คู่มือการใช้งานโปรแกรม ntop 3.2 ฉบับภาษาไทย

จัดทำโดย

นางสาวสิริกานต์ พุกกะวรรณะ
ดร.พนิตา พงษ์ไพบูลย์

18 มิถุนายน 2550

สงวนลิขสิทธิ์โดย

หน่วยปฏิบัติการวิจัยเทคโนโลยีเครือข่าย

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
National Electronic and Computer Technology Center (NECTEC)

สารบัญ

1. วิธีการเปิด-ปิดโปรแกรม NTOP 3

1.1. วิธีการเปิดโปรแกรม ntop 3
1.2 วิธีการปิดโปรแกรม ntop ผ่านทางโปรแกรม Web browser 4

2. วิธีการสืบค้นข้อมูลจากโปรแกรม NTOP 5

2.1. ข้อมูลเบื้องต้นเกี่ยวกับโปรแกรม ntop 5
2.2 ข้อมูลโดยรวมเกี่ยวกับเครือข่าย 6
2.3 รายละเอียดของแต่ละโฮสต์ 7
2.4 สถิติการใช้งานเครือข่าย 8
2.5 เน็คเวร์คโฟลว์ (Network Flow) 9
2.6 ปริมาณการใช้งานเครือข่ายของแต่ละผู้ใช้ แยกตามโพรโตคอล 10
2.7 อัตราการรับส่งข้อมูลของแต่ละโฮสต์ 11
2.8 กิจกรรมของโฮสต์ตามช่วงเวลา 12
2.9 ปริมาณการใช้งานเครือข่ายของแต่ละผู้ใช้ แยกตามแอพพลิเคชั่น 13
2.10 ข้อมูลเกี่ยวกัลมัลติคาสต์ (Multicast) 14
2.11 รายละเอียดของแต่ละโดเมน (Internet Domain) 15
2.12 กลุ่มของโฮสต์ (Host Cluster) 16
2.13 สัดส่วนของข้อมูลบนเครือข่าย 16
2.14 ทิศทางของข้อมูลบนเครือข่าย 18
2.15 ข้อมูลการใช้บริการเครือข่ายของผู้ใช้ 19
2.16 ระบบปฏิบัติการของแต่ละโฮสต์ 20
2.17 บทบาทของแต่ละโฮสต์ 21
2.18 ข้อมูลบนเครือข่ายภายใน (Network Map) 22
2.19 การติดต่อสื่อสารระหว่างโฮสต์ภายใน (Matrix) 22
2.20 ช่องสัญญาณไฟเบอร์แชนแนล (Fiber Channel) 23
2.21 เก็บข้อมูลบนเครือข่าย (Data Dump) 23
2.22 ดูล็อกไฟล์ 24
2.23 โฮสต์ที่ดูล่าสุด (ปลั๊กอิน) 25
2.24 ปริมาณโพรโตคอล ICMP ของแต่ละโฮสต์ (ปลั๊กอิน) 25
2.25 สรปอันดับโฮสต์ที่ใช้งานเครือข่ายมากที่สุด (ปลั๊กอิน) 26
2.26 สถิติต่างๆ ในรูปแบบของกราฟรูปภาพ (ปลั๊กอิน) 27
2.27 เก็บข้อมูลในรูปแบบ XML (ปลั๊กอิน) 27

3. วิธีการปรับแต่งค่าบนโปรแกรม NTOP 28

3.1. เปลี่ยนการ์ดแลน (Network Interface Card) 28
3.2 ตั้งค่าพื้นฐานต่างๆ บนโปรแกรม ntop 29
3.3 ตั้งค่าโปรแกรม ntop 33
3.4 ตั้งค่าการกรองแพ็คเก็ตขณะตรวจจับ 34
3.5 รีเซ็ตสถิติ 34
3.6 ตั้งค่าผู้ใช้งานโปรแกรม ntop 35
3.7 ป้องกันหน้า Web page 36

1. วิธีการเปิด-ปิดโปรแกรม ntop

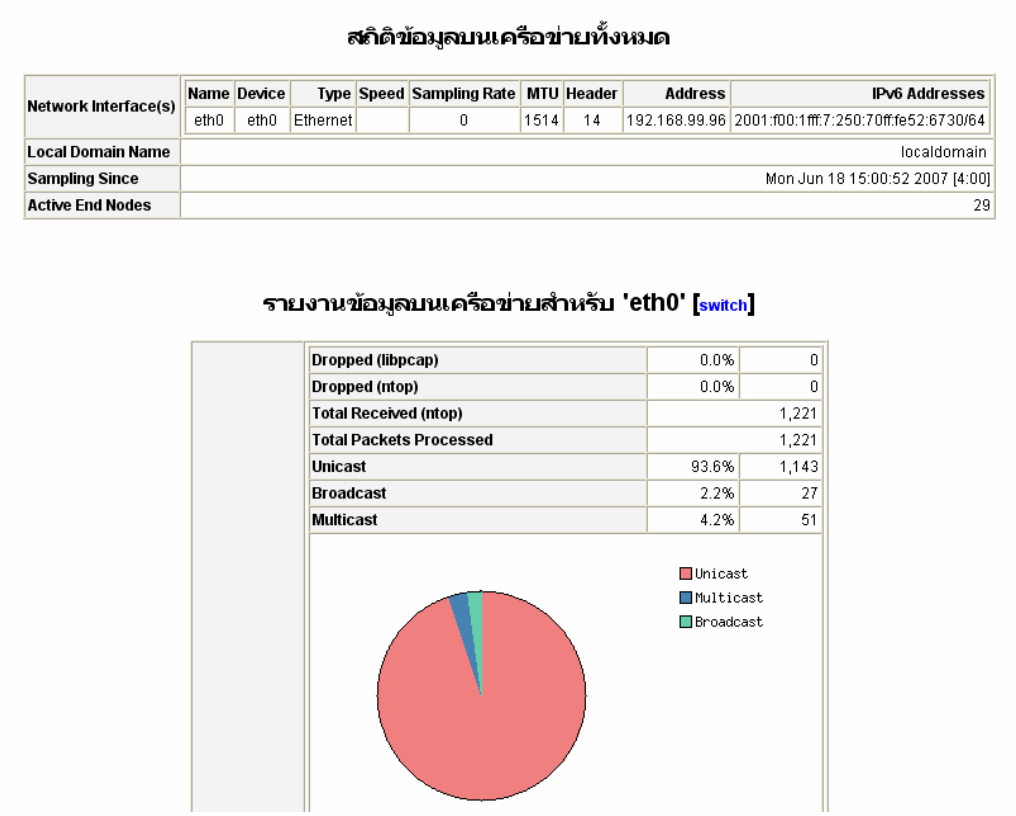
1.1. วิธีการเปิดโปรแกรม ntop

ขั้นตอนการเปิดโปรแกรม ntop มีขั้นตอนดังนี้

- เปิดโปรแกรม Web browser ขึ้นมา ตัวอย่างโปรแกรม Web browser ได้แก่ Mozilliar Firefox และ Internet Explorer เป็นต้น

- หลังจากเปิดโปรแกรม Web browser ขึ้นมาแล้ว ให้พิมพ์หมายเลขไอพีแอดเดรสของเครื่องที่ติดตั้งโปรแกรม ntop แล้วตามด้วยหมายเลยพอร์ต 3000 ลงบ่นช่อง URL เช่น หากเครื่องที่ติดตั้งโปรแกรม ntop มีหมายเลขไอพีแอสเดรสเป็น 192.168.99.96 ให้พิมพ์ "http://192.168.99.96000" ลงบนช่อง URL ดังรูป

- หลังจากนั้น โปรแกรม ntop จะแสดงหน้าแรกของโปรแกรม ดังรูป



สถิติข้อมูลบนเครือข่ายทั้งหมด

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		0	1514	14	192.168.99.96	2001:f00:1fff:7:250:70ff:fe52:6730/64
Local Domain Name	localdomain								
Sampling Since	Mon Jun 18 15:00:52 2007 [4:00]								
Active End Nodes	29								

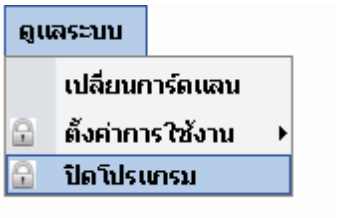
รายงานข้อมูลบนเครือข่ายสำหรับ 'eth0' [switch]

Dropped (libpcap)	0.0%	0
Dropped (ntop)	0.0%	0
Total Received (ntop)		1,221
Total Packets Processed		1,221
Unicast	93.6%	1,143
Broadcast	2.2%	27
Multicast	4.2%	51

1.2. <u>วิธีการปิดโปรแกรม ntop ผ่านทางโปรแกรม Web browser</u>

ขั้นตอนการปิดโปรแกรม ntop ผ่านทางโปรแกรม Web browser มีขั้นตอนดังนี้

- เข้าเมนู ***ดูแลระบบ → ปิดโปรแกรม*** ดังรูป



- หลังจากเลือกเมนูปิดโปรแกรม จะต้องใส่ Username และ Password ของผู้ดูแลระบบเพื่อยืนยันการปิดโปรแกรมอีกครั้ง ดังรูป (Username ของผู้ดูแลระบบบนโปรแกรม ntop คือ "admin" และ Password ขึ้นอยู่กับการกำหนดขณะติดตั้งโปรแกรม ntop)

- หลังจากนั้นรอประมาณ 25 วินาที โปรแกรม ntop ถึงจะปิดโปรแกรมอย่างสมบูรณ์ โดยหน้าจอโปรแกรม ntop หลังจากถูกปิด จะแสดงผล ดังรูป

2. วิธีการสืบค้นข้อมูลจากโปรแกรม ntop

2.1. <u>ข้อมูลเบื้องต้นเกี่ยวกับโปรแกรม ntop</u>

หากต้องการทราบถึงข้อมูลพื้นฐานเกี่ยวกับโปรแกรม ntop เช่น

- โปรแกรม ntop คือโปรแกรมอะไร และมีประโยชน์อย่างไรบ้าง
- การตั้งค่าต่างๆ บนโปรแกรม ntop
- ใครเป็นผู้พัฒนาโปรแกรม ntop
- คู่มือการใช้งานโปรแกรม ntop เบื้องต้น
- เมนูช่วยเหลือสำหรับผู้ใช้งานโปรแกรม ntop
- คำถามที่พบบ่อยเกี่ยวกับโปรแกรม ntop โดยรวมทั้งคำถามทางด้านเทคนิค และคำถามทั่วไปเกี่ยวกับการใช้งานโปรแกรม ntop
- ความหมายของสัญลักษณ์ต่างๆ บนโปรแกรม ntop

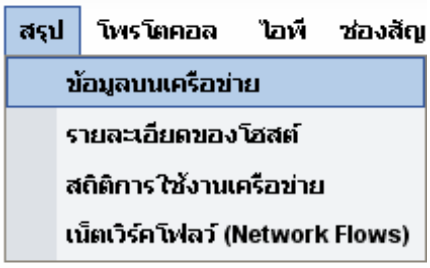
ข้อมูลพื้นฐานต่างๆ เหล่านี้สามารถเข้าไปดูได้ที่เมนู ***แนะนำ ntop*** ดังรูป

2.2. <u>ข้อมูลโดยรวมเกี่ยวกับเครือข่าย</u>

หากต้องการทราบรายละเอียดโดยรวมทั้งหมดของเครือข่าย เช่น

- ชื่ออุปกรณ์ที่ทำการตรวจจับข้อมูลบนเครือข่าย (Network Interface Card)
- หมายเลข IP address ของเครื่องที่ตรวจจับข้อมูลบนเครือข่าย
- สัดส่วนปริมาณข้อมูลแบบ Unicast และ Multicast ของทั้งเครือข่าย
- สัดส่วนขนาดของแพ็คเก็ตบนเครือข่าย
- สัดส่วนระหว่าง IP แพ็คเก็ต กับ Non-IP แพ็คเก็ต
- สถิติการรับส่งข้อมูลของทั้งเครือข่ายแยกตามโพรโตคอล มีหน่วยเป็น ไบต์ต่อวินาที (bytes/sec)

ข้อมูลเหล่านี้ สามารถเข้าไปที่เมนู ***สรุป → ข้อมูลบนเครือข่าย*** ดังรูป

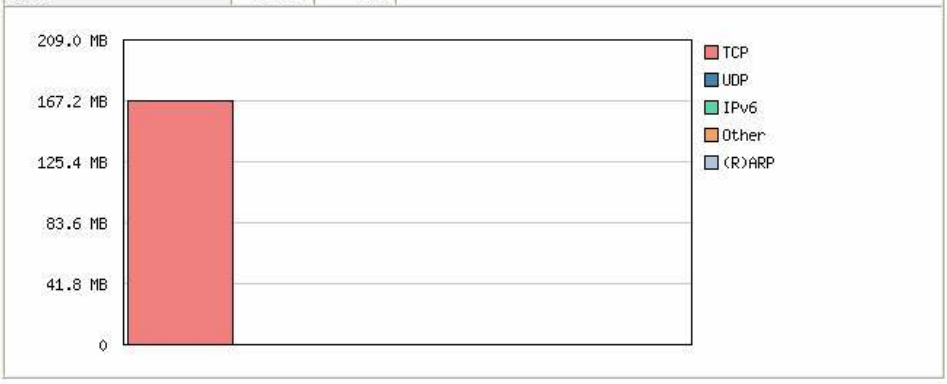


สถิติข้อมูลบนเครือข่ายทั้งหมด

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth0	eth0	Ethernet		0	1514	14	192.168.99.96	2001:f00:1fff:7:250:70ff:fe52:6730/64
Local Domain Name	localdomain								
Sampling Since	Mon Jun 18 15:32:14 2007 [3:11]								
Active End Nodes	125								

