

# ใบงาน

รหัสวิชา 30901-2011

วิชา การบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์



ครูผู้สอน วรกิจ วิริยะเกษามงคล

แผนกวิชาเทคโนโลยีสารสนเทศ

วิทยาลัยเทคนิคชลบุรี

## ใบงาน

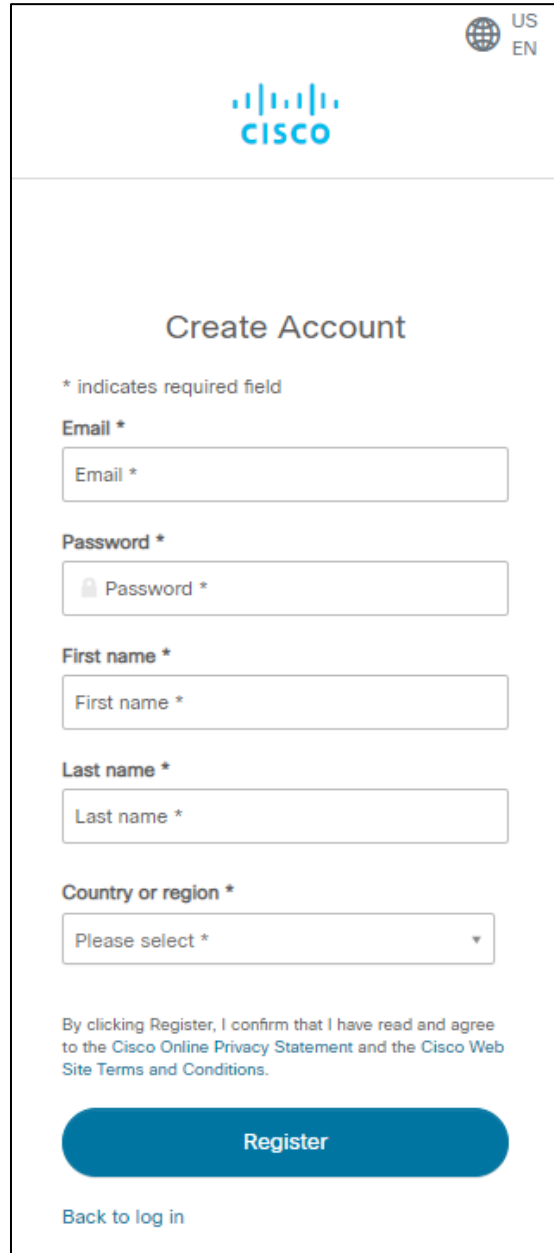
### ชื่องาน ติดตั้งโปรแกรมจำลองการเชื่อมต่อระบบเครือข่าย

ชื่อวิชา การบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ รหัสวิชา 30901-2011

---

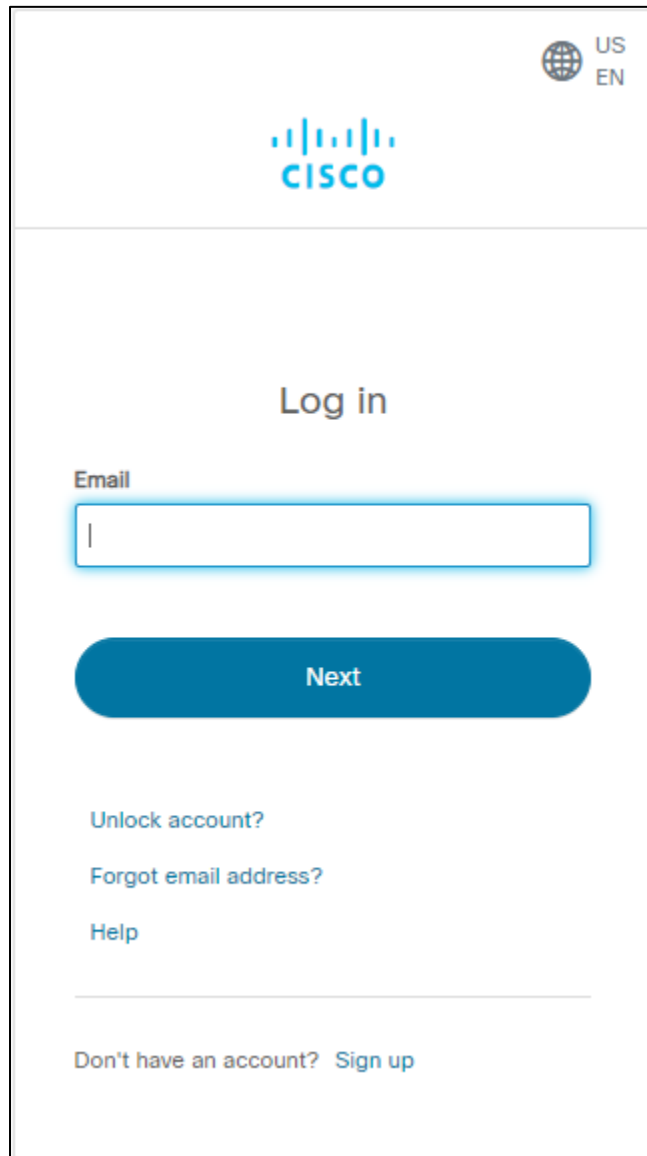
#### ขั้นตอนการติดตั้งโปรแกรม

Go to the Cisco Networking Academy website at netacad.com and create an account if you don't have one.



