

Mohamed Salem Salem Ali Easa

CCNA in 21 Hours

'640-802' syllabus

Mohamed Salem Salem Ali Easa

CCNA in 21 Hours

'640-802' syllabus



CCNA in 21 Hours : '640-802' syllabus

1st edition

© 2013 Mohamed Salem Salem Ali Easa & bookboon.com

ISBN 978-87-403-0476-3

Contents

	About this book	12
	Introduction	13
Part 1	NETWORK BASICS	14
Hour 1:	About Computer Networks	15
1.1	What is a computer network?	15
1.2	Computer network topologies	15
1.3	Simplex, half duplex and full duplex communication modes	19
1.4	Carrier Sense Multiple Access / Collision Detection (CSMA / CD) protocol	21
Hour 2:	Numbering systems	22
2.1	Decimal, hexadecimal and binary numbering systems	22
2.2	How to convert from binary to decimal	24
2.3	How to convert from decimal to binary	25
2.4	How to convert between hexadecimal and binary	26
2.5	How to convert between hexadecimal and decimal	29



ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

Hour 3:	TCP/IP and OSI suit	31
3.1	TCP/IP layers	31
3.2	Data encapsulation process	33
3.3	OSI model layers	34
Hour 4:	Network Interface Layer	36
4.1	Ethernet protocol in the physical layer	36
4.2	UTP cabling	39
4.3	‘Hub’, a device working in the physical layer	42
4.4	Ethernet protocol in the data link layer	42
4.5	What is the MAC address?	44
4.6	‘Switch’, a device working in the data link layer	45
4.7	Collision domain	46
Hour 5:	Internetworking Layer	48
5.1	IP (Internet Protocol)	48
5.2	Network IP?	50
5.3	Broadcast IP?	51
5.4	Unicast, multicast and broadcast communication	52



5.5	IP header	55
5.6	'Router', a device working in the internetworking layer	56
5.7	Broadcast domain	56
Hour 6:	Subnet Mask and Subnetting	58
6.1	Subnet mask	59
6.2	Subnet mask examples	61
6.3	Subnetting	64
Hour 7:	Network Infrastructure	67
7.1	NIC settings	67
7.2	Default gateway	67
7.4	DHCP sever	70
7.5	ARP	74
7.6	ICMP	77
Hour 8:	Transport and Application Layers	78
8.1	Transport layer protocols (TCP and UDP)	78
8.2	Application layer protocols	80

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub



Part 2	NETWORK CONFIGURATION	82
Hour 9:	Cisco IOS, The Router Device	83
9.1	LAN and WAN interfaces	83
9.2	The router's hardware	84
9.3	Booting up a router	86
Hour 10:	Cisco IOS, The CLI Commands	88
10.1	CLI (Command Line Interface) modes	88
10.2	Privileged mode commands, 'show' command	90
10.3	Privileged mode commands, network connectivity	93
10.4	Privileged mode commands, backing up and restoring processes	95
10.5	Global configuration mode commands	97
10.6	Specific configuration modes	99
10.7	CDP (Cisco Discovery Protocol)	100
Hour 11:	Routing Protocols	103
11.1	Routing protocols basics	103
11.2	Static routing	104



MAXIMIZE PRODUCTIVITY

**HELP YOUR ENTIRE
ORGANIZATION
BUILD EXPERTISE
IN SAP SOFTWARE.**

SAP Learning Hub

SAP

11.3	Dynamic routing	106
11.4	Distance vector routing	107
11.5	Routing loops	108
Hour 12:	RIP Routing Protocol	109
12.1	RIP is a classful routing protocol	110
12.2	RIPv2 (RIP version 2)	113
12.3	IGRP routing protocol	113
Hour 13:	OSPF Routing Protocol	114
13.1	OSPF neighbors and adjacencies in a LAN	115
13.2	OSPF configuration	116
13.3	DR election	117
Hour 14:	EIGRP Routing Protocol	119
14.1	EIGRP configuration	120
14.2	Administrative Distance (AD)	120
14.3	Default route	122

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



Hour 15:	Switch Operation	124
15.1	Switch operation and characteristics	124
15.2	Switch 'layer 2' functions	126
15.3	Port security	127
Hour 16:	Virtual LAN (VLAN)	128
16.1	Virtual LAN (VLAN) characteristics	128
16.2	VLAN switch port membership	132
16.3	Virtual LAN (VLAN) configuration	133
16.4	Routing between VLANs	135
16.5	VLAN Trunking Protocol (VTP)	138
Hour 17:	Spanning Tree Protocol (STP)	143
17.1	STP operation	145
17.2	STP port states	148
17.3	STP port fast	150
17.4	'RSTP', 'PVSTP+' and 'PVRST+'	152



JUMP-START CAREERS

**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub



Part 3	ADVANCED TOPICS	155
Hour 18:	Security	156
18.1	Security threats	156
18.2	Security threats mitigation	157
18.3	Access Control List (ACL)	158
18.4	NAT (Network Address Translation)	162
18.5	Static NAT, dynamic NAT and PAT	164
Hour 19:	Wide Area Networks (WAN)	170
19.1	Wide Area Network (WAN) basics	170
19.2	WAN connection types	172
19.3	HDLC and PPP protocols	173
19.4	PPP configuration	175
19.5	Frame Relay (FR)	176
19.6	FR congestion control	178
19.7	FR configuration	179



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub



Hour 20:	Wireless LAN	181
20.1	Wireless LAN basics	181
20.2	AP configuration	182
Hour 21:	IPv6	184
21.1	IPv6 basics	184
21.2	IPv6 addressing	185
21.3	IPv6 address configuration	187
21.4	IPv6 address types	188
21.5	IPv6 Routing protocols	189
21.6	Migration from IPv4 to IPv6	191

**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

SAP

About this book

This CCNA book offers you an easy, fast and precise understanding of the '640-802' CCNA syllabus.

By reading this course, you will acquire the necessary information and concepts about CCNA.

About the author:



Mohamed Salem is a communication engineer and an IT professional. He received his communication-engineering bachelor from Alexandria University in Egypt, and received his IT diploma from ITI, which is considered one of the best IT institutions in the Middle East. He is CCNA/CCNP and MCSA certified. He has worked as a communication engineer in a big system integrator company, and as an IT professional in a multinational mobile operator.

If you'd like to contact Mohamed Salem, you can send him an e-mail to m.ssalem@yahoo.com.

Alternatively, you can call him on +20-1118111687.

Introduction

This book gives a basic illustration for CCNA (Cisco Certified Network Associate), '640-802' syllabus, which is a pre-requisite certificate for most of the Cisco certifications.

CCNA course gives you the basic knowledge to operate a computer network.

In the first part of this book, network basics, you will learn different network layers, and the protocols that exist in every layer.

In the second part, network configurations, you will learn different networking devices, such as routers, switches, hubs, and the basic configurations for those devices. In addition, you will learn different routing protocols, which is responsible for delivering the sent data to its desired destination.

In the third part of this book, advanced topics, you will learn the basics of network security, wireless networks, and connecting your networks through the internet, and IPv6, which is a very important concept that will be used in all the networks in the near future.

This book does not get into the deep details of CCNA; however, it gives you a well understanding of '640-802' CCNA course concepts.

We hope that this book will be informative for you.

Part 1

NETWORK BASICS

Hour 1: About Computer Networks

1.1 What is a computer network?

A computer network is a collection of devices connected to each other, in order to allow every device to share its resources with other devices, and access other devices shared resources.

1.1.1 Computer network elements

End devices

Devices that have the resources to share with others, or devices that are used by the end users to access the shared resources.

Examples of the end devices are a 'PC', a 'laptop', a 'printer' and a 'server'.

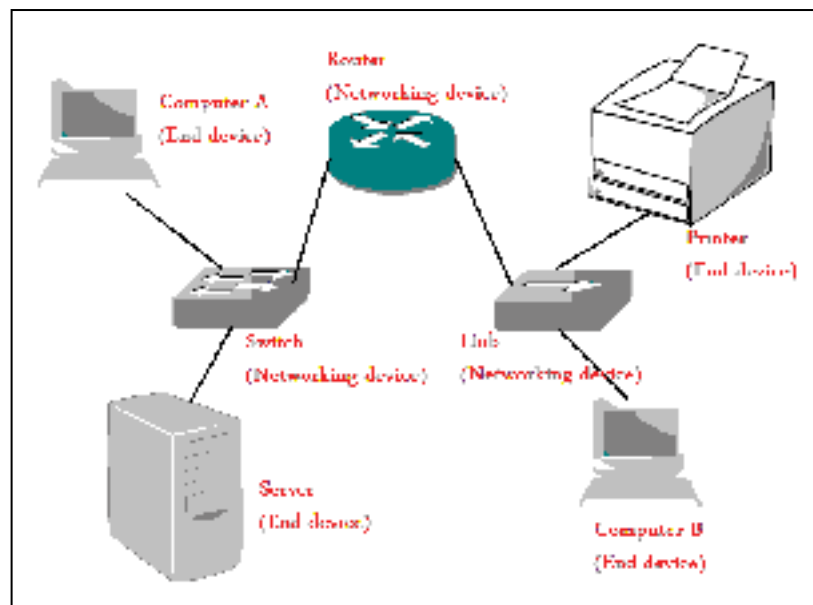


Figure 1.1 a computer network

Networking devices

Devices that are used to connect between end devices.

Examples of networking devices are a 'hub', a 'switch' and a 'router'.

1.2 Computer network topologies

There are different network topologies that we can use to connect network devices to each other.

1.2.1 Bus network topology

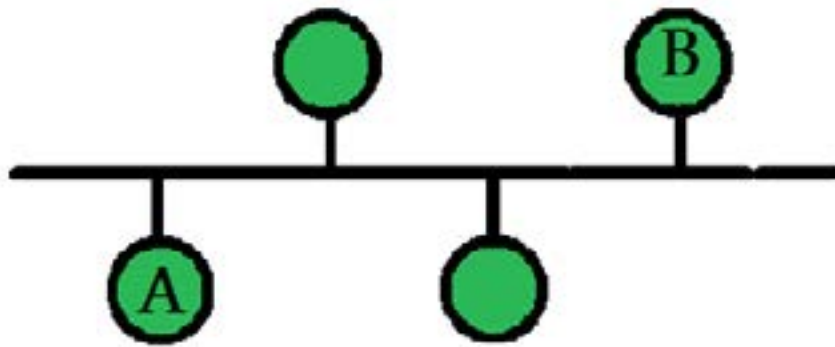


Figure 1.2: bus network topology

In this network topology, we use a bus – usually a copper cable or an optical fiber cable – to connect between network devices. This bus connects to the network devices through connectors that exit from it.

1.2.2 Ring network topology

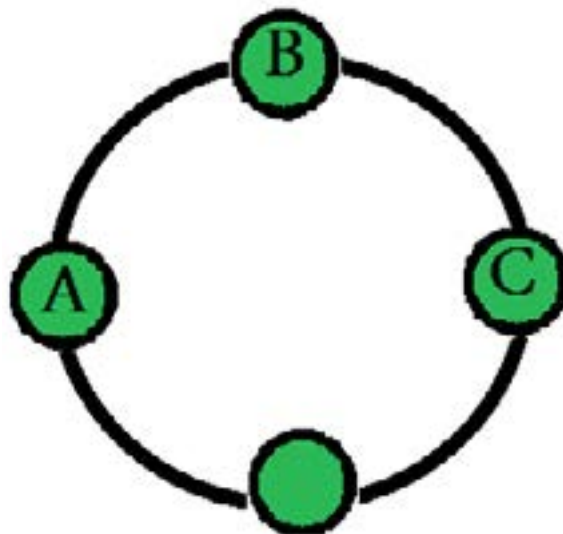
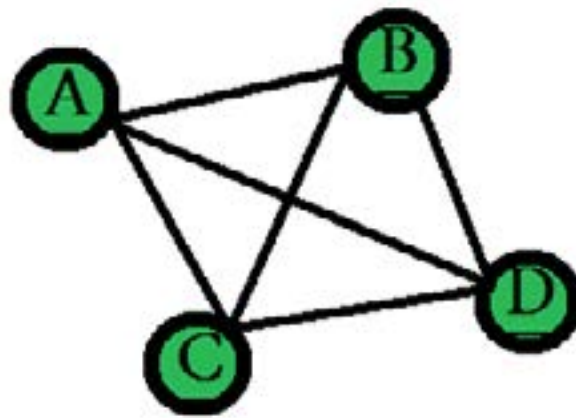


Figure 1.3: ring network topology

In the ring topology, we connect every network device to its neighbor devices; in order to make all the network devices form a ring.

1.2.3 Mesh network topology

Full mesh topology**Figure 1.4:** full mesh network topology

In the full mesh topology, we connect every network device to all the network devices that exists in the network. The advantage of this topology is the very high redundancy that it has.

Very high redundancy means that, if a path to a certain device became unavailable, there still an alternative path that can be used to reach this device.

ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

The disadvantage of the full mesh topology is that, it requires extensive number of connections between the devices.

Partial mesh topology

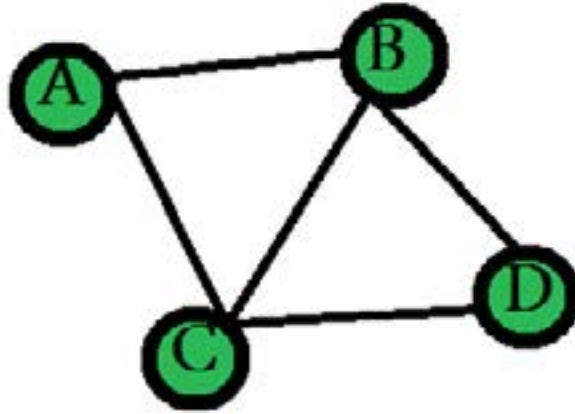


Figure 1.5: partial mesh network topology

In the partial mesh topology, every device is connected to some of the devices that exist in its network, not all devices like the full mesh topology.

The partial mesh topology requires fewer connections than the full mesh topology, which is considered an advantage. However, its redundancy is less than the full mesh topology.

1.2.4 Tree network topology

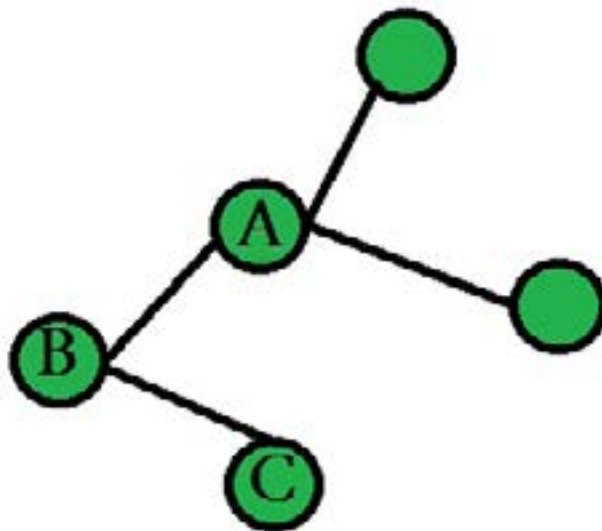


Figure 1.6: tree network topology

In (figure 1.6), 'device B' is a central device, called the 'hub device', while 'device A' and 'device C' are called the 'spoke devices'.

In this topology, the spoke devices talk to each other through the hub device.

The disadvantage of this topology is that, if the hub device became unavailable for any reason, the communication between spoke devices will not be possible. This is called 'single point of failure'.

1.2.5 Star network topology

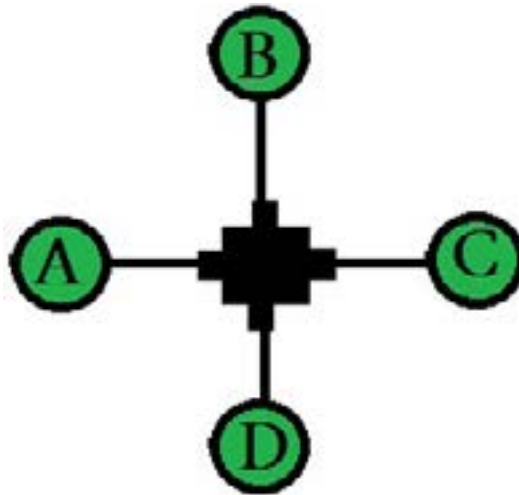


Figure 1.7: star network topology

This is the most widely used network topology.

In this topology, we use a central networking device to connect between all the end devices.

1.2.6 Hybrid network topology

This topology contains more than one of the previously illustrated network topologies connected to each other.

An example of this topology is connecting a star network topology to a ring network topology.

1.3 Simplex, half duplex and full duplex communication modes

1.3.1 Simplex communication mode



Figure 1.8: simplex communication mode

In the simplex communication mode, one of the devices is always the sender, while the other device is always the receiver.

As an example: the satellite (sender) and the dish (receiver).

1.3.2 Half duplex communication mode

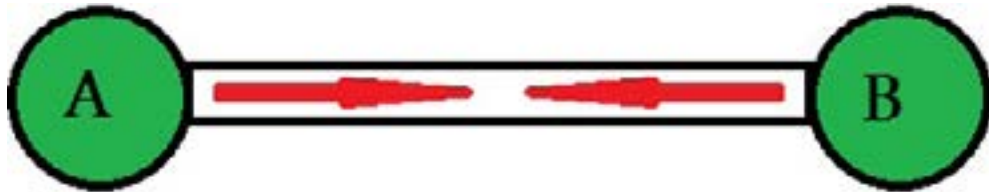


Figure 1.9: half-duplex communication mode

In the half-duplex communication mode, every device can only send or only receive in a certain time.

It means that the data could travel from 'device A' to 'device B' or from 'device B' to 'device A' in a certain time. Data could not travel in both directions in the same time.

An advertisement for SAP Learning Hub. The background shows a woman and a man in a modern office setting, looking at a tablet together. Overlaid on the image is the text 'NO-LIMITS LEARNING' in large yellow letters, followed by 'LEVERAGE SOCIAL LEARNING, COLLABORATION, QUALITY CONTENT, AND HANDS-ON PRACTICE.' in large black letters. At the bottom left is the 'SAP Learning Hub' logo, and at the bottom right is the 'SAP' logo.

NO-LIMITS LEARNING

**LEVERAGE SOCIAL LEARNING,
COLLABORATION, QUALITY
CONTENT, AND HANDS-ON
PRACTICE.**

SAP Learning Hub

SAP

1.3.3 Full duplex communication mode

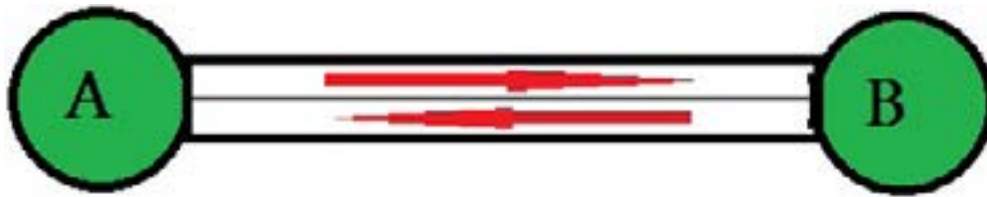


Figure 1.10: full duplex communication mode

In the full duplex communication mode, every device can send and receive data in the same time.

It is a two-way communication between the devices.

1.4 Carrier Sense Multiple Access / Collision Detection (CSMA / CD) protocol

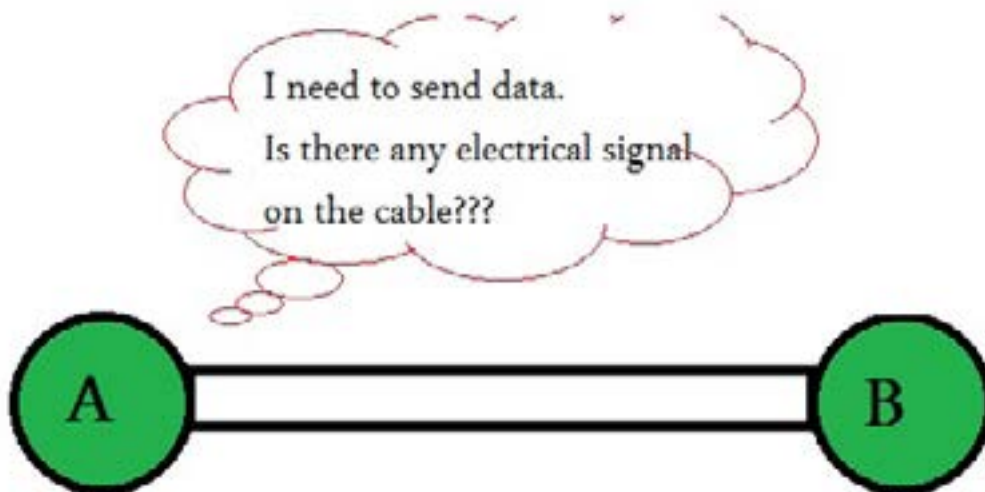


Figure 1.11: CSMA/CD protocol

Carrier Sense Multiple Access / Collision Detection (CSMA/CD) protocol is used in case of using the half-duplex communication mode. It prevents the collision between the data sent from different devices.

In this protocol, the device makes sure that there is no any electrical signal – which represents a data being sent by another device – exists on the cable before sending its own data.

Hour 2: Numbering systems

2.1 Decimal, hexadecimal and binary numbering systems

There are different systems that we can be used to write a certain number.

As an example, if we need to write the number 'sixty-three', we can use different numbering systems, as will be illustrated in this hour.

2.1.1 Decimal Numbering system

We learned this ordinary system from the childhood.

This system is formed from 10 digits (0, 1, 2, 3, 4, 5, 6, 7, 8, and 9) so; it is called the 'decimal numbering system'.

As an example, to write 'sixty-three' in the decimal numbering system, we simply write '63'.

An advertisement for SAP Learning Hub. The background is a blurred cityscape with a tall building. In the foreground, a man with glasses and a dark sweater is looking at a tablet. The text is overlaid on the image.

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub

SAP

2.1.2 Hexadecimal numbering system

This is a numbering system that is formed from 16 digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F).

As an example, if we need to write 'sixty-three' in the hexadecimal numbering system, we will write '3F'.

The digits from 'A' to 'F' in the hexadecimal system are equivalent to the numbers from '10' to '15' in the decimal system respectively.

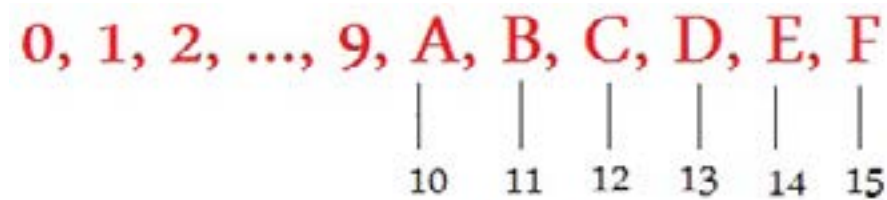


Figure 2.1: the relation between the hexadecimal and the decimal numbering systems.

2.1.3 Binary numbering system

This numbering system is formed from only two digits (0 and 1).

As an example, if we need to write 'sixty-three' in the binary numbering system, we will write '00111111'.

Binary numbering system, basic information

If we wrote a binary number '10010010', we should know the following,

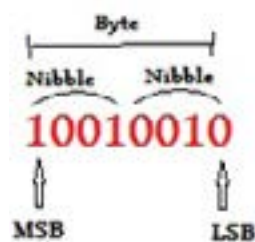


Figure 2.2: the binary number basic elements

1. Every '0' or '1' of the above digits is called a '**bit**'.
2. Every 4 bits are called a '*nibble*'.
3. Every two nibbles (8 bits) are called a '*byte*'.
This means that, **8 bits = 2 nibbles = 1 byte**.
4. The most left bit is called the '**most Significant Bit**' or the '**MSB**'.
5. The most right bit is called the '**least Significant Bit**' or the '**LSB**'.

2.2 How to convert from binary to decimal

To convert a number from the binary numbering system to the decimal numbering system, we should know the **weight** of every binary digit (bit) in this binary number.

The weight of every bit depends on its location in the binary number.

The MSB has the highest weight, while the LSB has the least weight.

As an example, if we have a binary number that is formed from eight bits. The weight of every bit will be as following,

128 64 32 16 8 4 2 1

Figure 2.3: the binary digits weight

The **LSB** weight = **1**

The **MSB** weight = **128**

To convert from the binary numbering system to the decimal numbering system, we multiply every bit by its weight then we aggregate all the results.

Example:

Convert the following binary number '**10010010**' to the decimal numbering system.

Answer:

We multiply every bit by its weight, and then we aggregate all the results.

128		64		32		16		8		4		2		1
x		x		x		x		x		x		x		x
1		0		0		1		0		0		1		0
128	+	0	+	0	+	16	+	0	+	0	+	2	+	0
= 146														

So, the binary number '**10010010**' = the decimal number '**146**'.

2.3 How to convert from decimal to binary

To convert from the decimal system to the binary system, we will also use the binary digits weight.



Figure 2.4: the binary digits weight

The way of conversion is as following,

We take the decimal number and divide it over the first weight **128**.

We write the result as the MSB in the binary number, and take the remaining and divide it over the second weight **64**.

We write the result as the bit before MSB, and take the remaining and divide it over the third weight **32**.

....

We continue doing the previous steps until the last weight **1**.

Example 1:

Convert the decimal number '65' to its equivalent binary number.



MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub

SAP

Answer:

$65/128 = 0$ and remaining 65

$65/64 = 1$ and remaining 1

$1/32 = 0$ and remaining 1

$1/16 = 0$ and remaining 1

$1/8 = 0$ and remaining 1

$1/4 = 0$ and remaining 1

$1/2 = 0$ and remaining 1

$1/1 = 1$ and remaining 0

So, the equivalent binary number will be = **01000001**

Example 2:

Convert the decimal number '133' to its equivalent binary number.

Answer:

$133/128 = 1$ and remaining 5

$5/64 = 0$ and remaining 5

$5/32 = 0$ and remaining 5

$5/16 = 0$ and remaining 5

$5/8 = 0$ and remaining 5

$5/4 = 1$ and remaining 1

$1/2 = 0$ and remaining 1

$1/1 = 1$ and remaining 0

So, the equivalent binary number will be = **10000101**

2.4 How to convert between hexadecimal and binary

2.4.1 Convert from hexadecimal to binary

The digits from 'A' to 'F' in the hexadecimal system are equivalent to numbers from '10' to '15' in the decimal system respectively.

0	1	2	...	9	A	B	C	D	E	F
					10	11	12	13	14	15

Figure 2.5: the relation between the hexadecimal and the decimal numbering systems.

To convert from the hexadecimal system to the binary system, we do the following,

1. Convert every digit in the hexadecimal number to its equivalent in the decimal numbering system.
2. Convert every number in the decimal system to its equivalent in the binary numbering system.

Figure (2.6) illustrates how we can convert from the hexadecimal numbering system to the binary numbering system.

<u>Hexadecimal</u>		<u>Decimal</u> (each digit alone)		<u>Binary</u>
2	_____	2	_____	0010
C	_____	12	_____	1100
3F	_____	3 15	_____	0011 1111
FF	_____	15 15	_____	1111 1111

Figure 2.7: hexadecimal to binary conversion

2.4.2 Convert from binary to hexadecimal

To convert from the binary system to the hexadecimal system, we make the following.

1. Convert every nibble (4 bits) in the binary number to its equivalent in the decimal system
2. Convert every decimal number to its equivalent in the hexadecimal.

<u>Hexadecimal</u>		<u>Decimal</u> (each digit alone)		<u>Binary</u>
2	_____	2	_____	0010
C	_____	12	_____	1100
3F	_____	3 15	_____	0011 1111
FF	_____	15 15	_____	1111 1111

Figure 2.7: hexadecimal to binary conversion

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



2.5 How to convert between hexadecimal and decimal

2.5.1 Convert from hexadecimal to decimal

The digits from 'A' to 'F' in the hexadecimal system are equivalent to numbers from '10' to '15' in the decimal system respectively.

0	1	2	...	9	A	B	C	D	E	F
					10	11	12	13	14	15

Figure 2.7: binary to hexadecimal conversion

To convert from the hexadecimal system to the decimal system, we do the following,

1. Convert every digit in the hexadecimal number to its equivalent in the decimal numbering system.
2. Convert every number in the decimal number to its equivalent in the binary numbering system.
3. Convert the binary number to its equivalent in the decimal numbering system.

Figure (2.9) illustrates how we can convert from the hexadecimal numbering system to the decimal numbering system.

<u>Hexadecimal</u>		<u>Decimal</u> (each digit alone)		<u>Binary</u>		<u>Decimal</u>
2	_____	2	_____	0010	_____	2
C	_____	12	_____	1100	_____	12
3F	_____	3 15	_____	0011 1111	_____	63
FF	_____	15 15	_____	1111 1111	_____	255

Figure 2.9: convert from the hexadecimal to the decimal numbering systems.

2.5.2 Convert from decimal to hexadecimal

To convert from the decimal system to the hexadecimal system, we make the opposite steps of the previous operation.

1. Convert the decimal number to its binary equivalent
2. Convert every nibble (4 bits) in the binary number to its equivalent in the decimal system.
3. Convert every number in the decimal number to its equivalent in the hexadecimal system.




<u>Decimal</u>		<u>Binary</u>		<u>Decimal</u> (each nibble alone)		<u>Hexadecimal</u>
2	_____	0010	_____	2	_____	2
12	_____	1100	_____	12	_____	C
63	_____	0011 1111	_____	3 15	_____	3F
255	_____	1111 1111	_____	15 15	_____	FF

Figure 2.10: decimal to hexadecimal conversion

Hour 3: TCP/IP and OSI suit

3.1 TCP/IP layers

The TCP/IP protocol suit divides the network communications into different layers.

As seen in figure (3.1), the layers are the network interface layer, the internetworking layer, the transport layer, and the application layer.

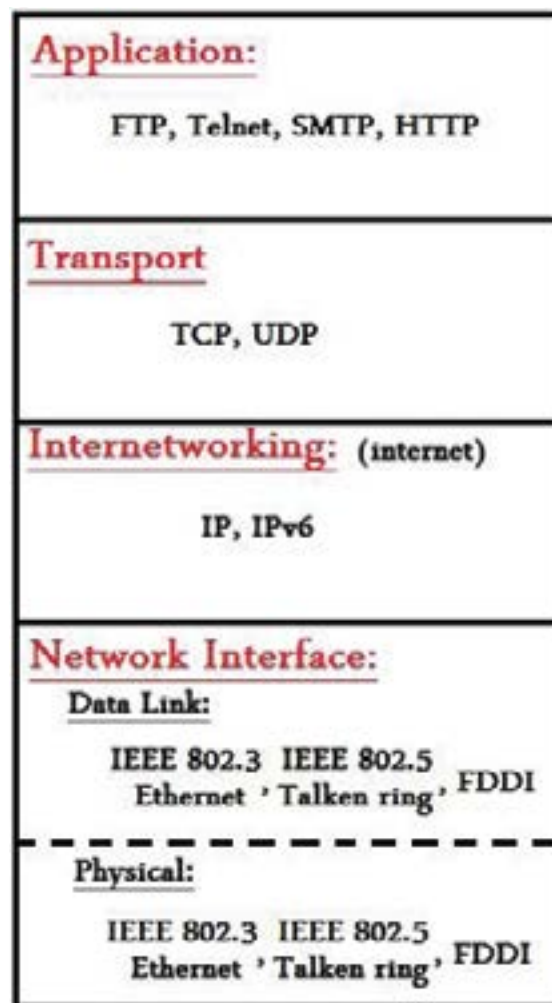


Figure 3.1: the TCP/IP protocol suit

Every layer of those layers has a determined role in the network communications.

the 'network interface layer' may be divided into two other layers, the 'physical layer', and the 'data link layer'.

The TCP/IP protocol suit has another two names, the 'internet protocol suit', and the 'DoD protocol suit'.

3.1.1 Physical layer (layer 1)

The physical layer translates the data that it receives from the upper layers to a physical entity –an electrical signal or an optical pulse- to be able to transmit it through the communication medium.

The physical layer specifies the network devices electrical and physical specifications. As an example, it defines the electrical and physical specifications of the network port that exists in the ‘network interface card (NIC)’, and defines the electrical and physical specifications for the cable that is connected to this network port.

3.1.2 Data link layer (layer 2)

The data link layer is responsible for the data communications between any two devices inside the same network.

This layer uses the ‘physical address’ of the communicating devices to distinguish between those devices.

Physical address: it is a hard coded address on the ‘Network Interface Card (NIC)’ of any network device.



JUMP-START CAREERS

**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub

SAP



Figure 3.2: the data link layer is responsible for communicating between two devices inside the same network

3.1.3 Internetworking layer (layer 3)

This layer may be called the 'Internet layer'.

The internetworking layer's role is to route the data between networks using the logical addresses.

Logical address: It is an address assigned to every network and every network device by the network administrator.

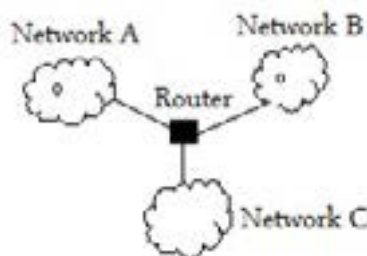


Figure 3.3: the internetworking layer is responsible for the communication between networks.

3.1.4 Transport layer (layer 4)

The transport layer's role is to make error correction, reliable delivery of data, segmentation of the data, and reassembling of the data, and it is responsible for the host-to-host communication.

3.1.5 Application layer (layer 5)

The application layer provides functions for users or their programs, and it is responsible for the data encryption and decryption, and the data compression and decompression.

3.2 Data encapsulation process

Suppose that we have two computers, a **source**, and a **destination**. The source computer sends some data to the destination computer.

In the **source computer**, every layer takes the data that is coming to it from the upper layer. Then, it adds a certain header to this data. Then, it delivers the data to the lower layer.

In the **destination computer**, every layer receives the data from the lower layer. Then, it removes the layer header. Then, it sends the data to the upper layer.

Every layer header contains important information that is used by this layer.

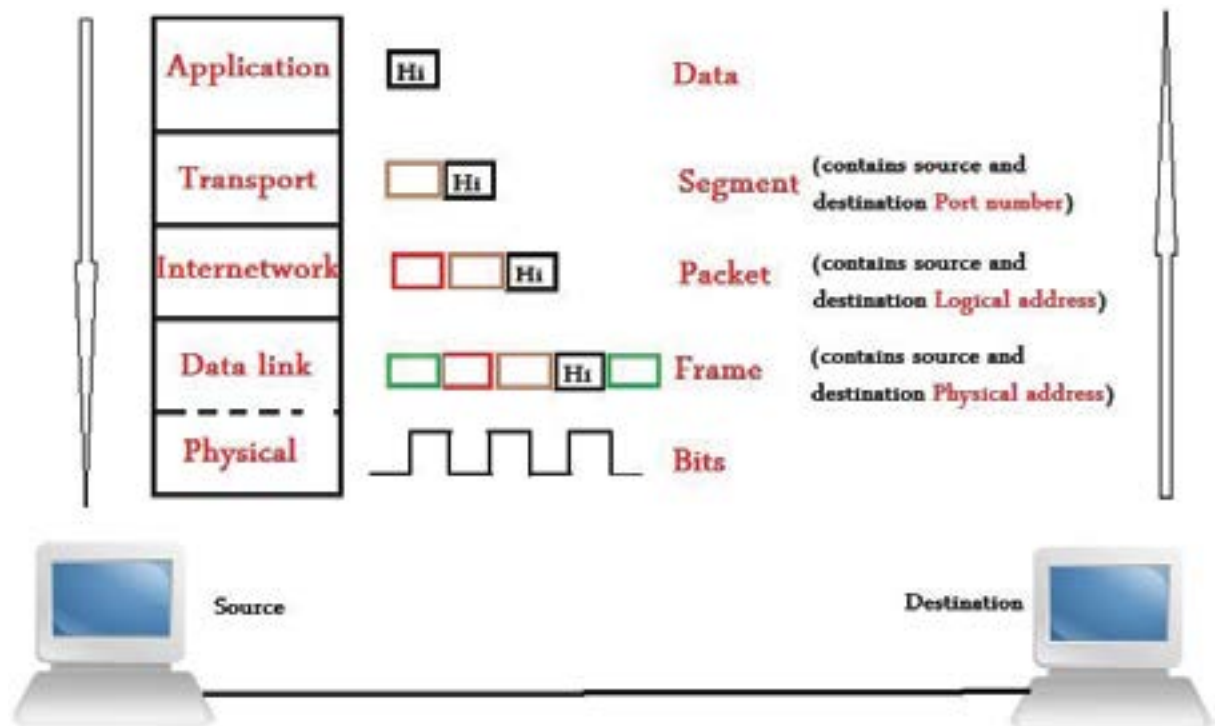


Figure 3.4: data encapsulation process

As seen in figure (3.4), the data in every layer is given a certain name,

In the transport layer, the data is called a **segment**.

In the internetworking layer, the data is called a **packet**.

In the data link layer, the data is called a **frame**.

The physical layer takes the data from the upper layer and sends it over the physical medium in the form of **bits**.

3.3 OSI model layers

The OSI (Open System Interconnection) model divides the network communication into seven layers.

Those layers are the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer.

Figure (3.5) illustrates the role of every layer of the seven layers.