การกระจายข้อมูลของโพรโตคอลทั้งหมด

Protocol	Data	Percentage				
IP	165.8 MB	100.0%	TCP	165.7 MB	100.0%	
			UDP	60.6 KB	0%	
			ICMPv6	3.5 KB	0%	
(R)ARP	1.0 KB	0%				
IPv6	3.5 KB	0%				
Other	2.0 KB	0%				

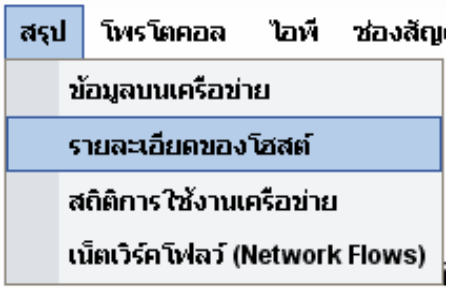


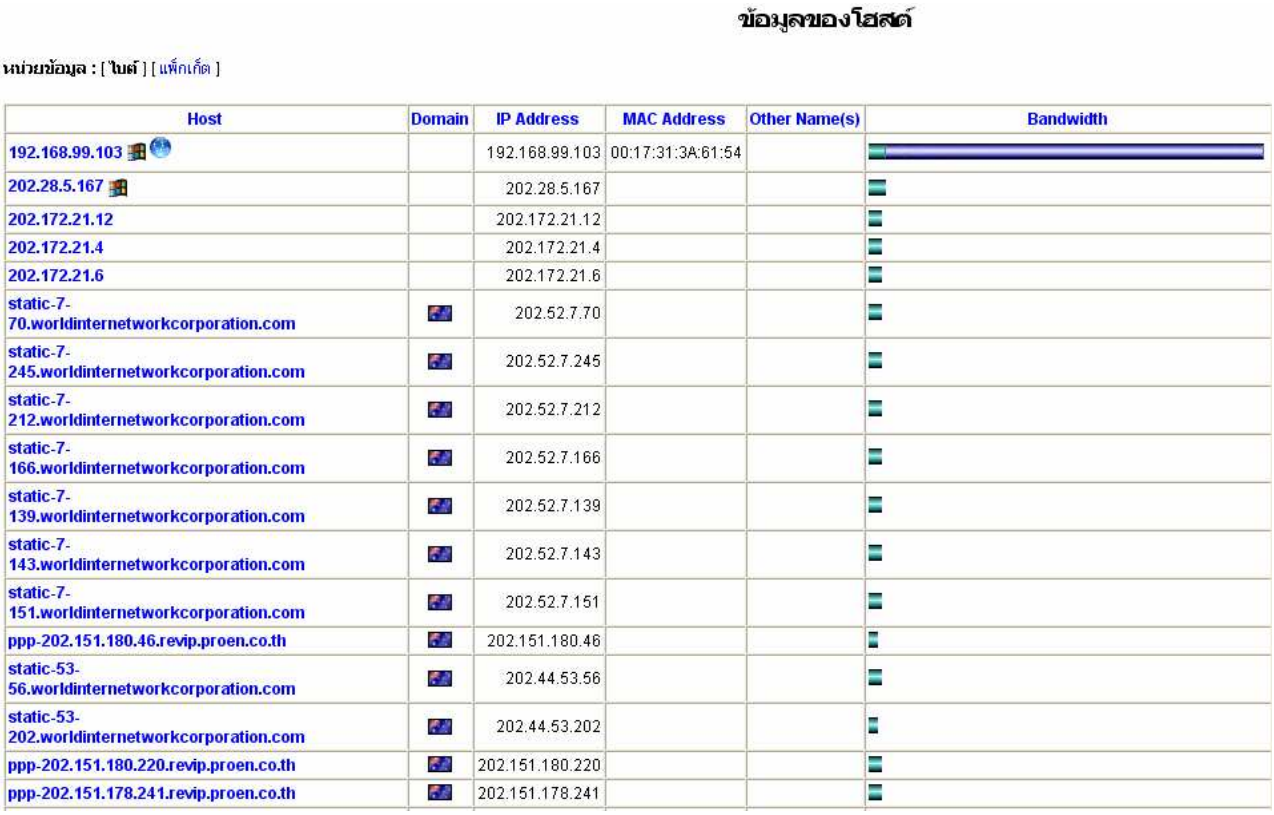
2.3. <u>รายละเอียดของแต่ละโฮสต์</u>

หากต้องการทราบข้อมูลเบื้องต้นเกี่ยวกับเครือข่ายของแต่ละโฮสต์ เช่น

- หมายเลขไอพีแอดเดรส (IP address)
- หมายเลขอุปกรณ์ดักจับเครือข่าย (MAC address)
- โดเมน (Domain)
- ปริมาณการใช้งานเครือข่าย (Bandwidth) โดยคิดเป็นร้อยละของการใช้งานเครือข่ายทั้งหมด

รายละเอียดของแต่ละโฮสต์เหล่านี้ สามารถเข้าไปดูได้ที่เมนู ***สรุป → รายละเอียดของโฮสต์*** ดังรูป





ข้อมูลของโฮสต์

หน่วยข้อมูล : [ไบต์] [แพ็กเก็ต]

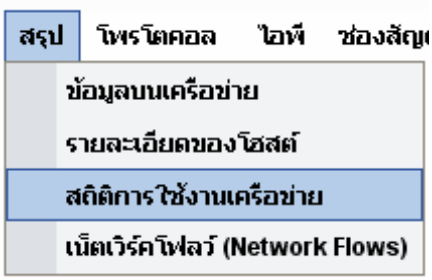
Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth
192.168.99.103		192.168.99.103	00:17:31:3A:61:54		
202.28.5.167		202.28.5.167			
202.172.21.12		202.172.21.12			
202.172.21.4		202.172.21.4			
202.172.21.6		202.172.21.6			
static-7-70.worldinternetworkcorporation.com		202.52.7.70			
static-7-245.worldinternetworkcorporation.com		202.52.7.245			
static-7-212.worldinternetworkcorporation.com		202.52.7.212			
static-7-166.worldinternetworkcorporation.com		202.52.7.166			
static-7-139.worldinternetworkcorporation.com		202.52.7.139			
static-7-143.worldinternetworkcorporation.com		202.52.7.143			
static-7-151.worldinternetworkcorporation.com		202.52.7.151			
ppp-202.151.180.46.revip.proen.co.th		202.151.180.46			
static-53-56.worldinternetworkcorporation.com		202.44.53.56			
static-53-202.worldinternetworkcorporation.com		202.44.53.202			
ppp-202.151.180.220.revip.proen.co.th		202.151.180.220			
ppp-202.151.178.241.revip.proen.co.th		202.151.178.241			

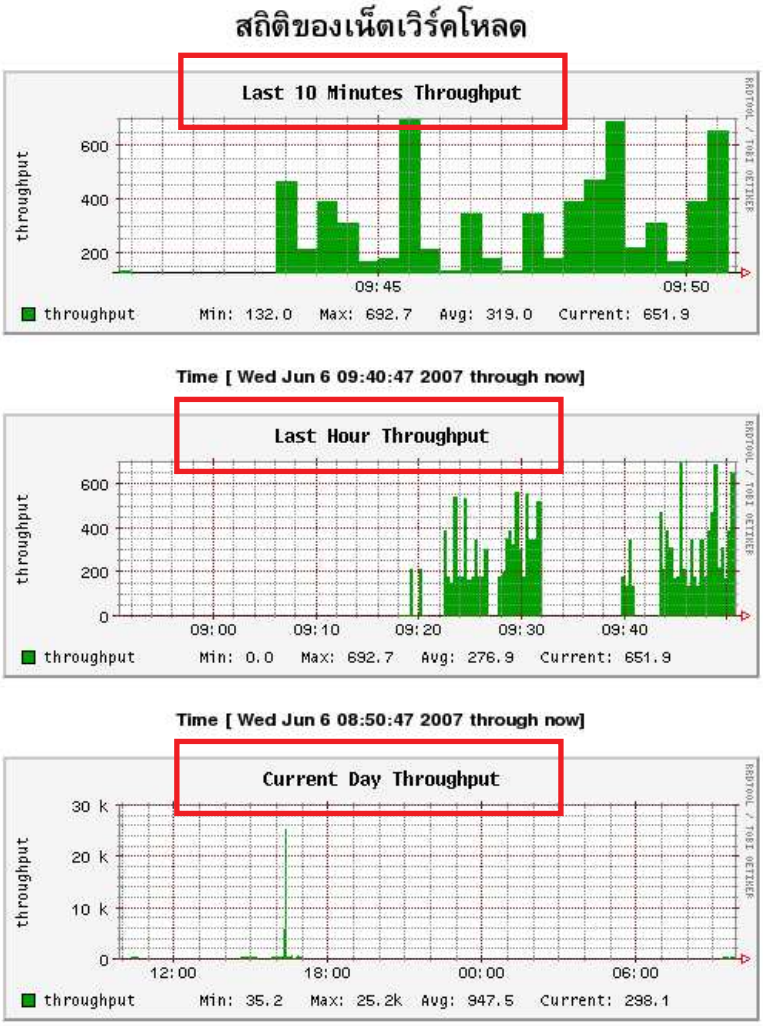
2.4. <u>สถิติการใช้งานเครือข่าย</u>

หากต้องการทราบอัตราการการรับส่งข้อมูลของเครือข่ายทั้งหมด (Throughput) ตามช่วงของเวลา เช่น

- อัตราการรับส่งข้อมูลของทั้งเครือข่ายใน 10 นาทีที่แล้ว
- อัตราการรับส่งข้อมูลของทั้งเครือข่ายใน 1 ชั่วโมงที่แล้ว
- อัตราการรับส่งข้อมูลของทั้งเครือข่ายของวันที่แล้ว
- อัตราการรับส่งข้อมูลของทั้งเครือข่ายของเดือนที่แล้ว

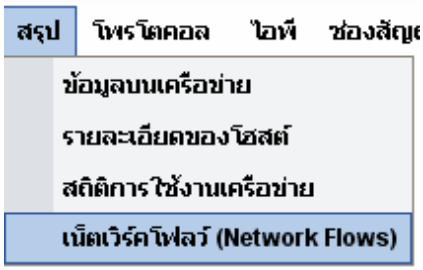
ในรูปแบบของกราฟรูปภาพ สามารถเข้าไปได้ที่เมนู ***สรุป → สถิติการใช้งานเครือข่าย*** ดังรูป

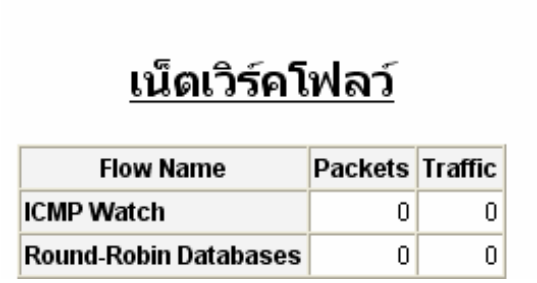




2.5. <u>เน็ตเวิร์คโฟลว์ (Network Flow)</u>

หากต้องการทราบปริมาณข้อมูลบนเครือข่ายของแต่ละปลั๊กอิน สามารถเข้าไปดูได้ที่เมนู ***สรุป → เน็ตเวิร์คโฟลว์ (Network Flows)*** ดังรูป



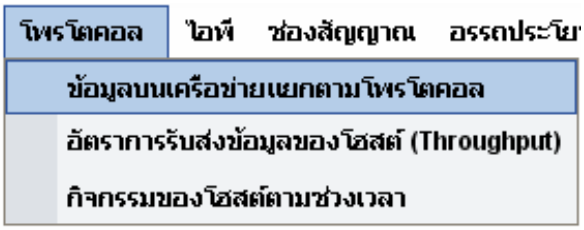


2.6. <u>ปริมาณการใช้งานเครือข่ายของแต่ละผู้ใช้ แยกตามโพรโตคอล</u>

หากต้องการทราบว่าแต่ละผู้ใช้มีการใช้งานเครือข่ายเป็นปริมาณเท่าไร โดยแยกตามโพรโตคอล ดังต่อไปนี้

- TCP
- UDP
- ICMP/ICMPv6
- DLC
- IPX
- Decnet
- ARP/RARP
- AppleTalk
- NetBios
- OSI
- IPv6
- STP
- IPS

สามารถเข้าไปดูได้ที่เมนู ***โพรโตคอล → ข้อมูลบนเครือข่ายแยกตามโพรโตคอล*** ดังรูป



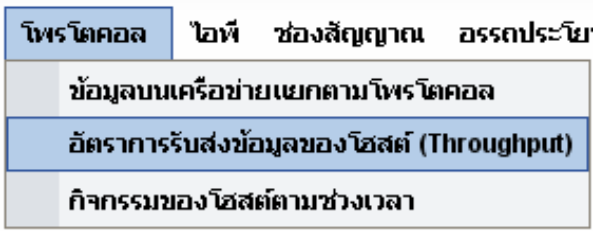
ข้อมูลบนเครือข่ายแยกตามโพรโตคอล: เฉพาะโฮสต์ภายใน(รับ-ส่ง)

