"	=	STRING:	14:da:e9:61:b0:1d
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"fe:80:00:00:00:00:00:00:90:48:3e:96:da:3b:45:08"	=	STRING:	e0:db:55:f7:69:fe
IP-MIB::ipNetToPhysicalPhysAddress.103.ipv6.	"fe:80:00:00:00:00:00:00:bc:b6:47:8d:ad:6e:50:fb"	=	STRING:	f0:4d:a2:61:b7:22

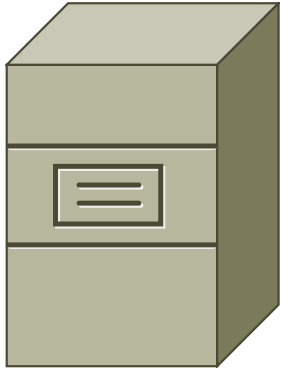
ภาพตัวอย่างผลลัพธ์จากการใช้คำสั่งใน SNMP เพื่อเรียกข้อมูลจาก ND table
ของอุปกรณ์ Layer3 Switch



แนวคิด

ภาพ ระบบเครือข่าย

RADIUS Server



Log การลง
ชื่อเข้าใช้

แนวคิด

```
Wed Apr 15 23:44:45 2015
Acct-Status-Type = Start
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "BC:EE:7B:53:4F:A0"
Called-Station-Id = "hotspot1"
NAS-Port-Id = "ether3"
User-Name = "test"
NAS-Port = 2148532238
Acct-Session-Id = "8010000e"
Framed-IP-Address = 10.5.50.254
Mikrotik-Host-IP = 10.5.50.254
Event-Timestamp = "Apr 15 2015 23:44:38 ICT"
NAS-Identifier = "MikroTik"
Acct-Delay-Time = 0
NAS-IP-Address = 172.30.232.93
Acct-Unique-Session-Id = "138d0e2d0f8763e9"
Timestamp = 1429116285
```

Mac

User

เวลา
อ้างอิง

ภาพตัวอย่าง Log ไฟล์ของ RADIUS Server

ARP

Physical Address	IP Address
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx

ND

Physical Address	IP Address
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx

Radius

User	Physical Address
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxx

+

+

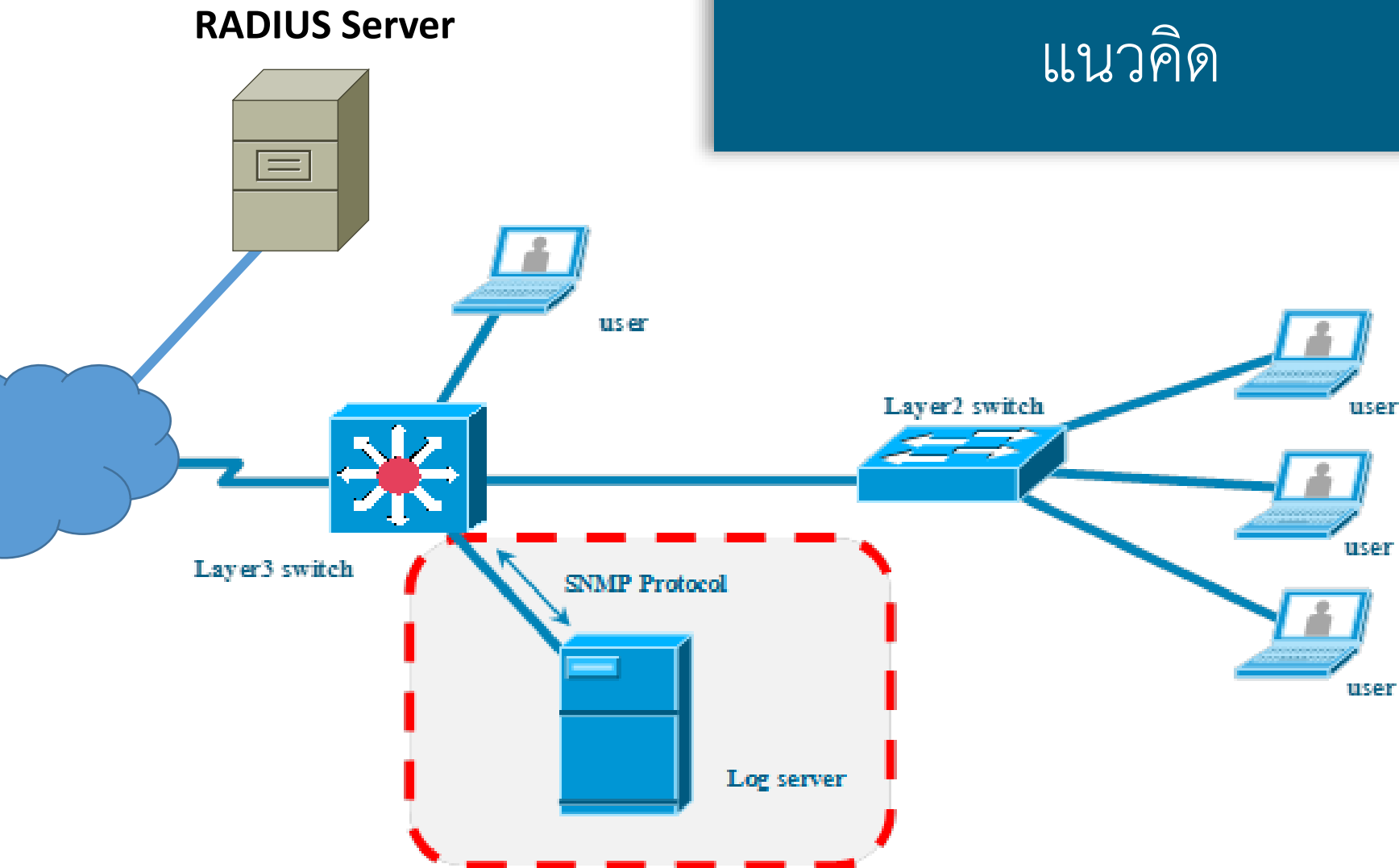
Database



Timpstamp	IPv6	IPv4	Physical Address	User
xxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxx
xxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxx	xxxxxxx