The screenshot shows the Cisco Networking Academy registration page. At the top right, there is a globe icon and the text 'US EN'. The Cisco logo is centered at the top. Below the logo, the heading 'Create Account' is displayed. A note states '\* indicates required field'. The form contains the following fields: 'Email \*' (text input), 'Password \*' (password input with a lock icon), 'First name \*' (text input), 'Last name \*' (text input), and 'Country or region \*' (dropdown menu with 'Please select \*' and a downward arrow). Below the fields, there is a confirmation statement: 'By clicking Register, I confirm that I have read and agree to the Cisco Online Privacy Statement and the Cisco Web Site Terms and Conditions.' At the bottom, there is a blue 'Register' button and a link for 'Back to log in'.

Log in to your account and go to the Packet Tracer course page.



US  
EN

**CISCO**

## Log in

Email

Next

[Unlock account?](#)

[Forgot email address?](#)

[Help](#)

---

Don't have an account? [Sign up](#)

Download the version of Packet Tracer you require.

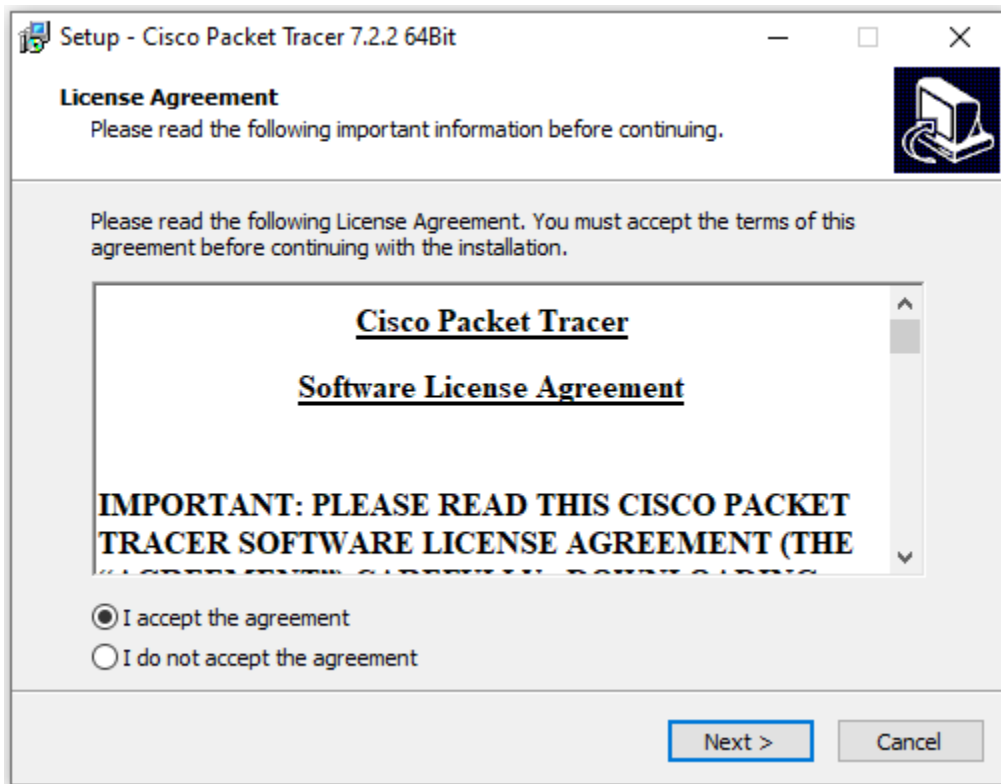
[Packet Tracer 8.2.1 MacOS 64bit](#)

[Packet Tracer 8.2.1 Ubuntu 64bit](#)