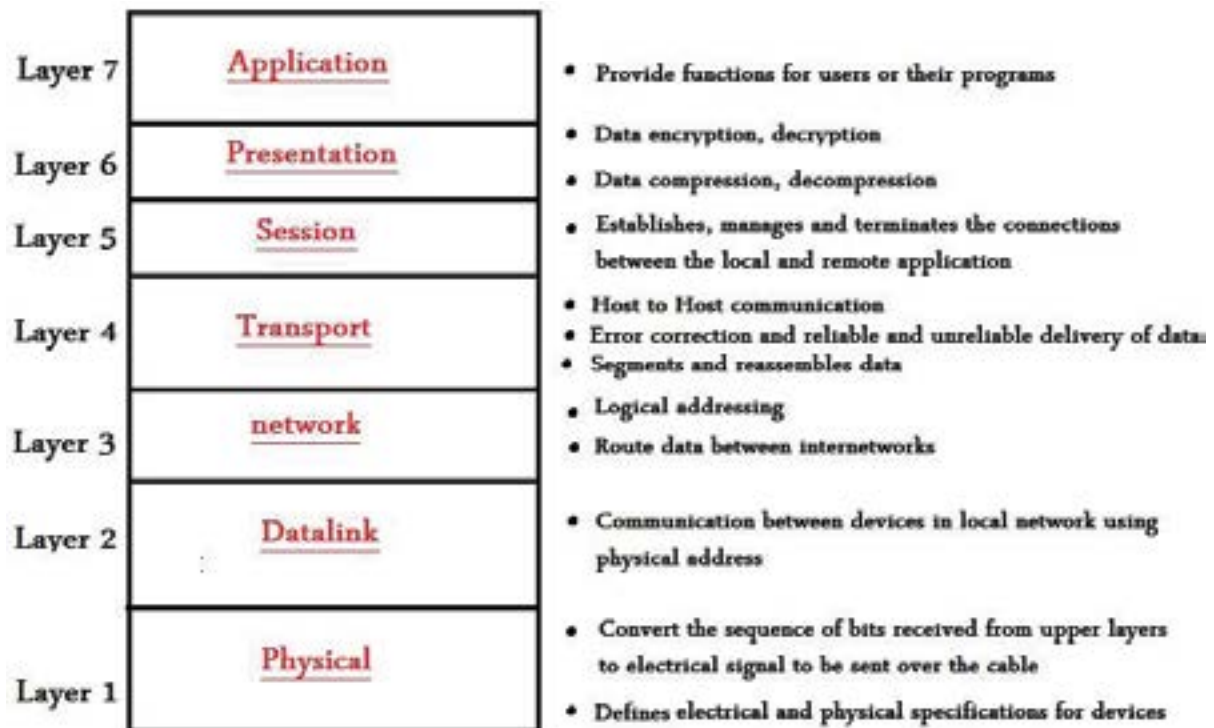


Figure 3.5: the OSI model



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub



Hour 4: Network Interface Layer

4.1 Ethernet protocol in the physical layer

The Ethernet protocol has another name, which is 'IEEE 802.3'. Moreover, it specifies the electrical and physical specifications of the devices' network interfaces, the cables, and the connectors that connect the network interfaces to the cables.

The Ethernet protocol determines some standards that are used to determine the specifications of the cables that connect between the network devices.

Every standard determines the cable type that should be used, and the maximum usable length of this cable.

4.1.1 Different cable types

1. Unshielded Twisted Pair (UTP)



Figure 4.1: the UTP cable and its connector 'RJ45'

The UTP cable consists of eight 'wires'. Every two wires are twisted with each other, and they are called a 'pair'. Therefore, the UTP cable has four pairs.

Every pair consists of two wires. One of them has a certain color and the other has the same color mixed with the white color.

The eight wires of the UTP cable has the following colors, brown, white brown, blue, white blue, orange, white orange, green, and white green.

The UTP cable connector is called the 'RJ45', which consists of eight pins. Every pin connects to one of the UTP wires.

2. Coaxial cable

Another cable type that can be used to connect between the end devices is called the 'coaxial cable' which is seen in the figure (4.2).



Figure 4.2: the coaxial cable

3. Optical fiber cable



Figure 4.3: the optical fiber cable

The optical fiber cable transmits optical pulses instead of electrical signals. So, it does not get interfered by electrical interference.

There are two types of the optical fiber cables, **single-mode**, and **multimode**.

4.1.2 Ethernet protocol cable standards

As seen in table (4.1), every standard determines the cable type it uses and the maximum length of this cable that can be used.

Standard	cable type	maximum length supported
10Base2 (thinnet)	Coaxial	200 m
10Base5 (thicknet)	Coaxial	500 m
100BaseTX	UTP (cat 5,6,7)	100 m
100BaseFX	Optical Fiber (multimode)	400 m
1000BaseT	UTP (cat 5)	100 m
1000BaseSX	Optical Fiber (multimode)	550 m
1000BaseLX	Optical Fiber (singlemode)	10 Km

Table 4.1: Ethernet protocol cable standards

As you can see, the standard name consists of three parts,

First part

It determines the connection speed,

If the first part is '10', this means that the speed of the connection is 10Mbps (**Ethernet connection**).

If the first part is '100', this means that the speed of the connection is 100Mbps (**fast Ethernet connection**).

If the first part is '1000', this means that the speed of the connection is 1000Mbps (**gigabit Ethernet connection**).

Second part

It determines the modulation technique; 'Base' means that the standard is using the 'baseband modulation'.

Third part

It determines the type of cable that should be used.

From the previous illustration, we can know that, '**100BaseFX**' means that the connection is a 'fast Ethernet' connection and the cable type is an 'optical fiber multimode' cable.



**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

SAP

4.2 UTP cabling

The UTP cable connector is called 'RJ45'. The 'RJ45' has eight pins; every pin should be connected to one of the UTP cable wires.



Figure 4.4: a UTP cable and its connector

There are three connection methods for the UTP cable with its connector, every method is used in a certain situation. The three methods are, 'straight through', 'cross over', and 'rolled'.

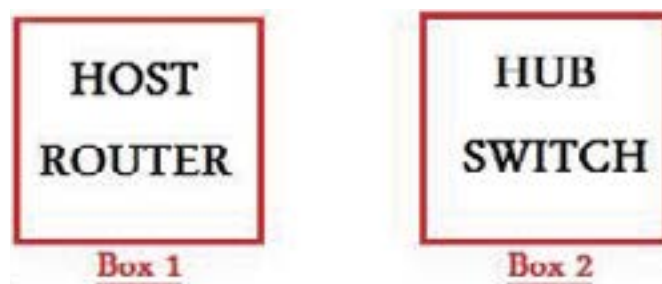


Figure 4.5: dividing network devices into two boxes

We can divide the network devices into two groups or boxes as seen in figure (4.5).

The devices in any network are one of the following, a host (e.g. a PC or a server), a hub, a switch, or a router.

As seen in figure (4.5), we can put the host and the router in the same group, and we can put the hub and the switch in the same other group.

If we need to connect between two devices that exist in the same group, we use a 'cross over' cable.

If we need to connect between two devices that exist in different groups, we use a 'straight through' cable.

Straight through cable

In the straight through cable, the first pin in the first connector is connected to the first pin in the second connector, and the same connection for the remaining pins as seen in figure (4.6).

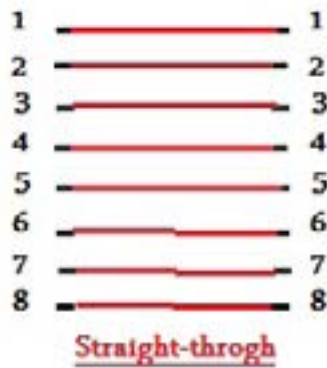


Figure 4.6: a straight through cable

Cross over cable

In the cross over cable, as seen in figure (4.7), we connect the first pin in the first connector to the third pin in the second connector, and we connect the second pin in the first connector to the sixth pin in the second connector, and the third pin in the first connector to the first pin in the second connector.

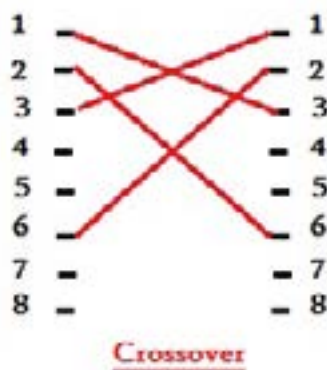


Figure 4.7: a cross over cable

Rolled cable

It is used to connect a PC to the router's consol port in case that we need to configure the router.

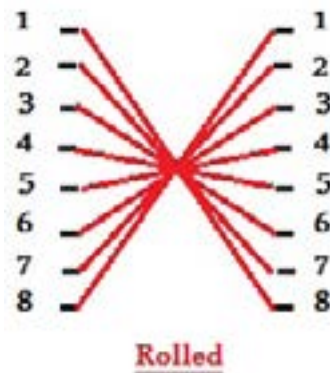


Figure 4.8: a rolled cable

As seen in figure (4.8), we connect the first pin in the first connector to the last pin in the second connector, and connect the second pin in the first connector to the seventh pin in the second connector, and so on until we reach the last pin.

ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

4.3 'Hub', a device working in the physical layer

As seen in figure (4.9), the 'hub' is a device that has several ports in it. Every port can be connected to a network device.

When the frames arrive to the hub on one of its ports, it forwards those frames to all the devices connected to its ports.

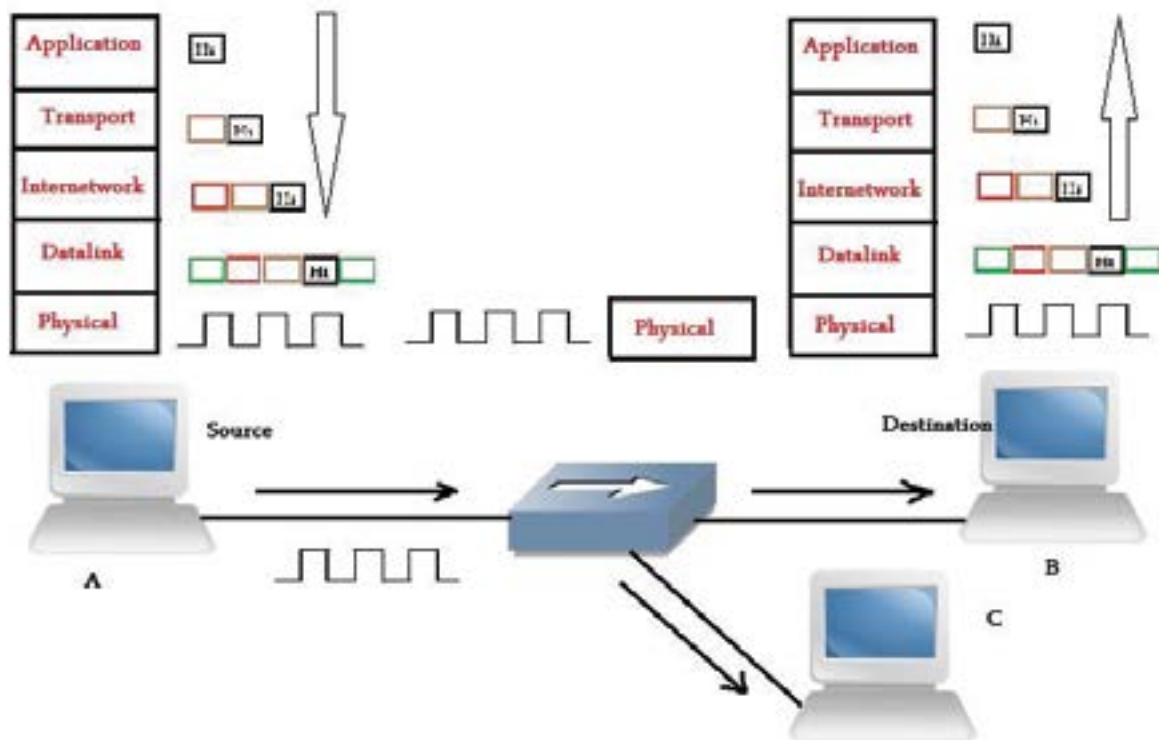


Figure 4.9: sending data between the end devices through a hub

As seen in figure (4.9), suppose that we have a network that contains several computers, 'computer A' needs to send some data to 'computer B'.

Simply, 'computer A' will send the data to the hub, and then the hub will take the data and flood it through all of its ports. Therefore, the data will reach 'computer B'.

4.4 Ethernet protocol in the data link layer

The function of the Ethernet protocol in the data link layer is to enable two end devices in the same network to be able to send data to each other using the physical address.

The physical address in the Ethernet protocol is called the 'MAC address'.

Suppose that we have three computers connected with a hub, as seen in figure (4.10).

Suppose that 'computer A' needs to send some data to 'computer B'.

To accomplish this task, 'computer A' will send a frame that contains the MAC address of the 'computer B' as the destination address.

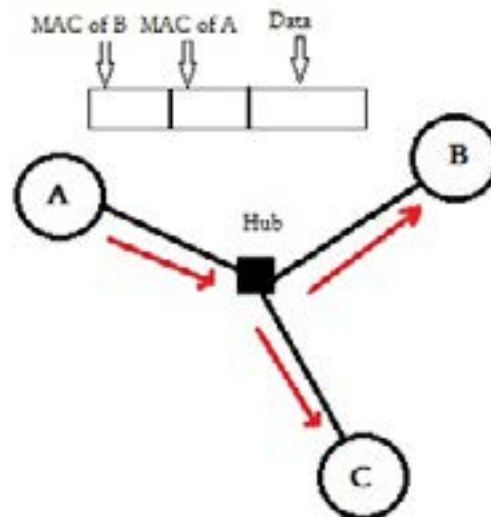


Figure 4.10: computers in the same network connected using a hub

4.4.1 Ethernet frame

In figure (4.11), we can see the full components of the Ethernet frame.

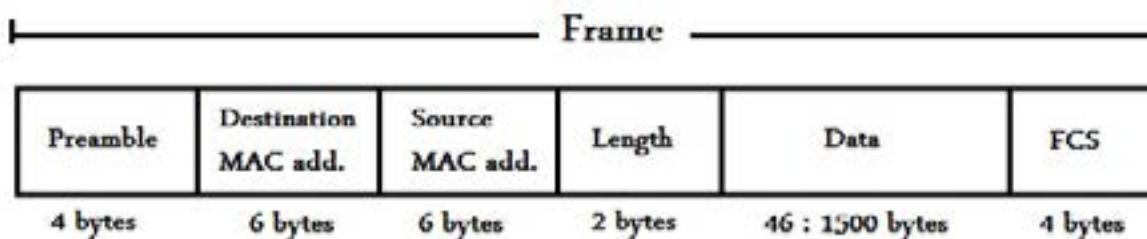


Figure 4.11: Ethernet frame

Data is the data that are received by the data link layer from the upper layers.

Preamble is a stream of bits that is used by the source and the destination to make synchronization between them.

Length is the length of the whole frame in bytes.

Destination MAC address is the MAC address of the destination device.

Source MAC address is the MAC address of the source device.

FCS (Frame Check Sequence), Ethernet uses it to check if there are any errors in the received frame, and it will reject the frame if any errors are found.

4.5 What is the MAC address?

The MAC (Media Access Control) address may be called the 'physical address' or the 'hardware address'.

The manufacturer of the network interface card (NIC) hard codes the MAC address on every (NIC).

Every NIC has its unique MAC address.

The MAC address consists of six bytes (48 bits).

The most significant 24 bits (3 bytes) represents the Organizationally Unique Identifier (OUI), which is a unique code for every manufacturer of the NICs.

The least significant 24 bits (3 bytes) represents the manufacturer assigned code to the NIC.

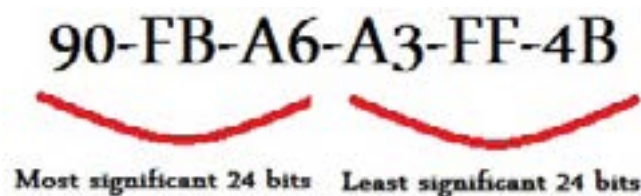


Figure 4.12: example of a MAC address



4.6 'Switch', a device working in the data link layer

The switch is an intelligent device, because when it receives an electrical signal on one of its ports, it does not flood it through all of the ports, but it looks at the destination MAC address and forwards the data through a certain port according to this destination MAC address. This process is called **'filtering'**.

The switch forwards the data it receives to a certain port depending on the **'MAC address table'**, which is stored on the switch's memory.

The MAC address table contains two columns, the 'Port Number', and the 'MAC address', as seen in figure (4.13).

MAC address table

Port	MAC add.
fa 0/0	AA
fa 0/1	BB
fa 0/2	CC

Figure 4.13: the MAC address table

4.6.1 Case study

In Figure (4.14), 'computer A' needs to send some data to 'computer B'.

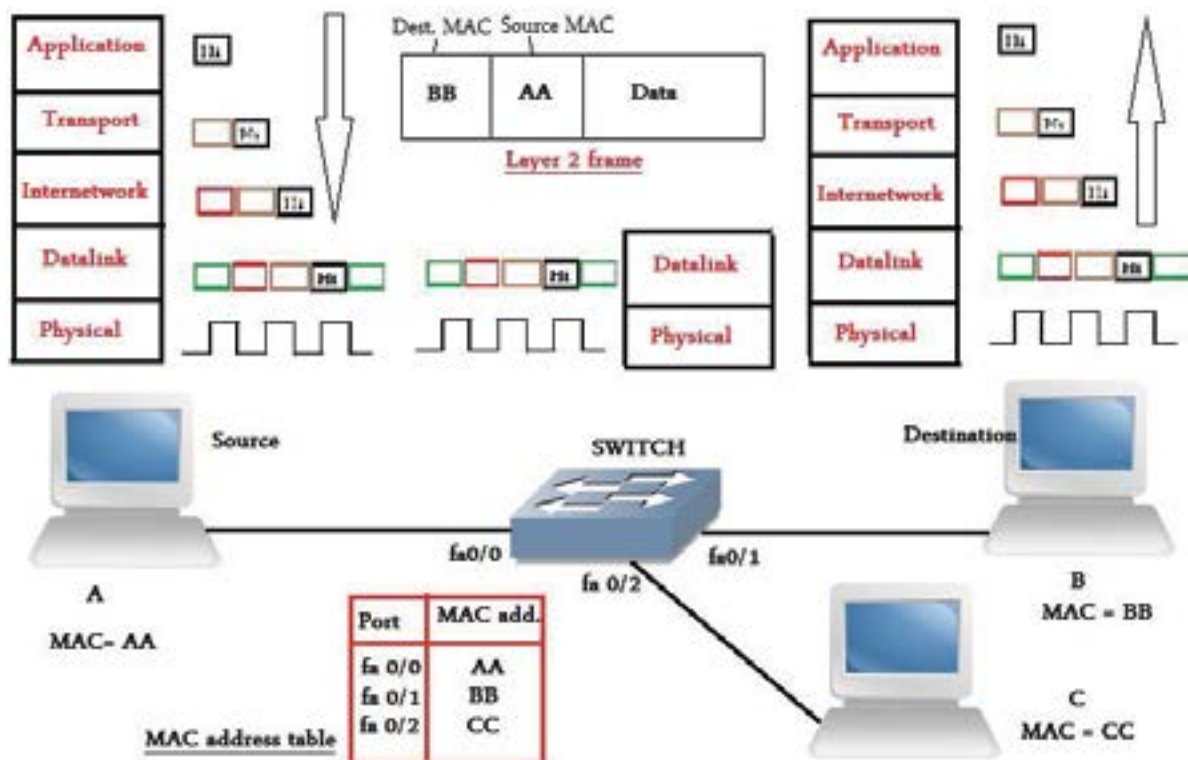


Figure 4.14: sending data through a switch

In this case, 'computer A' will send the frames with the MAC address of the 'computer B' as the destination MAC address. When the frames reach the switch, the switch will look for the destination MAC address in its MAC address table. Therefore, it will decide through which port it should forward the frames.

In this case, the switch will forward the frames through port 'fa 0/1'.

Some of the switch operation notes,

1. How does a switch build its MAC address table?

Whenever the switch receives a frame on any port of its ports, it will look at the source MAC address that exists in this frame. Then, it will record this MAC address in its MAC address table, combined with the switch port that received the frame.

2. What happens if the switch did not find any match to the destination MAC address in the MAC address table?

In this case, it will flood the frame out of all of its ports. Therefore, in this case it will work as a hub.

4.7 Collision domain

The collision domain is the group of devices that share the same medium. This means that if two of those devices sent some data in the same time, there will be a collision between those data.

The hub does not divide the collision domain

In figure (4.15), we have three computers connected with a hub. The three computers exist in the same collision domain. This means that if two of those devices sent some data at the same time, a collision will happen between those data. In addition, no device will receive any data.

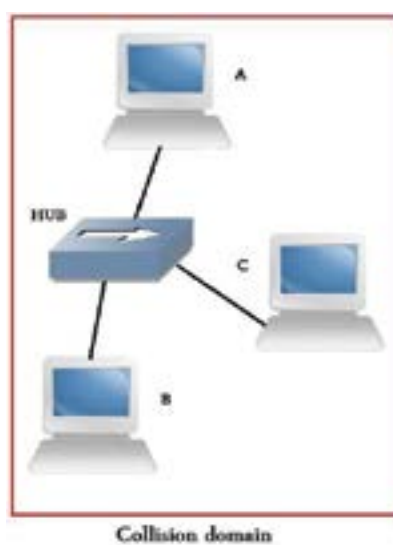


Figure 4.15: the hub does not divide the collision domain

To avoid the collision between the data, devices should use CSMA/CD protocol.

The switch divides collision domains

In figure (4.16), we have three computers connected with a switch.

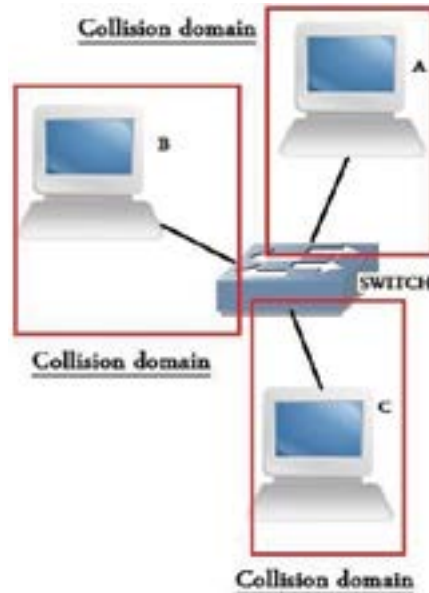


Figure 4.16: the switch divides the collision domain

The switch divides the collision domain. Therefore, every computer exists in its own collision domain. This means that if two of those computers sent some data in the same time, there will be no collision between those data.

So, using a switch will increase the through output of the network and will enhance the network performance.

Hour 5: Internetworking Layer

5.1 IP (Internet Protocol)

The function of the internetworking layer is to route the data between networks using the logical address.

One of the protocols that are working in the internetworking layer is the internet protocol.

The logical address in the internet protocol is called the 'IP address'.

The IP address is formed of four bytes, which are equivalent to 32 bits.

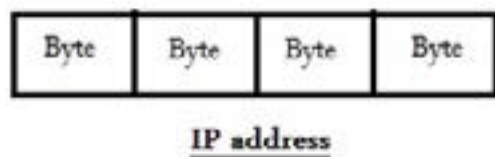


Figure 5.1: the IP address format

Every byte of the IP address equals a decimal value from the range '0:255'.

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub

SAP

The advertisement features a man in a dark sweater and glasses holding a tablet, standing in front of a blurred city skyline. The SAP logo is in the bottom right corner.

5.1.1 IP address classes

IP addresses are grouped into different 'IP classes' depending on the value of the first byte in every IP address.

From the class of the IP address, we can determine the network portion and the host portion of this IP address.

When we determine the network portion and the host portion of the IP address, we can determine the network IP and the broadcast IP of this IP address.



Figure 5.2: the classes of the IP address

From figure (5.2), we can deduce the following,

In the 'class A' IP address, the network portion is the first byte while the host portion is the last three bytes.

In the 'class B' IP address, the network portion is the first two bytes while the host portion is the last two bytes.

In the 'class C' IP address, the network portion is the first three bytes while the host portion is the last byte.

How to determine the class of the IP address

In the 'class A' IP addresses, the first byte in the IP address is a decimal value in the range '0: 127'.

In the 'class B' IP addresses, the first byte in the IP address is a decimal value in the range '128: 191'.

In the 'class C' IP addresses, the first byte in the IP address is a decimal value in the range '192: 223'.

In the 'class D' IP addresses, the first byte in the IP address is a decimal value in the range '224: 239'.

In the 'class E' IP addresses, the first byte in the IP address is a decimal value in the range '240: 255'.

5.2 Network IP?

The network IP is an IP address that is given to a network.

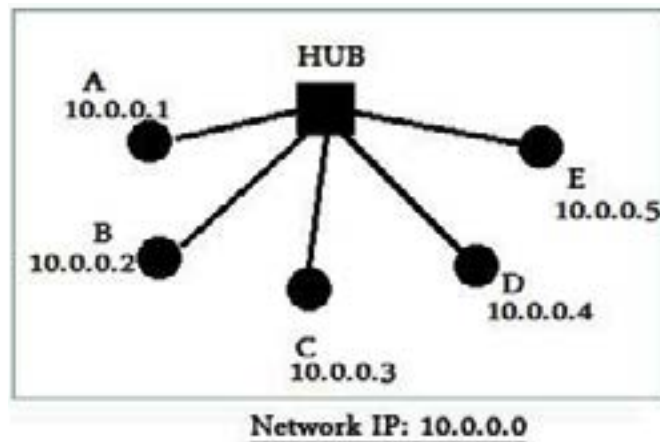


Figure 5.3: network IP

Suppose that we have some network devices that exist in the same network, the network administrator can assign a certain IP address to every device.

The network IP is the IP address of the network that contains all the network devices.

In figure (5.3), we can see that the network IP of the network that contains all the devices is '10.0.0.0'.

How to get the network IP from any IP address

To get the network IP from any IP address we should take the following steps,

1. Determine the network portion and the host portion in the IP address.
2. Convert the host portion of the IP address to 'zeros'.

Note, we should do 'step 2' while the IP address is written in the binary numbering format.

Case study:

Get the network IP for each of the following IPs,

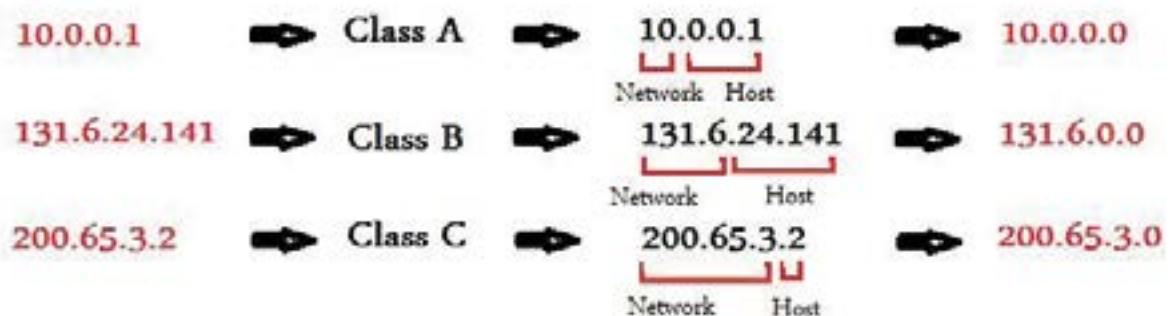


Figure 5.4: case study – getting the network IP address

5.3 Broadcast IP?

The broadcast IP is used when we need certain packets to reach all of the devices in a certain network.

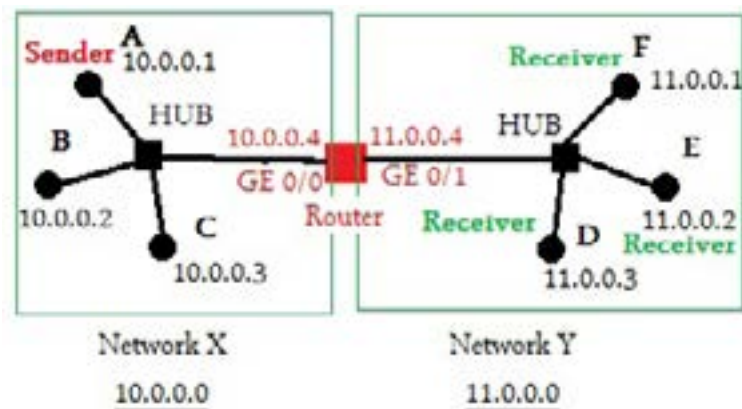


Figure 5.5: the broadcast IP

How to get the broadcast IP from any IP address

To get the broadcast IP from any IP address, we do the following,

1. Determine the network portion and the host portion in this IP address.
2. Convert the entire host portion to 'ones'.

MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub

SAP

Note, we should do 'step 2' while the IP address is written in the binary numbering format.

Case study:

Get the broadcast IP for each of the following IPs,

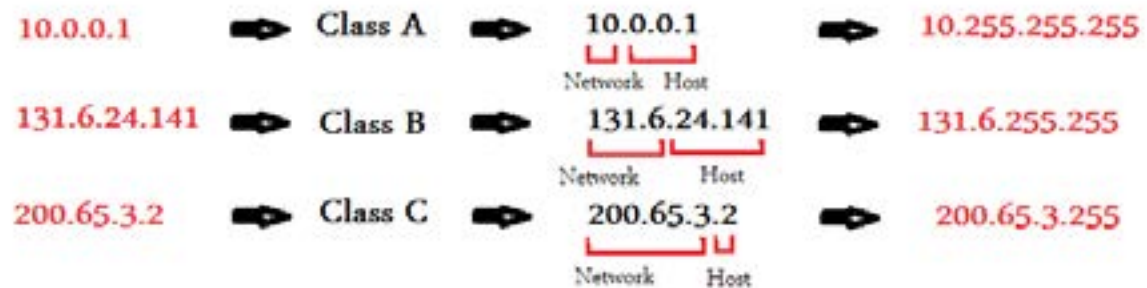


Figure 5.6: case study – getting the broadcast IP address

5.4 Unicast, multicast and broadcast communication

5.4.1 Unicast communication

Unicast communication is a 'one to one' communication. One device, a source, sends some data to only one device, a destination.

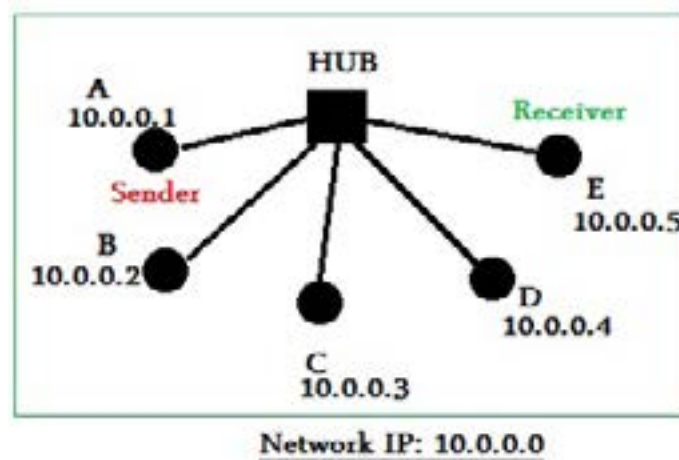


Figure 5.7: the unicast communication

In the unicast communication, the packet will be as following,

Dest. IP	Source IP	
10.0.0.5	10.0.0.1	Data

Figure 5.8: the unicast packet

5.4.2 Multicast communication

The multicast communication is a 'one to many' communication. One device is sending data to many devices in a certain network.

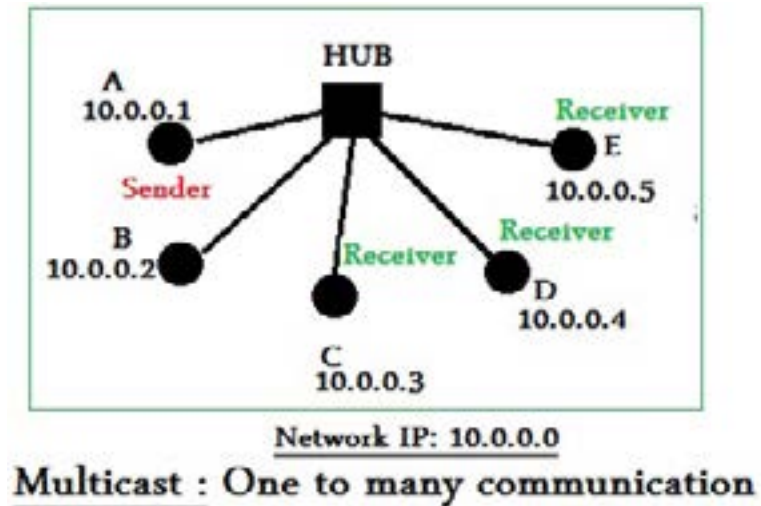


Figure 5.9: the multicast communication

In the multicast communication, the destination IP is a 'class D' IP address.

Dest. IP	Source IP	
224.0.0.10	10.0.0.1	Data

Figure 5.10: the multicast packet

5.4.3 Broadcast communication

The broadcast communication is a 'one to all' communication. One device is sending some data to all devices in a certain network.

Undirected broadcast

In the undirected broadcast communication, one device is sending data to **all the devices in its network**.

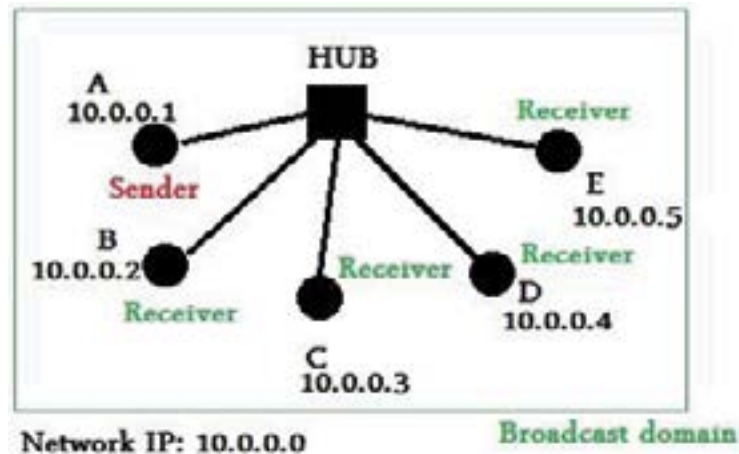


Figure 5.11: the undirected broadcast communication

In the undirected broadcast communication, the destination IP will be all ones (255.255.255.255).

Dest. IP	Source IP	
255.255.255.255	10.0.0.1	Data

Figure 5.12: the undirected broadcast packet

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



SAP

Directed broadcast

In the directed broadcast communication, one device is sending data to **all devices in a certain network**.

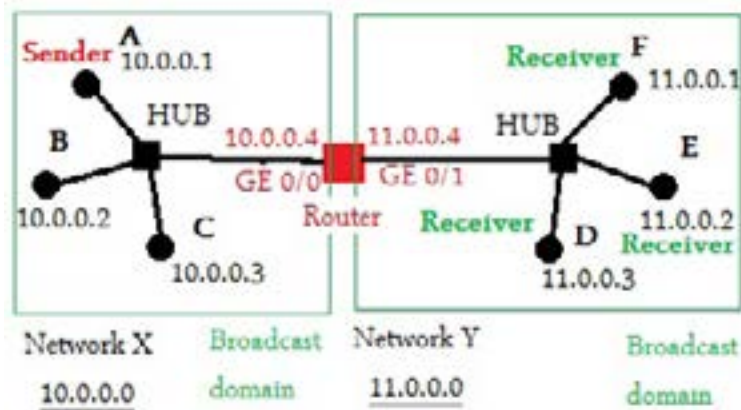


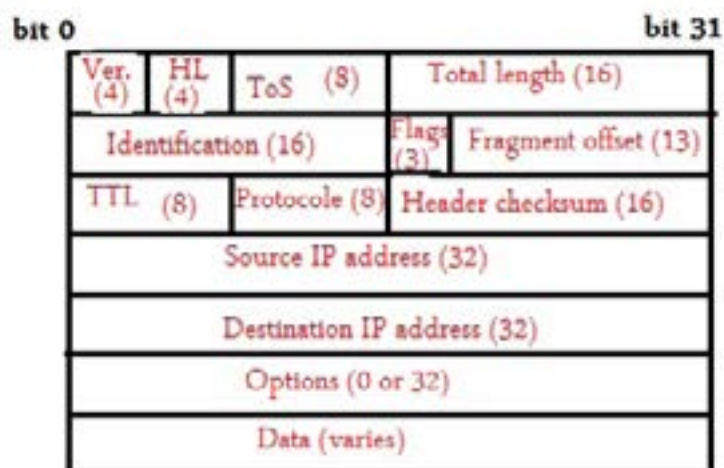
Figure 5.13: the directed broadcast communication

In this case, the destination IP will be the broadcast IP of the destination network.

Dest. IP	Source IP	
11.255.255.255	10.0.0.1	Data

Figure 5.14: the directed broadcast packet

5.5 IP header



IP header

Figure 5.15: the IP header

Ver: protocol version

HL: the header length in 32 bit unit.

ToS: (Type of Service), It helps the device to determine the priority of this packet.

Total length: is the total length of the packet including the header and the data.

Identification: it is a unique number for every packet.

Fragment offset: it is used in the fragmentation and the reassembly of the data.

TTL: (Time To Live), it is a lifetime for the packet. Every network device reduces TTL by one, when TTL=0, the packet will be discarded by the network device.

Protocol: it specifies the upper layer protocol.

Header Checksum: it is used to check if any errors occurred in the header during its transmission.

5.6 'Router', a device working in the internetworking layer

The router is a device working in the internetworking layer (layer 3). The function of the internetworking layer is to route the data between the networks.

The router is a device that contains several ports. Every port is connected to a certain network.

There is a table that is stored in the router's memory, called the 'routing table', which contains the data about which network is connected to which port.

5.7 Broadcast domain

The broadcast domain is the group of network devices, in this group, if one of the devices sent an undirected broadcast packet; this broadcast packet will reach all of the other devices in this group.

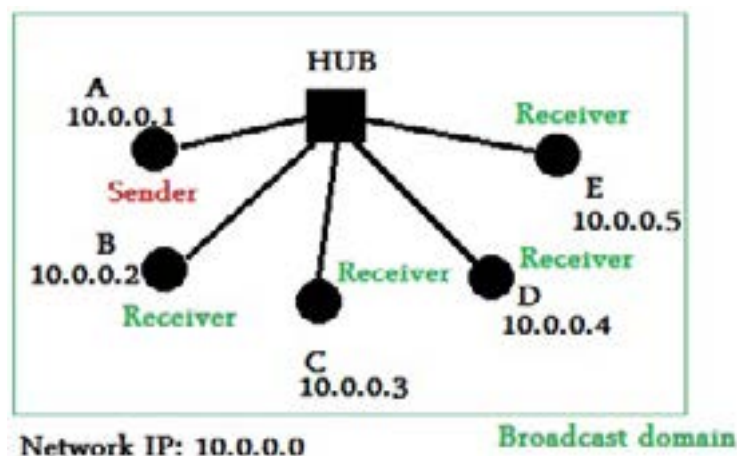


Figure 5.16: the broadcast domain

5.7.1 Broadcast domain vs. collision domain

'Layer 3' devices – like the router – divides the broadcast domain.

'Layer 2' devices – like the switch – divides the collision domain.

'Layer 1' device – like the hub – has no effect on any of both domains.

