RESUME DE COURS

FILIÈRE SYSTÈMES ET RÉSEAUX

M201 – METTRE EN PLACE UNE INFRASTRUCTURE RÉSEAUX

M202 – ADMINISTRER UN ENVIRONNEMENT WINDOWS

M203 – ADMINISTRER UN ENVIRONNEMENT LINUX

M204 – DÉCOUVRIR LES ENJEUX DE LA TECHNOLOGIE SDN

M205 – ADMINISTRER UN ENVIRONNEMENT CLOUD

M206 – SÉCURISER UNE INFRASTRUCTURE DIGITALE

Réalisé par : AMJOUN MOUAD

Année académique 2023 – 2024

M201 – METTRE EN PLACE UNE INFRASTRUCTURE RÉSEAUX

Modèle OSI et Modèle TCP/IP :

Le modèle OSI (Open Systèmes Interconnexion) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) sont deux modèles de référence utilisés pour décrire et comprendre les protocoles de communication dans les réseaux informatiques.

modèle OSI		Protocoles	modèle TCP/IP	
7	application	HTTP, FTP, SMTP, DNS	4	application
6	présentation	SSL/TLS, MIME		
5	session	NetBIOS, RPC , SSH		
4	transport	TCP , UDP , SCTP	3	transport
3	réseau	IP, ICMP, ARP	2	internet
2	liaison de données	Ethernet (802.3), Wi-Fi (802.11), HDLC, PPP	1	Accés réseau
1	physique	Ethernet, Wi-Fi, ATM, Fibre optique		

Les protocole TCP et UDP :

TCP :est un protocole de communication orienté connexion offrant une transmission fiable des données

UDP :est un protocole de non orienté connexion offrant une transmission plus rapide mais moins fiable

Mask/Mask générique:

/	Mask	Mask générique
24	255.255.255.0	0.0.0.255
25	255.255.255.128	0.0.0.127
26	255.255.255.192	0.0.0.63
27	255.255.255.224	0.0.0.31
28	255.255.255.240	0.0.0.15
29	255.255.255.248	0.0.0.7
30	255.255.255.252	0.0.0.3

UDP/TCP :

protocole	Avantage	inconvenient
TCP	FIABLE	LENT
UDP	RAPAIDE	NON FIABLE

définitions des termes:

DSL (Digital Subscriber Line): Technologie de transmission de données via les lignes téléphoniques traditionnelles.

ADSL (Asymmetric Digital Subscriber Line): Variante de DSL avec des vitesses de téléchargement supérieures aux vitesses de téléversement.

SDSL (Symmetric Digital Subscriber Line) vitesses de téléchargement et de téléversement symétriques.

DSLAM (Digital Subscriber Line Access Multiplexer): Équipement réseau qui agrège les connexions DSL des utilisateurs vers un réseau à haute vitesse.

FTTH (Fiber to the Home): Fibre optique directement jusqu'au domicile de l'utilisateur pour un accès Internet haut débit.

Les ports des communications:

SERVICE	PROTOCOLE	PORTS
TPTP	UDP	69
FTP	TCP	21
POP	TCP	110
SSH	TCP	23
DNS	UDP/UDP	53
DHCP	UDP	68 client 67 server
http	TCP	80
HTTPS	TCP	443
SMTP	TCP	25
IMAP	TCP	143
TELNET	TCP	23
SYSLOG	UDP	514

FTTB (Fiber to the Building): Fibre optique jusqu'au bâtiment, avec une distribution finale via des câbles internes.

FTTN (Fiber to the Node): Fibre optique jusqu'à un nœud de quartier, avec des connexions finales par des câbles en cuivre.

ISP (Internet Service Provider): Fournisseur de services Internet qui offre l'accès à Internet aux utilisateurs.

FAI (Fournisseur d'Accès Internet): Terme français pour ISP, offrant des services de connexion à Internet.

AS (Autonomous System): Réseau ou groupe de réseaux sous un contrôle administratif unique, utilisant un protocole de routage commu

CONFIGURATION DE BASE

- **Mode privilégié :** Router> enable
- **Mode Configuration global:**
- Router# configure terminal
- **sauvegarde de la configuration :**

Router# copy running-config startup-config

- **afficher la ram :** Router# show startup-config
- **Configuration de nom:**

Router(config)# hostname router-name

- **Configuration le mots de passe :**

Router(config)# enable password cisco1234

- **Configuration le mots de passe Crypter :**

Router(config)# enable secret cisco1234

- **Crypter les mots de passe :**

Router(config)# service password-encryption

- **Message de bannière:**

Router(config)# banner motd # message #

- **Configuration d'une adresse MAC statique:**

Switch(config)#mac address-table MAC pc1 vlan1 in f2/1

Désactiver la recherche DNS:

Router(config)# no ip domain-lookup

- **affichier d' adresse MAC :**

Switch# show mac address-table

- **Configuration de vty :**

Router(config)# line vty 0 4 (Switch0 15)
Router(config-line)# password cisco1234
Router(config-line)# login

- **Configuration de la console:**

Router(config)# line console 0
Router(config-line)# password cisco1234
Router(config-line)# login
Router(config-line)# logging synchronous

- **Configuration des interfaces:**

Router(config)# interface[type port]
Router(config-if)# ip address [address ip] [mask]
Router(config-if)# no shutdown
Router(config-if)# exit
Router# show ip interface

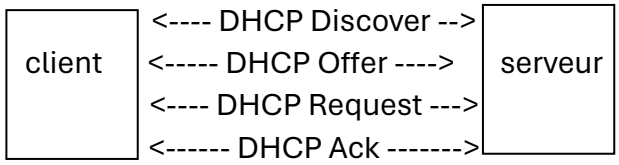
- **Configuration de la sécurité :**

Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum[n]
Switch(config-if)# switchport port-security mac-address sticky [mac-address]
Switch(config-if)# switchport port-security violation shutdown

DHCP

DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer automatiquement des adresses IP et d'autres configurations réseau à des appareils dans un réseau informatique

les principales étapes du processus DHCP



- **Configuration DHCP :**

Router(config)# ip dhcp pool ISTA
Router(dhcp-config)# network 192.168.0.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.0.0
Router(dhcp-config)# dns-server 217.17.17.1
Router(dhcp-config)# domain-name ISTA.MA
Router(config)# ip dhcp excluded-address 192.168.0.1

- **Configuration d'un relais DHCP :**

Router(config-if)# ip helper-address 192.168.2.1 (dhcp)

SSH ET TELNET:

Telnet: est un protocole qui permet l'accès à distance à des systèmes informatiques via une connexion texte

SSH : est un protocole essentiel pour l'accès sécurisé à distance et la gestion des systèmes informatiques.

- **Configuration de telnet :**

Router(config)# username ISTA password cisco1234
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password cisco 1234

- **Configuration de SSH :**

Router(config)#username ISTA password cisco1234
Router(config)#ip domain-name domain-name
Router(config)#ip ssh version 2
Router(config)#crypto key generate rsa
Router(config)#line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# login local

- **Affichier les information ssh:**

Router# show ip ssh

CONCEPTS DE COMMUTATION

Il semble que vous faites référence à deux techniques de commutation dans les réseaux informatiques : "store-and-forward" et "cut-through". Voici ce qu'elles signifient :

Commutation Par stockage et retranssian (store and forward): le commutateur reçoit la trame entière est assure la validité de la trame.

Commutation Parr coupure (Cut-Through) :le commutateur transfert la trame immédotenant après avoir déterminer l'adresse MAC de destination.

LES VLANS

les VLANS sont des outils puissants pour la segmentation et la gestion des réseaux, offrant des avantages tels que la sécurité renforcée, l'optimisation des performances et flexibilité dans le réseaux.

les types des VLANS :vlan par port , vlan par adresse mac , vlan par protocole

▪ **Configuration de VLANs :**

```
Switch(config)# vlan 2
Switch(config-vlan)# name ista
Switch(config)# interface f0/0
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch# show vlan
```

▪ **Configuration l'agrégation de VLANs (Trunk) :**

```
Switch(config)# interface f0/0
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 2
Switch(config-if)# switchport trunk allowed vlan 2
```

▪ **Configuration de Routage inter-vlan:**

```
Router(config)# interface f0/0
Router(config-if)# no shutdown
Router(config-if)# interface f0/0.2
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# ip address[@ ip] [ mask ]
```

▪ **Configuration de l'interface de gestion:**

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address [@ ip ] [mask]
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

VTP

VTP est un protocole utilisé dans les réseaux Cisco pour simplifier la gestion des VLANs en permettant une gestion centralisée et automatique des VLANs.

les modes VTP:

- **mode serveur :** créer, modifier et supprimer des VLANs sur le serveur VTP.
- **mode client :** appliquer les VLANs du serveur VTP sur le commutateur client.
- **mode transparent :** transmettre les mises à jour de VLANs, mais ne permet pas de créer ou de supprimer des VLANs.

Configuration de VTP :

```
Switch(config)# vtp mode {server | client |transparent}
Switch(config)# vtp domain [domain name]
Switch(config)# vtp password [password]
Switch(config)# vtp version 2
Switch(config)# vtp pruning
Switch# show vtp status
Switch# show vtp counters
```

DTP

DTP est un protocole utilisé dans les réseaux informatiques pour automatiquement négocier et configurer les liaisons de trunk entre les commutateurs (switches) d'un réseau.

les modes DTP principaux :

- Dynamic auto
- Dynamic desrible
- trunk
- access

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

SWITCH NIVEAU 3

switch de niveau 3: est un équipement réseau qui combine les fonctionnalités d'un switch et d'un routeur

▪ **Activation de routage de switch de niveau 3 :**

Switch(config)# ip routing

▪ **Afectation d'address ip:**

Switch(config)#int f0/0
Switch(config)#no swich port
Switch(config)# ip address 192.168.0.1
Switch(config)#no shutdown
Switch(config)#exit

▪ **Routage inter vlan de switch niveau 3 :**

Switch(config)# ip routing
Switch(config)# vlan 2
Switch(config)# int vlan 2
Switch(config-if)# ip address 192.168.0.1 255.255.255.0
Switch(config-if)# no shutdown

SPANNING-TREE (STP)

Le Protocole Spanning Tree (STP) fonctionne en identifiant un commutateur racine, en sélectionnant des ports racines et des ports désignés sur chaque commutateur, et en bloquant les autres ports. Cela permet de créer une arborescence sans boucle dans le réseau, ce qui garantit la convergence du trafic et évite les tempêtes de broadcast.

Les étapes de fonctionne protocole STP :

- Élection du commutateur racine (Root Bridge ou RB)
- Détermination du port racine (Root Port ou RP) sur chaque commutateur
- Détermination du port désigné (Designated Port ou DP) sur chaque segment
- Blocage des autres ports

les versions et variantes du Protocol STP :

- STP (Spanning Tree Protocol, IEEE 802.1D)
- RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w)
- MSTP (Multiple Spanning Tree Protocol, IEEE 802.1s)
- PVST (Per-VLAN Spanning Tree, Cisco Proprietary)
- PVST+ (Per-VLAN Spanning Tree Plus, Cisco Proprietary)
- RPVST+ (Rapid Per-VLAN Spanning Tree Plus, Cisco Proprietary)

▪ **Configuration de Rapid-PVST+ :**

Switch(config)# spanning-tree mode rapid-pvst

▪ **Configuration de STP :**

Switch (config)# int f0/1
Switch (config-if)# spanning-tree port fast
Switch(config)# spanning-tree vlan 1root primary
Switch(config)# spanning-tree vlan 1 root secondary
Switch(config)# spanning-tree vlan 1priority [value]
Switch(config)# spanning-tree bpduguard enable
Switch# show spanning-tree [detail | active]

ETHER CHANNEL:

ETHER CHANNEL : Une thechnique de ressau local entre deux commutation permettent de regouper plusieurs port fast ethernet ou gigabite ethernet ou un seul canal logique. EtherChannel utilisé 2 protocole de negociation :

- **PAgP :** est un protocole de Cisco il prend en charge les modes "auto" et "desirable".
- **LACP :** est un protocole de standard Il prend en charge les modes "active" et " passive ".

protocol	Link A mode	Link B mode	Negotiation result
PAGP	Auto	Auto	No negotiation
	Auto	Desirable	Negotiation successful
	Auto	On	No negotiation
	Desirable	Desirable	Negotiation successful
LACP	Passive	Passive	No negotiation
	Passive	Active	Negotiation successful
	Passive	On	No negotiation
	Active	Active	Negotiation successful
forcer	on	on	Negotiationsuccessful

Restricton d'implémenté de ETHER CHANNEL :

- Même cable
- Même configuration
- Même vitasse
- Même longeuer

▪ **Configuration Ether channel :**

```
Switch1(config)# interface range fa0/1 - 4
Switch1(config-if-range)# channel-group 1 mode on
Switch1(config-if-range)# int port-channel 1
Switch1(config-if-range)# switchport mode trunk
```

```
Switch2(config)# interface range fa0/1 - 4
Switch2(config-if-range)# channel-group 1 mode on
Switch2(config-if-range)# int port-channel 1
Switch2(config-if-range)# switchport mode trunk
```

LES PROTOCOLES DE REDONDANCE DE PASSERELLE PAR DEFAUT (FHRP)

FHRP : (First Hop Redundancy Protocol) Ils permettent à plusieurs routeurs de se partager le même adresse IP de passerelle par défaut, garantissant ainsi la redondance et la résilience du réseau en cas de panne d'un routeur._Voici quelques-uns des protocoles FHRP les plus couramment utilisés :

- **HSRP (Hot Standby Router Protocol) :** Développé par Cisco, HSRP est un protocole de routage de passerelle par défaut qui permet à plusieurs routeurs de fonctionner ensemble dans un groupe HSRP.