หมด] [ภายใน] [ภายนอก] ข้อมูล : [ทั้งหมด

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI	IPv6	STP	IPSEC	OSPF	IGMP	Other
192.168.99.103		570.6 MB	99.6 %	570.6 MB	27.2 KB	0	0	0	0	0	138	0	0	0	0	0	0	0	0	0
192.168.99.104		958.6 KB	0.2 %	954.4 KB	4.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.99.96		403.0 KB	0.1 %	364.0 KB	38.3 KB	0	0	0	0	0	750	0	0	0	0	0	0	0	0	0
192.168.99.105		385.7 KB	0.1 %	384.0 KB	1.0 KB	0	0	0	0	0	682	0	0	0	0	0	0	0	0	0
192.168.99.98		363.3 KB	0.1 %	336.5 KB	26.1 KB	0	0	0	0	0	138	0	0	0	0	0	0	0	600	0
192.168.99.92		178.3 KB	0.0 %	149.2 KB	17.4 KB	490	0	0	0	0	184	0	0	0	0	0	0	0	0	0
192.168.99.89		90.1 KB	0.0 %	85.5 KB	4.5 KB	0	0	0	0	0	184	0	0	0	0	0	0	0	0	0
192.168.99.88		30.4 KB	0.0 %	30.2 KB	0	0	0	0	0	0	184	0	0	0	0	0	0	0	0	0
192.168.99.1		6.4 KB	0.0 %	0	0	0	0	0	0	0	1.1 KB	0	0	0	0	0	0	0	0	12.0 KB
cisco cdpd/vtp:cc:cc:cc		5.4 KB	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5.4 KB
192.168.99.91		2.8 KB	0.0 %	0	2.7 KB	0	0	0	0	0	92	0	0	0	0	0	0	0	0	0

2.7. <u>อัตราการรับส่งข้อมูลของแต่ละโฮสต์</u>

หากต้องการทราบว่าปัจจุบันแต่ละผู้ใช้มีการรับส่งข้อมูลด้วยความเร็วเท่าไร (Current Throughput), เคยมีความเร็วในการรับส่งข้อมูลบนเครือข่ายสูงสุดเท่าไร (Peak Throughput) และค่าเฉลี่ยโดยรวมของความเร็วในการส่งข้อมูลเป็นเท่าไร (Average Throughput) สามารถเข้าไปที่เมนู ***โพรโตคอล → อัตราการรับส่งข้อมูลของโฮสต์ (Throughput)*** ดังรูป

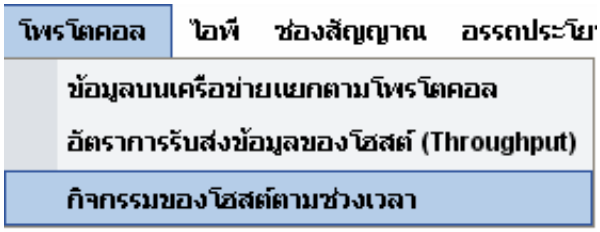


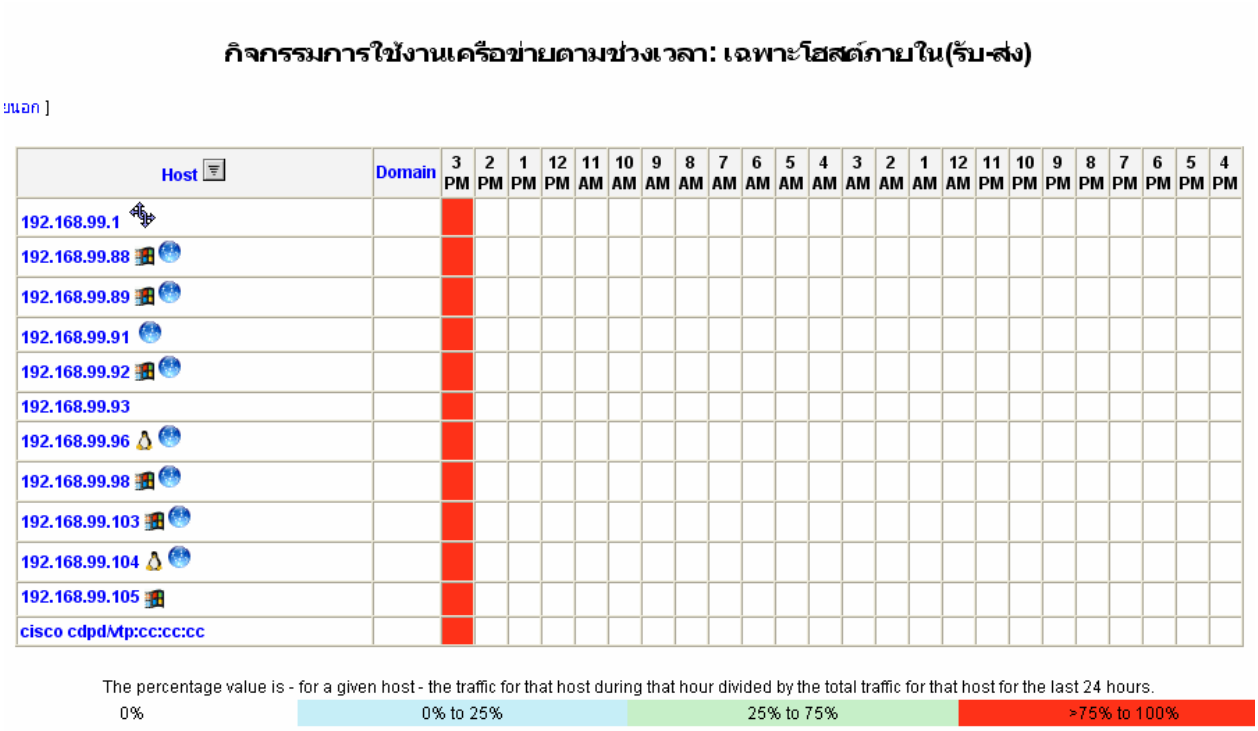
อัตราการรับส่งข้อมูล: เฉพาะโฮสต์ภายใน(รับ-ส่ง)

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
192.168.99.1		66.3 bps	66.3 bps	140.1 bps	0.1 Pkts/sec	0.1 Pkts/sec	0.1 Pkts/sec
192.168.99.88		2.4 Kbps	509.3 bps	2.7 Kbps	1.4 Pkts/sec	0.3 Pkts/sec	1.4 Pkts/sec
192.168.99.89		1.9 Kbps	938.2 bps	18.3 Kbps	1.1 Pkts/sec	0.4 Pkts/sec	5.6 Pkts/sec
192.168.99.91		60.5 bps	32.4 bps	196.9 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec
192.168.99.92		224.3 bps	14.2 Kbps	404.3 Kbps	0.5 Pkts/sec	2.9 Pkts/sec	65.7 Pkts/sec
192.168.99.96		847.6 bps	3.7 Kbps	15.6 Kbps	0.4 Pkts/sec	1.6 Pkts/sec	7.1 Pkts/sec
192.168.99.98		1.6 Kbps	3.3 Kbps	28.8 Kbps	0.6 Pkts/sec	1.4 Pkts/sec	9.8 Pkts/sec
192.168.99.103		6.4 Mbps	5.8 Mbps	13.3 Mbps	895.7 Pkts/sec	833.9 Pkts/sec	1842.0 Pkts/sec
192.168.99.104		6.4 Kbps	10.1 Kbps	215.2 Kbps	1.7 Pkts/sec	1.8 Pkts/sec	30.3 Pkts/sec
192.168.99.105		1.0 Kbps	3.6 Kbps	13.7 Kbps	0.5 Pkts/sec	1.5 Pkts/sec	5.4 Pkts/sec
cisco cdp/vtp:cc:cc:cc		56.4 bps	54.6 bps	116.7 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec

2.8. <u>กิจกรรมของโฮสต์ตามช่วงเวลา</u>

หากต้องการทราบว่า ภายใน 24 ชั่วโมงของวัน แต่ละผู้ใช้มีการใช้งานเครือข่ายเป็นร้อยละเท่าไรของปริมาณการใช้งานทั้งหมด สามารถเข้าไปดูได้ที่เมนู ***โพรโตคอล → กิจกรรมของโฮสต์ตามช่วงเวลา*** ดังรูป



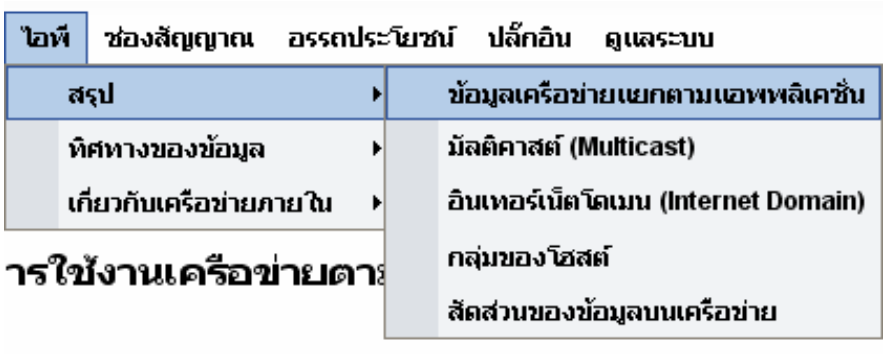


2.9. <u>ปริมาณการใช้งานเครือข่ายของแต่ละผู้ใช้ แยกตามแอพพลิเคชัน</u>

หากต้องการทราบว่าแต่ละผู้ใช้มีการใช้งานแต่ละแอพลิเคชันเป็นปริมาณเท่าไร เช่น

- แอพพลิเคชั่นจำพวกรับส่งไฟล์ข้อมูล ได้แก่ FTP
- แอพพลิเคชั่นจำพวก Web ได้แก่ HTTP
- P2P แอพพลิเคชั่น ได้แก่ Bittorent, eDonkey, Kazaa และ Gnutella
- แอพพลิเคชั่นจำพวก Chat ได้แก่ Messenger
- แอพพลิเคชั่นจำพวกรับส่งเมลล์ ได้แก่ Mail
- แอพพลิเคชั่นอื่นๆ ได้แก่ DNS, DHCP-BOOTP, Telnet, NBios-IP, SNMP, NNTP, NFS/AFS และ X11

สามารถเข้าไปดูข้อมูลได้ที่เมนู ***ไอพี → สรุป → ข้อมูลเครือข่ายแยกตามแอพพลิเคชั่น*** ดังรูป



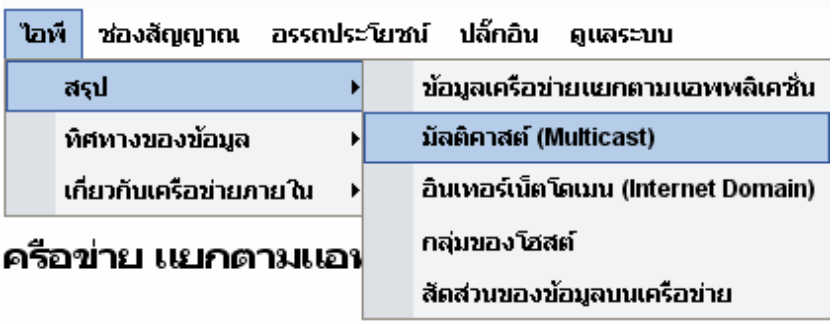
ข้อมูลบนเครือข่าย แยกตามแอพพลิเคชัน: เฉพาะโฮสต์ภายใน(รับ-ส่ง)

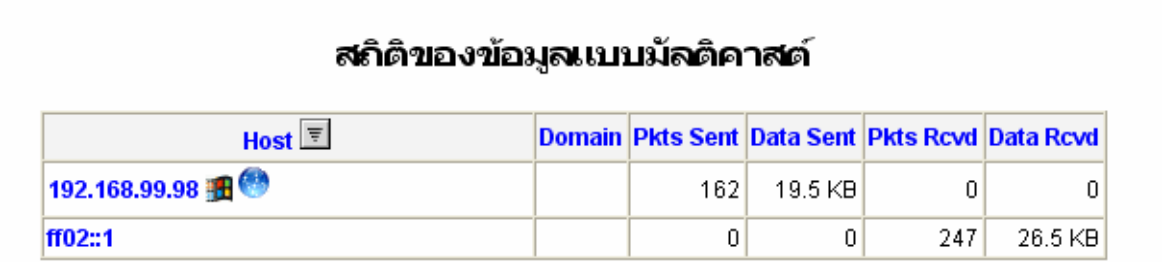
โฮสต์ : [ทั้งหมด] [ภายใน] [ภายนอก]

Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	VoIP	X11	SSH
192.168.99.103		932.8 MB	99.4 %	4.9 KB	18.5 MB	21.6 KB	0	3.9 KB	0	0	0	0	0	0	0	488
192.168.99.92		2.0 MB	0.2 %	0	1.5 MB	3.1 KB	0	486	0	0	0	0	0	0	0	51.9 KB
192.168.99.104		1.2 MB	0.1 %	5.7 KB	337.8 KB	15.0 KB	0	0	0	0	0	0	0	0	0	0
192.168.99.98		922.5 KB	0.1 %	0	726.2 KB	11.1 KB	0	500	0	0	0	0	0	0	0	0
192.168.99.96		444.3 KB	0.0 %	0	0	53.1 KB	0	0	0	0	0	0	0	0	0	0
192.168.99.105		424.0 KB	0.0 %	0	0	0	0	1.8 KB	0	0	0	0	0	0	0	0
192.168.99.89		112.7 KB	0.0 %	0	92.5 KB	5.6 KB	0	486	0	0	0	0	0	0	0	2.3 KB
192.168.99.88		84.5 KB	0.0 %	0	30.7 KB	378	0	0	0	0	0	0	0	0	0	10.8 KB
192.168.99.91		4.5 KB	0.0 %	0	0	538	0	4.0 KB	0	0	0	0	0	0	0	0
192.168.99.93		120	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	120
192.168.99.1		0	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0

