



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Understanding Networks

Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales

www.uwtsd.ac.uk

***Network Operating Systems
and Services (ACCA5023)***

Applied Computing - WISA



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

- **Module Induction**
- **Coursework Introduction**
- **Understanding Networks**
 - **Components**
 - **Architectures**
 - **IP Addressing**
 - **Servers**
- **Network Operating Systems**

Lab/ Tutorials

- **Research: IP Address, Network Communication, Network Components.**

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk

During this session, we shall start discussing about the details of our module (Lectures, Tutorials, Assessments etc.

We shall discuss various Networking Components, functionalities and Operations, Architectures and the enhancements in Network Operating systems



Module Induction

- Communication with Lecturer
- Two Coursework's (Multiple Dates!!!)

Component 1 50%	Research, build, and deploy, a Virtualised network	Report : 03/03/2026
Component 2 50%	Configure, and manage Virtualised network	Report : 11/05/2026 Demonstration: 12/05/2026

I - Introduction

➤ What is a?

- *Computer Network*
- *Types of Network*
- *Resources in a Network*
- *Components in a Network*
- *Hosts and Nodes – Are they same?*

I - Introduction

➤ Windows Server 2022

- Another version of the Microsoft OS for servers, is the follow-up to Windows Server 2019.
- Besides introducing Windows Server, right at the begin is to give an overview of the very basic concepts of computer networks.



Windows Server 2022
Book | Bekim Dauti, 3rd edition, Packt Publishing - ebooks Account, 16 Sept. 2022, Total pages 398
Essential
[View online](#)

[Full details](#) [Share](#) [More](#)



Windows Server 2022 & PowerShell All-in-One For Dummies (For Dummies (Computer/Tech))
Book | Sara Perrott, 1st edition, For Dummies, 16 Mar. 2022, Total pages 784
Essential
[View online](#)

Library processing



Windows Server 2019 administration fundamentals : a beginner's guide to managing and administering Windows Server environments
E-book | Dauti, Bekim., Second edition., Birmingham :, Packt Publishing, 2019., Total pages 1 online resource.
Essential
[View online](#)



UNIX and Linux system administration handbook /
E-book | Fifth edition., Addison-Wesley., 2017
Essential
[View online](#)



Linux Administration: A Beginner's Guide, Eighth Edition (NETWORKING & COMM - OMG)
Book | SOYINKA, 8th edition, McGraw Hill, 16 Mar. 2020, Total pages 688
Essential
[View online](#)

Library processing

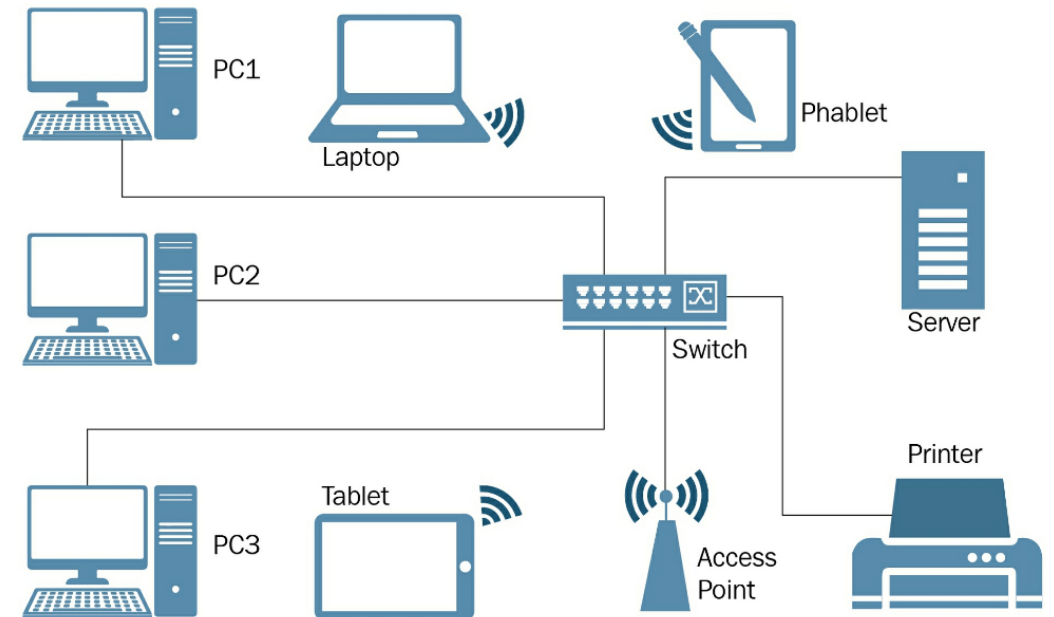
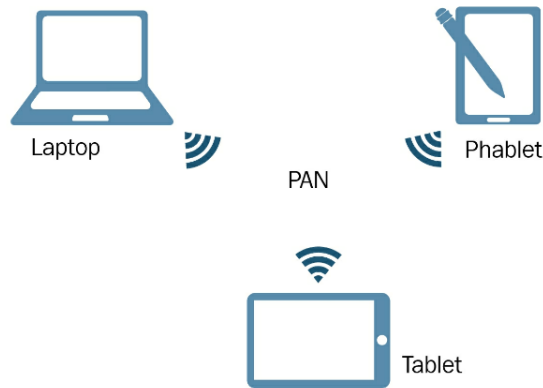
II – Understanding Networks

➤ What is a Computer Network?

- *A computer network is a group of computers connected to each other in order to share resources. The resources are usually data, network services, and peripheral devices*

➤ Types of Computer Network?

- *PAN / Home area Network (HAN)*
- *LAN*
- *MAN*
- *WAN*



III – Components

- Like PCs have components, computer networks also have their own **components**.
- Usually, while PCs and peripheral devices are known to most people, components such as **networking devices, networking media, and network operating systems (NOS)** are mostly known by Technicians/IT Professionals.

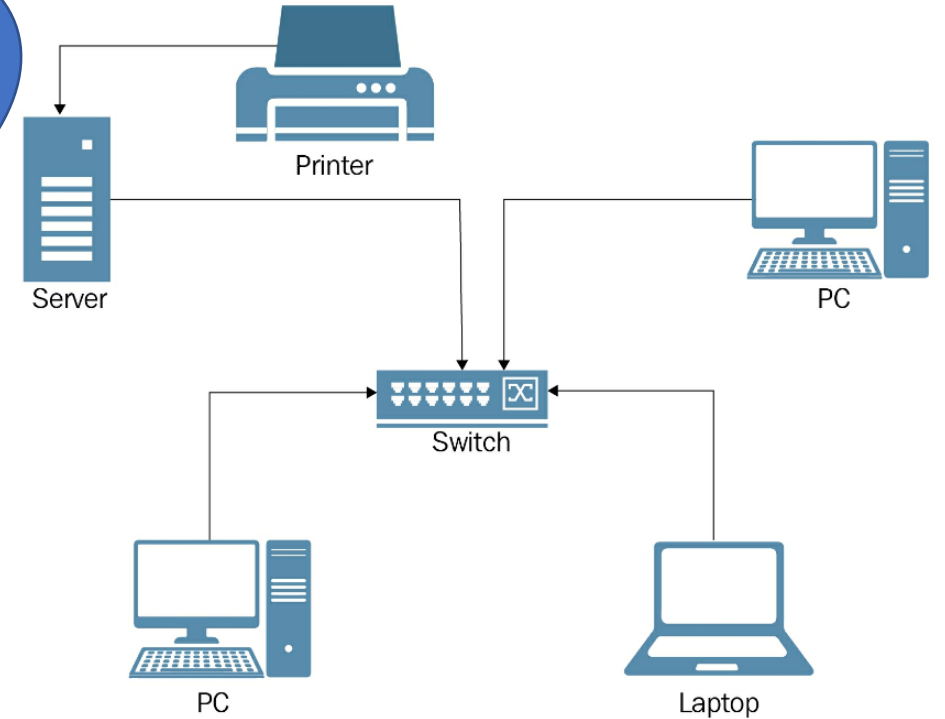
IV - Architecture

- Let's assume that the **server** has no reference for both **access to resources** and **providing resources**.

The word **servers** comes from the word **serve**. It means to provide services that benefit or help.

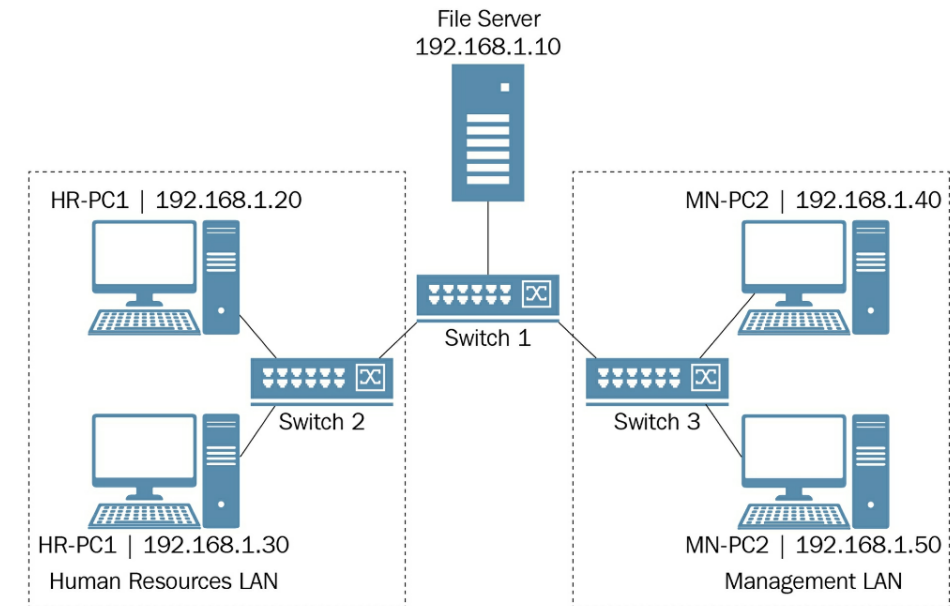
- From that, we can think of a server in a computer network as the computer that provides services to clients. In conclusion, the server serves the clients.

role in the



IV – Architecture

- Although clients and servers are the most important elements of a computer network, it depends upon **hosts and nodes**. Are they the same thing?
- No, they are not!
- While all hosts can be nodes, not every node can act as a host.
- A **host** is any device with an **IP address** assigned to its network interface that requests or provides networking resources on the network. (Eg. clients, servers, and routers).
- A **node** is any device that can receive and transmit the networking resources on the network. Nodes have a network interface that is used for their management.



IV – Architecture

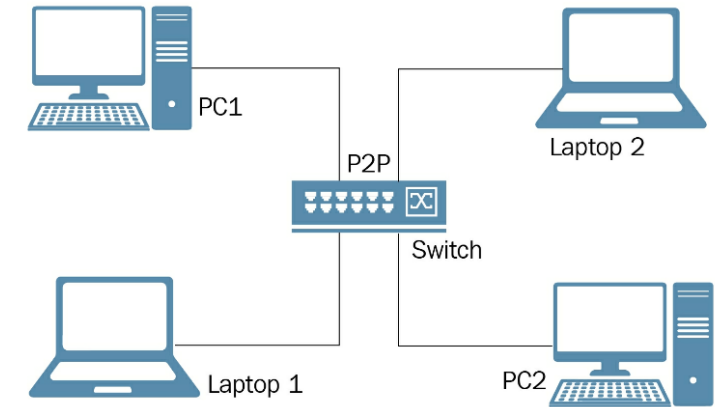
➤ Architecture:

➤ Peer to Peer (P2P)

- Peer-to-Peer (P2P) network architecture refers to a network model in which hosts or computers are equal in terms of capabilities and responsibilities.
- Depending on the circumstances, each host may be a client or server depending on whether it requests or provides services in that network.

➤ Client/ Server

- A client/server, often known as a domain-based network, is a computer network in which hosts have a predefined role.
- Hosts that request resources act as clients, whereas hosts that provide resources act as servers.
- In general, the client/server network architecture is a network with dedicated servers.
- Usually, LANs, MANs, and WANs represent the best examples of client/server computer networks.



V – IP Addressing – Using Number Systems

- An Internet Protocol address, popularly known as an IP address, is a logical element comprised of numbers that is assigned to host's network interface in order to identify it in a computer network.
- Network address helps the router identify a path within the whole network (e.g. the Internet). This number is assigned by the American Registry for Internet Numbers (ARIN) (or an ISP).
- Host address is assigned by the network administrator according to some internetworking address plan. Host addresses can be assigned dynamically.
- All hosts on the same network will have the same network number but each host is uniquely identified by its own host number.



Numbering Systems		
System	Base	Digits
Binary	2	0 1
Octal	8	0 1 2 3 4 5 6 7
Decimal	10	0 1 2 3 4 5 6 7 8 9
Hexadecimal	16	0 1 2 3 4 5 6 7 8 9 A B C D E F

V – IP Addressing: IPv4

➤ Is a logical network address that identifies a particular host. It is associated with a network interface card and It is unique on the network for communications

➤ 32 Bit | Dotted Decimal Notation (DDN) |

➤ 8 Bit Each (Decimal Octets) | 0 to 255 (4 Octets)

➤ **Public and Private Addresses**

- The Public addresses are used in the Internet
- The Private Addresses are used only within Lan's
- The Private Addresses could not be routed in Internet

➤ **Unicast**

The Packets are sent to only one device

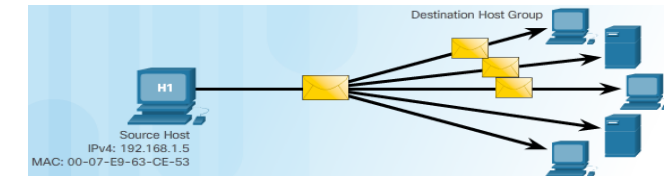
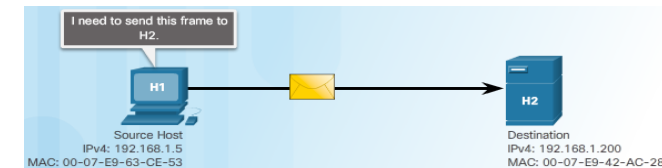
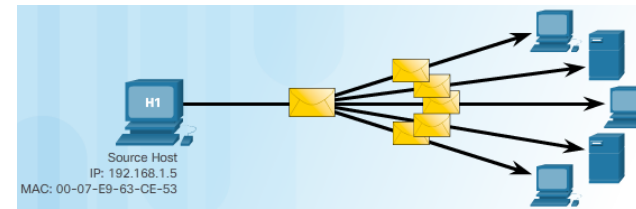
➤ **Multicast**

The Packets are sent to many devices

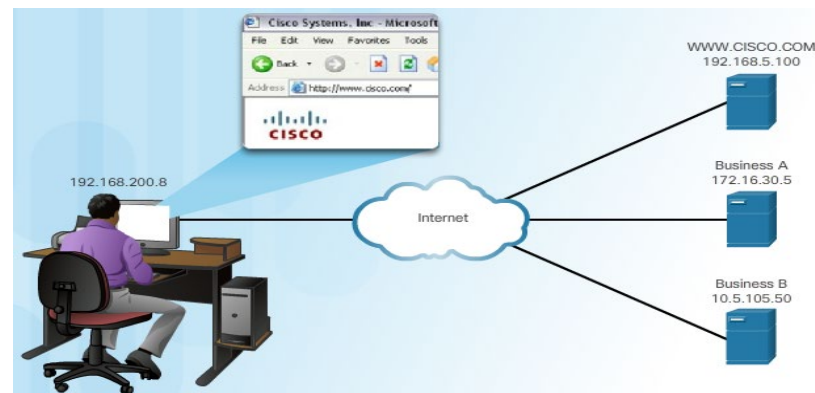
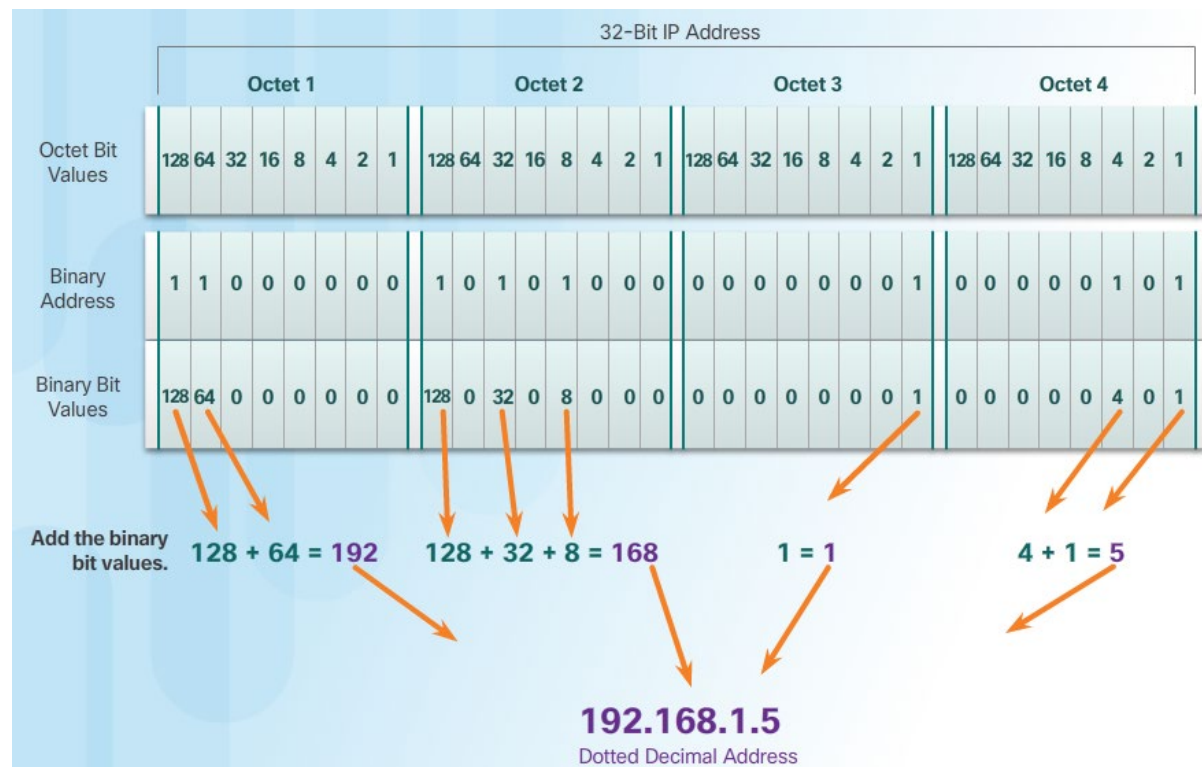
➤ **Broadcast**

The Packets are sent to all devices in the Network

Address Class	Number of Network Numbers Reserved	Network Addresses
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0



V – IP Addressing: IPv4 Subnet mask



	Network Portion				Host Portion
IPv4 Address	192	.	168	.	10
	11000000		10101000		00001010
Subnet Mask	255	.	255	.	0
	11111111		11111111		00000000

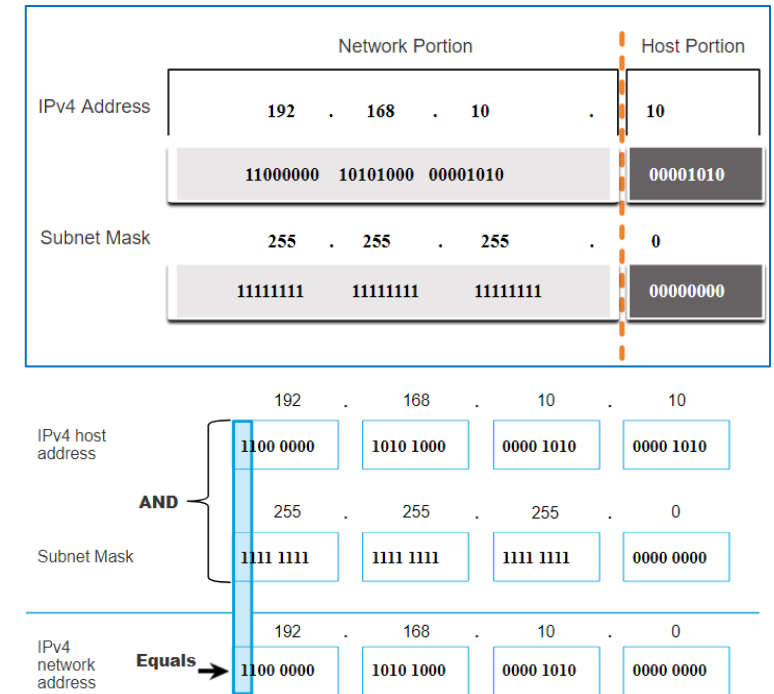
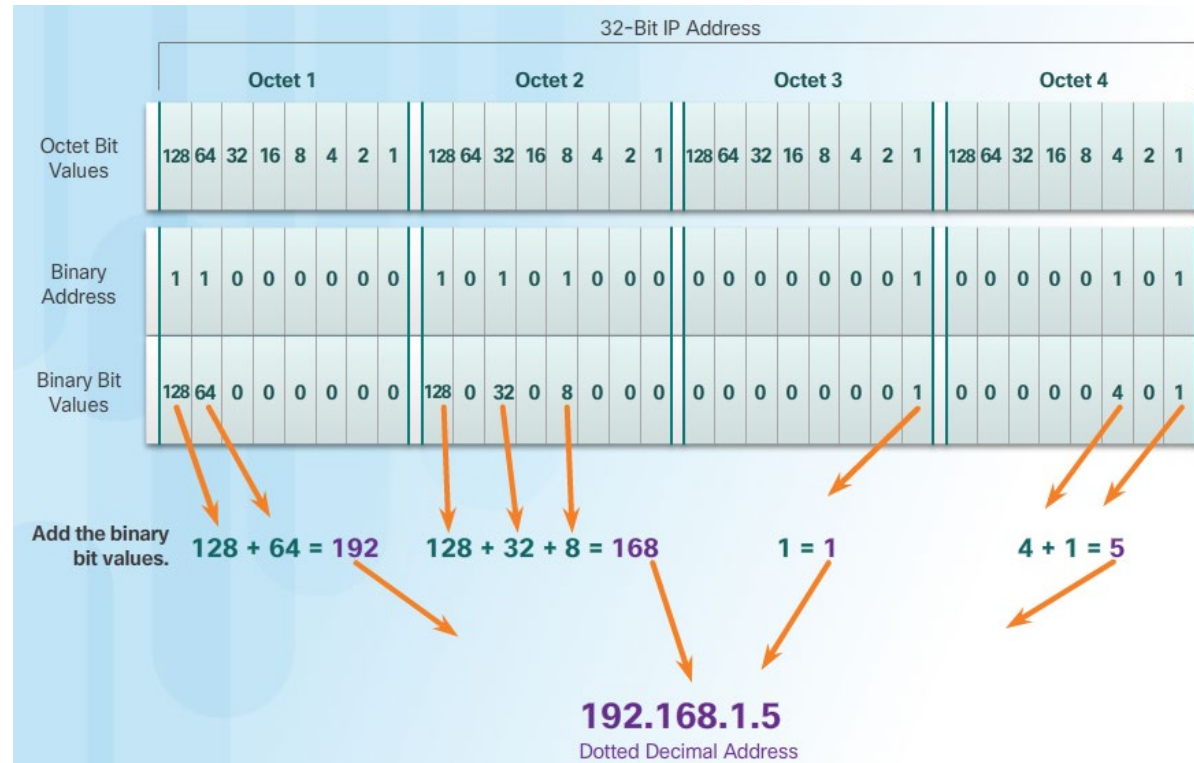
A subnet mask is used to determine the network and host portions.

V – IP Addressing: IPv4 Subnet mask

The actual process used to identify the network and host portions is called **ANDing**.

$1 \text{ AND } 1 = 1$,
 $0 \text{ AND } 1 = 0$,
 $1 \text{ AND } 0 = 0$,
 $0 \text{ AND } 0 = 0$

$1 = \text{True}$
 $0 = \text{False}$



V – IP Addressing: IPv4 Structure

- The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.
- A prefix length is a less cumbersome method used to identify a subnet mask address.
- Within each network are three types of IP addresses:
 - *Network address*
 - *Host addresses*
 - *Broadcast address*

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

V – IP Addressing: IPv4 Classes

Classful Addressing

Class A (*0.0.0.0/8 to 127.0.0.0/8*) supports extremely large networks.

Class B (*128.0.0.0/16 – 191.255.0.0/16*) supports the needs of moderate to large size networks.

Class C (*192.0.0.0/24 – 223.255.255.0/24*) supports small networks with a maximum of 254 hosts.

Classless Addressing

*IPv4 addresses allocated on any address bit boundary
Delays the depletion and exhaustion of IPv4 addresses
Classless Inter-Domain Routing (CIDR)*



V – IP Addressing: IPv4 Special Addresses

Loopback addresses

- ✓ 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- ✓ Commonly identified as only 127.0.0.1
- ✓ Used on a host to test if TCP/IP is operational.

Link-Local addresses

- ✓ 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- ✓ Commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses.
- ✓ Used by Windows DHCP clients to self-configure when no DHCP servers are available.

V – IP Addressing: IPv4 Assigning Addresses

Assigning Addresses

- Can be done statically or dynamically
- Assign an IPv4 address, subnet mask, default gateway and other necessary info for network communications

Static IPv4 addresses

- Hosts, such as servers and printers, that need particular addresses
- Can be time consuming and error prone
- Need to maintain an accurate list of which IPv4 addresses

Dynamic IPv4 Address Assignment

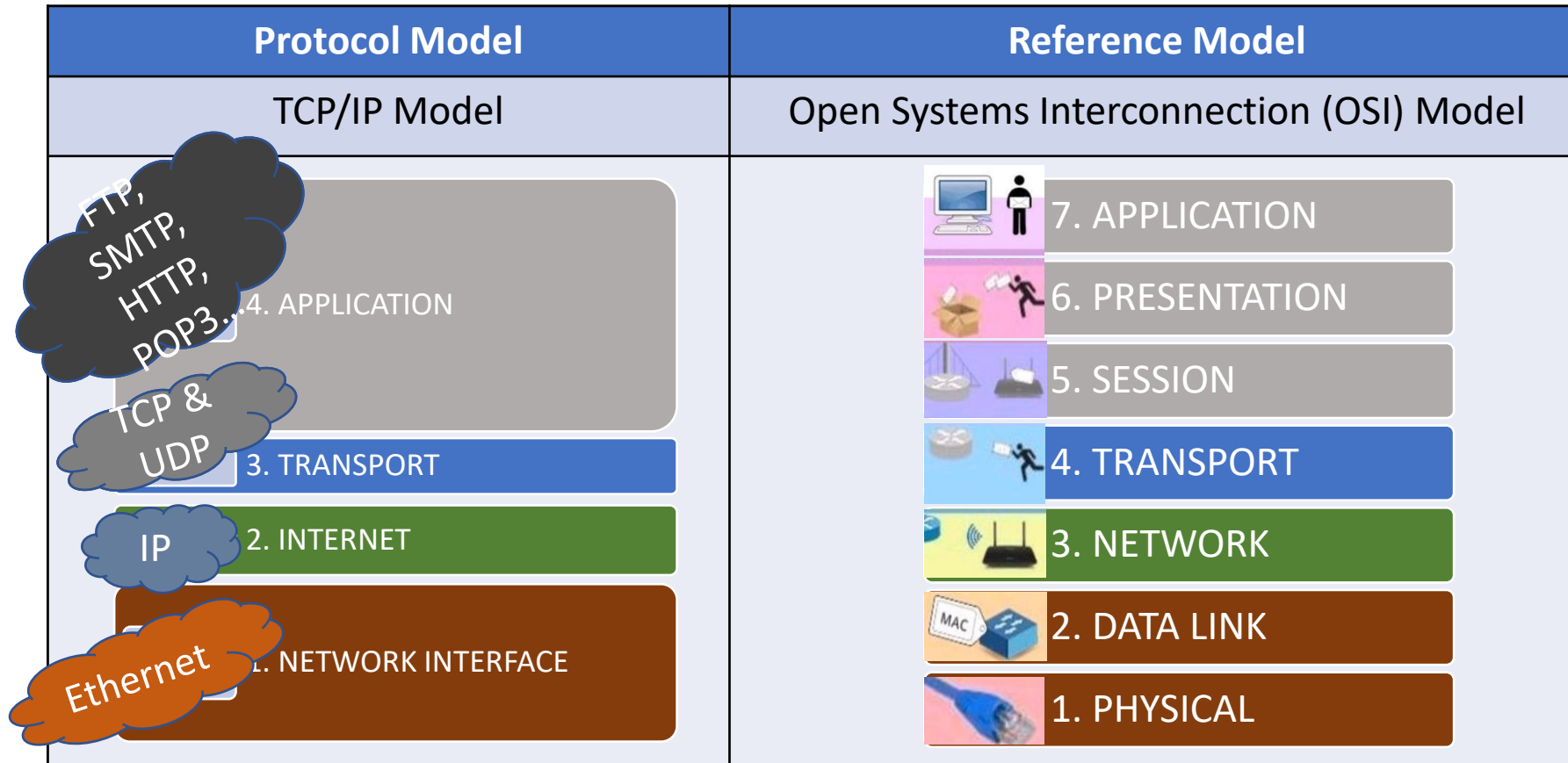
- Dynamic Host Configuration Protocol (DHCP) allows for automatic assignment of addressing information
- Preferred method of assignment for a large network
- IP addresses can be reallocated when they become available

V – IP Addressing: IPv6 Address

What is an IPv6 Address?

- Also the same as IPv4 (in the perspective of functioning) but with advantages. Both IPv4 and IPv6 will coexist in the near future and the transition will take several years.
- IPv6 addresses are **128 bits** in length and written in **hexadecimal**. It is **not case-sensitive** and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is **x:x:x:x:x:x:x:x**, with each “x” consisting of four hexadecimal values. In IPv6, a **hextet** is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:
2001:0db8:0000:1111:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
- For more details about IPv6 Addressing, refer to video recording (IPv6) and presentation (IPv6_Addressing), both available in Moodle References Tab.

VI – Infrastructure: Standards



OSI/ TCP-IP Protocol Suite

VI – Infrastructure: Devices

ROUTERS

- Routers are Layer 3 devices
- A router makes routing (best path) decisions based on Network Addresses.
- It examines packets and chooses the best path for them through the network.
- Routing is sometimes known as Layer 3 switching.

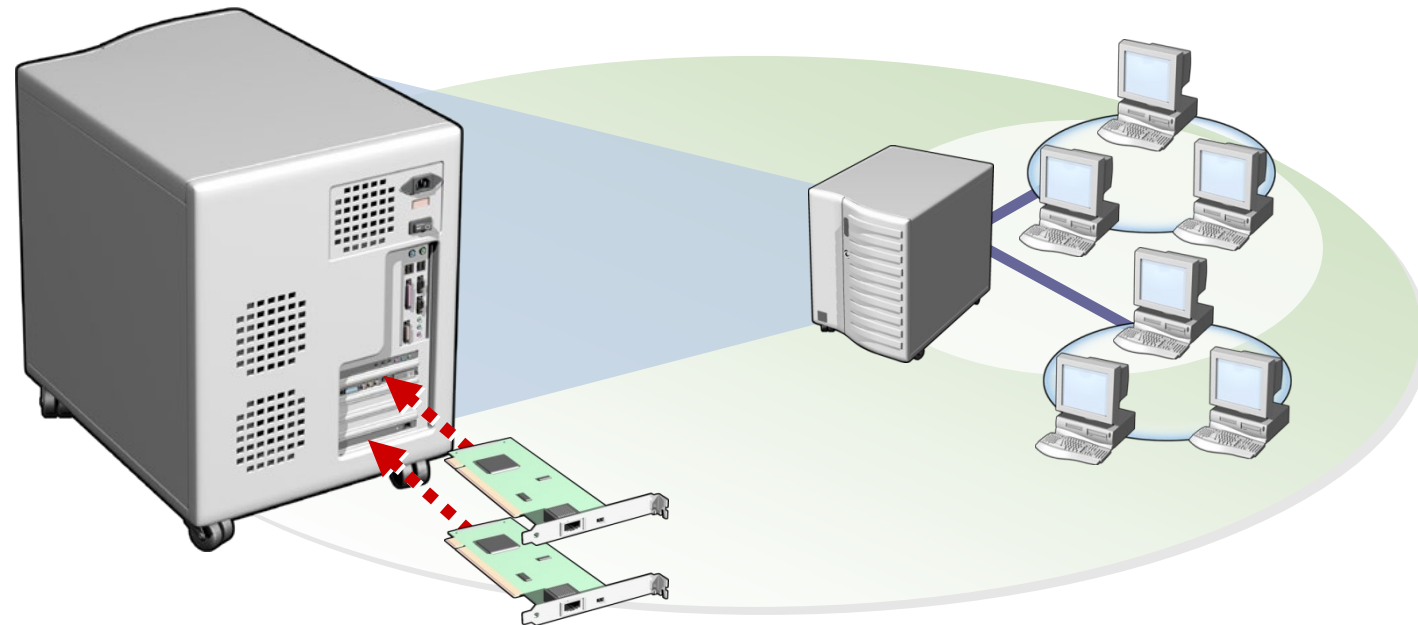
Main routing components

- Routing interface
- Routing protocol
- Routing table

Router types	Example
Hardware router	A device that performs routing as a dedicated function
Software router	A router that is not dedicated to performing routing only, but performs routing as one of multiple processes running on the router computer

VI – Infrastructure: Devices

A routing interface is an interface over which IP packets are forwarded



For a router to be able to route a packet it must know:-

- ✓ Destination address of packet
- ✓ Neighbour routers
- ✓ Possible routes to all remote networks
- ✓ The best route to each remote network
- ✓ How to maintain and verify routing information

The networks connect to the routers interfaces are known as **Directly Connected** networks

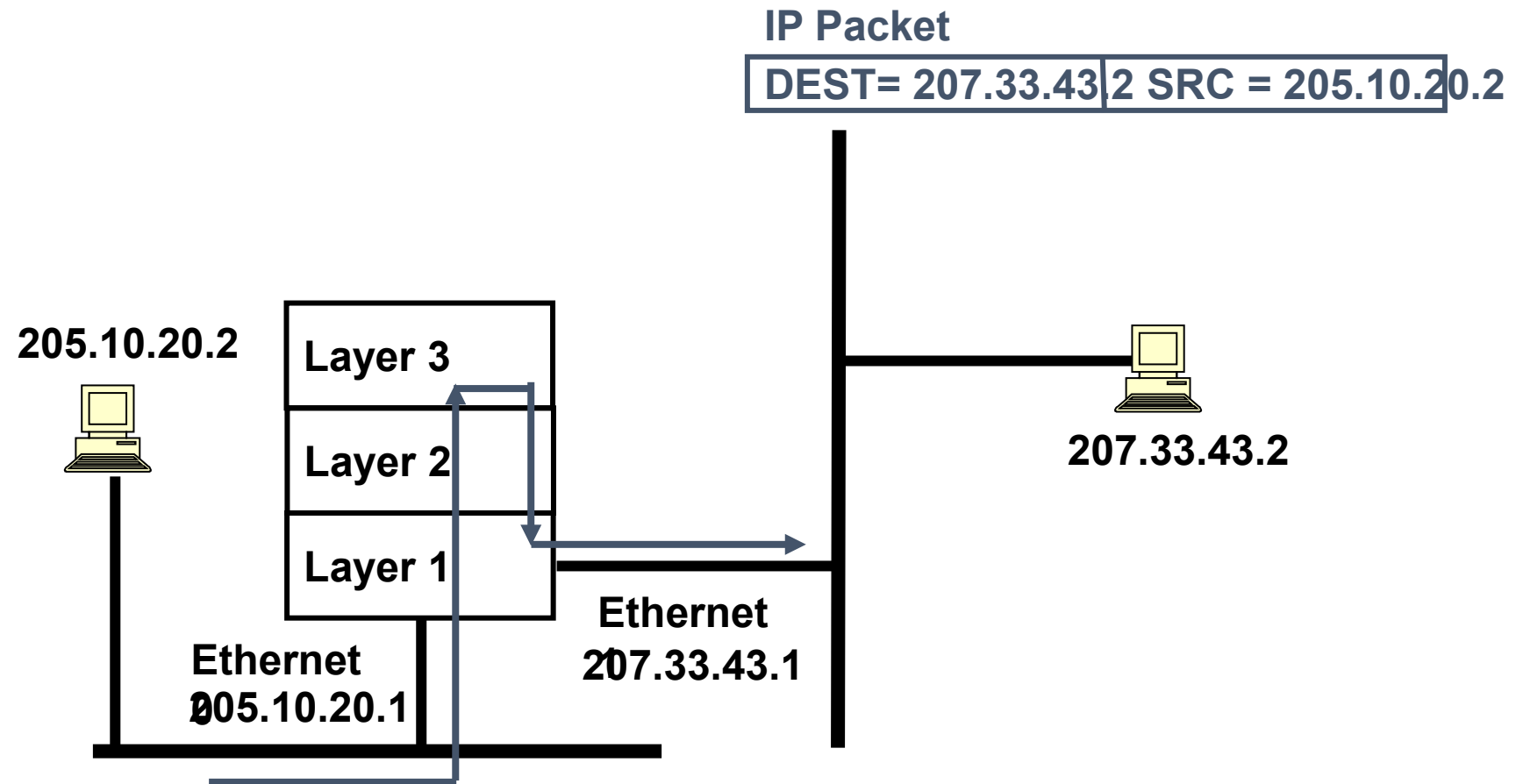
Either the administrator must add all routes to the remote networks, or the router must learn them itself.

VI – Infrastructure: Operations

Packet Forwarding...

- Host on network A **generates packet** for network B
- Host applies network mask to **destination network address of packet** and realises it is on a different network
- Host knows the IP address of the router (Default Gateway), so **recovers the MAC address for the router using ARP**
- Host **encapsulates the packet** in a Layer 2 frame using its own source MAC address and the destination MAC address of the router
- Router receives frame and recognises its own MAC address, so it strips of the **layer 2 framing and passes it to the Layer 3 IP network layer**
- Router **compares destination IP address with router table** to determine the interface by which the packet should be sent
- If the destination network is an Ethernet network directly connected to the router then ARP is used again to determine MAC address of destination host
- Router creates a layer 2 frame using its MAC address for the source and the destination host MAC address

VI – Infrastructure: Operations



VI – Infrastructure: Operations

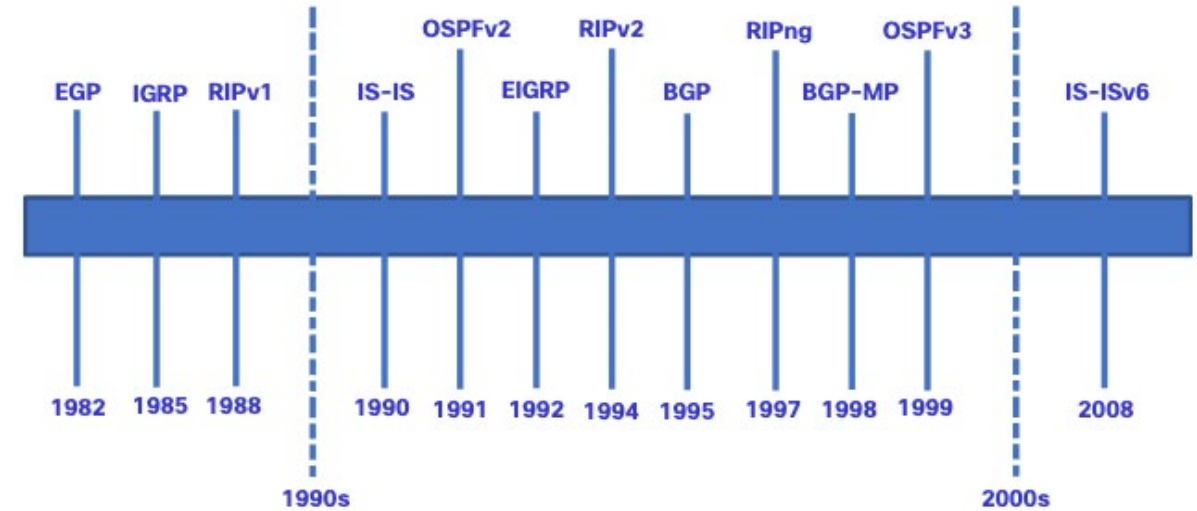
Routing Table...

- Routing table can be configured in many methods.
- **Static:**
 - Routing information is configured manually, no overhead on routers CPU, No bandwidth usage between routers.
 - Security – administrator only configures routes to certain networks
 - Administrator must fully understand the network to create the routing tables correctly, **Not feasible for large networks**
 - If a new network is added all the routers must be configured manually
- **Default:**
 - Used to send packets with a destination network number which doesn't match an entry in the routing table, to the next (default) router.
 - Used for routers on stub networks, which only have one exit from the network segment
- **Dynamic:**
 - To learn routes for themselves, routers must exchange routing information (updates) about the networks they each know about. This information is exchanged by Routing Protocols. If changes occur in the network then the routers inform each other of the change. This process is known as Dynamic Routing.

VI – Infrastructure: Operations

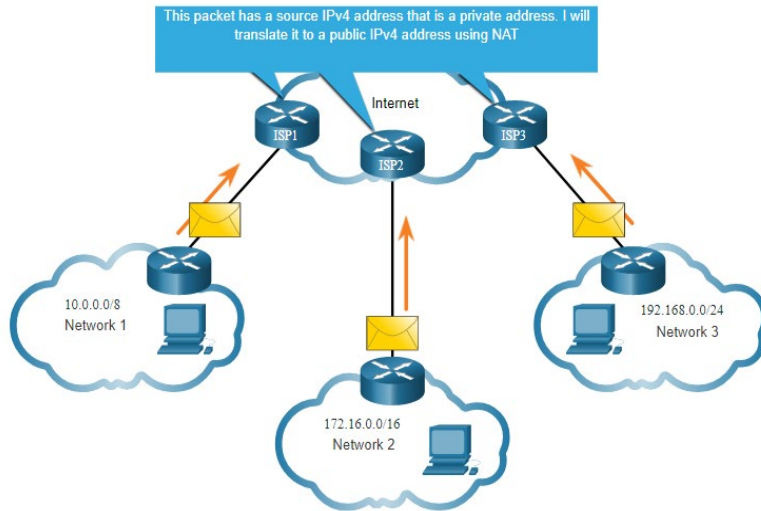
Feature	Dynamic Routing	Static Routing
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed
Path Predictability	Route depends on topology and routing protocol used	Explicitly defined by the administrator

VI – Infrastructure: Operations



	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

VI – Infrastructure: Operations



- ✓ **Network Address Translation (NAT)** translates private IPv4 addresses to public IPv4 addresses.
- ✓ NAT is typically **enabled on the edge router** connecting to the internet.
- ✓ It translates the **internal private address to a public global IP address**.
- ✓ Port Address Translation (PAT)
 - ✓ Translates multiple local IP addresses to a single external IP address supplied by ISP
 - ✓ Remembers source port number used by local machine when requesting a network service (e.g. web)
 - ✓ Responses are routed to correct local machine by looking up port number → now the destination port
- ✓ NAT & PAT can be applied together

VII – Servers

- ☐ Windows Server has evolved from a simple file server to an operating system that is capable of handling network services in complex environments such as corporate networks.
- ☐ Windows Server can provide network services such as domain controllers, web servers, print servers, and file servers.
- ☐ It often acts as a separate platform in which enterprise applications such as Exchange Server, SQL Server, SharePoint Server, and others are executed.
- ☐ With its robust performance and advanced security, nowadays, Windows Server is shaping cloud computing.

VII – Servers: Hardware & Software

- Computer hardware represents physical component of a server and software represents logical component of a server.
- The primary role of the server is to provide network services to the clients, a server requires powerful hardware too, because software such as Windows Server is designed to process large workloads.
- The hardware is required to be **durable and made of high-quality materials** so it can continually deliver services and support network-based operations. Hence, distinguishing it from the ordinary computer, a server needs a higher hardware.
- Servers are also specific to the types of services it provides like; a database server requires more memory and storage space.
- The **CPU, memory, disk, and network** are known to be the key system components that affect the overall performance of your servers.

VII – Servers: Hardware - CPU

- A **Central Processing Unit** (CPU), or processor, is a chip on a server's motherboard. (computer's brain). It is a component that does all the **processing and calculations**.
- Intel and AMD are the biggest CPU manufacturers for PCs and servers. Their newest CPUs on the market are based on 64-bit architecture, which differs from 32-bit architecture-based processors.
- In 64-bit architecture, 64 bits of data are exchanged between the CPU and RAM in each communication session. On the other hand, in 32-bit architecture, only 32 bits of data are exchanged per communication session between RAM and CPU. That is half as less data being communicated via 32-bit architecture as compared to a 64-bit architecture.
- In order to give out the performance, the CPU depend on RAM.

VII – Servers: Hardware – Memory, Disk

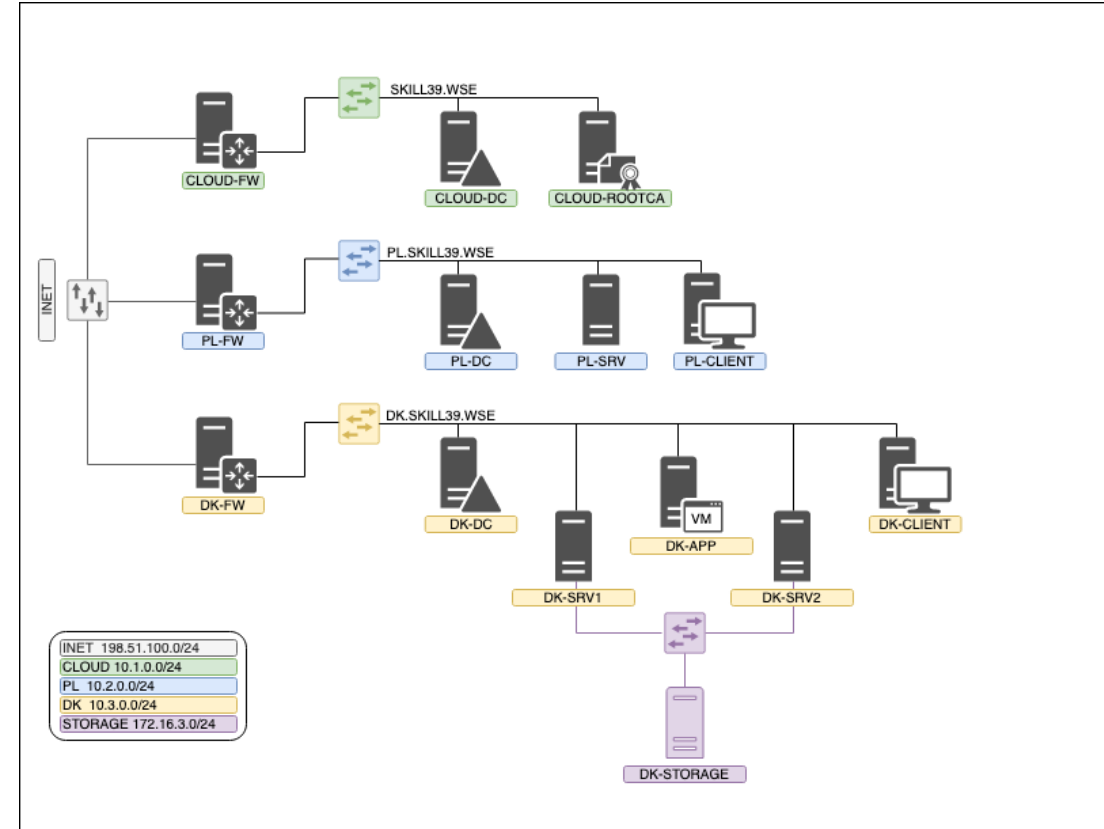
- RAM represents the **server's working memory**, which is used by Windows Server 2022 and server applications. Thus, the more RAM on the server, the more applications can run simultaneously.
- Data is usually stored on a disk. In servers, they mostly have more than one disk, which is referred to as the **server's disk sub-system**. As for disk performance, read/write speed is an element that must be taken into consideration, because the faster the disk's throughput, the higher the performance of your disk sub-system.

VII – Servers: Types

- **Rack-mountable servers** are designed to be installed in a frame called a rack. These servers usually populate on-premises server rooms or data centers:
- **Blade servers** are small modules known as blades that are installed on a server's chassis to save space and power. These servers usually populate data centers or supercomputer facilities.
- **Tower servers** are single big case servers that stand upright. These servers are usually either used for testing purposes or to provide local services in a SOHO.

VIII – Network Operating Systems

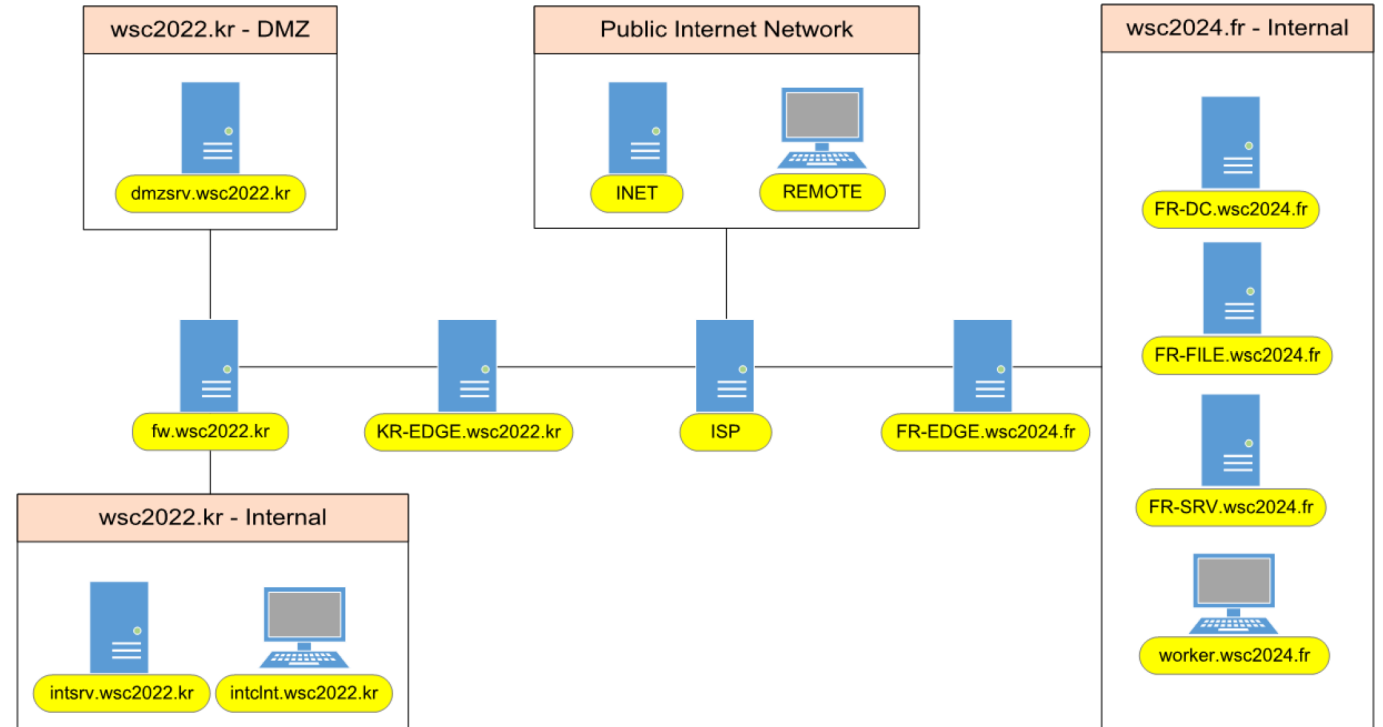
- A **Network Operating System (NOS)** is software
 - manage, maintains and provides resources in a network.
 - manage, maintains and provides access to resources.
 - shares files and applications and provides web services.
 - administers users, computers and provides tools for configuration, maintaining and providing resources, as well as other functions related to network resources.
- ***An NOS could be a Windows Server, Linux Server, and macOS Server as all of them are capable of providing network services.***
- ***A NOS is an important component when it comes to managing computer network resources.***



VIII – Network Operating Systems

FQDN	IP Address	Services	Operating System
ISP	210.103.5.254	---	Debian Linux 11.3 (CUI)
	210.103.5.62		
	210.103.5.126		
KR-EDGE.wsc2022.kr	10.1.1.2	S2S VPN	Debian Linux 11.3 (CUI)
	210.103.5.1		
fw.wsc2022.kr	192.168.1.254	Firewall, DHCP, Remote Access VPN	Debian Linux 11.3 (CUI)
	192.168.2.254		
	10.1.1.1		
intsrv.wsc2022.kr	192.168.1.1	OpenLDAP, FreeRADIUS, SNMP Agent	Debian Linux 11.3 (CUI)
intclnt.wsc2022.kr	DHCP	----	Debian Linux 11.3 (GUI)
dmzsrv.wsc2022.kr	192.168.2.1	DNS, WEB, FTP, MAIL, Monitoring	Debian Linux 11.3 (CUI)
FR-EDGE.wsc2024.fr	172.16.1.254	DHCP, S2S VPN, Web Application Proxy	Windows Server 2019 Datacenter (Core)
	210.103.5.65		
FR-DC.wsc2024.fr	172.16.1.1	DC, Sub CA, ADFS, Remote Desktop, SNMP Agent	Windows Server 2019 Datacenter (GUI)
FR-FILE.wsc2024.fr	172.16.1.2	DC, RAID5, File Server	Windows Server 2019 Datacenter (Core)
FR-SRV.wsc2024.fr	172.16.1.3	WEB, MAIL	Debian Linux 11.3 (CUI)
worker.wsc2024.fr	DHCP (172.16.1.100)	---	Windows 10 Enterprise
INET	210.103.5.129	DNS, WEB, MAIL, Root CA	Debian Linux 11.3 (CUI)
REMOTE	210.103.5.210	---	Windows 10 Enterprise

Logical topology



VIII – Network Operating Systems: Windows

- Windows OS is a Microsoft product. Windows Server powers many organizations' backend systems and provides network services for Windows-based hosts as well as to hosts with a non-Windows OS.
 - 1990's → Windows NT 3.5
 - 2000 → Windows Server 2000. It's a GUI-based OS;
The New Technology File System (NTFS) is the native files system.
 - 2003 → Windows Server 2003 (*architecture: both 32-bit, and 64-bit*)
 - 2008 → Windows Server 2008,
a Server Core edition was introduced, which is a CLI-based OS
 - 2012 → Windows Server 2012 (only 64-bit).
Resilient File System (ReFS) was introduced to replace NTFS.
For more details on ReFS:
<https://docs.microsoft.com/en-us/windows-server/storage/refs/refs-overview>
 - 2016 → Windows Server 2016
 - 2019 → Windows Server 2019 NTFS is a native file system.

VIII – Network Operating Systems: Windows

Server for the masses era 1996-2000	Enterprise era 2000-2008	Datacenter era 2009 - 2013	Cloud for the mass- es era 2016 - present
• Windows NT Server 3.5 • Windows NT Server 4.0	• Windows 2000 Server • Windows Server 2003	• Windows Server 2008 • Windows Server 2012	• Windows Server 2016 • Windows Server 2019

VIII – Network Operating Systems: Linux

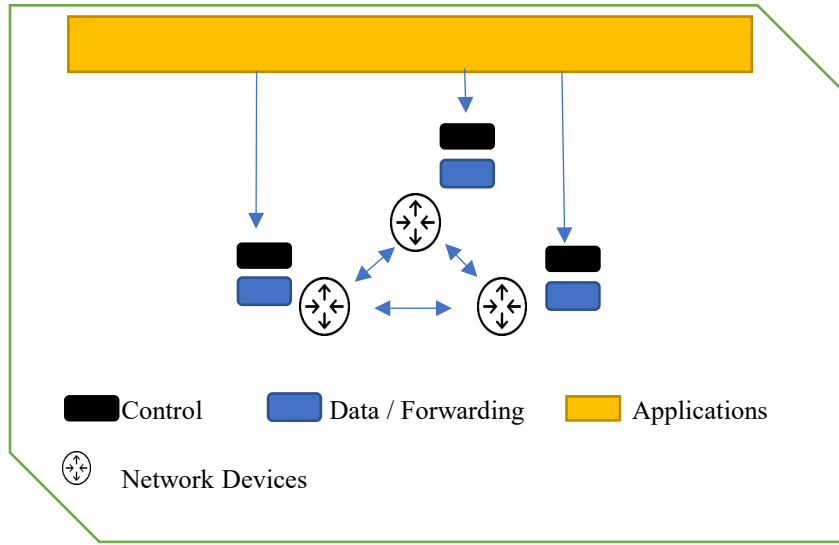
- Linux operating system is unequivocal.
- From MINIX → To improve functionality
- 1990s → Linus Torvalds developed a new operating system called Linux.
- Due to its security and open source nature, Linux Servers dominates majority of web servers and supercomputers.

(the GNU GPL project took over the licensing of Linux, the penguin became a Linux mascot, the first Linux booklet published was Linux Installation and Getting Started)

To know more on how to run Linux distros on Windows Server 2019

<https://docs.microsoft.com/en-us/windows/wsl/install-on-server>.

IX – NOS Services: Existing Network Infrastructure



Legacy Network Architecture

The existing network infrastructure (*addressed as Legacy Networks*)

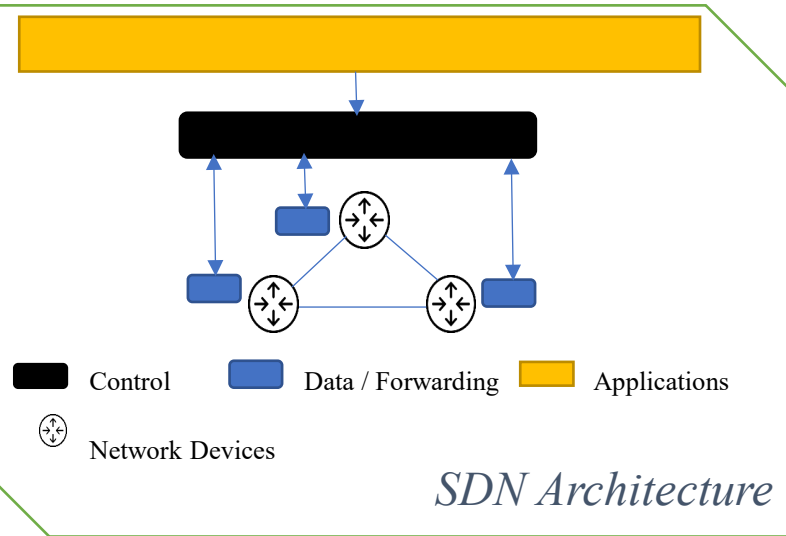
- the IP based protocols are based on the TCP/IP standards which are widely used in network communications.
 - better utilization of all the resources available and focus on all the specification of data starting from data formats, its transmission, addressing, routing till the data being received at the destination.
 - Enabling the existing standards to allow high throughput in the networks.
-
- Automatic reconfiguration and other response mechanisms have no concentration in the existing standards.
 - The communications between networks are heavier which raises the risk of increasing “performance” bottlenecks.
 - In the case of larger network size and during the increase of delay or bandwidth in a network, the potentiality of IP Networking is a big Question.

*The focus now laid on the physical routing devices.
network map & forwarding data packets is in one function.*

IX – NOS Services: SDN

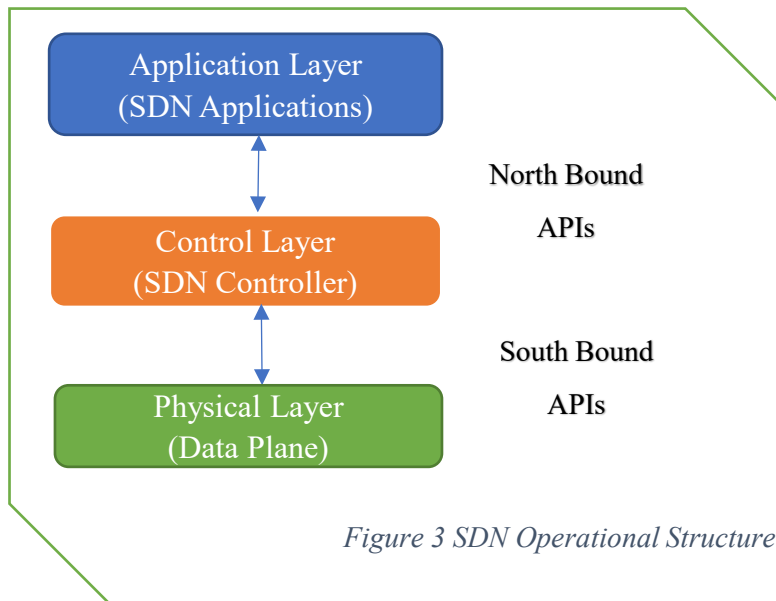
Software Defined Networking

- an upside-down epitome considering the existing network operations.
- a decoupled architecture with centralized control
- very cost effective and complexity impact technology.
- implicate closed networks & vendor specific proprietary implementations.
- Intelligence and flexibility provided to the control plane by decoupling it from data plane.
- This fundamental change in the operation brings linear perspective towards the approach of resolving the existing problems of the IP Networking Architecture.



SDN is a technology which helps in virtualization of physical network devices based on “On Demand” requirements.

IX – NOS Services: SDN



A logical centralized view over the network not only achieving flexibility but also cost efficiency and feasibility

Software Defined Networking

- The SDN architecture is a layered approach classified with three layers.
- The topmost layer is the application layer, where the applications dedicated or designed for the entire network control and operations are residing on various servers.
- The bottom most layer is the Physical Layer or a Data Plane layer which acts as a forwarding engine.
- The arbitrate layer in between the Application Layer and the Physical Layer is the Controller or a Control Plane layer rendering network services for the physical layer.
- The Application and the Control Layer relates to the North Bound Interface.
- The Control Layer and the Physical Layer relates to the South Bound Interface.

Summary

- Networks Components
- Architecture
- IP Addressing
- Infrastructure
- Servers,
- Server hardware and size(CPU, memory, disk, network interface)
- NOS

Diolch/Thank You
Any Questions?