Les étapes de HSRP : actif(active) , Standby , listen

- **VRRP (Virtual Router Redundancy Protocol) :** est un protocole de routage de passerelle par défaut standardisé par l'IETF.
- **GLBP (Gateway Load Balancing Protocol) :** Aussi développé par Cisco, GLBP est un protocole de routage de passerelle par défaut qui va au-delà de la simple redondance et offre également la capacité de répartir la charge entre plusieurs routeurs actifs dans un groupe GLBP.

▪ **Configuration HSRP :**

```
Router1(config)# int f0/0
Router1(config)#stand by 10 ip 192.168.0.254
Router1(config)# stand by 10  priority 150
Router1(config)# stand by 10 preempt
Router2(config)# int f0/0
Router2(config)#stand by 10 ip 192.168.0.254
Router2(config)# stand by 10  priority 100
Router2(config)# stand by 10 preempt
```

▪ **Configuration GLBP :**

```
Router1(config)# int f0/0
Router1(config)#stand by 10 ip 192.168.0.254
Router1(config)# stand by 10  priority 150
Router1(config)# stand by 10 preempt
Router1(config)# stand by 10 lood-balancing roud-robin
Router2(config)# int f0/0
Router2(config)#stand by 10 ip 192.168.0.254
Router2(config)# stand by 10  priority 100
Router2(config)# stand by 10 preempt
Router2(config)# stand by 10 lood-balancing roud-robin
```

LE ROUTAGE

Le routage est le processus de transfert de données d'un réseau à un autre à travers des dispositifs appelés routeurs. Ces routeurs utilisent des informations de routage pour déterminer le chemin optimal pour acheminer les données vers leur destination.il y a deux types de routage statiques et dynamique.

Distance administrative de routage

Source de routage	Distance administrative (AD)
Route directement connectée	0
Route statique	1
BGP	externe 20 interne 200
EIGRP	interne 90 externe170
OSPF	110
RIP	120

▪ Routage statiques

le routage statique : implique une configuration manuelle des routes et est adapté aux réseaux

Avantages du routage statique :

- Simplicité
- Moins de surcharge réseau
- Contrôle précis

▪ **Configuration de routes statiques** :

Router(config)#ip route 192.168.0.0 255.255.255.0 192.168.1.1

▪ **Vérification de la table de routage:**

Router# show ip route

▪ **changer la distance administrative:**

Router(config)#ip route 192.168.0.0 255.255.255.0 192.168.1.1 70

▪ **Configuration route statique par défaut :**

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

▪ **propagation de la route par défaut :**

Router(config-router)# default-information originate

▪ Routage dynamique

le routage dynamique : utilise des protocoles de routage pour échanger automatiquement des informations de routage et s'adapter aux changements de topologie , Voici quelques-uns des principaux protocoles de routage dynamique utilisés dans les réseaux informatiques :OSPF ,RIP ,EIGRP ,BGP

Avantages du routage dynamique : Adaptabilité ,Évolutivité ,Résilience

1. Le protocole de routage dynamique RIP

RIP est un protocole de routage simple et facile à configurer, adapté aux petits réseaux où les exigences de performances ne sont pas trop élevées.

▪ **Configuration de RIP :**

Router(config)# router rip
Router(config-router)# network 192.168.0.0
Router(config-router)# version 2

▪ **changer la distance administrative:**

Router(config-router)#destance 70

2. Le protocole de routage dynamique OSPF

OSPF (Open Shortest Path First) est un protocole de routage dynamique puissant et largement adopté, adapté aux environnements de réseaux de grande taille nécessitant une convergence rapide et une haute résilience. Sa capacité à diviser les réseaux en zones hiérarchiques et à sécuriser les échanges de messages de routage en fait un choix préféré pour les réseaux d'entreprise et les fournisseurs de services.

Fonctionnement d'OSPF :

1. Établissement des voisinages: Les routeurs OSPF établissent des relations de voisinage avec les routeurs adjacents en échangeant des messages Hello. Ces messages permettent de découvrir les routeurs voisins et de vérifier l'état des liaisons.

2. Base de Données des États de Liaison (LSDB): Chaque routeur maintient une LSDB, une carte complète de la topologie du réseau, qui est mise à jour par les LSA (Link State Advertisements). Les LSAs sont échangés entre les routeurs pour partager les informations sur les liaisons réseau.

3. Calcul du chemin le plus court: En utilisant les informations de la LSDB, chaque routeur exécute l'algorithme de Dijkstra pour calculer le chemin le plus court vers chaque destination. Le résultat de ce calcul est la table de routage.

4. Zones et segmentation: OSPF divise un réseau en plusieurs zones pour réduire la charge de calcul et la taille de la LSDB. Chaque zone est interconnectée via la zone backbone (Zone 0).

Avantages de OSPF : Scalabilité, Convergence rapide, Sécurité
Inconvénients de OSPF: Complexité, Utilisation des ressources

- **Configuration d'OSPF :**

Router(config)# router ospf 10
Router(config-router)# network 192.168.0.0 0.0.0.255 area 0

- **changer la priorité de ospf:**

Router(config)# int f0/0
Router(config-if)#ip ospf priority 50

- **Configuration route par défaut ospf:**

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2

- **propagation de la route par défaut ospf**

Router(config)# router ospf 10
Router(config-router)# default-information originate

- **Configuration une interface loopback:**

Router(config)#interface loopback 0
Router(config-if)#ip address 192.168.1.7 255.255.255.0

- **Configuration de la bande passante d'OSPF :**

Router(config-router)# auto-cost reference-bandwidth 1000

- **Configuration de la bande passante interface :**

Router(config)# int f0/0
Router(config-if)# bandwidth 64

- **Configuration de la cout :**

Router(config)# int f0/0
Router(config-if)# ip ospf cost 156

- **Configuration de la valeur des conteur:**

Router(config)# int 2/0
Router(config-if)# ip ospf hello-interval 5
Router(config-if)# ip ospf dead-interval 20

- **Désactive la mises ajour dons l'interface:**

Router(config)# router ospf 10
Router(config-router)#passive-interface s2/0

- **Configuration le router ID de ospf:**

Router(config-router)# router-id 1.1.1.1

3. Le protocole de routage dynamique EIGRP:

EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage avancé de Cisco qui utilise une combinaison de caractéristiques des protocoles de vecteur de distance et d'état de lien pour offrir une convergence rapide et une efficacité de routage. Il emploie l'algorithme DUAL (Diffusing Update Algorithm) pour calculer les chemins les plus courts et garantir des mises à jour de routage fiables et optimisées.

- **Configuration d'EIGRP :**

Router(config)# router eigrp 10
Router(config)# eigrp router-id 1.1.1.1`
Router(config-router)# network 192.168.0.0 0.0.0.255
Router(config-router)# no auto-summary

4. Le protocole de routage dynamique BGP:

BGP (Border Gateway Protocol) est un protocole de routage externe utilisé pour échanger des informations de routage entre systèmes autonomes (AS) sur Internet. Il détermine les meilleurs chemins basés sur des politiques et des attributs de routage, assurant ainsi l'interconnexion globale et la stabilité du réseau.

- **Configuration d'BGP :**

Router1(config-router)# neighbor 192.168.1.1 remote-as 6500
Router2(config)# router bgp 6500
Router2(config-router)# network 192.168.0.0 mask 255.255.255.0

LES ACL

Les Listes de Contrôle d'Accès (ACL, Access Control Lists) sont des outils de sécurité utilisés pour contrôler le trafic réseau en autorisant ou en bloquant des paquets en fonction de divers critères tels que les adresses IP source et destination, les ports, et les protocoles. Les ACL sont principalement utilisées sur les routeurs et les pare-feux pour sécuriser et gérer le flux de trafic à travers un réseau.

Les Types d'ACL:

- **ACL standard :**
  - Filtre le trafic uniquement sur la base de l'adresse IP source.

- Numéros de 1 à 99 et 1300 à 1999

- **ACL étendue :**
  - Filtre le trafic en fonction de l'adresse IP source et destination, du type de protocole (TCP, UDP, ICMP, etc.), et des ports source et destination.
  - Numéros de 100 à 199 et 2000 à 2699.

Les méthodes pour configurer des ACL sur des routeurs et commutateurs :

- **ACL Numérotées :** Les ACL numérotées utilisent des numéros pour identifier les listes d'accès. Les ACL standard et étendues ont des plages de numéros spécifiques.
- **ACL Nommées :** Les ACL nommées utilisent des noms au lieu de numéros, ce qui permet de mieux décrire l'objectif de l'ACL et de faciliter la gestion des règles

▪ **Configuration d'une ACL standard numerotée:**

```
Router(config)# access-list 1 deny 192.168.2.0 0.0.0.255
Router(config)# access-list 1 host 192.168.3.3
Router(config)# access-list 1permit any
Router(config)# int f0/0
Router(config-if)# ip access-group 1 in | out
Router# show access-lists
```

▪ **Configuration d'une ACL standard nommée :**

```
Router(config)# ip access-list standard ista
Router(config-std-nacl)#deny host 192.168.0.2
Router(config-std-nacl)# permit any
Router(config)# int f0/0
Router(config-if)# ip access-group  ista in| out
```

▪ **Configuration d'une ACL étendue numerotée:**

```
Router(config)# access-list 100 deny TCP 192.168.3.0 0.0.0.255 host 192.168.0.4 eq80
Router(config)# access-list 100 deny UDP 192.168.2.0 0.0.0.255 host 192.168.0.4 eq443
Router(config)# access-list 100 permit  ip any any
Router(config)# int f0/0
Router(config-if)# ip access-group 100 in | out
```

▪ **Configuration d'une ACL étendue nommée :**

```
Router(config)# ip access-list extended ista
Router(config-ext-nacl)# deny tcp host 192.1687.0.3 host 192.168.2.1 eq80
Router(config-std-nacl)# permit ip any any
Router(config)# int s2/0
Router(config-if)# ip access-group ista in| out
```

▪ **Interder le ping:**

```
Router(config)# access-list 101 deny ICMP host 192.168.0.2 host [@ip pc 2] echo |echo-reply
Router(config)# access-list 101 permit ip any any
Router(config)# int f0/0
Router(config-if)# ip access-group 101 in | out
```

NAT ET PAT

NAT (Network Address Translation) : est une méthode qui permet de modifier les adresses IP dans les paquets réseau en cours de transit. Il existe plusieurs types de NAT :

- **Static NAT (NAT statique) :**
  - Associe une adresse IP privée à une adresse IP publique fixe.
  - Utilisé pour rendre des ressources internes (comme des serveurs) accessibles depuis l'extérieur.

- **Dynamic NAT (NAT dynamique) :**
  - Utilise un pool d'adresses IP publiques et associe dynamiquement des adresses IP privées à celles-ci.
  - Utilisé pour mapper des adresses IP privées à un ensemble limité d'adresses IP publiques.

PAT (Port Address Translation) : une forme de NAT, est souvent appelée NAT Overload. Elle permet à plusieurs adresses IP privées d'utiliser une seule adresse IP publique en distinguant les connexions par les numéros de port.