2.10.<u>ข้อมูลเกี่ยวกับมัลติคาสต์ (Multicast)</u>

หากต้องการทราบรายละเอียดเกี่ยวกับข้อมูลบนเครือข่ายประเภทมัลติคาสต์ (Multicast Traffic) ว่ามีการรับและส่งเป็นปริมาณเท่าใด สามารถเข้าไปดูได้ที่เมนู ***ไอพี → สรุป → มัลติคาสต์***





สถิติของข้อมูลแบบมัลติคาสต์

Host	Domain	Pkts Sent	Data Sent	Pkts Rcvd	Data Rcvd
192.168.99.98		162	19.5 KB	0	0
ff02::1		0	0	247	26.5 KB

2.11.<u>รายละเอียดของแต่ละโดเมน (Internet Domain)</u>

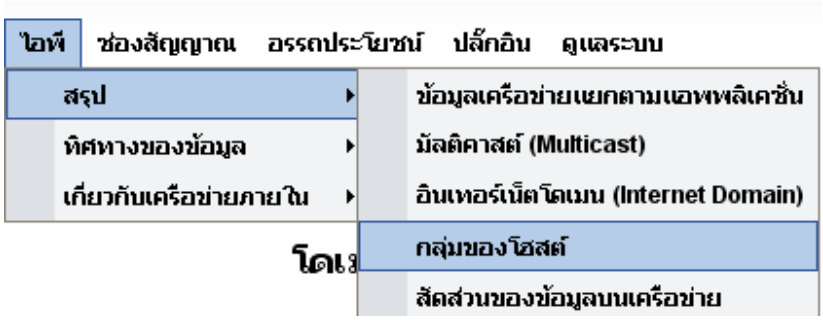
หากต้องการทราบว่าแต่ละโดเมน หรือแต่ละเครื่องแม่ข่ายมีการรับส่งข้อมูลเป็นปริมาณเท่าไร โดยแยกตามโพรโตคอล TCP, UDP, ICMP, และ ICMPv6 สามารถเข้าไปดูได้ที่เมนู ***ไอพี → สรุป → อินเตอร์เน็ตโดเมน (Internet Domain)*** ดังรูป

โดเมนทั้งหมด

Name	Domain	TCP/IP								ICMP			
		Total				TCP		UDP		IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
200-68.tampabay.res.rr.com		344	0.0%	1.8 KB	0.0%	0	0	344	1.8 KB	0	0	0	0
168.112.2o7.net		1.7 KB	0.0%	3.0 KB	0.0%	1.7 KB	3.0 KB	0	0	0	0	0	0
57.128.215.sta.isp-thailand.com		400	0.0%	806	0.0%	400	806	0	0	0	0	0	0
57.128.216.sta.isp-thailand.com		316.5 KB	0.0%	30.9 KB	0.2%	316.5 KB	30.9 KB	0	0	0	0	0	0
57.128.217.sta.isp-thailand.com		1.0 KB	0.0%	1.8 KB	0.0%	1.0 KB	1.8 KB	0	0	0	0	0	0
inter.net.th		111.0 KB	0.0%	17.1 KB	0.1%	111.0 KB	17.1 KB	0	0	0	0	0	0
static.asianet.co.th		32.7 KB	0.0%	9.1 KB	0.0%	32.7 KB	9.1 KB	0	0	0	0	0	0
red-83-50-38.dynamicip.rima-tde.net		0	0.0%	4.3 KB	0.0%	0	0	0	4.3 KB	0	0	0	0
120.238.221.broad.tj.tj.dynamic.163data.com.cn		0	0.0%	4.4 KB	0.0%	0	0	0	4.4 KB	0	0	0	0
cable.ubr12.newt.blueyonder.co.uk		0	0.0%	143	0.0%	0	0	0	143	0	0	0	0
vip.scd.yahoo.com		895	0.0%	713	0.0%	895	713	0	0	0	0	0	0
123.48-219.tttmaxnet.com		1.5 KB	0.0%	1.7 KB	0.0%	1.5 KB	1.7 KB	0	0	0	0	0	0
data.vip.sp1.yahoo.com		1.8 KB	0.0%	2.2 KB	0.0%	1.8 KB	2.2 KB	0	0	0	0	0	0
phx.gbl		97.0 KB	0.0%	28.7 KB	0.1%	97.0 KB	28.7 KB	0	0	0	0	0	0
cnet.com		1.1 MB	0.2%	77.4 KB	0.4%	1.1 MB	77.4 KB	0	0	0	0	0	0
google.com		1.4 MB	0.2%	85.7 KB	0.4%	1.4 MB	85.7 KB	0	0	0	0	0	0
siamidc.com		62	0.0%	62	0.0%	62	62	0	0	0	0	0	0
69.59.170.156		6.7 KB	0.0%	5.9 KB	0.0%	6.7 KB	5.9 KB	0	0	0	0	0	0
client.logicworks.net		2.3 KB	0.0%	1.6 KB	0.0%	2.3 KB	1.6 KB	0	0	0	0	0	0
uni-klu.ac.at		69.4 KB	0.0%	5.5 KB	0.0%	69.4 KB	5.5 KB	0	0	0	0	0	0
gits.net.th		2.4 KB	0.0%	3.0 KB	0.0%	2.4 KB	3.0 KB	0	0	0	0	0	0
seed.net.tw		120	0.0%	120	0.0%	120	120	0	0	0	0	0	0
ce.kmitl.ac.th		0	0.0%	186	0.0%	0	186	0	0	0	0	0	0

2.12.<u>กลุ่มของโฮสต์ (Host Cluster)</u>

หากต้องการทราบพฤติกรรมการคุยกันของโฮสต์ สามารถเข้าไปดูได้ที่เมนู ***ไอพี → สรุป → กลุ่มของโฮสต์*** ดังรูป

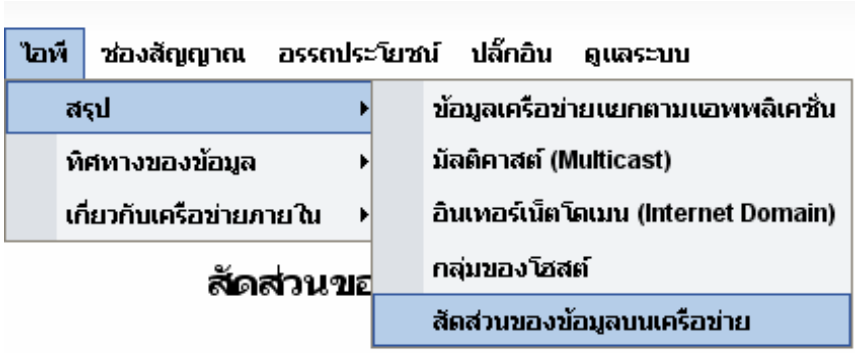


2.13.<u>สัดส่วนของข้อมูลบนเครือข่าย</u>

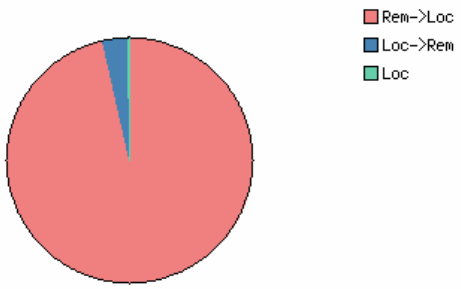
หากต้องการทราบปริมาณข้อมูลบนเครือข่าย โดยคิดเป็นสัดส่วนของปริมาณข้อมูลบนเครือข่ายทั้งหมด เช่น

- สัดส่วนระหว่างการคุยกันระหว่างเครือข่ายภายนอก->เครือข่ายภายใน, เครือข่ายภายใน->เครือข่ายภายนอก และ การคุยกันภายในเครือข่าย เป็นสัดส่วนเท่าไร
- สัดส่วนระหว่างโพรโตคอล TCP กับ UDP ของการคุยกันระหว่างเครือข่ายภายนอก->เครือข่ายภายใน, เครือข่ายภายใน->เครือข่ายภายนอก และภายในเครือข่ายด้วยกันเองเป็นสัดส่วนเท่าไร

ข้อมูลเหล่านี้ สามารถเข้าไปดูได้ที่เมนู ***ไอพี → สรุป → สัดส่วนของข้อมูลบนเครือข่าย***



สัดส่วนของโพรโตคอล IP



ข้อมูลภายในเครือข่าย

IP Protocol	Data	Percentage
TCP vs. UDP	510.1 KB	TCP 96.8 % / UDP 3.2 %

TCP/UDP Protocol	Data	Percentage	
NBios-IP	16.1 KB	3.2%	
Messenger	4.9 KB	0%	
Other TCP/UDP-based Protocols	489.1 KB	95.9%	

ข้อมูลภายนอกเครือข่าย->ภายในเครือข่าย

IP Protocol	Data	Percentage
TCP vs. UDP	1.4 GB	TCP 100 % / UDP 0 %

TCP/UDP Protocol	Data	Percentage	
FTP	11.7 KB	0%	
HTTP	25.1 MB	1.7%	
DNS	105.3 KB	0%	
NFS/AFS	0.2 KB	0%	
SSH	60.5 KB	0%	
eDonkey	46.0 MB	3.1%	
BitTorrent	1.5 KB	0%	
Messenger	156.9 KB	0%	
Other TCP/UDP-based Protocols	1.4 GB	95.1%	

ข้อมูลภายในเครือข่าย->ภายนอกเครือข่าย

IP Protocol	Data	Percentage
TCP vs. UDP	52.0 MB	TCP 100 % / UDP 0 %

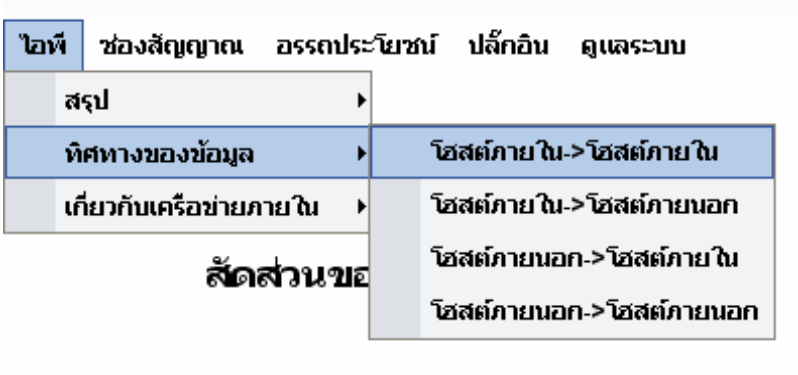
TCP/UDP Protocol	Data	Percentage	
FTP	11.2 KB	0%	
HTTP	1.4 MB	2.6%	
DNS	37.1 KB	0%	
Mail	0.2 KB	0%	
NFS/AFS	0.2 KB	0%	
SSH	43.4 KB	0%	
eDonkey	1.3 MB	2.5%	
BitTorrent	1.7 KB	0%	
Messenger	62.0 KB	0%	
Other IP-based Protocols	49.2 MB	94.5%	

2.14.<u>ทิศทางของข้อมูลบนเครือข่าย</u>

หากต้องการทราบโฮสต์มีการรับส่งข้อมูลไปในทิศทางใด เป็นปริมาณเท่าไร เช่น หากต้องการทราบว่า

- โฮสต์ภายในเครือข่ายมีการรับส่งข้อมูลไปยังโฮสต์ภายในด้วยกันเองเป็นปริมาณเท่าไร
- โฮสต์ภายในเครือข่ายมีการรับส่งข้อมูลไปยังโฮสต์ภายนอก (เครือข่ายภายนอก) เป็นปริมาณเท่าไร

ข้อมูลเหล่านี้ สามารถเข้าไปดูได้ที่เมนู ***ไอพี → ทิศทางของข้อมูล*** ดังรูป



โฮสต์ภายใน->โฮสต์ภายใน

Host	IP Address	Data Sent		Data Rcvd	
192.168.99.89	192.168.99.89	2.1 KB	0.4 %	0	0.0 %
192.168.99.91	192.168.99.91	5.0 KB	0.9 %	0	0.0 %
192.168.99.92	192.168.99.92	729	0.1 %	0	0.0 %
192.168.99.93	192.168.99.93	1.6 KB	0.3 %	0	0.0 %
192.168.99.96	192.168.99.96	428.4 KB	78.5 %	97.1 KB	18.5 %
192.168.99.98	192.168.99.98	1.2 KB	0.2 %	0	0.0 %
192.168.99.103	192.168.99.103	5.8 KB	1.1 %	0	0.0 %
192.168.99.105	192.168.99.105	101.0 KB	18.5 %	428.4 KB	81.5 %

Total Traffic	Data Sent	Data Rcvd	Used Bandwidth
535.7 KB	545.9 KB	525.5 KB	2.1 Kbps