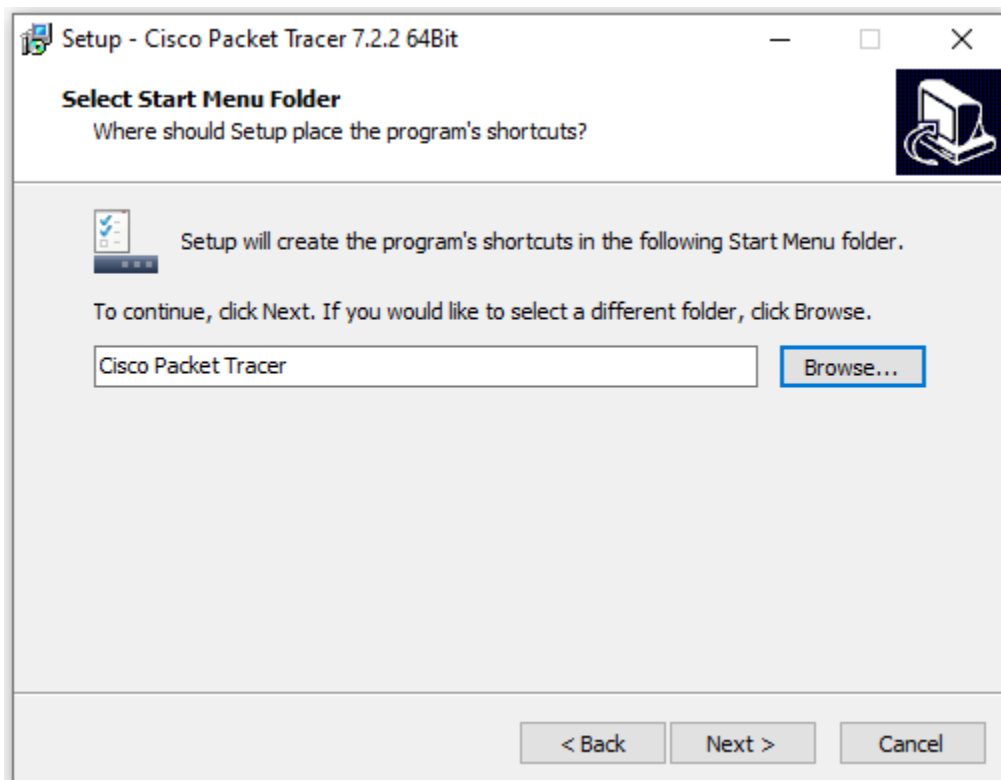
[Packet Tracer 8.2.1 Windows 64bit](#)

If you need more guidance, please follow the [Cisco Packet Tracer Download and Installation Instructions](#).

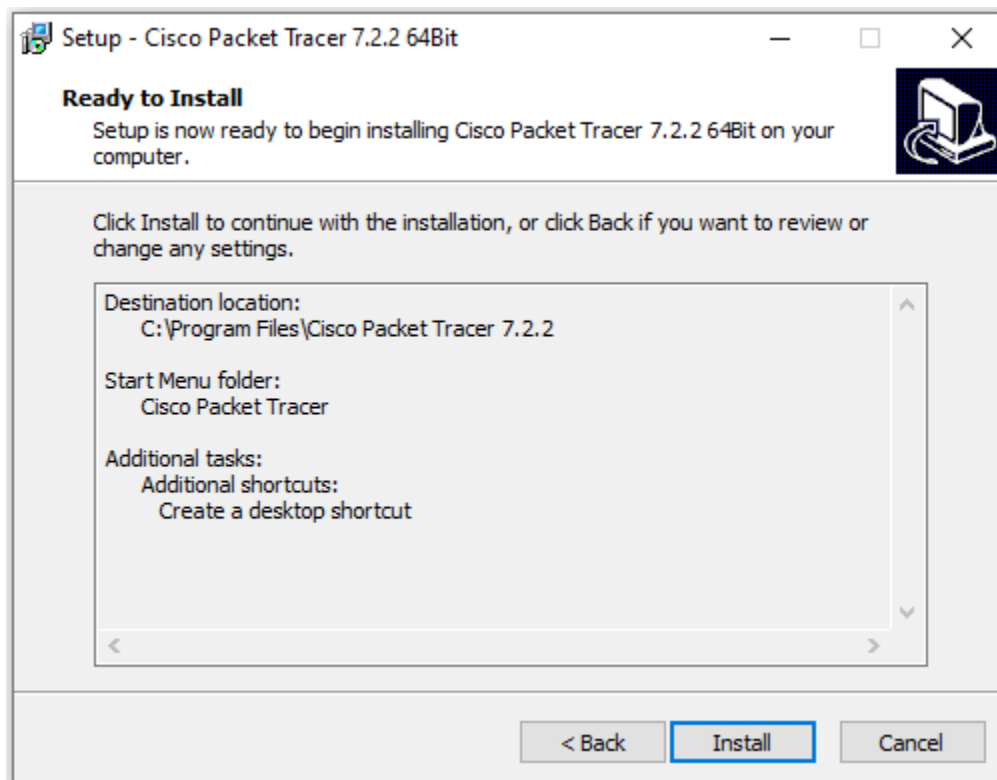
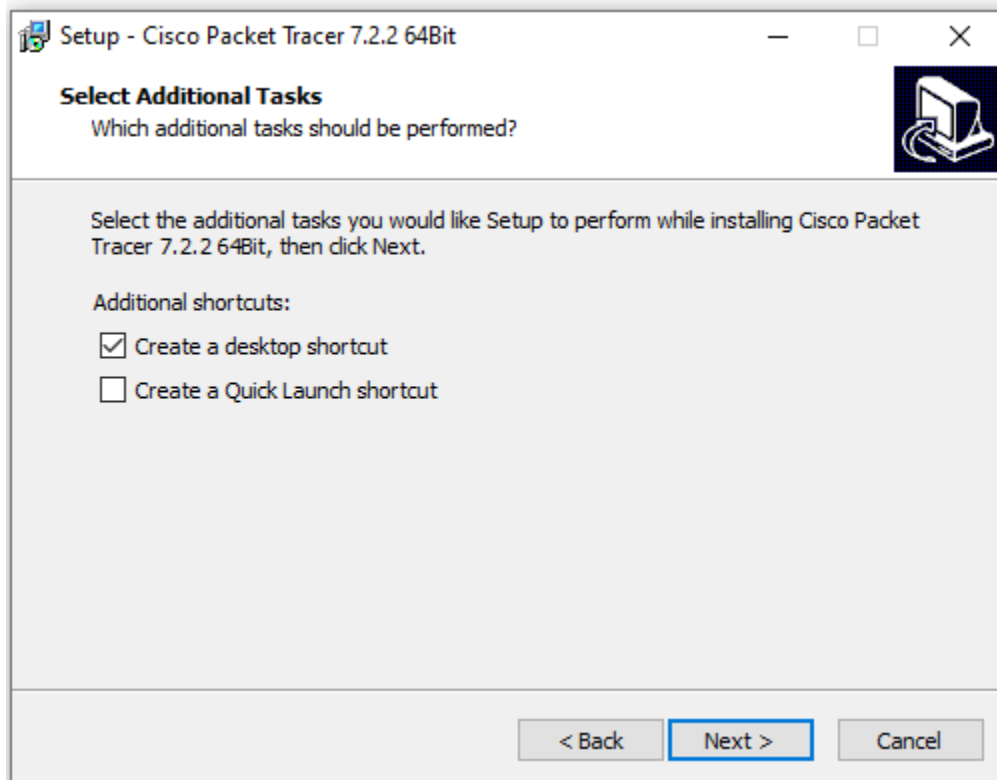
เมื่อดาวน์โหลดเสร็จสิ้นแล้วให้ทำการดับเบิลคลิกไฟล์ PacketTracer-x.x.x-win64-setup เพื่อทำการติดตั้ง จากนั้น เลือก **I accept the agreement** แล้วคลิก **Next**