- **Configuration de la NAT:**

```
Router(config)# ip nat pool ista 41.41.41.41.1 41.41.41.30 netmask 255.255.255.0
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool ista
Router(config)# interface f0/0
Router(config-if)# ip nat inside
Router(config)# interface s2/0
Router(config-if)# ip nat outside
```

- **Configuration de la PAT:**

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface s2/0 overload
 Router(config)# interface f0/0
Router(config-if)# ip nat inside
Router(config)# interface s2/0
Router(config-if)# ip nat outside
```

- **Configuration de la NAT+PAT:**

```
Router(config)# ip nat pool ista 41.41.41.41.1 41.41.41.30 netmask 255.255.255.0
Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool ista overload
Router(config)# interface f0/0
Router(config-if)# ip nat inside
Router(config)# interface s2/0
Router(config-if)# ip nat outside
```

- **Configuration de la NAT statique :**

```
Router(config)# ip nat inside source static 192.168.0.2 31.31.31.1
Router(config)# interface f0/0
Router(config-if)# ip nat inside
Router(config)# interface s2/0
Router(config-if)# ip nat outside
```

IPV6

Les adresses IPv6 (Internet Protocol version 6) représente la prochaine génération de protocoles Internet, offrant une solution aux limitations de l'IPv4 en termes d'espace d'adressage et d'améliorations fonctionnelles. Son adoption continue de croître à mesure que les besoins en adresses IP augmentent.
Voici des exemples d'adresses IPv6 :

Adresse Unicast Globale : 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Adresse Unicast Link-Local : fe80::1

- **Activier le routage ipv6:**

```
Router(config)# ipv6 unicast-routing
```

- **Configuration interface ipv6:**

```
Router(config)# interface G0/0
```

- **Configuration route par défaut ipv6 :**

```
Router(config)# ipv6 route ::/0 2001:A:B::2
```

- **propagation de la route par défaut :**

```
Router(config)# interface s0/0/0
```

Router(config-if)# ipv6 address 2001:A:A::1/64
Router(config-if)# ipv6 address FE80::1 link-local
Router(config-if)# no shutdown
Router(config)# interface S0/0/0
Router(config-if)# ipv6 address 2001:A:B::1/64
Router(config-if)# ipv6 address FE80::1 link-local
Router(config-if)# no shutdown

- **Configuration de routes statiques ipv6** :

Router(config)#ipv6 route 2001:A:C::1/64 2001:A:B::2
Router#show ipv6 route

- **Configuration de RIPng ipv6:**

Router(config)# interface G0/0
Router(config-if)# ipv6 rip ISTA enable
Router(config)# interface S0/0/0
Router(config-if)# ipv6 rip ISTA enable
Router(config-if)# ipv6 rip ISTA default-information orginate

- **Configuration de OSPF v3 ipv6:**

Router(config)# ipv6 router ospf 10
Router(config-rtr)# router-id 1.1.1.1
Router(config)# interface G0/0
Router(config-if)# ipv6 OSPF 10 area 0
Router(config)# interface S0/0/0
Router(config-if)# ipv6 OSPF 10 area 0

- **Configuration d'une ACL ipv 6 :**

Router(config)# ipv6 access-list ISTA
Router(config-ipv6-acl)# deny TCP 2001:A:A::/64 host 2001:A:C::4 eq 80
Router(config-std-nacl)# permit ipv6 any any
Router(config)# int g0/0
Router(config-if)# ipv6 trafic filter ista in
Router# show ipv6 access-lists

configuration dynamique d'adresse ipv6

Pour configurer la adresse ipv6 dynamique , il y a 3 méthodes :

1. **SLAAC (Stateless Address Autoconfiguration) :**
   - Les appareils génèrent leurs propres adresses IPv6 à partir du préfixe annoncé par le routeur et leur identifiant de l'interface.
   - Utilisé pour les configurations rapides et simples où les appareils se configurent automatiquement sans intervention supplémentaire.
2. **DHCPv6 Stateless (sans états):**
   - Utilisé en conjonction avec SLAAC.
   - Le routeur annonce les préfixes, et DHCPv6 fournit des informations supplémentaires comme les serveurs DNS et le domaine.
3. **DHCPv6 Stateful (avec états) :**
   - Le serveur DHCPv6 attribue des adresses IPv6 et d'autres informations de configuration.
   - Utilisé pour les configurations où une gestion plus stricte des adresses est nécessaire.

Le processus EUI-64 : (Extended Unique Identifier-64) est une méthode utilisée dans IPv6 pour générer automatiquement des identifiants d'interface uniques à partir des adresses MAC des interfaces réseau. est combinée avec le préfixe IPv6 de l'interface pour former l'identifiant d'interface IPv6..

Exemple de Processus EUI-64 :

Supposons que l'adresse MAC de l'interface soit `00:1A:2B:3C:4D:5E` et que le préfixe IPv6 de l'interface soit `2001:db8:1234:5678::/64`.

1. Préparation de l'Adresse MAC:
- Première partie (24 bits) : `001A2B`
- Deuxième partie (24 bits) : `3C4D5E`

2. Insertion du Préfixe EUI-64 :
- Deuxième partie après le préfixe EUI-64 : `FF:FE:3C4D:5E`

3. Inversion du Bit U/L:
- Le septième bit est inversé, donc `3C4D` devient `3D4D`.

4. Construction de l'Identifiant d'Interface IPv6 :
- Identifiant d'interface IPv6 : `3D4D:5EFF:FE3C:4D5E`

5. Formation de l'Adresse IPv6 :

- Adresse IPv6 complète : `2001:db8:1234:5678:3D4D:5EFF:FE3C:4D5E`

▪ **Configuration de la DHCPV6 sans états :**

```
Router(config)# ipv6 unicast-routing
Router(config)# ipv6 dhcp pool ista
Router(config-dhcp)# domain-name ista.ma
Router(config-dhcp)# dns-server 2001:A:A::10
Router(config)# interface fa 0/1
Router(config-if)# ipv6 dhcp server ista
Router(config-if)# ipv6 nd other-config-flag
```

▪ **Configuration de la DHCPV6 avec états :**

```
Router(config)# ipv6 dhcp pool ista
Router(config)# address prefix 2001:A:B::/64 lifetime infinite
Router(config-dhcp)# domain-name ista.ma
Router(config-dhcp)# dns-server 2001:A:A::10
Router(config)# interface fa 0/1
Router(config-if)# ipv6 dhcp server ista
Router(config-if)# ipv6 nd manged-config-flag
```

NTP

Le protocole NTP (Network Time Protocol) est utilisé pour synchroniser les horloges des ordinateurs à travers un réseau. Une configuration correcte de NTP est cruciale pour de nombreuses applications, y compris les logs, la sécurité, et la gestion des réseaux.

▪ **Configuration de la NTP:**

```
Router1(config)# ntp master 1
Router2(config)# ntp server 192.168.0.1
Router1#clock set 13:00:01 5 march 2023
Router2#show clock detail
Router2#show ntp passociations | ntp status
```

SYSLOGE

Syslog est un protocole standard utilisé pour envoyer des messages de journalisation (logs) à un serveur central appelé serveur Syslog. Les dispositifs réseau, tels que les routeurs et les switches Cisco, ainsi que les systèmes informatiques, peuvent utiliser Syslog pour enregistrer divers types de messages, y compris les erreurs, les avertissements, les notifications et les informations de débogage

logging trap [level] : Définit le niveau de sévérité des messages à envoyer au serveur Syslog. Les niveaux couramment utilisés incluent :

- **emergencies (0)** : Systèmes inutilisables.
- **alerts (1)** : Actions doivent être prises immédiatement.
- **critical (2)** : Conditions critiques.
- **errors (3)** : Conditions d'erreur.
- **warnings (4)** : Conditions d'avertissement.
- **notifications (5)** : Conditions normales mais significatives.
- **informational (6)** : Messages informatifs.
- **debugging (7)** : Messages de débogage.

▪ **Configuration de la Sysloge:**

```
Router(config)# service time tamps log date time
Router(config)# logging host[@ip]
Router(config)# logging trap debugging
```

SNMP

SNMP (Simple Network Management Protocol) est un protocole utilisé pour gérer et surveiller les dispositifs réseau tels que les routeurs, les switches, les serveurs, les imprimantes, etc. SNMP permet aux administrateurs de collecter des informations sur les périphériques réseau et de les gérer de manière centralisée

▪ **Configuration de la SNMP:**

```
Router(config)#snmp-server community [NAME] ro
```

PPP

PPP (Point-to-Point Protocol) est un protocole utilisé pour établir une connexion directe entre deux nœuds de réseau. Il est couramment utilisé sur les lignes série, les lignes téléphoniques et autres types de connexions de réseau. PPP supporte plusieurs méthodes d'authentification, dont les deux principales sont PAP (Password Authentication Protocol) et CHAP (Challenge Handshake Authentication Protocol).

Configuration de PAP :

```
R1(config)#username R2 pasword cisco2
R1(config)# interface s2/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication  pap
R1(config-if)#ppp pap sent- username R1 pasword cisco1
R2(config)#username R1 pasword cisco1
R2(config)# interface s2/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication  pap
R1(config-if)#ppp  pap sent- username R2 pasword cisco2.
```

Configuration de CHAP :

```
R1(config)#username R2 pasword cisco
R1(config)# interface s2/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R2(config)#username R1 pasword cisco
R2(config)# interface s2/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication  chap
R1#show interface s2/0
```

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) est un protocole qui encapsule PPP dans des trames Ethernet. Il est principalement utilisé pour établir une connexion point-à-point entre un client et un serveur sur une infrastructure Ethernet.

- **configration PPPOE:**

```
Router(config)# interface f0/0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# pppoe enable
Router(config-if)# no shutdown
Router(config)#int virtual – templates 1
Router(config)#ip unnumbered f0/0
Router(config)#peer default ip address Pool ISTA
Router(config)#ppp authentication chap
Router(config)#vpdn enable
Router(config)# vplan-group OFPPT
Router(config)#accept-dialer
Router(config)# protocole pppe
Router(config)#virtual-template 1
Router(config)#lp local Pool [name] 10.1.1.10 10.1.1.20
Router(config)#username [name] password CISCO
```

LLDP

LLDP (Link Layer Discovery Protocol) est un protocole standardisé de couche 2 utilisé pour la découverte des voisins réseau et le partage des informations entre les dispositifs voisins. Contrairement à CDP, qui est spécifique à Cisco, LLDP est un protocole ouvert et peut être utilisé avec une variété d'équipements réseau de différents fabricants. Il est largement utilisé dans les environnements réseau pour la gestion et le dépannage

- **configuration LLDP :**

```
Router(config)#LLdp run
Router#show LLdp reighdrs
```

CDP

CDP (Cisco Discovery Protocol) est un protocole propriétaire développé par Cisco pour la découverte et la surveillance des dispositifs Cisco sur un réseau local. Il fournit des informations utiles sur les dispositifs voisins et est largement utilisé dans les environnements réseau Cisco pour la gestion et le dépannage

- **configuration CDP :**

```
Router(config)#cdp run
Router(config)# interface s2/0
Router(config)# cdp Enable
Router(config)# interface f0/0
Router(config)# cdp Enable
```

Router#show cdp reighdrs

VPN

VPN (virtuel privet network) crée une connexion sécurisée et chiffrée entre deux réseaux ou entre un utilisateur et un réseau, en utilisant Internet comme infrastructure de transport.

Types de VPN :

1. VPN d'accès distant :
    - Permet aux utilisateurs individuels de se connecter à un réseau privé depuis n'importe où dans le monde, généralement via un logiciel VPN sur leur ordinateur ou leur appareil mobile.
2. VPN site à site :
    - Établit une connexion sécurisée entre deux réseaux locaux, tels que les bureaux distants d'une entreprise ou les succursales.
3. VPN basé sur le cloud :
    - Les services VPN hébergés sur des serveurs cloud offrent une solution pratique pour les petites entreprises ou les utilisateurs individuels sans avoir à configurer ou à gérer leur propre infrastructure VPN

Avantages de VPN:

• Réduction des coûts
• Sécurité
• Évolutivité
• Compatibilité avec la technologie haut-débit

▪ **configuration vpn:**

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash sha
Router(config-isakmp)# encryption
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp key cisco address 192.168.2.2
Router(config)#crypto ipsec transform-set ista esp-des esp-md5-hmac
Router(config)#crypto map IPSECMAP 10 ipsec-isakmp
Router(config-crypto)#set peer 192.168.2.2
Router(config-crypto)#match address 110
Router(config-crypto)#exit
Router(config)#interface s2/0
Router(config-if)#crypto map vpnmap
Router(config-if)#exit
Router(config-if)#access-list 101 permit ip 192.168.3.0 0.0.0.255
```

GRE

GRE (Generic Routing Encapsulation) est un protocole de tunnelisation largement utilisé dans les réseaux informatiques. Il permet d'encapsuler des paquets de données de divers protocoles réseau dans des paquets IP standard pour les transmettre sur un réseau IP.

▪ **configuration GRE :**

```
Router(config)#interface Tunnel 0
Router(config)#tunnel mode gre ip
```

Router(config)#ip address 192.168.4.1 255.255.255.0
Router(config)#tunnelsource s2/0
Router(config)#Tunnel destination 192.168.2.2

IPSEC

IPsec (Internet Protocol Security)est un protocole essentiel pour sécuriser les communications sur les réseaux IP. Grâce à ses capacités de cryptage, d'authentification et d'intégrité des données, IPsec est largement utilisé pour établir des VPN sécurisés, interconnecter des réseaux distants et protéger les communications sensibles. Malgré sa complexité de configuration, il reste un choix populaire pour les organisations cherchant à garantir la sécurité de leurs communications réseau.