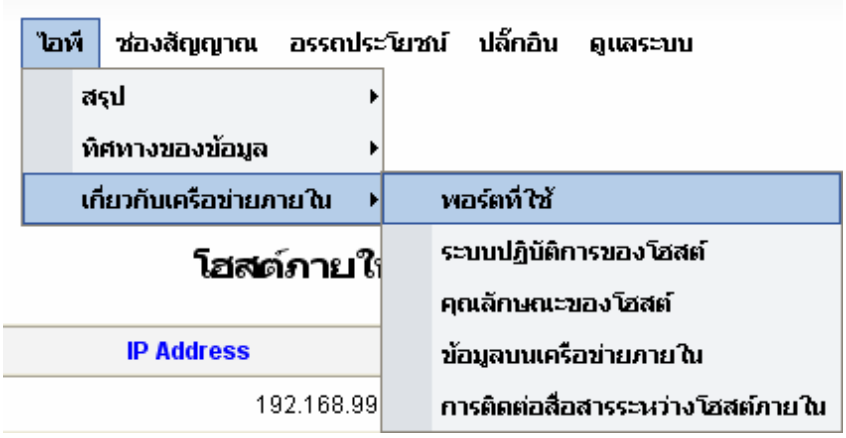
โฮสต์ภายใน->โฮสต์ภายนอก

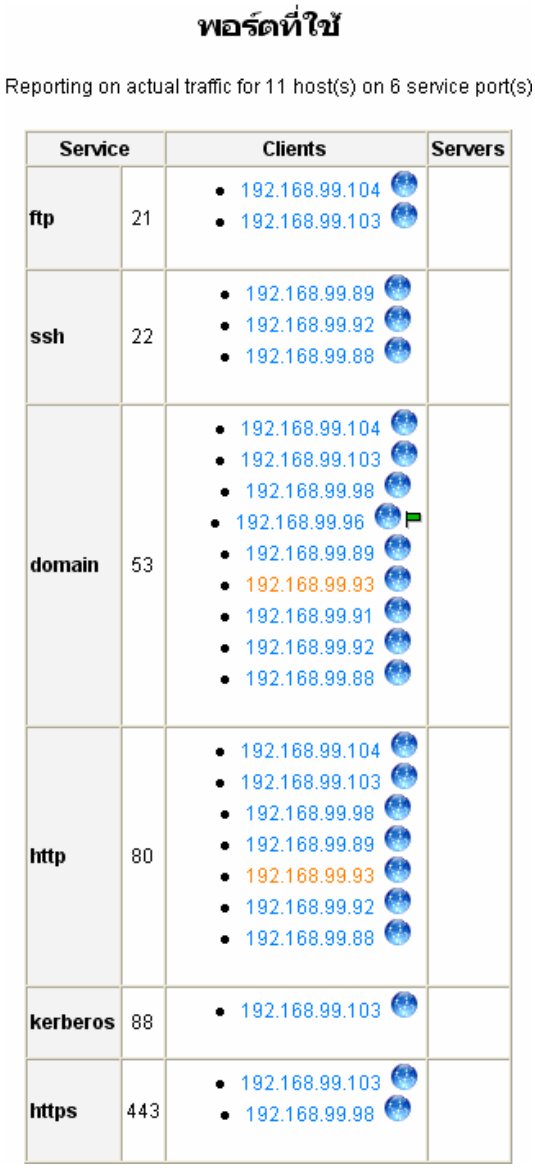
Host	IP Address	Data Sent		Data Rcvd	
192.168.99.88	192.168.99.88	209.4 KB	0.3 %	914.4 KB	0.1 %
192.168.99.89	192.168.99.89	50.5 KB	0.1 %	461.5 KB	0.0 %
192.168.99.91	192.168.99.91	264	0.0 %	274	0.0 %
192.168.99.92	192.168.99.92	218.4 KB	0.3 %	1.8 MB	0.1 %
192.168.99.93	192.168.99.93	105.1 KB	0.2 %	1.1 MB	0.1 %
192.168.99.96	192.168.99.96	23.4 KB	0.0 %	57.4 KB	0.0 %
192.168.99.98	192.168.99.98	197.0 KB	0.3 %	795.1 KB	0.0 %
192.168.99.103	192.168.99.103	60.2 MB	98.4 %	1.6 GB	99.5 %
192.168.99.104	192.168.99.104	194.2 KB	0.3 %	2.7 MB	0.2 %
192.168.99.105	192.168.99.105	9.1 KB	0.0 %	39.5 KB	0.0 %

Total Traffic	Data Sent	Data Rcvd	Used Bandwidth
1.7 GB	61.2 MB	1.6 GB	6.5 Mbps

2.15.<u>ข้อมูลการใช้บริการเครือข่ายของผู้ใช้</u>

หากต้องการทราบว่าปัจจุบันมีผู้ใช้ภายในเครือข่ายใช้บริการแอพพลิเคชัน หรือใช้บริการอะไรอยู่บ้าง เช่น มีผู้ใช้คนใดมีการใช้บริการเว็บ หรืออีเมลล์อยู่ เป็นต้น สามารถเข้าไปดูได้ที่เมนู ***ไอพี → เกี่ยวกับเครือข่ายภายใน → พอร์ตที่ใช้*** ดังรูป





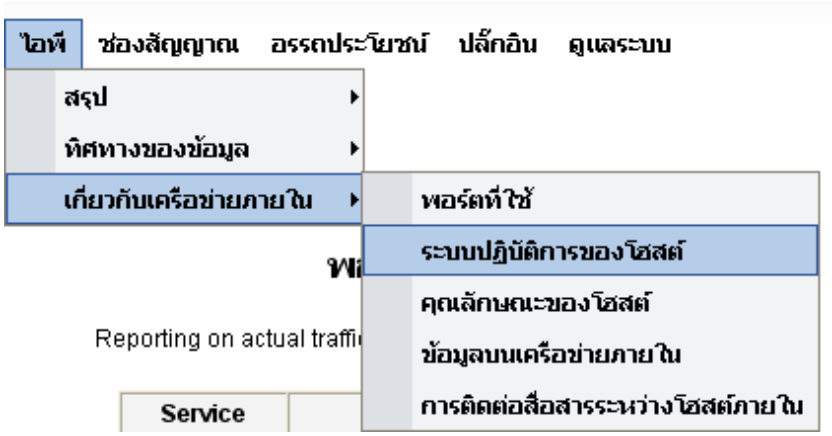
พอร์ตที่ใช้

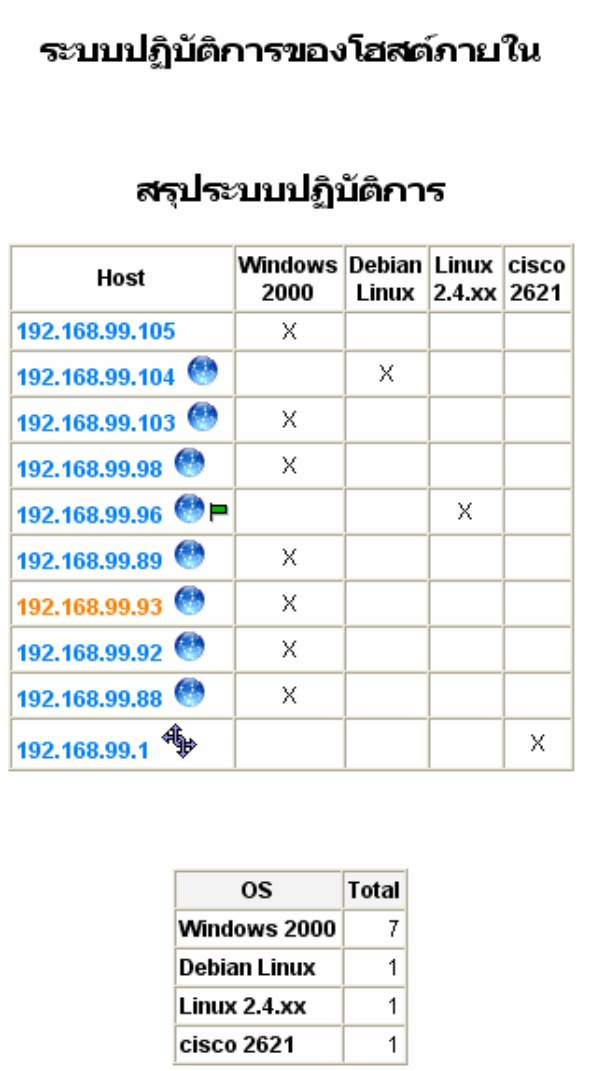
Reporting on actual traffic for 11 host(s) on 6 service port(s)

Service		Clients	Servers
ftp	21	• 192.168.99.104 • 192.168.99.103	
ssh	22	• 192.168.99.89 • 192.168.99.92 • 192.168.99.88	
domain	53	• 192.168.99.104 • 192.168.99.103 • 192.168.99.98 • 192.168.99.96 • 192.168.99.89 • 192.168.99.93 • 192.168.99.91 • 192.168.99.92 • 192.168.99.88	
http	80	• 192.168.99.104 • 192.168.99.103 • 192.168.99.98 • 192.168.99.89 • 192.168.99.93 • 192.168.99.92 • 192.168.99.88	
kerberos	88	• 192.168.99.103	
https	443	• 192.168.99.103 • 192.168.99.98	

2.16. <u>ระบบปฏิบัติการของแต่ละโฮสต์</u>

หากต้องการทราบว่าแต่ละโฮสต์ในเครือข่ายมีระบบปฏิบัติการ (Operating System) อะไร เช่น ระบบปฏิบัติการ Window หรือ Linux สามารถเข้าไปดูได้ที่เมนู ***ไอพี → เกี่ยวกับเครือข่ายภายใน → ระบบปฏิบัติการของโฮสต์*** ดังรูป





ระบบปฏิบัติการของโฮสต์ภายใน

สรุประบบปฏิบัติการ

Host	Windows 2000	Debian Linux	Linux 2.4.xx	cisco 2621
192.168.99.105	X			
192.168.99.104		X		
192.168.99.103	X			
192.168.99.98	X			
192.168.99.96			X	
192.168.99.89	X			
192.168.99.93	X			
192.168.99.92	X			
192.168.99.88	X			
192.168.99.1				X

OS	Total
Windows 2000	7
Debian Linux	1
Linux 2.4.xx	1
cisco 2621	1

2.17.<u>บทบาทของแต่ละโฮสต์</u>

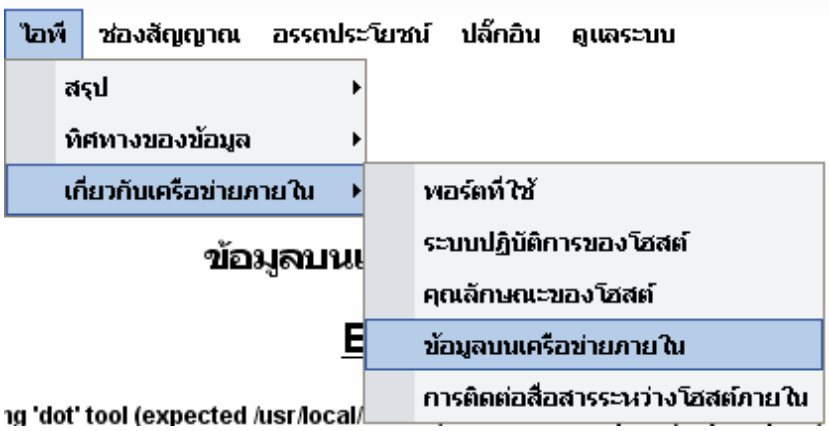
หากต้องการทราบว่าแต่ละโฮสต์ในเครือข่ายมีบทบาทหรือทำหน้าที่อะไรบนเครือข่าย เช่น ทำหน้าที่เป็น Gateway, Printer, DHCP server, DHCP client หรืออื่นๆ สามารถเข้าไปดูได้ที่เมนู ***ไอพี → เกี่ยวกับเครือข่ายภายใน → คุณลักษณะของโฮสต์*** ดังรูป

คุณลักษณะของโฮสต์ภายใน

Host	Unhealthy Host	L2 Switch Bridge	Gateway	VoIP Host	Printer	NTP/DNS Server	SMTP/POP/IMAP Server	Directory/FTP/HTTP Server	DHCP/WINS Server	DHCP Client	P2P
192.168.99.104						X					
192.168.99.103						X					
192.168.99.98						X					
192.168.99.96	X					X					
192.168.99.89						X					
192.168.99.93						X					
192.168.99.92						X					
192.168.99.88						X					
192.168.99.1			X								
Total	1 [9.1 %]		1		8						

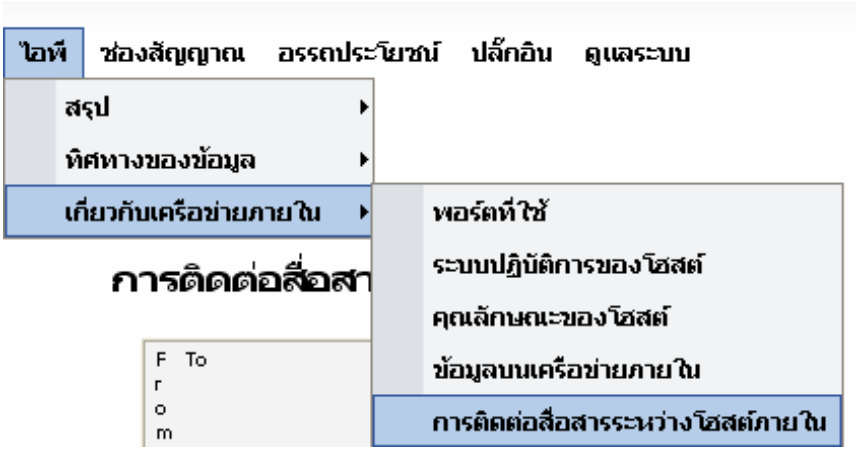
2.18.<u>ข้อมูลบนเครือข่ายภายใน (Network Map)</u>

หากต้องการทราบการการเชื่อมโยงกันของโฮสต์ภายในเครือข่าย หรือ Map สามารถเข้าไปดูได้ที่เมนู ***ไอพี → เกี่ยวกับเครือข่ายภายใน → คุณลักษณะของโฮสต์*** ดังรูป



