

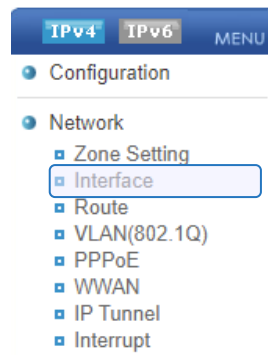


# Interfaces

หลังจากที่มีการสร้าง Zone หรือเปิด Port การใช้งานแล้วถ้าไม่มีการกำหนดค่า IP Address ให้กับ Zone จะไม่สามารถเชื่อมต่อ Port นั้นๆกับอุปกรณ์ Switch, Router ได้

ขั้นตอนการสร้าง Interfaces

1.เปิดเมนู Network / Interfaces



2.ให้เลือก Zone ที่ต้องการกำหนด IP Address



ข้อความ หรือ ชื่อ ที่แสดงเกิดจากการสร้าง Zone

Support : support.th@nit.co.th  
Sales : rung@nit.co.th  
Mobile : 081=985-6916  
Web : www.netinfotech.co.th  
Line : nit.sharetech

### 3.NU จะเปิดหน้าจอการ Setting

Enable	STATIC ▼
MTU	1500 ( 1400 ~ 1500 )

- 3.1 ที่ Enable จะมีเมนูให้เลือก OFF, STATIC, DHCP ความหมายคือ
- STATIC จะเป็นการ Manual กำหนด IP Address ให้ Zone
  - DHCP จะเป็นการรับ IP Address จาก Router หรืออุปกรณ์อื่นๆ
  - OFF ปิด Interfaces นี้เพื่อไม่ใช้งาน

3.2 MTU ค่ามาตรฐาน คือ 1500 **⚠** ห้ามทำการแก้ไขเปลี่ยนแปลง

Interface Name	zone1
MAC address	00:60:e0:88:77:ff
Defined as an external	<input checked="" type="checkbox"/>

3.3 Interfaces name จะแสดงชื่อตามที่มีการสร้างจากหัวข้อ Zone

3.4 MAC address เป็น MAC address ของ Interfaces นั้นๆ **ห้ามแก้ไข**

3.5 Define as an external ถ้าเราจะใช้ Interfaces ที่กำลัง Setting เป็นขา WAN ให้คลิกเครื่องหมายถูก เพื่อบอกกับ NU ว่า Interfaces นี้เป็น Gateway แต่ถ้าใช้เป็น LAN / DMZ ไม่ต้องคลิกเครื่องหมายถูก

Visit Control	
Enable Visis	<input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTPS
Firewall Protection	
Firewall Protection Items	<input type="checkbox"/> SYN <input type="checkbox"/> ICMP <input type="checkbox"/> UDP <input type="checkbox"/> Port Scan <input type="button" value="Log"/>

3.6 Visit Control เป็นการกำหนดการติดต่อหรือการสื่อสารกับ Interfaces เช่น

- SNMP ถ้าคลิกถูก เป็นการอนุญาตให้อุปกรณ์ หรือซอฟต์แวร์ สามารถร้องขอใช้ข้อมูล SNMP
- Ping ถ้าคลิกถูกจะเป็นการอนุญาตให้บุคคลภายนอกสามารถ Ping มาที่ Interfaces นี้ได้
- HTTPS ถ้าคลิกถูกจะเป็นการอนุญาตให้เข้าใช้งานอุปกรณ์ NU ได้

3.7 Firewall Protection item คือการป้องกันความเสี่ยงที่เป็น DDOS ถ้าคลิกจะป้องกันสามารถดูความเสี่ยงได้จากการคลิก ที่ ปุ่ม Log สีฟ้า



**ควรที่จะไม่อนุญาต Port Scan เพื่อป้องกันการเดาสุ่ม Port บนอุปกรณ์ NU**

#### 4. ขั้นตอนถัดไปจะเป็นขั้นตอนในการกำหนด IP Address ให้กดปุ่ม Add

#### 4.1 Type ถ้าเลือก STATIC จะ Setting สองแบบคือ

##### 4.1.1 ถ้า Interfaces กำหนดให้เป็น WAN

- เป็นการกำหนดค่า IP Address ที่ได้จากผู้บริการ (FIX IP Address) โดยตรง
- Name ใส่ชื่อของ Interfaces จะเป็นอะไรก็ได้ให้เราเข้าใจเช่น TOT, TRUE, 3BB
- IP ให้นำ Public IP Address ที่ได้จาก ISP มากรอกลง
- Mask ให้สอบถามจาก ISP เช่น 255.255.255.240
- Default gateway คือ IP Address ของ Router เพื่อความถูกต้อง ควรที่จะถาม ISP ก่อนทุกครั้ง
- Auto set designate gateway เป็นการกำหนดว่าเราจะให้ Port นี้ เป็น Gateway ในการออกอินเทอร์เน็ต เราจะเรียกว่า Designate Gateway

ให้คลิกเครื่องหมายถูก และกรอกชื่อตรง Policy route name ชื่อนี้จะถูกเรียกใช้ใน Policy