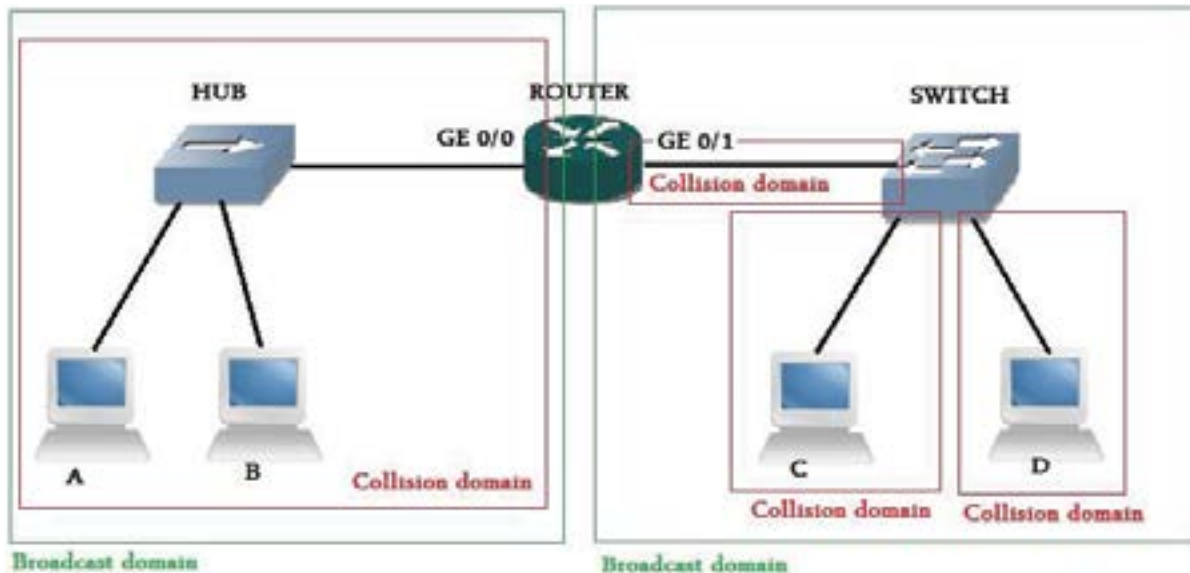


Figure 5.17: the broadcast domain vs. the collision domain

JUMP-START CAREERS

GIVE STUDENTS ONLINE ACCESS TO A VAST BODY OF KNOWLEDGE ABOUT SAP SOLUTIONS.

SAP Learning Hub, student edition

SAP Learning Hub

The background of the advertisement shows a young man with brown hair, wearing a red and white striped shirt, sitting on stone steps and looking down at a tablet computer he is holding. A yellow bag strap is visible over his shoulder. The SAP logo is in the bottom right corner.

Hour 6: Subnet Mask and Subnetting

When we understand the following rule, it will help us in the understanding of the subnetting.

Suppose that we have **1 place** that we need to replace it with a binary number. What numbers can be used? The answer is '0' or '1', which are 2 values or (**2¹ values**), from decimal '0' to decimal '1'.

x	0 or 1	2	0 : 1	2¹
---	--------	---	-------	----------------------

Suppose that we have **2 places** that we need to replace it with binary number. What numbers can be used? The answer is '00', '01', '10' or '11', which are 4 values or (**2² values**), from decimal '0' to decimal '3'.

xx	00 or 01 or 10 or 11	4	0 : 3	2²
----	----------------------	---	-------	----------------------

Now, if you have **3 places**... you will have 8 values (**2³ values**), from decimal '0' to decimal '7'.

xxx	000 or 001 or 010 or 011 or 100 or 101 or 110 or 111	8	0 : 7	2³
-----	---	---	-------	----------------------

Therefore, what if we have 4 or 5 or...8 places?

xxxx	0000 or 0001 or or 1111	16	0 : 15	2⁴
⋮				
xxxxxxxx	00000000 or 11111111	256	0 : 255	2⁸

From the previous, we can deduce that,

Number of available Binary values = **2^N** where N = Number of bits

6.1 Subnet mask

Always, you will find the subnet mask information associated with any IP address.

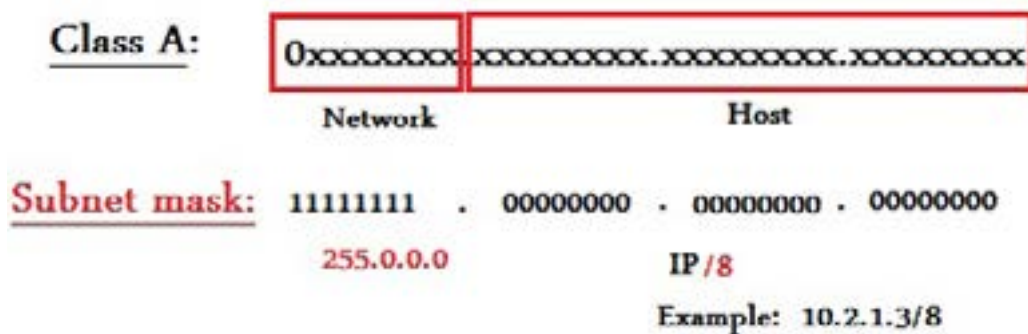
The subnet mask enables you to know the network portion and host portion of any IP address.

If no subnet mask information is associated with the IP, then the default is to determine the network portion and the host portion of this IP address depending on its IP class.

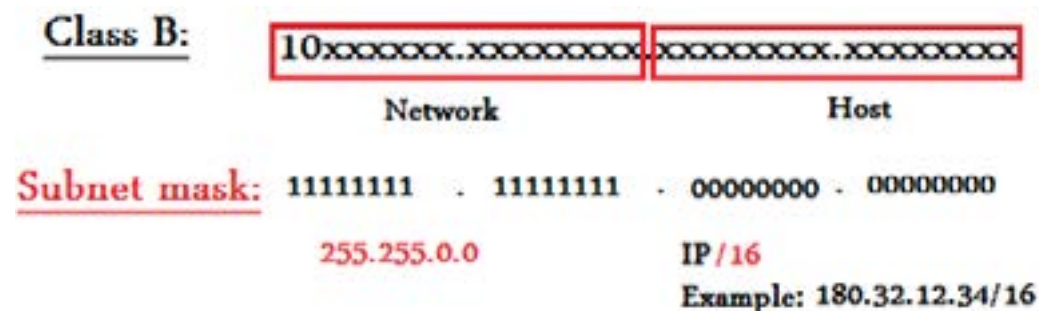
The subnet mask determines the network portion and the host portion of an IP address by converting the network portion to all ones and converting the host portion to all zeros.

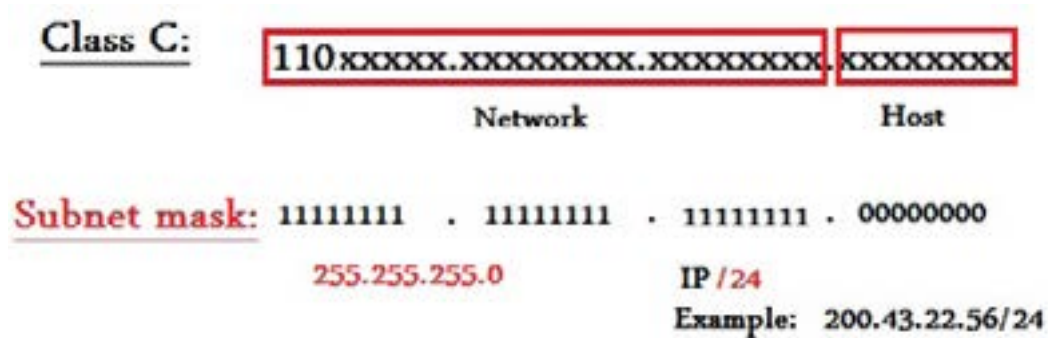
Therefore, for the 'class A' subnet mask, the first byte will be all ones and the last three bytes will be all zeros.

Class A IP subnet mask



Class B IP subnet mask



Class C IP subnet mask**6.1.1 Getting the network IP using the subnet mask**

To get the network IP from any IP address, we should convert the host portion to zeros.

The theoretical method to get the network IP, is to make a logical AND operation between the IP and its subnet mask.



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub



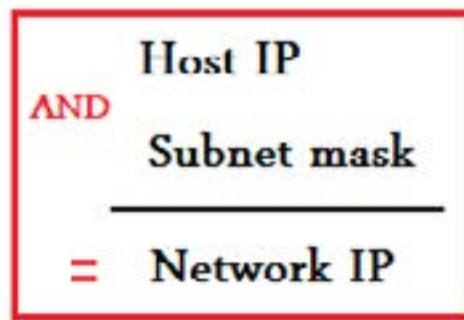


Figure 6.1: getting the network IP

The following illustrates the AND function,

A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

AND function

Figure 6.2: the logical AND function

6.2 Subnet mask examples

Example 1

Get the network IP and the broadcast IP from the following IP and subnet mask '193.129.2.131/25'. In addition, get the number of available host IPs, and determine the first and the last available host IP.

Solution:

1. convert IP to Binary format

11000001.10000001.00000010.10000011

2. get the subnet mask

11111111.11111111.11111111.10000000

Network
Host

3. Network IP = IP AND subnet mask (Convert all host portion to 0s)

11000001.10000001.00000010.10000000 = 193.129.2.128

4. Broadcast IP: (convert all host portion to ones),

11000001.10000001.00000010.11111111 = 193.129.2.255

5. First available IP= Network IP + 1 = 193.129.2.129

6. Last available IP= Broadcast IP - 1 = 193.129.2.254

To get the number of available host IPs, we use the following rule,

Number of host IP
addresses available =

$$2^{\text{Number of host bits}} - 2$$

Therefore, the number of available host IPs =

$$2^7 - 2 = 126$$

Example 2

Get the network IP and the broadcast IP from the following IP and subnet mask '130.5.192.68/26'. In addition, get the number of available host IPs, and determine the first and the last available host IP.

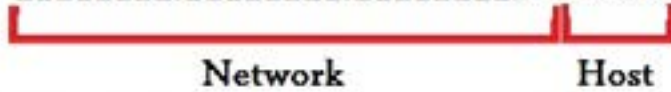
Solution:

1. convert IP to Binary format

10000010.00000101.11000000.01000100

2. get the subnet mask

11111111.11111111.11111111.11000000



3. Network IP = IP AND subnet mask (Convert all host portion to 0s)

10000010.00000101.11000000.01000000 = 130.5.192.64

4. Broadcast IP: (convert all host portion to ones),

10000010.00000101.11000000.01111111 = 130.5.192.127

5. First available IP = Network IP + 1 = 130.5.192.65

6. Last available IP = Broadcast IP - 1 = 130.5.192.126

HANDS-ON PRACTICE FOR EFFECTIVE LEARNING

EXPERIENCE SAP SOFTWARE FIRSTHAND TO BUILD KNOWLEDGE AND ENHANCE SKILLS.

SAP Live Access

SAP Learning Hub



The number of available host IPs=

$$2^6 - 2 = 62$$

6.3 Subnetting

Suppose that we have one network IP and we have three networks. How we can use this only one network IP to be able to assign one network IP to every network of our networks?

The solution is to make 'subnetting'.

6.3.1 What is subnetting?

Subnetting is to get many 'network IPs' from only one network IP, by changing in the network portion and the host portion in the original network IP.

6.3.2 Subnetting example 1

You have one 'class C' IP address (194.5.24.0), and you have two networks, every one of them has 100 computers. You should subnet this IP to fulfill your needs.

Solution:

Convert the given IP to binary formatting and determine the network portion and the host portion.

Determine how many bits you need to add to the network portion in order to have the correct number of network IPs.

$$2 \text{ Networks} = 2^1 \text{ Networks} \quad \text{I need 1 bit}$$

$$11000010.00000101.00001100.00000000$$

Network
Host

Now, you can get the new subnet mask

$$\text{Subnet mask} = 11111111.11111111.11111111.10000000 = 255.255.255.128 \text{ or } /25$$

Make sure you can cover the number of host IPs in every network.

$$\text{Available hosts} = 2^7 - 2 = 126$$

Now, you can get the subnetted network IPs.

First Network:

11000010.00000101.00001100.00000000 = 194.5.24.0/25

Broadcast IP: 11000010.00000101.00001100.01111111 = 194.5.24.127/25

Second Network:

11000010.00000101.00001100.10000000 = 194.5.24.128/25

Broadcast IP: 11000010.00000101.00001100.11111111 = 194.5.24.255/25

6.3.3 Subnetting example 2

You have one 'class B' IP address (134.18.0.0), and you have three networks, every one of them has 100 computers. You should subnet this IP to fulfill your needs.

Solution:

Convert the given IP to binary formatting and determine the network portion and the host portion.

10000110.00010010.00000000.00000000

Network Host

Determine how many bits you need to add to the network portion in order to have the correct number of network IPs.

4 Networks = 2^2 Networks
I need 2 bits

10000110.00010010.00000000.00000000

Network Host

Now, you can get the new subnet mask.

Subnet mask =
 $11111111.11111111.11000000.00000000 = 255.255.192.0 \text{ or } /18$

Make sure you can cover the number of host IPs in every network.

Available hosts in each network
 $= 2^{14} - 2 = 65,534$

Now, you can get the subnetted network IPs.

<u>First Network:</u>	10000110.00010010. 00 000000.00000000	= 134.18.0.0/18
<u>Second Network:</u>	10000110.00010010. 01 000000.00000000	= 134.18.64.0/18
<u>Third Network:</u>	10000110.00010010. 10 000000.00000000	= 134.18.128.0/18
<u>Fourth Network:</u>	10000110.00010010. 11 000000.00000000	= 134.18.192.0/18



ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

Hour 7: Network Infrastructure

7.1 NIC settings

Every network device has a Network Interface Card (NIC) installed in it.

To see the settings that exists on this network interface card, we can open your command prompt and write the following command,

```
Ipconfig /all
```

This will show us all the NIC settings as seen in figure (7.1),

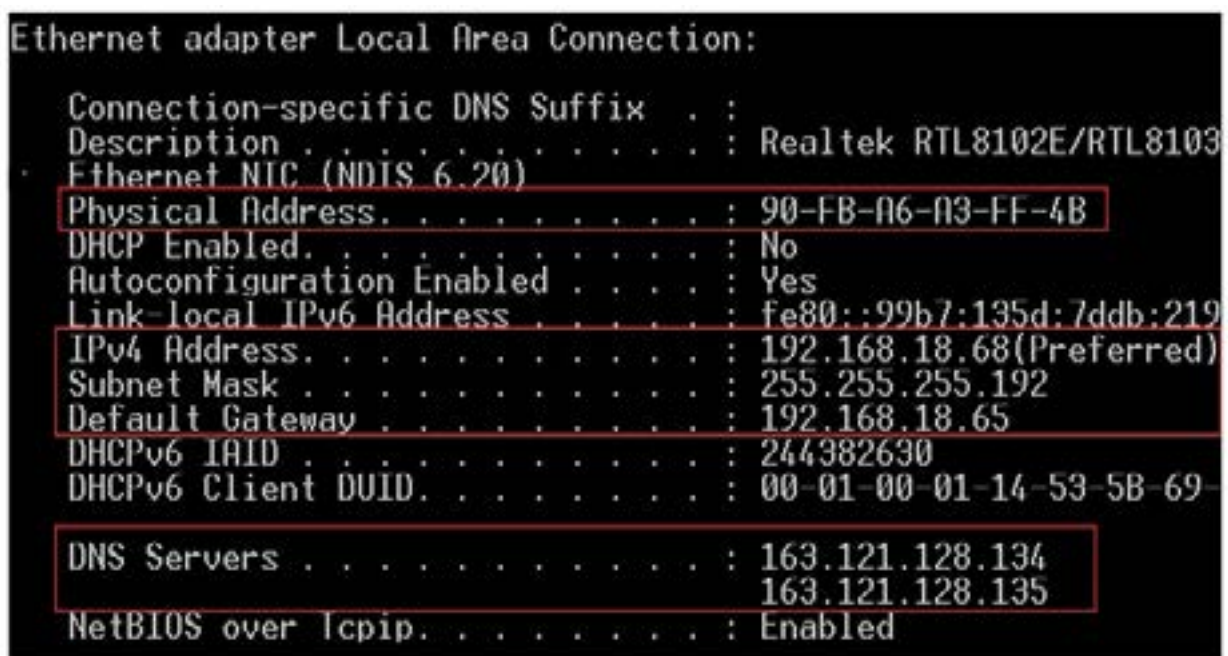


Figure 7.1: the NIC settings

We already know the 'physical address', the 'IPv4 address' and the 'subnet mask'.

Nevertheless, what is the 'default gateway', the 'DNS servers' and the 'DHCP'? That is what we should know in this hour.

7.2 Default gateway

The default gateway is the gateway that interconnects all the network devices in the network with the external world.

In figure (7.2), the default gateway is the router's interface GE0/0.

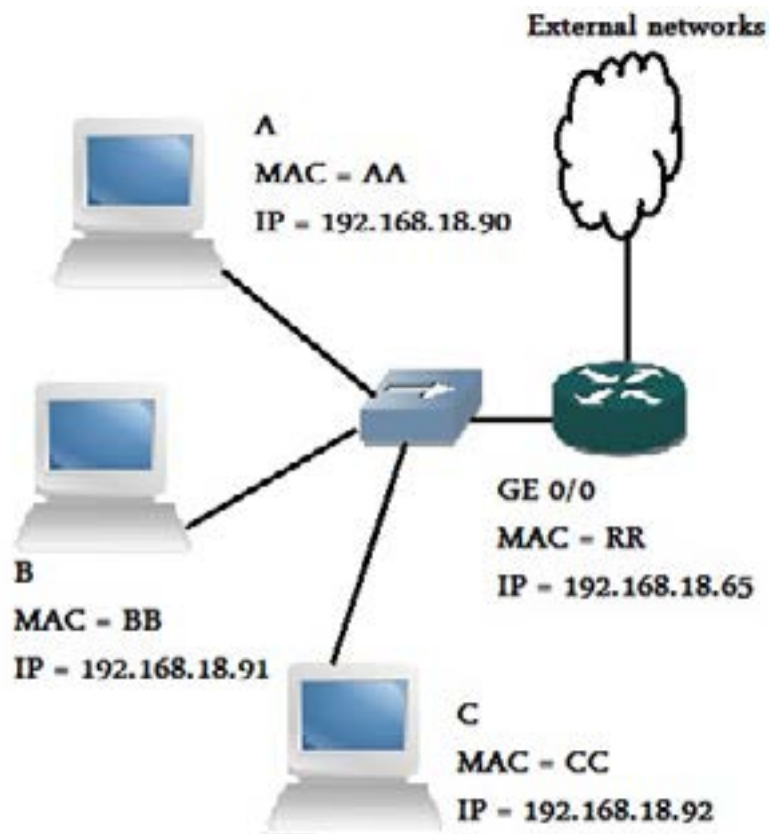


Figure 7.2: the default gateway

In figure (7.2), if 'computer A' needs to send a packet to a computer that exists inside its network, – e.g. 'computer C' –, it will send the packet directly to it as seen in figure (7.3),

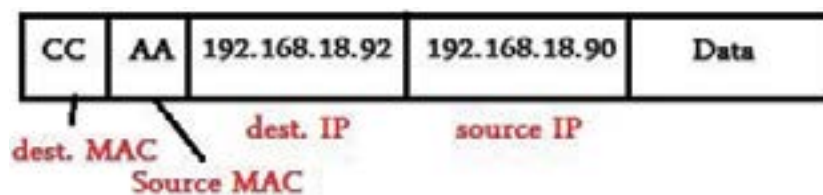


Figure 7.3: sending a packet inside the network

If 'computer A' needs to send a packet to a computer that exists outside its network – e.g. computer 10.0.0.1 that exists outside the network –, it will send the packet to the default gateway as seen in figure (7.4),

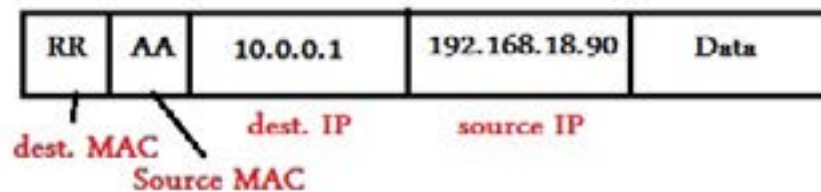


Figure 7.4: sending a packet outside the network

You can observe that the destination IP is the IP address of the computer that exists outside the network while the destination MAC address is the MAC address of the default gateway. This is because that 'layer 2', where the MAC address operates, is responsible for the communication between any two nodes inside the same network.

7.3 DNS server

The DNS (Domain Name System) server is responsible of resolving the names to IP addresses.

This is because computers are able to deal with the IP addresses not the names.

NO-LIMITS LEARNING

**LEVERAGE SOCIAL LEARNING,
COLLABORATION, QUALITY
CONTENT, AND HANDS-ON
PRACTICE.**

SAP Learning Hub

SAP

The advertisement features a woman and a man in a modern office setting, looking at a tablet together. The background is a bright, glass-walled office.

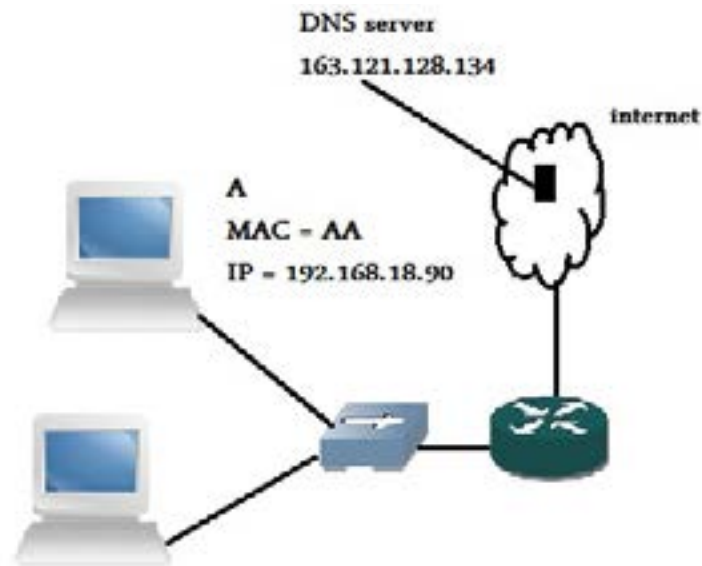


Figure 7.5: the DNS server

Suppose that you are setting on 'computer A' and need to browse Google's website, the following will happen,

1. You open up the web browser and write 'www.google.com' in the address bar
2. 'Computer A' asks the DNS server about the IP of 'www.google.com' (remember that the DNS server IP is already configured on your NIC)
3. the DNS server tells 'computer A' that the IP of 'www.google.com' is '209.85.149.103'
4. 'Computer A' starts the communication with '209.85.149.103'

7.4 DHCP sever

The DHCP (Dynamic Host Configuration Protocol) server is used to automatically configure NIC settings.

The NIC settings contains the following,

1. IP address
2. Subnet mask
3. Default gateway IP
4. DNS server IP

There are two ways to configure the NIC settings,

1. Manually

The network administrator configures every NIC manually. This method has high administrative effort, which is a disadvantage. So, this method is used only when the number of network devices is small.

2. Automatically (using the DHCP server)

The DHCP server will automatically provide every NIC with the required configuration. This method has a little administrative effort, which is an advantage.

7.4.1 The DHCP configuration

There are some values that should be configured on the DHCP server, the network administrator configure those values on the DHCP server. The following are the values that should be configured on the DHCP server,

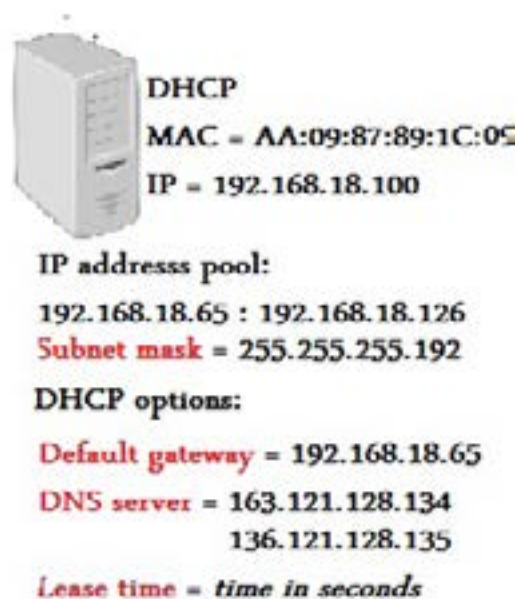


Figure 7.6: the DHCP server

1. IP address pool

The IP address range that the DHCP server uses to assign the IP addresses to the network devices.

2. Subnet mask

The subnet mask that should be assigned to the network devices.

3. DHCP options

It includes the following, the 'default gateway IP', the 'DNS server IPs' and the 'lease time'.

The 'lease time' is the lifetime of the IP address that is assigned to a network device. The network device should renew its IP address from the DHCP server before this time expires.

7.4.2 NIC settings assignment process

Suppose that 'computer A' in figure (7.7) is starting up and needs to take the NIC configurations from the DHCP server. The following will happen,

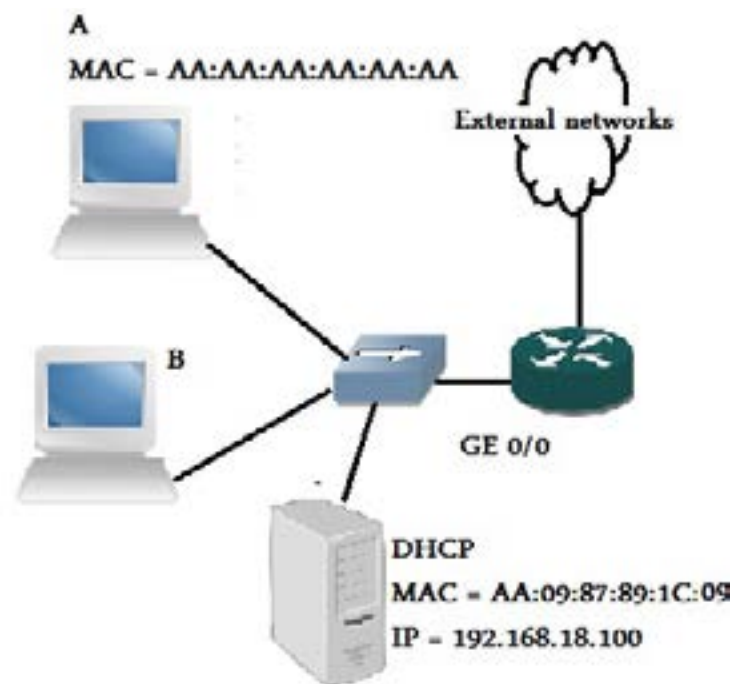


Figure 7.7: getting the NIC settings

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub



1. 'Computer A' sends a broadcast 'DHCPDISCOVER' message as following,

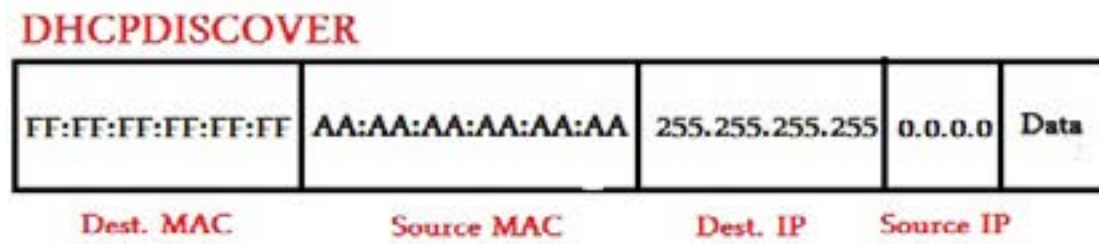


Figure 7.8: 'DHCPDISCOVER' packet

Source MAC: the MAC address of 'computer A'.

Destination MAC: the 'layer 2' broadcast (all Ones).

Source IP: all zeros (This means that this computer is asking for its IP address).

Destination IP: 'layer 3' broadcast (all Ones).

2. The DHCP sends a unicast 'DHCPOFFER' message to 'computer A' offering it an IP address.
3. 'Computer A' sends a broadcast 'DHCPREQUEST' message requesting the offered IP address.
4. The DHCP sends a unicast 'DHCPACK' message to 'computer A' acknowledging it that the offered IP is assigned to you.

Note: The network administrator may configure the router to work as a DHCP server.

7.4.3 APIPA

APIPA (Automatic Private IP Addressing) is a range of IP addresses (169.254.0.0: 169.254.255.255).

Suppose that a computer is configured to take its NIC settings from a DHCP server.

At startup, the computer will try to communicate with the DHCP by sending a broadcast 'DHCPDISCOVER' message.

If the computer is unable to communicate with the DHCP to have its NIC settings from it, it will give itself an APIPA IP address which is an IP address in the range (169.254.0.0: 169.254.255.255).

7.5 ARP

ARP is the 'Address Resolution Protocol'.

Every computer contains a table called the 'ARP table' stored in its memory. This table contains the IP and the MAC addresses of the other devices.

ARP table

IP	MAC
192.168.18.91	BB
192.168.18.65	RR

Figure 7.9: the ARP table

If a source computer needs to send some data to a destination computer, the source computer must know the IP address and the MAC address of the destination computer.

If the source computer knows only the IP address of the destination computer, it will use the 'ARP protocol' to know the MAC address of the destination computer and store those IP and the MAC addresses in its ARP table.



MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub

SAP

7.5.1 Case study

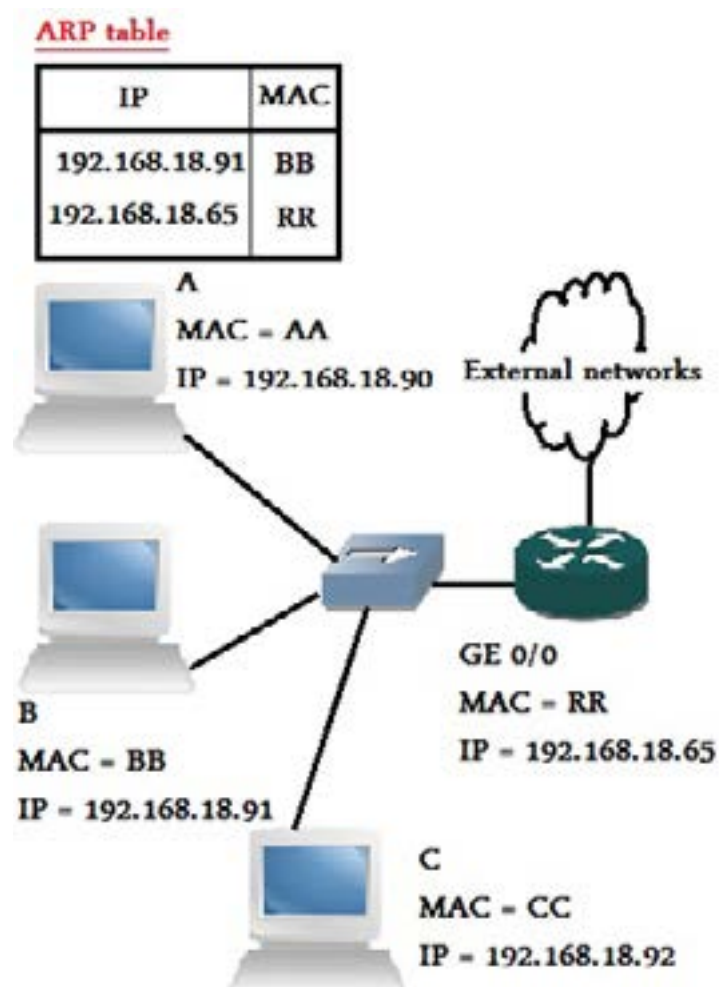
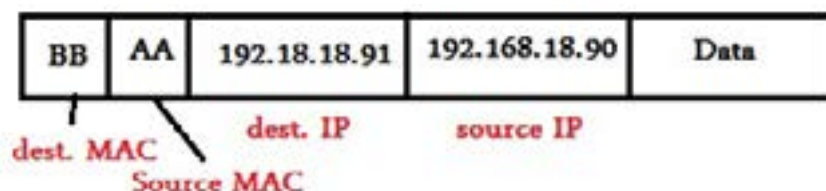


Figure 7.10: the ARP protocol

In figure (7.10), suppose the following,

Computer A needs to send some data to 192.168.18.91 (computer B)

In this case, 'computer A' will find the MAC address of 192.168.18.91 in the ARP table. Therefore, 'computer A' will simply send the data to 'computer B' as following,



Computer A needs to send some data to 192.168.18.92 (computer C)

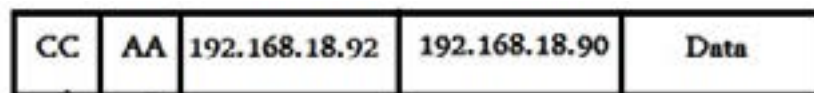
1. In this case, 'computer A' will not find the MAC address of 192.168.18.92 in its ARP table.
Therefore, it will use the ARP protocol to get the MAC address of 192.168.18.92 as following,



2. Then, 192.168.18.92 will reply to 'computer A' telling it its MAC address as following,



3. Then, 'computer A' will simply send the data to 192.168.18.92 as following,



7.5.2 Proxy ARP

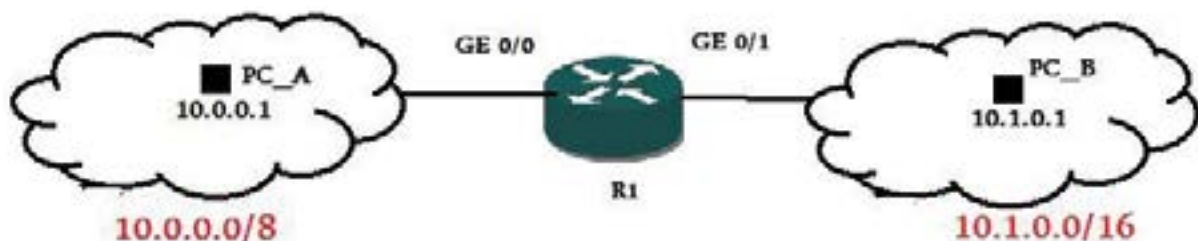


Figure 7.11: the proxy ARP

The proxy ARP is used when the computer needs to know the MAC address of a computer in a different network.

As seen in figure (7.11), if PC_A needs to know the MAC address of PC_B, it will use the proxy ARP.

7.5.3 RARP (Reverse ARP)

It is used if the computer knows the MAC address of the destination computer, and it needs to know its IP address.

Currently, the DHCP replaced the RARP. Therefore, nobody uses RARP now.

7.6 ICMP

ICMP (Internet Control Message Protocol) provides the network devices with the information about different network problems.

Examples of ICMP messages:

- **Echo request and echo reply:**
It is used to examine the network connectivity.
- **The destination unreachable:**
The router uses ICMP to send a message to the sender in case that the destination is unreachable.

7.6.1 Case study

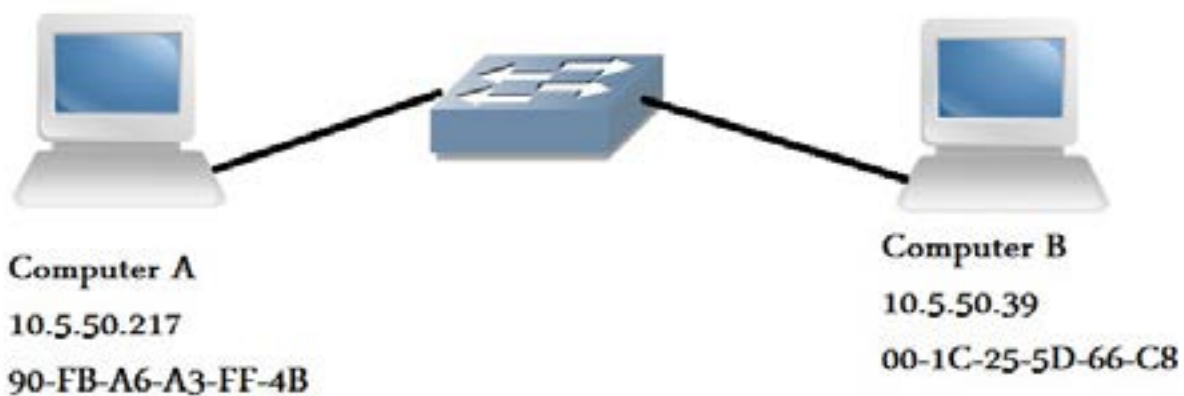


Figure 7.12: ICMP protocol case study

In figure (7.12), you are sitting on 'computer A' and need to test the connectivity to 'computer B'.

First, 'computer A' will use **ARP** protocol to know the MAC address of 'computer B'.

Then, 'computer A' will use **ICMP** protocol to send an **echo request** to 'computer B'.

Then, 'computer B' will use **ICMP** protocol to send an **echo reply** to 'computer A'.

If the echo request and the echo reply are successful, you will know that there are no problems in the connectivity between the source and the destination.

Hour 8: Transport and Application Layers

8.1 Transport layer protocols (TCP and UDP)

As you remember, the transport layer function is to determine the destination application using the port number, and to make error detection and correction, and data segmentation and reassembling.

There are two main protocols that are used in the transport layer, they are the 'TCP' and the 'UDP'.

The difference between the two protocols is summarized in table (8.1).



FAST ADOPTION, FAST ROI

**EQUIP BUSINESS
USERS TO ADOPT
SAP SOLUTIONS.**

SAP Learning Hub, user edition

SAP Learning Hub

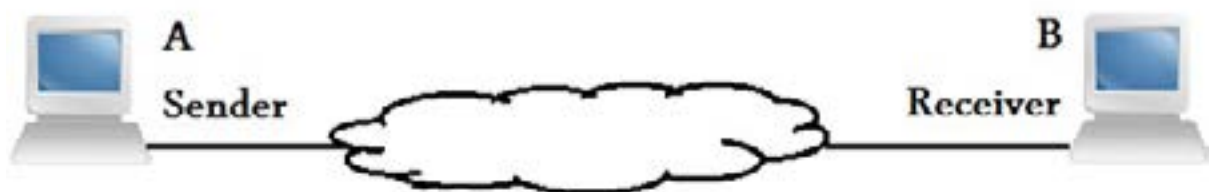
SAP

TCP	UDP
Reliable protocole	Unreliable protocole
Connection oriented	NO Connection oriented
Aknowledgment	NO Aknowledgment
Sequencing	NO Sequencing
Flow control	NO Flow control
High overhead	Low overhead

Table 8.1: the difference between the TCP and the UDP

To understand the terminologies stated in table (8.1) let us study the following,

Suppose that we have two computers, a source, and a destination.



Connection oriented, the source establishes a session with the destination before sending any data.

Acknowledgement, the source waits for the destination acknowledgement about receiving the sent segments before sending the new segments.

Sequencing, the source gives a sequence number for every segment it sends, in order to be correctly reassembled at the destination.

Flow control, the destination can control the flow of the data that comes from the source.