แนวทางการทำงาน

แนวคิด



ภาพรวมระบบที่ได้ออกแบบ

ส่วนที่ 1
ใช้ภาษา
PERL

แนวคิด

ส่วนที่ 2
ใช้ **mysql**

Script ในการดึง
ข้อมูล

รวบรวมและจัดเรียง
ข้อมูล

ส่วนที่ 3
ใช้ภาษา

PHP,HTML

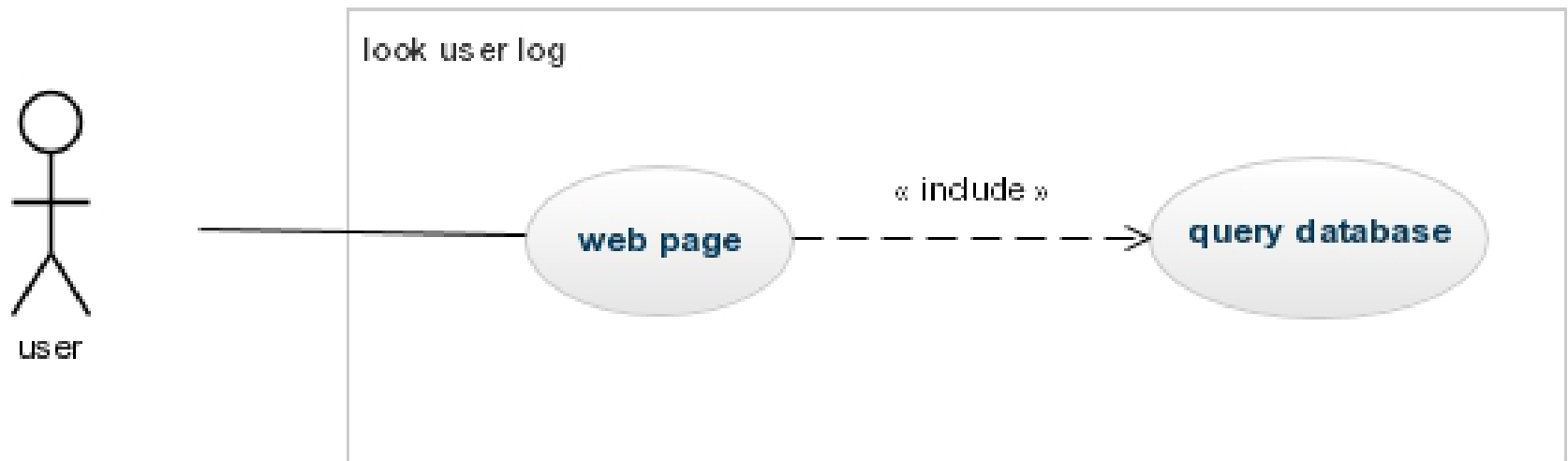
เว็บสำหรับเรียกดู
ข้อมูล



Database

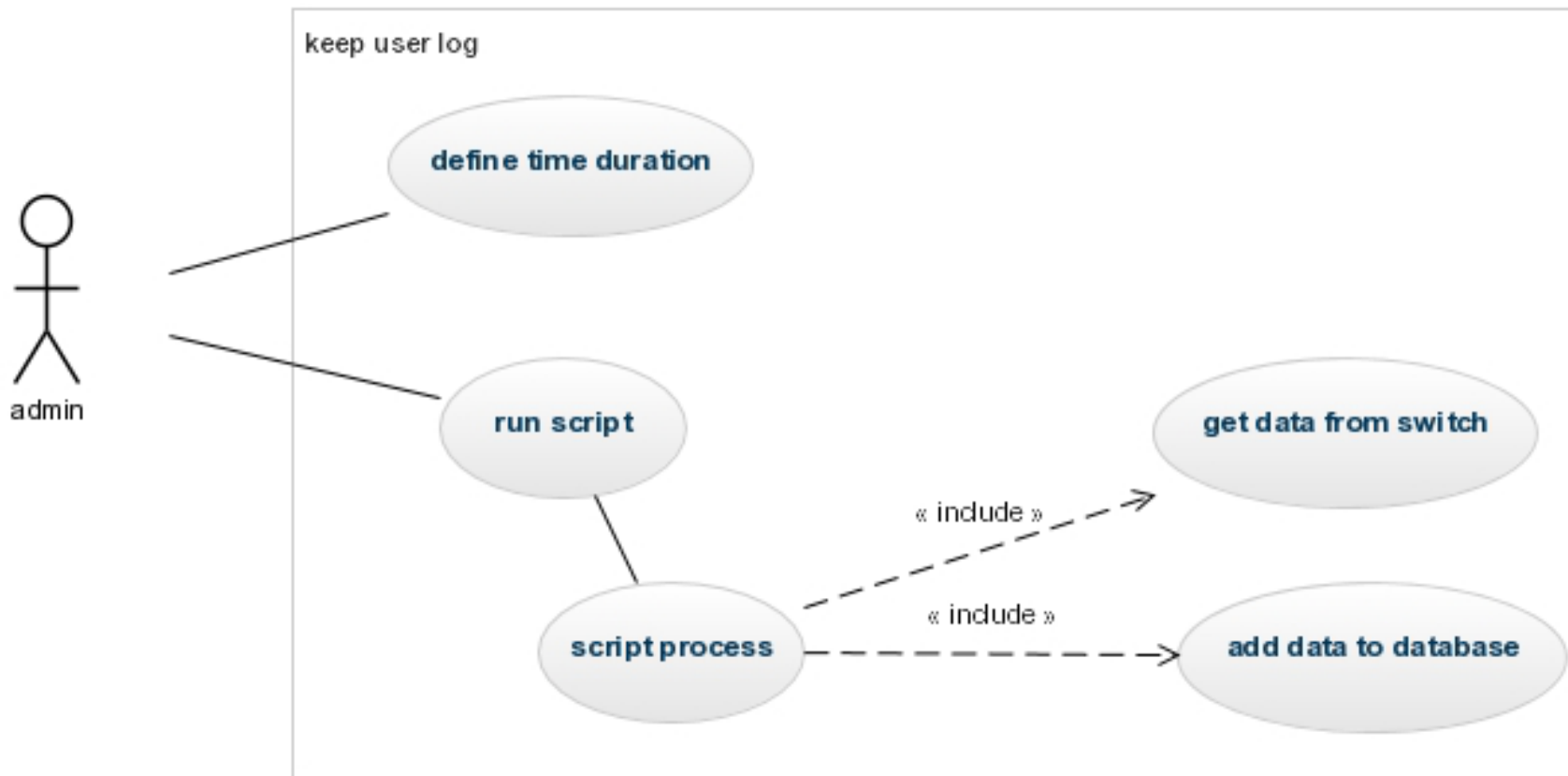
ส่วนประกอบหลักของโครงการ

แนวคิด



ภาพ **usecase diagram** ของผู้ใช้ทั่วไป

แนวคิด



ภาพ **usecase diagram** ของผู้ดูแลระบบ

สิ่งที่ได้ดำเนินการไปแล้ว

สิ่งที่ได้ดำเนินการไปแล้ว

PERL

Script ในการดึง
ข้อมูล

รวบรวมและ
จัดเรียงข้อมูล

mySQL



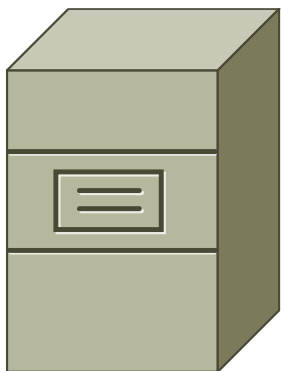
Database

PHP

เว็บสำหรับเรียกดู
ข้อมูล

ส่วนประกอบหลักของโครงการ

RADIUS Server

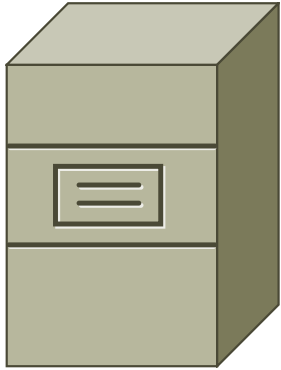


สิ่งที่ได้ดำเนินการไปแล้ว



ภาพตัวอย่างหน้า Login โดยใช้ RADIUS Server

RADIUS Server



Log การลง
ชื่อเข้าใช้

สิ่งที่ได้ดำเนินการไปแล้ว

```
Wed Apr 15 23:44:45 2015
Acct-Status-Type = Start
NAS-Port-Type = Wireless-802.11
Calling-Station-Id = "BC:EE:7B:53:4F:A0"
Called-Station-Id = "hotspot1"
NAS-Port-Id = "ether3"
User-Name = "test"
NAS-Port = 2148532238
Acct-Session-Id = "8010000e"
Framed-IP-Address = 10.5.50.254