- Management IP ถ้าคลิกถูกจะเป็นการอนุญาตให้ใช้ IP Address ในการ Remote เข้ามาบริหารจัดการ NU แต่จะสอดคล้อง กับการอนุญาต HTTPS ในข้อ 3 ด้วย
- กดปุ่ม Add และทดสอบสามารถเชื่อมต่ออินเทอร์เน็ตได้หรือไม่

##### 4.1.2 ถ้า Interfaces กำหนดให้เป็น LAN ให้ใส่ข้อมูลเพียง Name, IP, Mask นอกนั้นไม่ต้องใส่ข้อมูล เพราะ LAN ไม่จำเป็นต้องใช้ Gateway

#### 4.2 Type เลือก PPPoE เพราะ Link ที่เราเข้าเป็น Fiber Optic และต้องมีการ Dial ด้วย

## 4.2 Type เลือก PPPoE เพราะ Link ที่เราเข้าเป็น Fiber Optic และต้องมีการ Dial ด้วย

**Add PPPoE :**

Name

Enable

Interface zone2 (WAN2-DYN) ▾

Account

Password  Show

MTU  (1400 ~ 1492)

IPv6

VLAN ID  (0 ~ 4094, 0 => Indicates not to use the vlan tag)

Auto Set  Designated Gateway  Default gateway

- Name ให้ใส่ชื่อที่สื่อความหมายเช่น 3BB-GW, TOT-GW ฯลฯ
- Enable จะถูก Default ให้เป็น Active ไม่ต้องทำอะไรทั้งสิ้น
- Interfaces จะถูก Default มากจาก Interfaces ที่เราต้องการสร้าง IP Address
- Account / Password ต้องขอจาก ISP ใช้ในการ หมุนไปที่ ISP เพื่อร้องขอการออกอินเทอร์เน็ต
- MTP ไม่ต้อง Setting
- VLAN ID ถ้า ISP ต้องให้ใส่ข้อมูลให้กรอกตาม ISP ถ้าไม่ต้องการให้เป็น 0
- Auto Set ให้เป็นค่า Default ความหมายเหมือน STATIC

**PPPOE Alive Detection**

Detection Method 
 DNS  ICMP  ARP  NONE

- PPPOE Alive Detection เป็น Function ในการตรวจสอบว่า Link นั้นๆ Down หรือไม่ให้เลือก ICMP และกรอกข้อมูล 8.8.8.8 ที่ช่อง Detected IP address

**Visit Control**

Enable Visis 
 SNMP  Ping  HTTPS

**Firewall Protection**

Firewall Protection Items 
 SYN  ICMP  UDP  Port Scan Log

- เป็นการกำหนดสิทธิเข้าถึงอุปกรณ์ NU และป้องกันความเสี่ยงที่จะเกิดขึ้นกับ Interfaces นี้

## 5. หลังจาก Setting แล้วช่วยให้ทำการทดสอบด้วย Tool / Connection Test /Ping

- Tools
  - ▣ Connection Test
  - ▣ Capture Packet
- Log
- Status

Ping	Trace Route	DNS Query	Port Scan	IP Route	Int
<b>Ping Setting</b>					
Target IP or Domain	<input type="text"/> ( Max. 30 characters )				
Package Size	<input type="text" value="32"/>	Bytes ( Range : 1 - 9999 )			
Count	<input type="text" value="4"/>	( Range : 0 - 9999, 0 means no limit )			
Timeout	<input type="text" value="1"/>	Seconds ( Range : 1 - 9999 )			
Using Interface & IP ?	<input type="text" value="zone0 (LAN)"/>	<input type="text" value="192.168.99.253"/>			
Assign Gateway	<input type="text" value="None"/>				

- Target ให้ใส่ 8.8.8.8
- Using Interfaces & IP เป็นการกำหนดว่าเราจะใช้ Interfaces ไหนในการ Ping ให้เลือก Interfaces ที่สร้างเสร็จแล้ว
- กดปุ่ม Ok เพื่อทำการ Ping ถ้าขึ้นตามรูปด้านล่างแสดง Setting ถูกต้อง และ ISP มีการไหล่กระแสสัญญาณอินเทอร์เน็ตให้แล้ว

```

PING 8.8.8.8 (8.8.8.8) from 192.168.1.2 : 32(60) bytes of data.
40 bytes from 8.8.8.8: icmp_seq=1 ttl=246 time=44.1 ms
40 bytes from 8.8.8.8: icmp_seq=2 ttl=246 time=23.9 ms
40 bytes from 8.8.8.8: icmp_seq=3 ttl=246 time=23.7 ms
40 bytes from 8.8.8.8: icmp_seq=4 ttl=246 time=24.0 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 23.758/29.009/44.196/8.770 ms

```



ข้อระมัดระวังหรือข้อจำกัดคือทุกๆ Interfaces จะต้องไม่ Setting IP Address กลุ่มเดียวกันหรือ Subnet เดียวกันเด็ดขาด