2.19.<u>การติดต่อสื่อสารระหว่างโฮสต์ภายใน (Matrix)</u>

หากต้องการทราบว่า โฮสต์ภายในเครือข่ายมีการคุยกันเองเป็นปริมาณเท่าไร สามารถเข้าไปดูได้ที่เมนู ***ไอพี → เกี่ยวกับเครือข่ายภายใน → คุณลักษณะของโฮสต์*** ดังรูป



2.20.<u>ช่องสัญญาณไฟเบอร์แชนเนล (Fiber Channel)</u>

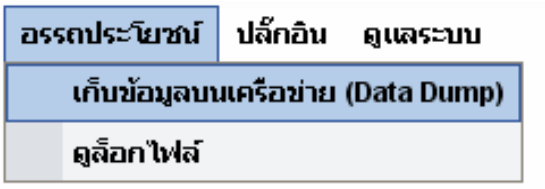
หากต้องการทราบข้อมูลรายละเอียดเกี่ยวกับข้อมูลบนช่องสัญญาณไฟเบอร์แชนเนล (Fiber Channel) เช่น ต้องการทราบ

- ปริมาณข้อมูลบนเครือข่ายบนช่องสัญญาณไฟเบอร์แชนเนล
- อัตราการรับส่งข้อมูลบนเครือข่าย (Throughput) บนไฟเบอร์แชนเนล
- กิจกรรมบนช่องสัญญาณไฟเบอร์แชนเนล
- รายละเอียดของโฮสต์บนไฟเบอร์แชนเนล

ข้อมูลเหล่านี้สามารถเข้าไปดูได้ที่เมนู ***ช่องสัญญาณ → ไฟเบอร์แชนเนล (Fiber Channel)*** ดังรูป

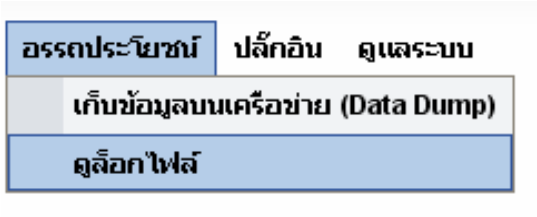
2.21.<u>เก็บข้อมูลบนเครือข่าย (Data Dump)</u>

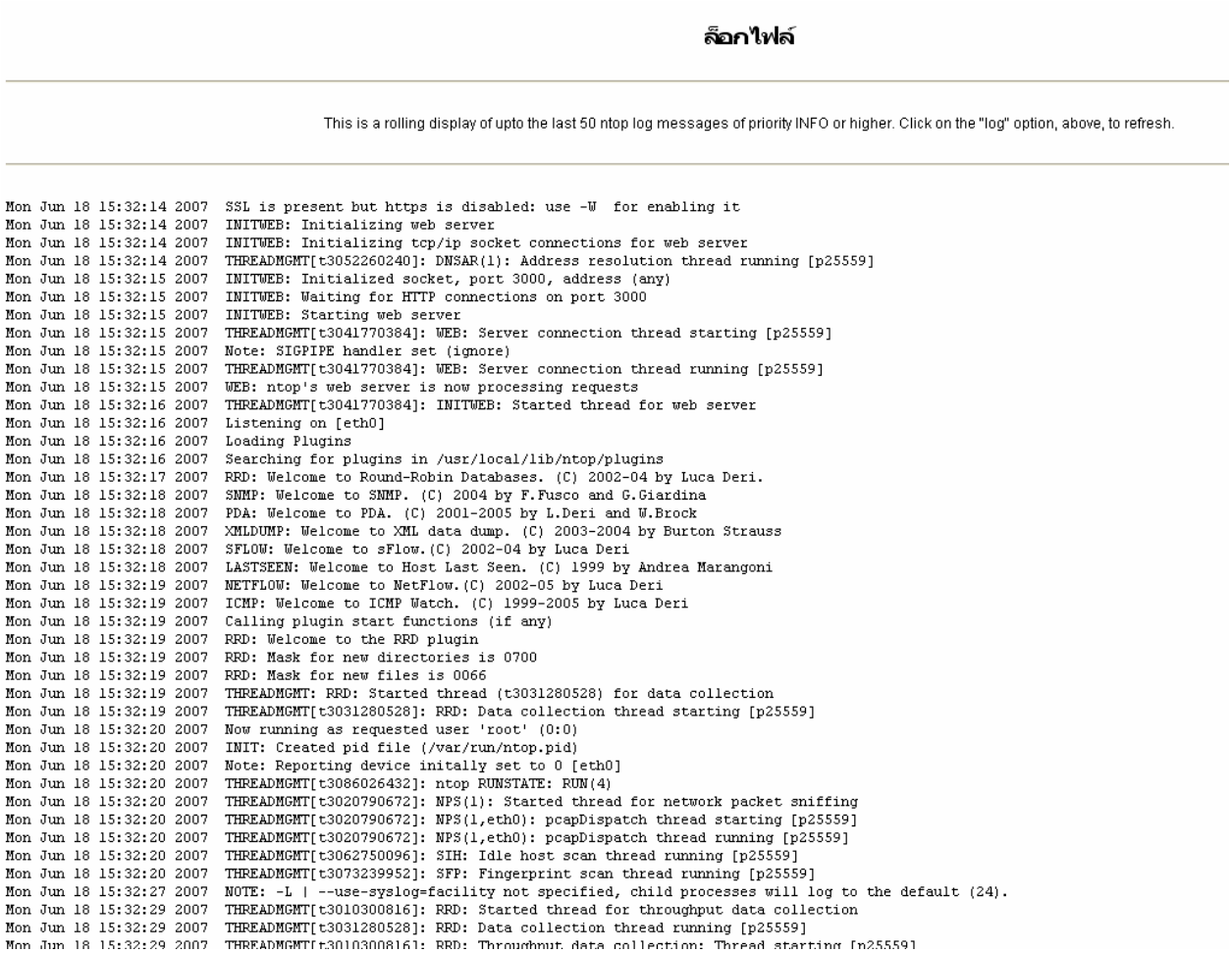
หากต้องการเก็บข้อมูลบนเครือข่ายในรูปแบบต่างๆ เช่น รูปแบบตัวอักษร (Text format) หรือในรูปแบบ XML (XML format) สามารถเข้าไปได้ที่เมนู ***อรรถประโยชน์ → เก็บข้อมูลบนเครือข่าย (Data Dump)*** ดังรูป เมนูนี้เหมาะสำหรับบุคคลที่ต้องการนำข้อมูลจากโปรแกรม ntop ไปวิเคราะห์ต่อนอกเหนือจากที่โปรแกรม ntop ได้เตรียมไว้ให้ เช่น อาจนำไปหาโฮสต์ที่ใช้งานเครือข่ายอย่างไม่เหมาะสมตามนโยบายขององค์กร เป็นต้น โปรแกรมที่สามารถนำมาดึงข้อมูลออกจากโปรแกรม ntop ได้แก่ wget เป็นต้น



2.22.ดูล็อกไฟล์

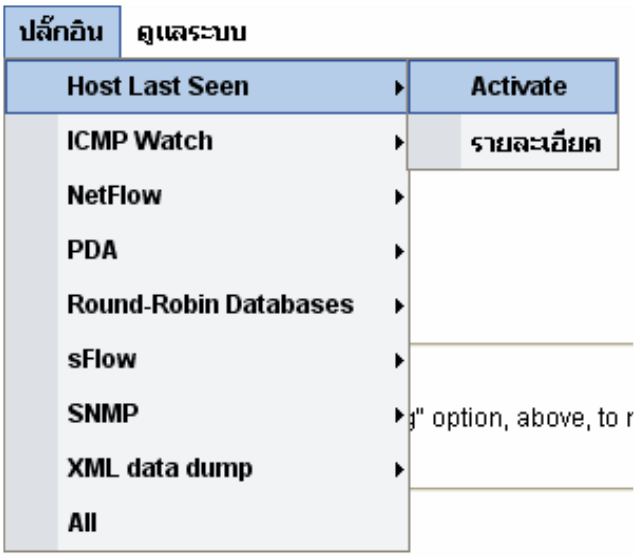
หากต้องการดูรายงานการทำงานของโปรแกรม ntop หรือล็อกไฟล์ (Log File) ของโปรแกรม ntop สามารถเข้าไปดูได้ที่เมนู ***อรรถประโยชน์ → ดูล็อกไฟล์*** ดังรูป

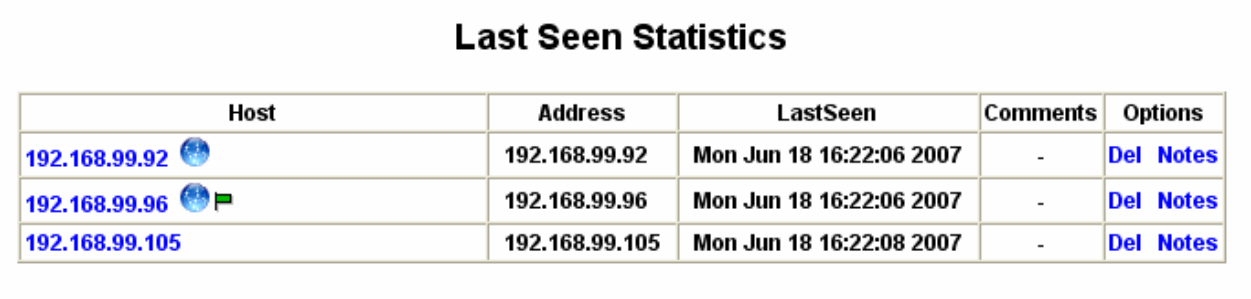




2.23.<u>โฮสต์ที่ดูล่าสุด (ปลั๊กอิน)</u>

หากต้องการทราบว่าโฮสต์ที่ดูล่าสุดมีอะไรบ้าง สามารถไป Activate ได้ที่เมนู ***ปลั๊กอิน → Host Last Seen*** ดังรูป



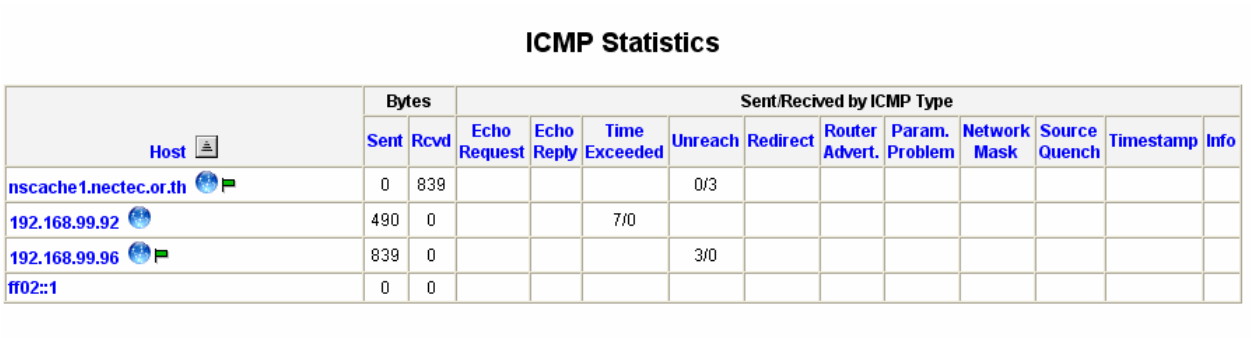


Last Seen Statistics

Host	Address	LastSeen	Comments	Options
192.168.99.92	192.168.99.92	Mon Jun 18 16:22:06 2007	-	Del Notes
192.168.99.96	192.168.99.96	Mon Jun 18 16:22:06 2007	-	Del Notes
192.168.99.105	192.168.99.105	Mon Jun 18 16:22:08 2007	-	Del Notes

2.24.<u>ปริมาณโพรโตคอล ICMP ของแต่ละโฮสต์ (ปลั๊กอิน)</u>

หากต้องการทราบรายงานข้อมูลเครือข่ายเฉพาะโพรโตคอล ICMP ของแต่ละโฮสต์ สามารถเข้าไป Activate และ ดูได้ที่เมนู ***ปลั๊กอิน → ICMP Watch*** ดังรูป



ICMP Statistics

Host	Bytes		Sent/Recived by ICMP Type										
	Sent	Rcvd	Echo Request	Echo Reply	Time Exceeded	Unreach	Redirect	Router Advert.	Param. Problem	Network Mask	Source Quench	Timestamp	Info
nscache1.nectec.or.th	0	839				0/3							
192.168.99.92	490	0			7/0								
192.168.99.96	839	0				3/0							
ff02::1	0	0											