Fonctionnalités d'IPsec :

1. **Confidentialité des données** :
   - IPsec chiffre les données pour les protéger contre les interceptions non autorisées.
2. **Authentification des données** :
   - IPsec vérifie l'identité des dispositifs qui communiquent entre eux pour s'assurer que les données proviennent de sources fiables.
3. **Intégrité des données** :
   - IPsec utilise des mécanismes pour vérifier que les données n'ont pas été modifiées pendant leur transit.
4. **Protection contre les attaques de rejeu** :
   - IPsec utilise des numéros de séquence et des vérifications de temps pour empêcher la réinjection de paquets interceptés.

Protocoles principaux :

- **AH (Authentication Header)** : Fournit des services d'authentification et d'intégrité des données, mais ne chiffre pas les données.
- **ESP (Encapsulating Security Payload)** : Fournit des services de chiffrement, d'authentification et d'intégrité des données.

VOIP

VoIP (Voice over Internet Protocol) est une technologie qui permet de transmettre des communications vocales et multimédia sur Internet ou d'autres réseaux basés sur le protocole IP. Voici une vue d'ensemble de VoIP, ses composants, ses avantages, ses inconvénients et ses utilisations courantes.

Avantages de VoIP :

1. **Réduction des coûts :**Les appels VoIP sont généralement moins coûteux que les appels téléphoniques traditionnels, surtout pour les longues distances et les appels internationaux.
2. **Flexibilité et mobilité :**Les utilisateurs peuvent passer et recevoir des appels de n'importe où avec une connexion Internet.
3. **Fonctionnalités avancées :**VoIP offre des fonctionnalités telles que la messagerie vocale, l'identification de l'appelant, le transfert d'appels, les conférences téléphoniques, et l'intégration avec d'autres services de communication (ex. messagerie instantanée, vidéo).

▪ **configuration VOIP :**

R1(config)# ip dhcp pool ista
R1(dhcp-config)# network 192.168.0.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.0.1
R1(dhcp-config)# option 150 ip 192.168.0.2
S3(config)# interface rqng f0/1-24
S3(config-if)# switchport access vlan 20
R1(config)#telphony-srvice
R1(config-telphony)#max-ephone 10

R1(config-telphony)#max dn10
R1(config-telphony)#ip source-address 192.168.0.2 port 2000
R1(config-telphony)#auto assign 1 to 10
R1(config-telphony)#create cnf
R1(config-telphony)#exit
R1(config)#ephone-dn1
R1(config-ephone-dn1)# number1001
R1(config)#ephone-dn2
R1(config-ephone-dn1)# number1002

- **La routage de la voie ip :**

Router1(config)# dial-peer voice 1 voip
Router1(config-dialpeer)# destination-pattern 2...
Router1(config-dialpeer)# session target ipv4: 10.0.0.2

- **Configurer les phones manuellement**

R1(config)#ephone1
R1(config-ephone)# mac address @ mac ephone
R1(config-ephone)# buton 1:1

Wi-Fi

Wi-Fi (Wireless Fidelity), ou réseaux Les réseaux sans fil, sont des réseaux de communication qui permettent la transmission de données sans l'utilisation de câbles physiques.

Types de Réseaux Sans Fil :

1. WLAN (Wireless Local Area Network):
- Utilisé pour connecter des appareils à courte distance, généralement dans un bâtiment ou un campus.
- Norme la plus courante : IEEE 802.11 (Wi-Fi).

2. WPAN (Wireless Personal Area Network):
- Utilisé pour les connexions à très courte portée, généralement autour d'une personne.
- Exemples : Bluetooth (IEEE 802.15), Zigbee.

3. WWAN (Wireless Wide Area Network) :
- Utilisé pour les connexions à longue distance, couvrant des zones géographiques étendues.
- Exemples : Réseaux cellulaires (3G, 4G, 5G), WiMAX (IEEE 802.16).

4. WMAN (Wireless Metropolitan Area Network) :
- Utilisé pour les connexions sans fil à moyenne portée, couvrant une ville ou une métropole.
- Exemple : WiMAX.

Normes Wi-Fi :

Normes	Fréquence	Débit maximal
IEEE 802.11	2.4 GHz	2 Mbps
IEEE 802.11b	2.4 GHz	11 Mbps
IEEE 802.11a	2.4 GHz	54 Mbps
IEEE 802.11g	2.4 GHz	54 Mbps
IEEE 802.11n	2.4 GHz et 5 GHz	600 Mbps
IEEE 802.11ac	5 GHz	1.3 Gbps
IEEE 802.11ad	5 GHz	7 Gbps
IEEE 802.11ax (Wi-Fi 6)	2.4 GHz et 5 GHz	9.6 Gbps

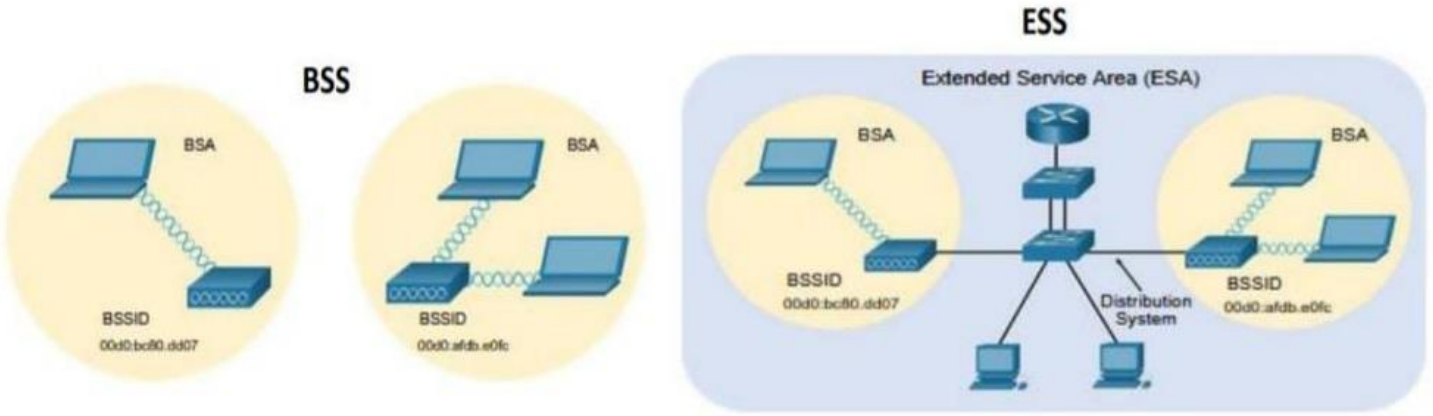
5GHZ est plus bande passant que **2.4 GHZ**

Avantages des Réseaux Sans Fil :

1. Mobilité : Permet aux utilisateurs de se déplacer librement tout en restant connectés au réseau.

2. Flexibilité : Facilité d'ajouter ou de déplacer des dispositifs sans recâblage physique.

3. Coût :Réduction des coûts d'installation et de maintenance par rapport aux réseaux câblés.
4. Scalabilité : Facilité d'extension du réseau en ajoutant simplement plus de points d'accès
Modes de topologie Wifi :



ESS (Extended Service Set): Ensemble de plusieurs points d'accès interconnectés, partageant le même SSID pour une couverture Wi-Fi étendue et continue.
BSA (Basic Service Area): Zone de couverture fournie par un seul point d'accès dans un BSS, définie par la portée de son signal radio.
ESA (Extended Service Area): Zone de couverture totale d'un ESS, constituée de plusieurs BSAs interconnectés.
BSS (Basic Service Set) : Unité de base d'un réseau Wi-Fi,
composée d'un point d'accès et des périphériques connectés à celui-ci.

M202 – ADMINISTRER UN ENVIRONNEMENT WINDOWS

Windows Server 2019:

Un serveur : un ordinateur poissant offre plusieurs services, Exemples : DHCP, DNS, WEB, Mail

Windows Server 2019: est un système d'exploitation de Microsoft orienté serveur

Les différentes éditions Windows Server 2019:

- Essential
- Standard : max deux machines virtuelles

Configuration minimale pour installer Windows Server 2019 :

- Processeur 1,4 GHz 64 bits
- Mémoire vive (RAM) : 2 Go (installation complète), 512mo (Installation minimale)
- Espace disque disponible : 15 Go

Configuration de base de Serveur

- **Renommer l'ordinateur:** Rename-Computer -NewName "nom" -Restart
- **Redémarrer le serveur:** Restart-Computer
- **Arrêter le serveur :** Stop-Computer
- **Récupérer le nom de cartes réseaux :** get-NetIPInterface
- **Configuration Réseau:** new-NetIPAddress –InterfaceIndex 12 –IPAdress 172.16.0.200 –PrefixLength 24 – DefaultGateway 172.16.0.1
- **Configurée mais l'adresse du serveur DNS :** Set-DNSClientServerAddresses –InterfaceIndex 12 –ServerAddresses 172.16.0.10,172.16.0.11
- **Joindre le serveur au Domaine**: add-Computer –DomainName Adatum.com –Restart
- **Convertir une installation minimale en une installation complète:** get-WindowsFeature -Name *GUI* | Install-WindowsFeature -IncludeAllSubFeature - IncludeManagementTools -Restart
- **Convertir une installation complète en une installation minimale :** get-WindowsFeature -Name *GUI* | Uninstall-WindowsFeature -Restart

Installation et configuration du serveur DNS:

Noms d'hôtes : nom d'ordinateur qui être associé à une adresse IP. Le nom peut comprendre jusqu'à 255 caractères

Nom NetBIOS : Représenter un ordinateur unique ou un groupe d'ordinateurs. Compte 16 caractères

DNS : (Domain Name System). C'est un système permettant la résolution des noms de machines en adresses IP et inversement. (Port 53 tcp/udp)

FQDN : (Fully Qualified Domain Name) Nom de domaine complètement qualifié est une séquence de noms de domaine qui spécifie l'emplacement complet d'un objet dans la hiérarchie du DNS

Arborescence de domaines DNS : Le DNS considère le réseau comme une arborescence de domaines. Voici un schéma sur le fonctionnement de l'arborescence

Les types des Requête DNS : Une requête est une demande de résolution de noms envoyée à un serveur DNS

- **Requête récursive :** le serveur DNS envoyée une réponse complète au client, le serveur DNS peut communiquer avec d'autre serveur DNS Pour chercher la réponse
- **Requêtes itératives :** le serveur DNS envoyée la meilleure réponse au client. Le résultat référence à un autre serveur DNS situé plus bas dans l'arborescence DNS.

Les type des serveur DNS :

- **Serveur Primaire :** (Principal) e c'est un serveur permet d'ajoute, modifier, Supprimer des hôtes de la zone. (Tous les droits administrateur)

- **Serveur Secondaire :** c'est un serveur qui permet de lecture seule de la zone. On peut consultes ls zone mais on ne peut pas ajouter au modifier les informations.
- **Serveur cache :** c'est un serveur qui contient l'historique des résolutions effectués sur le réseau Pendant une durés déterminée

Les zones DNS : Une zone DNS est une partie spécifique de l'espace de noms DNS qui contient des enregistrements DNS. Les types de zone DNS :

- **Zones de recherche directe :** résolvent les noms d'hôtes en adresses IP
- **Zones de recherche inverse :** résout les adresses IP en noms de domaine

Le transfert des zones DNS :C'est l'envoyé de la zone vers le serveur secondaire par le serveur principal pour mettre ajour

Notification DNS :C'est un message envoyé par le serveur principal ou serveur secondaire pour l'informe qui il y a des modifications de la zone pour le trensfert.

Les types d'enregistrements DNS :

- **SOA** : Permet de définir les informations relatives à la zone. En l'occurrence le nom du serveur DNS primaire et l'adresse électronique du contact technique. Il est composé de plusieurs champs :
  - **Serial** : C'est le numéro de série à incrémenter à chaque modification du fichier.
  - **Refresh :** définit la période de rafraîchissement des données.
  - **Retry :** si une erreur survient au cours du dernier rafraîchissement.
  - **Expire :** le serveur sera considéré comme non disponible au bout du délai Expire.
  - **Negative cache TTL :** la durée de validité des données communiquée par le serveur.
- **NS :** enregistrements de nom des serveurs dns
- **MX :** enregistrements sur le serveur de messagerie.
- **A :** associe un nom d'hôte à une adresse ipv4 (32 bits)
- **AAAA :** associe un nom d'hôte à une adresse ipv6 (128 bits)
- **CNAME :** enregistrements d'un alias vers un client déjà enregistré
- **PTR :** enregistrements de la résolution inverse

Redirection des requêtes :

Si le serveur ne peut pas résoudre certains domaines, il rediriger la requête à un autre serveur DNS

Mises à jour dynamiques : c'est l'inscription d'un client automatiquement, Les mises à jour dynamiques sont importantes pour les clients DNS qui changent d'emplacement, car elles peuvent inscrire et mettre à jour dynamiquement leurs enregistrements de ressources sans intervention manuelle

Installation et configuration du système DNS Power Shell :

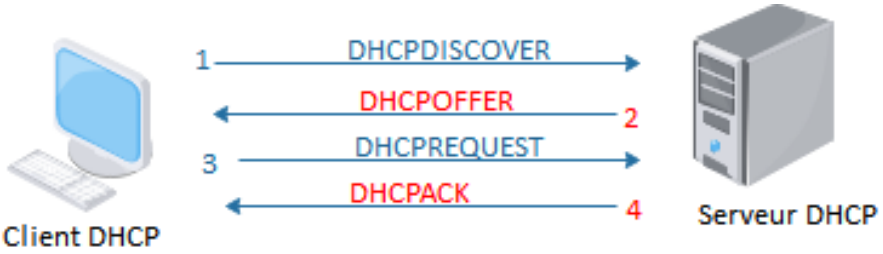
- **Installer le rôle du serveur DNS :** Install-WindowsFeature DNS –IncludeManagementTools
- **Configurer le serveur principal zone de recherche directe :** Add-DnsServerPrimaryZone -Name "nom de la zone " -ZoneFile "nomdelazone.dns"
- **Configurer le serveur principal zone de recherche inverse :** Add-DnsServerPrimaryZone -NetworkID Adresseréseau/Cidr -ZoneFile "PartieRéseauA L'envers.in-addr.arpa.dns
- **Configurer le serveur secondaire zone de recherche inverse:** Add-DnsServerSecondaryZone -NetworkID Adresseréseau/Cidr -ZoneFile "PartieRéseauA L'envers .in-addr.arpa.dns -MasterServers @IPServeurPrimaire
- **Configurer le serveur secondaire zone de recherche directe :** Add-DnsServerSecondaryZone -Name " NomdeZone " -ZoneFile " NomdeZonePrimaire .dns" -MasterServers @IPServeurPrimaire
- **transfert de zone:** Set-DnsServerPrimaryZone NomdeZone -SecureSecondaries TransferAnyServer -Notify Notify
- **Enregistrement NS :** Add-DnsServerResourceRecord -ZoneName NomdeZone -NS -Name "." -NameServer NomServeurDNS (FQDN)

- **Enregistrement A:** Add-DnsServerResourceRecord -ZoneName NomdeZone -Name NomHôte -A -IPV4Address @IPdu Hôte
- **Enregistrement AAAA :** Add-DnsServerResourceRecord -ZoneName NomdeZone -Name NomHôte -AAAA - IPV6Address @IPdu Hôte
- Enregistrement CNAME : Add-DnsServerResourceRecord -ZoneName NomdeZone -Name NomHôte -CNAME - HostNameAlias NomHôteOriginal
- **Enregistrement MX :** Add-DnsServerResourceRecord -ZoneName NomdeZone -Name NomHôte -MX -MailExchange NomDomaineduHôte (FQDN) -Preference Priorité
- **Enregistrement PTR :** Add-DnsServerResourceRecord -ZoneName NomdeZoneInverse -Name NumérHôte (IP) -PTR -PtrDomainName NomDomaineduHôte (FQDN)
- **Réaliser une redirection vers l'adresse :** Add-DnsServerForwarder -IPAddress 8.8.8.8 -PassThru
- **Afficher la configuration DNS :** Get-DnsServer
- **Lancer la mise à jour dynamique :** ipconfig /registerdns ou Register-DNSClient
- **Afficher le cache serveur :** ipconfig / displaydns ou Get-dnsservercache
- **Afficher le cache client :** ipconfig / displaydns ou Get-dnsclientcache
- **Vider le cache DNS:** Clear-DnsClientCache
- **Exporter la zone :** Export-DnsServerZone -Name "NomZone" -FileName "NomFichier"
- **Résolution des problèmes liés à la résolution de noms :** Nslookup

Installation et configuration du serveur DHCP :

DHCP: (Dynamic Host Configuration Protocol) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP/IP des client. Il attribue dynamiquement des informations telles que: Adresse IP, Masque de sous-réseau ,Passerelle par défaut, Serveurs DNS ,Durée du bail

Les requêtes et les messages DHCP :



Les étendues DHCP : est une plage d'adresses IP disponibles pour le bail et gérées par un serveur DHCP.

La durée de baile DHCP : c'est la durée de vie minimal d'adresse IP dynamique de client offre par le serveur DHCP

le processus de renouvellement de bail DHCP:

- le client envoie une demande de renouvellement DHCP avant l'expiration de son bail.
- Le serveur DHCP, s'il est disponible, répond positivement en renouvelant le bail et en actualisant la durée.
- En cas d'absence de réponse du serveur, le clint continue à utiliser son adresse IP actuelle jusqu'à l'expiration du bail, puis doit renouveler via une nouvelle demande DHCP

L'agent de relais DHCP : est un dispositif réseau qui facilite la communication entre les clients DHCP et les serveurs DHCP situés sur des sous-réseaux différents

L'adresse APIPA : (Automatique Prive IP Addressing) : configuration de adresse Automatique lorsque le client ne obtenir Pas une adresse par le serveur DHCP et donner une adresse don la Plage 169.254.0.1 a 169.254.255.254

Installation et configuration du système DHCP Power Shell :

- **Installer le rôle DHCP:** Install-WindowsFeature DHCP -IncludeManagementTools

- **Ajouter une étendue DHCP :** Add-DhcpServerV4Scope -Name "DHCP Scope" -StartRange @IPDebut -EndRange @AdresseIPFin -SubnetMask MasqueSousRéseau
- **Exclure une plage d'adresse :** Add-DhcpServerv4ExclusionRange -ScopeID AdresseRéseau -StartRange @IPDebut - EndRange @IPFin -state active
- **Ajouter les options de passerelle de routeur :** Set-DhcpServerv4OptionValue -OptionID 3 -Value 10.0.0.1 -ScopeID 10.0.0.0 - ComputerName DHCP1
- **Ajouter les options de serveur DNS :** Set-DhcpServerV4OptionValue -DnsServer @IPServeurDNS -Router @IPPasserelle
- **Définir de la durée du bail pour une étendue** : Set-DhcpServerv4Scope -ScopeID AdresseRéseau -LeaseDuration 1.00:00 :00 5.
- **Redémarrer le serveur DHCP :** Restart-service dhcpserver
- **Afficher l'étendue :** Get-DhcpServerv4Scope
- **Réserver une adresse a une machine :** Add-DhcpServerv4Reservation -ScopeID AdresseRéseau -IPAddress @IP - ClientId @Mac -Description "description de la réservation"

Installation du server ADDS:

Active Directory est un service utilisé pour stocker des informations des utilisateurs et Géré, Contrôle, Organise Des objets (unité d'organisation, utilisateur, profile, group) aux ressources réseau sur un domaine.

Contrôleur de Domaine (DC) : un server installer active directory qui permet de contrôler des utilisateurs en mem Domain

Avantages d'AD : • Sécurité • Évolutivité • Administration souple et simplifiée

Structure logique : organise les ressources (Unité d'organisation, Domaine, Arbre, Forêt)

Structure physique : elle configure et gère le trafic réseau (Contrôleur de domaine, Site)

Une forêt : est un regroupement d'une ou plusieurs arborescences de domaine

Arber : Une arborescence est une hiérarchie de domaines liés entre eux.

Un domaine : est constitué d'un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.

Catalogue Global : est une base de données contenant des informations sur tous les objets d'Active Directory dans une forêt .

Les relations d'approbation : sont des liens de confiance permettant aux utilisateurs authentifiés dans leur domaine d'accéder aux ressources d'un autre domaine.

La réplication : est le processus de synchronisation des données entre les contrôleurs de domaine, assurant la cohérence des informations à travers une forêt.

Site : C'est une combinaison d'un ou plusieurs sous-réseaux IP connecté par une liaison haut débit. Les sites

Mappent la structure physique du réseau.

Un RODC : (Read Only Domain Controller) est un contrôleur de domaine en lecture seule utilisé dans les environnements où la sécurité et la fiabilité sont des préoccupations majeures. Il permet de répliquer les données de l'Active Directory sans autoriser les modifications locales, réduisant ainsi les risques de compromission.

La base de données NTDN : (NT Directory Database) est la base de données utilisée par Active Directory pour stocker des informations sur les objets du domaine

Les Partitions Active directory (NTDS Partitions):

- **La partition de domaine** : cette partition contient les informations de tous les objets d'un domaine (ordinateur, groupe, utilisateur,etc..) Console : Utilisateurs et Ordinateurs Active directory

- **La partition de configuration**: cette partition contient la topologie de la forêt (informations sur les domaines, les liens entre les contrôleurs domaines, les sites, etc.).Console: Sites et Services Active directory
- **La partition de schéma :** cette partition contient l'ensemble des définitions des classes d'objets et attributs, qu'il est possible de créer au sein de l'annuaire Active Directory
- **La partition Application (partition DNS) :** contient la base de données DNS. Console : DNS

Les Cinq rôles maîtres d'opération FSMO :

FSMO : (Flexible Single Master Operation) sont des rôles critiques qui assurent la cohérence et l'intégrité de la base de données Active Directory.

• **Rôle maître de schéma** : a qui gère la modification du schéma sur le serveur. Il ne peut y avoir qu'un seul maître de schéma dans une forêt.

• **Maître de dénomination de domaine :** qui gère l'ajout et la suppression de domaine dans une forêt. Il ne peut y avoir qu'un seul maîtrede ce type dans une forêt

• **Maître RID :** qui alloue un identificateur SID unique à 1'intérieur d'un domaine (pour un utilisateur, un groupe...). Il ne peut y avoir qu'un seul maître RID dans un domaine.

• **Maître infrastructure :** permet de maintenir les liens entre les utilisateurs et les groupes auxquels ils appartiennent et gère lees objets. Unique au sein d'un domaine

• **Maître émulateur PDC :** contrôleur de domaine principale assure la sécurité (verrouillage compte, changement mot de passe.) Il est unique au sein d'un domaine

Installation du contrôleur de domaine sous PowerShell :

- **ajouter le rôle ADDS:** Install-WindowsFeature -name AD-Domain-Services –IncludeManagementTools
- **Vérifier l'installation: Get**- WindowsFeature AD-Domain-Services
- **Configuration Nouvelle Forêt :** Import-Module ADDSDeployment Install-ADDSForest -DomainName nom
- **Vérifier l'installation:** Get-ADDomain

Gestion d'objets ADDS:

Gestion des Unités organisationnelles :

- **Ajouter une Ou :** New-ADOrganizationalUnit -Name TRI -Path " dc=ntic,dc=ma"
- **Ajouter l'unité à l'unité** : New-ADOrganizationalUnit -Path "ou=TRI,dc=ntic,dc=ma" -Name TP
- **Modifier la sécurité contre la suppression de ou :** Set-ADOrganizationalUnit -Identity "ou=TRI,dc=ntic,dc=ma" - ProtectedFromAccidentalDeletion $false
- **Supprimer une OU :** Remove-ADOrganizationalUnit "ou=TRI, dc=ntic,dc=ma" -recursive
- **Afficher la liste des OÙ :** Get-ADOrganizationalUnit –filter *

Gestion des utilisateurs:

- **Ajoute un utilisateur :** New-ADUser -Name "Ziti Ilham" -Path "ou=tri,dc=ntic,dc=ma"
- **Les Option :** -GivenName Ilham -Surname ZITI - SamAccountName IZITI -UserPrincipalName IZITI@ntic.ma -DisplayName "Ilham ZITI" -Description "Utilisateur test TP ADDS" –EmailAddress ilhamziti@ntic.ma - MobilePhone "02023553678" -Department NTIC - City Oujda -HomePhone "0536677888" -Path "ou=tri, dc=ntic,dc=ma" - AccountPassword (Read-Host -AsSecureString "merci de saisir votre mot de passe") - PassThru -PasswordNeverExpires $true -ChangePasswordAtLogon 1 - CannotChangePassword 0 -enable $true
- **Activer un compte :** enable-ADAccount -Identity iziti
- **Désactiver le compte :** Disable-ADAccount -Identity iziti
- **Déverrouiller un le compte :** Unlock-ADAccount iziti
- **Supprimer un utilisateur : Remove**-ADUser iziti
- **Recherche d'un utilisateur :** get-ADUser -filter * -SearchBase " ou=tri,dc=ntic,dc=ntic"
- **Pour d'afficher les propriétés de l'utilisateur :** get-ADUser iziti -Properties *

Gestion des profils:

Profil par Défaut : Le Profil par Défaut dans un environnement Windows est un modèle de profil utilisateur utilisé comme base pour créer les profils des nouveaux utilisateurs.

Profil Obligatoire : Un Profil Obligatoire est un modèle de profil utilisateur qui garantit une uniformité d'environnement à chaque connexion.

Profils Itinérants : Les Profils Itinérants sont des profils utilisateur stockés sur un serveur central et chargés sur n'importe quel ordinateur auquel un utilisateur se connecte.

- **Créer un utilisateur profile**: New-ADUser -Name "Ziti Ilham" -Path "ou=tri,dc=ntic,dc=ma" –ProfilePath \\AD1\Ressource - HomeDirectory C:\ Donnees - AccountPassword (Read-Host -AsSecureString "merci de saisir votre mot de passe") - PassThru -ChangePasswordAtLogon 1

Gestion Groupe:

Groupe : ensemble d'utilisateurs ou ordinateur, Les groupes sont caractérisé par leurs étendue et leur type

Type de groupe :

- **Distribution :** sont utilisés pour créer des listes de distribution électronique
- **Sécurité :** sont utilisés pour affecter des autorisations à des ressources partagées

Etendu du groupe:

- **Domaine local :** membres de plusieurs domaines, visible dons le domaine.
- **Globale :** membres même domaines, visible dons la foret.
- **Universelle :** membres de plusieurs domaines, visible dons la foret.

Contenu d'un Groupe Global : Un groupe global peut contenir des utilisateurs, des groupes globaux d'autres domaines et des groupes de sécurité universels en tant que membres

- **Ajouter un groupe:** New-ADGroup -name "Stagiaire" -Path "ou=tri,dc=ntic,dc=ma" - GroupCategory Security -groupscope Global
- **ajouter l'utilisateur au groupe :** Add-ADGroupMember -Identity "Stagiaire" -Member "iziti"
- **ajouter un autre groupe au groupe** : Add-ADGroupMember -Identity "Stagiaire" -Members StageOujda,StageRabat
- **Modifier Groupe :** Set-ADGroup -Identity "cn=stagiaire,ou=tri,dc=ntic,dc=ma" -GroupCategory Distribution
- **Supprimer un groupe :** Remove-ADGroup stagiaire
- **Gestion ordinateur:**
- **Ajouter un ordinateur :**New-ADComputer -Name "PC1" -SamAccountName "PC1" -Path "OU=tri,DC=ntic,DC=ma" -Enabled $true -Location "Direction"
- **déplacer un ordinateur dans une unité d'organisation :**Move-ADObject -Identity "CN=PC2,OU=informatique, DC=ofppt,DC=ma" -TargetPath "OU=informatique,DC=ofppt,DC=ma"
- **Supprimer un ordinateur** : Remove-ADComputer -Identity "cn=PC1,ou=tri,dc=ntic,dc=ma"

Gestion des Objet de stratégie de groupe (GPO) :

Les stratégies de groupe :(group Policy Object) configurer et appliquer des paramètres des utilisateurs et des ordinateurs au sein d'un domaine ou d'une unité d'organisation (OU)dans un environnement Active Directory

L'ordre d'application des GPO: 1- locale sur l'ordinateur 2-le site 3- de domaine 4-unité d'organisation (OU)

Types de GPO : GPO d'Ordinateur , GPO d'Utilisateur

Les PSO (Password Settings Object) : permettent de définir des politiques de mot de passe spécifiques à des groupes ou utilisateurs particuliers, offrant une flexibilité supplémentaire par rapport aux GPO générales.

GPO en PowerShell

- **Ajouter une GPO :** New-GPO –Name "cmd"

- **Lier GPO a une unité :** New-GPLink cmd –target "ou=tri,dc=ntic,dc=ma" –LinkEnabled yes
- **Renommer GPO :** rename-gpo -name ancien nom -targetname nouveau nom
- **Supprimer un lien GPO:** Remove-GPLink NomGPO –target "dn "
- **Supprimer une GPO:** Rmove-Gpo NomGPO
- **Forcer l'application des stratégies de groupe :**gpupdate /force

Gestion du système de fichier DFS :

DFS : (Distributed File System) est un système de fichiers distribué qui permet de organiser les répertoires partagés et accessibles à partir de plusieurs serveurs au sein d'un réseau.

Racine DFS : Point d'entrée principal d'un système DFS, contient le chemin d'accès aux différentes liaisons DFS qui lui sont associées.

Dossier : Le dossier sera le nom du partage affiché côté client et dans la configuration du serveur.

La cible : représente le chemin d'accès vers le dossier partagé situé sur ce serveur.

Les avantages de DFS : sécurité, simplicité, évolutivité, performance

Les clichés instantanés des dossiers partagent :

C'est la sauvegarde des versions Précédant des dossiers Partages sur le serveur. Le cliché peut être active sur une ou des partitions Pour sauvegarde des les Version Précédant afin de los récupères en cas d'erreur de modification ou de suppression. On peut planifier la création de clicher et limité la taille de Stockage.

le quota :est la gestion des quotas de disque, qui contrôle l'utilisation de l'espace disque par les utilisateurs ou les groupes.

Quota inconditionnel : est limite l'utilisation de l'espace disque sans égard à d'autres critères que la quantité d'espace occupée.

Quota conditionnel : est associé à des critères supplémentaires.

Installation DFS via PowerShell

- **Install DFS Namespace feature:** Install-WindowsFeature -Name FS-DFS-Namespace -IncludeManagementTools
- **Install DFS Replication feature**: Install-WindowsFeature -Name FS-DFS-Replication -IncludeManagementTools

Service de plainent de Windows (WDS)

WDS : permet d'installer Windows sur les machines clients par réseau

- les clients doivent avoir une carte réseau PXF Pour être installer par le serveur.

-le service DHCP st nécessaire pour distribuer les adresse IP ou client du réseau, afin de Pouvoir Communier avec le serveur WDS

M203 – ADMINISTRER UN ENVIRONNEMENT LINUX

I. Configuration de base de serveur:	
Modifier le nom avec le fichier	vi /etc/hostname srv1
Modifier le nom avec lacommande	Hostnamectl set hostname srv1
Redemarrer la machine	reboot
Désactiver le Pare-Feu	systemctl stop firewalld.service
desavtiver au démarrage automatiquement	systemctl disable firewalld.service
Configuration de carte réseau: Outil if config	
Configurer l' interface	ifconfig <dev> <adresse_ip> [netmask <mask>] [broadcast <addr>]
Activation de l'interface	ifconfig <dev> up
Arrêt de l'interface	ifconfig <dev> down
Affichage les interface	Ifconfig
Configuration de carte réseau: Outil ip	
Configuration:	ip addr add <address> dev <intrfas ame>
Affichage des informations	ip addr show dev
Configuration de carte réseau: fichier de configuration	
Le chemin de Fichiers	/etc/sysconfig/network-scripts/ifcfg-eth0)
Configurer l'interface	**DEVICE=eth0** **IPADDR=192.168.1.2** **NETMASK=255.255.255.0** **NETWORK=192.168.1.0** **BROADCAST=192.168.1.255** **ONBOOT=yes** **BOOTPROTO=none** **DNS=8.8.8.8** **GETWAY=192.168.0.1** **DOMAIN=ID.MA**
Activation de l'interface	if up eth0
Arrêt de l'interface	ifconfig down eth0

Installation et configuration du serveur DNS :

DNS : Domain Name System. C'est un système hiérarchique distribué permettant la résolution des noms de machines en adresses IP et inversement, utilise le port 53.

Il existe deux types de :

- **Requêtes : requêtes récursives et requêtes itératives.**
- **Serveur DNS Principal (Master) et DNS secondaire (Slave).**
- **Zone : Zones de recherche directe, et zones de recherche inversée**

Le fichier /etc/resolv.conf : est un fichier de configuration utilisé par le système pour définir les serveurs DNS qu'il doit utiliser pour résoudre les noms de domaine en adresses IP.

installation online	dnf install bind -9*
Installation hors line	rpm -ivh bind -9
Vérification d'installation	rpm -qa bind

Le chemin de Fichiers	/etc/named.conf
Démarrage du service	systemctl start named.service
Configuration globale	listen-on port 53 { 127.0.0.1;192.168.10.20 }; allow-query { 192.168.10.0/24; };
Configuration de serveur DNS principal	
Création des zone directe	zone id.ma in { type master ; file id.ma.direct ; allow-transfer{192.168.10.21;}; notify yes; allow-update{any;}; } ;
Création des zone inverse	zone 10.168.192.in-addr.arpa in { type master ; file id.ma.inverse; allow-transfer{192.168.10.21;}; notify yes; allow-update{any;}; } ;
Les Enregistrement de la zone directe	Vi /var/etc/named/id.ma.directe $TTL1D @ IN SOA srvdns.id.ma. pc.id.ma. (64 ; serial number 3600 ; refresh 600 ; retry 86400 ; expire 3600) ; minimum TTL @ IN NS srvdns.id.ma @ IN MX 10 mail.id.ma srvdns.id.ma IN A 192.168.10.1 srvdns.id.ma IN AAAA 201:ABVD::2 www IN A 192.168.10.1
Les Enregistrement de la zone inverse	Vi / var/etc/named/id.ma.inverse $TTL1D @ IN SOA srvdns.id.ma. pc.id.ma. (64 ; serial number 3600 ; refresh 600 ; retry 86400 ; expire 3600) ; minimum TTL @ IN NS srvdns.id.ma 2 IN PTR srvdns.id.ma
Configuration de serveur DNS secondaire	
Création des zone directe	zone id.ma in {

	type slave; file id.ma.direct ; master 192.168.10.20; allow-notify { 192.168.10.20; }; } ;
Création des zone inverse	zone 10.168.192.in-addr.arpa in { type slave ; file id.ma.inverse; master 192.168.10.20; allow-notify { 192.168.10.20; }; } ;

Configuration DDNS

DDNS (Dynamic Domain Name System) est un service qui permet de mettre à jour automatiquement les enregistrements DNS d'un nom de domaine lorsqu'une adresse IP change, facilitant ainsi l'accès aux appareils ayant des adresses IP dynamiques

Au niveau du serveur DNS	Dans named.conf indiquer l'adresse IP du serveur DHCP dans l'option allow-update
Au niveau du serveur DHCP	ajouter les lignes suivantes dans dhcpd.conf : **ddns-updates on;** **ddns-update-style interim;** **serveur DNS local.** **deny client-updates;** **auprès du serveur DNS.** **ddns-domainname "Nom de la zone directe";** **ddns-rev-domainname "nom de la zone inverse";** **authoritative;** **zone Nom de zone directe. {** **primary 192.168.2.1;** **}** **zone Nom de zone inverse. {** **primary 192.168.2.1;** **}**

Installation et configuration du serveur DHCP :

DHCP (Dynamic Host Configuration Protocol) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine. (UDP 68 CLIENT 67 SERVER)

installation online	dnf install dhcp -server *
Installation hors line	rpm -ivh dhcp
Vérification d'installation	rpm -qa dhcp
Démarrage du service	systemctl start dhcpd
Le chemin de Fichiers	/etc/dhcp/dhcpd.conf

Configuration de serveur dhcp	subnet 192.168.10.0 netmask 255.255.255.0 {
	range 192.168.10.30 192.168.10.60;
	option routers 192.168.10.1;
	option domain-name “id.ma";
	option domain-name-servers 192.168.10.20, 192.168.10.21;
	default-lease-time 600;
	max-lease-time 7200;
	}

Réservation Adresse IPV4	host PC1 {
	option host-name "PC1.example.com";
	hardware ethernet 00:A0:78:8E:9E:AA;
	fixed-address 192.168.1.4;
	}

Installation et configuration du serveur SAMBA :

Samba est permet le partage de fichiers et d'imprimantes entre des systèmes Linux et des systèmes Windows. (TCP/UDP 137)

installation online	dnf install samba
Installation hors line	rpm -ivh samba
Vérification d’installation	rpm -qa samba
Démarrage du service	systemctl start smb.service systemctl start nmb.service
Le chemin de Fichiers	/etc/samba/smb.conf
les paramètres généraux du serveur	**[global]** **workgroup =** MYGROUP **netbios name =** posteN **security =** share (méthode d’authentification)
les paramètres d’accès aux répertoires	**[partage1]** **comment =** Répertoire partagé 1 **path =** /opt/partage1 **browseable =** yes **public =** no **writable =** yes **printable =** no **group =** partage
les paramètres des imprimantes	**[Bureau150]** **comment =** Laserjet 2100 **printer =** lj2100 **valid users =** ahmed ali mohammed **path =** /var/spool/lj2100 **public =** no **writable =** no **printable =** yes **browseable =** yes

Configuration de l'utilisateur et dossier partager	**Créer un répertoire** : mkdir partage **Créer un groupe :** groupadd ntic 3 **Créer un utilisateur :** useradd -g ntic 3 user1 **Définir un mot de passe Samba :** smbpasswd -a user1 **Modifier les droits du répertoire** : chgrp -R ntic partage chmod -R o+xw partage

Installation et configuration du serveur NFS :

NFS (Network File System) est un protocole permettant de monter des disques en réseau. Le port utilisé par NFS c'est 2049. NFS est compatible avec l'IPv4 et IPv6

installation online	dnf install nfs-utils
Installation hors line	rpm -ivh nfs-utils
Vérification d'installation	rpm - qa nfs-utils
Démarrage du service	systemctl start nfs-server
Le chemin de Fichiers	/etc/export
Configuration de service nfs	**<dossier partagé> <hôte>(<options>)** <dossier partagé> : chemin de dossier partagé <hôte> : @IP, Nom Domaine, nom de hôte <options> : indique les options de partage : ▪ rw : droit lecture et écriture, ▪ ro : droit de lecture seule (option par defaut) ▪ root_squash : spécifie que le root du serveur NFS n'a pas les droits de root sur le répertoire partagé ▪ no_root_squash : le root distant équivaut root local ▪ all_squash : force le mapping de tous les utilisateurs vers l'utilisateur anonyme. ▪ anonuid : indique l'UID de l'utilisateur ▪ anongid : indique le GID de l'utilisateur anonyme **Ex :** /home/ofppt/testN 192.168.147.215(rw)
Exporter le partage	exportfs -ra
Lister les info du montage	showmount -e host
Montage client	mount -t nfs serveur1:/pub /mnt/pub
Montage automatique	vi /etc/fstab server1:/pub /mnt/pub nfs defaults 0 0
Activer le montage	mount -a

Installation et configuration du serveur FTP

FTP (File Transfer Protocol) permet de transfert de fichiers entre un client et un serveur sur un réseau. Il facilite le partage de fichiers et le transfert de données entre différents systèmes informatiques (TCP 21)

installation online	dnf install vsftpd
Installation hors line	rpm -ivh vsftpd
Vérification d'installation	rpm - qa vsftpd
Démarrage du service	systemctl start vsftpd
Le chemin de Fichiers	/etc/ vsftpd/vsftpd.conf

Configuration de service ftp:	**anonymous_enable=NO** //Pas de connexions **listen_port=21** // Spécifie le port d'écoute **local_enable=YES** // Autoriser les utilisateurs locaux **write_enable=YES** //Autoriser le droit d'écriture **local_umask=022** //Fixer le masque local a 022 **anon_upload_enable=NO** //Refuser le upload **anon_mkdir_write_enable=NO** // Refuser l'ecriture **idle_session_timeout=600** // Temps avant déconnexion **max_clients=50** //Nombre maximum de connexion **max_per_ip=4** // Nombre maximum de connexion venant de la même IP **ftpd_banner=Bienvenue sur mon ftp perso** //Bannière de bienvenue **chroot_local_user=YES** **chroot_list_enable=NO** **allow_writeable_chroot=YES** //les trois lignes limite les utilisateurs à leur répertoire

Installation et configuration du serveur TELNET :

Telnet est un client léger permettant d'ouvrir une connexion et une session sur une machine distante proposant un serveur telnet . Ce serveur est souvent lancé depuis xinetd ou inetd

installation online	dnf install xinetd
Installation hors line	rpm -ivh xinetd
Vérification d'installation	rpm - qa xinetd
Démarrage du service	systemctl start xinetd
Activation au démarrage du service	systemctl enable xinetd
Le chemin de Fichiers	/etc/xinetd.d/telnet
Syntaxe du fichier de configuration **Au niveau de serveur**	service telnet **{** **disable =** no **flags =** REUSE **socket type =** stream **wait =** no **user =** root **server =** /usr/sbin/in.telnetd **log on failure +=** USERID **}**
Au niveau de client	telnet (ou telnet @ip ou telnet localhost) telnet> open (to) 192.168.1.2 Trying 192.168.1.2... Connected to 192.168.1.2. login: FARID Password:

Installation et configuration du serveur SSH :

SSH (Secure Shell) est un programme mais aussi un protocole de communication sécurisé. Grâce à SSH, on peut se connecter à distance sur une machine et transférer des fichiers. Le numéro de port utilisé par le serveur est 22

installation online	dnf install openssh-server
Installation hors line	rpm -ivh openssh-server
Vérification d'installation	rpm - qa openssh-server
Démarrage du service	systemctl start sshd
Activation au démarrage du service	systemctl enable sshd
Le chemin de Fichiers	/etc/ssh/sshd_config
Syntaxe du fichier de configuration	**PermitRootLogin** yes **Port** 22 **ListenAddress** 192.168.1.210 **PermitEmptyPasswords** no
Redémarrage du service	Service sshd restart
Au niveau du client ssh	ssh root@192.168.1.2 on windows on utiliser Putty, WinSCP

Installation et configuration du serveur RAID :

RAID(Redundant Array of Independent Disks) est une technologie qui combine plusieurs disques durs en une seule unité logique pour améliorer les performances et/ou la redondance des données.

Types de RAID:

RAID 0 (Stripping) :

- Description: Les données sont divisées en blocs et réparties sur plusieurs disques.
- Avantages: Performances améliorées en lecture et écriture.
- Inconvénients: Pas de redondance, la perte d'un disque entraîne la perte de toutes les données.

RAID 1 (Mirroring) :

- Description: Les données sont copiées en miroir sur deux disques.
- Avantages: Haute redondance, récupération facile en cas de panne d'un disque.
- Inconvénients: Espace de stockage réduit de moitié.

Installation de RAID : dnf install mdadm

Création de l'ensemble RAID:

- **RAID 0 :** mdadm --create --verbose /dev/md0 --level=0 --raid-devices=2 /dev/sda /dev/sdb
- **RAID 1 :** mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 /dev/sda /dev/sdb

Installation et configuration du serveur LDAP :

LDAP (Lightweight Directory Access Protocol) est un protocole utilisé pour accéder et gérer les services d'annuaires, qui contiennent des informations sur les utilisateurs, les groupes, les périphériques, et d'autres objets. Les annuaires LDAP sont souvent utilisés dans les réseaux d'entreprise pour la gestion des informations de manière centralisée. Il fonctionne principalement sur le port 389.

installation online	dnf install openldap-clients openldap-servers openldap-devel openldap-compat
Installation hors line	rpm -ivh openldap
Vérification d'installation	rpm - qa openldap
Démarrage du service	systemctl start slapd.service
Activation Du démarrage	systemctl enable slapd.service

Le chemin de Fichiers	/etc/openldap/slapd.d/
mot de passe root LDAP	Slappasswd
Configuration	dn: olcDatabase={2}hdb,cn=config changetype: modify replace: olcSuffix olcSuffix: dc=id,dc=local dn: olcDatabase={2}hdb,cn=config changetype: modify replace: olcRootDN olcRootDN: cn=ldapadm,dc=id,dc=local dn: olcDatabase={2}hdb,cn=config changetype: modify replace: olcRootPW olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Redémarrage du service	Systemctl restart slapd
Ex fichier ldif: Domaine, OU, groupe, user **vim base.ldif20**	dn: dc=ilham,dc=local ObjectClass: top ObjectClass: domain dc: ilham dn: ou=tri,dc=ilham,dc=local ObjectClass: top ObjectClass: organizationalUnit ou: tri dn: cn=202,ou=tri,dc=ilham,dc=local ObjectClass: posixGroup cn: 202 gidNumber: 202 memberuid: ahmed description: testgroupe dn: uid=ahmed,ou=tri,dc=ilham,dc=local ObjectClass: top ObjectClass: person ObjectClass: inetorgperson cn: ahmed serraji sn: serraji givenname: ahmed description: testuser uid: ahmed telephonenumber: 1233444 mail: eee@jhhhh

Installation et configuration du serveur HTTP :

HTTP (hyper texte Transfer protocole) est un protocole de communication qui permet le transfert de documents hypertextes, tels que des pages web, entre un client (souvent un navigateur web) et un serveur. Il fonctionne principalement sur le port 80 (HTTP) ou le port 443 (HTTPS pour une communication sécurisée)
Le fichier /etc/hosts est un fichier de configuration qui associe des adresses IP à des noms d'hôtes.

installation online	dnf install httpd*
Installation hors line	rpm -ivh httpd
Vérification d'installation	rpm - qa httpd*
Démarrage du service	systemctl start httpd
Activation au démarrage du service	systemctl enable httpd
Le chemin de Fichiers	/etc/httpd/conf/httpd.conf
Les stratus https	1xx : Informations 2xx : requête Succès 3xx : Redirections 4xx : Erreurs du client 5xx : Erreurs du serveur
Autoriser le http sur le firewall	firewall-cmd --permanent --addport =80/tcp firewall-cmd --permanent --addport =443/tcp firewall-cmd --permanent --relade
Répertoire du site	1. Création du répertoire pour le site : #mkdir -p /var/www/html/ntic.local 2. Modification des droits : #chown -R apache:apache ntic.local #chmod -R 755 ntic.local 3. Création du fichier index.html : #vim /var/www/html/ntic.lcal/index.html 4. Exemple du fichier index : <html> <head> <title>Welcome to ntic.local</title> </head> <body> l'Exemple de virtual host fonctionne </body> </html>
Virtual Host	**vi /etc/httpd/conf.d/nomdoamine.conf** **<VirtualHost 192.168.2.3:80>** **ServerAdmin** admin@ntic.local **ServerName** ntic.local **ServerAlias** www.ntic.local **DocumentRoot** /var/www/html/ntic.lcal/ **ErrorLog** /var/log/httpd/error_log **CustomLog** /var/log/httpd/access_log combined **</VirtualHost>**
Configuration de fichier hosts	Vi /etc/hosts 192.168.10.20 ista.ma
Sécuriser Apache2 avec SSL	1. Installation du mod ssl : dnf install mod_ssl 2. Création du certificat :

HTTPS	openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out /etc/httpd/server.crt -keyout /etc/httpd/server.key 3. modifier le Virtual Host <VirtualHost *:80> ServerName ntic.local/ Redirect / https://ntic.local/ </VirtualHost> <VirtualHost *:443> ServerName ntic.local DocumentRoot /var/www/html/ntic SSLEngine on SSLCertificateFile /etc/httpd/server.crt SSLCertificateKeyFile /etc/httpd/server.key </VirtualHost>

M204 – DÉCOUVRIR LES ENJEUX DE LA TECHNOLOGIE SDN

problématiques des réseaux traditionnels:

- Complexité
- Passage à l'échelle
- Dépendance aux constructeurs

Le cloud computing

Le cloud computing :est un modèle de prestation de services informatiques via Internet

- rapidement les ressources informatiques
- solutions flexibles et configurables
- Économies de coûts

Services cloud :

- SaaS(Software as a service) :l'accès aux services qui sont fournis via Internet.
- PaaS (Plate-forme as a service) :l'accès aux outils et services de développement
- IaaS (Infrastructure as a Service) : l'accès à l'équipement réseau, aux services réseau virtualisés

Modèles de cloud :

- Cloud publics :accessibles par le grand public.
- Cloud privés : une entreprise ou à une entité spécifique,
- Cloud hybrides :est constitué de deux ou plusieurs nuages partie privée, partie publique
- Cloud communautaires : Il est similaire au privé et est utilisé par un groupe de personnes

Le data center

Le data center : une installation physique où sont regroupés et gérés des équipements informatiques

- contrôle complet sur l'infrastructure informatique
- performances et des temps de réponse rapides
- personnaliser infrastructure selon leurs beso

La virtualisation

La virtualisation : est une technologie qui permet de créer des versions virtuelles d'un environnement informatique, des serveurs, des réseaux, du stockage

Virtualisation des serveurs : La virtualisation des serveurs permet de consolider le nombre de serveurs nécessaires en utilisant les ressources inactives

Avantages de la virtualisation :

- Réduction des coûts matériels, de l'énergie et de l'espace occupé.
- Provisionnement plus rapide des serveurs.
- Optimisation des ressources

La virtualisation réseau : est une technologie qui permet de créer des versions virtuelles des ressources réseau physiques offre de nombreux avantages en termes de flexibilité

avantages de Automatisation

- productivité accrue,
- une production plus uniforme
- l'analyse rapide de grandes quantités de données
- l'utilisation de robots dans des environnements dangereux.

Formats de données

XML	JSON	YAML

<Servers>
<Server>
<name>Server1</name>
<owner>John</owner>
<created>123456</created>
<status>active</status>
</Server>
</Servers>
	{
	Servers: [
	{
	name: Server1,
	owner: John,
	created: 123456,
	status: active
	}
	]
	}
		Servers:
		- name: Server1
		owner: John
		created: 123456
		status: active

API

API : (Application Programing Interface) est les méthodes pour demander et fournir des données ou des fonctionnalités entre différentes parties d'un logiciel

- **API ouvertes ou API publiques :** Ces API sont disponibles au
- **API internes ou privées :**Ce sont des API qui sont utilisées par une organisation ou une entreprise.
- **API partenaires :** utilisées entre une entreprise et ses partenaires

Types d'API de service Web :

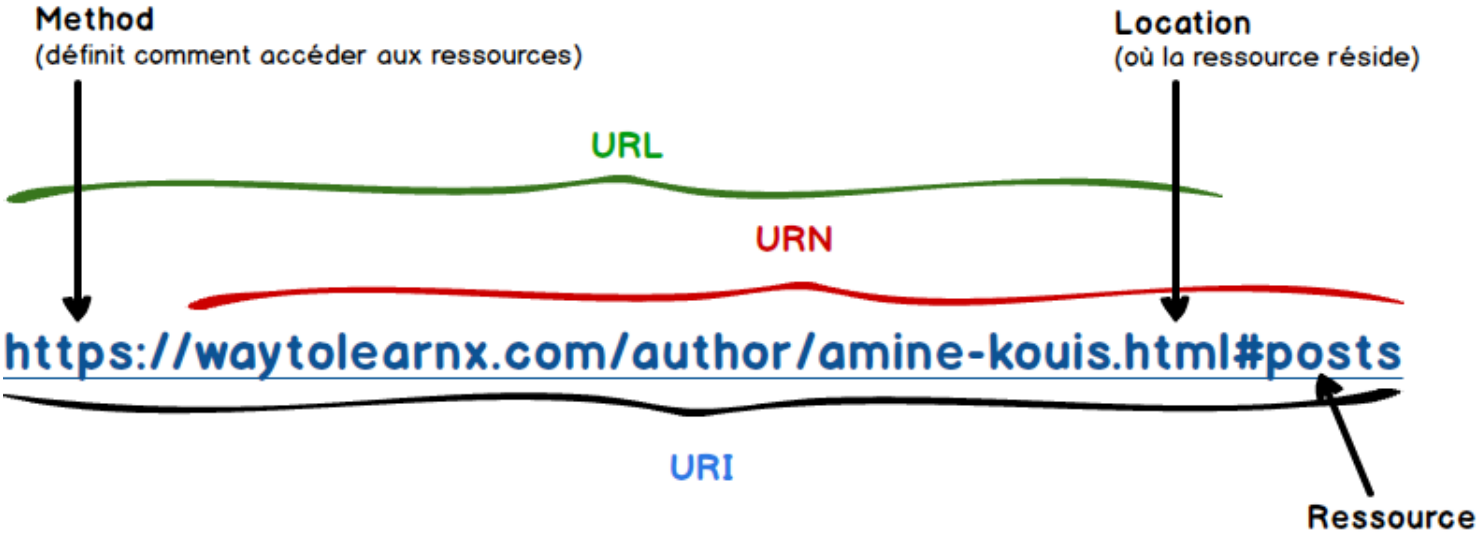
- Protocole d'accès aux objets simples (SOAP)
- Transfert d'état représentatif (REST)
- Langage de balisage extensible-Appel de procédure à distance (XML-RPC)
- Java Script notation d'objet-Appel de procédure à distance (JSON-RPC)

URL-URN-URI

URI : est une chaîne de caractères qui identifier une ressource sur Internet. Il comprend URL et URN

URN : identifie l'espace de noms de la ressource sans protocole.

URL : définit l'emplacement précis de la ressource avec protocole.#



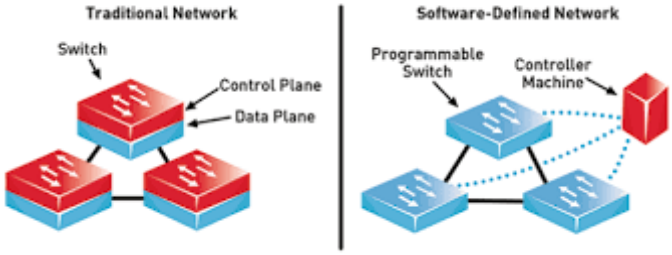
SDN

SDN :(Software-Defined Networking) est une architecture de réseau qui virtualise le réseau et sépare le contrôle du réseau de l'infrastructure matérielle

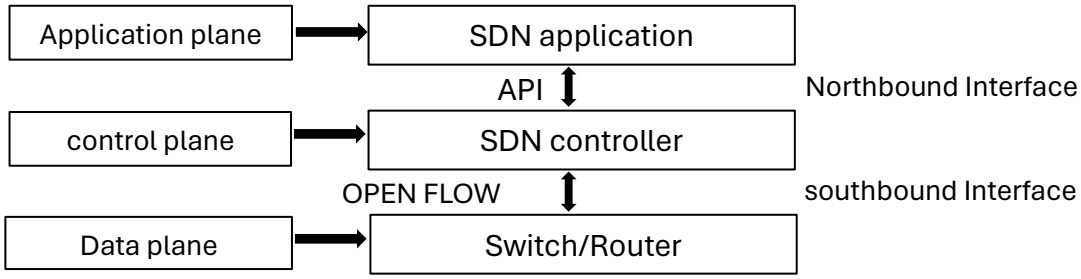
Les avantages de SDN :

- gestion centralisée et programmable
- configuration à distance
- Simplification
- Fiabilité et sécurité accrues
- Le coute
- automatisation des opérations réseau.

Architectures traditionnelles et SDN



Architectures de SDN :



Types d'architecture SDN :

- SDN basé sur les appareils
- SDN basé sur un contrôleur
- SDN basé sur des politiques

Modèles de la technologie SDN :

- **Model Flow-Based :** Chaque flux est configuré individuellement par le contrôleur
- **Model Aggregated :** Une entrée de flux couvre de grands groupes de flux
- **Model Reactive :** Premier paquet de contrôleur de déclencheurs de flux à insérer des entrées de flux
- **Model Proactive :** Le contrôleur pré-remplit la table de flux dans le commutateur

Les applications de la technologie SDN :

- SD-MN – SOFTRAN
- SD-Acces
- SD-WAN selon l'ONUG
- La technologie SD-WAN
- Les pré-requis SD-WAN selon l'ONUG
- WAN hybride et overlay
- a disponibilité du réseau
- SDWAN avec le cloud
- Connectivité flexible
- SD-WAN sécurisé
- Optimisation du trafic voix

Les solutions de la technologie SDN :

- Cisco ACI (Application Centric Infrastructure)
- Cisco APIC-EM
- Cisco DNA (Digital Network Architecture)

la différence entre NFV et SDN :

NFV :(Network Fonctions Virtualization)est une technologie qui permet de virtualisés les fonctions réseau NFV se concentre sur la virtualisation des fonctions réseau, tandis que SDN se concentre sur la séparation du plan de contrôle et du plan de données En bref, NFV virtualise les fonctions réseau tandis que SDN virtualise le contrôle du réseau.

OpenFlow :

OpenFlow :est un protocole standardisé qui permet la communication entre le contrôleur SDN et les commutateurs réseau.

OpenStack :

OpenStack : est une plateforme open source de cloud computing qui offre une infrastructure en tant que service (IaaS). Il permet de gérer de manière flexible et évolutive des ressources informatiques telles que le stockage, le réseau et le calcul, dans un environnement de cloud privé, public ou hybride

Présentation du Protocole OpenFlow

OpenFlow est un protocole essentiel pour la gestion des réseaux définis par logiciel (SDN). Il permet le contrôle à distance de la table de transfert d'un commutateur ou d'un routeur, en offrant une interface ouverte pour la gestion du trafic réseau. Développé initialement à l'université de Stanford, OpenFlow facilite la gestion du trafic entre les routeurs, les commutateurs et les points d'accès sans fil via un contrôleur central .

2. Architecture du Protocole OpenFlow

L'architecture d'OpenFlow se compose de plusieurs éléments clés :

- **Flow Table (Table de flux)** : Chaque commutateur OpenFlow contient une table de flux qui dirige le traitement des paquets en fonction des règles définies par le contrôleur.
- **Messages OpenFlow** : Trois types de messages sont supportés par OpenFlow :
  - **Messages asynchrones** : Envoyés du commutateur vers le contrôleur pour notifier des événements comme l'arrivée d'un paquet ou un changement d'état.
  - **Messages symétriques** : Échangés dans les deux sens sans sollicitation, tels que les messages Hello et Echo.
  - **Messages contrôleur-vers-commutateur** : Initiés par le contrôleur pour gérer directement l'état du commutateur, incluant des requêtes de configuration et des modifications d'état.

3. Les Switches OpenFlow

OpenFlow est compatible avec différents types de commutateurs :

- **Commutateurs matériels** : Offrent une vitesse de traitement élevée mais ont des limitations d'espace pour les entrées de la table de flux.
- **Commutateurs logiciels** : Fonctionnent sur des ordinateurs standard avec des performances relativement faibles mais peuvent stocker une grande quantité d'entrées de flux.
- **Commutateurs hybrides** : Combinent des éléments matériels et virtuels pour offrir des performances améliorées par rapport aux commutateurs logiciels purs.

4. Sécurité et Évolution d'OpenFlow

La sécurité dans les réseaux SDN utilisant OpenFlow couvre plusieurs aspects :

- **Disponibilité** : Gestion de la résilience et de la tolérance aux pannes grâce à des mécanismes de basculement et de répartition de charge.
- **Contrôle d'accès et intégrité** : Assurer que seuls les contrôleurs autorisés peuvent gérer les commutateurs et que les données échangées restent intègres.

Les versions d'OpenFlow ont évolué pour améliorer ces aspects, avec des fonctionnalités de changement de rôle du contrôleur et des mécanismes de basculement plus sophistiqués pour maintenir la continuité du service en cas de défaillance du contrôleur

M205-ADMINISTRER UN ENVIRONNEMENT CLOUD

Evolution des performances de processeurs

Les performances des processeurs ont évolué de manière spectaculaire au fil des années. Cette progression est principalement due à plusieurs facteurs :

- **Augmentation de la densité de transistors:** Selon la loi de Moore, le nombre de transistors sur une puce double environ tous les deux ans, ce qui a permis une augmentation exponentielle de la puissance de traitement.
- **Amélioration de la conception des processeurs:** Les avancées dans les architectures de processeurs, telles que l'architecture multi-cœur, ont permis d'augmenter les performances en parallèle et en efficacité énergétique.
- **Optimisation logicielle:** Les logiciels sont constamment optimisés pour tirer parti des nouvelles capacités matérielles, ce qui contribue à une meilleure utilisation des ressources processeur.
- **Technologies avancées:** Les processeurs modernes intègrent des technologies telles que l'hyper-threading, les instructions vectorielles avancées (AVX), et des architectures spécialisées comme les GPU (unités de traitement graphique).

Les systèmes distribués

Les systèmes distribués sont essentiels pour les infrastructures modernes. Ils permettent de répartir les tâches et les ressources sur plusieurs ordinateurs interconnectés, offrant des avantages significatifs :

- **Performance :** La distribution des tâches permet d'augmenter les performances globales du système.
- **Fiabilité:** La redondance et la tolérance aux pannes augmentent la fiabilité.
- **Scalabilité:** Les systèmes distribués peuvent facilement évoluer en ajoutant plus de nœuds.

Contraintes et limites des centres de données

Les centres de données, qui forment l'infrastructure de base des systèmes de cloud computing, doivent faire face à plusieurs contraintes :

Capacité physique : Limitations en termes de nombre de serveurs et de stockage.

Refroidissement : Nécessité de systèmes de refroidissement efficaces pour prévenir la surchauffe.Consommation d'énergie: Les centres de données consomment énormément d'énergie, impactant les coûts et l'environnement.

Disponibilité: Nécessité de garantir une disponibilité continue via des mesures de redondance.

Sécurité: Protection des données contre les menaces extérieures et intérieures.

Coût: Coûts élevés pour la construction, l'exploitation et la maintenance des infrastructures.

Le cloud computing

Le cloud computing a révolutionné la manière dont les données et les applications sont gérées et déployées :

- Flexibilité : Les utilisateurs peuvent accéder aux ressources à la demande et payer uniquement pour ce qu'ils utilisent.
- Économie d'échelle: Les fournisseurs de cloud peuvent offrir des services à un coût réduit grâce à la mutualisation des ressources.
- Agilité: Les entreprises peuvent rapidement ajuster leurs ressources selon les besoins, accélérant les délais de mise sur le marché.

Les caractéristiques du Cloud Computing :

- Accès à distance: Accès aux ressources via Internet.
- Ressources partagées : Utilisation de ressources communes pour une meilleure efficacité.
- