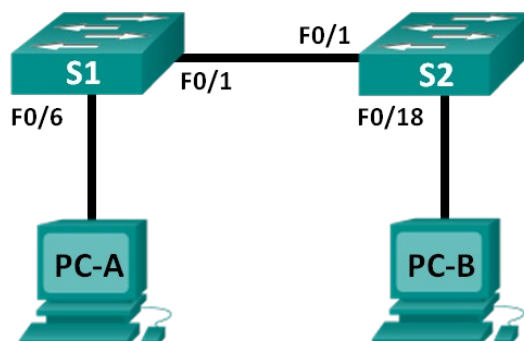


## Lab 2 Activity 2.1 - Building a Simple Network (Not assessed)

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

### Objectives

**Part 1: Compute binary values for IP Address and Subnet Mask**

**Part 2: Set Up the Network Topology (Ethernet only)**

**Part 3: Configure PC Hosts**

**Part 4: Configure and Verify Basic Switch Settings**

### Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will investigate the relationship between the IP address and subnet Mask. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status.

You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

**Note:** The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note:** Make sure that the switches have been erased and have no startup configurations. Refer to Appendix A for the procedure to initialize and reload a switch.

### Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, 8 or 10 with terminal emulation program, such as PuTTY or Tera Term)

- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

### Part 1: Investigate relationship between IP Address and Subnet Mask

In Part 1, you will investigate the relationship between the IP Address and subnet masks for PC-A and PC-B.

Note that this Activity is not assessed and does not need to be submitted but you should show it to your laboratory demonstrator as you go to confirm that it is correct. The non-assessed sections are for supporting your understanding of key concepts and should be completed before doing the assessment.

#### Step 1: Compute the binary values for PC-A and PC-B IP addresses and Subnet Masks

IP Addresses:

Device	IP Address	Binary version of IP address
PC-A	192.168.1.10	_____ . _____ . _____ . _____
PC-B	192.168.1.11	_____ . _____ . _____ . _____

Subnet Masks:

Device	Subnet Mask	Binary version of Subnet Mask address
PC-A	255.255.255.0	_____ . _____ . _____ . _____
PC-B	255.255.255.0	_____ . _____ . _____ . _____

#### Step 2: Perform Logical AND on PC-A IP address with PC-A Subnet Mask

The subnet mask is used to isolate the network part of the IP address. This is very useful when working with subnets (a topic formally introduced in Chapter 7 of the course). To isolate the network part of the IP address, perform a LOGICAL AND on the IP address and the subnet mask for PC-A and PC-B.

PC-A: Binary IP address:

Binary subnet mask:

Binary Result:

	_____ . _____ . _____ . _____
	_____ . _____ . _____ . _____
AND	_____ . _____ . _____ . _____

What is the decimal value of the Binary result from the above LOGICAL AND computation?

Decimal result:

\_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Why is part of the result the same as the original IP address, and why is the other part of the result set to 0?

---

---

Repeat the LOGICAL AND computation for PC-B:

PC-A: Binary IP address:

Binary subnet mask:

Binary Result:

	_____	.	_____	.	_____	.	_____
	_____	.	_____	.	_____	.	_____
AND							
	_____	.	_____	.	_____	.	_____

What is the decimal value of the Binary result from the above LOGICAL AND computation?

Decimal result: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Are PC-A and PC-B on the same network?

---

How can you tell?

---

---

## Part 2: Set Up the Network Topology (Ethernet only)

In Part 2, you will cable the devices together according to the network topology.

### Step 1: Power on the devices.

Power on all devices in the topology. The switches do not have a power switch; they will power on as soon as you plug in the power cord.

### Step 2: Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

### Step 3: Connect the PCs to their respective switches.

- Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.
- Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.

### Step 4: Connect PC-A to the console port of Switch S1.

After cabling the network devices to the PCs, connect PC-A to the Console port of Switch S1. This will be the console connection that you will use to configure the Switch.

### Step 5: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.

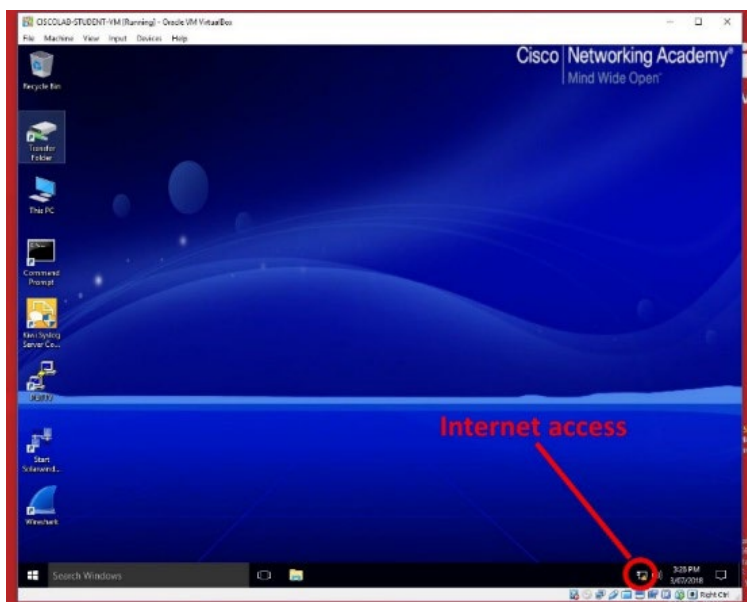
## Part 3: Configure PC Hosts

### Step 1: Turn off the firewall on the virtual machine only

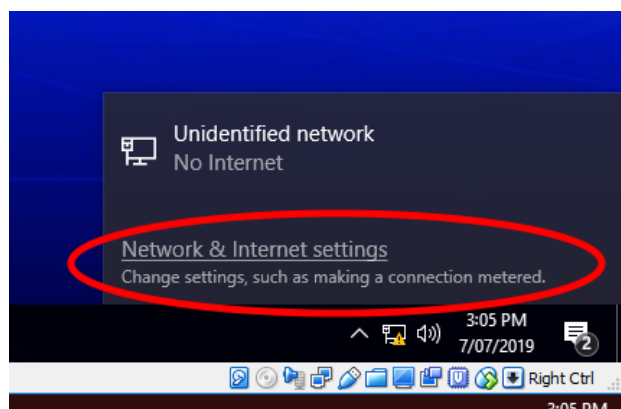
Open the Virtual machine environment on each physical PC that you will be using:



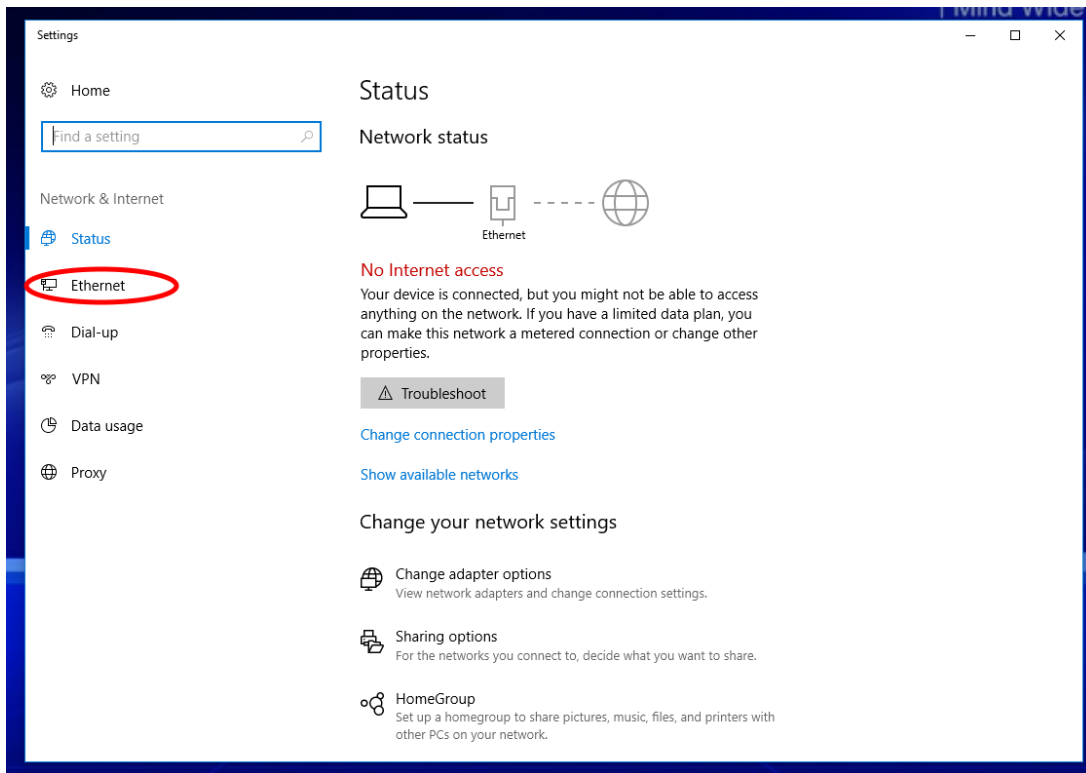
- Turn off the firewall on each of the virtual machine environments: In the Virtual machine, left-click the Network Internet access icon:



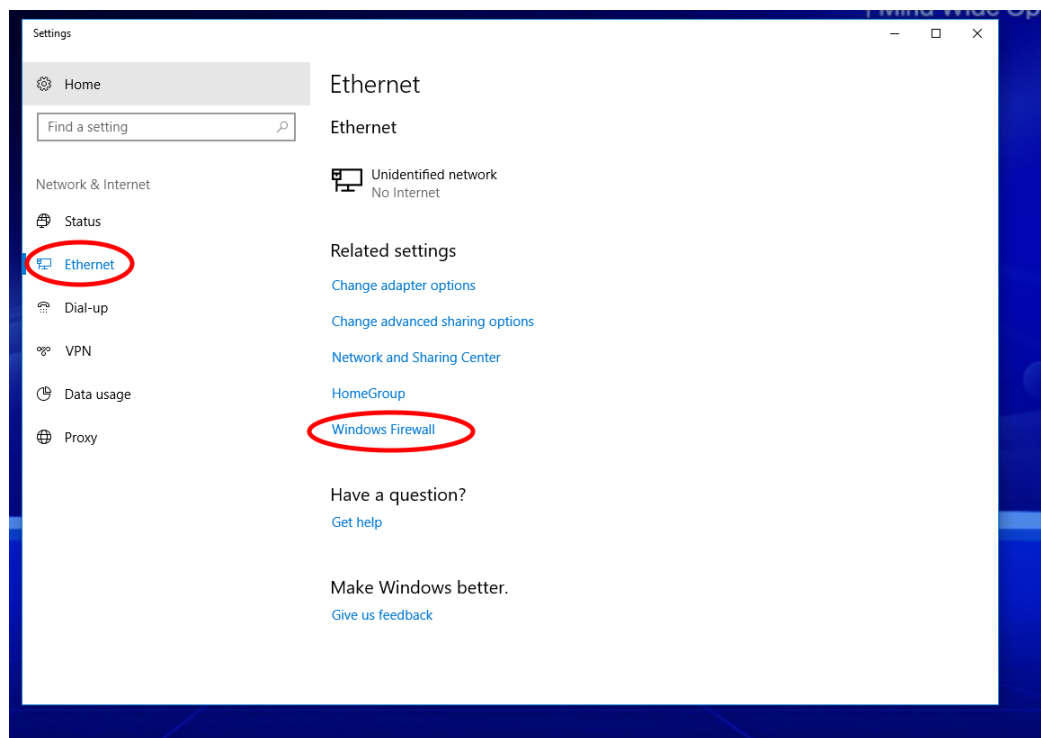
- Click on the Network & Settings popup.