2.25.<u>สรุปอันดับโฮสต์ที่ใช้งานเครือข่ายมากที่สุด (ปลั๊กอิน)</u>

หากต้องการ Top Five ของโฮสต์ที่ใช้งานเครือข่ายมากที่สุด สามารถเข้าไป Activate และ ดูได้ที่เมนู ***ปลั๊กอิน → PDA*** ดังรูป (เมนูนี้เหมาะสำหรับ PDA โดยเฉพาะ)

ntop for PDAs

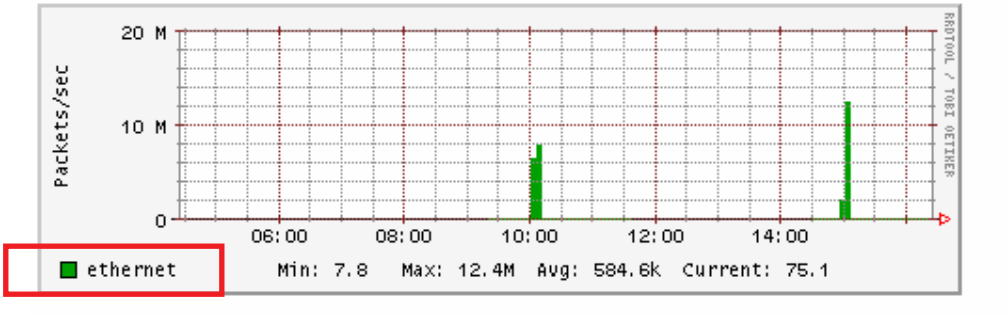
Top Sending Hosts	Total
192.168.99.103	73.3 MB
202.172.21.4	46.4 MB
203.145.117.222	44.3 MB
202.52.7.179	44.3 MB
202.52.7.143	43.3 MB

Top Receiving Hosts	Total
192.168.99.103	1.9 GB
58.9.76.254	3.4 MB
58.9.122.5	2.7 MB
58.8.99.81	2.4 MB
61.91.92.5	2.0 MB

Stats	Total
Sampling Time	50:46
Total	2,415,687
Unicast	0 [0.0%]
Broadcast	266 [0.0%]
Multicast	710 [0.0%]

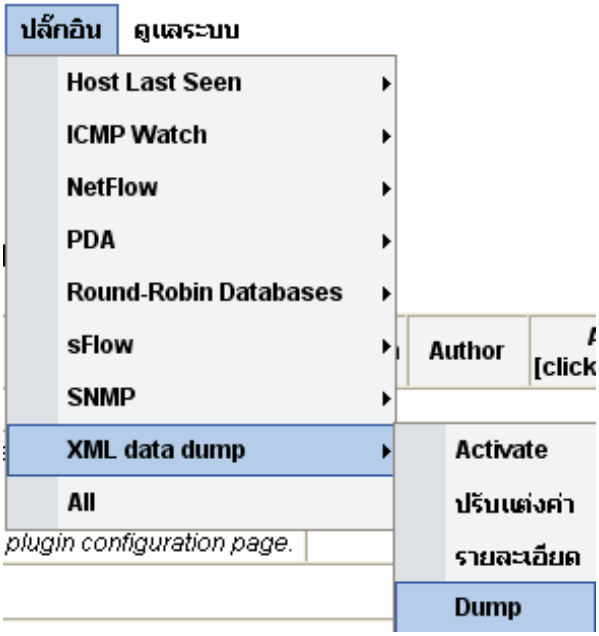
2.26.<u>สถิติต่างๆ ในรูปแบบของกราฟรูปภาพ (ปลั๊กอิน)</u>

หากต้องการสืบค้นข้อมูลเครือข่ายประเภทต่างๆ เช่น ข้อมูลเครือข่ายประเภท Ethernet Packet ใน 10 ชั่วโมงที่แล้ว ให้อยู่ในรูปแบบกราฟรูปภาพ ดังรูป สามารถเข้าไปสืบค้นข้อมูลได้ที่ ***ปลั๊กอิน → Round-Robin Databases*** ดังรูป



2.27.<u>เก็บข้อมูลในรูปแบบ XML (ปลั๊กอิน)</u>

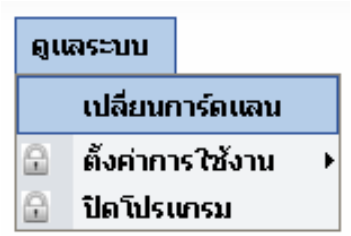
หากต้องการดึงข้อมูลจากโปรแกรม ntop ในรูปแบบ XML format ให้สามารถเข้าไปดูได้ที่เมนู ***ปลั๊กอิน → XML Data Dump*** ดังรูป

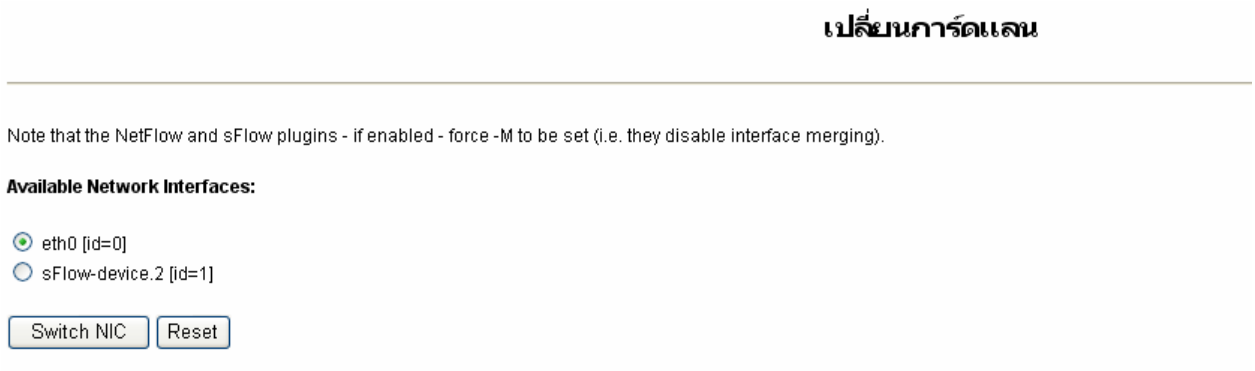


3. วิธีการปรับแต่งค่าบนโปรแกรม ntop

3.1. <u>เปลี่ยนการ์ดแลน (Network Interface Card)</u>

ในกรณีที่เครื่องที่ทำการติดตั้งโปรแกรม ntop มีการ์ดแลนมากกว่าหนึ่งอัน ผู้ดูแลระบบอาจต้องการเปลี่ยนการ์ดแลนเพื่อเปลี่ยนอุปกรณ์ในการตรวจจับข้อมูลบนเครือข่าย วิธีการเปลี่ยนการ์ดแลน สามารถเข้าไปได้ที่เมนู ***ดูแลระบบ → เปลี่ยนการ์ดแลน*** ดังรูป



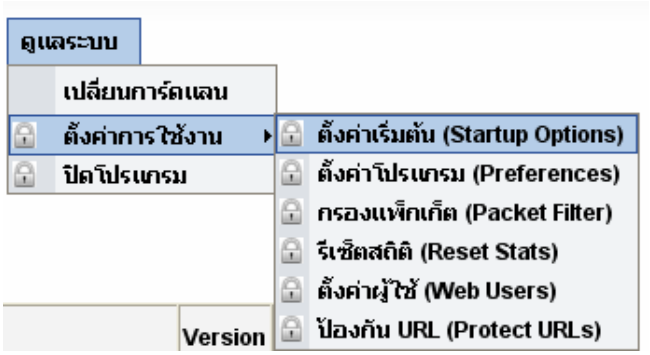


3.2. <u>ตั้งค่าพื้นฐานต่างๆ บนโปรแกรม ntop</u>

ตั้งค่าเริ่มต้นพื้นฐานของโปรแกรม ntop เช่น

- ตั้งค่าพื้นฐาน
  - เลือกการ์ดแลนที่ใช้ในการตรวจจับข้อมูลบนเครือข่าย
  - หมายเลขพอร์ตในการเรียกดูข้อมูลจากโปรแกรม ntop ผ่านทางโปรแกรม Web browser
  - โหมดของการเปิดโปรแกรม ntop
- ตั้งค่าการแสดงผล
  - อัตราการรีเฟรชของหน้าเว็ปเพจของโปรแกรม Web browser
  - ภาษาในการแสดงผล
  - จำนวนแถวในการแสดงผล
- ตั้งค่าเกี่ยวกับโพรโตคอลไอพี
  - ตรวจจับโพรโตคอลอะไรบ้าง
- ตั้งค่าเกี่ยวกับช่องสัญญาณไฟเบอร์แชนแนล
- ตั้งค่าเทคนิคชั้นสูง
  - การตั้งค่าเกี่ยวกับการจัดการ Memory
- ตั้งค่าการแก้ไขโปรแกรม ntop (Debugging)
  - ตั้งต่าเกี่ยวกัย Debugging Mode
  - ตั้งค่าเกี่ยวกับ Syslog

การตั้งค่าพื้นฐานต่างๆ สามารถเข้าไปตั้งค่าได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → ตั้งค่าเริ่มต้น (Startup Options)*** ดังรูป



ตั้งค่า ntop

[**ตั้งค่าพื้นฐาน**] [ตั้งค่าการแสดงผล] [ตั้งค่า IP] [ตั้งค่า FC] [ตั้งค่าขั้นสูง] [ตั้งค่าการแก้ไข]

Preference	Configured Value
การ์ดแลนที่ใช้ดักจับ (-i)	☑ eth0 ☐ lo
ตำแหน่งของไฟล์ที่ดักจับ (-f)	อ่านจากไฟล์ที่ดักจับ (มีลำดับเหนือกว่าการดักจับแพ็กเก็ตที่อินเทอร์เฟส)
Filter Expression ที่ดักจับ (-B)	จำกัด traffic ที่ให้ Ntop เห็น โดยไวยากรณ์ BPF
อัตราการสุ่มแพ็คเกต (-C)	0 อัตราการสุ่ม [1 = ไม่มีการสุ่ม]
เซิฟเวอร์ HTTP (-w)	3000 เซิฟเวอร์ HTTP [ที่อยู่:] พอร์ตของเว็บ Ntop
เซิฟเวอร์ HTTPS (-W)	0 เซิฟเวอร์ HTTPS [ที่อยู่:] พอร์ตของเว็บ Ntop
เปิดการทำงาน Session Handling (-z)	○ Yes ◉ No
เปิดการทำงาน Protocol Decoders (-b)	○ Yes ◉ No
Flow Spec (-F)	Flow เป็นเส้นทางของแพ็กเกตที่ดักจับได้ซึ่งสอดคล้องกับเงื่อนไขที่ระบุเอาไว้
ที่อยู่ซับเน็ตภายใน (-m)	หมายเลขซับเน็ตภายใน ที่ Ntop ใช้ในการรายงาน (ใช้ , ระหว่างแต่ละชุด). จำเป็นในการดักจับแพ็กเก็ตลงไฟล์
Sticky Hosts (-c)	○ Yes ◉ No ไม่ลบโฮสต์จากหน่วยความจำแม้โฮสต์นั้นจะไม่มีกิจกรรม
Track Local Hosts (-g)	○ Yes ◉ No ดักจับข้อมูลเฉพาะโฮสต์ภายใน
ปิดการทำงานโหมด Promiscuous (-s)	○ Yes ◉ No ไม่ตั้งค่าอินเทอร์เฟสในโหมด promiscuous
รันเป็นเซอร์วิส (-d)	○ Yes ◉ No รัน Ntop เป็นเซอร์วิส

Save Preferences | Restore Defaults

ตั้งค่า ntop

[ตั้งค่าพื้นฐาน] [**ตั้งค่าการแสดงผล**] [ตั้งค่า IP] [ตั้งค่า FC] [ตั้งค่าขั้นสูง] [ตั้งค่าการแก้ไข]

Preference	Configured Value
อัตราการรีเฟรช (-r)	120 เวลาที่ใช้หน่วง (ในหน่วย วินาที) ในการรีเฟรชหน้าเวบอัตโนมัติ
จำนวนแถวมากสุด (-e)	0 จำนวนแถวมากสุดที่ให้ Ntop แสดงในแต่ละเพจ
แสดงเมนูของ	○ IP ○ FC ◉ Both
ไม่แสดงรายละเอียดของ Invalid LUNs	○ Yes ◉ No ไม่ต้องแสดงรายละเอียดของ LUNs ที่ไม่มีอยู่
ใช้ W3C	◉ Yes ○ No สร้างเอกสาร HTML 4.01 ที่ตรงตาม (อาจไม่สมบูรณ์) มาตรฐาน w3c
ตั้งค่า Ntop สำหรับ	◉ ค่าปกติ ○ โรงเรียน ○ อินเทอร์เน็ต คาเฟ่ ○ กำหนดเอง
ภาษา	○ English ◉ ไทย

Save Preferences | Apply Preferences | Restore Defaults

ตั้งค่า ntop

[ตั้งค่าพื้นฐาน] [ตั้งค่าการแสดงผล] [**ตั้งค่า IP**] [ตั้งค่า FC] [ตั้งค่าขั้นสูง] [ตั้งค่าการแก้ไข]

Preference	Configured Value
ใช้ IPv4 หรือ IPv6 (-4/-6)	○ v4 ○ v6 ◉ ทั้งคู่
ชื่อโดเมนภายใน (-D)	[ ] ใช้เมื่อ Ntop นั้นเกิดปัญหาในการหาชื่อโดเมน หรือในกรณีของการดักจับไฟล์
ไม่ใช้ DNS (-n)	○ Yes ◉ No ข้ามการทำงานของ DNS เซิร์ฟเวอร์, ให้โชว์เฉพาะค่าตัวเลขไอพีแอดเดรสเท่านั้น
โพรโตคอล TCP/UDP ที่รายงาน (-p)	[ ] รูปแบบคือ <label>=<protocol list> [, <label>=<protocol list>] หรือชื่อของไฟล์ที่มีรูปแบบนี้
P3P-CP	[ ] คืนค่าของ p3p compact policy เฮดเดอร์
P3P-URI	[ ] คืนค่าของ p3p policyref เฮดเดอร์
โฮสต์ Mapper URL (-U)	[ ] URL ของ mapper.pl มีประโยชน์ในการหาตำแหน่งทางภูมิศาสตร์ ของโฮสต์

