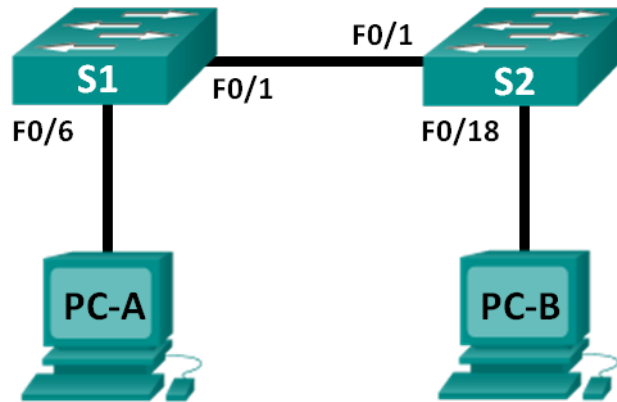


Lab - Building a Simple Network

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: Set Up the Network Topology (Ethernet only)

Part 2: Configure PC Hosts

Part 3: 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 also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

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 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Set Up the Network Topology (Ethernet only)

In Part 1, 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.

- a. 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.
- b. 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.

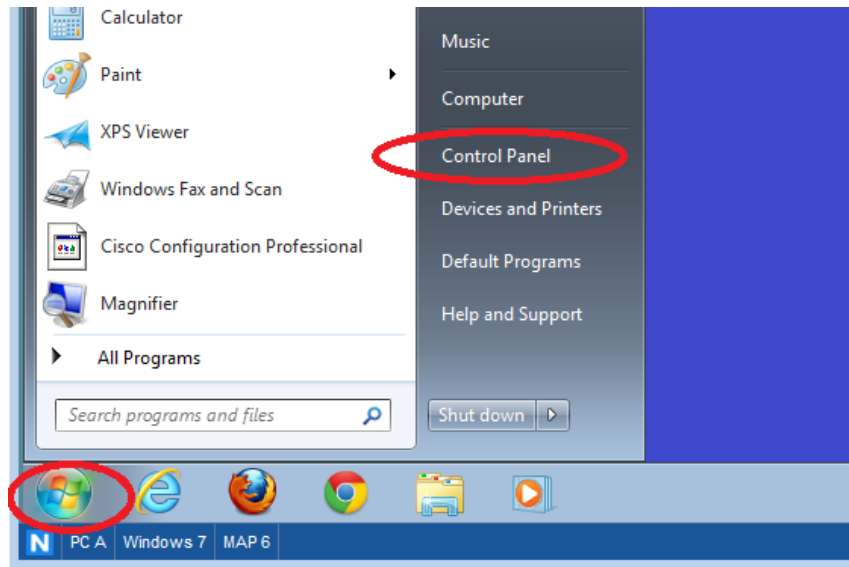
Step 4: Visually inspect network connections.

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 2: Configure PC Hosts

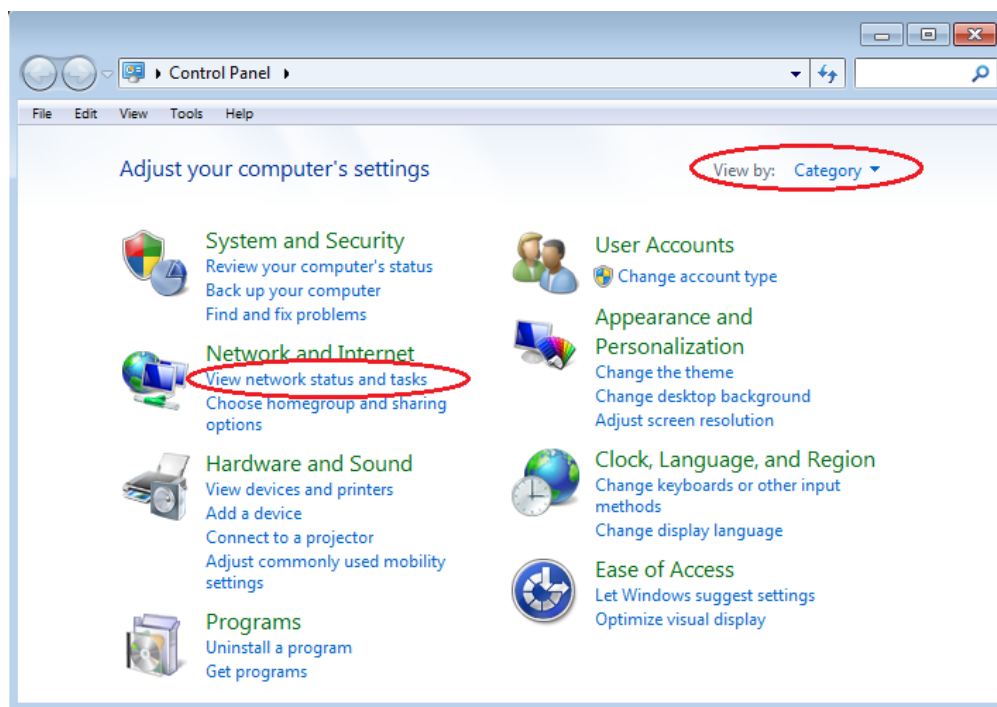
Step 1: Configure static IP address information on the PCs.

- a. Click the **Windows Start** icon and then select **Control Panel**.

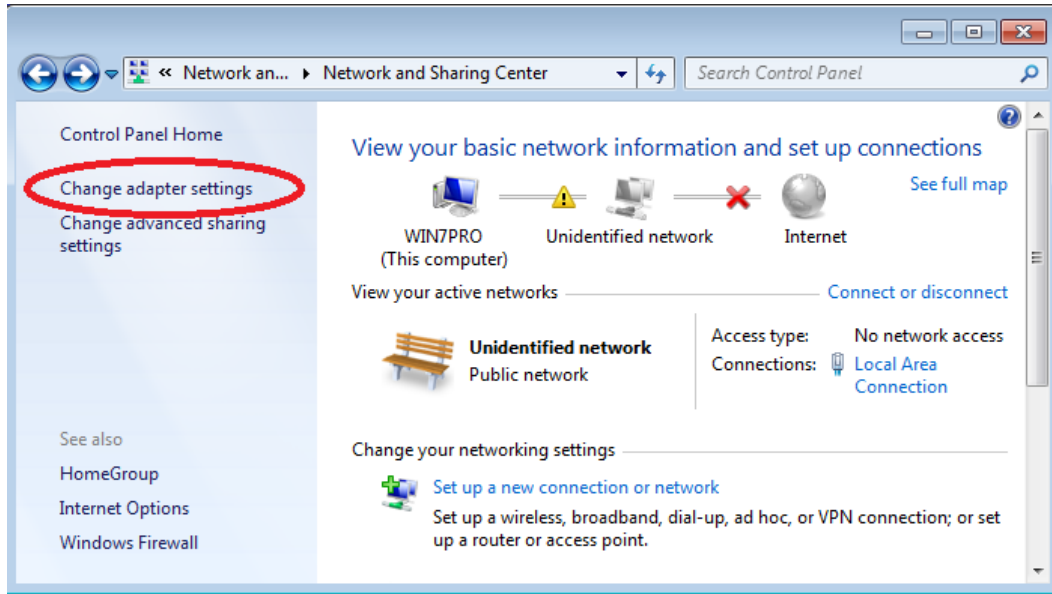


- b. In the Network and Internet section, click the **View network status and tasks** link.

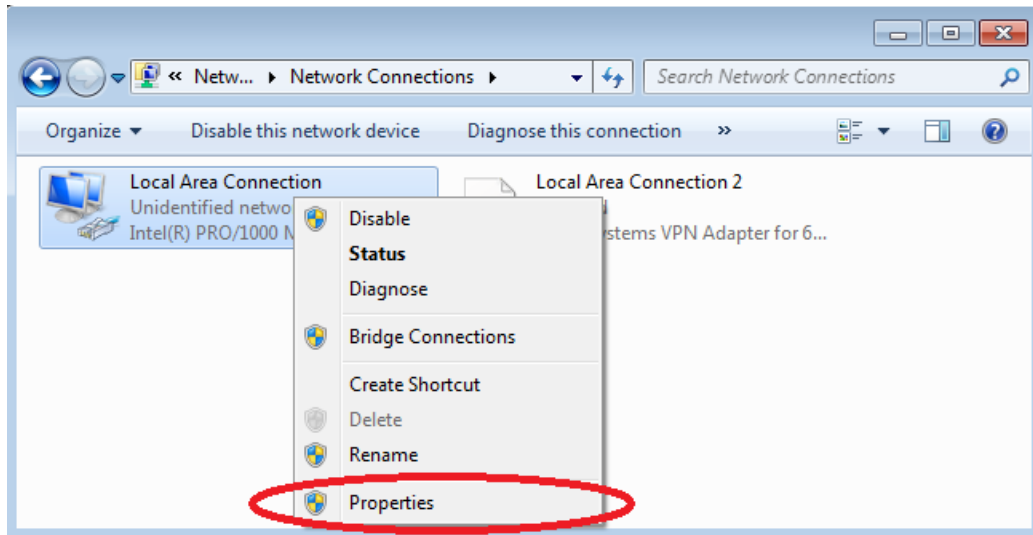
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by:** and change this option to display by **Category**.



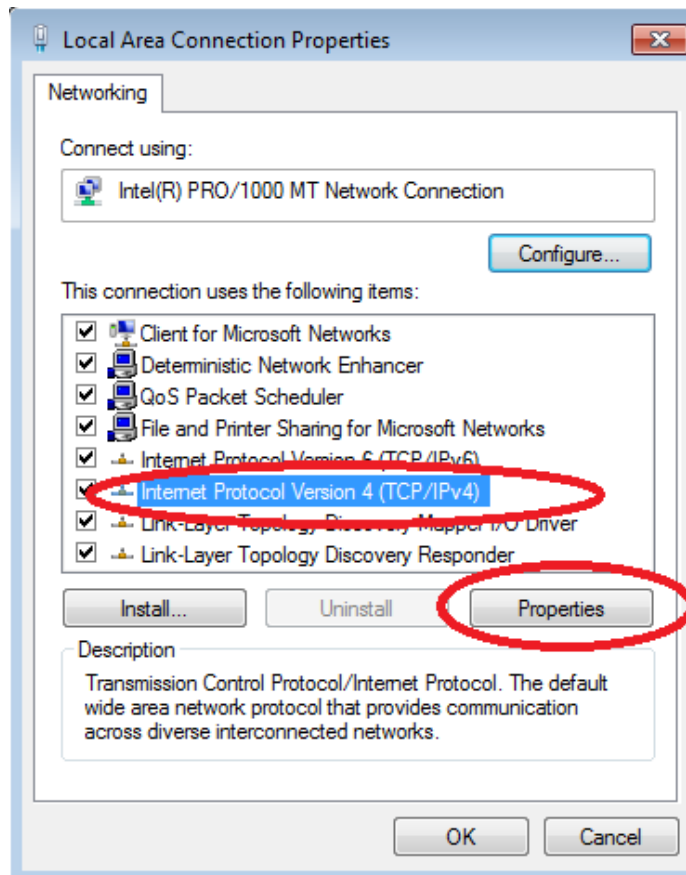
- c. In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



- d. The Network Connections window displays the available interfaces on the PC. Right-click the **Local Area Connection** interface and select **Properties**.

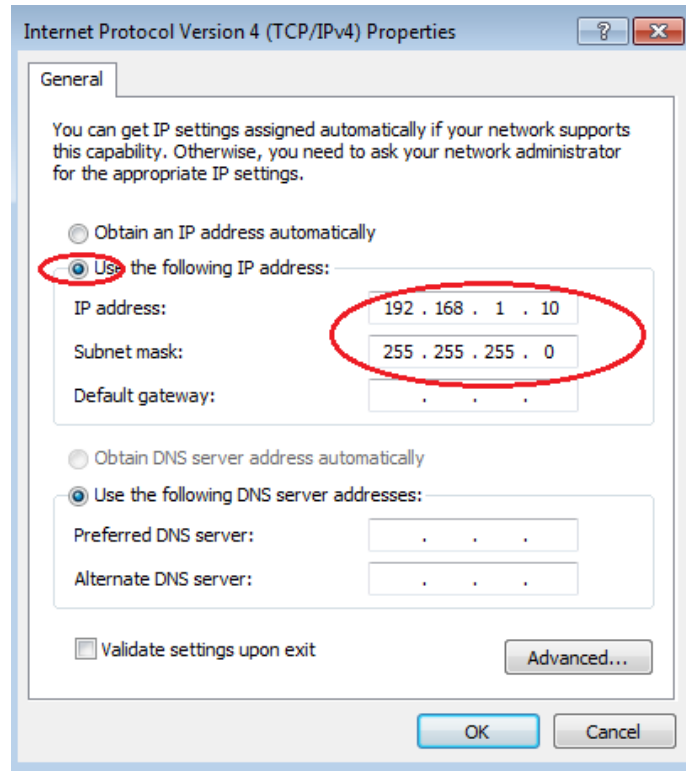


- e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



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

- f. 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.

- g. 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.
- h. Repeat the previous steps to enter the IP address information for PC-B.

Step 2: Verify PC settings and connectivity.

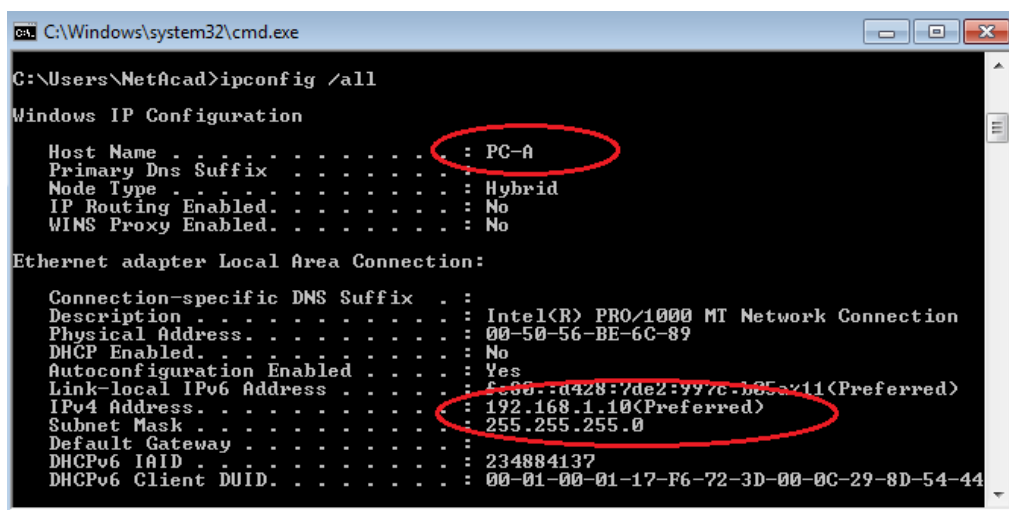
Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

- a. From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



Lab - Building a Simple Network

- b. 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

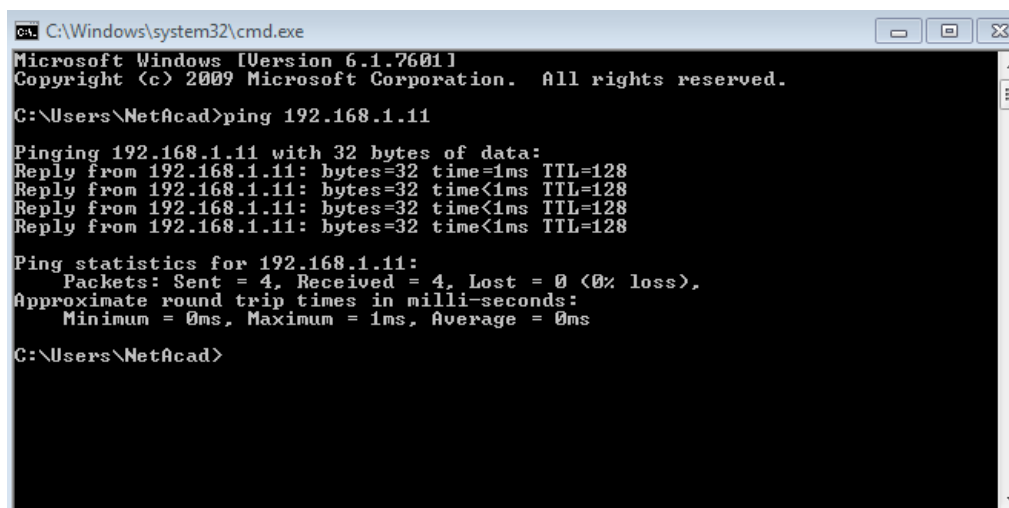
Windows IP Configuration

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 . . . . . : 234884137
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- c. 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?

The ping was successful on the first attempt after carefully checking that the ports and IP configurations were set correctly. I know the ping was successful as I had a reply from 192.168.1.11.

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 3: Configure and Verify Basic Switch Settings

Step 1: Console into the switch.

Using Tera Term, establish a console connection to the switch from PC-A.

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)#
```

The prompt changed to reflect global configuration mode.

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.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
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 **#**, are often used.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full extent
of the law. #
S1(config)# exit
S1#
```

Step 8: Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Step 9: 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. 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/kLkDq9BGho1QM5EnRtoyr8cHAUg.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  
login  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end  
  
S1#
```

Step 10: 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 (fc1)  
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  
(fc1)  
  
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>

Lab - Building a Simple Network

If you require further assistance please contact us by sending email to 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 11: 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

Lab - Building a Simple Network

```
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
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 12: Repeat Steps 1 to 12 to configure switch S2.

The only difference for this step is to change the hostname to S2.

Step 13: Record the interface status for the following interfaces.

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1	Up	Up	Up	Up
F0/6	Up	Up	Down	Down
F0/18	Down	Down	Up	Up
VLAN 1	Administratively Down	Down	Administratively Down	Down

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

By default, the ports are always down until cables are connected to the ports. We have connected cables only to the ports that show as 'Up', which would prove that it is the case.

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

Many things could prevent a ping from being sent between the PCs, including the incorrect configuration of IP address on either/both of the PCs, incorrect cables being used between the PCs and switches (cross over instead of straight through) or incorrect cables between the two switches. If an

incorrect IP address was entered, or ports were shut down, they would also prevent a ping from being sent. The use of firewalls may also prevent a ping being sent if they are blocked by the firewall.

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

Appendix A: Initializing and Reloading a Switch

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

```
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

Step 3: Delete the VLAN file.

- If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
```

```
Erase of nvram: complete  
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload  
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no  
Switch>
```

Reflection (Max word count 200):

Write your reflection based on what you learned from this activity. This could include operation of Switch, configs and testing network connectivity.

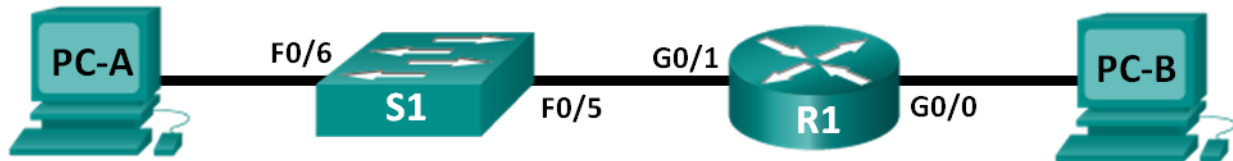
During this lab I learned how to add basic security to a switch through the use of local passwords and how to encrypt these passwords using the service command, along with how to set a login banner to warn users that unauthorized access is not prohibited. I learned how to set host names for both switches and also applied IP addresses and subnet masks which were necessary for the PCs to be able to communicate. I was then able to verify the connection of the PCs by using a PING from PC-A to PC-B and then vice versa. During this I also learned that by using a firewall, a PING can be blocked, however a firewall was not used in this lab.

I also learned how to use show commands to display the switch configurations, their IOS versions and the interface status. Whilst looking at the interface statuses for both switches, I noticed that all ports were down, except the ones which had cables connected, which showed that the ports become 'up' automatically on connection without the need to run the 'no shutdown' command.

After this I learned how to save running configurations to an area of flash memory called Non-volatile Random Access Memory (NVRAM) so that they can be applied again.

Lab - Building a Switch and Router Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Display Device Information

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. Test your knowledge by trying to configure the devices without referring to the content or previous activities.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, 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. Refer to the **Error! Reference source not found.** at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

- a. Attach the devices shown in the topology diagram, and cable, as necessary.
- b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their basic configurations.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Assign static IP information to the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.
- c. Ping PC-B from a command prompt window on PC-A.

Why were the pings not successful?

The routing is not set up between the devices therefore they are unable to communicate. IP addresses and default gateways must first be configured.

Step 2: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the router.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.
- f. Assign **cisco** as the console password and enable login.

- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the clear text passwords.
- i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate both interfaces on the router.
- k. Configure an interface description for each interface indicating which device is connected to it.
- l. Save the running configuration to the startup configuration file.
- m. Set the clock on the router.

Note: Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

- n. Ping PC-B from a command prompt window on PC-A.

Were the pings successful? Why?

At first the pings were not successful. I realized this was because I had enabled the two interfaces (gigabit ethernet 0/0 and 0/1) on the router but had not configured the IP addresses for them. After I configured the IP addresses I tried to ping them again. However, after troubleshooting I noticed that I had also not set the default gateways for both PCs.

After setting them I tried to ping PC-B once more and this time it was successful.

Part 3: Display Device Information

In Part 3, you will use **show** commands to retrieve information from the router and switch.

Step 1: Retrieve hardware and software information from the network devices.

- a. Use the **show version** command to answer the following questions about the router.

What is the name of the IOS image that the router is running?

System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"

How much DRAM memory does the router have?

DRAM configuration is 64 bits wide with parity disabled.

How much NVRAM memory does the router have?

255K bytes of non-volatile configuration memory.

How much Flash memory does the router have?

249856K bytes of ATA System CompactFlash 0 (Read/Write)

- b. Use the **show version** command to answer the following questions about the switch.

What is the name of the IOS image that the switch is running?

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)

How much dynamic random access memory (DRAM) does the switch have?

21039K bytes of memory.

How much nonvolatile random-access memory (NVRAM) does the switch have?

63488K bytes of flash-simulated non-volatile configuration memory.

What is the model number of the switch?

WS-C2960-24TT

Step 2: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

What code is used in the routing table to indicate a directly connected network? - **C**

How many route entries are coded with a C code in the routing table? - **2**

What interface types are associated to the C coded routes?

The Router on Gigabit Ethernet

Step 3: Display interface information on the router.

Use the **show interface g0/1** to answer the following questions.

What is the operational status of the G0/1 interface?

GigabitEthernet0/1 is up, line protocol is up (connected).

What is the Media Access Control (MAC) address of the G0/1 interface?

The address is 0004.9aad.2002.

How is the Internet address displayed in this command?

Internet address is 192.168.1.1/24.

Step 4: Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

- a. Enter the **show ip interface brief** command on the router.

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0       192.168.0.1     YES manual  up              up
GigabitEthernet0/1       192.168.1.1     YES manual  up              up
Serial0/0/0              unassigned      YES unset  administratively down down
Serial0/0/1              unassigned      YES unset  administratively down down
R1#
```

- b. Enter the **show ip interface brief** command on the switch.

```
Switch# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Vlan1                   unassigned      YES manual  up              up
FastEthernet0/1         unassigned      YES unset  down            down
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	up	up
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
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

Switch#

Reflection

1. If the G0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

The command to be used would be 'no shutdown' once on the G0/1 interface.

2. What would happen if you had incorrectly configured interface G0/1 on the router with an IP address of 192.168.1.2?

The router would be unable to connect, and would have to be re-configured using the correct IP address of 192.168.1.1.

3. Explain the operation of a Router and a Switch.

The operation of a router is to connect computer networks, such as connecting a home network to the internet. Routers work by transferring packets of data between networks to establish and sustain communication between two nodes. They operate at Layer 3 (network) of the OSI model. Routers use destination IP addresses in the data packet to determine the forwarding address [1].

The operation of a network switch is to connect devices together on a single network or LAN. Unlike routers, switches use MAC addresses to forward data and use packet switching to receive, process and forward data. Switches can either operate on Layer 2 (data link) or Layer 3 (network) of the OSI model [2].

Notes:

Default gateway – now have 2 subnets so we used a router to connect and make 1 network. Default gateway sets the route between the sub networks.

References:

[1] "Router Operation", *Erg.abdn.ac.uk*, 2019. [Online]. Available: <https://erg.abdn.ac.uk/users/gorry/course/inet-pages/router-opn.html>. [Accessed: 25- Nov- 2019].

[2] Cisco, "How Does a Switch Work? Learn How to Setup a Network", *Cisco*, 2019. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html>. [Accessed: 25- Nov- 2019].

Lab: IPv4, Subnetting, VLSM and IPv6 Addressing

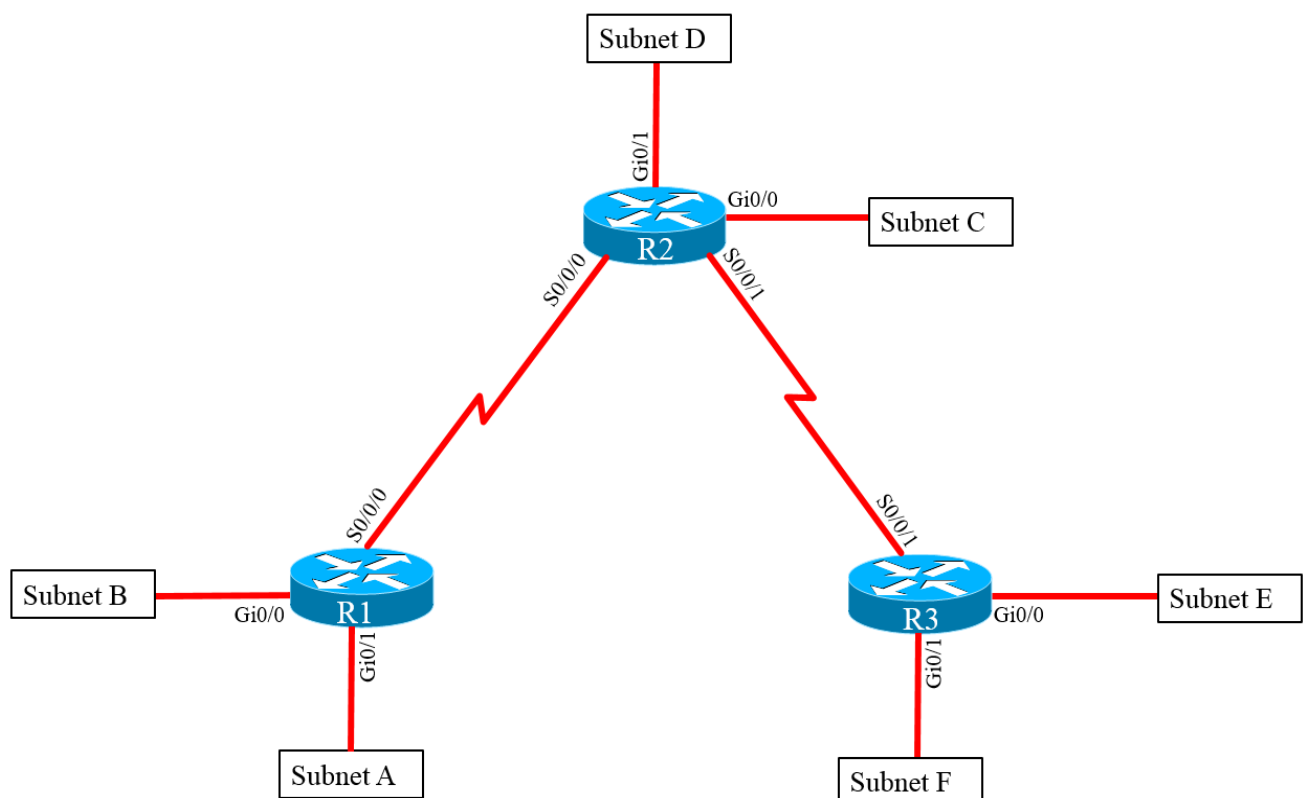
Part 1: Understanding IPv4 and IPv6 addressing (word count 1000)

This part of lab worksheet require you research and write a report on **“Features of IPv6”**. You may discuss but not limited to structure, address types, advanced functionalities and security.

Please See Appendix A for the report, titled “Features of IPv6”.

Part 2: Subnetting and VLSM

NOTE: To complete this part you would need full understanding of Lab 10 to 14.



Using the Network address 172.16.2.0/24 (ignore the /24 as noted by Lecturer), VLSM the network to support the following requirements:

Subnet A: 16 hosts

Subnet B: 2000 hosts

Subnet C: 6 hosts

Subnet D: 500 hosts

Subnet E: 60 hosts

Subnet F: 180 hosts and Serial links between routers

Table 1

Subnet	Network Address	Subnet mask	First Address	Last Address	Broadcast Address
B (2000 hosts)	172.16.2.0 /21	255.255.248.0	172.16.2.1	172.16.9.254	172.16.9.255
D (500 hosts)	172.16.10.0 /23	255.255.254.0	172.16.10.1	172.16.11.254	172.16.11.255
F (180 hosts)	172.16.12.0 /24	255.255.255.0	172.16.12.1	172.16.12.254	172.16.12.255
E (60 hosts)	172.16.13.0 /26	255.255.255.192	172.16.13.1	172.16.13.62	172.16.13.63
A (16 hosts)	172.16.13.64 /27	255.255.255.224	172.16.13.65	172.16.13.94	172.16.13.95
C (6 hosts)	172.16.13.96 /29	255.255.255.248	172.16.13.97	172.16.13.102	172.16.13.103
F Serial Link R1 to R2	172.16.13.104 /30	255.255.255.252	172.16.13.105	172.16.13.106	172.16.13.107
F Serial Link R2 to R3	172.16.13.108/30	255.255.255.252	172.16.13.109	172.16.13.110	172.16.13.111

Appendix A

Report: Features of IPv6 below.



FEATURES OF IPV6

BSc Computing Portfolio
Computer Architecture and Networks | ACCD4001

Siobhan Kelly Stephens
1800709

1. Introduction

The internet protocol, or IP are a set of rules governing the routing and addressing of data packets sent over the internet, which enables internetworking and forms the basis of the internet. It has the task of delivering packets from a source host to a destination host using IP addresses [1]. The IP defines addressing methods and packet structure that encapsulate the data to be sent, in the Network (3rd) layer of the OSI model [2].

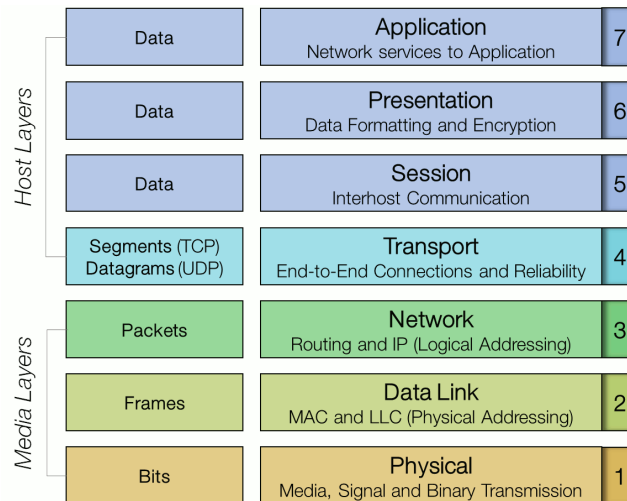


FIGURE 1. OSI MODEL - [3] [4]

IPv4, which was introduced in 1983 has been proven as a robust addressing protocol [5]. It uses 32-bit IP addresses to allow for a maximum of 4,294,967,296 addresses. However, over the years with the increased adoption of technology in everyday life through the Internet of Things, IP addresses began to run out.

According to Statistica [6], there are approximately 26.6 billion internet connected devices in 2019, and this is estimated to rise to 75.4 billion by 2025, therefore, the number of IPv4 addresses is not great enough. Although the shortage of IPv4 addresses began many years ago, the adoption of technology such as Carrier Grade Network Address Translation (CGN) has greatly increased the lifespan of IPv4. Carrier grade NAT translates private IP addresses within an ISP's network to a smaller number of public IP addresses, similarly to how individuals and organizations use NAT to translate a public IP for multiple internal private IP addresses [7].

As a result of the IPv4 address shortage, in 1998, the Internet Engineering Task Force (IETF) created Internet Protocol version 6. IPv6 has been designed to incorporate all possible future requirements of the Internet. The main improved feature of IPv6 over IPv4, is its amount of logical address space.

As of November 1st 2019, the percentage of users accessing google over IPv6 was 27%, and is growing quickly considering this number was only 5% in January 2015 [8].

2. Features of IPv6

As discussed in section 1, the creation of IPv6 was necessary due to the saturation of IPv4 addresses. Other points that have been improved on are simplification of the packet header, improved support for extensions and options, improved security and authentication and new traffic flow labelling capabilities. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 2460 [9].

2.1 IPv6 Structure

An IPv6 address is made of 128 bits, divided into 16-bit blocks and allows for approximately 3.4×10^{38} or 340 trillion, trillion, trillion addresses. Each block is converted into a 4-digit Hexadecimal number and is separated by colons. As an IPv6 address is long, rules such as omitting leading zeros and omitting blocks of consecutive zeros are used to shorten the address [10].

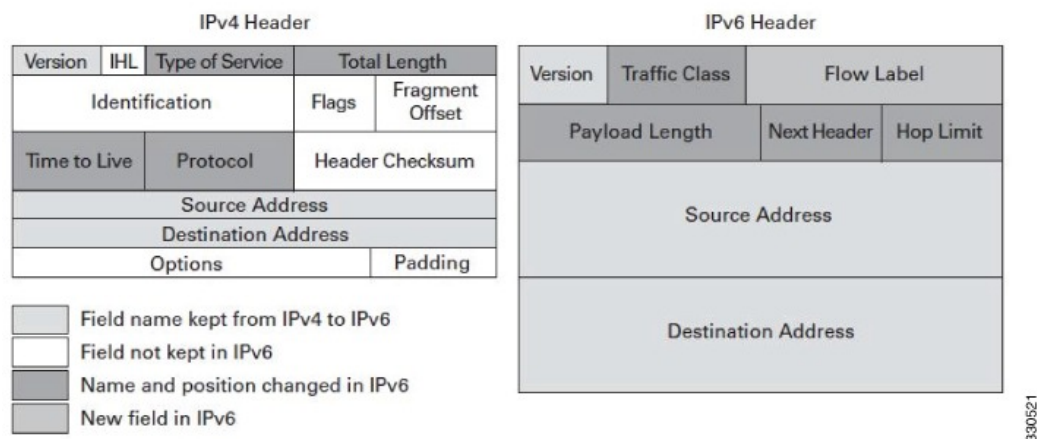


FIGURE 2. COMPARISON OF IPV4 AND IPV6 HEADERS [11].

IPv6's headers have been highly simplified and have removed unnecessary information and options present in previous version's headers. Unlike variable length IPv4 headers which range from 20 to 60 bytes, IPv6 headers are a fixed length of 40 bytes meaning that fields such as total length (IPv4) are redundant, and instead now only payload length must be used [9]. IPv6 headers can include optional extension headers. The extension header may contain information that can help routers understand how to handle the given packet or flow. IPv4 provides only 40-bytes for options however IPv6 is extensible to allow as much options as the size of the packet itself [10].

2.2 Security Improvements

The enormous address space covered by IPv6 makes port scanning far more difficult than IPv4 for attackers that may want to scan the ports of a victim's network in order to gather information on it [12].

In IPv4, the only security feature offered is a security option field as IP Security or IPSec was an optional aspect of IPv4 that is now mandatory. IPSec provides authenticity, confidentiality, integrity and access control to each IP packet through both Encapsulating Security Payload (ESP) and Authentication Header (AH) [13].

Address Resolution Protocol has been replaced in IPv6 by Neighbor Discovery (ND) Protocol. ARP suffers from vulnerabilities such as ARP Spoofing, where an attacker exploits the interaction of IP and ethernet protocols by sending forged ARP reply packets to the victim [14]. ARP attacks can allow attackers to the system which can then leave it vulnerable to other attacks including Man-in-the-Middle attacks and session hijacking [14]. In the IPv6 protocol, the ID portion of a layer 3 address is directly derived from a device's layer 2 MAC address and therefore ARP is redundant.

IPv6 has also introduced the possibility of binding a public signature key to an IPv6 address resulting in a Cryptographically Generated Address (CGA), which provides additional security by allowing the user to provide a 'proof of ownership' for a particular IPv6 address and aims to prevent spoofing attacks.

Despite improved security, IPv6 cannot prevent attacks on layers above the network layer [12].

2.3 Addressing Modes

IPv6 supports three different addressing modes. Firstly, Unicast. A unique unicast address acts as an identifier for a single host. The IP packet contains both source and destination addresses, and the packet is delivered to the interface identified by that address [15].

Next, a multicast address acts as an identifier for a pre-defined group of interfaces. An IP packet destined for a multicast address is delivered to the multiple interfaces of that group [15].

Finally, new to IPv6 are anycast addresses. In this addressing mode, multiple hosts are assigned the same Anycast IP address. When a host wants to communicate with another host with an Anycast IP, it sends a Unicast message. With the help of complex routing mechanisms, the Unicast message is delivered to the host closest to the Sender in terms of Routing cost [16].

2.3 Transition from IPv4 to IPv6

Currently, there is a main barrier preventing the complete transitioning from IPv4 to IPv6, which is that IPv6 is not backward compatible. This is unlike most other technologies which allow backward compatibility to ensure a smooth transition and means that multiple technologies must be used, such as Dual Stack Routers.

Dual Stack Routers can be configured with both IPv4 and IPv6 addresses to provide a medium for hosts to access the server without changing their respective IP versions [17].

Where different IP versions exist on transit networks, tunneling provides a solution where a user's data can pass through a non-supported IP version, such as from IPv4 to IPv6 or vice versa [18].

Another method of transitioning to IPv6 is by the use of NAT-PT, or Network Address Translation – Protocol Translation enabled device. A NAT-PT device takes an IPv4 packet, removes the IPv4 header and adds an IPv6 header, then passes it through the internet. When a response from an IPv6 server comes for the IPv4 host, the router does the opposite [19].

3. Conclusion

IPv6 aims to provide enough addresses for the foreseeable future and also incorporates new and improved features as discussed in this report such as IPSec and improved performance.

IPv4 is still used in the large majority of the internet however due to the issues with IPv4 outlined above IPv6 adoption is increasing at a fast pace. On 6th June 2012, all major ISP's were shifted to IPv6 during "World IPv6 Launch" however others are still to follow [20].

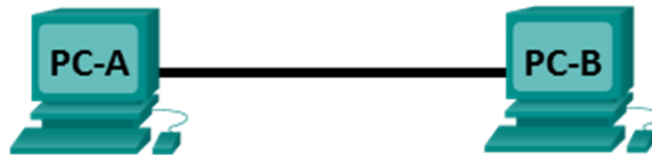
For a full transition over to IPv6, it must be implemented end to end, meaning it must be enabled by network hardware vendors, transit providers, access providers, content providers and endpoint hardware makers [21], which is still likely to take many years.

4. References

- [1] H. Frystyk, "The Internet Protocol Stack," 1994. [Online]. Available: <https://www.w3.org/People/Frystyk/thesis/TcpIp.html>. [Accessed: 01-Dec-2019].
- [2] W. R. Parkhurst, *Routing first-step*. Cisco, 2004.
- [3] Cisco, "Cisco Networking Fundamentals," 2006.
- [4] C. Goedegebure, "The OSI Model." [Online]. Available: <https://www.coengoedegebure.com/osi-model/>. [Accessed: 01-Dec-2019].
- [5] Cloudflare, "What is the Internet Protocol? | Cloudflare." [Online]. Available: <https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/>. [Accessed: 01-Dec-2019].
- [6] Statistica, "IoT: number of connected devices worldwide 2012-2025." [Online]. Available: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>. [Accessed: 01-Dec-2019].
- [7] Lee Schlesinger, "Whatever happened to the IPv4 address crisis?," 2014. [Online]. Available: <https://www.networkworld.com/article/2174297/whatever-happened-to-the-ipv4-address-crisis-.html>. [Accessed: 01-Dec-2019].
- [8] Google, "IPv6 – Google." [Online]. Available: <https://www.google.com/intl/en/ipv6/statistics.html>. [Accessed: 01-Dec-2019].
- [9] S. E. Deering, "Internet Protocol, Version 6 (IPv6) Specification."
- [10] Tutorials Point, "Learn Internet Protocol Version 6," 2014.
- [11] Cisco, "Routing and Bridging Guide vA5(1.0), Cisco ACE Application Control Engine - Overview of IPv6 [Cisco Services Modules] - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/rtrbrgdgd/ipv6.html. [Accessed: 01-Dec-2019].
- [12] Government of the Hong Kong Special Administration, "IPv6 SECURITY," 2011.
- [13] E. Durdađi and A. Buldu, "IPV4/IPV6 security and threat comparisons," in *Procedia - Social and Behavioral Sciences*, 2010, vol. 2, no. 2, pp. 5285–5291.
- [14] A. Shrivastava, "Security Issues With Address Resolution Protocol," 2008.
- [15] "IPv6 Addressing | IPv6.com." [Online]. Available: <https://www.ipv6.com/general/ipv6-addressing/>. [Accessed: 01-Dec-2019].
- [16] Tutorials Point, "IPv6 - Addressing Modes." [Online]. Available: https://www.tutorialspoint.com/ipv6/ipv6_addressing_modes.htm. [Accessed: 01-Dec-2019].
- [17] Cisco, "Dual Stack IPv4/IPv6 Devices," 2010.
- [18] IBM, "IPv6 tunneling." [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/network/tcpip_ipv6_tunnel.html. [Accessed: 01-Dec-2019].
- [19] T. Point, "Transition From IPv4 to IPv6 - Tutorialspoint." [Online]. Available: https://www.tutorialspoint.com/ipv6/ipv6_ipv4_to_ipv6.htm. [Accessed: 01-Dec-2019].
- [20] "World IPv6 Launch." [Online]. Available: <https://www.worldipv6launch.org/>. [Accessed: 02-Dec-2019].
- [21] J. Streebel, "IPv4 vs IPv6," 2019. [Online]. Available: <https://pagely.com/blog/ipv4-vs-ipv6/>. [Accessed: 02-Dec-2019].

Lab – Understanding Ethernet Cable Standards

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.10.1	255.255.255.0	N/A
PC-B	NIC	192.168.10.2	255.255.255.0	N/A

Objectives

Part 1: Analyze Ethernet Cabling Standards and Pinouts

Part 2: Build an Ethernet Crossover Cable

Part 3: Test an Ethernet Crossover Cable

Background / Scenario

In this lab, you will build and terminate an Ethernet crossover cable and test it by connecting two PCs together and pinging between them. You will first analyze the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) 568-A and 568-B standards and how they apply to Ethernet cables. You will then construct an Ethernet crossover cable and test it. Finally, you will use the cable you just constructed to connect two PCs together and test it by pinging between them.

Note: With autosensing capabilities available on many devices, such as the Cisco 1941 Integrated Services Router (ISR) switch, you may see straight-through cables connecting like devices.

Required Resources

- One length of cable, either Category 5 or 5e. Cable length should be 0.6 to 0.9m (2 to 3 ft.)
- 2 RJ-45 connectors
- RJ-45 crimping tool
- Wire cutter
- Wire stripper
- Ethernet cable tester (optional)
- 2 PCs (Windows 7 or 8)

Part 1: Analyze Ethernet Cabling Standards and Pinouts

The TIA/EIA has specified unshielded twisted pair (UTP) cabling standards for use in LAN cabling environments. TIA/EIA 568-A and 568-B stipulates the commercial cabling standards for LAN installations;

Lab - Building an Ethernet Crossover Cable

these are the standards most commonly used in LAN cabling for organizations and they determine which color wire is used on each pin.

With a crossover cable, the second and third pairs on the RJ-45 connector at one end of the cable are reversed at the other end, which reverses the send and receive pairs. The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. Crossover cables are normally used to connect hubs to hubs or switches to switches, but they can also be used to directly connect two hosts to create a simple network.

Reflection:

Write a research report (Max word count 600) on Cat 5e and 6 Ethernet cable standards.

Please see Appendix A for Report.

Step 1: Analyze diagrams and tables for the TIA/EIA 568-A standard Ethernet cable.

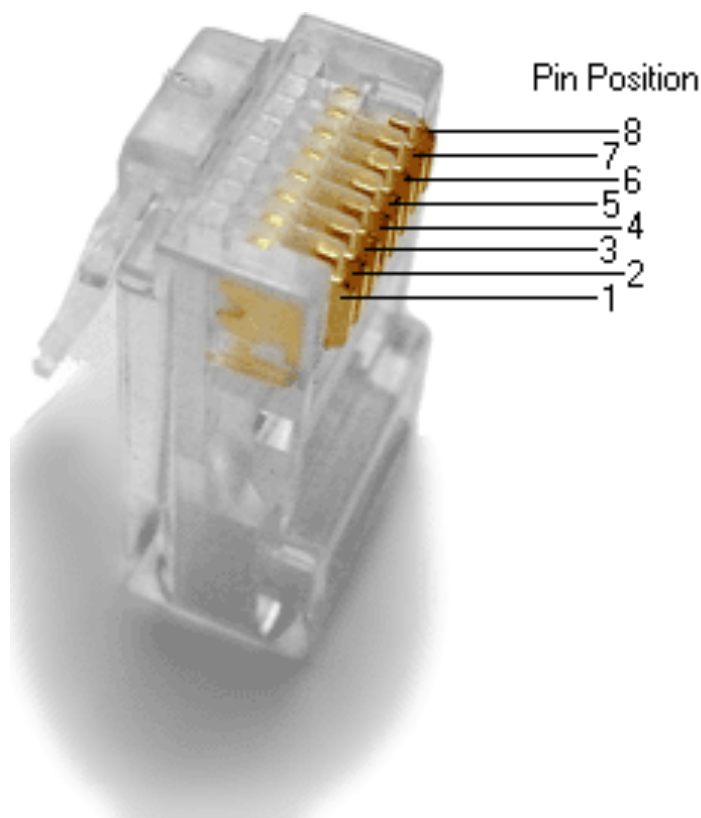
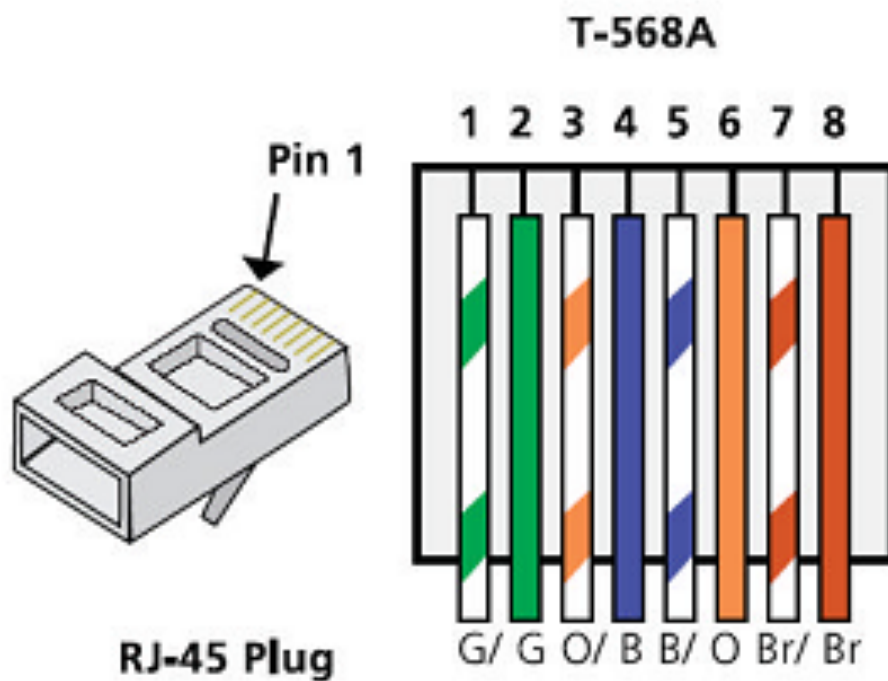
The following table and diagrams display the color scheme and pinouts, as well as the function of the four pairs of wires used for the 568-A standard.

Note: In LAN installations using 100Base-T (100 Mb/s), only two pairs out of the four are used.

568-A 10/100/1000Base-TX Ethernet

Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Green	Transmit	BI_DA+
2	2	Green	Transmit	BI_DA-
3	3	White/Orange	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Orange	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-

The following diagrams display how the wire color and pinouts align with an RJ-45 jack for the 568-A standard.



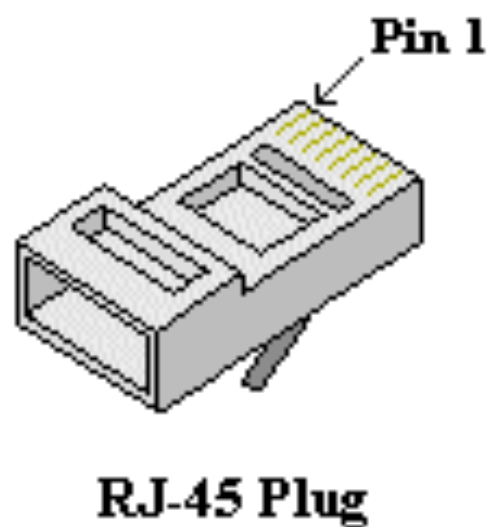
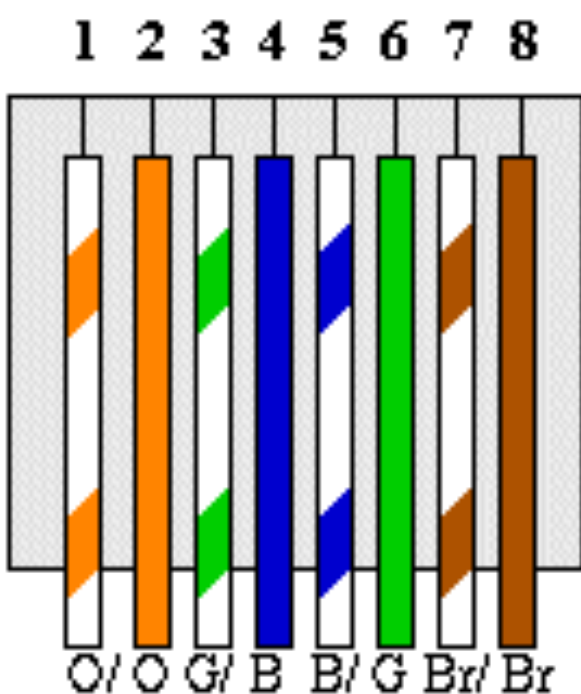
Step 2: Analyze diagrams and tables for the TIA/EIA 568-B standard Ethernet cable.

The following table and diagram display the color scheme and pinouts for the 568-B standard.

568-B 10/100/1000-BaseTX Ethernet

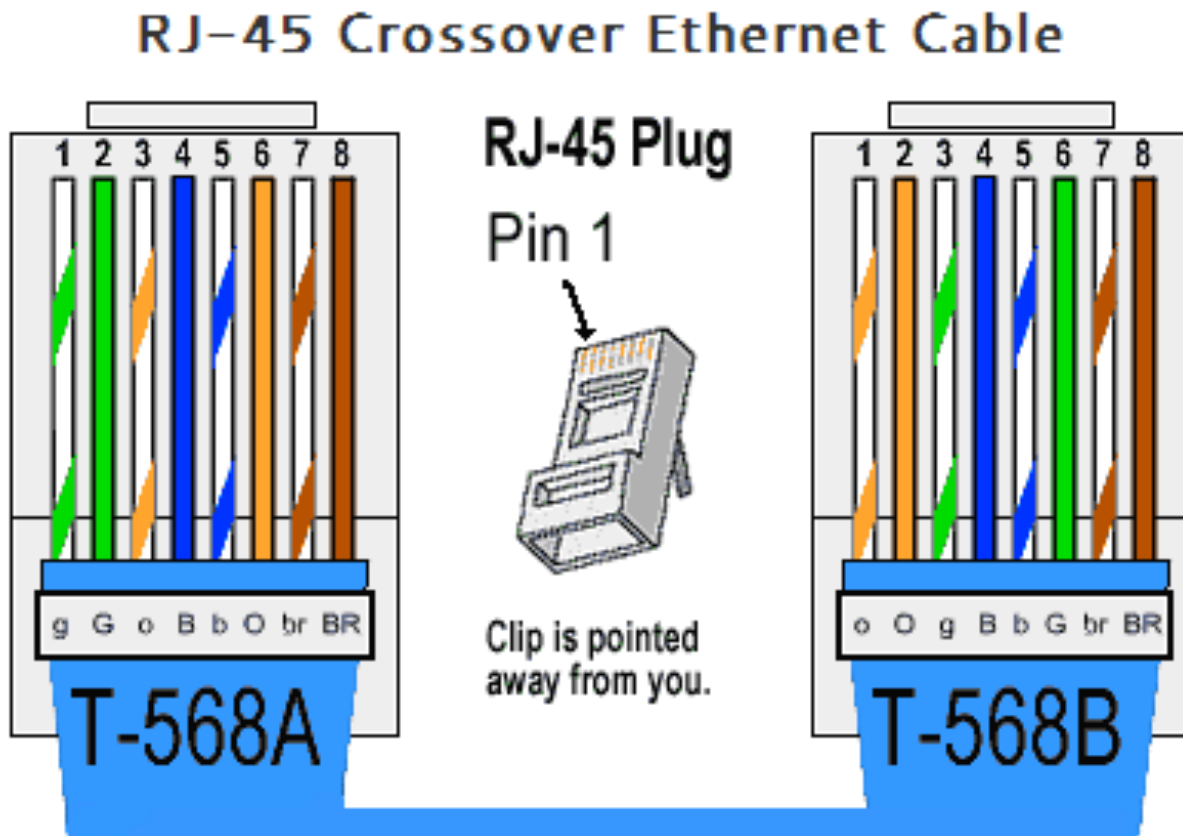
Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Orange	Transmit	BI_DA+
2	2	Orange	Transmit	BI_DA-
3	3	White/Green	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Green	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-

T-568B



Part 2: Build an Ethernet Crossover Cable

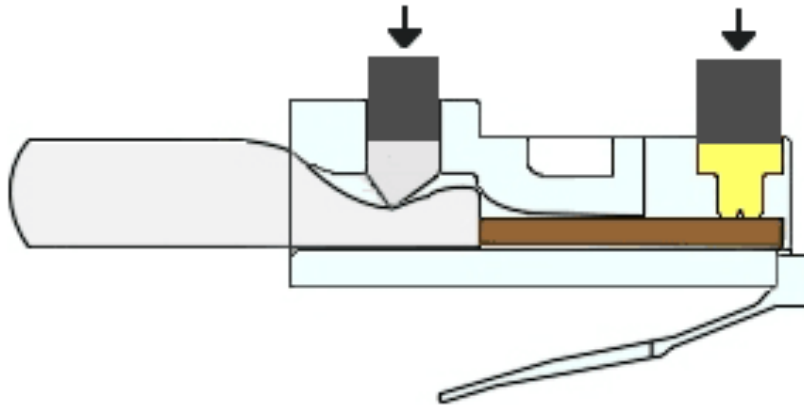
A crossover cable has the second and third pairs on the RJ-45 connector at one end, reversed at the other end (refer to the table in Part 1, Step 2). The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. The two following diagrams illustrate this concept.



Step 1: Build and terminate a TIA/EIA 568-A cable end.

- Determine the cable length required. (Your instructor will let you know the cable length you should make.)
Note: If you were making a cable in a production environment, the general guideline is to add another 12 in. (30.48 cm) to the length.
- Cut off a piece of cable to the desired length and using your wire stripper, remove 5.08 cm (2 in.) of the cable jacket from both ends.
- Hold the four pairs of twisted cables tightly where the jacket was cut away. Reorganize the cable pairs into the order of the 568-A wiring standard. Refer to the diagrams, if necessary. Take as much care as possible to maintain the twists in the cable; this provides noise cancellation.
- Flatten, straighten, and line up the wires using your thumb and forefinger.
- Ensure that the cable wires are still in the correct order for the 568-A standard. Using your wire cutters, trim the four pairs in a straight line to within 1.25 to 1.9 cm (1/2 to 3/4 in.).
- Place an RJ-45 connector on the end of your cable, with the prong on the underside pointing downward. Firmly insert the wires into the RJ-45 connector. All wires should be seen at the end of the connector in their proper positions. If the wires are not extending to the end of the connector, take the cable out, rearrange the wires as necessary, and reinsert the wires back into the RJ-45 connector.

- g. If everything is correct, insert the RJ-45 connector with cable into the crimper. Crimp down hard enough to force the contacts on the RJ-45 connector through the insulation on the wires, thus completing the conducting path. See the following diagram for an example.



Step 2: Build and terminate a TIA/EIA 568-B cable end.

Repeat steps 1a to 1g using the 568-B color wiring scheme for the other end.

Part 3: Test an Ethernet Crossover Cable

Step 1: Test the cable.

Many cable testers will test for length and mapping of wires. If the cable tester has a wire map feature, it verifies which pins on one end of the cable are connected to which pins on the other end.

If your instructor has a cable tester, test the crossover cable for functionality. If it fails, check with your instructor first as to whether you should re-cable the ends and re-test.

Step 2: Connect two PCs together via NICs using your Ethernet crossover cable.

- Working with a lab partner, set your PC to one of the IP addresses shown in the Addressing Table (see page 1). For example, if your PC is **PC-A**, your IP address should be set to **192.168.10.1** with a **24-bit subnet mask**. Your partner's IP address should be **192.168.10.2**. The default gateway address can be left empty.
- Using the crossover cable you made, connect the two PCs together via their NICs.
- On the PC-A command prompt, ping the PC-B IP address.

Note: The Windows firewall may have to be temporarily disabled for pings to be successful. If the firewall is disabled, make sure you re-enable it at the conclusion of this lab.

- Repeat the process and ping from PC-B to PC-A.

Assuming IP addressing and firewall are not issues, your pings should be successful if the cables were properly made.

Reflection

- Which part of making cables did you find the most difficult?

The cabling exercise was tricky, being sure to not cross the cables from their correct positions when inserting into the RJ-45 connector. I found that when I thought I had inserted them correctly, infact they had twisted and were then in the wrong position.

Once I had inserted them correctly, I proceeded to crimp the connector. I then tested my cable, and found that some of the pins were not making a connection. On closer inspection, I noticed that two of the wires had not been fully inserted into the connector and therefore were not making a connection.

I then re-created my cable but cutting and stripping the end once more, and re-arranging the cable to the correct pattern. This time I took more care to insert the wires and crimp them, and after testing, my cable was working correctly.

Personally, I felt that the most difficult aspect of cabling was the correct insertion of the wires into the RJ-45 connector.

2. Why do you have to learn how to make a cable if you can easily buy pre-made cables?

There may be many circumstances where making a cable would be more suitable, including those where an 'odd' length of cable is required, which is often the case in small home networks. Another reason would be for the repair of existing cables, for example if a cable is of sufficient length but has a damaged connector, the cable can be stripped and a new connector could be fitted.

Appendix A

Report titled "Cat5e and Cat6 Cabling Standards" below.



CAT 5E AND CAT 6 CABLING STANDARDS

University of Wales Trinity Saint David

BSc Computing Portfolio
Computer Architecture and Networks | ACCD4001

Siobhan Stephens
1800709

1. Introduction

Also known as Ethernet cables, Category 5e and Category 6 cables are structured cabling for computer networks. The cable standards have been developed by the Telecommunications Industry Association (TIA) and Electronics Industries Alliance (EIA) along with input from Industry, with the standard covering the cable's construction, performance and testing requirements [1]. The most common form of network cable is an Unshielded Twisted Pair, or UTP, the standard of which is managed by the Institute of Electrical and Electronics Engineers (IEEE) and is referred to as 802.3 [2].

Ethernet cables may be straight through, crossover or rollover, the difference of which vary by the wiring of the connectors on each end. They are produced with eight wires, each protected by a coloured plastic coating, and then twisted together into four twisted pairs using the colours shown in figure 1. The twisted pairs are then covered by an outer plastic jacket.

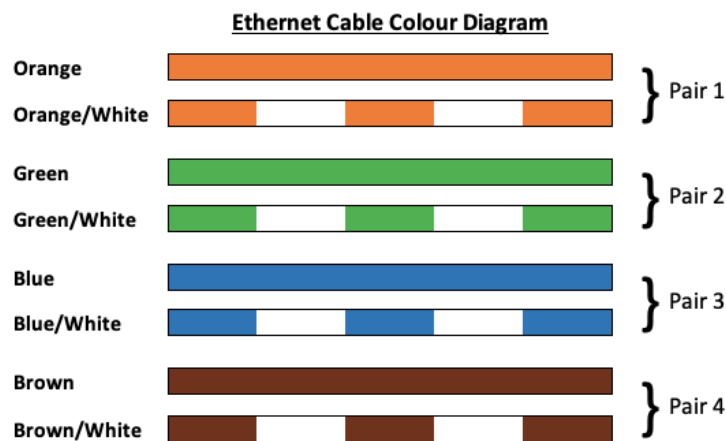


Figure 1. Ethernet Cable Colour Diagram [3]

The standard connectors for Ethernet cables are known widely as RJ-45, however this refers to telephone connectors, and the correct name for the connectors are “modular 8P8C” [4].

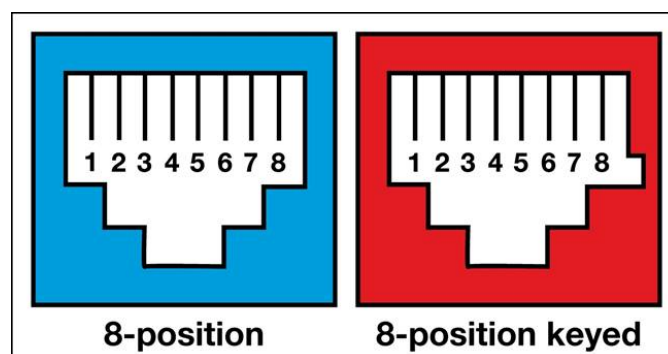


Figure 2. Modular 8P8C vs RJ-45 Connector [4]

2. Category 5e Cable Standard

The standard for Cat5 cables was first defined in TIA/EIA-568-A in 1991, which specified the performance and test requirements for frequencies up to 100MHz. Later, in 1995, the standard was updated to TIA/EIA-568-B for Category 5e cables. Similarly to their predecessor, Cat5e also use a frequency of 100MHz however, Cat5e cables have the capacity to handle greater bandwidth, and are typically used for Ethernet networks of 1000Mbps/1Gbps [5].

Cat5e cables support both half and full-duplex Fast Ethernet communication in conjunction with Carrier Sense Multiple Access with Collision Detection (CSMA/CD) [6]. According to CableK, Cat5e has “stricter specifications for Power Sum Equal-Level Far-End, Near-End Crosstalk, Attenuation, and Return Loss than those for CAT5” [7].

The T568A and T568B wiring schemes specify pin to pair assignments and the cable is connected using modular 8P8C connectors on either end [8].

3. Category 6 and 6a Cable Standards

Category 6 cables and connectors are defined by the TIA/EIA-568-B standard. Cat6 cables, like their predecessors, also use 8P8C connectors however the connectors must be rated for Category 6 performance. Cat6 cables support higher bandwidths than Cat5e, and vary in construction as Cat6 twisted pairs are wound more tightly, and are often fitted with foil or braided shielding (STP) [1]. The added shielding works to prevent electrical interference, referred to as crosstalk [9], and noise interference, both of which were an issue associated with previous cables.

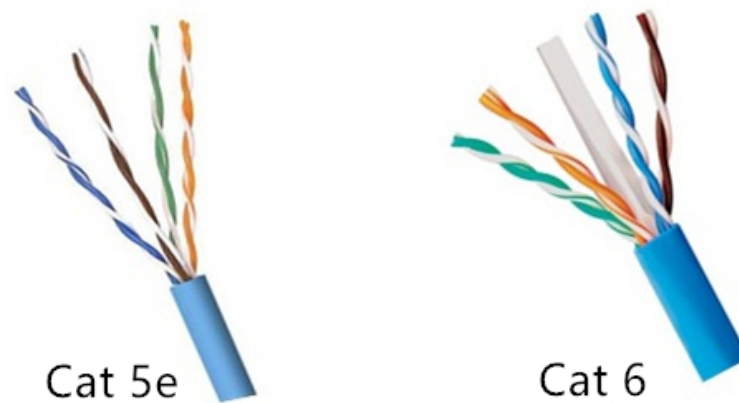


Figure 3. Cat5e vs Cat6 Cable [10].

They operate on a frequency of 250MHz, and can support theoretical speeds of up to 10Gbps, however only over distances up to 55 meters. Category 6 cables are also backwards compatible with other cabling standards and network protocols [11] and therefore are suitable for the following ethernet speeds: 10BASE-T (10Mbit/s); 100BASE-TX Fast Ethernet (100Mbit/s), 1000BASE-T/ 1000BASE-TX Gigabit Ethernet (1Gbit/s) and 10GBase-T (10 Gbit Ethernet) [12].

Comparison of Cat5, Cat5e, Cat6 and Cat6a Cables

	Cat 5	Cat 5e	Cat 6	Cat 6a
Date Introduced	1991	2001	2002	2008
Frequency	Up to 100MHz	100MHz	250MHz min, 500MHz max	Up to 500MHz
Maximum Cable Length	100m	100m or 50m at max rate	100m at 1,000Mbps, 55m max for Gigabit Ethernet	10Gbps over 100m
Theoretical Top Speed	100Mbps	1000Mbps at 50m	10Gbps over 55m	10Gbps over 100m
Attenuation (min at 100MHz)	22dB	22dB	19.8dB	N/A
Shielding	Unshielded Twisted Pair	Unshielded Twisted Pair or Shielded Twisted Pair	Unshielded Twisted Pair or Shielded Twisted Pair	Unshielded Twisted Pair or Shielded Twisted Pair
Connector	8P8C (aka RJ-45)	8P8C (aka RJ-45)	8P8C (aka RJ-45)	8P8C (aka RJ-45)
Reduced Crosstalk	No	Yes, over Cat5	Yes, over Cat5e	Yes, over Cat6
Wiring Scheme	T568A and T568B	T568A and T568B	T568A and T568B	T568A and T568B
Other Features	Isn't widely used (succeeded by Cat5e)	Most commonly used	Has tighter twists than Cat5e. Allows two-way communication on each pair of wires.	Thicker than Cat6

Figure 4. Comparison Table of Cable Standards [13] [14] [15]

The Cat6 standard has been superseded by Cat6a, or Augmented Cat 6 which operates on a frequency of 500MHz and according to Scherer has “improved alien crosstalk characteristics, allowing 10GBASE-T to be run for the same distance as previous protocols” [11]. The IEEE first published the standard (802.3an) in September 2006 [16].

Cat6a offer speeds of up 10Gbit/s (10GBASE-T) over distances up to 100m. The cables differ in construction from most Cat6 cables as they are always shielded [11].

4. Conclusion

Cat5e is currently the most widely used standard in industry, with Cat6 increasing in popularity. According to [17], whilst theoretically Cat6 cables may provide better performance to Cat5e, albeit with a premium price [18], most computers and networking devices are only able to transmit a frequency of 100MHz, therefore, in reality the difference in performance is likely to be negligible.

However, with the fast growth and improvement of technology, it is recommended to use the most up to date standard in order to help future proof a network [19]. As a result, Cat6a cables are likely to become more common due to their higher bandwidth, better distance and reduced crosstalk.

Newer standards including Cat7 and Cat7a have been defined by ISO 11801, which is the international standard for Generic Cabling for Customer Premises [20], however neither have yet been recognised by the TIA/EIA.

5. References

- [1] “FAQ: Ethernet Standards - Eland Cables | Eland Cables.” [Online]. Available: <https://www.elandcables.com/the-cable-lab/faqs/faq-what-are-the-ethernet-standards>. [Accessed: 02-Dec-2019].
- [2] “IEEE 802.3-2018 - IEEE Standard for Ethernet.” [Online]. Available: https://standards.ieee.org/standard/802_3-2018.html. [Accessed: 02-Dec-2019].
- [3] Cisco, “B-1 Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide A P P E N D I X B Connector Pin Assignments.”
- [4] K. Waldoock, “RJ45 or 8P8C Connectors? Finding the True Ethernet Standard | Arrow.com.” [Online]. Available: <https://www.arrow.com/en/research-and-events/articles/rj45-connectors>. [Accessed: 02-Dec-2019].
- [5] Jonathan Austin Rust and Rustcraft Industries LLC, “Data Cable, Connector and Crimping System and Method,” 2017.
- [6] Cisco, “Carrier Sense Multi-Access/Collision Detection (CSMA/CD) - Cisco Systems.” [Online]. Available: https://www.cisco.com/en/US/tech/tk389/tk214/tk125/tsd_technology_support_sub-protocol_home.html. [Accessed: 02-Dec-2019].
- [7] “CAT 5, cat 5e, cat6, cat6a, cat7, cat8 Cable Standards | Cablek.” [Online]. Available: <http://www.cablek.com/technical-reference/cat-5---5e--6--6a---7--8-standards>. [Accessed: 02-Dec-2019].
- [8] “Cisco Sem1 - Cable Labs.” [Online]. Available: <http://academy.delmar.edu/Courses/ITNW1425/cisco1labs.htm>. [Accessed: 05-Dec-2019].
- [9] Hewlett-Packard, “Cross Talk in Unshielded Twisted Pair Cables,” 1995.
- [10] “Cat5e vs Cat6 Cable - Which do You Choose?” [Online]. Available: <http://www.fiber-optical-networking.com/cat-5e-cat-6-choose.html>. [Accessed: 08-Dec-2019].
- [11] Christopher Scherer and Johnathon Sholtis, “Networking Cable Tracer System,” 2015.
- [12] Cisco, “10 Gbps Cabling,” 2008.
- [13] Custom.CA, “CAT3 vs. CAT5 vs. CAT6 - CustomCable,” 2011. [Online]. Available: <https://customcable.ca/cat5-vs-cat6/>. [Accessed: 08-Dec-2019].
- [14] CableK, “Cat5, Cat 5e, Cat6, Cat6a Cable Standards.” [Online]. Available: <http://www.cablek.com/technical-reference/cat-5---5e--6--6a---7--8-standards>. [Accessed: 08-Dec-2019].
- [15] RouterSwitch, “Cisco CCNA Part: Types of Ethernet Cabling,” 2016. [Online]. Available: <https://blog.router-switch.com/2016/01/cisco-ccna-part-types-of-ethernet-cabling/>. [Accessed: 08-Dec-2019].
- [16] IEEE, “IEEE 802.3an-2006 - IEEE Standard for Information Technology,” *IEEE*, 2006. [Online]. Available: https://standards.ieee.org/standard/802_3an-2006.html. [Accessed: 06-Dec-2019].
- [17] B. K. Soorty, S. S. Kolahi, N. Chand, and Z. Qu, “Performance comparison of category 5e vs. category 6 cabling systems for both IPv4 and IPv6 in Gigabit Ethernet,” in *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, 2010, pp. 1525–1529.
- [18] Diffen, “Cat5e vs Cat6 - Difference and Comparison.” [Online]. Available: https://www.diffen.com/difference/Cat5e_vs_Cat6. [Accessed: 09-Dec-2019].
- [19] T. Lite, “Cat5e, Cat6 or Cat6a?,” 2017. [Online]. Available: <https://blog.triplite.com/which-ethernet-cable-should-you-use-cat5e-cat6-or-cat6a/>. [Accessed: 09-Dec-2019].

- [20] FS, “Network Cable Standards for Generic Cabling: TIA 568 vs ISO 11801 vs EN 50173,” 2019. [Online]. Available: <https://community.fs.com/blog/network-cable-standards-tia-568-vs-iso-11801-vs-en-50173.html>. [Accessed: 09-Dec-2019].

Lab - Accessing Network Devices with SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Basic Security Measures on the Router and Switch

Part 3: Configure the Router for SSH Access

Part 4: Configure the Switch for SSH Access

Part 5: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plaintext passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

- Configure PC-A with an IP address and subnet mask.
- Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection. – *Ping was Successful.*

Part 2: Configure Basic Security Measures on the Router

Step 1: Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

Step 2: Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

- Change the privileged EXEC encrypted password to meet guidelines.

```
R1(config)# enable secret Enablep@55
```

(Note: password length must meet criteria being set later)

- Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Step 3: Secure the console and VTY lines.

- You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

- The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R1(config)# login block-for 30 attempts 2 within 120
```

What does the **2 within 120** mean in the above command?

The two in the above command refers to the number of attempts the user can fail before being blocked for 30 seconds, where the two failed attempts are within 120 seconds of each other.

What does the **block-for 30** mean in the above command?

Block-for 30 refers to the number of seconds a user is blocked for until they are able to retry. As stated above, this timeout has been set for a short period for the lab. However, in a real-world application, the timeout would be higher to improve security.

Step 4: Verify that all unused ports are disabled.

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command. Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0/0	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
Serial0/0/1	unassigned	YES	NVRAM	administratively down	down

Part 3: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

- Configure the domain for the device.

```
R1(config)# ip domain-name ccna-lab.com
```

Step 2: Configure the encryption key method.

Command changed from "crypto key generate rsa modulus 1024" as this was incorrect.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

```
R1(config)#
```

```
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enable
```

Worked correctly.

Step 3: Configure a local database username.

```
R1(config)# username admin privilege 15 secret adminpass
```

The above command would not work, due to the earlier password constraint set, which limits passwords to be a minimum of 10 characters in length.

```
R1(config)# username admin privilege 15 secret Admin1p@55
```

Note: A privilege level of 15 gives the user administrator rights.

Step 4: Enable SSH on the VTY lines.

- a. Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.

1) In a real-world application, Telnet should not be enabled as it is a security risk (as noted above).

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input telnet ssh
```

The above command was incorrect, as it combined both telnet and ssh in one command. Instead, the command should be run separately for each, as below. However, due to the fact that telnet is not secure, I have not enabled it.

```
R1(config-line)# transport input ssh
```

```
R1(config-line)# transport input telnet
```

- b. Change the login method to use the local database for user verification.

```
R1(config-line)# login local
```

```
R1(config-line)# end
```

```
R1#
```

Step 5: Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
R1#
```

Step 6: Establish an SSH connection to the router.

- a. Start Tera Term from PC-A.

- b. Use Tera Term to telnet to R1.

Does R1 accept the Telnet connection? Explain.

R1 does not accept a Telnet connection as telnet has not been enabled. Telnet is not enabled as it is a security risk.

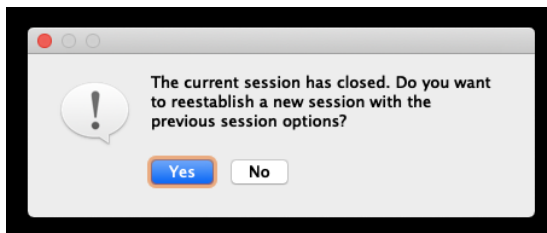


Figure 1. Screenshot showing failed telnet connection.

- c. Use Tera Term, establish an SSH session to R1. Use the username **admin** and password **Admin1p@55** (changed above to meet minimum criteria). You should be able to establish an SSH session with R1.

Does R1 accept the SSH connection?

The SSH connection was successful using the correct credentials, as shown below in the screenshot.

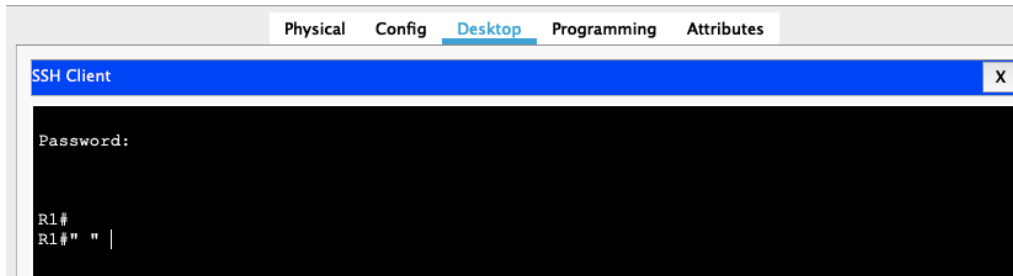


Figure 2. Screenshot showing successful SSH connection using credentials

- d. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

What happened after you failed to login the second time?

After entering the incorrect credentials twice, the session was ended and the following alert was displayed.

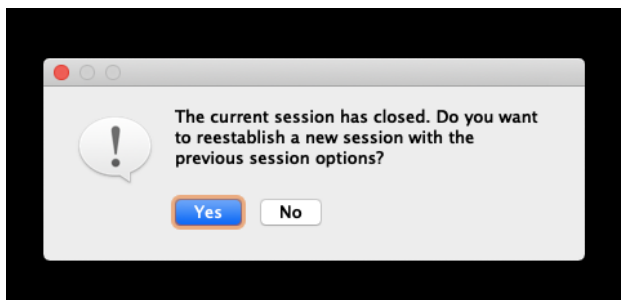


Figure 3. Screenshot of blocked session after two failed login attempts using incorrect credentials.

- e. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

```
R1# show login
```

```
A default login delay of 1 second is applied.  
No Quiet-Mode access list has been configured.
```

```
Router enabled to watch for login Attacks.  
If more than 2 login failures occur in 120 seconds or less,  
logins will be disabled for 30 seconds.
```

```
Router presently in Quiet-Mode.  
Will remain in Quiet-Mode for 14 seconds.  
Denying logins from all sources.
```

R1#

- f. After the 30 seconds has expired, SSH to R1 again and login using the **admin** username and **Admin1p@55** for the password.

After you successfully logged in, what was displayed?

Experienced a bug during this section of the lab as packet tracer would not allow me to re-enter my correct password once the incorrect password had been blocked. Restarted packet tracer to continue the lab and the bug had gone.

When I tried again, the banner message set earlier in the lab was displayed as expected.

- g. Enter privileged EXEC mode and use **Enablep@55** for the password.

If you mistype this password, are you disconnected from your SSH session after two failed attempts within 120 seconds? Explain.

Once the password had been mistyped the session was disconnected. I had to wait 30 seconds before being able to re-enter my password due to the restrictions set earlier in the lab.

- h. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Part 4: Configure the Switch for SSH Access

In Part 3, you will configure the switch in the topology to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Step 1: Configure the basic settings on the switch.

- Console into the switch and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names. (*no ip domain-lookup*)
- Assign **class** as the privileged EXEC encrypted password. (*enable secret class*)
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plain text passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.
 - interface vlan 1*
 - ip address 192.168.1.11 255.255.255.0*
- Save the running configuration to the startup configuration file.

1) *copy running-config startup-config*

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

- a. Configure the device name as listed in the Addressing Table.
- b. Configure the domain for the device.

```
S1(config)# ip domain-name ccna-lab.com
```

- c. Configure the encryption key method.

```
S1(config)# crypto key generate rsa modulus 1024
```

Incorrect command above, corrected to the following command below.

```
S1(config)# crypto key generate rsa general-keys modulus 1024
```

- d. Configure a local database username.

```
S1(config)# username admin privilege 15 secret adminpass
```

- e. Enable Telnet and SSH on the VTY lines.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh - enables SSH ONLY (not Telnet)
```

- f. Change the login method to use the local database for user verification.

```
S1(config-line)# login local
```

```
S1(config-line)# end
```

Step 3: Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

Initially, I was unable to SSH to the switch. After using the show running-config command I was able to troubleshoot the issue, which was that the port was shut. After running the no shutdown command and retrying to SSH, it was successful and displayed the banner I had previously set.

Part 5: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
```

```
-p      Connect to this port
-v      Specify SSH Protocol Version
-vrf    Specify vrf name
WORD    IP address or hostname of a remote system
```

Step 2: SSH to R1 from S1.

- a. You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass - (Changed now to "Admin1p@55" to meet password criteria)** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****
```

```
R1#
```

- b. You can return to S1 without closing the SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1#
S1#
```

- c. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

- d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

What versions of SSH are supported from the CLI?

The switch supports SSH Protocol V1 and V2 as shown in the screenshot below, produced by running the **ssh -v** command on the switch.

```
S1#ssh -v ?
 1 Protocol Version 1
 2 Protocol Version 2
.. " " ..
```

Figure 4. Screenshot of SSH version from CLI on Switch 1

How would you provide multiple users, each with their own username, access to a network device?

In order to provide multiple users access to a device with their own username and password, the following command can be run “**username {username} privilege {level} secret {password}**”.

Lab Reflection:

During this lab, I encountered a few commands that did not work in packet tracer, such as the crypto key generate command. However, I was able to use the '?' help in order to find the correct command.

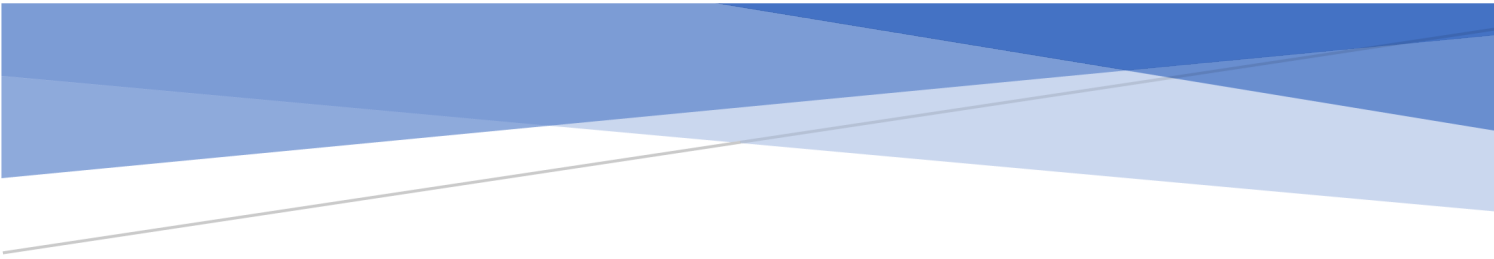
I also encountered a bug during the lab when testing my password timeouts. The bug caused me to be locked out of the router and would not accept my correct credentials. To overcome this I restarted packet tracer and was able to continue.

Overall, I learned many things in this lab, including how to set basic password requirements, and how to SSH into a router.

Report (max 800 words):

Write a research report comparing various Encryption standards, e.g AES, SHA, DES, RSA.

Please see report attached below titled 'Comparison of Common Encryption Standards'.



COMPARISON OF COMMON ENCRYPTION STANDARDS

University of Wales Trinity Saint David

BSc Computing Portfolio
Computer Architecture and Networks | ACCD4001

Siobhan Kelly Stephens
1800709

1. Introduction

Encryption is the process of taking plain text and turning it into an unrecognisable and unreadable format [1] for the purpose of providing confidentiality, integrity, non-repudiation and authentication of data [2]. Data Integrity and Confidentiality make up two sides of the CIA triad, which defines the basic aims of information security [3].

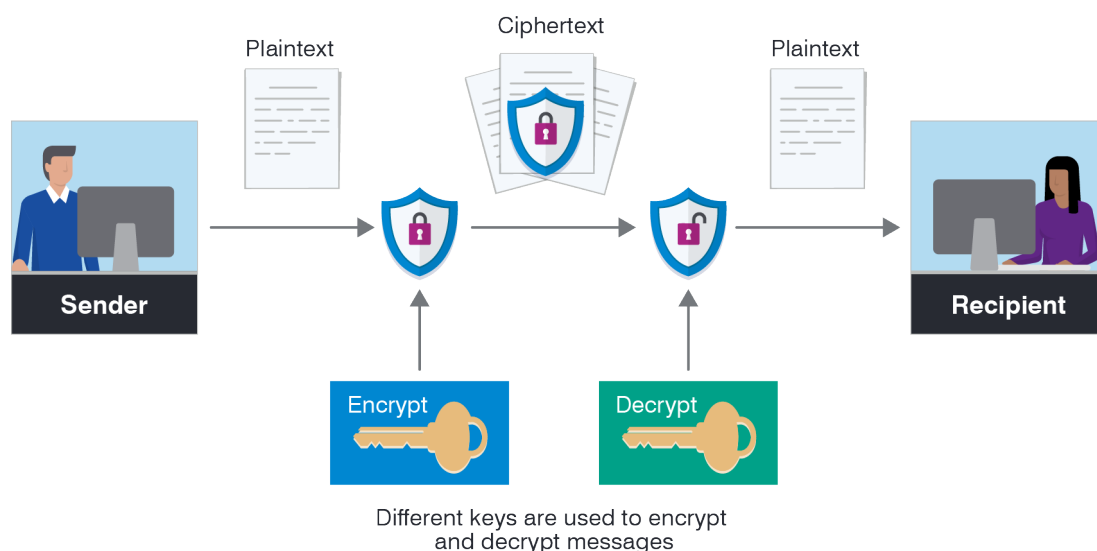


FIGURE 1. ENCRYPTION AND DECRYPTION [4].

A hashing algorithm is the process of applying a mathematical function to plain text and transforming it into a fixed-size unique hash value. As a result of this process, data is obscured. Hashing algorithms are irreversible, and therefore can be referred to as one-way encryption [5].

Encryption is highly important in modern technology and therefore different techniques and methods have been used to protect sensitive data. Organisations face fines of up to €20mil or 4% of turnover, if they do not have adequate security on data they hold [6].

2. Encryption Standards

There are many modern encryption standards that all vary in complexity and system requirements. Encryption can fall into one of two categories, asymmetric or symmetric (See Appendix A.1).

2.1 Advanced Encryption Standard (AES)

The AES algorithm was published by National Institute of Standards and technology (NIST) in 2000. AES was introduced to replace the DES algorithm and overcome many of its vulnerabilities. The AES algorithm is symmetric and takes a fixed 128-bit block and then uses either a 128-bit, 192-bit or 256-bit key [7].

The number of transformation rounds that are applied to the plain text is defined by the key size specified for the AES cipher. 128-bit keys undergo 10 rounds, 12 rounds for 192-bit and finally 14 rounds for 256-bit keys. Using the same encryption key, a set of reverse rounds are applied to transform the ciphertext into plaintext [7].

2.2 Secure Hashing Algorithm (SHA)

SHA was developed by the US National Security Agency (NSA) [5]. There are different versions of the Secure Hashing Algorithm such as SHA-1 and variations of SHA-2. SHA-2 is the successor to SHA-1 and contains many improvements over SHA-1. From 2016 onwards, SSL/TLS certificates must use SHA-256 as a minimum [8].

SHA-1 was first published in 1995 and uses a 160-bit hash, whereas SHA-2 comes in various bit-lengths, with 256-bit being the most common (known as SHA-256). A larger bit size provides more security as there are more possible combinations, which is important in order to prevent collisions, which are dangerous to security as they allow two files to produce the same hash – in the case of certificates, this could mean a certificate appears to be valid when it was never signed [8].

SHA has many uses along with certificates such as obscuring passwords in databases and identifying the tampering of files - due to the major difference in hash values as a result of an ‘avalanche’ effect [9].

2.3 Data Encryption Standard (DES) and Triple DES

DES was developed in 1970 at IBM by Horst Feistel [10]. It is a symmetric encryption that consists of a number of rounds, where each round contains bit-shuffling, non-linear substitutions and exclusive OR operations [10]. It expects a 64-bit input plus a 56-bit key to produce a 64-bit cipher/plaintext [11].

By 1997, DES was cracked by Deschall proving it to be insecure [12], and therefore a more secure encryption was required. In response, Triple DES or 3DES was introduced in 1998. 3DES applies the DES algorithm three times to each block by encrypting with a first key, decrypting with a second key, and encrypting with a third key. 3DES is embedded into payment systems, standards and technology in the finance industry, however in November 2017, NIST restricted the usage of 3DES so that it could no longer be used for TLS, IPsec or large file encryption [13].

2.4 RSA

RSA, or Rivest, Shamir, and Adelman, is an asymmetric public-key encryption algorithm based on prime factorization, developed in 1978. RSA is the standard encryption method for transmitting important data over the internet, and is built into many products such as Microsoft’s Internet Explorer [14].

RSA produces a variable block size cipher and works by finding the product of two large prime numbers and applying additional mathematical operations to create both the public and private keys [15].

RSA is used for SSL/TLS, S/MIME and Secure Shell encryption and digital signature functions [15].

3. Comparison of Encryption Standards

Figure 2 below outlines the main characteristics of the RSA, DES, 3DES and AES encryption algorithms. The SHA hashing algorithm will not be considered in this section.

Comparison of RSA, DES, 3DES and AES Encryption Algorithms				
	RSA	DES	3DES	AES
Creators	Rivest, Shamir, and Adelman in 1978	IBM in 1975	IBM in 1978	Vincent Rijem, John Daemon in 2001
Key Length	Depends on no of bits in the modulus n where $n = p * q$ (1024/2048 most common)	56 bits	168 bits	128, 192 or 256 bits
Round(s)	1	16	48	10 for 192-bit keys, 12 for 192-bit keys, 14 for 256bit keys
Block Size	Variable	64 bits	64 bits	128 bits
Cipher Type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed of Algorithm (relative)	Slowest	Slow	Very Slow	Fast
Security (relative)	Least secure	Insecure	Adequate	Excellent
Storage Requirements	Large, due to the greater key size required for security	Minimal storage requirments	Minimal storage requirments	Minimal storage requirments
Resistant to Quantum Computing	No	No	No	Likely

FIGURE 2. COMPARISON OF ENCRYPTION STANDARDS FROM MULTIPLE SOURCES [16][17].

As shown above, AES provides the highest level of security, and is the only algorithm likely to remain secure against quantum computing. RSA has not yet been cracked, however would likely be easily brute-forced using quantum computing [16].

Unlike the other algorithms, RSA requires large storage requirements due to its greater key size required to maintain a level of security, and Parmar et al [16] stated that “to achieve the same level of security provided by 2048-bit RSA, AES requires only a 112-bit key”.

AES is the fastest algorithm for encryption and decryption, with RSA being the slowest due to the key generation time [16]. 3DES is more slow than DES due to it applying the same algorithm three times. AES is faster than DES and 3DES due to its greater block size, meaning it has to iterate the encryption less times [10].

4. Conclusion

Based on the above comparisons, AES offers the best memory and storage efficiency along with performance as an encryption algorithm, plus the highest security and is likely to be future proof against quantum computing.

However, if authentication is required, then RSA should be used. It does offer a reasonable level of security but requires greater key generation time [16] and will likely need to be updated in the coming years.

If only data obscuring is required, SHA-256 should be used as it is currently the most supported hashing algorithm which balances security, hash collisions and performance.

It must be noted that despite strong encryption on data, physical hardware must be adequately protected in order to keep data secure.

5. References

- [1] Kim Porter and Norton, "What is encryption and how does it protect your data?" [Online]. Available: <https://us.norton.com/internetsecurity-privacy-what-is-encryption.html>. [Accessed: 05-Dec-2019].
- [2] A. Muhammad and R. Hikmat, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *Int. J. Comput. Appl.*, vol. 143, no. 4, pp. 11–17, Jun. 2016.
- [3] M. Cabric, "Confidentiality, Integrity, and Availability," in *Corporate Security Management*, Elsevier, 2015, pp. 185–200.
- [4] Proofpoint, "Encryption - What It Is, Types, Algorithms, & More." [Online]. Available: <https://www.proofpoint.com/us/glossary/encryption>. [Accessed: 05-Dec-2019].
- [5] R. Chaves, L. Sousa, N. Sklavos, G. Kalogerido, P. Kitsos, and F. Sheik, "Secure Hashing: SHA-1, SHA-2, and SHA-3," 2016.
- [6] "Fines / Penalties | General Data Protection Regulation (GDPR)." [Online]. Available: <https://gdpr-info.eu/issues/fines-penalties/>. [Accessed: 05-Dec-2019].
- [7] A. Muhammad Abdullah and A. Muhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Application of Petri Nets in Computer Networks View project Advanced Encryption Standard (AES) A," 2017.
- [8] P. Nohe, "The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms." [Online]. Available: <https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/>. [Accessed: 05-Dec-2019].
- [9] P. Witoolkollachit, "The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images: A comparison study," 2016.
- [10] M. I. Ali, Z. Ahmed, M. Tariq Mahmood, and S. Rahman, "AES, DES, Triple DES Encryption Efficiency Analysis."
- [11] "Difference Between DES and AES (with Comparison Chart) - Tech Differences," 2016. [Online]. Available: <https://techdifferences.com/difference-between-des-and-aes.html>. [Accessed: 06-Dec-2019].
- [12] "Brute Force Cracking the Data Encryption Standard | RSA Conference." [Online]. Available: <https://www.rsaconference.com/industry-topics/blog/brute-force-cracking-the-data-encryption-standard>. [Accessed: 06-Dec-2019].
- [13] J. Henry, "3DES is Officially Being Retired." [Online]. Available: <https://www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired>. [Accessed: 06-Dec-2019].
- [14] "What is RSA Encryption?" [Online]. Available: <https://www.techopedia.com/definition/21852/rsa-encryption>. [Accessed: 06-Dec-2019].
- [15] M. Rouse, "RSA algorithm (Rivest-Shamir-Adleman)," 2018. [Online]. Available: <https://searchsecurity.techtarget.com/definition/RSA>. [Accessed: 05-Dec-2019].
- [16] N. J. Parmar and P. K. Verma, "A comparative evaluation of algorithms in the implementation of an ultra-secure router-to-router key exchange system," *Secur. Commun. Networks*, vol. 2017, 2017.
- [17] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, 2018, vol. 2018-Janua, pp. 1–7.
- [18] Phillip A Laplante, *Encyclopedia of Computer Science and Technology Volume II*, II. CRC Press Taylor & Francis Group, 2017.

6. Appendix A

Appendix A.1

Symmetric encryption uses a single key for both encryption and decryption and is much faster than asymmetric, whereas asymmetric encryption requires two separate keys, a public key and a private key known together as a key pair, for encryption and decryption [18].