Because the **TCP** can use the above-mentioned characteristics, it is a **reliable protocol**.

Because the **UDP** can't use the above mentioned characteristics, it is an **unreliable protocol**

TCP has high overhead, this means that its header size is big. Therefore, it consumes a lot from the network BW.

UDP has low overhead: this means that its header size is small. Therefore, it does not consume a lot from network BW.

As seen in the figures (8.1) and (8.2), we can see that the header of the TCP is larger than the header of the UDP.

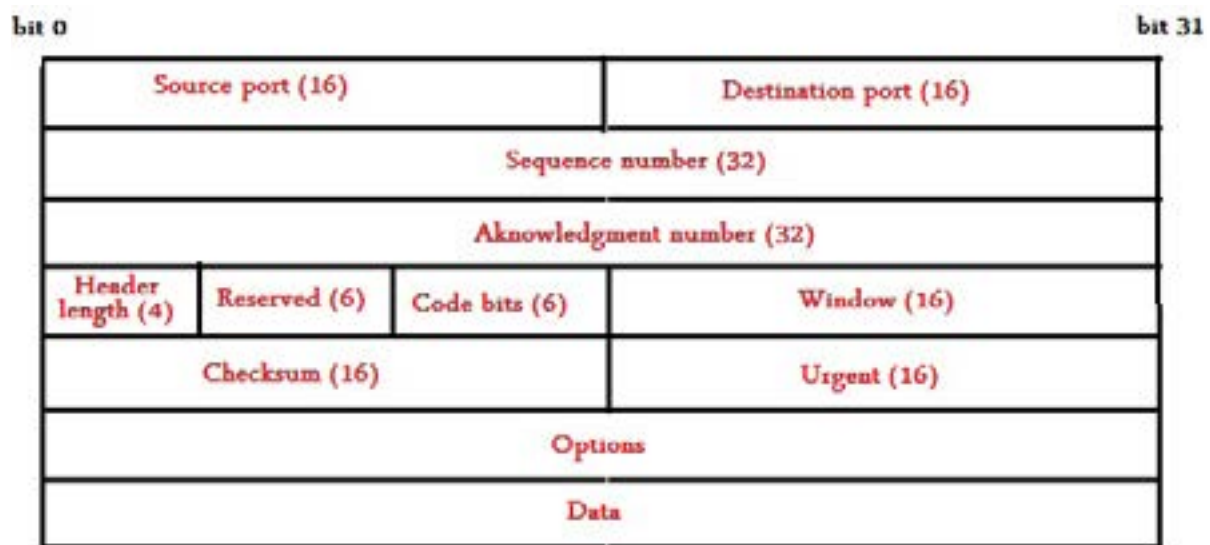


Figure 8.1: the TCP header

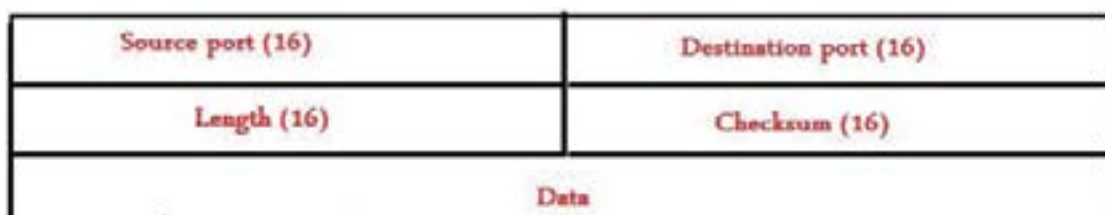


Figure 8.2: the UDP header

8.2 Application layer protocols

As you remember, the function of the application layer is that, it is an interface between the TCP/IP protocol stack and the programs and services.

Every protocol of the application layer protocols uses either TCP or UDP, and it uses a certain port number.

The following are examples of the protocols that are used in the application layer,

Telnet:

The telnet uses the TCP port 23. It is used to remotely access and control the network resources. It allows telnet client to access the resources of the telnet server.

SSH:

SSH uses TCP port 22. It is the secured version of the telnet.

FTP (File Transfer Protocol):

FTP uses TCP port 21. It is used to transfer files. (E.g. downloading any file from a web server)

TFTP (Trivial FTP):

TFTP uses UDP port 69. It is a stripped down version of the FTP. It is faster than the FTP, but it is not as reliable as FTP, this is because that it uses UDP.

SMTP (Simple Mail Transfer Protocol):

The SMTP uses TCP port 25. It is used to send e-mails.

DNS (Domain Name System):

DNS uses TCP port 53, and UDP port 53. It resolves hostnames into IPs.

HTTP (Hypertext Transfer Protocol):

HTTP uses TCP port 80. It is used to browse the internet.

HTTPS (HTTP Secure):

HTTPS uses TCP port 443. It is the secured version of the HTTP.

Part 2

NETWORK CONFIGURATION

Hour 9: Cisco IOS, The Router Device

9.1 LAN and WAN interfaces

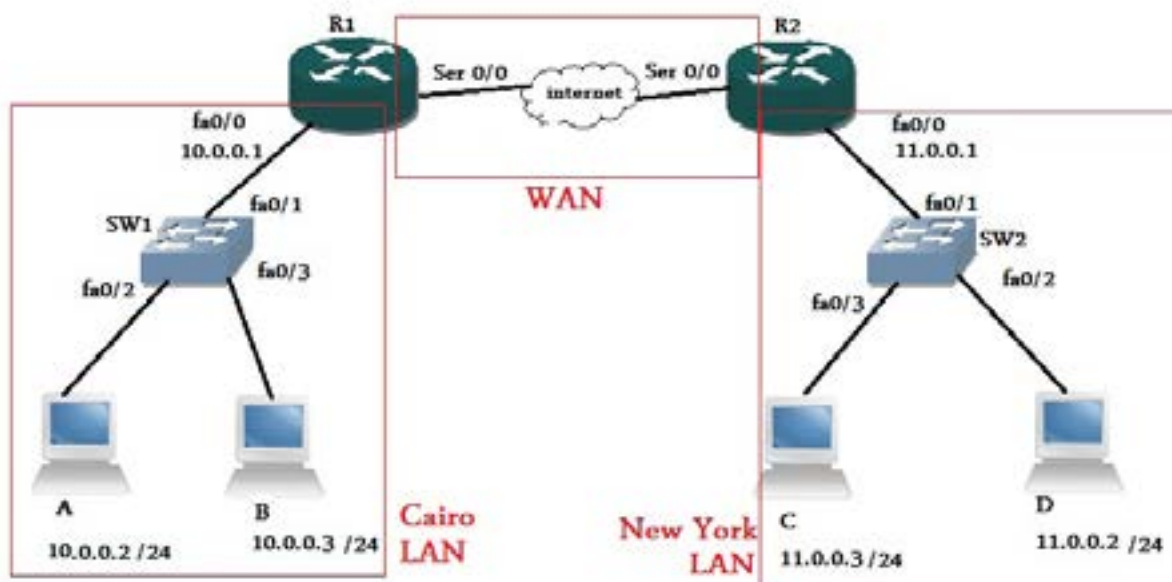


Figure 9.1 LAN vs. WAN

Suppose that a company has two branches, one of them is in Cairo, and the other one is in New York.

The network that exists in Cairo branch is called a 'LAN' (Local Area Network).

The network that exists in New York branch is called a 'LAN' (Local Area Network).

The network that connects between the two branches through the internet is called a 'WAN' (Wide Area Network).

Therefore, we can deduce the following,

The LAN (local area network) is the network that exists in a limited boundary of a geographical area.

The WAN (wide area network) is the network that exists in a wide geographical area.

As you can see in the figure (9.1),

The LAN is always connected to the router through its 'ethernet port'. Therefore, the ethernet port is the LAN interface.

The WAN is always connected to the router through its 'serial port'. Therefore, the serial port is the WAN interface.

9.2 The router's hardware

Every router contains hardware and software. In addition, there are many router models, every model has its certain capabilities and features and external body shape.

Every router's model contains a certain number of ethernet ports and serial ports. However, some router models allow you to increase the number of ports by plugging some modules in them.

In figure (9.2), you can see a router that contains only two ethernet ports.



Figure 9.2: a router.

We can increase the number of the ethernet ports by plugging a module that contains extra number of ethernet ports in the router.

In figure (9.3), you can see the router's module that contains the extra ethernet ports.



Figure 9.3: a router's module.

In figure (9.4), you can see the place that accepts the external router's module.



Figure 9.4: a router that accepts an external module.

9.2.1 Configuring a router



Figure 9.5: some ports of the router.

In figure (9.5), you can see a router that contains a serial port, an ethernet port, a consol port, and an auxiliary port.

To configure a router, we have three methods to connect to it,

Using a consol port

Simply connect the computer to the consol port using a rolled cable.

An advertisement for SAP Learning Hub. It features a young man with brown hair, wearing a pink and orange striped shirt, sitting on stone steps and looking down at a tablet computer. The background is a blurred outdoor setting. Overlaid on the image is the text 'JUMP-START CAREERS' in large, bold, yellow capital letters. Below it, in large, bold, black capital letters, is 'GIVE STUDENTS ONLINE ACCESS TO A VAST BODY OF KNOWLEDGE ABOUT SAP SOLUTIONS.' Underneath that, in smaller black text, is 'SAP Learning Hub, student edition'. At the bottom left is the 'SAP Learning Hub' logo, and at the bottom right is the 'SAP' logo in a blue square.

Using an auxiliary port

The auxiliary port enables us to connect to the router while we are away from the company, this is done by connecting the auxiliary port to a modem, and if we need to connect to the router from outside the company, we dial up this modem, which connects us to the router.

Using the telnet

Using any telnet application in our computer enables us to telnet the router and configure it. (Of course, you must be the network admin to have the telnet username and password).

9.3 Booting up a router

9.3.1 Memory types on the router

Flash memory

It contains Cisco IOS (the operating system that operates the router).

NVRAM (non-volatile RAM)

It holds the 'startup configuration' and the 'configuration register value'.

Startup configuration is the configuration configured on the router and then stored to the NVRAM.

Configuration register value is a value that determines the booting sequence of the router.

ROM

It contains the 'POST' and the 'Bootstrap'.

POST (power on self-test) is a program that checks the router's hardware when starting up.

Bootstrap is a program that loads the IOS when the router starts up.

RAM

It holds the 'running configuration'.

The difference between the RAM and the other memory types is that when the power gets off, all the data that exists on the RAM will be deleted.

Running configuration is the actual configuration that the router uses.

9.3.2 The startup configuration vs. the running configuration

The startup configuration is the configuration that configured on the router and then stored to the NVRAM. So that the configuration will never be deleted when the router shuts down.

The actual configuration that the router uses while it is working, is the running configuration that exists on the RAM.

When the router starts up, it loads the startup configuration from the NVRAM to the RAM; this is done in order to make it the running configuration that the router should work from.

9.3.3 The router booting up sequence

1. POST checks the router's hardware.
2. Bootstrap loads Cisco IOS from the flash memory.
3. Cisco IOS looks for the startup configuration in the NVRAM.
4. The startup configuration is copied to the RAM, which converts this configuration to be the running configuration that the router should use in its operation.



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub



Hour 10: Cisco IOS, The CLI Commands

10.1 CLI (Command Line Interface) modes

The CLI (Command Line Interface) is the software interface that the network admin uses in order to configure the router.

Every CLI mode contains some commands that enable us to configure a certain set of functions on the router.

We can move through different modes using some commands as will be explained in this hour.

10.1.1 Setup mode (initial configuration mode)

This mod contains interactive configuration dialogue that enables us to configure the router.

When the router starts up, it will take the startup configuration from the NVRAM and copy it to the RAM in order to use it.

If the router did not find any startup configuration, it will enter to the 'setup mode', and it will ask us if we need to use the initial configuration dialogue in order to configure the router.

It is optional to us to use this dialogue or not.



Figure 10.1: the initial configuration dialogue.

If we refused to use this dialogue, the router will enter to the 'user EXEC mode'.

10.1.2 The 'user EXEC mode'

In this mode, every line in the CLI starts with the following,

Router>

If a user name and a password are configured on the router, the router will ask us to write them to be able to access the next mode, which is the 'privileged mode'.

To enter to the 'privileged mode', we write the command,

Router> enable

As seen in figure (10.2).

A terminal window with a black background and green text. The text shows the command sequence: 'Router>' followed by 'enable' on the next line, and then 'Router#' on the third line. A green cursor is positioned after the 'Router#' prompt.

Figure 10.2: the user EXEC mode.

10.1.3 The privileged mode

In this mode, every line in the CLI starts with the following,

Router#

This mode contains the basic operation monitoring commands, and it is used to test the network connectivity, and to make a backup and restoration of the router's configuration and the Cisco IOS.

To enter to the next mode, the 'global configuration mode', we write the command,

Router# configure terminal

As seen in figure (10.3).

A terminal window with a black background and green text. The text shows the command sequence: 'Router#configure terminal' followed by 'Enter configuration commands, one per line. End with CNTL/Z.' on the next line, and then 'Router(config)#' on the third line. A green cursor is positioned after the 'Router(config)#' prompt.

Figure 10.3: the privileged mode.

10.1.4 The global configuration mode

In this mode, every line in the CLI starts with the following,

Router(config)#

This mode contains most of the basic configuration commands.

To enter to one of the next modes like the 'interface mode', we write the command,

```
Router(config)# interface interface
```

As seen in figure (10.4).

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa 0/0
Router(config-if)#
```

Figure 10.4: the global configuration mode.

10.1.5 Specific configuration modes

They are the modes that contain commands that affect the interfaces or the processes on the router, like the 'interface mode' and the 'router configuration mode'.

10.2 Privileged mode commands, 'show' command

10.2.1 The 'show' command

The 'show' command enables us to view the router's configuration and operation. Example of the 'show' commands,



**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

The 'show version' command

Router# show version

```
Image text-base: 0x80008098, data-base: 0x80CEA424
ROM: ROMMON Emulation Microcode
ROM: C2600 Software (C2600-I-M), Version 12.3(22), RELEASE SOFTWARE (fc2)

R1 uptime is 1 hour, 44 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0
x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

cisco 2621 (MPC860) processor (revision 0x202) with 56320K/9216K bytes of memory
.
Processor board ID 000000000000 (1880125456)
M860 processor: part number 0, mask 0
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Figure 10.5: the 'show version' command.

The 'show version' command enables us to view the version of the Cisco IOS that exists on the router, the RAM size, and the interfaces that exist on the router, the NVRAM size, the flash memory size, and the configuration register value.

The 'show ip interface brief' command

Router# show ip interface brief

This command enables us to view every router interface status

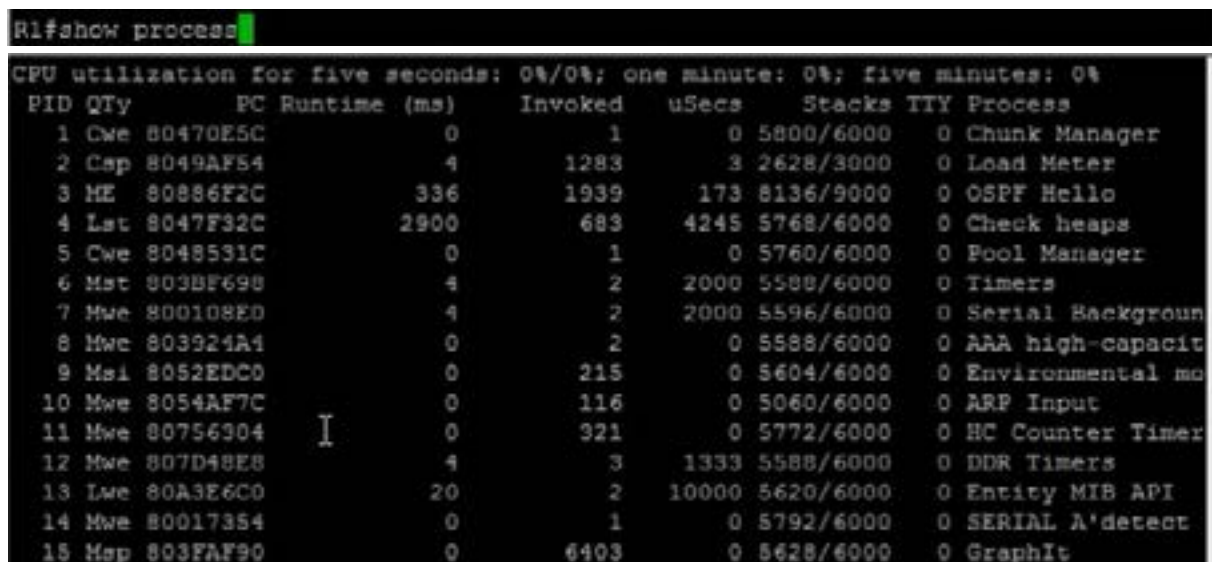
```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
ocol
FastEthernet0/0          10.0.0.1        YES NVRAM   up          up
Serial0/0                 50.0.0.1        YES NVRAM   up          up
FastEthernet0/1          unassigned      YES NVRAM   administratively down down
Serial0/1                 unassigned      YES NVRAM   administratively down down
```

Figure 10.6: the 'show ip interface brief' command.

The 'show process' command

Router# show process

It enables us to view every process on the router and the process CPU utilization.



```

R1#show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTY      PC Runtime (ms)  Invoked  uSecs   Stacks  TTY Process
  1 Cwe 80470E5C      0         1      0 5800/6000 0 Chunk Manager
  2 Cap 8049AF54      4       1283      3 2628/3000 0 Load Meter
  3 ME 80886F2C     336       1939     173 8136/9000 0 OSPF Hello
  4 Lst 8047F32C    2900        683    4245 5768/6000 0 Check heaps
  5 Cwe 8048531C      0         1      0 5760/6000 0 Pool Manager
  6 Mst 803BF698      4         2     2000 5588/6000 0 Timers
  7 Mwe 800108E0      4         2     2000 5596/6000 0 Serial Backgroun
  8 Mwe 803924A4      0         2      0 5588/6000 0 AAA high-capacit
  9 Msi 8052EDC0      0        215      0 5604/6000 0 Environmental mo
 10 Mwe 8054AF7C      0        116      0 5060/6000 0 ARP Input
 11 Mwe 80756304      0        321      0 5772/6000 0 HC Counter Timer
 12 Mwe 807D48E8      4         3     1333 5588/6000 0 DDR Timers
 13 Lwe 80A3E6C0     20         2    10000 5620/6000 0 Entity MIB API
 14 Mwe 80017354      0         1      0 5792/6000 0 SERIAL A'detect
 15 Map 803FAF90      0       6403      0 5628/6000 0 GraphIt
  
```

Figure 10.6: the 'show process' command.

The 'show running-config' command

Router# show running-config

This command shows us the entire running configuration that exists on the RAM.

The 'show startup-config' command

Router# show startup-config

This command shows me the entire startup configuration that exists on the NVRAM.

10.2.2 The 'debug' command

The 'debug' command enables us to view all the packets that exit from and enter to the router.

The 'debug ip icmp' command

Router# debug ip icmp

This command enables us to view all the packets that are belonging to the 'ICMP protocol'.


```

R1#debug ip icmp
ICMP packet debugging is on
R1#ping 11.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/52/72 ms
R1#
*Mar 1 02:06:33.251: ICMP: echo reply rcvd, src 11.0.0.2, dst 50.0.0.1
*Mar 1 02:06:33.303: ICMP: echo reply rcvd, src 11.0.0.2, dst 50.0.0.1
*Mar 1 02:06:33.339: ICMP: echo reply rcvd, src 11.0.0.2, dst 50.0.0.1
*Mar 1 02:06:33.383: ICMP: echo reply rcvd, src 11.0.0.2, dst 50.0.0.1
*Mar 1 02:06:33.459: ICMP: echo reply rcvd, src 11.0.0.2, dst 50.0.0.1

```

Figure 10.7: the 'debug ip icmp' command.

10.3 Privileged mode commands, network connectivity

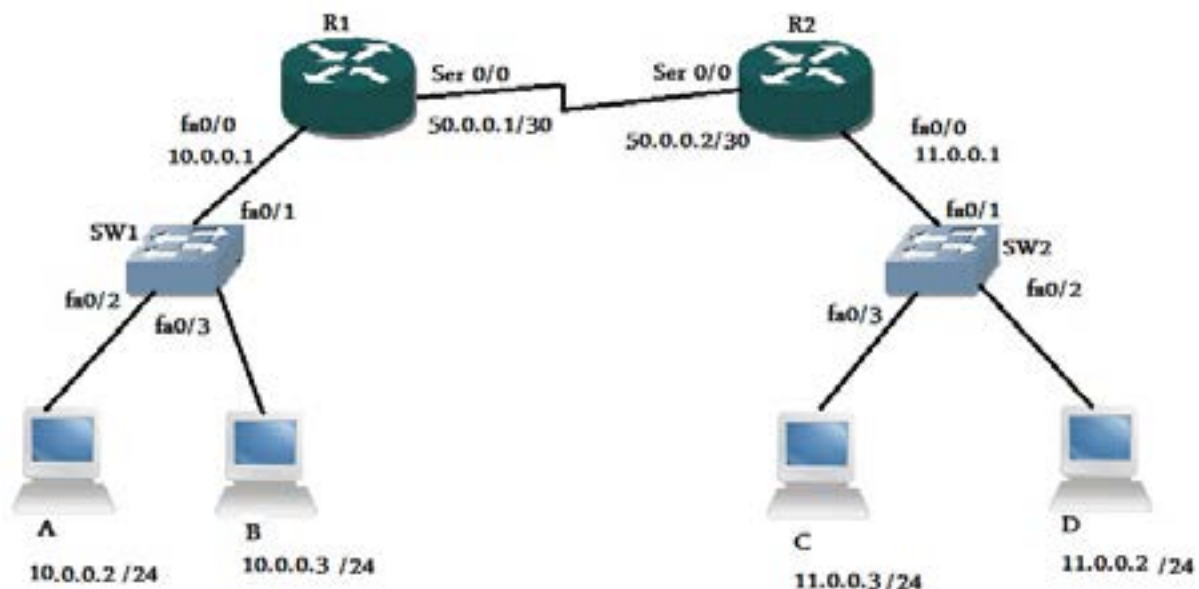


Figure 10.8: the network connectivity.

10.3.1 The 'ping' command

Router# ping ip_address

The 'ping' command is used to examine the network connectivity problems in a certain network.

In figure (10.8), suppose that we are on 'computer A' and needs to make sure that 'computer A' is able to reach 'computer D'.

From 'computer A', we make a 'ping' to 'computer D' (11.0.0.2) as following,

```
PC_A#ping 11.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/65/80 ms
PC_A#
```

Figure 10.9: the 'ping' command.

As seen in figure (10.8), 'computer A' sent five echo requests to 'computer D', and received five echo replies from 'computer D'. Which mean that 'computer A' is able to reach computer D.

10.3.2 The 'traceroute' command

Router# traceroute ip address

The 'traceroute' command is used to know the nodes that exist in the path between the source and the destination, and if there is a network connectivity problem, it helps us in determining in which node in the path this problem exists.



ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

In figure (10.8), suppose that we need to know the nodes that exist in the path between 'router A' and 'computer D'.

From 'router A' we make a 'traceroute' to 'computer D' (11.0.0.2) as following,

```
PC_A#traceroute 11.0.0.2

Type escape sequence to abort.
Tracing the route to 11.0.0.2

 0 10.0.0.1 32 msec 28 msec 20 msec
 1 50.0.0.2 48 msec 36 msec 16 msec
 2 11.0.0.2 36 msec 36 msec *
```

Figure 10.10: the 'traceroute' command.

As you can see in figure (10.10), that data exits from 'router A' and passes through (10.0.0.1) which is the 'R1'. Then, it passes through (50.0.0.2) which is the 'R2'. Then, it arrives to (11.0.0.2) which is the 'computer D'.

Suppose that there is a problem in the 'R2' connection with 'computer D', in this case the data will arrive to (50.0.0.2) which is R2. Then (11.0.0.2) will be marked as 'unreachable'. Therefore, we can know that the network connectivity problem exists in the connection between the 'R2' and the 'computer D'.

10.4 Privileged mode commands, backing up and restoring processes

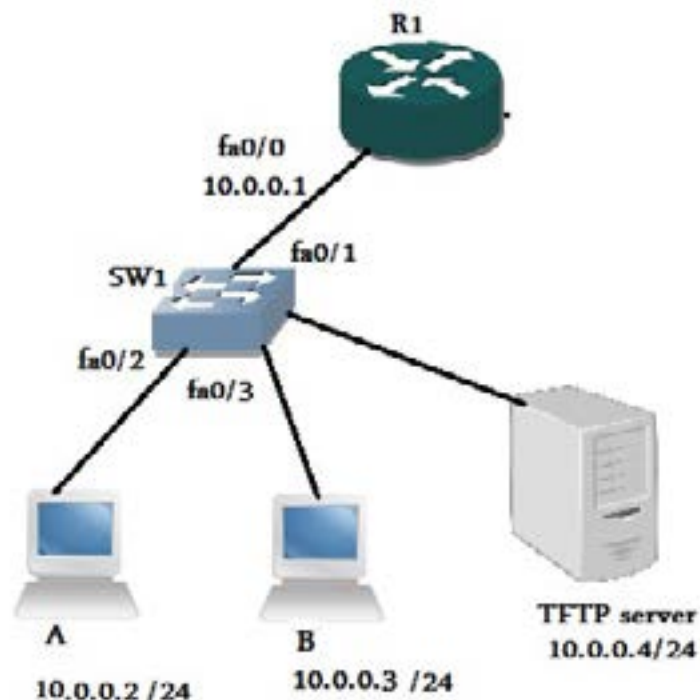


Figure 10.11: backing up and restoring.

In figure (10.11), the TFTP server is used to back up the Cisco IOS and the router's configuration, and to retrieve the Cisco IOS and the router's configuration from it to the router.

We use the 'copy' command to copy a file from the router to the TFTP, and vice versa.

10.4.1 Backing up an restoring the Cisco IOS

The 'copy flash tftp' command

```
Router# copy flash tftp
```

This command is used to make backing up for the router's Cisco IOS, this is done by taking a copy from the Cisco IOS that exists on the router's flash memory, and put this copy on the the TFTP server.

When we write this command, the router will ask us for the Cisco IOS' file name and the TFTP server's IP address.

The 'copy tftp flash' command

```
Router# copy tftp flash
```

This command is used to make a restoring for the Cisco IOS from the TFTP server to the router's flash memory.

This command also can be used if we have a newer Cisco IOS version on the TFTP server, and we need to copy it to the router's flash memory to replace the older version that exists on the router. This process is called the Cisco IOS upgrading.

10.4.2 Backing up and restoring the router's configuration

The 'copy running-config startup-config' command

```
Router# copy running-config startup-config
```

This command is used to copy the running configuration that exists on the RAM to the startup configuration that exists on the NVRAM.

The 'copy running-config tftp' command

```
Router# copy running-config tftp
```

This command is used to back up the running configuration on the TFTP server.

The 'copy tftp running-config' command

```
Router# copy tftp running-config
```

This command is used to restore the router's configuration from the TFTP server to the router's RAM.

10.5 Global configuration mode commands

10.5.1 Configuring a host name

We use the following command in order to assign a name to the router,

```
Router(config)# hostname name
```

```
Router(config)#hostname R1
R1(config)#
```

Figure 10.12: assigning a hostname to the router.

You can observe that the hostname is changed from 'Router' to the new hostname 'R1'.



10.5.2 Configuring a password

Enable PW

Enable password is the password that the router asks us to enter when we try to enter to the privileged mode from the user exec mode, as seen in figure (10.13).

```
R1>enable
Password: █
```

Figure 10.13: asking for the password.

To assign the password, we use the following command,

```
Router(config)# enable password password
```

```
R1(config)#enable password cisco
```

Figure 10.14: assigning a password.

Enable secret PW

It is the same as the 'enable password', but the difference is that it is stored in the router's configuration in an encrypted form.

To configure a 'secret PW', we use the following command:

```
Router(config)# enable secret password
```

```
R1(config)#enable secret cisco
```

Figure 10.14: assigning a secret password.

Console PW

The console PW is used to authenticate the user when he tries to connect to the router through its console port.

To assign a console PW to the router, we use the commands seen in figure (10.15).

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
```

Figure 10.15: assigning a console password.

Auxiliary PW

The auxiliary PW is used to authenticate the user when he tries to connect to the router through its auxiliary port.

To assign an auxiliary PW to the router, we use the commands seen in figure (10.16).

```
R1(config)#line aux 0
R1(config-line)#password cisco
R1(config-line)#login
```

Figure 10.16: assigning an auxiliary password.

Telnet PW

The telnet PW is used to authenticate the user when he tries to connect to the router through the telnet.

To assign a telnet PW to the router, we use the commands seen in figure (10.17)

```
R1(config)#line vty 0
R1(config-line)#password cisco
R1(config-line)#login
```

Figure 10.17: assigning a telnet password.

10.6 Specific configuration modes

10.6.1 The 'router configuration mode'

This mode is one of the specific configuration modes. In addition, it is used to configure the routing protocols on the router.

10.6.2 The 'interface configuration mode'

The interface configuration mode is one of the specific configuration modes. In addition, it is used to assign an IP address to a certain interface, and bringing up or shutting down a certain interface.

To enter to the interface configuration mode from the global configuration mode, we use the following command:

Router(config)# interface *type number*

```
R1(config)#interface serial 0/0
R1(config-if)#
```

Figure 10.18: entering to the interface mode.

To assign an IP address and a subnet mask to a certain interface, we use the following command:

```
Router(config)# ip address ip subnetmask
```

The 'no shutdown' command is used to bring up the interface; this is because its default status is 'shutdown'.

```
R1(config)#interface serial 0/0
R1(config-if)#ip add
R1(config-if)#ip address 50.0.0.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#no shutdown
```

Figure 10.19: assigning an IP address to an interface, and bringing it up.

10.7 CDP (Cisco Discovery Protocol)

The CDP is a Cisco proprietary protocol that allows us to know the neighbors of the device that we are currently connected to.

An advertisement for SAP Learning Hub. The background is a blurred cityscape with a tall building. In the foreground, a man with glasses and a dark sweater is looking at a tablet. The text is overlaid on the image.

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub

SAP

Suppose that we have the following network,

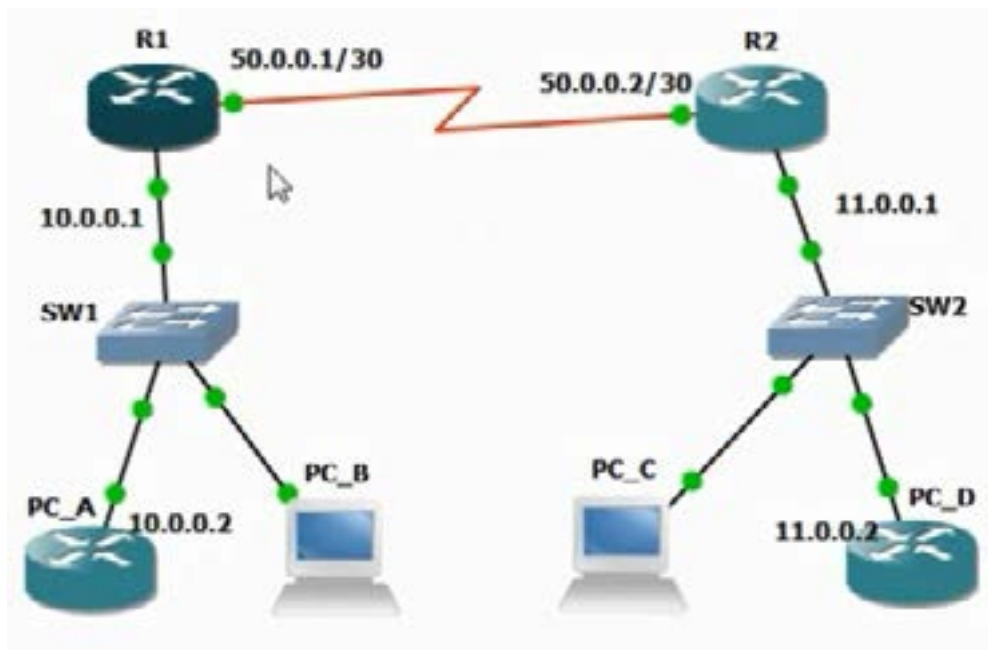


Figure 10.19: CDP protocol is used to know the neighboring devices.

You are connected to R1 and need to know its neighbors. Simply, you can use the following command,

```
Router# show cdp neighbors
```

Then, you will be able to show the neighboring devices of R1 as seen in figure (10.21).

```
R1#show CDP neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID         Local Interface   Holdtime    Capability   Platform   Port ID
PC_A              Fas 0/0          135         H            2621       Fas 0/0
R2                Ser 0/0          133         R            2621       Ser 0/0
```

Note that this result is not accurate because it came from a simulator not a real router.
Right result neighbors should be R2 and SW1.

Figure 10.10: the CDP neighbors.

The CDP protocol operation depends on the following,

Every Cisco networking device is sending a CDP packet every a specific time period to its neighbor. This CDP packet contains some information about the device.

The 'CDP timer' is the periodic duration in which the Cisco networking device is sending a CDP packet.

The 'CDP hold time' is the amount of time in which a Cisco networking device will hold the received CDP packet from its neighbor.

To display the CDP timer and the hold time values, we can use the following command,

```
Router# show cdp
```

A woman with long dark hair, wearing a grey sleeveless top, stands in profile looking at a smartphone. She is positioned in front of a large window that looks out onto a green landscape. The background is slightly blurred, emphasizing the woman and the text overlay.

MAXIMIZE PRODUCTIVITY

**HELP YOUR ENTIRE
ORGANIZATION
BUILD EXPERTISE
IN SAP SOFTWARE.**

SAP Learning Hub

SAP

Hour 11: Routing Protocols

11.1 Routing protocols basics

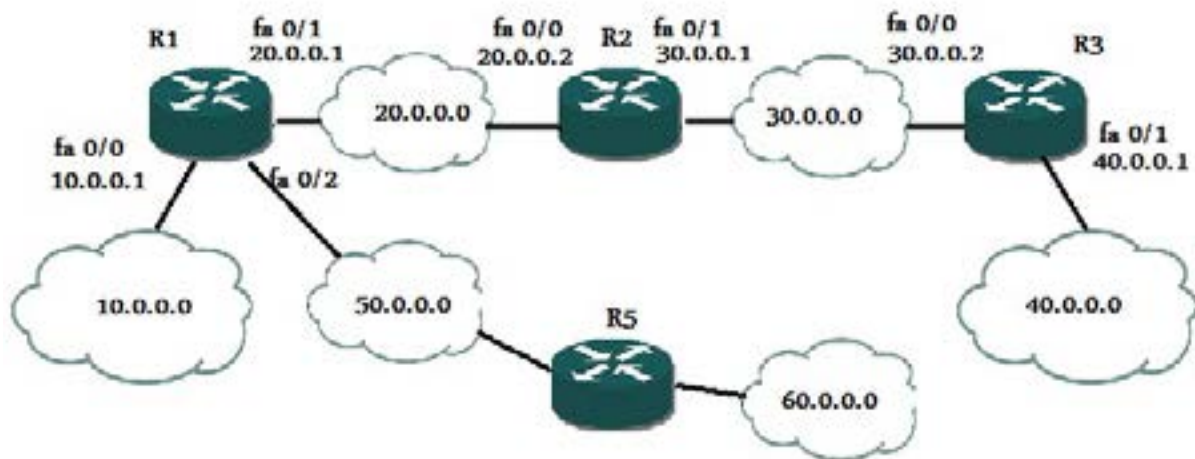


Figure 11.1: some routers connected to some networks.

11.1.1 What is a 'routing protocol'?

Suppose that we have a group of routers connected to a group of networks as seen in figure (11.1), the routing protocol is used to inform every router the path to every network.

By default, every router knows about its direct connected networks – because those networks are stored in its routing table –, but it does not know about other networks.

As an example, the router 'R1' knows by default about networks (10.0.0.0, 20.0.0.0, 50.0.0.0). However, it does not know about other networks.

To make 'R1' knows about all other networks, we use the routing protocols.

11.1.2 Routing protocol types

Static routing protocol

In the static routing protocol, the administrator of the network manually configures every router.

Therefore, this method has high administrative effort on the administrator.

Dynamic routing protocol

In the dynamic routing protocol, the routers automatically communicate with each other, and exchange data about the networks it knows about. Therefore, every router knows the path to every network.

This method consumes from the router's CPU and the network's bandwidth.

11.1.3 Comparison between static routing & dynamic routing

Static routing	Dynamic routing
Advantages Low CPU utilization Low BW utilization Disadvantages More administrative efforts	Disadvantages High CPU utilization High BW utilization Advantages Low administrative efforts

Table 11.2: a comparison between static and dynamic routing.

11.2 Static routing

In the static routing, the administrator manually configures every router.

To make that, the administrator logs in to the router and enters to the 'global configuration mode'.

In the 'global configuration mode', the administrator writes the following command,

```
Router(config)# ip route network IP subnet mask next hop IP
```

Or

```
Router(config)# ip route network IP subnet mask exit interface
```

Where,

'Network IP' is the network IP of the destination network.

'Subnet mask' is the subnet mask of the destination network.

'Next hop IP' is the IP of the next hop router interface.

'Exit interface' is the router's interface that the router should send the packet through it.

Suppose we have the network in figure (11.2),

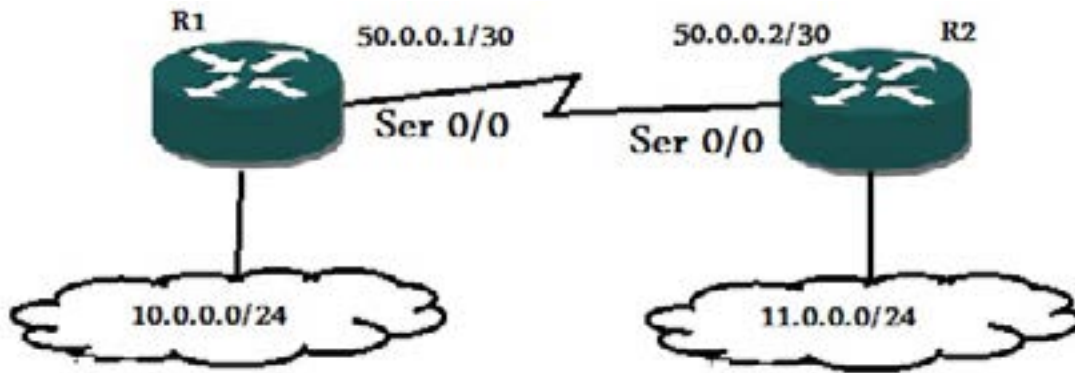


Figure 11.2

The administrator needs to configure 'R1' to be able to reach the network '11.0.0.0/24'.

Then, the parameter will be as following,

Network IP = 11.0.0.0

Subnet mask = 255.255.255.0

Next hop IP = 50.0.0.2

Exit interface = ser 0/0

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



11.3 Dynamic routing

In the dynamic routing, the routers communicate with each other in order to exchange the network's information.

Every router should determine the shortest path (least cost path) to every network in order to store this path in its routing table to use it.

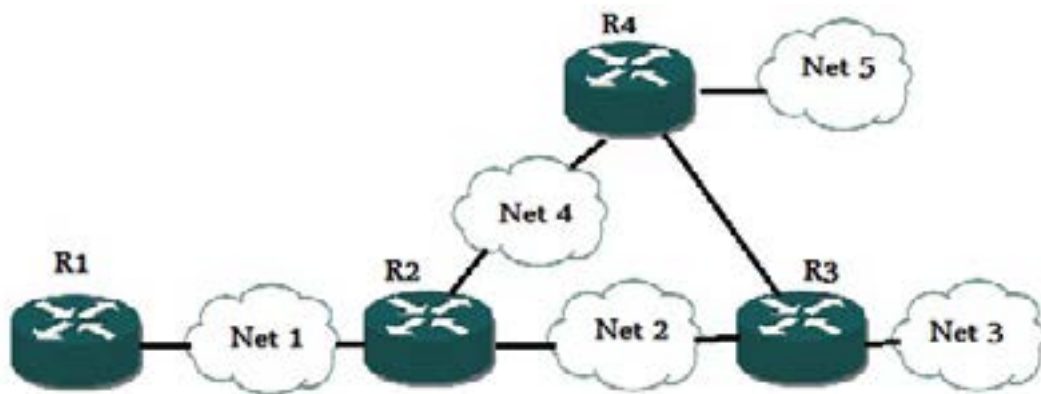


Figure 11.3

In figure (11.3), 'R2' is able to reach 'Net3' through two paths – through 'R4' and through 'R3'. 'R2' should determine the shortest path to 'Net3' and store it in its routing table in order to use it.

11.3.1 Dynamic routing protocol types

The dynamic routing protocols are divided into two groups,

Distance vector routing protocols

In this type,

- Updates are sent periodically (every specific time).
- Updates contain information about the entire routing table.
- Updates are sent only to neighboring routers.

Link state routing protocols

In this type,

- Updates are sent when a change occurs in the routes.
- Updates contains information about only the affected routes.
- Updates are sent to the entire network.

11.4 Distance vector routing

In the distance vector routing, every router sends its entire routing table to only neighboring routers, and this is done every periodic time.

So, every router knows only about its neighboring routers.

The cost of the path – path metric – in the distance vector routing is determined by the ‘hop count’, which is the number of hops – routers – between the source and the destination.

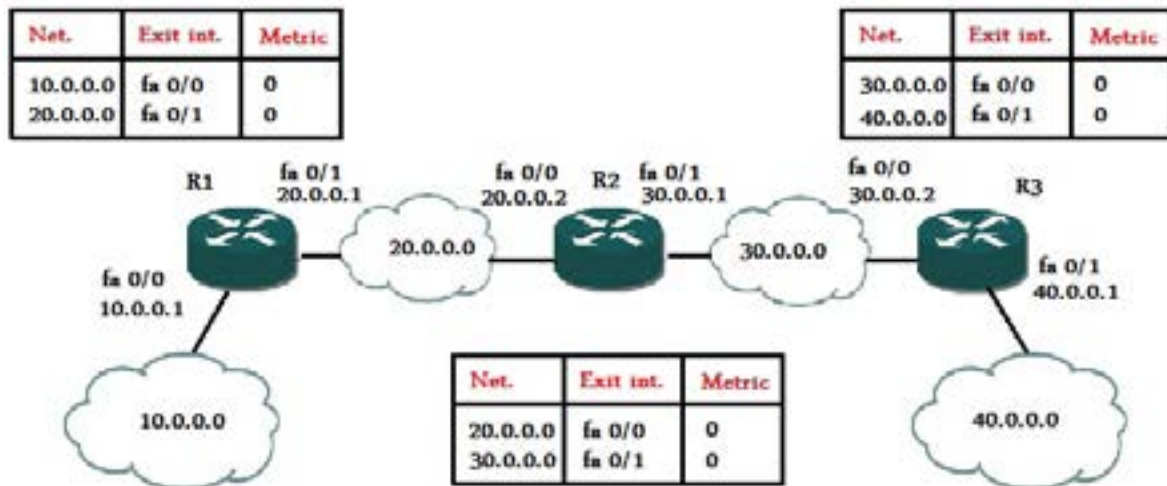


Figure 11.4: the distance vector routing

By default, every router knows its direct connected networks as seen in figure (11.4).

R1 sends its routing table to R2.

R2 sends its routing table to R1 and R3.

R3 sends its routing table to R2.

After the routing table exchange between all routers, the routing table of R1, R2, and R3 respectively will be as following,

Net.	Exit int.	Metric
10.0.0.0	fa 0/0	0
20.0.0.0	fa 0/1	0
30.0.0.0	fa 0/1	1
40.0.0.0	fa 0/1	2

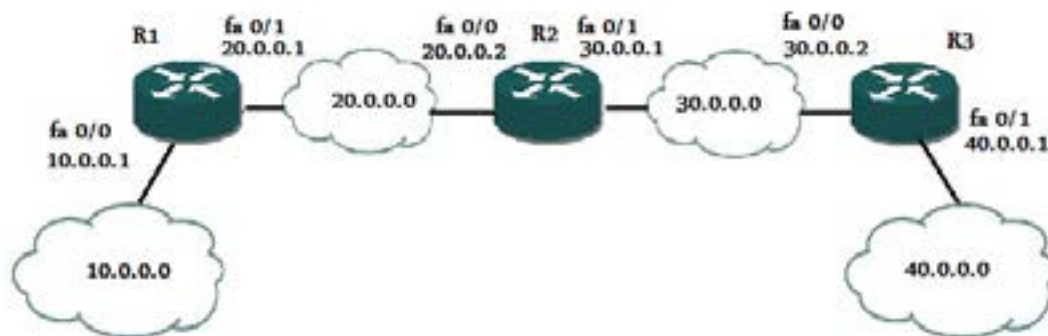
Net.	Exit int.	Metric
20.0.0.0	fa 0/0	0
30.0.0.0	fa 0/1	0
10.0.0.0	fa 0/0	1
40.0.0.0	fa 0/1	1

Net.	Exit int.	Metric
30.0.0.0	fa 0/0	0
40.0.0.0	fa 0/1	0
20.0.0.0	fa 0/0	1
10.0.0.0	fa 0/0	2

Figure 11.5: the routing tables after the route exchange

As you can see in figure (11.5), now every router is able to reach every network.

11.5 Routing loops



The routing loop is a problem that causes the packets to enter in a loop between the routers.

This problem happens because of the exchange of incorrect route information between the routers.

The routing loop may happen in a network that is using a distance vector routing protocol.

11.5.1 Routing loop solution

To solve the routing loop problem, we have many solutions,

Maximum hop count

Every packet contains a field in its IP header, which is called the 'TTL' (Time To Live). The TTL value is reduced every time it passes by a router.

Therefore, if a routing loop happened, the packet will be discarded after a while when the TTL value become zero.

Split horizon

It is a simple rule that says, 'never send routing updates out of the interface this update is received from'.

Route poisoning

When a path to a network becomes unavailable, inform all the routers that, this network has infinite metric, so that all routers will update its routing table with this information.

Hold downs

This rule states that, when a route is marked as 'unreachable', stay in hold down state for a time that equals to the hold down time.

The 'hold down state' means, do not accept updates about this route.

Hour 12:RIP Routing Protocol

RIP (Routing Information Protocol) is a distance vector routing protocol.

In this protocol, the metric used to calculate the path cost is the 'hop count'.

The maximum hop count in the RIP protocol is '15'. It means that, a network that uses the RIP routing protocol cannot contain more than 15 routers, which is a disadvantage in the RIP protocol.

RIP timers

Route update timer: it is the interval between the routing updates (30 sec.).

Route invalid timer: it is the period before a router determines that a route is unreachable (180 sec.).

Route flush timer: it is the period between the route 'invalid' state, and its removal from the routing table (240 sec.).

Holddown timer: the router will be in the hold down state during this period, this is done after an update packet is received telling that a certain route is unreachable (default = 180 sec.).



JUMP-START CAREERS

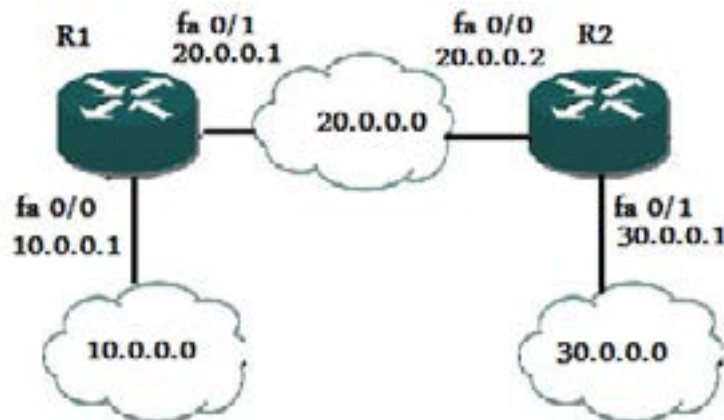
**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub

SAP

RIP configuration



To configure a router to use the RIP routing protocol, we write the following commands,

```
Router(config)# router rip
```

```
Router(config-router)# network ip address
```

To verify the router's RIP configuration, we need to see the routing table of the router.

To see the routing table, we write the following command,

```
Router# show ip route
```

12.1 RIP is a classful routing protocol

A 'classful routing protocol' means that the RIP protocol does not send the subnet mask information with the network updates.

Therefore, RIP does not support the 'discontiguous networks', the 'CIDR', and the 'VLSM'. This will be discussed in the following pages.

12.1.1 Discontiguous networks

In discontiguous networks, every router thinks it has the only 10.0.0.0/8 network

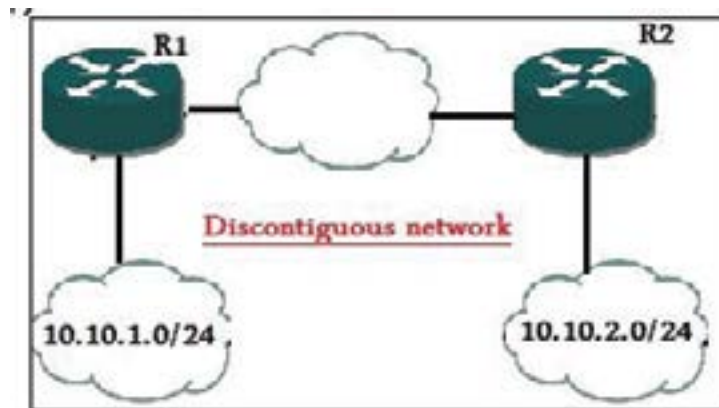


Figure 12.1: the discontiguous networks

12.1.2 CIDR

CIDR (Classless Inter-Domain Routing) is to route the data between the networks that has subnet mask information are different from the default subnet masks.

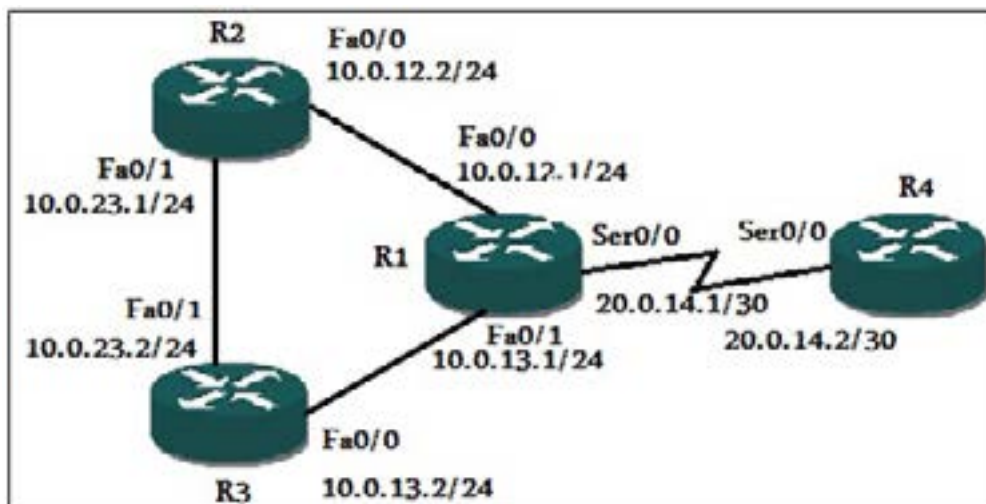


Figure 12.2: CIDR

12.1.3 VLSM

VLSM (Variable Length Subnet Mask) is to have networks with variable subnet masks that are subnetted from one network IP.

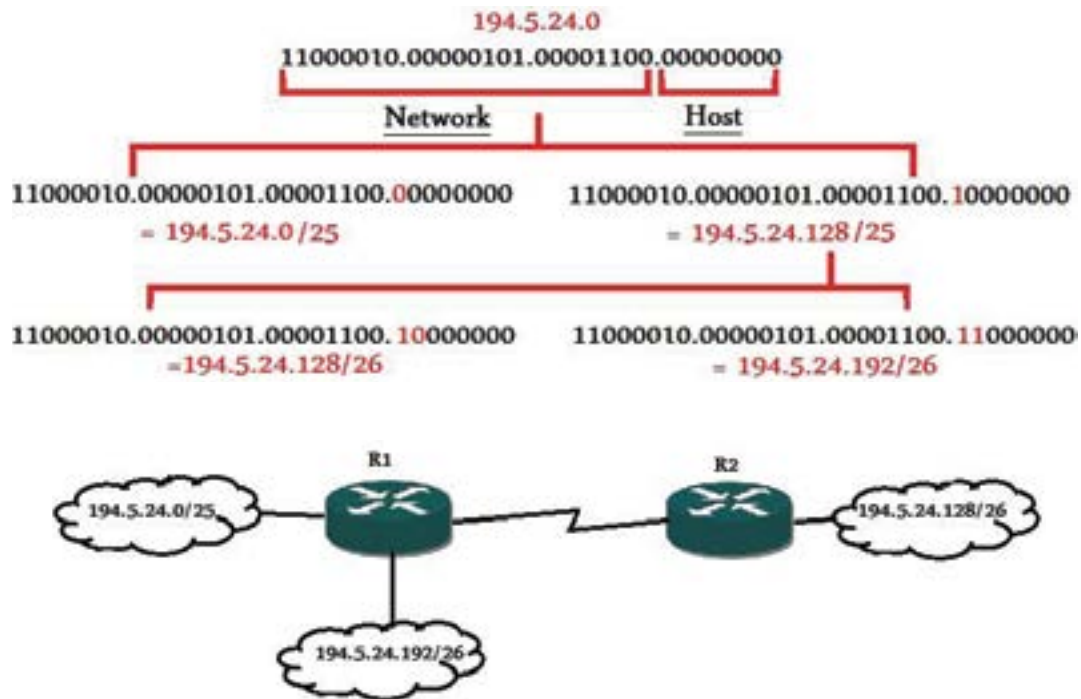


Figure 12.2: VLSM

LEARN BY DOING

DEVELOP EXPERTISE IN SAP SOLUTIONS THROUGH EXPLORATION AND PRACTICE.

SAP Live Access

SAP Learning Hub



12.2 RIPv2 (RIP version 2)

The advantage of the RIPv2 protocol over the RIP protocol is that, it is a 'classless routing protocol'

This means that RIPv2 sends the subnet mask information with the network updates.

Therefore, RIPv2 supports the 'discontiguous networks', the 'CIDR' and the 'VLSM'.

12.2.1 RIPv2 configuration

In order to configure the router to work with RIPv2, we write the following commands,

```
Router(config)# router rip
```

```
Router(config-router)# version 2
```

```
Router(config-router)# network ip address
```

```
Router(config-router)# no auto-summary
```

12.2.2 Passive Interface configuration

We can configure any interface as a 'passive interface', this is used in order to not send or receive any network updates on a certain interface.

To configure the 'passive interface, we use the following command,

```
Router(config-router)# passive-interface interface
```

12.3 IGRP routing protocol

IGRP (Interior Gateway Routing Protocol) is a Cisco proprietary protocol, which means that it could not be configured on any device except a Cisco device.

It is a classful routing protocol.

The maximum hop count is '255', which is an advantage over the RIP protocol, which has only '15'.

The metric used to calculate the path cost is the 'Delay' and the 'bandwidth'.

Currently, Cisco does not support the IGRP protocol.

Hour 13:OSPF Routing Protocol

OSPF (Open Shortest Path First) routing protocol is a link state routing protocol. Therefore, every router sends a network update once a change happens in the routes in its routing table. In addition, this network updates contain only the affected routes, and are sent to the entire network.

This allows every router to build a database that reflects the structure of the entire network. In addition, allow every router to have a faster convergence time than the distance vector routing protocols.

The convergence time is the time required to find an alternative path to a certain network, once its main path is unavailable.

OSPF characteristics

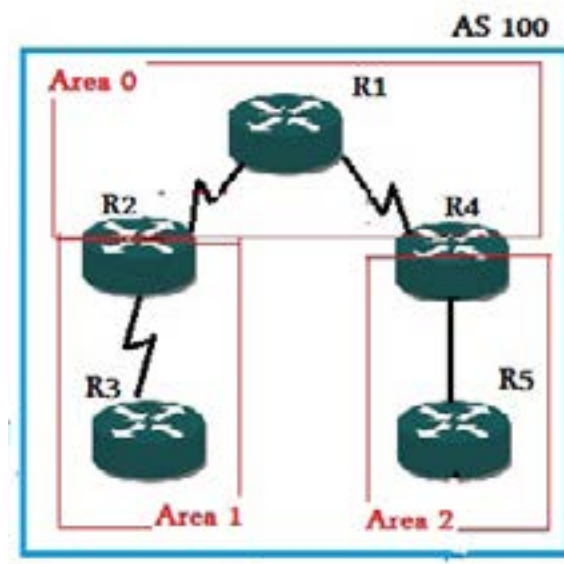


Figure 13.1

- It is a classless routing protocol. This means that it supports the CIDR, the VLSM and the discontiguous networks.
- The default cost of the path = '100M/BW'.
- It uses the 'Dijkstra Shortest Path First (SPF)' algorithm to determine the best path to every network.
- It logically segments the network into areas, as seen in figure (13.1).
- It uses 'area 0' (the backbone area) at the top of the hierarchy, this means that all other areas must be connected to 'area 0'.
- It uses area numbers from the range (0: 65535).

13.1 OSPF neighbors and adjacencies in a LAN

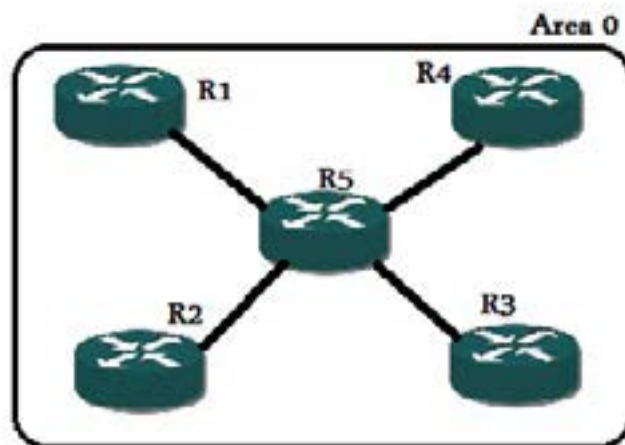


Figure 13.2

- Routers send multicast 'hello packets' out of the OSPF interfaces to discover the OSPF neighbors.
- The hello packets are sent every time period called the 'hello time'.
- If no hello packet is received from a certain router during a time period called the 'dead time', this router will be considered as unavailable.
- The hello packets are sent to a multicast IP address '224.0.0.5'.
- The network administrator may configure the routers to authenticate each other before exchanging the routing updates.
- The following conditions must be met for the neighborship to be established between two routers,
 1. The same hello/ dead timers.
 2. The same subnet mask.
 3. The same area ID.
 4. The authentication type and PW.
- The routers that exist in the same area elect one router as a 'DR' (Designated Router), and another router as a 'BDR' (Backup Designated Router).
- All routers in the area establish an adjacency with the 'DR' and the 'BDR'.
- All network updates are sent to the 'DR' and the 'BDR' on the IP address '224.0.0.6' using a 'router LSA' (Link State Advertisement).
- The 'DR' and the 'BDR' forward the network updates to the routers that exist in their area, this is done by sending a 'network LSA' on a multicast IP address '224.0.0.5'.

13.2 OSPF configuration

To configure the OSPF routing on a router, we write the following commands,

```
Router(config)# router ospf process number
```

```
Router(config-router)# network network IP wildcard mask area area number
```

The **Process Number** is a locally significant number on every router.

The **network IP** is the destination network IP.

The **wildcard mask** is a reversed subnet mask. To get it, change every '1' to '0' and every '0' to '1' as seen in figure (13.3).

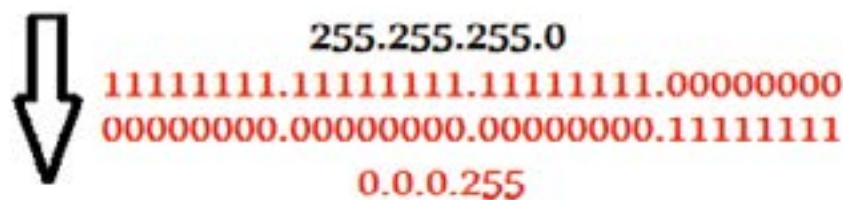


Figure 13.3: the wildcard mask

**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

13.2.1 Passive interface configuration

Configuring an interface as a passive interface prevents it from sending or receiving the 'hello packets'.

To configure an interface as a passive interface, we use the following command,

```
Router(config-router)# passive-interface interface
```

13.3 DR election

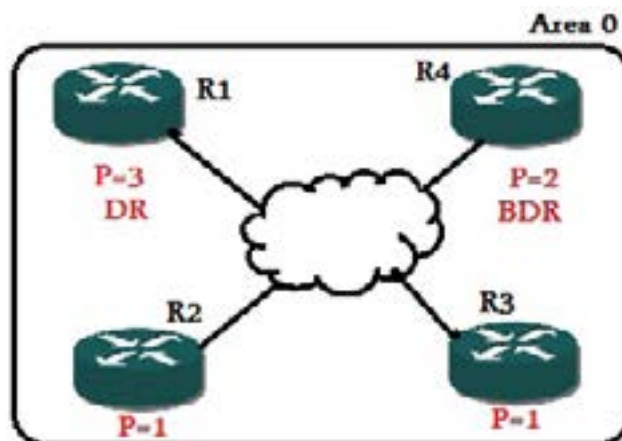
In the OSPF protocol, the routers in every area elect a 'DR' and a 'BDR'.

When a router needs to send network updates to the other routers in the area, it sends this update to the 'DR' and the 'BDR'. Then, the 'DR' and the 'BDR' forward this update to all the routers in the area.

How routers elect the 'DR'?

1. First, choose the router with highest router priority.
2. If all the priorities are the same, choose the router with the highest 'router ID'.

13.3.1 Router priority



The default router priority for every router is '1'.

The router priority can be changed manually using the following command,

```
Router(config-if)# ip ospf priority 2
```

13.3.2 Router ID (RID)

1. The 'RID' is statically assigned using the following command,

```
Router (config)# router ospf 0  
Router(config-router)# router-id 1.1.1.1
```

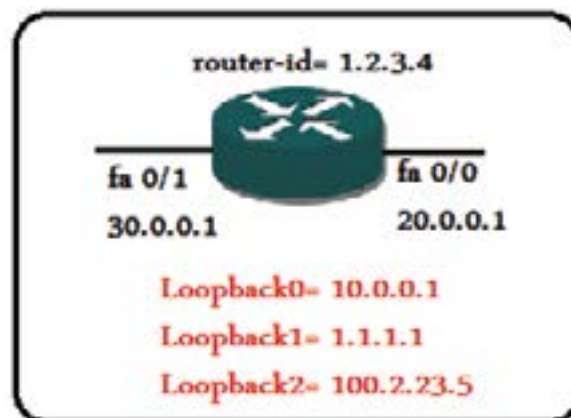
2. If no statically assigned 'RID' exists, the 'RID' will be the highest loopback interface IP, the loopback interface is a virtual interface that can be configured on the router.
To configure a loopback interface, use the following commands,

```
Router(config)# interface loopback0  
Router(config-if) ip address 10.10.10.10 255.255.255.255
```

3. If no loopback interface is configured on the router, the 'RID' will be the highest interface IP on the router.

Example:

Determine the 'RID' of the below router,



Solution

RID= the statically assigned RID = 1.2.3.4

If there wasn't statically assigned RID,

RID = the highest loopback interface IP = 100.2.23.5

If there was not a loopback interface configured,

RID = the highest interface IP = 30.0.0.1

Hour 14:EIGRP Routing Protocol

EIGRP (Enhanced IGRP) is a hybrid routing protocol. It has some characteristics from both the distance vector routing and the link state routing.

EIGRP Characteristics

- It is a Cisco proprietary. It only works on Cisco devices.
- It is a classless routing protocol; this means that it supports the CIDR, the VLSM and the discontinuous networks.
- The maximum hop count is '255'.
- It uses 'DUAL' (Diffusion Update Algorithm) to find the best path to the networks.
- It can load balance between up to six unequal cost paths.
- It uses the 'successor route' and the 'feasible successor route' for fast convergence.
- The 'successor route' is the route that is installed in the routing table in order to use it to reach a certain network.
- The feasible successor route can be considered as a backup for the successor route.



ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

EIGRP metrics

The default metrics used by the EIGRP protocol to calculate the path cost are the 'delay' and the 'bandwidth'.

However, EIGRP protocol can use the delay, the bandwidth, the load, and the reliability as the path cost metrics.

EIGRP neighborship

- The routers that are running EIGRP discover neighbors using the 'hello' messages.
- The routers must have the following conditions to form a neighborship,
 1. The same AS number (Autonomous System number); the autonomous system is the network that exists under the same administration.
 2. The same path cost metrics.
- Only neighbors can exchange routes with each other using the multicast IP address '224.0.0.10'.

EIGRP tables

Routers that are running EIGRP contain three tables,

The neighbor table: it contains the EIGRP neighbors.

The topology table: it contains the 'EIGRP topology, including the successor and the feasible successor routes.

The routing table: it contains the routes that are currently used to route the data.

14.1 EIGRP configuration

To configure the EIGRP protocol on a router, we use the following commands,

```
Router(config)# router eigrp AS_number
```

```
Router(config-router)# network IP_address wildcard_mask
```

```
Router(config-router)# no auto-summary
```

14.2 Administrative Distance (AD)

The 'Administrative Distance' (AD) is a number assigned to every routing protocol.

Figure (14.1), lists the 'AD' for every routing protocol,

Connected	0
Static routing	1
RIP	120
IGRP	100
OSPF	110
EIGRP	90

Figure 14.1: the administrative distance

In figure (14.2),

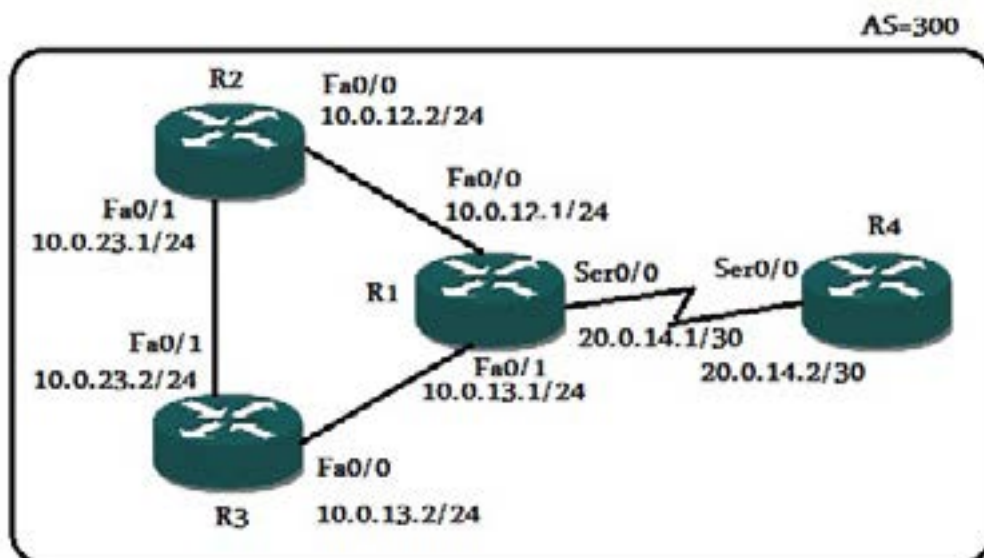


Figure 14.2

Suppose that 'R3' has the RIP protocol and the OSPF protocol running on it.

The RIP protocol is telling R3 that, to reach the network '20.0.14.0/30', send the data to R1.

The OSPF protocol is telling R3 that, to reach network '20.0.14.0/30', send the data to R2.

Which path will R3 use to reach '20.0.14.0/30'?

It will use the path that was installed in the routing table by the routing protocol that has the **lowest AD**.

Because the RIP protocol's AD is '120'. Moreover, because the OSPF protocol's AD is '110', R3 will use the path installed by the OSPF protocol.

Therefore, to reach the network '20.0.14.0/30', R3 will send the data to R2.

14.3 Default route

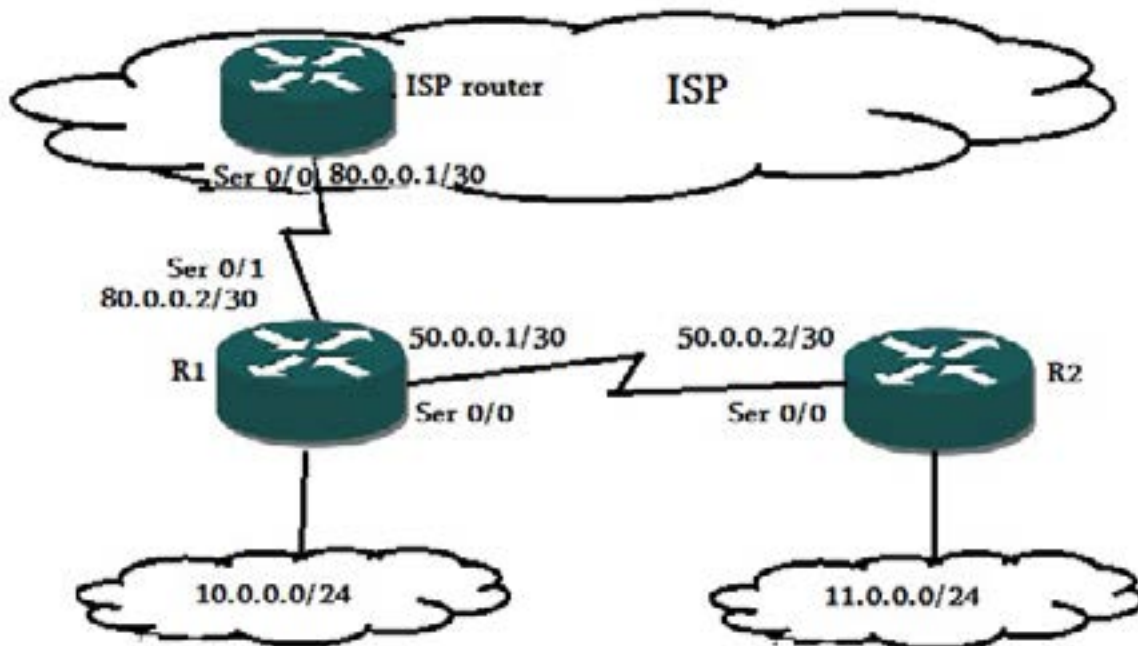


Figure 14.3

NO-LIMITS LEARNING

**LEVERAGE SOCIAL LEARNING,
COLLABORATION, QUALITY
CONTENT, AND HANDS-ON
PRACTICE.**

SAP Learning Hub

SAP

A woman and a man are standing in front of a large window, looking at a tablet together. The woman is on the left, wearing a white top, and the man is on the right, wearing a striped shirt. The background is a bright, modern office interior with large windows.

In figure (14.3), suppose that R1 needs to send some data to a certain destination that exists in the internet. In addition, R1 searched for this destination in its routing table to determine the next hop. However, R1 did not find any entry for this destination in its routing table. What should R1 do?

In this case, R1 should send the data to the 'default route'.

The default route is an entry in the routing table that is used by the router in case that it did not find any entry for the destination network in its routing table.

The default route entry in the routing table is '0.0.0.0' and the subnet mask is '0.0.0.0'.

14.3.1 Default route configuration.

To configure the default route we use one of the following commands in the global configuration mode,

```
Router(config)# ip route 0.0.0.0 0.0.0.0 next hop IP address
```

Or

```
Router(config)# ip route 0.0.0.0 0.0.0.0 exit interface
```

Another method is to configure a default network is using the following command,

```
Router(config)# ip default-network network IP address
```

In this method, the network IP must be reachable using one of the routing protocols.

Hour 15: Switch Operation

15.1 Switch operation and characteristics

Switches are 'layer 2' devices that forward the frames between the devices connected to its ports using the MAC address table that exists on the switch.

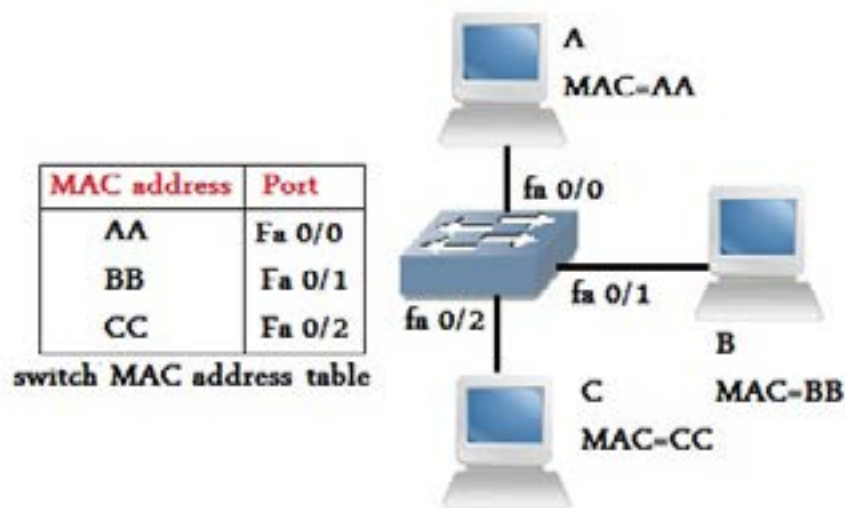


Figure 15.1: switch operation

In figure (15.1), suppose that 'computer A' needs to send a frame to 'computer C'.

'Computer A' will send a frame with the destination MAC address equals to 'CC' to the switch.

The switch will look for MAC address 'CC' in its routing table.

The switch will find the MAC address connected to its 'fa 0/2' port.

Therefore, the switch will forward the frame through its 'fa 0/2' port to reach the destination computer 'computer C'.

15.1.1 Switch characteristics



Figure 15.2: a switch

Switches use hardware ASICs (Application Specific Integrated Circuits) to switch the frames between its ports. Therefore, switches are faster than routers (taking into consideration that, switches are 'layer 2' devices, while routers are 'layer 3' devices).

Switches divide the collision domain, while it does not divide the broadcast domain.

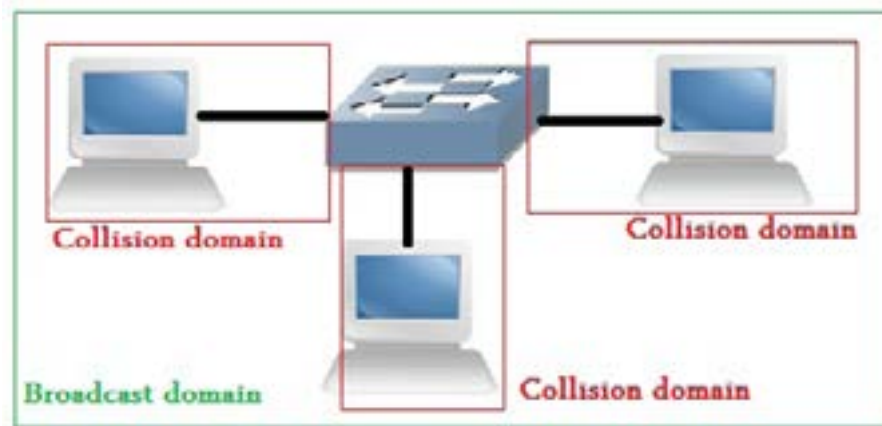


Figure 15.3: switches divide the collision domain

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub



15.2 Switch 'layer 2' functions

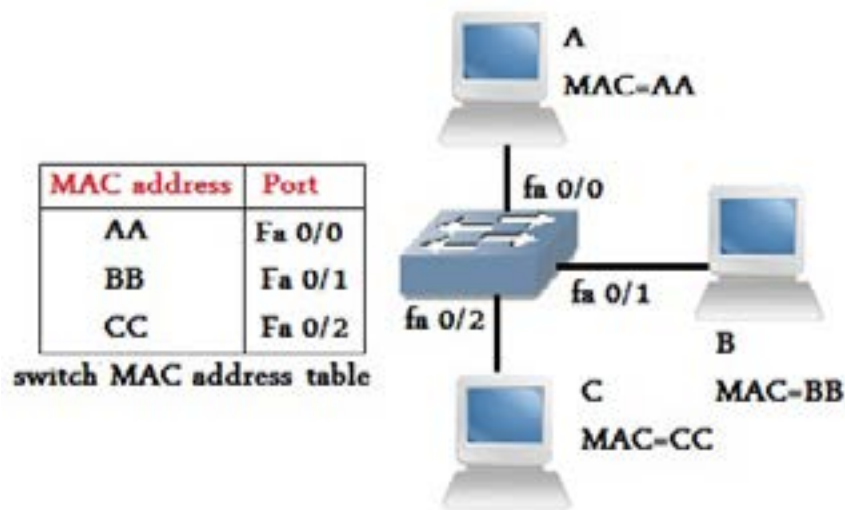


Figure 15.4: switch operation

15.2.1 Address learning

The switches build its MAC address table by recording the source MAC address for every frame it received, combined with the port number that the frame is received on.

To view the MAC address table on the switch, we can use the following command,

```
Switch# show mac address-table
```

We can put a static entry in the MAC address table using the following command,

```
Switch(config)#mac address-table static mac-address vlan vlan-id interface port no.
```

Note that, the 'VLAN' term will be illustrated in the next hour.

15.2.2 Frame forwarding (filtering)

The switches take the forwarding decision depending on the information that exists in its MAC address table.

When the switch receives a frame, the switch will look at the destination MAC address in the frame, and decide through which port it should forward this frame by looking for this MAC address in its MAC address table.

If the switch did not find the destination MAC address in its MAC address table, the frame will be flooded out through all of the switch interfaces, except the interface the frame came from.

15.3 Port security

The port security is used to prevent the users from attaching any unauthorized device to the network.

The port security does this role by limiting the number of MAC addresses that are allowed for every switch port.

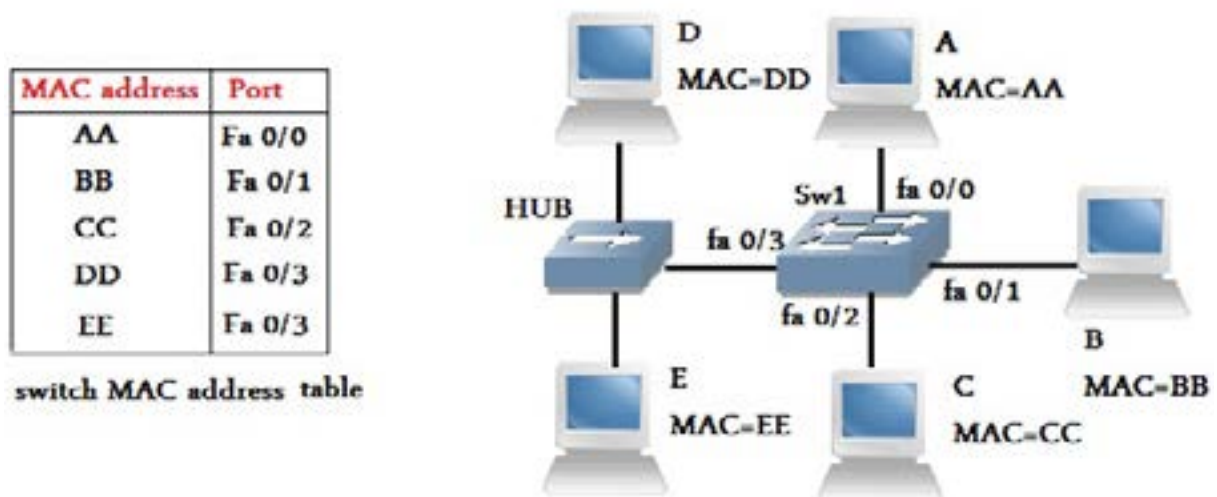


Figure 15.5: port security

In figure (15.5), suppose that the port security is configured on the interface 'fa 0/3' in order to limit the number of MAC addresses allowed to connect to this port to only two MAC addresses.

Currently, there are two MAC addresses connected to 'fa 0/3', which are 'DD' and 'EE'.

So currently, there are no more devices allowed to connect to the port 'fa 0/3'.

15.3.1 Port security configuration

To configure the port security on a switch port we can use the following commands,

```
Switch(config)# interface port type/number
```

```
Switch(config-if)#switchport port-security maximum number of allowed MACs addresses
```

```
Switch(config-if)#switchport port-security violation {shutdown | restrict }
```

In the last command you can use the 'shutdown' keyword or the 'restrict' keyword.

Shutdown: the port will shutdown and the administrator should manually bring it up

Restrict: the port will not shutdown but it will refuse to receive any data from or send any data to the restricted device.

Hour 16:Virtual LAN (VLAN)

16.1 Virtual LAN (VLAN) characteristics

Using VLANs enhances the network performance, and the network security, and enhances the management flexibility of the network.

16.1.1 VLANs enhance the network performance

Suppose that we have the following network:

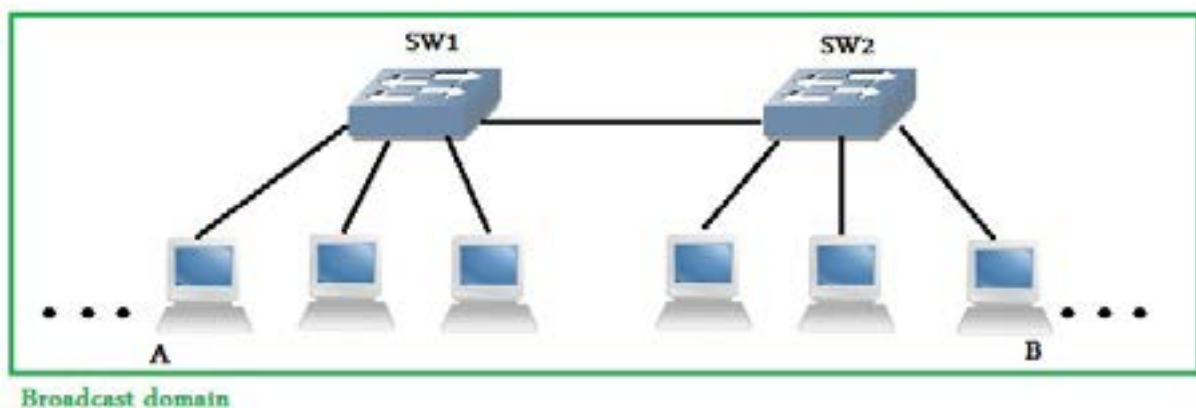


Figure 16.1: a network without a VLAN

MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub





In figure (16.1), all the devices exist in the same broadcast domain. This is because that the switches do not divide the broadcast domains.

We can divide this LAN into many VLANs by assigning every switch port to a certain VLAN. Every VLAN will have its own broadcast domain as seen in figure (16.2).

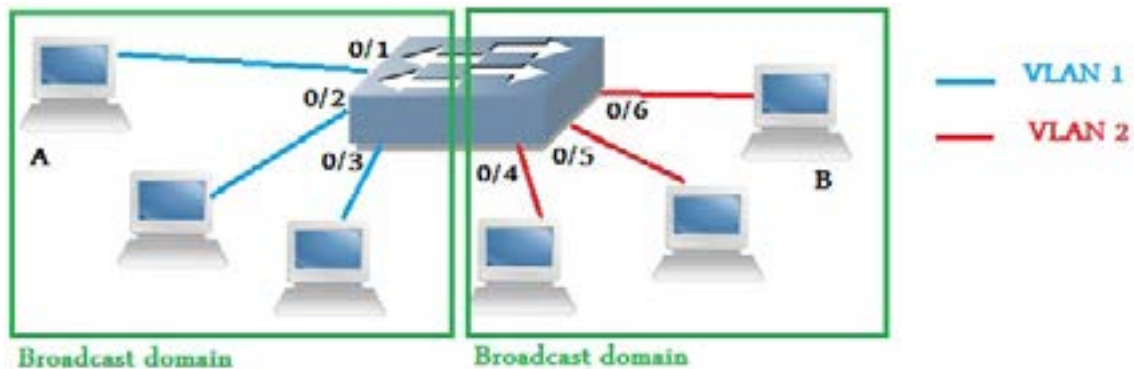


Figure 16.2: a network that is divided to VLANs

Dividing one broadcast domain into many broadcast domains enhances the network performance.

16.1.2 VLANs enhance the network security

Every department in the company should exist in its own LAN as seen in figure (16.3).

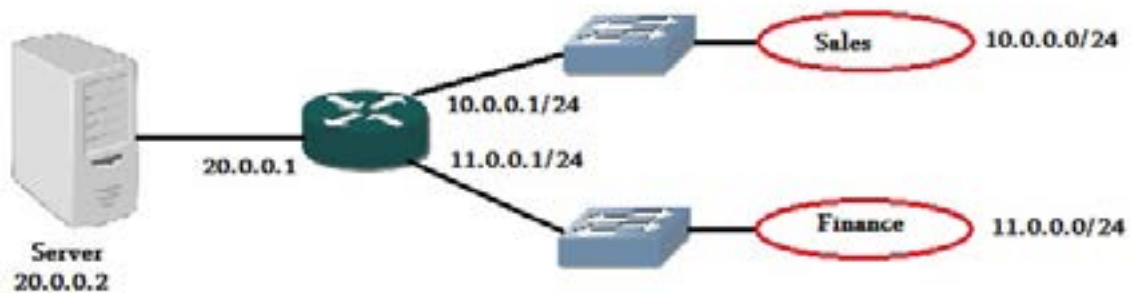


Figure 16.3: every department exists in its own LAN

This enhances network security because,

1. The broadcast packet sent from one department will not reach any computer in another department. As an example, in figure (16.3), if a computer in the 'sales' department sent a broadcast, it will reach all the computers in the 'sales' LAN. However, it will not reach any computer in the 'finance' LAN.
2. We can control the access to the network resources. As an example, in figure (16.3), we can configure our network to allow the 'sales' LAN (10.0.0.0/24) to access the server '20.0.0.2', while not allowing the 'finance' LAN (11.0.0.0/24) to access the same server.

As you can see in figure (16.3), to put every department in its own LAN, we need to dedicate some switches to every department, and to connect every department's LAN to its own router's interface. Therefore, if we have ten departments, we will need ten router interfaces, which will cost us a lot of money.

VLANs allow us to divide one LAN into many VLANs. Every VLAN will have its own network IP, and it will work as a totally separated LAN, and will have all the options that exist to a regular LAN. In addition, all the VLANs can connect to only one router's interface, as seen in figure (16.4).

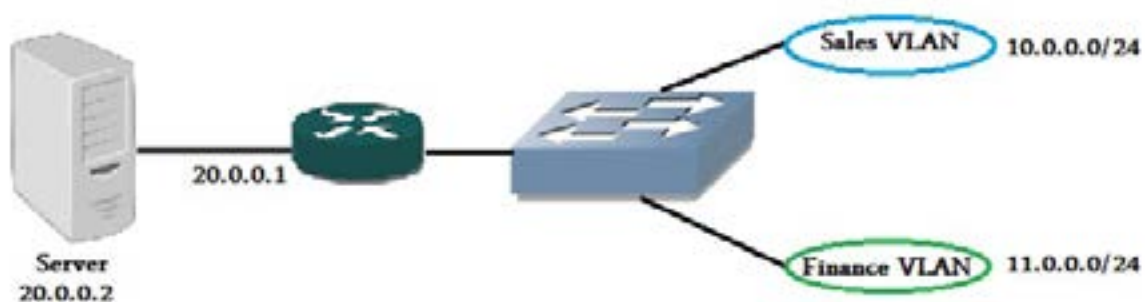


Figure 16.4: every department exists in its own VLAN

Therefore, VLANs enhance the network security by allowing us to put the computers of every department in its own VLAN.

16.1.3 VLANs enhance the management flexibility

VLANs allow the network administrator to put any computer in any VLAN, regardless of its physical location.

Suppose that our company has three floors and three departments, the sales, the finance and the HR.

We can configure the three VLANs, the sales VLAN, the finance VLAN and the HR VLAN, on every switch in every floor as seen in figure (16.5).

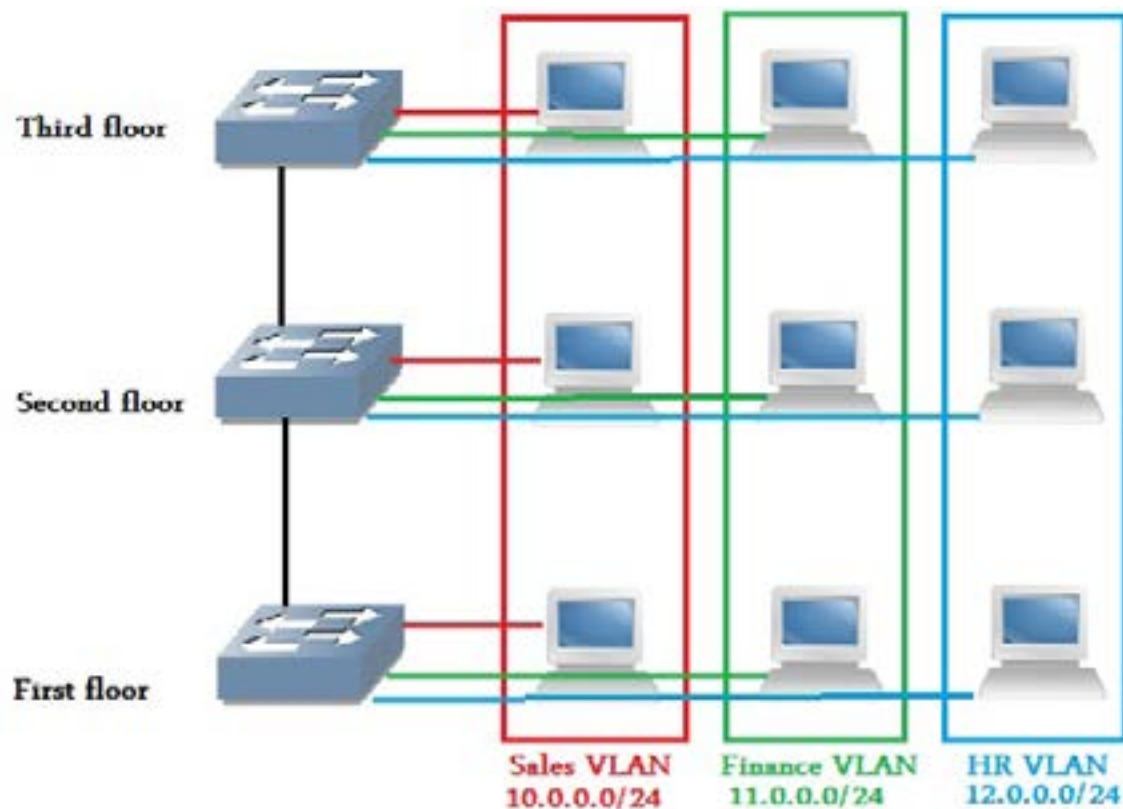


Figure 16.5: VLANs enhance the network management

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



Doing that will allow us to connect a sales computer to the 'sales' VLAN, regardless this computer exists in the first floor or in the second floor or in the third floor. This is also applicable to other department computers, which enhances the network management flexibility.

16.2 VLAN switch port membership

Every port in a switch can be assigned to a certain VLAN.

Static port

The administrator manually assigns the switch port to a certain VLAN.

Dynamic port

The port is automatically assigned to a certain VLAN, depending on the device attached to this port. This is done using a server that is called the 'VMPS' (VLAN Membership Policy Server).

Trunk port

The switch uses the trunk port to pass the frames from all the VLANs to another switch. This is done after tagging every frame with its VLAN number.

Generally, the trunk ports are used to connect between switches.

Suppose that we have two switches, every switch contains two VLANs (VLAN 1 and VLAN 2), as seen in figure (16.6).

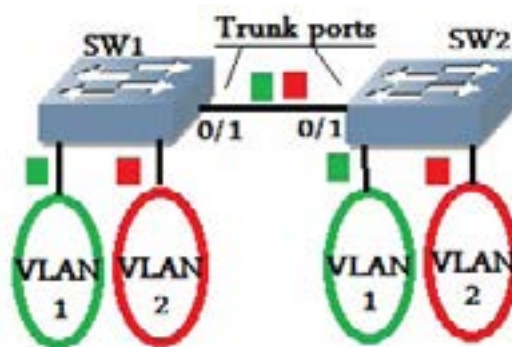


Figure 16.6: the trunk port

What happens if a computer in the 'VLAN 1' on the 'SW1' sends some data to a computer in the 'VLAN 1' on the 'SW2'?

The 'SW1' will tag the frames with the VLAN1's tagging.

Then, the 'SW1' will send the frames through its trunk port to reach the 'SW2'.

The 'SW2' will receive the frames, and it will find the VLAN1's tagging that exists on them.

Accordingly, the 'SW2' will pass those frames to 'VLAN1' ports. Therefore, it will reach the destination computer.

VLAN tagging methods:

There are two frame-tagging methods.

1. 'ISL' it is a Cisco proprietary method.
2. 'IEEE802.1Q'

The native VLAN

When a switch receives an untagged frame through its trunk port, it will consider it as it is belonging to its 'native VLAN'.

The default native VLAN is the 'VLAN 1'. However, the administrator can configure any VLAN on the switch to be the native VLAN.

16.3 Virtual LAN (VLAN) configuration

16.3.1 Configuring a VLAN on a switch

We can configure a VLAN on a switch using the following commands,

```
Sw(config)#vlan vlan_number
```

```
Sw(config-vlan)#name vlan_name
```

To view the VLAN information,

```
Sw#show vlan brief
```

VLANs information is stored in the VLAN database file (vlan.dat), which is stored in the switch's flash memory.

16.3.2 VLAN access port configuration

We can configure a switch port as an access port as following,

```
Sw(config)#interface port_number
```

```
Sw(config-if)#switchport mode access
```

```
Sw(config-if)#switchport access vlan vlan_number
```

16.3.3 VLAN trunk port configuration

We can configure a switch port as a trunk port as following,

```
Sw(config-if)#switchport mode trunk
```

```
Sw(config-if)#switchport trunk encapsulation { dot1q | isl | negotiate }
```

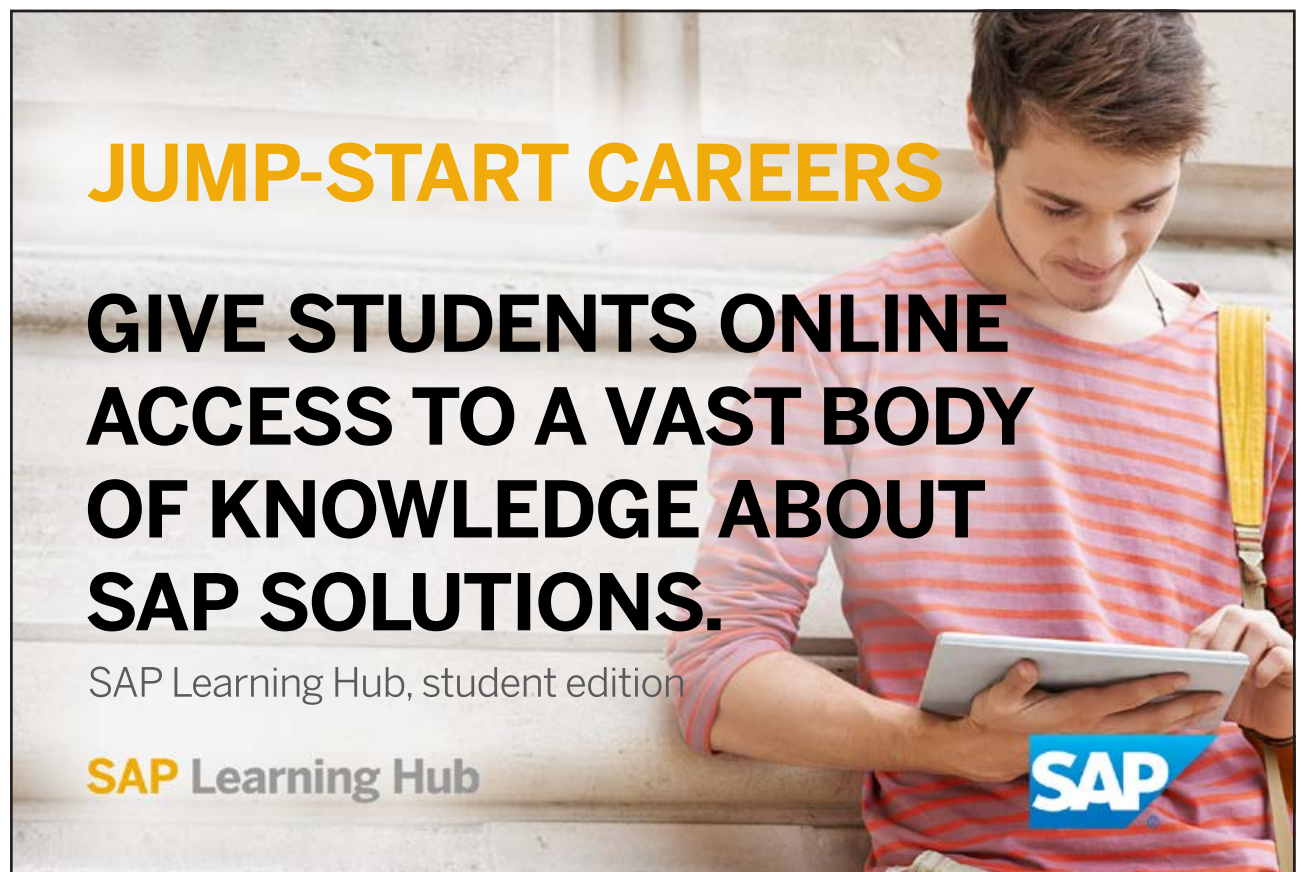
'Dot1q': to make the switch uses the 'IEEE802.1Q' to tag the frames.

'Isl': to make the switch uses the 'ISL' to tag the frames.

Negotiate: to negotiate the tagging method between the two switches.

The following command allows us to allow only certain VLANs to be able to pass through the trunk port. By default, all VLANs are allowed to pass through the trunk port.

```
Sw(config-if)#switchport trunk allowed vlan vlan numbers
```



JUMP-START CAREERS

**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub

SAP

Another way to configure the trunk port,

Suppose that we have two switches connected to each other as seen in figure (16.7).

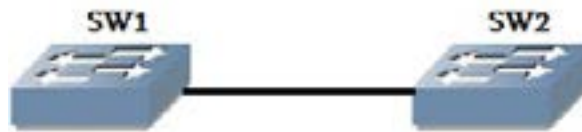


Figure 16.7: switches connected by a trunk port

We can use the following command on SW1,

```
Sw(config-if)#switchport mode dynamic { desirable | auto }
```

Desirable: means that the SW1's port will actively try to make the link between it and SW2 a trunk link.

Auto: the SW1 will passively accept to make the link a trunk link.

If we need to make the SW1's port never be a trunk port, we can use the following command,

```
Sw(config-if)#switchport nonegotiate
```

In this case, the SW1 will never convert this port to a trunk port.

16.4 Routing between VLANs

As you know, every VLAN has its own network IP. In addition, if we have two VLANs, we need a 'layer 3' device – a router – to route the data between those two VLANs.

We have two methods to route the data between the VLANs, the first one is the ordinary method, and the second one is called the 'router on a stick' method.

16.4.1 The ordinary routing method

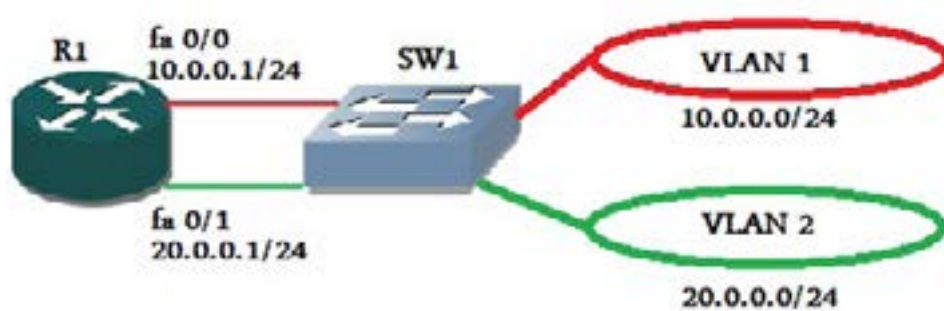


Figure 16.8: ordinary routing between the VLANs

In this method, we need a router's interface for every VLAN.

We assign an IP to the first router's interface (fa 0/0) that belongs to VLAN1. (IP = 10.0.0.1)

In addition, we assign an IP to the second router's interface (fa 0/1) that belongs to VLAN2. (IP = 20.0.0.1)

We connect one of the switch ports that belong to VLAN1 to 'fa 0/0'.

We connect one of the switch ports that belong to VLAN2 to 'fa 0/1'.

All VLAN1 devices should be assigned a default gateway IP address '10.0.0.1'.

All VLAN2 devices should be assigned a default gateway IP address '20.0.0.1'.

Therefore, the router now sees two direct connected networks that it can route between them.

The router configuration will be as following,

```
Router(config)#interface fa 0/0
```

```
Router(config-if)#ip address 10.0.0.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#interface fa 0/1
```

```
Router(config-if)#ip address 20.0.0.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

16.4.2 Router on a stick method

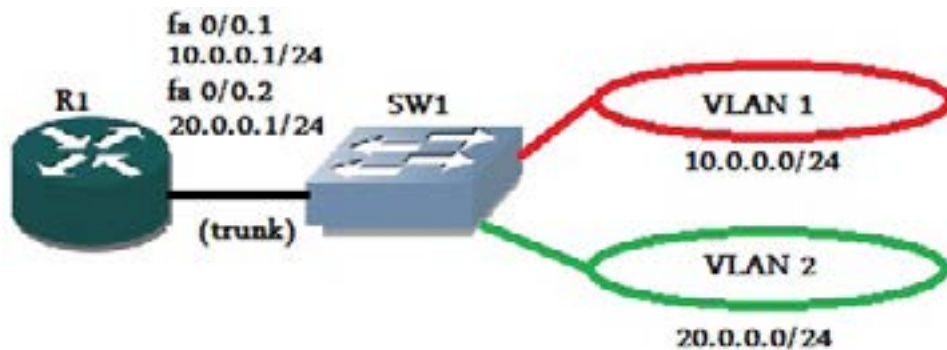


Figure 16.8: router on a stick method

In this method, we logically divide the router's interface 'fa0/0' into sub-interfaces 'fa0/0.1' and 'fa0/0.2'.

We assign an IP to the first sub-interface 'fa 0/0.1' that belongs to VLAN1. (IP = 10.0.0.1)

In addition, we assign an IP to the second sub-interface 'fa 0/0.2' that belongs to VLAN2. (IP = 20.0.0.1)

LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub

SAP

We configure a switch port as a trunk port and connect it to the router's interface.

All VLAN1 devices should be assigned a default gateway IP address '10.0.0.1'.

All VLAN2 devices should be assigned a default gateway IP address '20.0.0.1'.

Therefore, the router now sees two direct connected networks that it can route between them.

The router configuration will be as following,

```
Router(config)#interface fa 0/0
```

```
Router(config-if)#no ip address
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#interface fa 0/0.1
```

```
Router(config-subif)#encapsulation dot1q 1
```

(1 is the VLAN number)

```
Router(config-subif)#ip address 10.0.0.1 255.255.255.0
```

```
Router(config-subif)#interface fa 0/0.2
```

```
Router(config-subif)#encapsulation dot1q 2
```

(2 is the VLAN number)

```
Router(config-subif)#ip address 20.0.0.1 255.255.255.0
```

16.5 VLAN Trunking Protocol (VTP)

The VTP is used to maintain the consistency of the VLAN information between the switches that exist in the same VTP domain.

Suppose that we have many switches in our network, we can put all those switches in one VTP domain. Then, we do not need to configure our VLANs on all the switches, we can configure our VLANs only on one switch, the VTP server, and this VLAN information will propagate through all the switches in the VTP domain.

16.5.1 VTP modes

Every switch of the switches that exist in the VTP domain can be configured to work in one of the following VTP modes,

‘Server’ VTP mode

Switches working in the server mode propagate the VLAN information to other switches using the ‘VTP advertisements’. Every ‘VTP advertisement’ has a ‘VTP revision number’, which helps the other switches to determine if this ‘VTP advertisement’ is new or old.

In this mode,

- The VLAN information can be locally modified, we can connect to the switch that is working as the VTP sever, and change the VLANs configuration that exists on it.
- Once a change occurs in the VLAN database, the ‘VTP revision number’ is incremented by one, and a ‘VTP advertisement’ is sent to all the switches in the VTP domain.
- Every VTP domain must contain at least one VTP server.

‘Client’ VTP mode

Switches working in the client mode take its VLAN information from the switches that are working in the server mode.

In this mode,

- The VLAN information cannot be locally modified.
- The switch builds its VLAN information from the VTP advertisement received from the VTP server.

‘Transparent’ VTP mode

In this mode,

- Switches do not apply VLAN information received from the VTP server on itself.
- In VTPv2 (VTP version 2), switches working in the transparent mode forward the VTP information that received from the VTP server to the other switches.

16.5.2 VTP characteristics

- To communicate VLAN information between the switches, the 'VTP domain name', and the 'VTP Password' must be the same on all the VTP domain switches. In addition, at least one of the switches must work in the VTP server mode.
- VTP advertisements are sent only on the trunk links.
- VTP advertisement contains the 'VTP domain name' and the 'VTP revision number'.

16.5.3 VTP pruning

When the VTP pruning is enabled on a switch that exists in the VTP domain, the broadcasts are not forwarded to this switch unless there are ports in it that belong to the VLAN that the broadcast propagates in. By default, the VTP pruning is disabled on the switches.

Suppose that we have the network in figure (16.9), the broadcast should propagate in VLAN5. This is because that the computer that generated this broadcast exists in VLAN5.

The broadcast will propagate through SW1, SW2 and SW3, This is because that, those switches have ports that are belonging to VLAN5.

The broadcast will **not** propagate through SW5 and SW4, because those switches do not have ports that are belonging to VLAN5.



**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

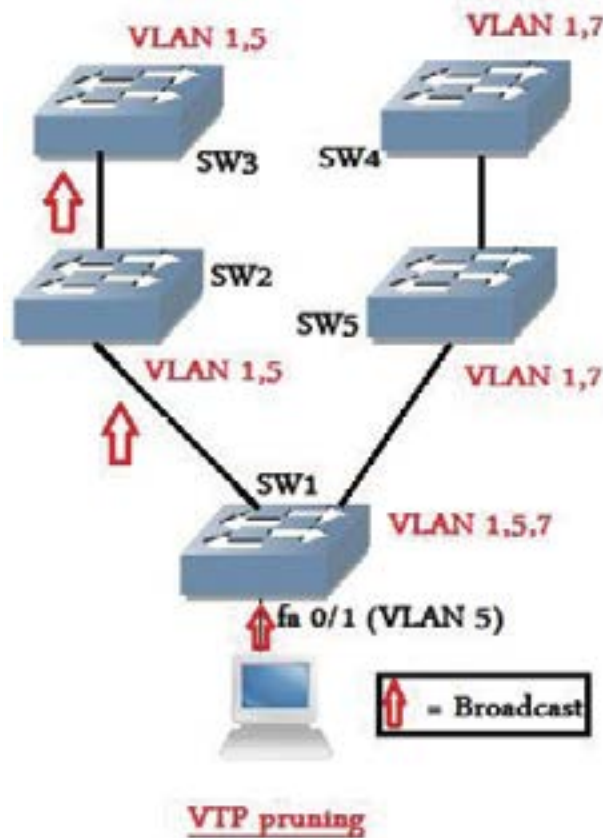


Figure 16.9: VTP pruning

16.5.4 VTP configuration

To configure VTP on a switch, we can use the following commands,

```
Switch(config)#vtp domain domain_name
```

```
Switch(config)#vtp password vtp_password
```

```
Switch(config)#vtp mode { server | client | transparent }
```

```
Switch(config)#vtp version 2
```

(to enable VTP version 2)

```
Switch(config)#vtp pruning
```

(to enable VTP pruning)

To view the VTP information, we can use the following command,
Switch#show vtp status

The default VTP configuration on the switches are,

VTP mode: server

VTP version: version 1

VTP pruning: disabled

A woman with dark hair, wearing a white blazer, is looking upwards and to the right while holding a large document or folder. The background is a bright, slightly blurred outdoor scene with a blue sky and white clouds. The text is overlaid on the left side of the image.

ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

Hour 17: Spanning Tree Protocol (STP)

To avoid any loops in a switched network, we use the STP (Spanning Tree Protocol). This is done by blocking the traffic on all the redundant links.

Loops in a switched network will cause a 'broadcast storm', which will destroy the network performance by consuming the entire network bandwidth.

Broadcast storm

In the following network, suppose that 'computer A' sent a broadcast,

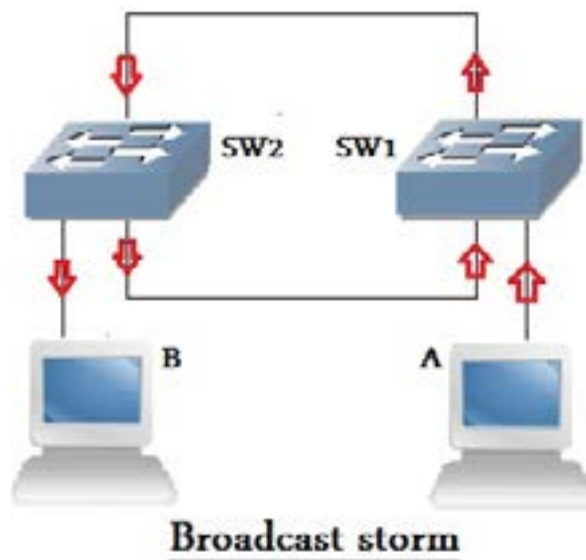


Figure 17.1: a broadcast storm

When 'computer A' sends a broadcast frame, the switch will forward it through all of its ports. Therefore, it will reach SW2 through the two links that connects SW2 with SW1. Then, SW2 will flood the broadcast frame out of all its ports. Therefore, it will reach SW1 through the two links that connects it with SW2... we have a broadcast storm.

STP will simply block traffic on one of the two links that connect between the SW1 and the SW2, which will prevent the broadcast storm.

STP terms

We have to understand the following terms in order to be able to understand the operation of the STP.

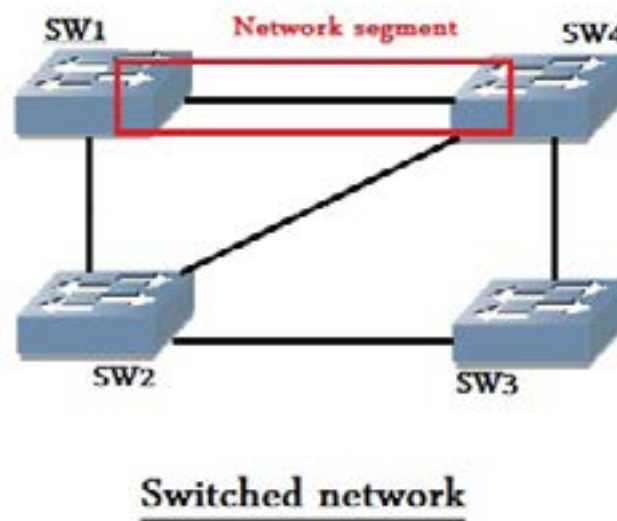


Figure 17.2: a switched network

BPDU (Bridge Protocol Data Unit): switches running the STP send the BPDU frames every regular interval. This is done to exchange the information with other switches.

Bridge ID (BID): the BID is a combination of the switch priority and the switch MAC address.

'BID = SW priority.SW MAC address'

The default switch priority = 32768 (which equals to the hexadecimal number 0x8000).

The administrator can manually configure the switch priority using the following command,

```
Switch(config)#spanning-tree vlan 1 priority SW priority
```

Port ID: every switch port has a port ID.

The port ID is a combination of the port priority and the port number.

'Port ID = port priority.port number'

The port priority can be a number in the range '0:255'.

The default port priority = 128

Link cost: It is a value given to every link depending on its bandwidth (BW).

BW	Cost
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

Table 17.1: the link cost

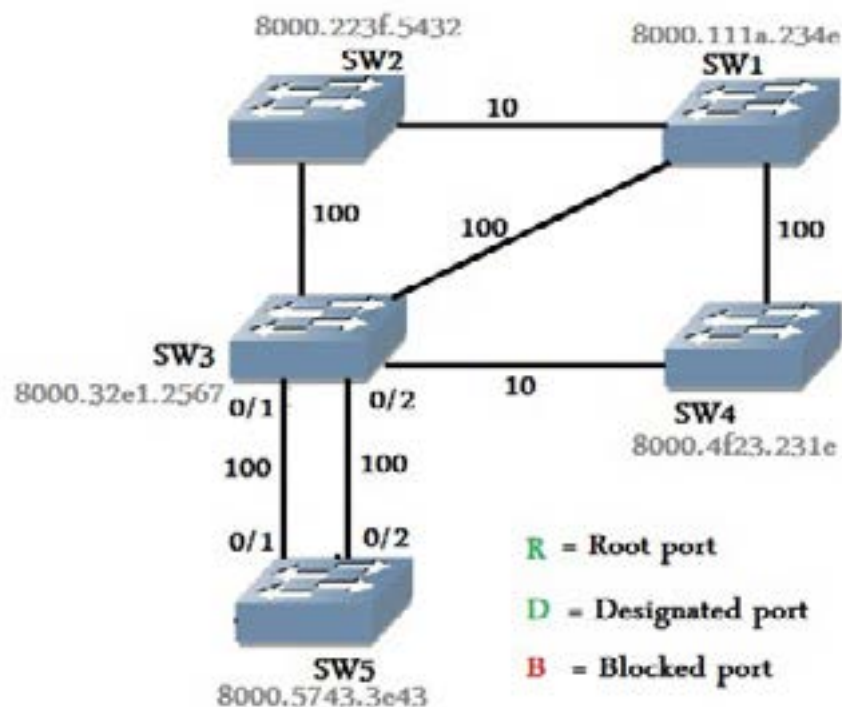
Root Bridge: the root Bridge is the switch that has the lowest bridge ID (BID) in the switched network.

Root port: the root port is the port that has the shortest path (least cost path) to the root bridge.

Designated port: the designated port is the port that has the shortest path (least cost path) to the root bridge in every network segment.

17.1 STP operation

To learn the operation of the STP, suppose that we have the network in figure(17.3).

**Figure 17.3:** STP operation

In figure (17.3), every switch has its BID written on it, and every link has its BW in Mbps written on it.

The following is the operation of the STP to remove all redundant links,

1. The switch with the lowest BID is elected as the 'Root Bridge', and all ports in this switch are considered 'designated ports', as seen in figure (17.4).

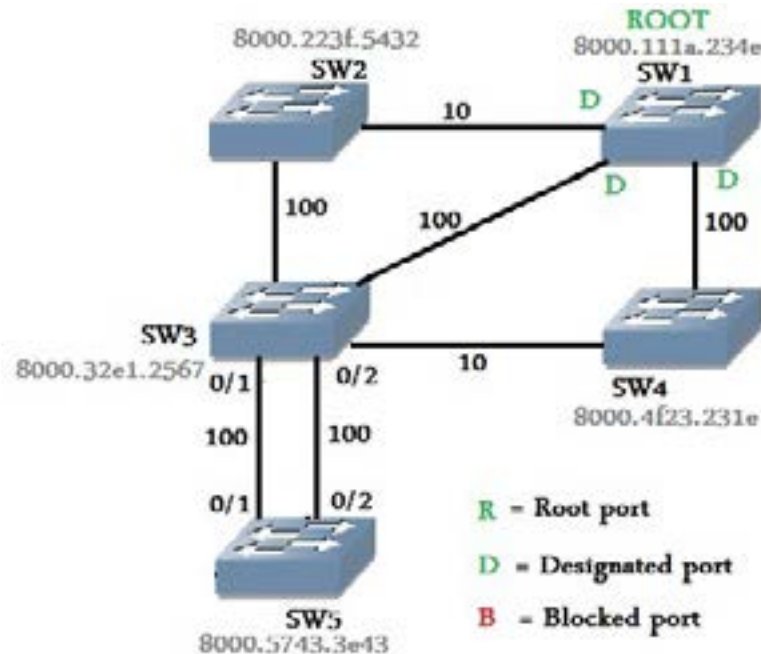


Figure 17.4: STP operation

NO-LIMITS LEARNING

LEVERAGE SOCIAL LEARNING, COLLABORATION, QUALITY CONTENT, AND HANDS-ON PRACTICE.

SAP Learning Hub



2. Every switch elects its '**root port**' by finding the port that has the least cost to the root bridge, as seen in figure (17.5).

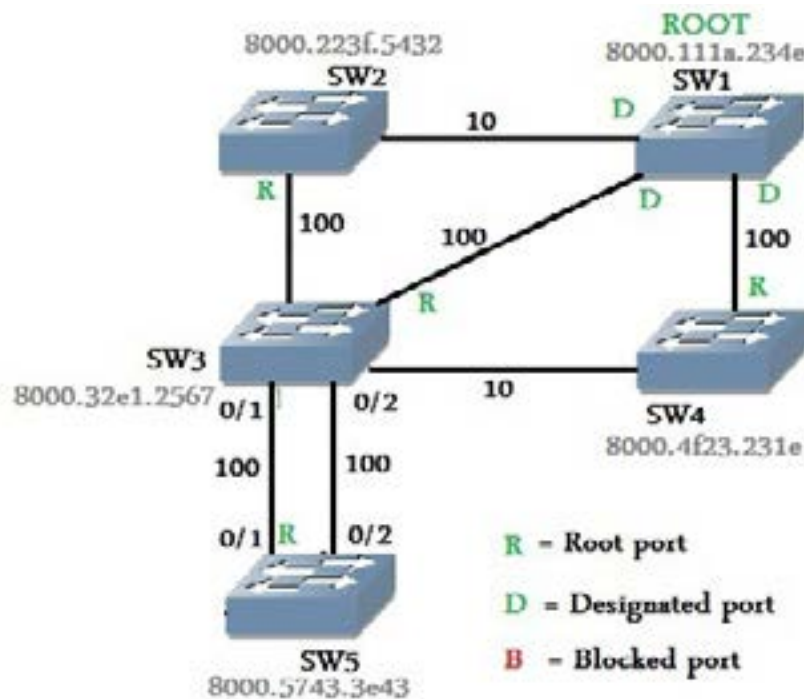


Figure 17.5: STP operation

3. Port with the least cost path to the root bridge in every network segment is elected as a '**Designated port**', as seen In figure (17.6).

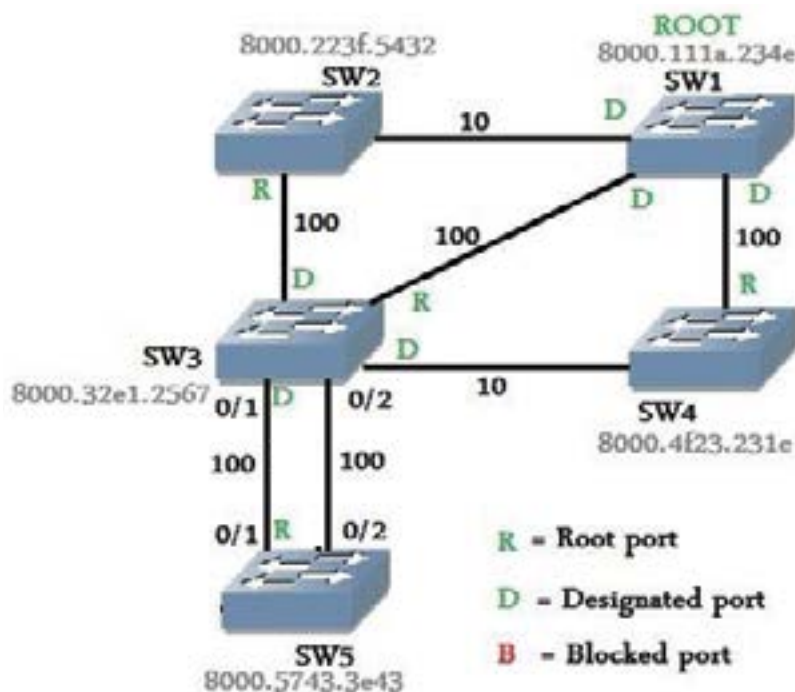


Figure 17.6: STP operation

4. All non-root and non-designated ports are put in the 'blocking state', where it does not forward any frames, as seen in figure (17.7).

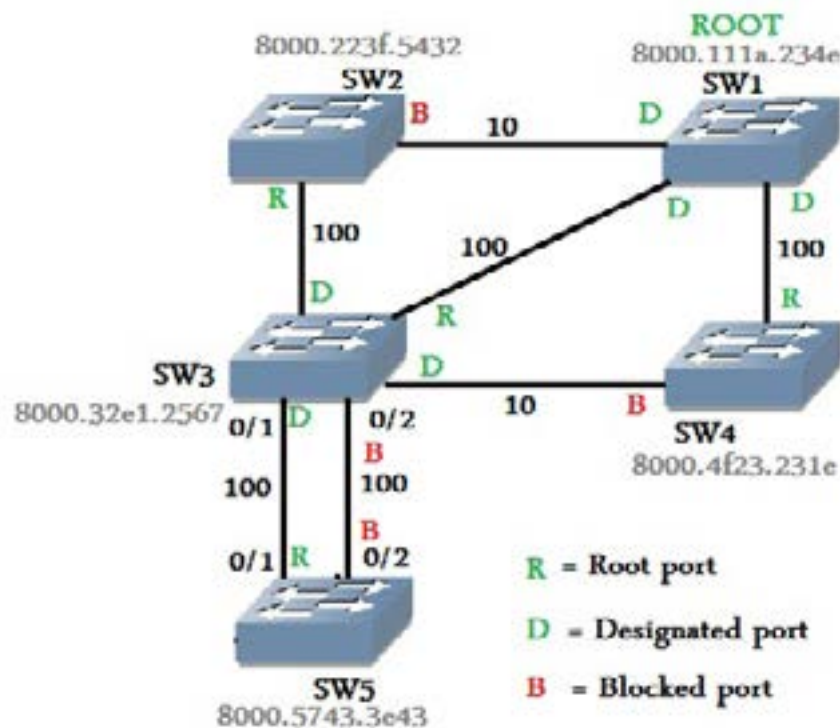


Figure 17.7: STP operation

Now, the STP has removed all the redundant links that exist in the switched network.

Election criteria for the 'root ports' and the 'designated ports'

The election criteria are the port that has the lowest cost path to the root bridge.

If the costs are equal, the port that exists in the switch that has lowest BID.

If the BIDs are equal, the port that has the lowest PID.

You can view the STP statistics using the following command,

```
Switch#show spanning-tree
```

17.2 STP port states

The ports in the STP protocol may exist in one of the following states; the blocking state, the listening state, the learning state, and the forwarding state.

17.2.1 'Blocking' state

In this state, the port does not forward any frames; it only receives BPDUs.

If the port that is in the 'blocking state' did not receive any BPDU during the 'maximum age time', which by default equals to 20 sec., the port will enter to the 'listening state'.

17.2.2 'Listening' state

In this state, the port does not forward any frames; it only receives BPDUs to determine the port role in the STP.

The port will remain in the 'listening state' for a 'forward delay time', which by default equals to 15 sec., and then the port will enter to the 'learning state'.

17.2.3 'Learning' state

In this state, the port does not forward any frames; it receives BPDUs to learn all the network paths.

The port will remain in the 'learning state' for a 'forward delay time', which by default equals to 15 sec., and then it will enter to the 'forwarding state'.

An advertisement for SAP Learning Hub. The background is a blurred image of a person holding a tablet. The text is overlaid on the image. The top part says "THE ANSWER TO YOUR LEARNING NEEDS" in large, bold, yellow capital letters. Below that, in large, bold, black capital letters, it says "GET QUALITY, FLEXIBLE, AND ECONOMICAL TRAINING WHEN AND WHERE IT'S NEEDED." At the bottom left, the "SAP Learning Hub" logo is displayed, with "SAP" in yellow and "Learning Hub" in grey. At the bottom right, the "SAP" logo is displayed in blue with a white "S" and a registered trademark symbol.

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub

SAP

17.2.4 'Forwarding' state

In this state, the port forwards and receives all the frames.

Generally, in the STP, the port may stay only in the 'blocking state' or in the 'forwarding state'.

The 'listening state' and the 'forwarding state' are transient states between the 'blocking state' and the 'forwarding state'.

STP convergence time

It is the time consumed until all of the ports are either in a 'blocking state' or in a 'forwarding state'.

As you can observe, the time consumed for a port to transit from the 'blocking state' to the 'forwarding state' is a long time, (max age time '20sec.' + forward delay time '15 sec.' + forward delay time '15 sec.'). Therefore, the port may need about 50 sec. to transit from the 'blocking state' to the 'forwarding state', which is a very long time. This problem may affect the network stability.

The solutions for this long time problem are developed. Those solutions will be discussed in the following points ('port fast' and 'rapid STP').

17.3 STP port fast

The 'STP port fast' is used to speed up the convergence time on certain ports. This is used when the network administrator is sure that this port will not form any switching loop, as an example, the ports that are connected to an end device.

The 'STP port fast' allows the port to transit directly from the 'blocking state' to the 'forwarding state' without passing through the 'listening state' and the 'learning state', which reduces the transit time.

17.3.1 Port fast configuration

Suppose that we have the network in figure (17.8),

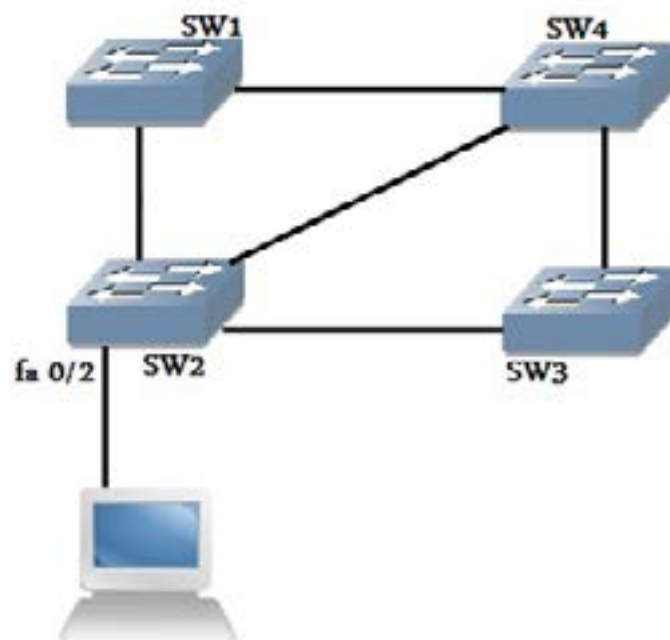


Figure 17.8: STP port fast

The network administrator may configure the 'STP port fast' on 'fa0/2' on 'SW2'. This is because that, this port is connected to an end device.

To configure the port fast, we use the following commands,

```
Switch(config)#interface interface number
```

```
Switch(config-if)#spanning-tree portfast
```

17.3.2 Features recommended to be used on ports that have 'STP port fast' enabled

BPDU guard

If a BPDU is received on the port that has the 'STP port fast' enabled, the 'BPDU guard' puts this port in the 'error disabled' state.

This is because of that, if there is any BPDU received on a port, this means that this port is connected to another switch; hence, this port may form a loop.

BPDU filter

If a BPDU is received on the port that has the 'STP port fast' enabled, the 'BPDU filter' takes the port out of the 'STP port fast' and forces it to be a part of the STP topology.

This is because of that, if there is any BPDU received on a port, this means that this port is connected to another switch and this port may form a loop.

17.4 'RSTP', 'PVSTP+' and 'PVRST+'

17.4.1 'RSTP' (Rapid STP)

The RSTP, which is the 'IEEE802.1w' protocol, speeds up the convergence time. This means that a switch that is running RSTP has a faster convergence time than a switch that is running STP.

RSTP do the following,

It designates an 'alternative port', which is considered an alternative to the 'root port' on every switch. This is done in order to use this alternative port when the 'root port' is unavailable.

Designating a 'backup port' for the 'designated port' in order that when the 'designated port' is down for any reason, this 'backup port' becomes the 'designated port'.

The switches that are running the RSTP can work with the switches that are running the STP. This is because of that, the RSTP is compatible with the STP.



MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub

SAP

RSTP port states

The ports that exist in a switch that is running the RSTP may be in one of the following states,

Discarding: all incoming frames are dropped.

Learning: do not forward any frames. Only receive BPDUs to learn the network paths.

Forwarding: forward and receive all the frames.

RSTP configuration

To configure the RSTP on a switch, we use the following command,

```
Switch(config)#spanning-tree mode rapid-pvst
```

17.4.2 'PVSTP+' (Per-VLAN STP+)

In the ordinary STP, the entire switched network has only one STP instance.

In the PVSTP+, every VLAN in a switched network has its own STP instance.

Suppose that we have the network in figure (17.9),

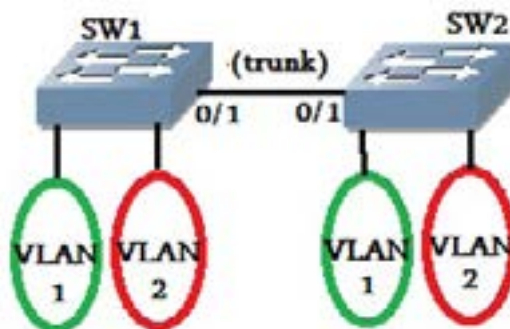


Figure 17.9: Per-VLAN STP+

Using the PVSTP+, VLAN1 will have its own STP instance, and VLAN2 will have its own STP instance.

- PVSTP+ is enabled by default on the switches that are running the STP.
- PVSTP+ uses the 'Extended BID' instead of the 'BID', which was in the STP.

'Extended BID = Switch priority.VLAN ID (VID).MAC address'

17.4.3 'PVRST+' (Per-VLAN RSTP+)

In the PVRST+, every VLAN in a switched network has its own RSTP instance.

Suppose that we have the network in figure (17.10),

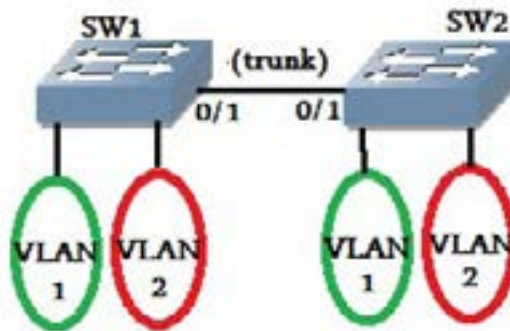


Figure 17.10: Per-VLAN RSTP+

Using the PVRST+, VLAN1 will have its own RSTP instance, and VLAN2 will have its own RSTP instance.

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



Part 3

ADVANCED TOPICS

Hour 18:Security

18.1 Security threats

There are many security threats that can affect our network, and the network administrator must be aware of how to prevent those security threats from harming the network.

Some kinds of the security threats are listed below,

DOS (Denial of service) and DDoS (Distributed Denial of service) attacks

The attacker floods the network servers with a huge stream of traffic, this traffic may be ping requests or any other kind of requests that keep the server busy with a huge number of junk work, which dramatically slow the network performance, and may bring it down.

Man-in-the-middle attack

The attacker convinces the two parties of the communication that he is the other party. If two nodes (node_A, node_B) are communicating with each other, the attacker convinces node_A that he is node_B, and convinces node_B that he is node_A. Therefore, the attacker is able to see all the communication between the two nodes, and he is able to inject faked packets in the communication between them.

IP spoofing

The attacker pretends that he has an IP address that differs from its real IP address. This pretended IP address may be an address of a source device that the network trusts of, or any other address that allow the attacker to gain unauthorized rights.

Packet sniffers

It is a program that can capture the network traffic and analyze it. An attacker can use a packet sniffer program in order to capture the network traffic that is not intended to be sent to him, and to know the information that he should not know.

Password attacks

The attacker tries to get an account password to pretend that he is an authorized person. He may get the password by guessing it, by using trial and error, or by claiming that he forgot the password, or any other mean that may cheat the system.

Brute force attacks

The attacker tries to decrypt the encrypted data using several methods. By decrypting the encrypted data, he may know sensitive information, passwords, and many other sensitive data that he should not know.

Virus

The virus is a malicious program that can harm the computers. It can reach the computer through the internet, removable mediums, or any other way.

Trojan horse

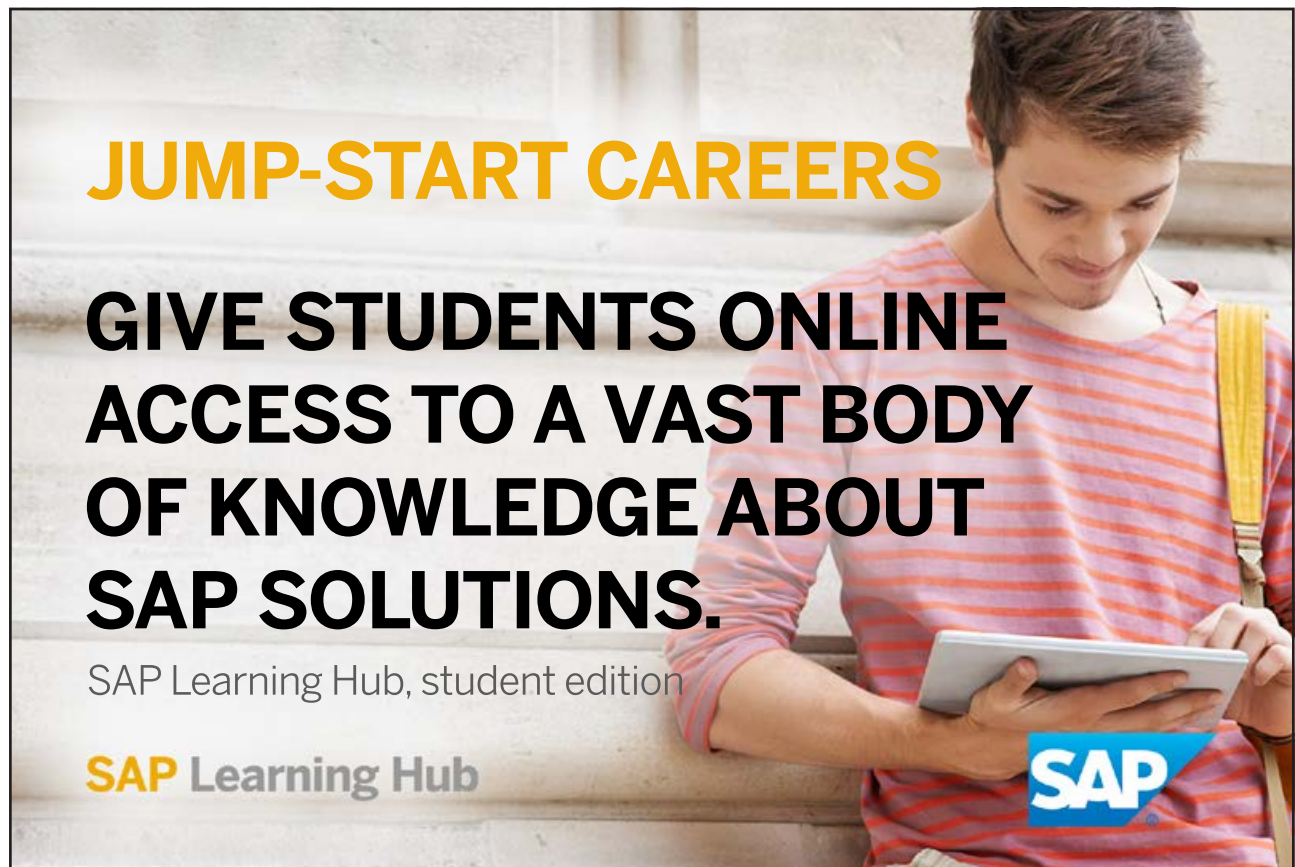
Trojan horse is a program that pretends to be an innocent program that provides you with a certain function. However, this program has a malicious code that can badly harm the computers.

18.2 Security threats mitigation

The network administrator can use appliances and applications that can be installed on his network in order to mitigate the security threats that may affect his network.

Firewall

It may be a device that is installed in the network, or it may be software that is installed on the end devices.



JUMP-START CAREERS

**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub

SAP

The firewall protects the network from unauthorized access that may come from outside the network. It controls the communication between the network and the external world to allow only authorized communications to pass through it.

IDS (Intrusion Detection System)

A device or software, it detects malicious activities and alerts the network administrator with them.

IPS (Intrusion Prevention System)

It is a device or software that detects and prevents the malicious activities, and alerts the network administrator with them.

Antivirus

It is a program that detects and removes the malicious programs.

Antispyware

A program that detects and removes spyware programs, which collects personal information from the computer.

18.3 Access Control List (ACL)

Access control list (ACL) is a powerful tool that enables network administrators to control the traffic in their network. Using ACLs, a network administrator can authorize certain networks to be able to access certain resources.

Suppose that we have the network:

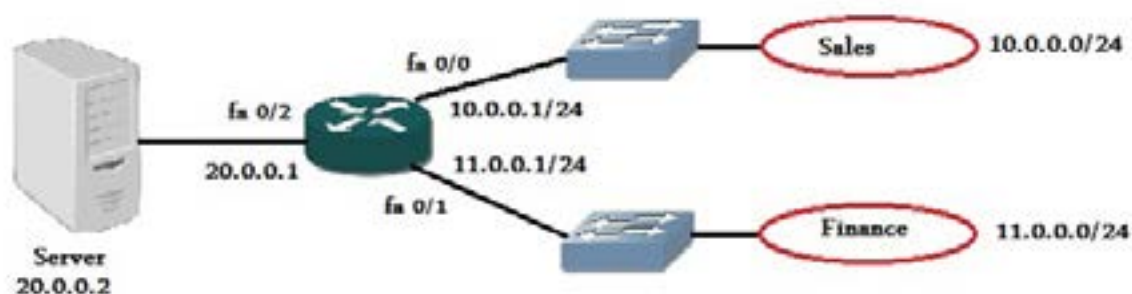


Figure 18.1

By using ACLs, the network administrator can authorize the 'sales' network computers to access the server, while preventing the 'finance' network computers from accessing the same server. Over that, the network administrator can determine exactly which protocols on the server may be accessed from the 'sales' network computers.

18.3.1 Standard access list

Every ACL should have a unique number. Standard ACLs number can be from (1: 99).

Standard ACLs use only the source IP address to determine if a certain packet is allowed, or is not allowed to access the resource.

To configure an ACL we use the following command,

```
Router(config)#access-list ACL number {deny | permit} source IP wild card mask
```

To apply an ACL to router's interface, we use the following command,

```
Router(config-if)#ip access-group ACL number {in | out}
```

(in/out is the direction the ACL should be applied to)

In figure (18.1), suppose that we need to configure the router in order to prevent the packets that come from the 'finance' network (11.0.0.0 255.255.255.0) from accessing the server, while allowing the packets with any other source IP address.

The following commands show how to configure the ACL, and how to apply it on the router's interface,

```
Router(config)#access-list 1 deny 11.0.0.0 0.0.0.255
```

(if the denied IP is only one IP address (e.g. 11.0.0.1), we can write **host 11.0.0.1** instead of **11.0.0.1 0.0.0.0**)

```
Router(config)#access-list 1 permit any
```

(**any** means any IP address. Instead, we can write, **0.0.0.0 255.255.255.255**)

To apply the configured ACL on a certain interface,

```
Router(config)#interface fa 0/2
```

```
Router(config-if)#ip access-group 1 out
```

(**out** means that this ACL will be applied on packets that exit from the interface fa 0/2)

Note that in ACLs, the router will match the packet with every configured rule, respectively from the first rule to last rule. If a certain match found for the packet, it will be applied. If no match is found, the packet will be denied.

Therefore, it is very important to write the rule (access-list ACL number permit any) as the last rule in the access list. This is done in order to allow any unrestricted packets.

18.3.2 Extended access list

Every ACL should have a unique number. Extended ACLs number can be from (100: 199).

Extended access list can use a source IP address, a destination IP address, a protocol and port numbers to determine if a certain packet is allowed or not allowed.



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub



To configure the extended ACL, we use the following command,

```
Router(config)#access-list ACL number protocol source IP wild card mask destination  
IP wild card mask eq { the port number | the protocol name}
```

ACL number: from 100 to 199

Protocol: may be TCP, UDP or IP

Source IP: the source IP address

Wild card mask: the wild card mask of the source IP address

Destination IP: the destination IP address

Wild card mask: the wild card mask of the destination IP address

The port number or the protocol name: the port number of the protocol, or in case that it is a well-known port number, we can write the protocol name. As an example, if the port number is 23, I can write the protocol name **telnet** instead of the port number.

To apply the ACL to the router's interface, we use the following command,

```
Router(config-if)#ip access-group ACL number {in | out}
```

(**in/out** is the direction the ACL should be applied to)

18.3.3 Case study

In figure (18.1), suppose that the network administrator needs to allow only the 'sales' network computers to access the server, only using the **telnet protocol**, taking into consideration that the telnet uses the port number 23.

The administrator will configure the router using the following commands,

```
Router(config)#access-list 101 permit tcp 10.0.0.0 0.0.0.255 20.0.0.2 0.0.0.0 eq 23
```

```
Router(config)#interface fa 0/2
```

```
Router(config-if)#ip access-group 101 out
```

Note that, in this case study, we did not write the explicit permit condition (access-list ACL number permit ip any any) as the last rule in the ACL. This is because that we need every packet that does not our rules to be denied.

In case that we need to permit every packet that do not match any of ACL rules, we should write the explicit permit rule (access-list ACL number permit ip any any) as the last rule in the ACL.

18.4 NAT (Network Address Translation)

NAT is the process of changing the source IP address of the packet while sending it through a 'layer 3' device such as a router.

NAT is developed and used because the IP addresses in the world are about to be drained.

18.4.1 Private IP vs. public (real) IP

NAT divided the IP addresses into two types:

1. Private IP addresses
2. Public IP addresses

The private IP addresses are the addresses in the following ranges,

10.0.0.0 : 10.255.255.255

172.16.0.0 : 172.31.255.255

192.168.0.0 : 192.168.255.255



**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

Any other IP address is a public IP address.

The 'public IP' may be called the 'real IP' or the 'global IP'.

The 'private IP' may be called the 'virtual IP' or the 'local IP'.

In the NAT configuration, we can assign a private IP address to any device that does not exist on the internet. While any device that exist on the internet should be assigned a public IP address.

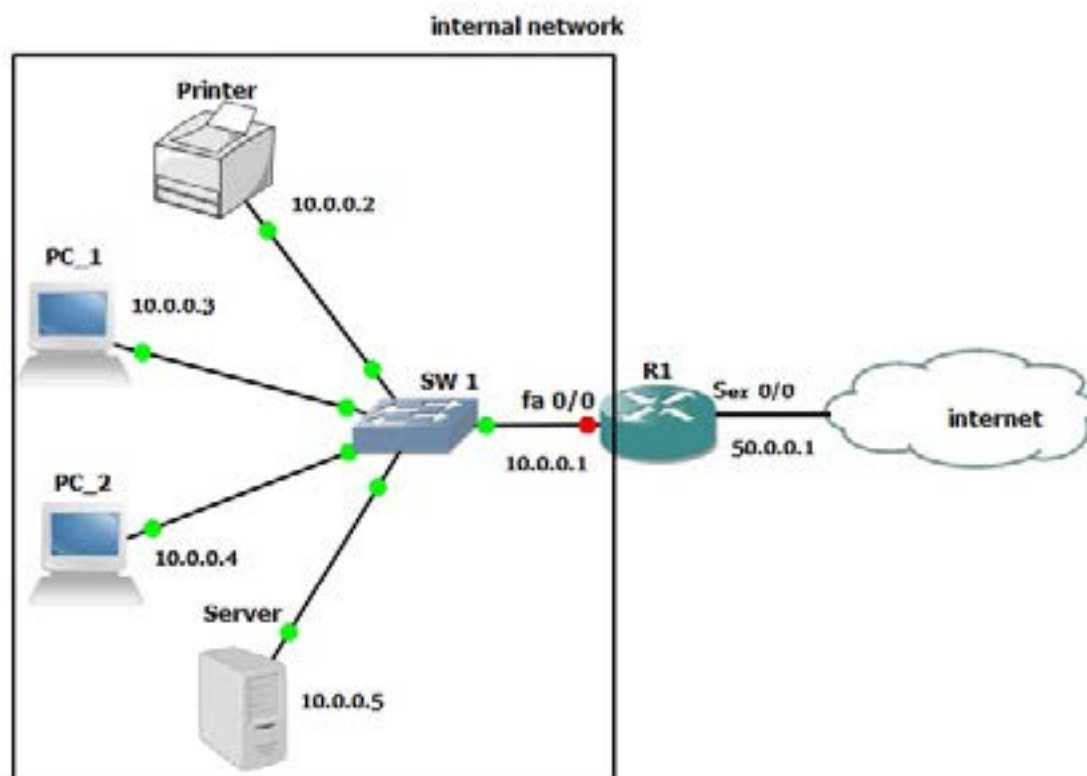


Figure 18.2

In figure (18.2), a 'private IP address' should be assigned to all the devices that exist in the internal network like, PC_1, PC_2, the printer, the server, and the internal router's interface fa 0/0.

However, a 'public IP address' should be assigned to all the devices that exist on the internet like the external router's interface ser 0/0.

Our deduction is that, any interface or device that should be accessible from the internet is assigned a public IP address. While any device or interface that should not be accessible from the internet is assigned a private IP address.

18.4.2 How NAT works?

In figure (18.2), when an internal device needs to communicate with a device that exists on the internet (like a web server), the internal device will send the packets to the router's interface 'fa 0/0'. Then, the router will change the source IP address that exists in the packet to a public IP address, and then send the packet to the web server, so that when the web server needs to reply to the packet, it will send the reply to this public IP address. Then the router will send the reply to the internal device.

18.5 Static NAT, dynamic NAT and PAT

18.5.1 Static NAT

In the static NAT, every private IP address is statically mapped to a public IP address.

The network administrator statically configures the router to change every private IP address to a certain public IP address.

Case study

In figure (18.3), suppose that PC_1 needs to communicate with a web server on the internet,

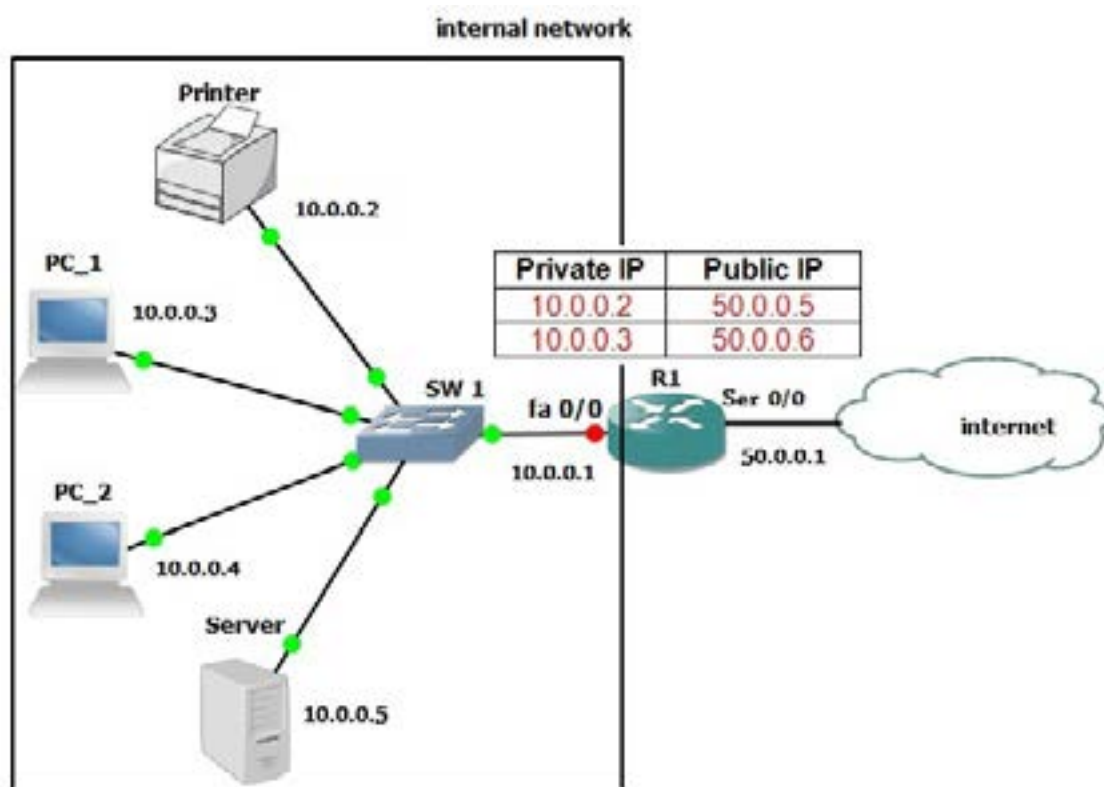


Figure 18.3

The router will change the source IP address in the packets that comes from the PC_1. It will set the source IP address in the packets to '50.0.0.6' instead of '10.0.0.3'.

Therefore, when the web server needs to reply to PC_1, it will reply to '50.0.0.6', and then the router will forward this reply to PC_1.

Static NAT configuration

To configure the static NAT on a router, we use the following command,

```
Router(config)#ip nat inside source static private IP public IP
```

To configure NAT in the network in figure (18.3),

```
Router(config)#ip nat inside source static 10.0.0.2 50.0.0.5
```

```
Router(config)#ip nat inside source static 10.0.0.3 50.0.0.6
```

```
Router(config)#interface fa 0/0
```

```
Router(config-if)#ip nat inside
```



ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

(This means that NAT configuration will be applied to the packets of the internal network through this interface).

```
Router(config-if)#interface ser 0/0
```

```
Router(config-if)#ip nat outside
```

(This means that NAT configuration will be applied to the packets of the external network through this interface).

18.5.2 Dynamic NAT

In the dynamic NAT, the network administrator configures an IP pool on the router. This pool contains a range of public IPs that should be used in the NAT process.

Dynamic NAT configuration

We use the following command to configure the dynamic NAT,

```
Router(config)#ip nat inside source list ACL number pool pool name
```

To configure the network that exist in figure (18.3) to use the dynamic NAT, we use the following commands,

```
Router(config)#access-list 1 permit 10.0.0.0 255.255.255.0
```

(Configures Access list that contains private IPs that NAT should be applied on).

```
Router(config)#ip nat pool abc 50.0.0.2 50.0.0.6 netmask 255.255.255.0
```

(Configures a pool of public IPs that contain 5 IPs).

```
Router(config)#ip nat inside source list 1 pool abc
```

(Configures the NAT operation between the private IPs that contained in the 'access-list 1' and the public IPs that contained in the pool 'abc').

```
Router(config)#interface fa 0/0
```

```
Router(config-if)#ip nat inside
```

(This means that the NAT configuration will be applied to the packets of the internal network through this interface).

```
Router(config-if)#interface ser 0/0
```

```
Router(config-if)#ip nat outside
```

(This means that the NAT configuration will be applied to the packets of the external network through this interface).

18.5.3 PAT Port Address Translation

It is also known as 'overloading' or 'many to one NAT'. In this NAT type, we can map any number of private IP addresses to only one public IP address.

Therefore, PAT reserves the number of the public IP addresses used in the network. In addition, it is the most widely used technique.

PAT maps many private IPs to only one public IP by using the port addresses as following,



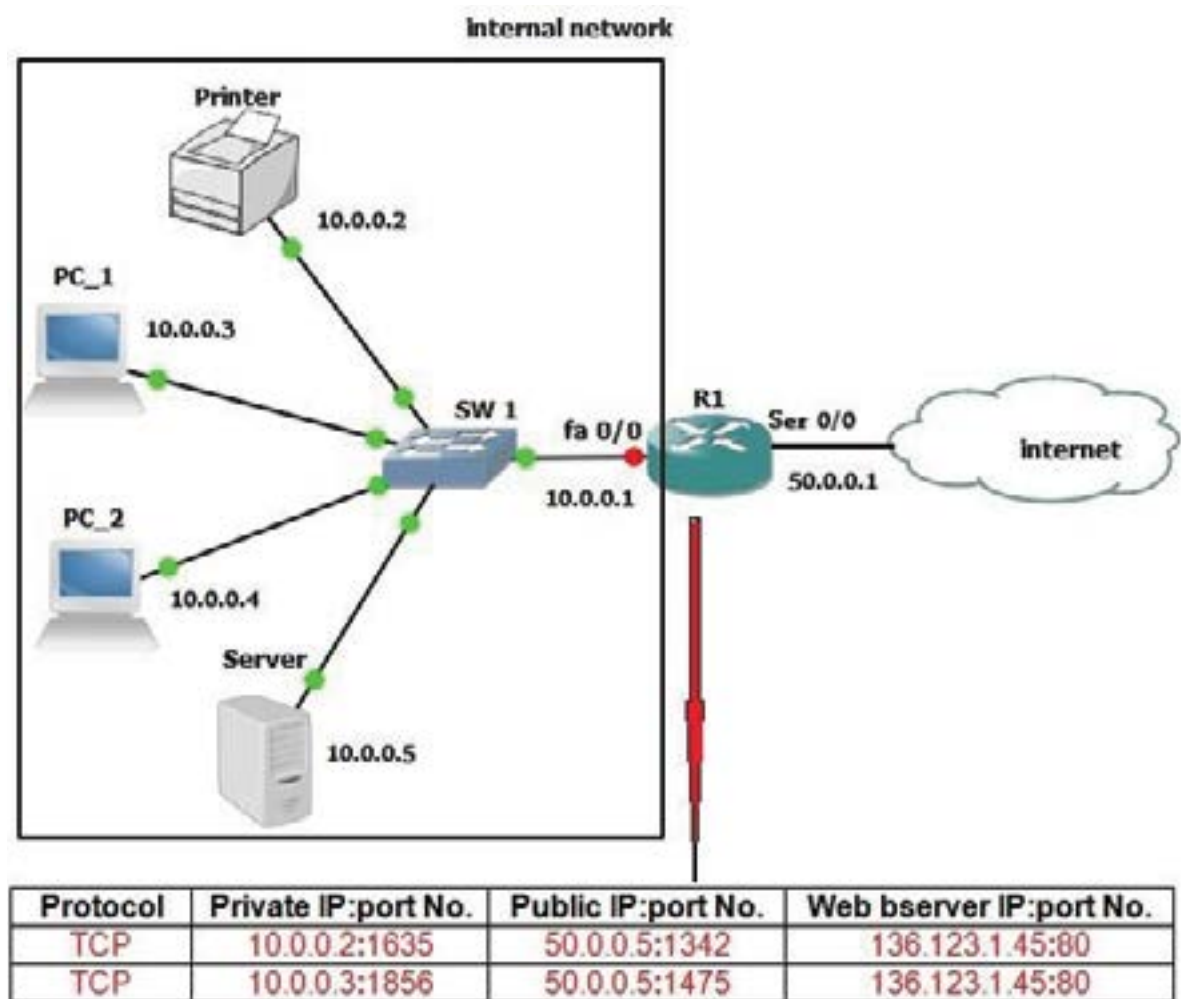


Figure 18.4

In figure (18.4), suppose that PC_1 and PC_2 need to communicate with a web server that exists on the internet, and it has an IP address of '136.123.1.45'.

The router will map both PC_1 and PC_2 IPs to only one public IP '50.0.0.5'.

However, the router will give a different source port number to the packets of every session of the two sessions.

As seen in figure (18.4), the router will give a source port number '1342' to the packets of the PC_1's session with the web server.

In addition, the router will give a source port number '1475' to the packets of the PC_2's session with the web server.

Therefore, when the web server replies to the router, the router will know the required internal destination by looking at the destination port number.

If the destination port number is '1342', the router will forward the packets to PC_1.

If the destination port number is '1475', the router will forward the packets to PC_2.

The advantage of the PAT is that, all the internal devices can access the internet using only on public IP address.

PAT configuration

To configure the network in figure (18.4), we use the following commands,

```
Router(config)#access-list 1 permit 10.0.0.0 255.255.255.0
```

(Configures Access list that contains private IPs that NAT should be applied on)

```
Router(config)#ip nat pool abc 50.0.0.2 50.0.0.2 netmask 255.255.255.0
```

(Configures a pool of public IPs that contain only **one** IP, it may be any number of IPs)

```
Router(config)#ip nat inside source list 1 pool abc
```

(Configures NAT operation between the private IPs that contained in access-list 1 and public IPs that contained in pool abc)

```
Router(config)#interface fa 0/0
```

```
Router(config-if)#ip nat inside
```

(This means that NAT configuration will be applied to packets of the internal network through this interface)

```
Router(config-if)#interface ser 0/0
```

```
Router(config-if)#ip nat outside
```

(This means that NAT configuration will be applied to packets of the external network through this interface)

Hour 19: Wide Area Networks (WAN)

19.1 Wide Area Network (WAN) basics

- The WAN is a network that extends over a wide geographical area.
- Generally, the WAN networks are used to connect between several LANs of a certain company.
- The company does not own the WAN, but it always takes the WAN from a 'Service Provider'.

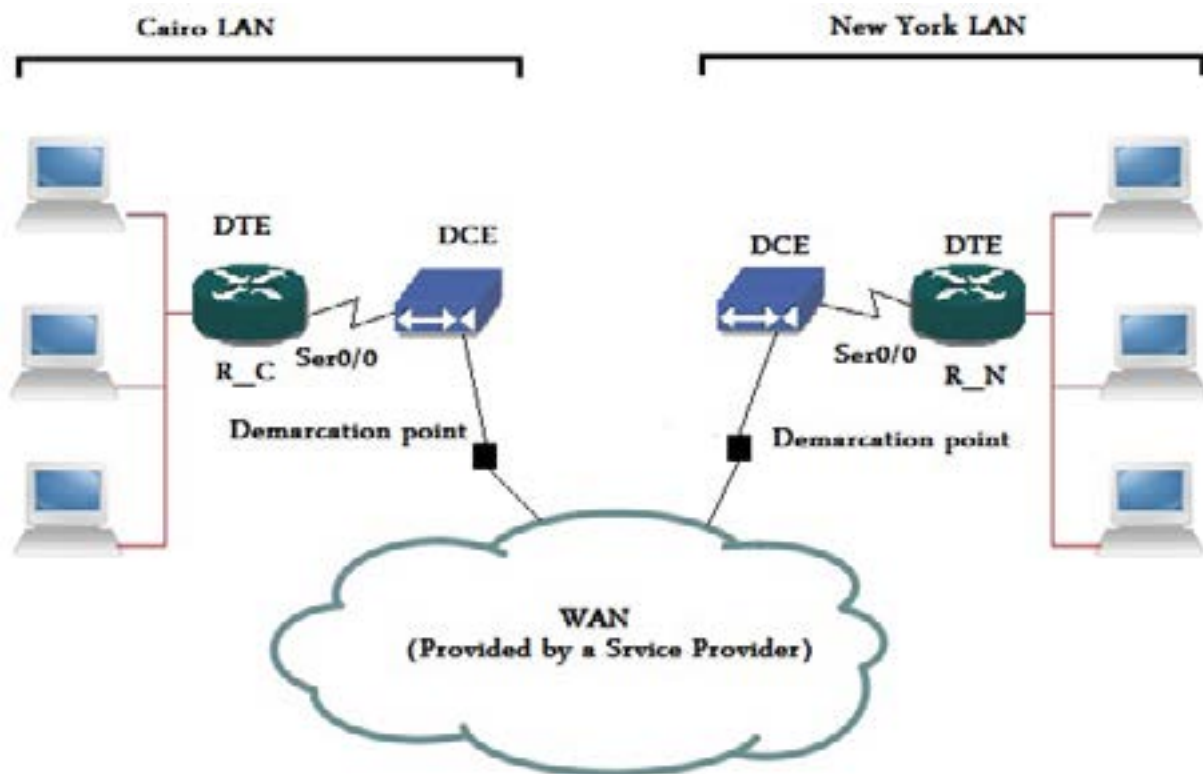


Figure 19.1: the WAN connection

CPE (Customer Premises Equipment)

- CPE is any circuit or equipment that is located in the customer's side, e.g., a router, computers, etc....

Demarcation point

- The demarcation point is the point at which the service provider responsibility ends, and the customer responsibility begins.

Local loop

- The local loop is the physical link that connects between the demarcation point and the service provider's network edge.

DCE (Data Communication Equipment)

- The DCE is a device that provides a 'clock signal' for the DTE.
- The DCE may be a 'CSU/DSU' in case it terminates a digital circuit, e.g. a 'T1 circuit', or it may be a 'modem' in case that it terminates an analog local loop, e.g. a telephone line.

DTE (Data Terminal Equipment)

- Typically, the router's interface that connects to the DEC is a DTE. It takes the clocking signal from the DCE.

CSU/DSU (Channel Service Unit/Data Service Unit)

- It is the DCE device that provides the clocking for the DTE and connects it to the digital circuit.

Modem

- It is the DCE device provides clocking for the DTE, and connects it to an analog line.
- The device that converts the signals that come through an analog line into digital information, and decodes the digital information and converts it into signals that can be transmitted over an analog line.

A promotional banner for SAP Learning Hub. The background is a blurred cityscape with a tall building. In the foreground, a man with glasses and a dark sweater is looking at a tablet. The text is overlaid on the image in large, bold, sans-serif fonts. The top line is in yellow, and the rest is in black. The SAP Learning Hub logo is in the bottom left, and the SAP logo is in the bottom right.

**THE ANSWER TO
YOUR LEARNING NEEDS**

**GET QUALITY, FLEXIBLE, AND
ECONOMICAL TRAINING WHEN
AND WHERE IT'S NEEDED.**

SAP Learning Hub

SAP

19.2 WAN connection types

There are several WAN connection types that can be used in a WAN network to connect between the customer networks.

19.2.1 Leased line

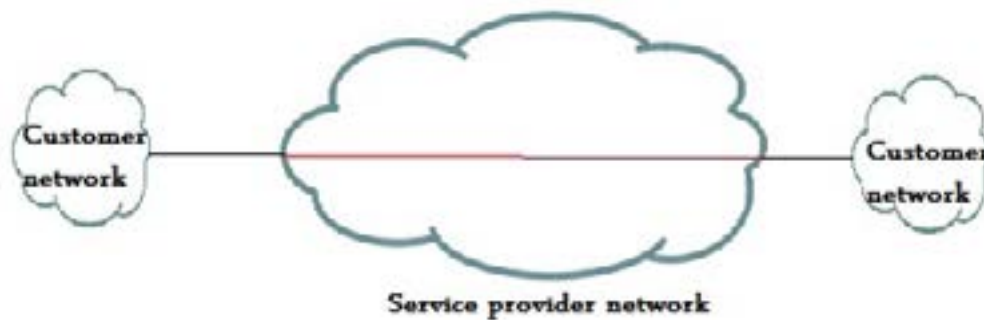


Figure 19.1: leased line

- It may be called a 'dedicated connection' or a 'point-to-point connection'
- It is a dedicated connection between the customer networks, and it passes through the WAN network that is provided by the service provider.
- The leased line advantage is its high quality.
- The leased line disadvantage is that, it is very expensive, and its limited flexibility.

19.2.2 Circuit switching

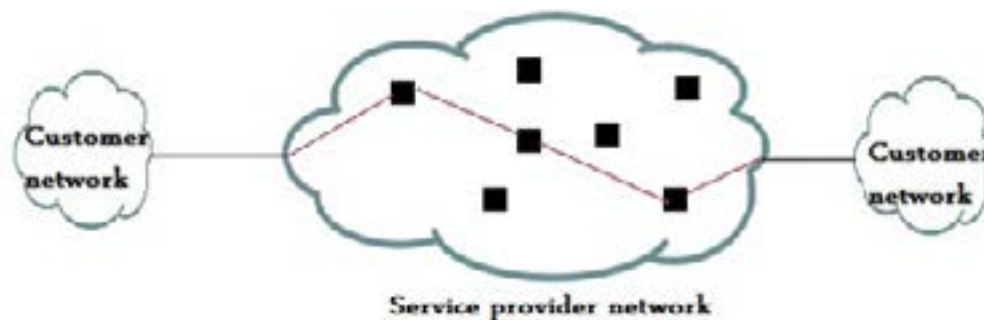


Figure 19.2: circuit switching

- In the circuit switched connection, a dedicated path is established between the customer networks, no one can use this path at this time except this customer.
- This dedicated path is established only in the time when the customer networks need to communicate with each other.
- The customer is billed depending on the time of using this path, not on the amount of data sent.

- The circuit switching advantage is that, it is efficient; this is because it is a dedicated path for the customer. Therefore, the bit rate will be constant.
- The circuit-switching disadvantage is that it has a low speed bit rate.

19.2.3 Packet switching

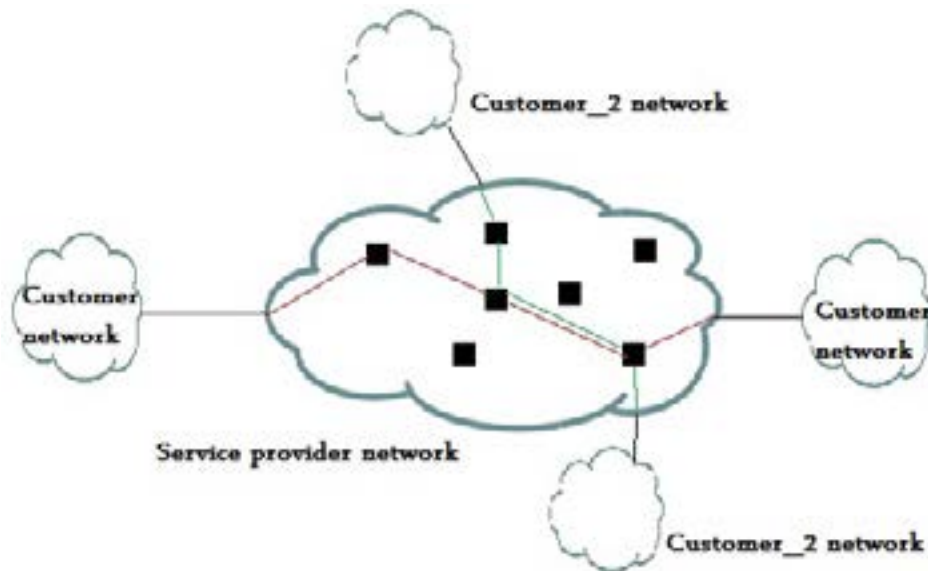


Figure 19.3: packet switching

- In the packet switching connection, the path between the customer networks is not dedicated for this customer.
- This path, or a part of it, may be shared with other traffic from other customers.
- In the packet switching, the customer is billed depending on the amount of data that is transmitted.
- The packet switching advantage is the low compared to leased lines, and it can provide high data rates compared to the circuit switching.
- The packet switching disadvantage is that it needs more complex implementation in the service provider's network.

19.3 HDLC and PPP protocols

- HDLC and PPP protocols are used in case that the customer is using a point-to-point link to connect between his networks.
- HDLC and PPP protocols are working in the data link layer.

19.3.1 HDLC (High Level Data Link Control) Protocol

- HDLC is the protocol that is used by default on the router's serial interfaces.
- HDLC is a proprietary protocol, this means that unless you have all of your routers are from the same vendor, you will not be able to use this protocol.

19.3.2 PPP (Point-to-Point Protocol)

- PPP is a non-proprietary protocol. It means that if you have several routers from different vendors, you should use PPP.
- PPP uses LCP (Link Control Protocol) to establish and terminate the point-to-point connections.
- PPP uses NCP (Network Control Protocol) to allow the usage of different network layer protocols.

PPP supports the following options (which is not supported by HDLC)

Authentication: peer routers authenticate with each other before establishing a connection. Two authentication methods may be used, PAP and CHAP.

Multilink: a router can consider several physical interfaces as one logical interface. E.g. if a router has three 2Mbps links, we can configure it to consider them as one 6Mbps link.

Compression: the router compresses the sent frames in order to increase the throughput of the connection.

Error detection: the router can detect any errors during the frame transmission.

A woman with long dark hair, wearing a grey sleeveless top, is standing in profile, looking down at a smartphone she is holding. She is positioned in front of a large window that looks out onto a bright, green outdoor area. The background is slightly blurred, emphasizing the woman and the text overlay.

MAXIMIZE PRODUCTIVITY

HELP YOUR ENTIRE ORGANIZATION BUILD EXPERTISE IN SAP SOFTWARE.

SAP Learning Hub

SAP

19.4 PPP configuration

To configure PPP on a router's serial interface, we use the following commands,

```
Router(config)#interface interface
```

```
Router(config-if)#encapsulation ppp
```

PPP authentication:

Suppose that we have two routers needs to authenticate with each other. We will configure the two routers as following,



Figure 19.4: two routers connected using PPP

We **must** configure the **same password** on the two routers in order to be able to authenticate with each other.

We use the following commands to configure the authentication of the routers,

```
Router(config)#username peer hostname password password
```

```
Router(config)#interface interface
```

```
Router(config)#ppp authentication {PAP | CHAP}
```

PAP: Password is sent in clear text format.

CHAP: More secure than PAP, It is a three way handshaking authentication method.

In figure (19.4), to configure the routers to authenticate with each other,

Router1's configuration,

```
Router1(config)#username Router2 password abcd
Router1(config)#interface ser 0/0
Router1(config-if)#ppp authentication CHAP
```

Router2's configuration,

```
Router2(config)#username Router1 password abcd
Router2(config)#interface ser 0/0
Router2(config-if)#ppp authentication CHAP
```

19.5 Frame Relay (FR)

- The frame relay (FR) is a packet switching technology. It is used in the service provider's network.
- The frame relay (FR) is a cost efficient technology. It reduces the costs of the connection.

19.5.1 Virtual Cuircuits

- The frame relay (FR) can provide a VC (Virtual Circuit) between the customer networks, so that the customer feels like he has a dedicated connection or a leased line between his networks.

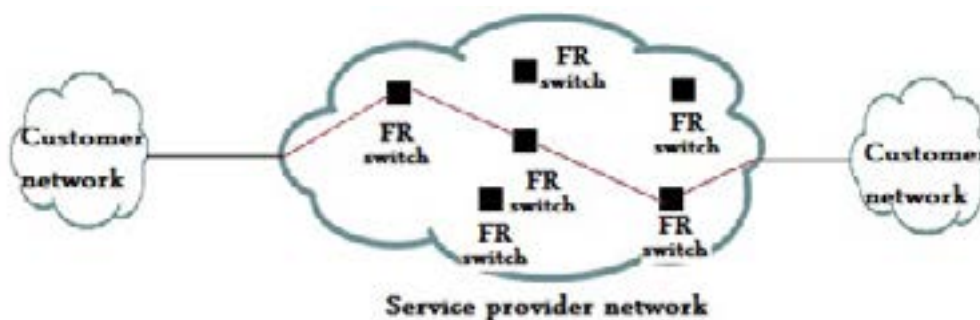


Figure 19.5: frame relay virtual circuits

- Two types of VC (Virtual Circuit) exist, PVC (Permanent Virtual Circuit), and SVC (Switched Virtual Circuit).

PVC (Permanent Virtual Circuit) is a virtual circuit that exists between the customer networks and always used in the communication between the customer networks.

SVC (Switched Virtual Circuit) is a virtual circuit that is not permanent. A new VC is established for every new session between the customer networks.

19.5.2 DLCI

- DLCIs (data Link connection identifiers) identify the PVCs to the customer's DTE interfaces.

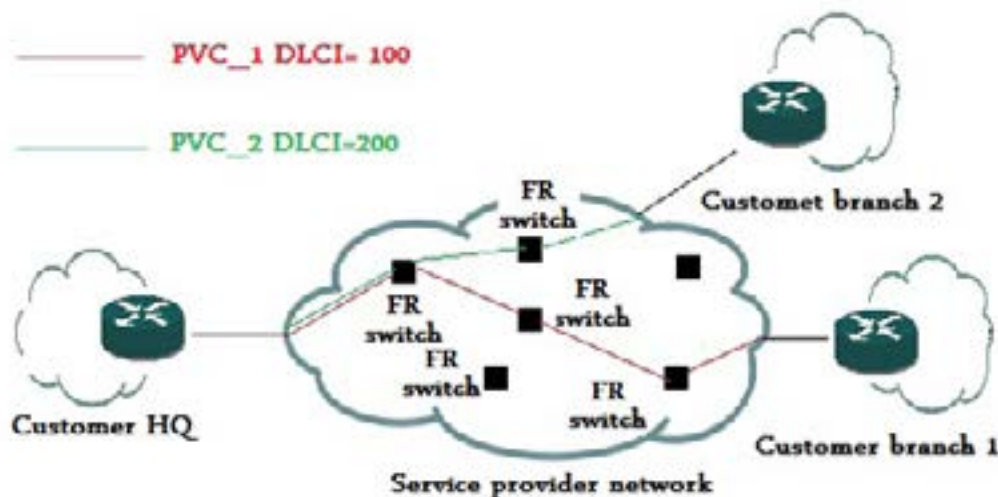


Figure 19.6: identifying PVCs using the DLCI

FAST ADOPTION, FAST ROI

EQUIP BUSINESS USERS TO ADOPT SAP SOLUTIONS.

SAP Learning Hub, user edition

SAP Learning Hub



- As seen in figure (19.6), the customer's HQ router serial interface can be divided into two sub-interfaces; every sub interface will use one PVC to connect to one of the branches.
- Every sub-interface will be assigned a DLCI that is mapped to the PVC it uses.
- The service provider provides the DLCI number of the PVC to the customer.

19.5.3 LMI

- LMI (local management interface) is a protocol that exchanges the information about the status of the virtual circuit between the customer's router (DTE), and the service provider's device (DCE).

19.6 FR congestion control

19.6.1 CIR vs. access rate

- When a customer deals with a service provider to connect between the customer networks, the deal contains two important values, the CIR, and the access rate.
- CIR (committed information rate) is the bit rate that is guaranteed by the service provider to be delivered to the customer's connection.
- Access rate is the maximum bit rate that can be used by the customer.

19.6.2 DE (discard eligibility)

- DE (discard eligibility) is a bit in the FR header.
- When the customer consumes the CIR of his connection and starts sending frames above his CIR, the DE bit in those frames will be set.
- When there is congestion in the network of the service provider, the FR switches in the service provider's network will start discarding the frames that has its DE bit set.

19.6.3 FECN and BECN

- FECN (forward explicit congestion notification) and BECN (backward explicit congestion notification) are two bits in the FR header.
- When there is congestion in the service provider's network, the FR switch will set the FECN bit in the frames it forwards to the destination DTE, this is done to inform the destination that there is congestion in the network.
- When there is congestion in the service provider's network, the FR switch will set the BECN bit in the frames it forwards to the source DTE, this is done in order to tell the source that there is congestion in the network, the source DTE in response should slow down its sending rate.

19.7 FR configuration

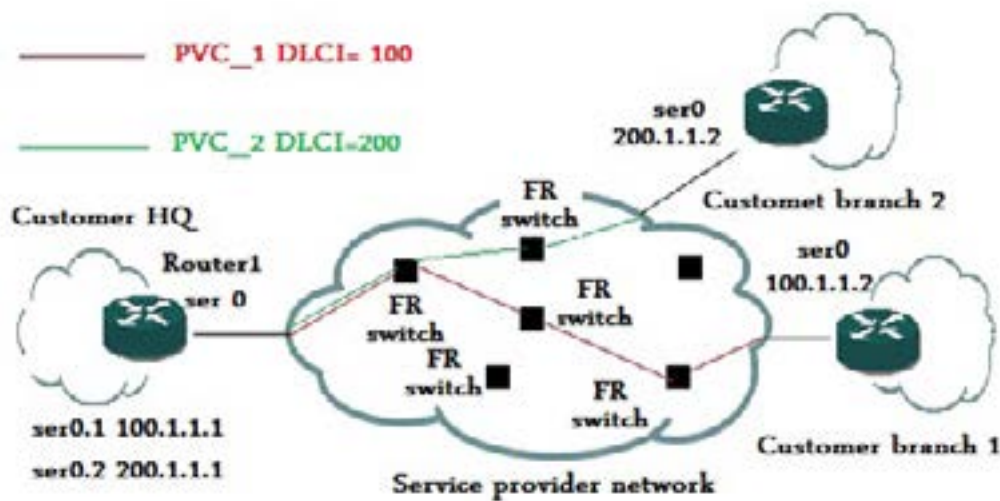


Figure 19.6: identifying PVCs using the DLCI

- In figure (19.7), we need to configure the router1's serial interface to connect to its network branch routers through the service provider's frame relay (FR) network.
- First, we divide (ser0) physical interface into two logical sub-interfaces (ser0.1, ser0.2).
- Then, we configure ser0.1 sub-interface to use PVC_1 (DLCI=100) to connect to the 'branch 1' router.
- Then, we configure ser0.2 sub-interface to use PVC_2 (DLCI=200) to connect to the 'branch 2' router.
- The following commands are used to make this configuration,

```
Router1(config)#interface ser0
```

```
Router1(config-if)#encapsulation frame-relay
```

```
Router1(config-if)#no shutdown
```

(To bring the interface up)

```
Router1(config-if)#interface ser0.1 point-to-point
```

(creates ser0.1 sub interface and determine its operation in point-to-point mode)

```
Router1(config-subif)#ip address 100.1.1.1 255.255.255.0
```

```
Router1(config-subif)#frame-relay interface-dlci 100
```

(To make ser0.1 use PVC_1 to connect to branch 1 router)

```
Router1(config-subif)#interface ser0.2 point-to-point
```

(creates ser0.2 sub interface and determine its operation in point-to-point mode)

```
Router1(config-subif)#ip address 200.1.1.1 255.255.255.0
```

```
Router1(config-subif)#frame-relay interface-dlci 200
```

(To make ser0.1 use PVC_2 to connect to branch 2 router)

Hour 20: Wireless LAN

20.1 Wireless LAN basics

- The wireless LAN allows users to connect to the network, while they are moving. They do not have to sit in a fixed place.
- The wireless LAN decreases the need for cables.
- The disadvantage of the wireless LAN is that it is not as stable as the wired network.
- The antenna types and direction of the wireless LAN devices may affect the wireless LAN performance.
- The microwave ovens and the cordless phones can interfere with the wireless LAN, because they work in the same frequency range.

20.1.1 Wireless LAN protocols

- There are three main protocols that are used in the wireless LAN, they are 'IEEE 802.1a', 'IEEE 802.1b' and 'IEEE 802.1g'.
- 'IEEE802.1a' works in the 5GHz frequency range, and it can support the speeds up to 54 Mbps.
- 'IEEE802.1b' works in the 2.4GHz frequency range, and it can support speeds up to 11 Mbps.
- 'IEEE802.1g' works in the 2.4GHz frequency range, and it can support speeds up to 54 Mbps.



JUMP-START CAREERS

**GIVE STUDENTS ONLINE
ACCESS TO A VAST BODY
OF KNOWLEDGE ABOUT
SAP SOLUTIONS.**

SAP Learning Hub, student edition

SAP Learning Hub

SAP

20.1.2 Access point (AP)

- The wireless LAN main device is the 'access point (AP)'.
- The access point (AP) is the central device in the wireless LAN; it sends and receives the signals with the wireless LAN clients.
- There are two wireless LAN hierarchies, the 'BSS', and the 'ESS'.

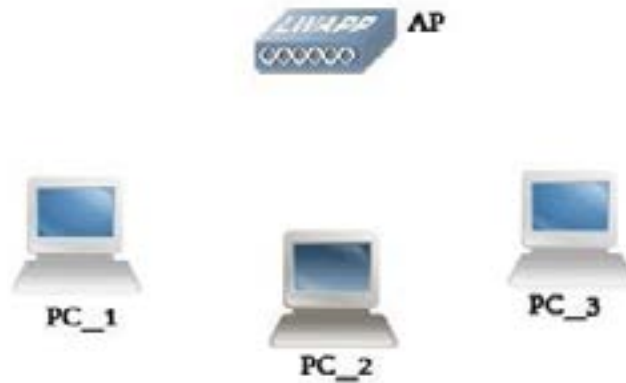


Figure 20.1: an access point

BSS (Basic Service Set)

In 'BSS', the wireless clients use only one AP to connect to each other, as seen in figure (20.1). It is usually used in a small office or in a home.

ESS (Extended Service Set)

In 'ESS', two or more BSSs are connected by a distribution system. It is usually used when we need to cover a large geographical area.

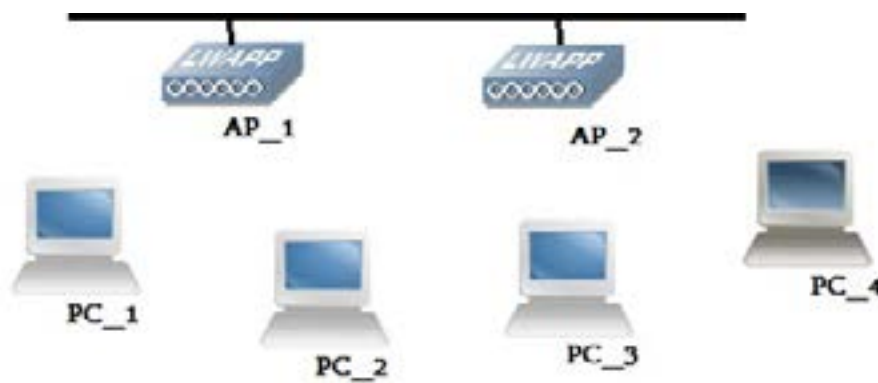


Figure 20.2: ESS

20.2 AP configuration

There are three basic parameters that should be configured on the AP; they are the 'SSID', the 'RF channel' and the 'authentication method'.

20.2.1 SSID (Service Set Identifier)

- Every wireless LAN must have its own SSID, which is a unique string of characters.
- The SSID is configured on the AP, and the AP broadcasts it to the wireless clients.
- If the AP is configured not to broadcast its SSID, the SSID of this AP should be manually configured on the wireless clients that need to connect to this AP.

20.2.2 RF channel

- Many RF channels can be used on every AP.
- Every AP can be configured to use a certain RF channel.
- If you have more than one AP in the same place, you can configure every AP of your APs to operate on a different non-overlapping RF channel, in order not to interfere with other APs.

20.2.3 Wireless security

- Wireless security prevents any unauthorized access to the wireless network.
- There are two types of encryption, the 'WEP' and the 'WPA'.
- WPA is preferred over WEP because WPA changes the encryption key dynamically, which gives more security to the wireless LAN.
- All wireless clients should have the correct encryption key in order to be able to communicate with the AP.
- The network administrator can use the 'open access' option. This means that, no authentication is required to connect to this wireless LAN.
- 'Open access' is usually used in the public places to allow all people to use this wireless network.
- The network administrator can determine which devices can communicate with the AP. This is done by manually recording the MAC addresses of the allowed devices on the AP. This is called the 'MAC address authentication'.

Hour 21:IPv6

21.1 IPv6 basics

- Soon, IPs will be totally consumed. There will be no more available IPs. In order to solve this problem, IPv6 was developed.
- The ordinary IP scheme we were using in the previous hours is called the IPv4.
- The IPv6 scheme contains 8 blocks separated by a column. Every block contains 16 bit. This means that the IPv6 scheme contains 128 bit ($8 \times 16 = 128$). It is larger than IPv4, which was only 32 bits long.
- Any IPv6 interface can be assigned any number of IPv6 addresses.

2001:0003:1b53:76ba:f678:8261:43bd:3ab1

IPv6 example

Figure 21.1: IPv6



LEARN BY DOING

**DEVELOP EXPERTISE
IN SAP SOLUTIONS
THROUGH EXPLORATION
AND PRACTICE.**

SAP Live Access

SAP Learning Hub

SAP

21.1.1 IPv6 address shortening

- As you can see in figure (21.1), it is big! Therefore, two rules were developed in order to be able to write IPv6 in a simpler manner.

Rule1: remove any leading zeros from every block.

Rule2: replace the contiguous block of zeros with a double column. This is permitted to be done only **one time** in every IPv6 address. If you have more than one contiguous block of zeros, you can apply this rule only to one contiguous block of them.

Example:

Write the following IPv6 address in the simplest way.

2001:0000:0000:006b:0000:0000:0874:4c32

Solution:

Apply rule 1 2001:0:0:6b:0:0:874:4c32

Apply rule 2 2001::6b:0:0:874:4c32

So, the answer is **2001::6b:0:0:874:4c32**

21.2 IPv6 addressing

The IPv6 interfaces can get its IPv6 address by using two methods, manually and automatically.

21.2.1 Manual addressing

The administrator manually configures an IPv6 address on the IPv6 interface.

21.2.2 Automatic addressing

There are two ways to get an automatic address, the 'stateless addressing', and the 'stateful addressing'.

Stateless addressing

- In this method, the interface can deduce its IPv6 address from its MAC address, and the 'network prefix' it receives from the router that is connected in its network.
- The IPv6 address is formed from two parts, they are a 64 bits network prefix, and a 64 bits interface ID.
- The 64 bits interface ID can be called the 'EUI-64 address'.

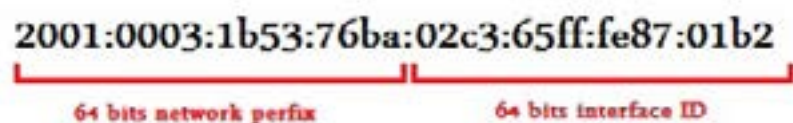


Figure 21.2: stateless addressing

- In stateless addressing, the 64 bits interface ID can be deduced by the interface itself from its MAC address as following,

MAC address= 00:c3:65:87:01:b2

1. insert fffe in the middle of MAC address 00c3:65ff:fe87:01b2

2. change the seventh bit to one 02c3:65ff:fe87:01b2

So, the interface ID = 02c3:65ff:fe87:01b2

- The interface can get its network prefix from the router that connects to its network via a message from the router called the 'router advertisement (RA)'.
- So now, the interface knows its network prefix and its interface ID.
- The interface IPv6 address is a 64 bits network prefix combined with a 64 bits interface ID.

2001:0003:1b53:76ba:02c3:65ff:fe87:01b2

64 bits network prefix 64 bits interface ID

Figure 21.3: stateless addressing

Stateful addressing

- If no router is found or the router advertisement (RA) message states that a DHCP should be used, the interface gets its IP using the stateful addressing.
- In this method, a DHCP server is installed in the network, so that every interface can get its IPv6 address from this DHCP using the DHCPv6 protocol.

21.3 IPv6 address configuration

To manually configure an IPv6 address on an interface we make the following,

First, we enable the IPv6 routing on the router using the following command,

```
Router(config)#ipv6 unicast-routing
```

Second, we configure an IPv6 address on the IPv6 interface using the following command,

```
Router(config-if)#ipv6 address ipv6 address/mask
```

Therefore, the actual configuration will be,

```
Router(config-if)#ipv6 address 2001:3:1b53:76ba:02c3:65ff:fe87:01b2/64
```

Or we can configure the network portion and let the interface deduce the interface ID part from its MAC address using the following command,

```
Router(config-if)#ipv6 address 2001:3:1b53:76ba::/64 eui-64
```



**HANDS-ON PRACTICE
FOR EFFECTIVE LEARNING**

**EXPERIENCE SAP
SOFTWARE FIRSTHAND
TO BUILD KNOWLEDGE
AND ENHANCE SKILLS.**

SAP Live Access

SAP Learning Hub

To let the interface get its IP address automatically, we do the following,

First, we enable the IPv6 routing on the router using the following command,

```
Router(config)#ipv6 unicast-routing
```

Second, we enable the IPv6 on every interface that should automatically take an IPv6 address. This is done using the following command,

```
Router(config-if)#ipv6 enable
```

21.4 IPv6 address types

The following are the types of the IPv6 address,

Link local address

- Every IPv6 interface assigns a link local address to itself.
- Every IPv6 interface **must** have a link local address, even if the interface has been assigned another address. This is because the link local addresses are mandatory for the operation of IPv6 protocols.
- It is used only inside the network.
- The link local IPv6 addresses exist in the '**FE80::/10**' range. This means that the link local IPv6 addresses must start with [1111 1110 10].

Unique local address

- It can be used only inside the network; it cannot be routed across the global internet, the same as the private addresses in IPv4.
- It is nearly unique. It means that there is a very small probability that you may find two IPv6 interfaces that have the same unique local address.
- Unique local address exist in the '**FC00::/7**' range. This means that the unique local addresses must start with [1111 110].

Global unicast address

- The global unicast addresses that can be routed across the global internet.
- The global unicast addresses exist in the '**2000::/3**' range. This means that it must start with [001].

21.4.1 IPv6 communication modes

There are three communication modes in IPv6, they are the unicast, the multicast and the anycast. There is no broadcast in IPv6.

Unicast: one to one communication.

Multicast: one to many communication.

Anycast: one to the nearest communication. This means that we can give the same IPv6 addresses to many devices, and the data that is sent from one sender will be delivered to only the nearest receiver found from those devices.

21.4.2 IPv6 special addresses

'0:0:0:0:0:0:0:0' (equals to **'::'**)

This is the source address of the interface when requiring an IPv6 address using the stateful addressing.

'0:0:0:0:0:0:0:1' (equals to **'::1'**)

It is the loop back address of the IPv6 interface.

'FF00::/8'

This is the range of the IPv6 multicast addresses.

'3FFF:FFFF::/32' and **'2001:0DB8::/32'**

This range is reserved for examples and documentation.

21.5 IPv6 Routing protocols

- In IPv6, there are new versions of the ordinary routing protocols that we were using in IPv4
- Three protocols may be used in IPv6. They are, RIPng, OSPFv3 and EIGRPv6.

21.5.1 RIPng

In this protocol,

- The network updates are sent to a multicast IPv6 address **'FF02::9'**.
- To configure RIPng on the router, we enable it on every interface that should participate in the RIPng routing. This is done using the following command,

```
Router(config-if)#ipv6 rip process number enable
```

- To verify the routing functionality, we may use one of the following commands,

```
Router#Show ipv6 rip
```

```
Router#debug ipv6 rip
```

21.5.2 OSPFv3

In this protocol,

- The network updates are sent to the 'DR' on 'FF02::6'.
- The DR forward the network updates to its adjacencies on 'FF02::5'.
- To configure OSPFv3 on the router, we enable it on every interface that should participate in OSPFv3 routing using the following command,

```
Router(config-if)#ipv6 ospf process number area area number
```

- To verify the routing functionality, we may use on of the following command,

```
Router#debug ipv6 ospf packet
```

A woman with long dark hair, wearing a white blazer, is looking upwards and to the right while holding a large document or folder. The background is a bright blue sky with white clouds. The text is overlaid on the left side of the image.

ANYTIME, ANYWHERE

**LEARNING ABOUT
SAP SOFTWARE HAS
NEVER BEEN EASIER.**

SAP Learning Hub – the choice of
when, where, and what to learn

SAP Learning Hub

SAP

21.5.3 EIGRPv6

In this protocol,

- The hello packets and the network updates are sent to a multicast IPv6 address 'FF02::A'.
- To configure EIGRPv6 on the router, we first bring it up on the router using the following commands,

```
Router(config)#ipv6 router eigrp AS number
```

```
Router(config-rtr)#no shutdown
```

Then, we enable EIGRPv6 on every interface that should participate in the EIGRPv6 routing process using the following command,

```
Router(config-rtr)#ipv6 eigrp AS number
```

21.6 Migration from IPv4 to IPv6

There are many techniques that enable the network administrator to migrate their network from IPv4 to IPv6 without making any interruptions for the operation of the network.

21.6.1 Dual stack routing

- In this migration method, both IPv4 and IPv6 are running on the router simultaneously. Therefore, both IPv4 and IPv6 devices will be able to work on your network.
- The network administrator may gradually increase the number of IPv6 devices until he gets a pure IPv6 network.

21.6.2 Tunneling

- In this migration method, IPv6 packets are encapsulated into IPv4 packets, in order to make the IPv6 devices able work in an IPv4 network.
- There are many types of tunneling such as, the '6 to 4 tunneling', the 'Teredo tunneling' and the 'ISATAP tunneling'.

21.6.3 Proxying and translation

In this method, we use a device that can translate between IPv4 and IPv6 to work as the translator agent between the IPv4 devices and the IPv6 devices.

- The process of this device is the same as the NAT process in IPv4. However, the NAT process here is between the IPv4 and the IPv6.