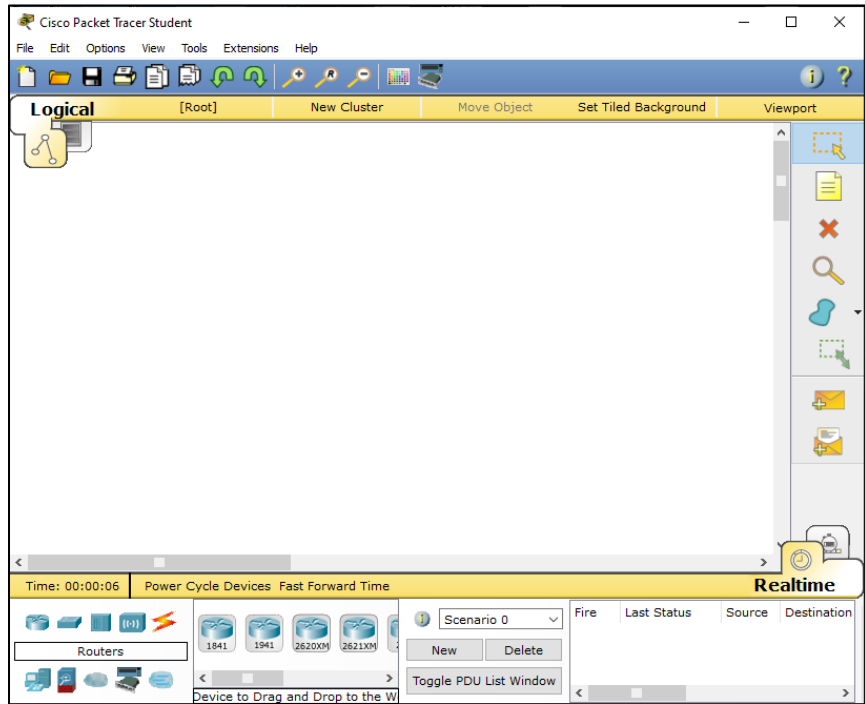
เลือกตำแหน่งจัดเก็บ shortcuts ของซอฟต์แวร์แล้วคลิก **Next**



เลือกว่าจะติดตั้ง shortcuts ไว้ส่วนใดบ้าง แล้วคลิก Next



เมื่อติดตั้งเสร็จสิ้น คลิก Finish



## Cisco Router Modes

Cisco routers are a vital component of modern networks, and they come with a variety of different modes that allow users to configure and manage them. Understanding these modes and how to use them effectively can help network administrators to optimize their network performance and troubleshoot issues more efficiently.

In this article, we will discuss the different Cisco router modes, including their purpose and how to access them. We will also provide examples of common tasks that can be performed in each mode and provide tips for using them effectively.

### User EXEC Mode

The User EXEC mode, also known as user mode or privileged mode, is the default mode that a Cisco router is in when it first starts up. This mode allows users to view basic information about the router and its configuration, but it does not allow for any changes to be made.

To access the User EXEC mode, simply connect to the router using a terminal program and enter the "enable" command. This will prompt the user for a password if one has been set. Once in User EXEC mode, users can view the current configuration of the router by entering the "show running-config" command.