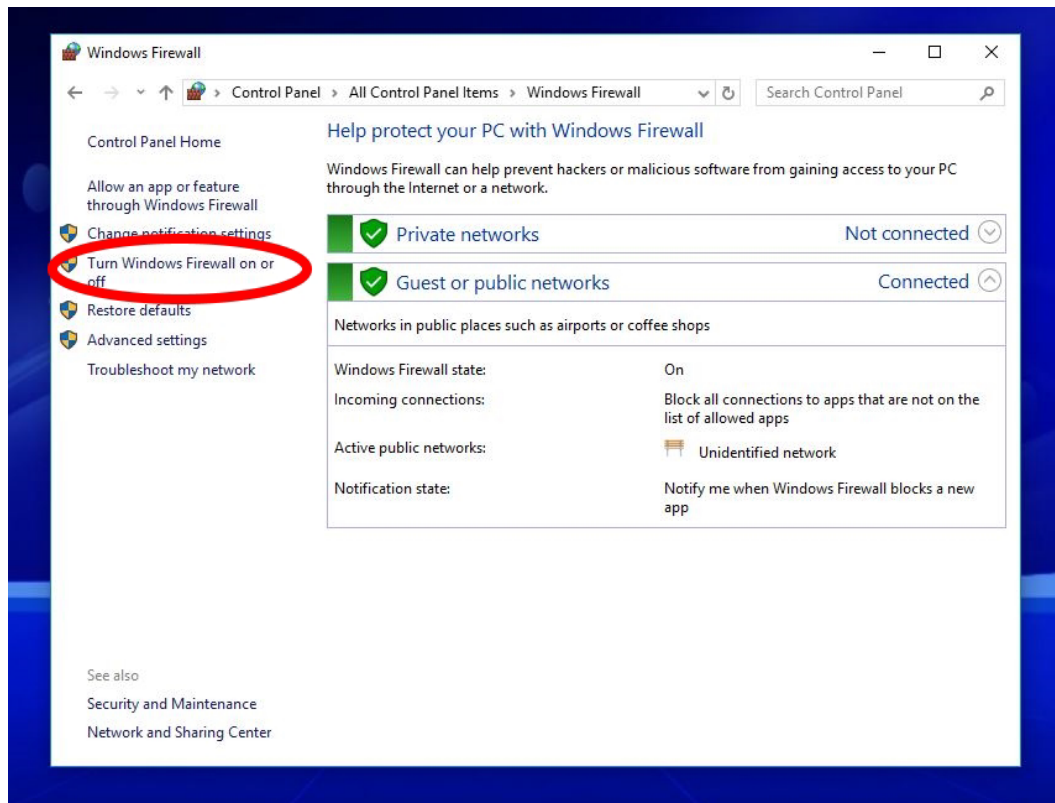
- c. In the left pane of the Network and Sharing Center window, click the Ethernet link.



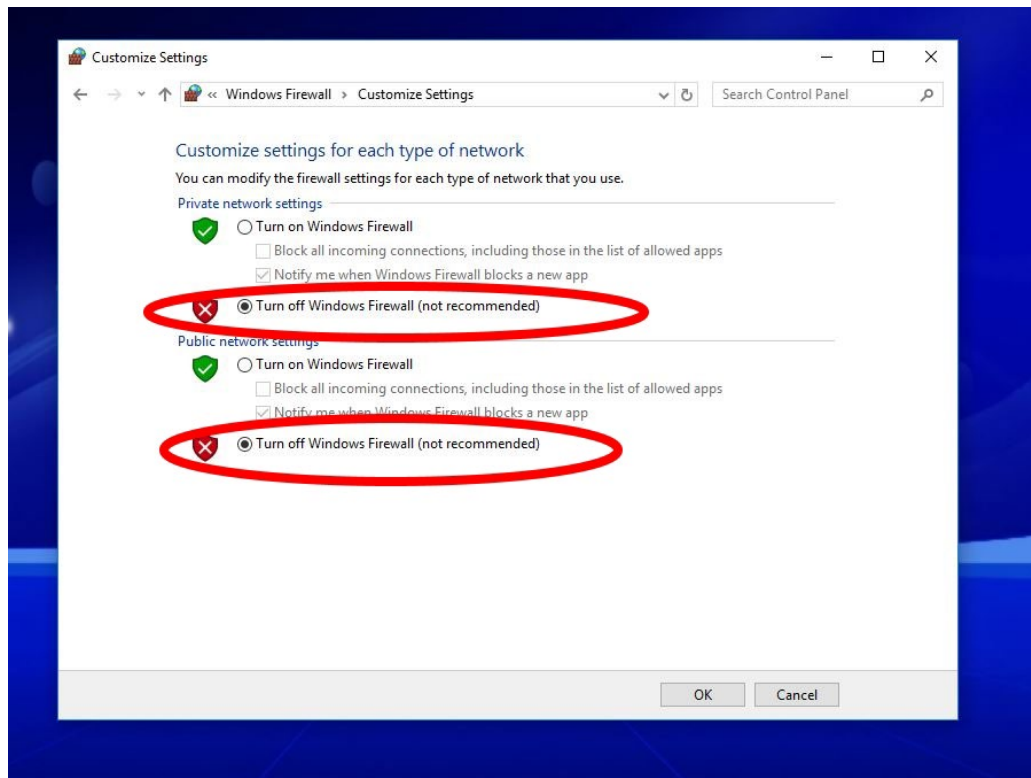
- d. In the middle pane of the Ethernet page, click **Windows Firewall** link.



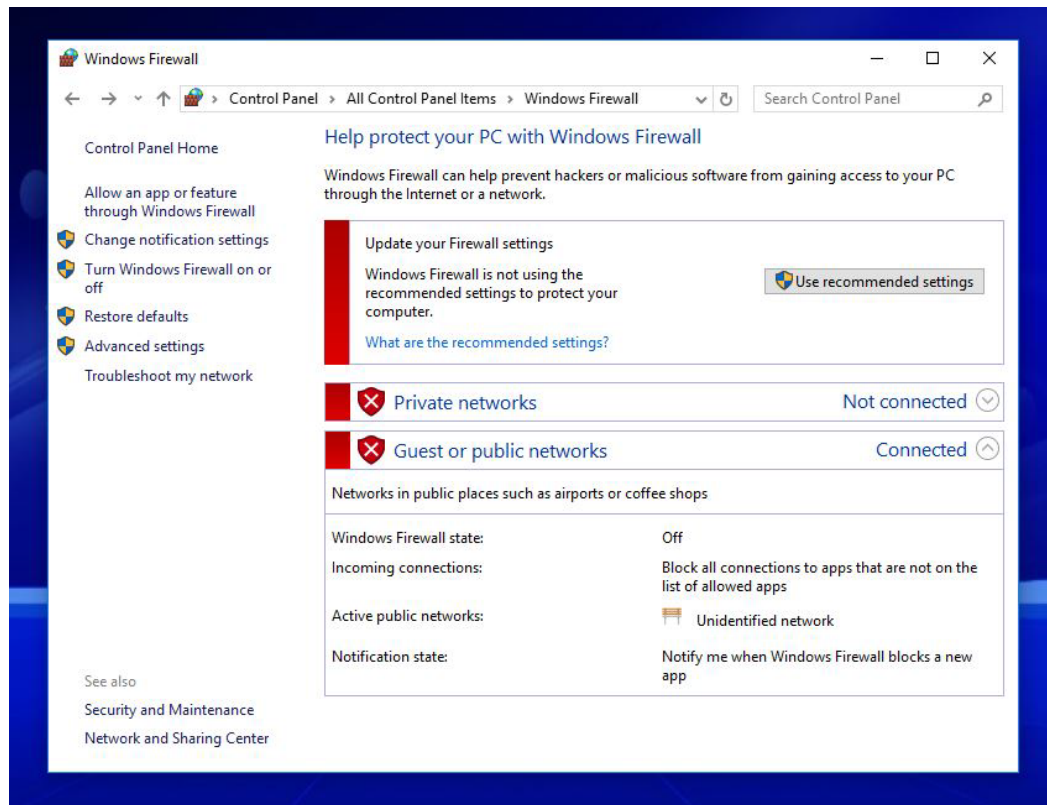
- e. If the firewall is already off, go to Part 3 Step 2. Otherwise, click on **Turn Windows Firewall on or off**



- f. Click on Turn off Windows Firewall for both private and public networks and press OK

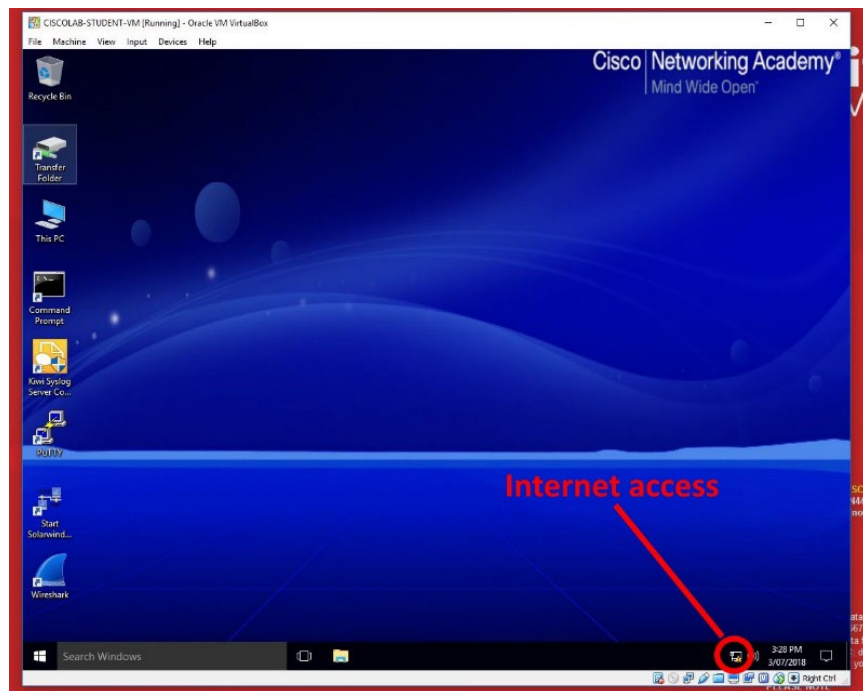


g. You should now see the following screen:

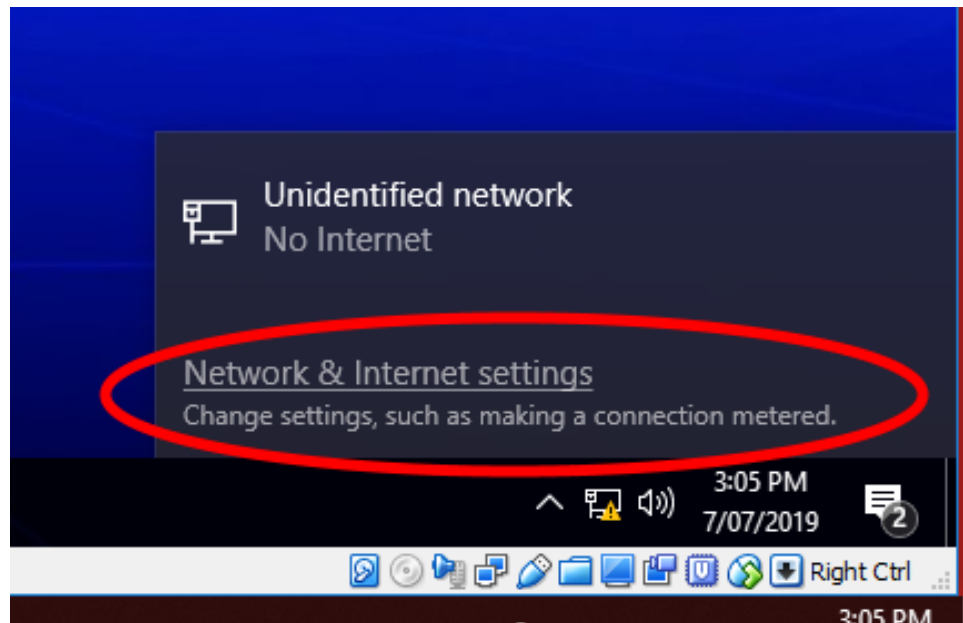


### Step 2: Configure static IP address information on the PCs.

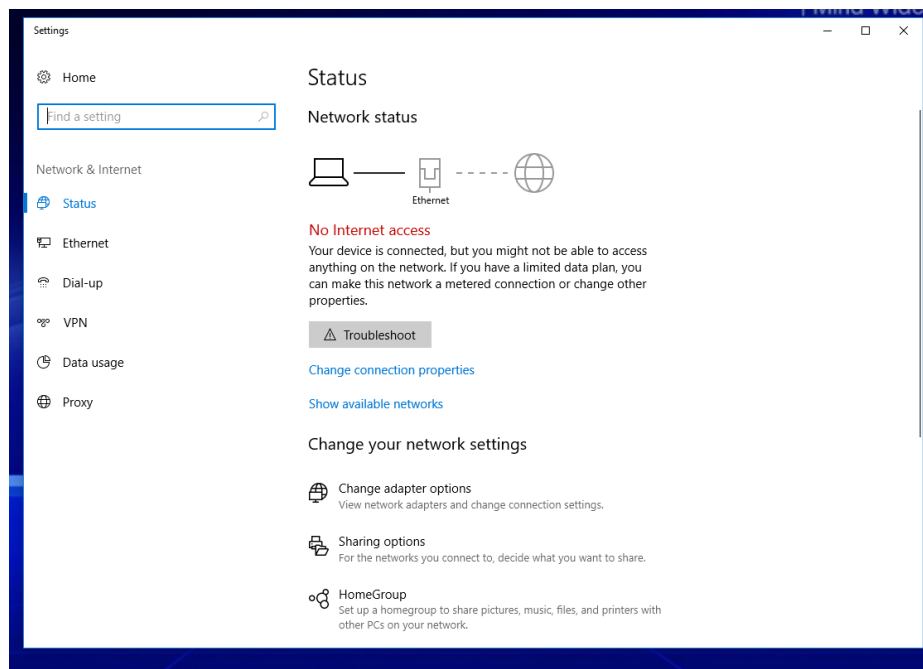
a. In the Virtual machine, left-click the Network Internet access icon:



- b. Click on the Network & Internet Settings popup.



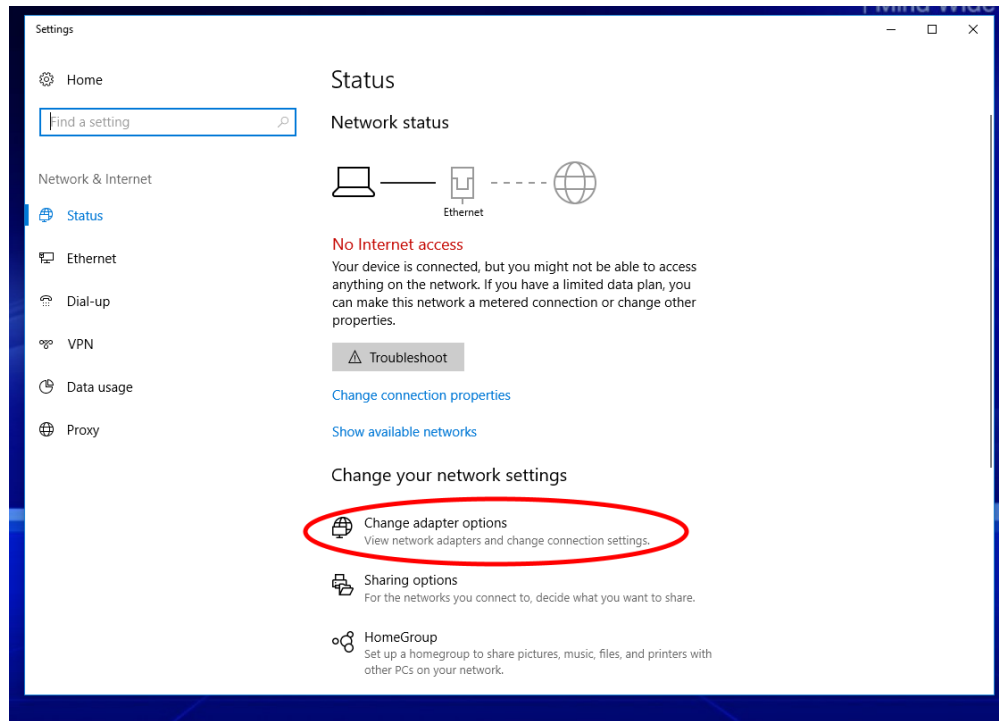
- c. You should now see the following screen, do not navigate away from the Status tab.



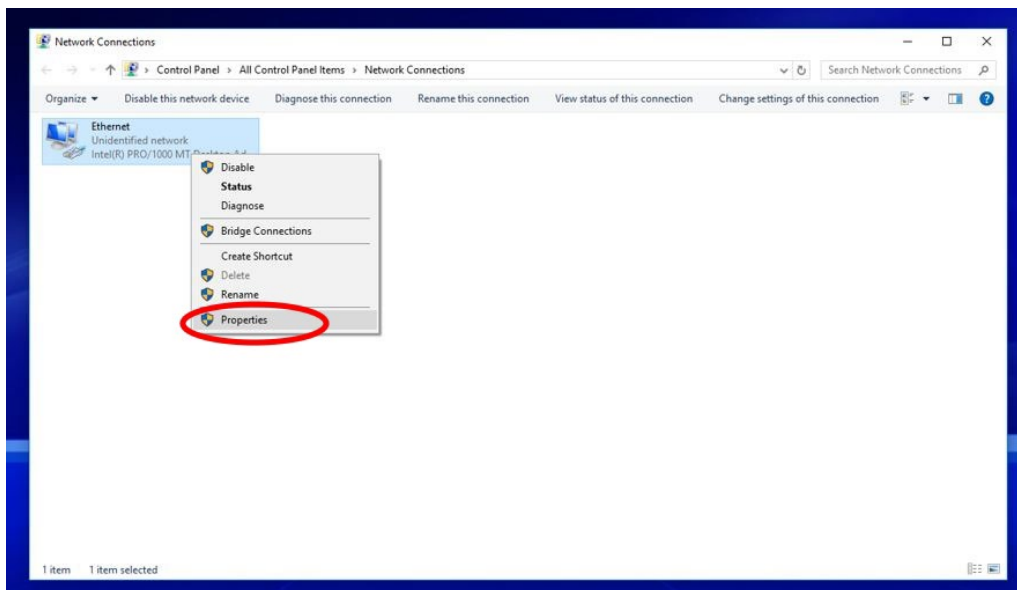


## Lab - Building a Simple Network

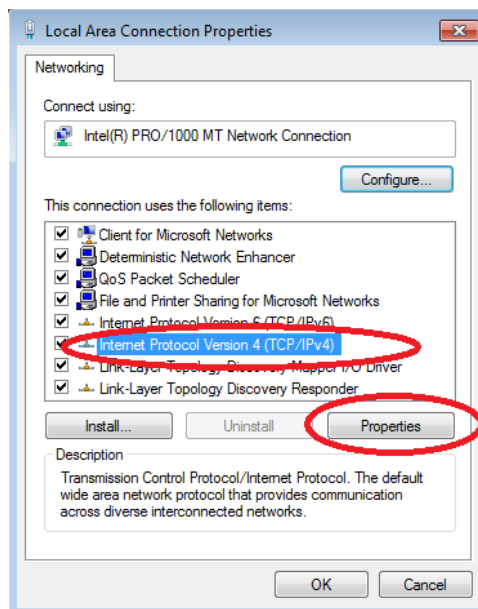
- d. At the bottom of the middle pane of the status tab, click the **Change adapter options** link.



- e. The Network Connections window displays the available interfaces on the PC. Right-click the **Ethernet** interface and select **Properties**.

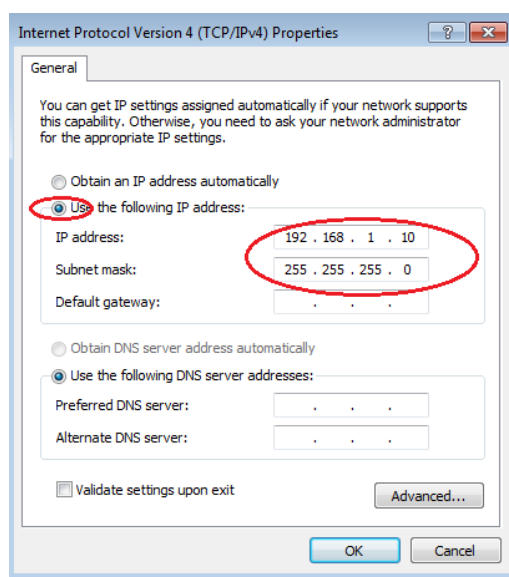


- f. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



**Note:** You can double-click **Internet Protocol Version 4 (TCP/IPv4)** to display the Properties window.

- g. Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.



**Note:** In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B's IP address information.

- h. After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter. Note that you must press OK twice before the configuration will be applied. Before this, the IP address is not assigned to the PC.
- i. Repeat the previous steps to enter the IP address information for PC-B.

### Step 3: Verify PC settings and connectivity.

In the virtual machine, use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

- From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, press Enter. Alternatively, you can double-click on the command prompt icon on the virtual machine desktop.
- the cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.



```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC-A
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-50-56-BE-6C-89
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:185a%11(Preferred)
    IPv4 Address. . . . . : 192.168.1.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
    DHCPv6 IAID . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- Type **ping 192.168.1.11** and press Enter.

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

Were the ping results successful? \_\_\_\_\_

If not, troubleshoot as necessary.

**Note:** If you did not get a reply from PC-B, try to ping PC-B again. If you still do not get a reply from PC-B, try to ping PC-A from PC-B. If you are unable to get a reply from the remote PC, then have your instructor help you troubleshoot the problem.

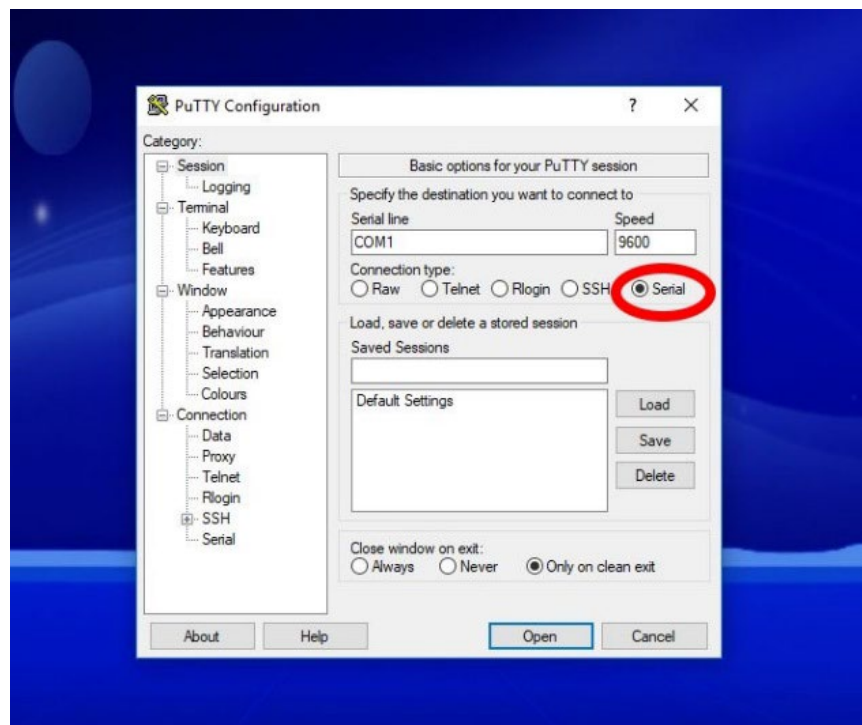
## Part 4: Configure and Verify Basic Switch Settings

### Step 1: Console into the switch.

In part 1, you connected PC-A to the Console input on Switch S1. You will now use a terminal program to connect to Switch S1 and configure it using the console connection from PC-A to Switch S1.

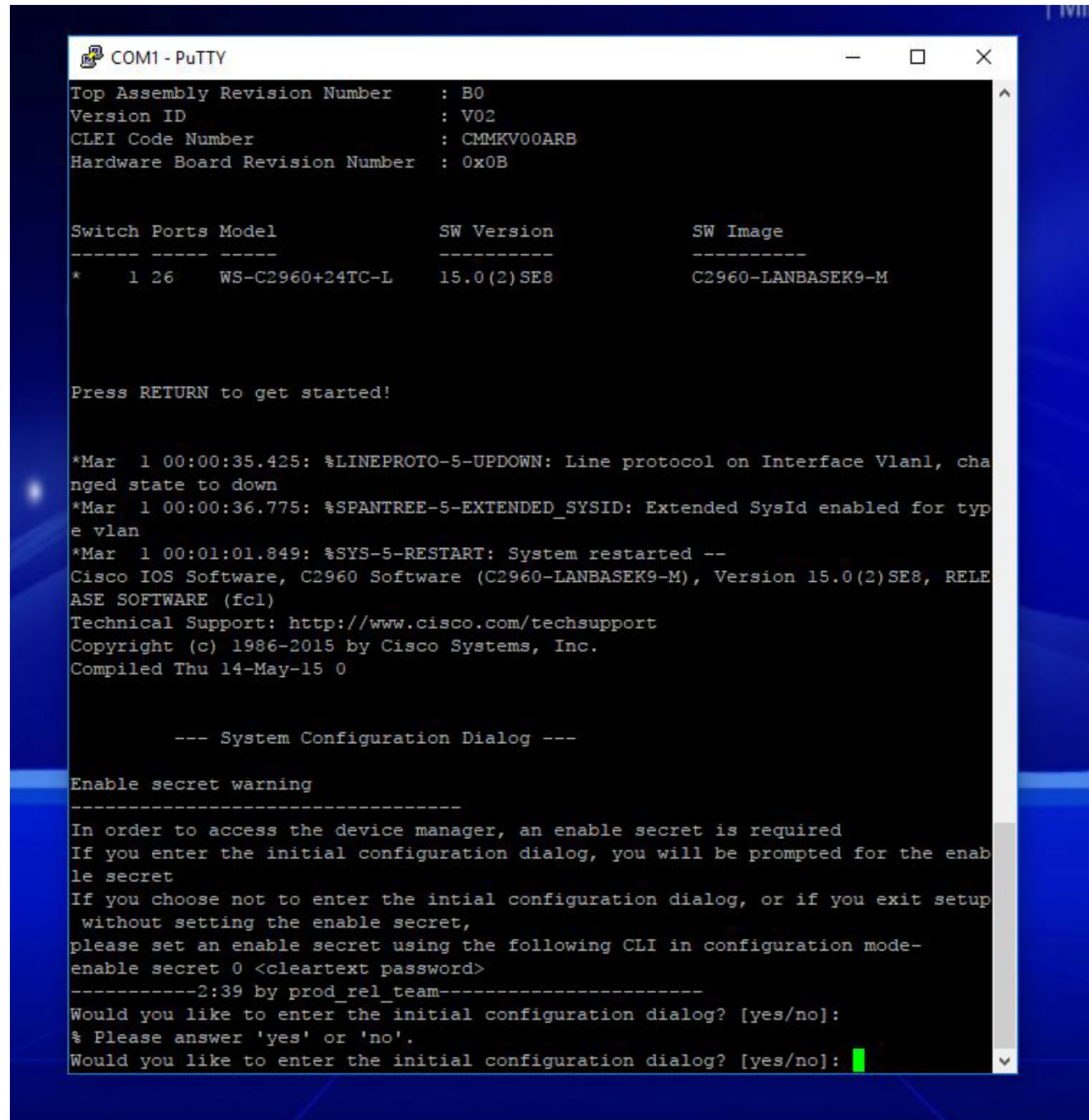
**Note: If the Switch has already been configured previously (for example it has a name that is not 'Switch', see your tutor and refer to Appendix A to clear and reload it.**

Using PuTTY or Tera Term, establish a console connection to the switch from PC-A. Select Serial as Connection type, and click on Open.



## Lab - Building a Simple Network

A new window will open into which you can type commands to the device on the other end of the console cable (in this case the switch). Note: You may have to hit enter once or twice to wake up the device.



```
COM1 - PuTTY
Top Assembly Revision Number : B0
Version ID : V02
CLEI Code Number : CMMKV00ARB
Hardware Board Revision Number : 0x0B

Switch Ports Model          SW Version  SW Image
-----
*  1 26   WS-C2960+24TC-L  15.0(2)SE8  C2960-LANBASEK9-M

Press RETURN to get started!

*Mar  1 00:00:35.425: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar  1 00:00:36.775: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Mar  1 00:01:01.849: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE8, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 14-May-15 0

--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the initial configuration dialog, or if you exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----2:39 by prod_rel_team-----
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]:
```

Depending on the state of the device, you may need to work through one or more prompts:

The above image shows the initial configuration dialog prompt.

**IMPORTANT:** If you see this prompt when you console to the Switch, enter “No” to skip this step as we will be configuring the switch manually (see diagram on next page for example output).

```

COM1 - PuTTY
Version ID : V02
CLEI Code Number : CMMKV00ARB
Hardware Board Revision Number : 0x0B

Switch Ports Model          SW Version  SW Image
-----
*    1 26    WS-C2960+24TC-L    15.0(2)SE8    C2960-LANBASEK9-M

Press RETURN to get started!

*Mar  1 00:00:35.425: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to down
*Mar  1 00:00:36.775: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for typ
e vlan
*Mar  1 00:01:01.849: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE8, RELE
ASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 14-May-15 0

--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enab
le secret
If you choose not to enter the initial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----2:39 by prod_rel_team-----
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>

```

### Step 2: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

```

Switch> enable
Switch#

```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

### Step 3: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#
```

Note: The prompt changed to reflect global configuration mode. You can use **'exit'** to go back one level, or **'end'** to go back to privileged exec mode directly. In this case **exit** would take you back to the privileged exec mode from Step 2 with prompt: Switch#

### Step 4: Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1  
S1(config)#
```

### Step 5: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup  
S1(config)#
```

### Step 6: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured and a login is required on the console line (con 0).

Set the enable secret password:

```
S1(config)# enable secret class
```

Configure the console line:

```
S1(config)# line con 0  
S1(config-line)# password cisco  
S1(config-line)# login  
S1(config-line)# exit  
S1(config)#
```

To prevent the switch from interrupting you when typing commands, turn on synchronous logging from within the console line configuration.

```
S1(config)# line con 0  
S1(config-line)# logging synchronous  
S1(config-line)# exit  
S1(config)#
```



### Step 7: Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the **single quote** ', are often used. Note that the banner and its text are a single line, there is no enter between the words "and" and "prosecuted" in the example below:

```
S1(config)# banner motd 'Unauthorised access is strictly prohibited and
prosecuted to the full extent of the law.'
S1(config)# exit
S1#
```

### Step 8: Display the current configuration.

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging when you see the "- - More -" prompt. The commands configured in Steps 1 – 8 are highlighted below.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!

<output omitted>

!
banner motd ^C
```



```
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  login
line vty 5 15
  login
!
end

S1#
```

### Step 9: Display the IOS version and other useful switch information.

Use the **show version** command to display the IOS version that the switch is running, along with other useful information. Again, you will need to use the spacebar to advance through the displayed information.

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fcl)

S1 uptime is 1 hour, 38 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:  
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

```
cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.
```

```
Processor board ID FCQ1628Y5LE
```

```
Last reset from power-on
```

```
1 Virtual Ethernet interface
```

```
24 FastEthernet interfaces
```

```
2 Gigabit Ethernet interfaces
```

```
The password-recovery mechanism is enabled.
```

```
64K bytes of flash-simulated non-volatile configuration memory.
```

```
Base ethernet MAC Address      : 0C:D9:96:E2:3D:00
```

```
Motherboard assembly number    : 73-12600-06
```

```
Power supply part number       : 341-0097-03
```

```
Motherboard serial number      : FCQ16270N5G
```

```
Power supply serial number     : DCA1616884D
```

```
Model revision number          : R0
```

```
Motherboard revision number    : A0
```

```
Model number                   : WS-C2960-24TT-L
```

```
System serial number           : FCQ1628Y5LE
```

```
Top Assembly Part Number       : 800-32797-02
```

```
Top Assembly Revision Number   : A0
```

```
Version ID                     : V11
```

```
CLEI Code Number               : COM3L00BRF
```

```
Hardware Board Revision Number : 0x0A
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0 (2) SE	C2960-LANBASEK9-M

```
Configuration register is 0xF
```

```
S1#
```

### Step 10: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command. Press the spacebar to advance to the end of the list.

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down

## Lab - Building a Simple Network

```
FastEthernet0/11    unassigned    YES unset    down          down
FastEthernet0/12    unassigned    YES unset    down          down
FastEthernet0/13    unassigned    YES unset    down          down
FastEthernet0/14    unassigned    YES unset    down          down
FastEthernet0/15    unassigned    YES unset    down          down
FastEthernet0/16    unassigned    YES unset    down          down
FastEthernet0/17    unassigned    YES unset    down          down
FastEthernet0/18    unassigned    YES unset    down          down
FastEthernet0/19    unassigned    YES unset    down          down
FastEthernet0/20    unassigned    YES unset    down          down
FastEthernet0/21    unassigned    YES unset    down          down
FastEthernet0/22    unassigned    YES unset    down          down
FastEthernet0/23    unassigned    YES unset    down          down
FastEthernet0/24    unassigned    YES unset    down          down
GigabitEthernet0/1  unassigned    YES unset    down          down
GigabitEthernet0/2  unassigned    YES unset    down          down
S1#
```

### Step 11: Repeat Steps 1 to 12 to configure switch S2.

The only differences for this step are to connect PC-A to the console port of Switch S2 (just move the cable on the Switch side) and when configuring Switch S2 to change the hostname to S2.

### Step 12: Record the interface status for the following interfaces.

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1				
F0/6				
F0/18				
VLAN 1				

Why are some FastEthernet ports on the switches up and others are down?

---

---

### Reflection

What could prevent a ping from being sent between the PCs?

---

**Note:** It may be necessary to disable the PC firewall to ping between PCs.

**Ask your workshop tutor to check your work as you go and before leaving the class.**

**DO NOT TURN OFF the equipment until you have received feedback.**