Mikrotik-Host-IP = 10.5.50.254
Event-Timestamp = "Apr 15 2015 23:44:38 ICT"
NAS-Identifier = "MikroTik"
Acct-Delay-Time = 0
NAS-IP-Address = 172.30.232.93
Acct-Unique-Session-Id = "138d0e2d0f8763e9"
Timestamp = 1429116285
```

Mac

User

เวลา
อ้างอิง

ภาพตัวอย่าง Log ไฟล์ของ RADIUS Server

สิ่งที่ได้ดำเนินการไปแล้ว

IPv6

2015-4-20 05:41:52
BC:EE:7B:53:4F:A0
user7

Mac

2015-4-20 21:57:45
BC:EE:7B:53:4F:A0
user7

user

ตัวอย่างผลลัพธ์จากการทดลอง

สิ่งที่ได้ดำเนินการไปแล้ว

IPv6

Mac

user2	2001:03c8:9009:01f5:c868:d6a7:9d52:8a51	18:3:73:d5:70:7b	172.30.245.181	2015-6-25 15:54:39
user4	fe80:0000:0000:0000:213b:2f9c:f226:d362	0:23:54:26:b4:34	172.30.245.176	2015-6-25 15:54:39
user2	fe80:0000:0000:0000:4874:82fe:9b53:a715	18:3:73:d5:70:7b	172.30.245.181	2015-6-25 15:54:39
user5	2001:03c8:9009:01f7:a870:93b4:51c6:fbcb	74:d0:2b:7:3c:a8	172.30.247.199	2015-6-25 15:54:39
user7	2001:03c8:9009:01f7:b872:7894:b954:b613	4c:72:b9:b1:bb:ff	172.30.247.188	2015-6-25 15:54:39
user7	fe80:0000:0000:0000:4e72:b9ff:feb1:bbff	4c:72:b9:b1:bb:ff	172.30.247.188	2015-6-25 15:54:39
user5	fe80:0000:0000:0000:a870:93b4:51c6:fbcb	74:d0:2b:7:3c:a8	172.30.247.199	2015-6-25 15:54:39

user

ตัวอย่างผลลัพธ์จากการทดลอง

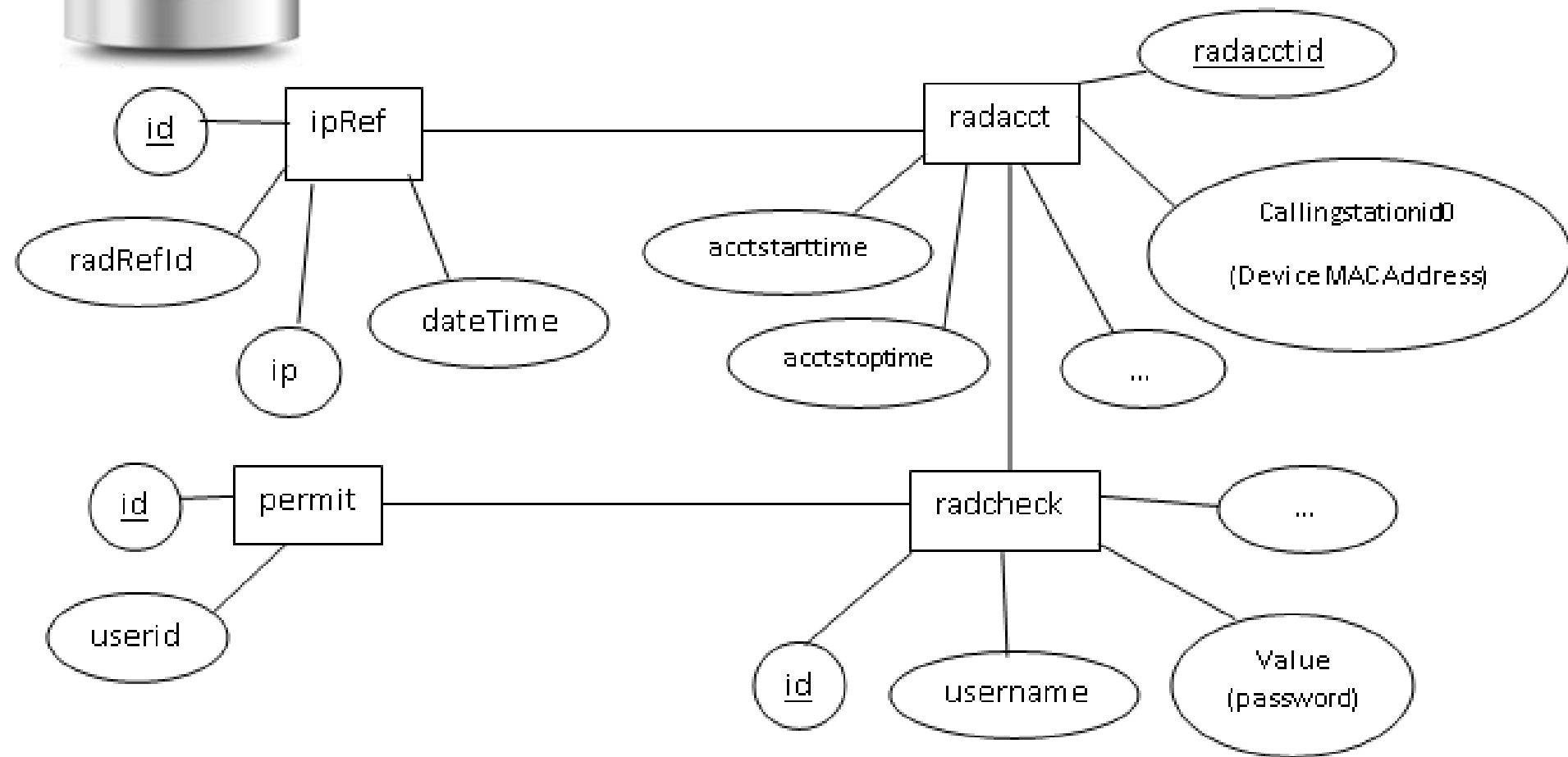
IPv4

เวลาอ้างอิง

Database

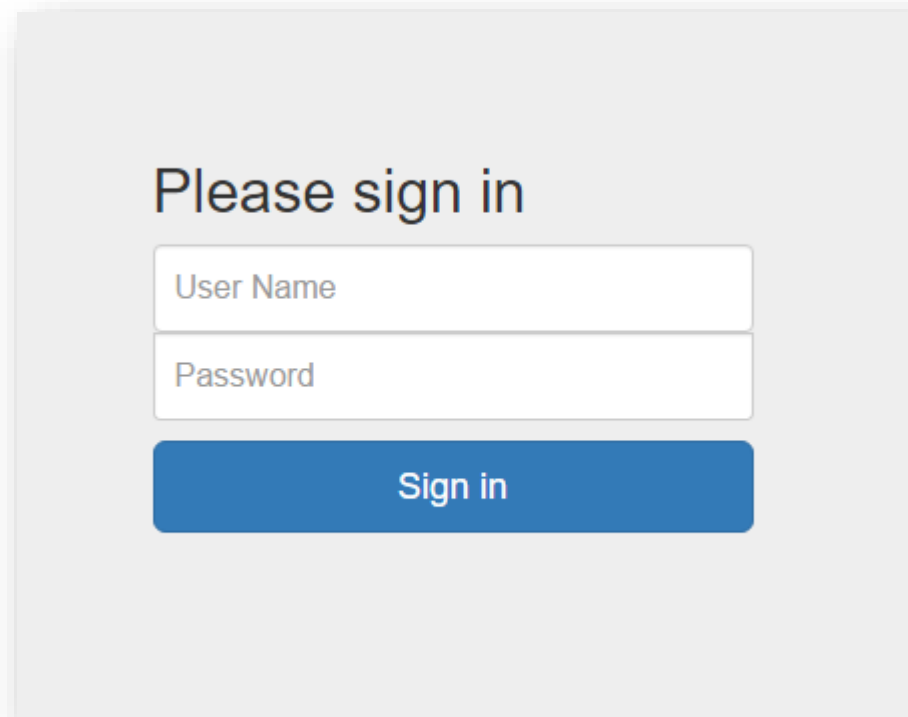


สิ่งที่ได้ดำเนินการไปแล้ว



ภาพ ER diagram ของฐานข้อมูล

สิ่งที่ได้ดำเนินการไปแล้ว



Please sign in

User Name

Password

Sign in

ตัวอย่างผลลัพธ์จากโครงการ

สิ่งที่ได้ดำเนินการไปแล้ว

User Log Management System

User : tua Permission : ADMIN [logout](#)

User : tua
Permission : ADMIN
[logout](#)

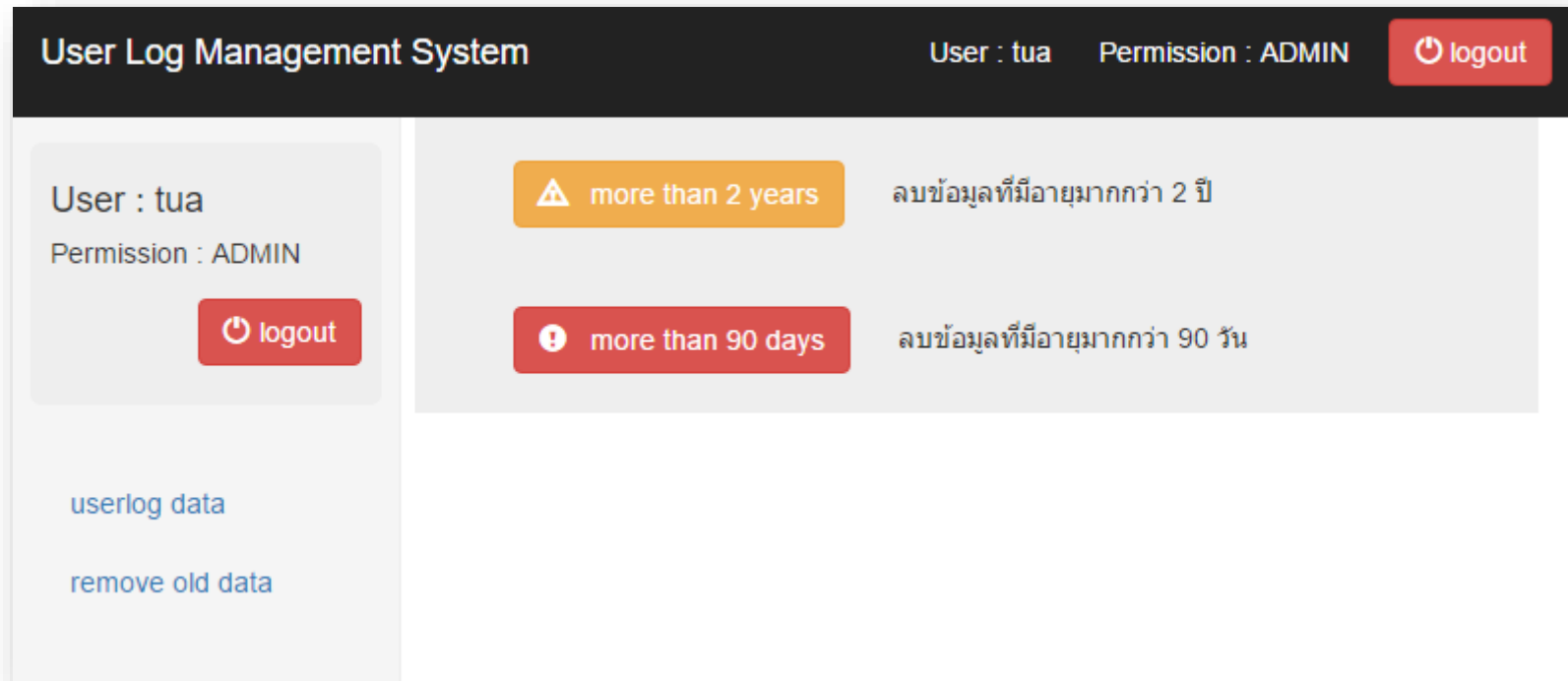
date time between --:-- and --:--
☒ IP(v4) Address ☐ IP(v6) Address ☐ Mac Address

[Search](#)

Username	ACC time start	ACC time stop	Type	Physical Address	IP Address
tua	2016-10-04 16:38:51	connect until now	Ethernet	BC-EE-7B-53-4F-A0	172.30.231.15 2001:03C8:9009:01E7:50F8:8439:99C0:DD70 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-09-30 23:25:50	2016-10-02 17:38:14	Ethernet	BC-EE-7B-53-4F-A0	172.30.231.14 2001:03C8:9009:01E7:A572:2D13:C27D:2F46 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB
tua	2016-09-27 18:12:21	2016-09-30 23:22:16	Ethernet	BC-EE-7B-53-4F-A0	172.30.231.14 2001:03C8:9009:01E7:11A3:2149:521A:BFE3 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-09-23 18:01:51	2016-09-27 18:11:59	Ethernet	BC-EE-7B-53-4F-A0	172.30.231.13 2001:03C8:9009:01E7:44C6:735D:5D8B:5356 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB

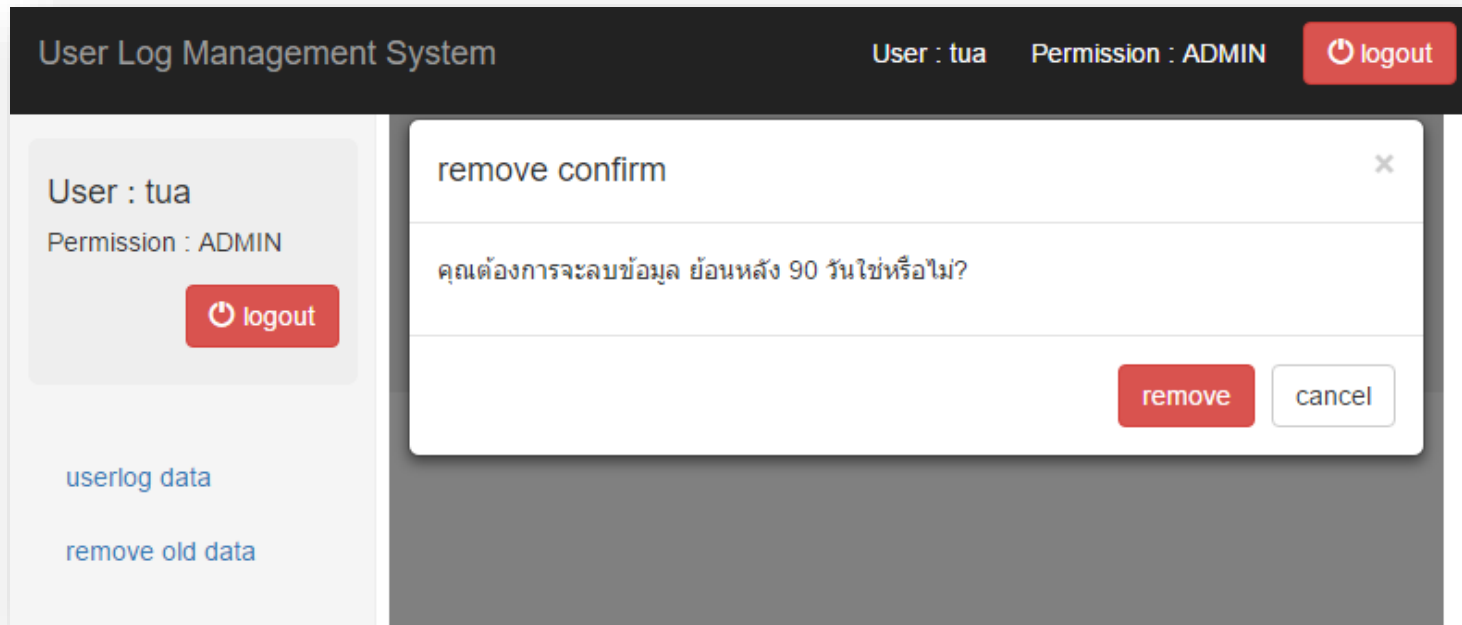
ตัวอย่างผลลัพธ์จากโครงการ

สิ่งที่ได้ดำเนินการไปแล้ว



ตัวอย่างผลลัพธ์จากโครงการ

สิ่งที่ได้ดำเนินการไปแล้ว



ตัวอย่างผลลัพธ์จากโครงการ

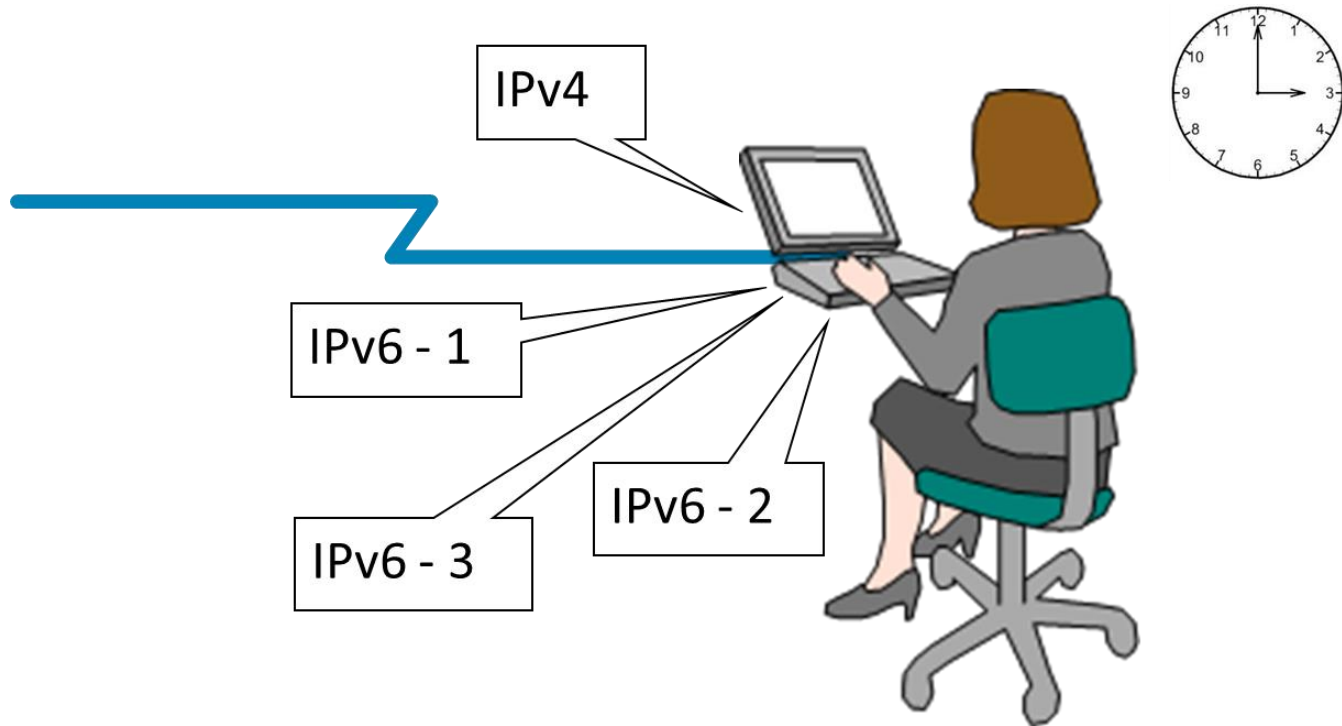
สรุป

สรุป



ที่มาและความสำคัญ

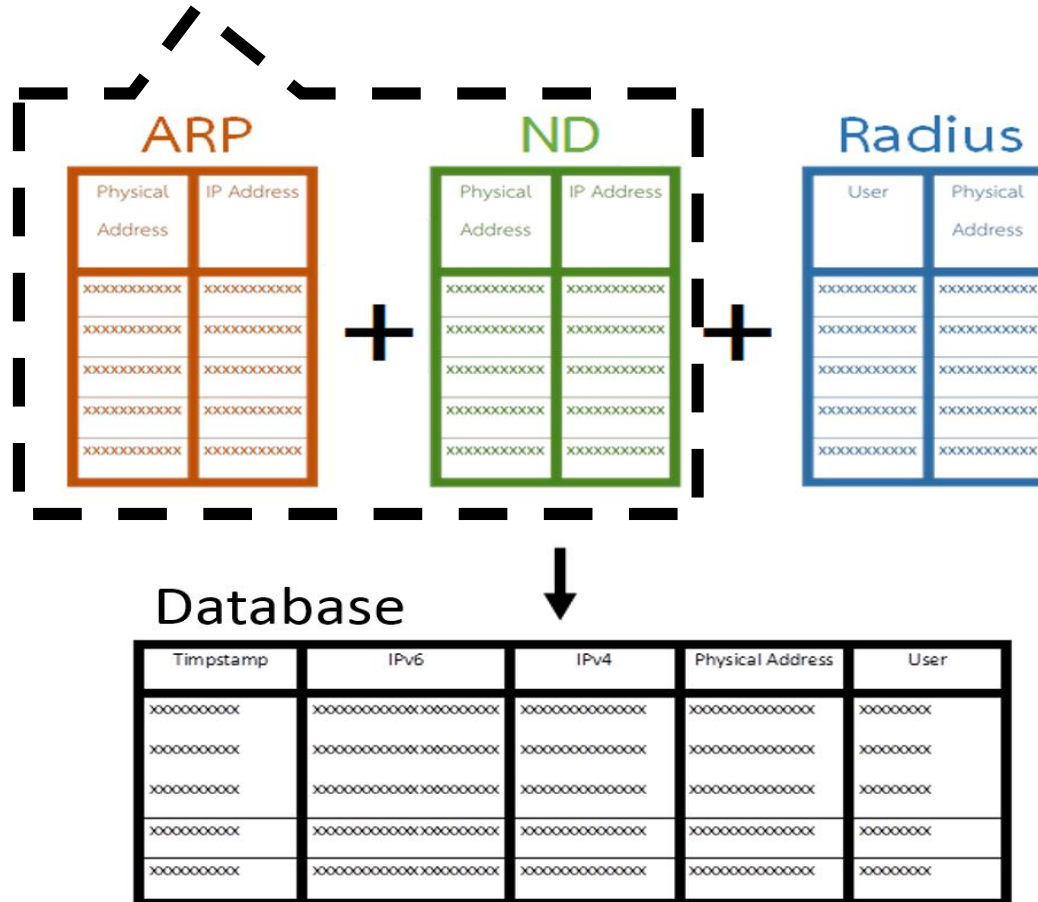
สรุป



แนวคิดของโครงการ

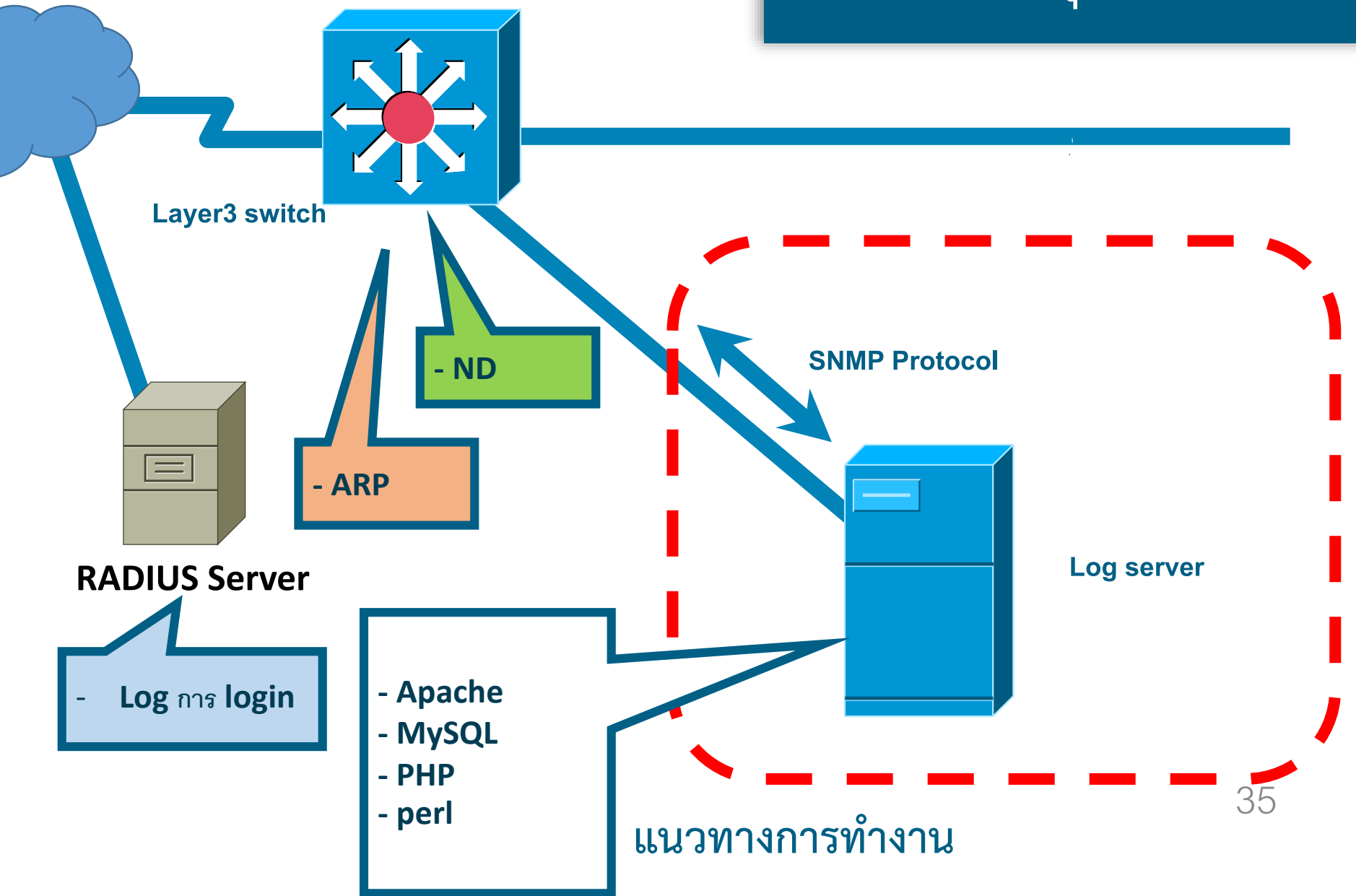
สรุป

ข้อมูลจาก อุปกรณ์สวิต



แนวทางการทำงาน

สรุป



สรุป

PERL

Script ในการดึง
ข้อมูล

รวบรวมและ
จัดเรียงข้อมูล

mySQL



Database

PHP

เว็บสำหรับเรียกดู
ข้อมูล

ส่วนประกอบหลักของโครงการ

สิ่งที่ได้ดำเนินการไปแล้ว

User Log Management System

User : tua Permission : ADMIN [logout](#)

User : tua
Permission : ADMIN
[logout](#)

[userlog data](#)
[print report](#)
[remove old data](#)

date time between --:-- and --:--

[Search](#)

Username	ACC time start	ACC time stop	Device Vender	Physical Address	IP Address
tua	2016-11-28 15:51:16	connect until now	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:D421:C472:D16C:4F27 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-11-15 16:04:19	2016-11-24 09:57:29	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.17 2001:03C8:9009:01E7:71B1:3C53:BCFA:F4CB FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-10-04 16:38:51	2016-10-05 06:21:47	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.15 2001:03C8:9009:01E7:50F8:8439:99C0:DD70 FE80:0000:0000:0000:71B1:3C53:BCFA:F4CB
tua	2016-09-30 23:25:50	2016-10-02 17:38:14	ASUSTek COMPUTER INC.	BC-EE-7B-53-4F-A0	172.30.231.14 2001:03C8:9009:01E7:4578:8D18:887D:8E16

ตัวอย่างผลลัพธ์จากโครงการ

คำถามและข้อเสนอแนะ

ขอบคุณครับ