### Examples of tasks that can be performed in User EXEC mode include

- Viewing the router's current IP address and other basic information
- Viewing the current configuration of the router
- Pinging other devices on the network to test connectivity
- Troubleshooting basic connectivity issues

### Tips for using User EXEC mode

Remember that changes cannot be made in this mode, so if you need to make changes to the router's configuration, you will need to enter Privileged EXEC mode.

Use the "show running-config" command to quickly view the current configuration of the router and identify any issues.

### Privileged EXEC Mode

The Privileged EXEC mode, also known as privileged mode or configuration mode, allows users to make changes to the router's configuration. This mode is accessed by entering the "enable" command in User EXEC mode and then entering the appropriate password.

Examples of tasks that can be performed in Privileged EXEC mode include –

- Changing the router's IP address and other network settings
- Configuring interfaces and subinterfaces
- Setting up access control lists (ACLs)
- Configuring routing protocols such as OSPF or BGP
- Saving the router's configuration to flash memory

Tips for using Privileged EXEC mode –

Use the "show running-config" command to view the current configuration of the router before making any changes.

Use the "copy running-config startup-config" command to save your changes to the router's configuration.

Be careful when making changes to the router's configuration, as mistakes can cause the router to become inaccessible or disrupt network connectivity.

## Global Configuration Mode

The Global Configuration mode allows users to make changes to the router's global configuration settings, such as the hostname and the enable secret password. This mode is accessed by entering the "configure terminal" command in Privileged EXEC mode.

Examples of tasks that can be performed in Global Configuration mode include –

- Changing the router's hostname
- Setting the enable secret password
- Configuring the router's clock settings
- Configuring the router's virtual terminal (VTY) settings
- Configuring the router's SNMP settings

Tips for using Global Configuration mode –

Use the "show running-config" command to view the current global configuration settings before making any changes.

Use the "copy running-config startup-config" command to save your changes to the router's configuration.

Be mindful of the impact that changes in Global Configuration mode may have on other parts of the network, such as the VTY settings that control remote access to the router.



# Interface Configuration Mode

The Interface Configuration mode allows users to make changes to the configuration of specific interfaces on the router. This mode is accessed by entering the "configure terminal" command in Privileged EXEC mode and then entering the "interface" command followed by the name of the interface that you want to configure.

Examples of tasks that can be performed in Interface Configuration mode include –

- Configuring the IP address and subnet mask for an interface
- Enabling or disabling an interface
- Configuring duplex and speed settings for an interface
- Configuring security settings for an interface, such as access control lists (ACLs)
- Configuring routing protocols such as OSPF or BGP on an interface

Tips for using Interface Configuration mode –

Use the "show running-config" command to view the current configuration of the interface before making any changes.

Use the "no shutdown" command to enable an interface that has been disabled, and the "shutdown" command to disable an interface that is currently enabled.

Be mindful of the impact that changes in Interface Configuration mode may have on other parts of the network, such as the routing protocols that are configured on the interface.

# Router Configuration Mode

The Router Configuration mode allows users to configure routing protocols such as OSPF, BGP, EIGRP and so on. This mode is accessed by entering the "configure terminal" command in Privileged EXEC mode and then entering the "router" command followed by the name of the routing protocol you want to configure.

Examples of tasks that can be performed in Router Configuration mode include –

- Configuring routing protocols such as OSPF or BGP
- Configuring routing tables
- Configuring redistribution of routing protocols
- Configuring route summarization
- Configuring filtering and summarization of routes

Tips for using Router Configuration mode –

Use the "show running-config" command to view the current configuration of the routing protocol before making any changes.

Be mindful of the impact that changes in Router Configuration mode may have on other parts of the network, such as the routing tables and other routing protocols that are configured on the router.

## Classes of IP addresses

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.

Classes of IP addresses are:

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

Consider the following IP addresses:

- **10.50.120.7** – because this is a Class A address, the first number (10) represents the network part, while the remainder of the address represents the host part (50.120.7). This means that, in order for devices to be on the same network, the first number of their IP addresses has to be the same for both devices. In this case, a device with the IP address of 10.47.8.4 is on the same network as the device with the IP address listed above. The device with the IP address 11.5.4.3 is not on the same network, because the first number of its IP address is different.
- **172.16.55.13** – because this is a Class B address, the first two numbers (172.16) represent the network part, while the remainder of the address represents the host part (55.13). A device with the IP address of 172.16.254.3 is on the same network, while a device with the IP address of 172.55.54.74 isn't.

**NOTE**

The system of network address ranges described here is generally bypassed today by use of the [Classless Inter-Domain Routing \(CIDR\)](#) addressing.

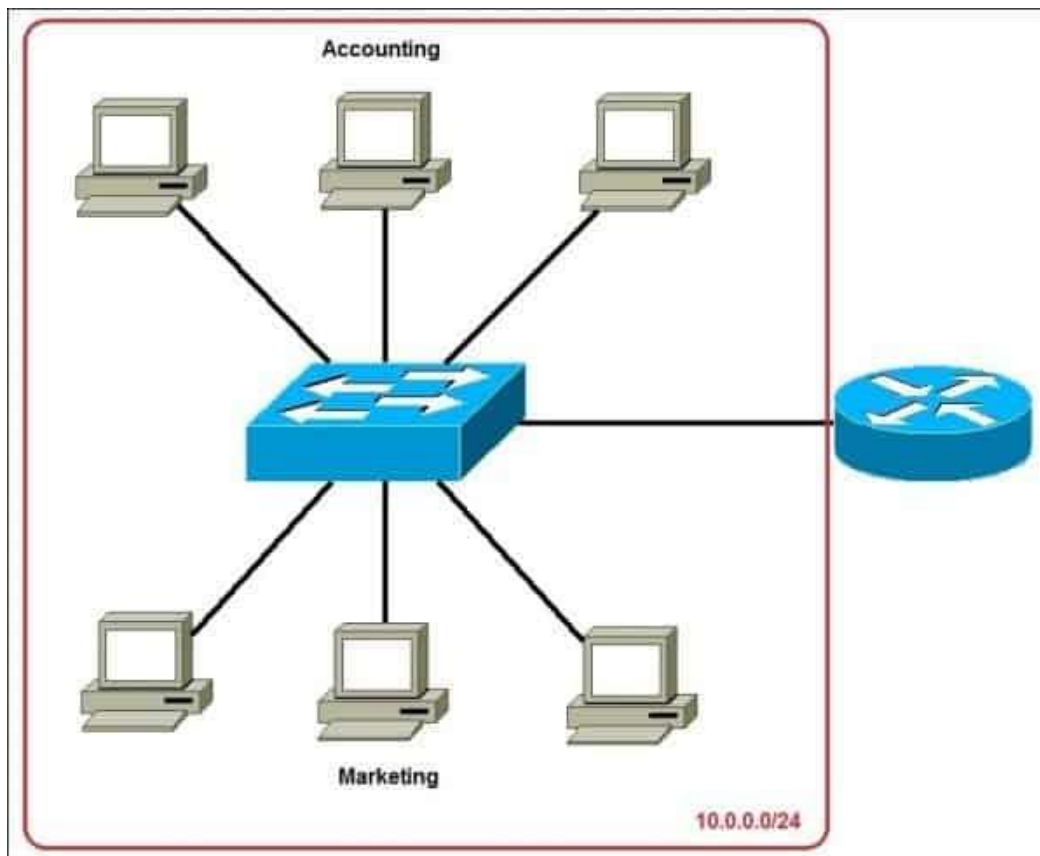
Special IP address ranges that are used for special purposes are:

- **0.0.0.0/8** – addresses used to communicate with the local network
- **127.0.0.0/8** – loopback addresses
- **169.254.0.0/16** – link-local addresses (APIPA)

## Subnetting Explained

**Subnetting** is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network, and reduces the size of the broadcast domain.

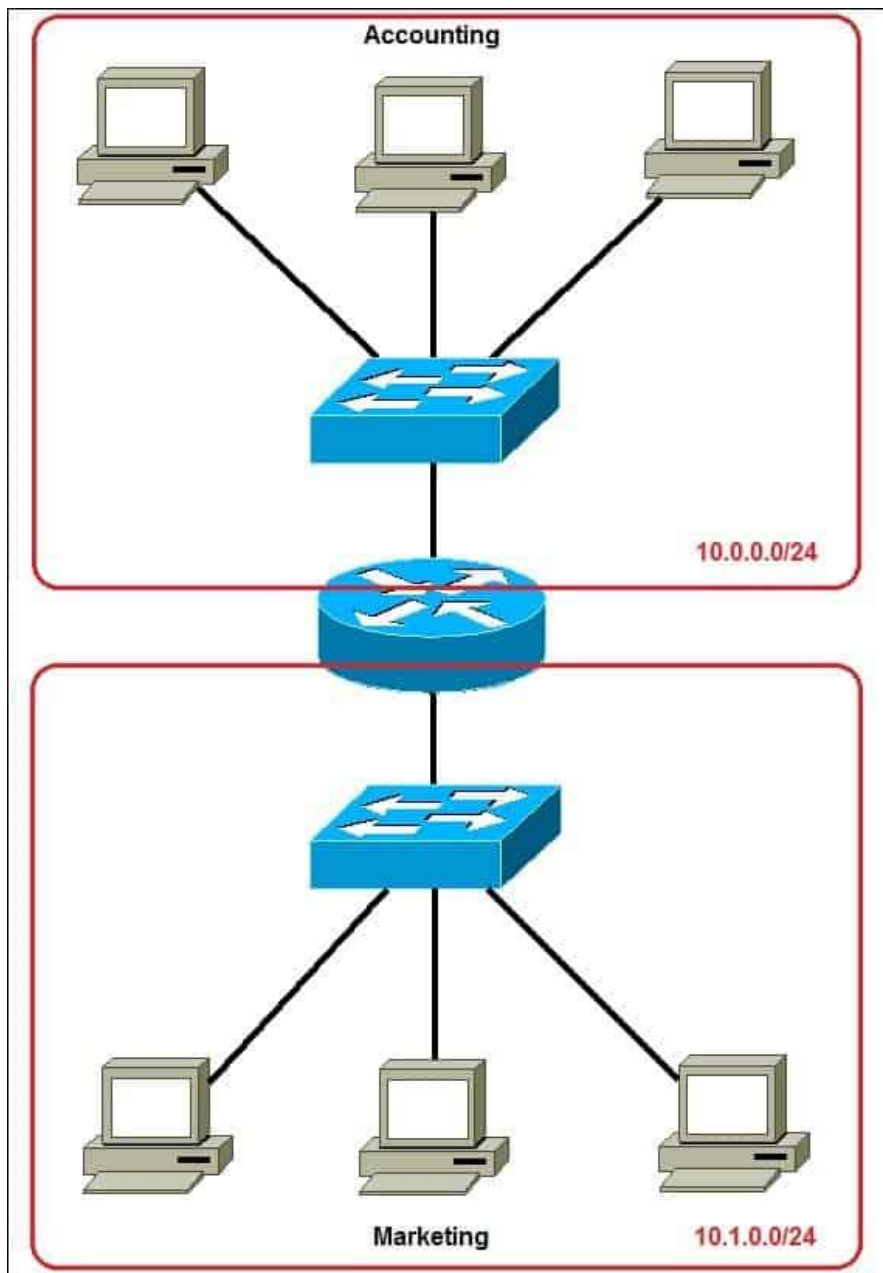
Consider the following example:



In the picture above we have one huge network: **10.0.0.0/24**. All hosts on the network are in the same subnet, which has the following disadvantages:

- **a single broadcast domain** – all hosts are in the same broadcast domain. A broadcast sent by any device on the network will be processed by all hosts, creating lots of unnecessary traffic.
- **network security** – each device can reach any other device on the network, which can present security problems. For example, a server containing sensitive information shouldn't be in the same network as the user's workstations.
- **organizational problems** – in large networks, different departments are usually grouped into different subnets. For example, you can group all devices from the **Accounting** department in the same subnet and then give access to sensitive financial data only to hosts from that subnet.

The network above could be subnetted like this:



Now, two subnets were created for different departments: **10.0.0.0/24** for Accounting and **10.1.0.0/24** for Marketing. Devices in each subnet are now in a different broadcast domain. This will reduce the amount of traffic flowing on the network and allow us to implement packet filtering on the router.

## show interfaces status command

The status of an interface on a Cisco switch can be checked using the *show interface TYPE* exec mode command. Consider the following example:

```
SW1#show interfaces fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0040.0b21.0b01 (bia 0040.0b21.0b01)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
  drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
  Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
```

```
2357 packets output, 263570 bytes, 0 underruns  
0 output errors, 0 collisions, 10 interface resets  
0 babbles, 0 late collision, 0 deferred  
0 lost carrier, 0 no carrier  
0 output buffer failures, 0 output buffers swapped out
```

As you can see from the output above, this command gives us plenty of information about the specified interface. Here is a brief description of the most important lines:

- **FastEthernet0/1 is up, line protocol is up (connected)** – indicates that the interface is in the up and up state
- **Hardware is Lance, address is 0040.0b21.0b01** – Lance indicates the chipset used by the port. The MAC address of the port is also listed
- **BW 100000 Kbit, DLY 1000 usec** – the bandwidth and delay of the interface
- **Full-duplex, 100Mb/s** – the port operates in the full duplex mode and supports the speed of up to 100Mb/s
- **956 packets input, 193351 bytes, 0 no buffer** – the total number and size of packets received by the port.
- **Received 956 broadcasts** – the total number of broadcast packets received by the device.
- **0 input errors, 0 CRC, 0 frame...** – the number of received packets that were received incorrectly.
- **2357 packets output, 263570 bytes, 0 underruns** – the total number and size of packets sent by the port.
- **0 output errors, 0 collisions** – the number of packets that were not sent because of an error and the number of Ethernet collisions.



# ใบงาน / ใบความรู้

## ชื่องาน การออกแบบระบบเครือข่าย

ชื่อวิชา การบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์

รหัสวิชา 30901-2011

### 6 หลักการพื้นฐานออกแบบระบบเครือข่าย LAN สมัยใหม่

(<https://www.techtalkthai.com/6-modern-lan-network-design-for-network-engineers/>)

#### 1. ออกแบบจากการใช้งาน ไม่ใช่พีเจอร์ของระบบเครือข่าย

ในสมัยก่อนนั้นเราอาจทำการศึกษาผลิตภัณฑ์แต่ละค่ายและนำพีเจอร์นั้นๆ มาใช้ออกแบบระบบเครือข่าย แต่ปัจจุบันนี้การมองไปที่อุปกรณ์ที่จะนำมาใช้งานเชื่อมต่อเครือข่ายจริงๆ ว่าจะต้องใช้อะไรบ้างแล้วจึงค่อยออกแบบระบบเครือข่ายนั้นก็ถือเป็นแนวทางที่สมเหตุสมผลกว่า ด้วยการที่ระบบเครือข่ายในปัจจุบันนั้นมีทั้งอุปกรณ์ IoT และอุปกรณ์อื่นๆ ที่ไม่ใช่ PC เข้ามาเกี่ยวข้องเป็นจำนวนมากนั่นเอง