Save Preferences | Restore Defaults

ตั้งค่า ntop

[ตั้งค่าพื้นฐาน] [ตั้งค่าการแสดงผล] [ตั้งค่า IP] [**ตั้งค่า FC**] [ตั้งค่าขั้นสูง] [ตั้งค่าการแก้ไข]

Preference	Configured Value
ไฟล์ WWN Mapper (-N)	[ ] ตำแหน่งของไฟล์ที่จับคู่ VSAN/FC_ID กับ WWN/Alias

Save Preferences | Restore Defaults

ตั้งค่า ntop

[ตั้งค่าพื้นฐาน] [ตั้งค่าการแสดงผล] [ตั้งค่า IP] [ตั้งค่า FC] [**ตั้งค่าขั้นสูง**] [ตั้งค่าการแก้ไข]

Preference	Configured Value
จำนวน Hash สูงสุด (-x)	8192 จำกัดจำนวนโฮสต์ที่มากที่สุดที่จะเก็บในตาราง hashเพื่อจำกัดปริมาณการใช้พื้นที่ในหน่วยความจำของ Ntop
จำนวน Sessions สูงสุด (-X)	32768 จำกัดจำนวน session ที่มากที่สุดที่จะเก็บในตาราง เพื่อจำกัดปริมาณการใช้พื้นที่ในหน่วยความจำของ Ntop
ไม่รวมอินเทอร์เฟส (-M)	○ Yes ◉ No Yes = รายงานข้อมูลของทุกอินเทอร์เฟสรวมกัน (ถ้าเป็นไปได้), No = รายงานข้อมูลของแต่ละอินเทอร์เฟสแยกกัน
ไม่ลบ Session ทิ้งก่อนเวลา	○ Yes ◉ No ให้ Ntop รอเวลาให้ session จบก่อนจึงลบทิ้ง
ตั้งค่า Pcap ให้เป็น Nonblocking	○ Yes ◉ No ใช้บนระบบปฏิบัติการที่ไม่มีฟังก์ชั่น select(). **คำเตือน**: การใช้ตัวเลือกนี้จะทำให้ CPU ทำงานหนักขึ้นมาก ปรึกษาหน้าคู่มือการใช้และคำถามที่พบบ่อย
ไม่แสดงเวบหากมีปัญหา memory error	○ Yes ◉ No เปลี่ยนจากค่าปริยายที่ให้แสดงเวบที่มีเนื้อหาคงที่ในกรณีที่มีปัญหา memory error เกิดขึ้นจนกว่า ntop จะถูกปิด
ไม่เชื่อ MAC Address (-o)	○ Yes ◉ No ในบางกรณีอาจต้องใช้ตัวเลือกนี้ เช่น การทำ port/VLAN mirror
ตำแหน่งสำหรับเก็บ Pcap Log (-O)	/usr/local/var/ntop ไดเร็กทอรี่สำหรับเก็บไฟล์ที่ดักจับแพ็กเก็ต
ใช้ SSL Watchdog	○ Yes ◉ No
ไม่ใช้ SchedYield	○ Yes ◉ No

Save Preferences | Restore Defaults

ตั้งค่า ntop

[ตั้งค่าพื้นฐาน] [ตั้งค่าการแสดงผล] [ตั้งค่า IP] [ตั้งค่า FC] [ตั้งค่าขั้นสูง] [**ตั้งค่าการแก้ไข**]

Preference	Configured Value
เปิดใน debug mode (-K)	○ Yes ◉ No แสดงข้อความสำหรับ debugging Ntop
ระดับ Trace (-t)	3 ระดับของรายละเอียดข้อมูล debugging ที่ ntop แสดง
เก็บแพ็กเก็ตอื่นๆ (-j)	○ Yes ◉ No เก็บแพ็กเก็ตที่ ntop ไม่สามารถจำแนกประเภทได้
เก็บแพ็กเก็ตน่าสงสัย (-q)	○ Yes ◉ No สร้างไฟล์เพื่อเก็บแพ็กเก็ตที่น่าสงสัย
เก็บ HTTP Requests (-a)	 สั่งให้จัดเก็บ HTTP requests และระบุตำแหน่งที่เก็บ log file
ใช้ Syslog (-L)	-1 ส่งข้อความไปยัง log ของระบบแทนที่จะส่งออกที่หน้าจอ
เขียนไฟล์ที่ดักจับ (-l)	 สร้างไฟล์ที่ได้จากการดักจับแพ็กเก็ตในรูปแบบของlibpcap
ไม่ใช้ข้อมูลเพิ่มเติมของ Mutex	○ Yes ◉ No ยกเลิกการเก็บข้อมูลเพิ่มเติมเกี่ยวกับการล็อคและปลดล็อก ของ Mutex ต่างๆ ที่ Ntop ใช้

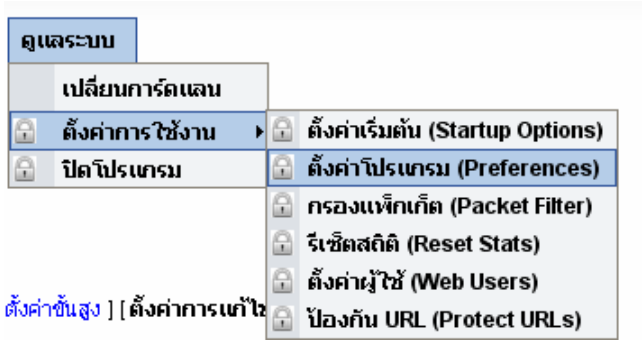
Save Preferences | Restore Defaults

3.3. <u>ตั้งค่าโปรแกรม ntop</u>

การตั้งค่าบนโปรแกรม ntop เช่น

- ค่าช่วงเวลาการเก็บข้อมูลลง Database (RRD Database)
- ค่าเกี่ยวกับปลั๊กอินต่างๆ

สามารถเข้าไปตั้งค่าได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → ตั้งค่าโปรแกรม (Preferences)*** ดังรูป

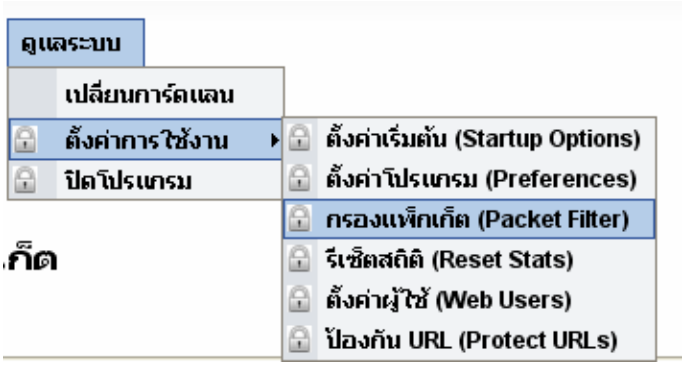


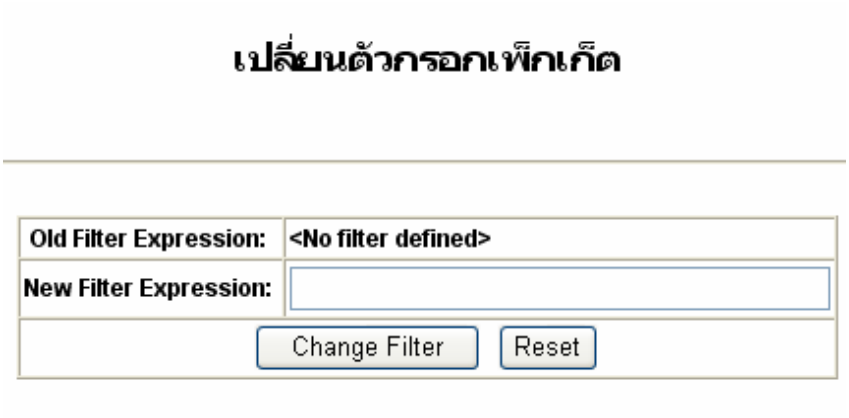
แก้ไขการตั้งค่าโปรแกรม

Preference	Configured Value	Action
rrd.dataDumpInterval	300	Set
globals.localityPolicy	0	Set
pluginStatus.Round-Robin Databases	1	Set
pluginStatus.PDA	1	Set
ntop.enableSessionHandling	0	Set
ntop.devices	eth0	Set
pluginStatus.SNMP	0	Set
sflow.2.debug	0	Set
actualReportDeviceId	0	Set
sflow.2.sflowAssumeFTP	0	Set
ntop.enablePacketDecoding	0	Set
pluginStatus.XML data dump	0	Set
ntop.printFcOrIp	3	Set
pluginStatus.NetFlow	0	Set
sflow.2.sflowInPort	0	Set
sflow.2.sflowAggregation	0	Set
rrd.dataDumpDays	90	Set
pluginStatus.ICMP Watch	1	Set
ntop.schedYield	0	Set
ntop.disableMutexExtraInfo	0	Set
ntop.maxNumLines	0	Set
sflow.2.blackList		Set
rrd.dataDumpFlows	0	Set
ntop.w3c	1	Set
ntop.disableInstantSessionPurge	0	Set

3.4. <u>ตั้งค่าการกรองแพ็คเก็ตขณะตรวจจับ</u>

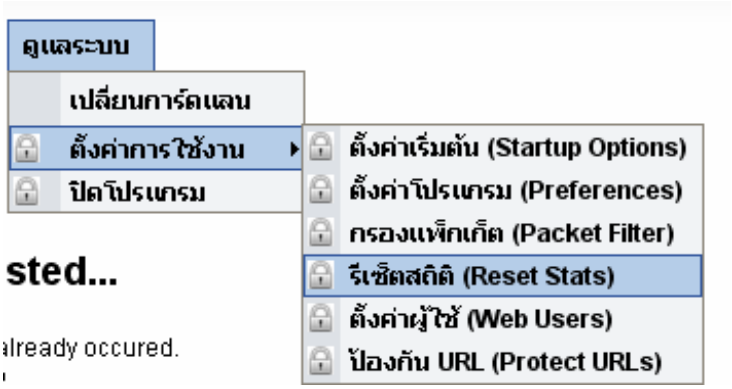
หากกรณีที่ผู้ดูแลระบบไม่ต้องการตรวจจับบางแพ็คเก็ต หรือไม่ต้องการตรวจจับบางโพรโตคอล อาจใช้เมนูนี้ช่วยในการรองแพ็คเก็ต โดยสามารถเข้าไปตั้งค่าได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → กรองแพ็คเก็ต (Packet Filter)*** ดังรูป





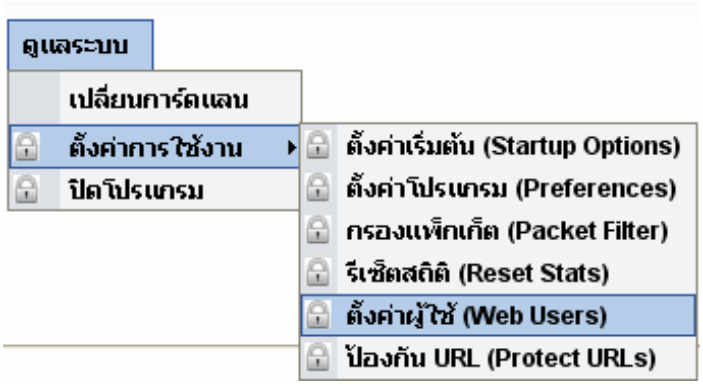
3.5. <u>รีเซ็ตสถิติ</u>

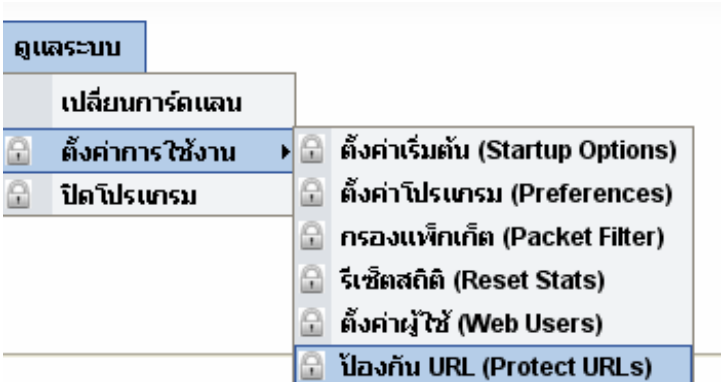
หากผู้ดูแลระบบต้องการรีเซ็ตค่าต่างๆ ที่เคยตปรับแต่งไว้ ให้เหมือนค่าเริ่มต้น สามารถเข้าไปรีเซ็ตได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → รีเซ็ตสถิติ (Reset Stats)*** ดังรูป



3.6. <u>ตั้งค่าผู้ใช้งานโปรแกรม ntop</u>

โปรแกรม ntop สามารถให้ผู้ดูแลระบบให้สิทธิ์ผู้ใช้อื่นๆ สามารถเข้าถึงโปรแกรม ntop ผ่านทางโปรแกรม Web Browser ได้ โดยผู้แลระบบสามารถเข้าไปตั้งค่าผู้ใช้ได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → ตั้งค่าผู้ใช้ (Web Users)*** ดังรูป



3.7. <u>ป้องกันหน้า Web Page</u>

หากผู้ดูแลระบบไม่ต้องการให้ผู้ใช้คนอื่นเข้าถึงบางหน้า Web Page ของโปรแกรม ntop สามารถเข้าไปป้องกันหน้า Web Page ได้ที่เมนู ***ดูแลระบบ → ตั้งค่าการใช้งาน → ป้องกัน URL (Protect URLs)*** ดังรูป