แนวทางเบื้องต้นคือควรจะต้องทำการจำแนกพฤติกรรมและความต้องการของแต่ละอุปกรณ์ออกจากกันให้ชัดเจน แล้วจึงค่อยออกแบบ Topology และโครงสร้างพื้นฐานที่จำเป็น ทั้งในแง่ของ Bandwidth, Application ไปจนถึงการใช้พลังงานที่อาจต้องจ่ายผ่าน PoE ด้วย

#### 2. ออกแบบให้ง่ายต่อการบริหารจัดการ และการรักษาความมั่นคงปลอดภัย

การออกแบบระบบเครือข่ายให้เข้าใจง่ายและบริหารจัดการง่ายขึ้น นอกจากจะทำให้ทำงานได้สะดวกแล้ว ก็ยังจะช่วยลดความเสี่ยงทางด้านความมั่นคงปลอดภัยให้น้อยลงไปด้วย ดังนั้นจึงควรออกแบบระบบเครือข่ายให้ง่ายต่อการตั้งค่า, การติดตั้งใช้งาน, การบริหารจัดการ และการแก้ไขปัญหาเมื่อเอาไว้ตั้งแต่แรก รวมถึงสามารถตรวจสอบและจัดการการเชื่อมต่อไปยังระบบแบบ On-Premises ภายใน Data Center และ Cloud ได้อย่างยืดหยุ่นด้วย เพื่อให้ง่ายต่อการแก้ไขปัญหาในระยะยาวนั่นเอง

#### 3. ใช้เทคโนโลยีให้คุ้มค่าที่สุด และลดความซับซ้อนของระบบลง

นำเทคโนโลยีใหม่ๆ และนวัตกรรมต่างๆ มาใช้งานเพื่อให้ธุรกิจได้รับประโยชน์จากเทคโนโลยีอื่นๆ อย่างเต็มที่ ไม่ว่าจะเป็นลดค่าใช้จ่ายในการติดตั้ง, การลดความซับซ้อนของระบบเครือข่าย, การเพิ่มความยืดหยุ่นให้สามารถติดตั้งใช้งานอุปกรณ์ใหม่ๆ เพิ่มเติมได้อย่างง่ายดาย และทำให้ผู้ใช้งานยังคงเชื่อมต่อระบบเครือข่ายได้อย่างง่ายดายไม่ติดขัด

#### 4. เลือกใช้เทคโนโลยีที่เป็นมิตรกับสิ่งแวดล้อม

ประเด็นเรื่องสิ่งแวดล้อมเองก็ถือว่าสำคัญ ไม่ว่าจะเป็นการเลือกอุปกรณ์ที่มีมาตรฐานทางด้านพลังงานและการเลือกใช้วัสดุที่เป็นมิตรกับสิ่งแวดล้อม ไปจนถึงการออกแบบระบบเครือข่ายให้ยังคงใช้ระบบโครงสร้างพื้นฐานเดิมที่มีอยู่แต่ก่อนได้โดยไม่ต้องรื้อทำใหม่ทั้งหมด รวมถึงการนำ Switch PoE คุณภาพสูงที่ใช้พลังงานได้อย่างคุ้มค่ามาใช้ลดปริมาณพลังงาน, สามารถควบคุมการเปิดปิดอุปกรณ์ได้ และยังลดการเดินสายลงอีกด้วย

## 5. แบ่ง LAN ออกเป็นสัดส่วนอย่างเหมาะสม

แบ่งสัดส่วนของระบบเครือข่ายในระดับ Logical เพื่อให้สามารถรองรับ Application และการทำงานได้อย่างหลากหลายโดยเดินสาย LAN ให้น้อยลง ซึ่งแนวทางนี้ก็ยังส่งผลดีต่อการแบ่งสัดส่วนของอุปกรณ์ประเภทต่างๆ ออกจากกัน และลดความเสี่ยงที่อาจเกิดขึ้นในระบบเครือข่ายในแง่ของความมั่นคงปลอดภัยได้ด้วย

## 6. จัดสรรการใช้ทรัพยากรใหม่ให้ตอบโจทย์ ROI อย่างคุ้มค่าสูงสุด

เมื่อระบบเครือข่ายสามารถทำงานได้อย่างคุ้มค่าแล้ว ในงบประมาณรอบถัดไปก็อาจหันมาเสริมขีดความสามารถในการสื่อสารทางธุรกิจให้คุ้มค่ายิ่งขึ้น เพื่อช่วยลดค่าใช้จ่ายและการลงทุนโดยรวมลง และทำให้มีงบประมาณสำหรับลงทุนในระบบ Endpoint หรือ Application ใหม่ๆ ที่จะช่วยสร้างขีดความสามารถในการแข่งขันของธุรกิจให้ดียิ่งขึ้น และคุ้มค่ายิ่งขึ้นต่อไปได้อีกทางหนึ่งด้วย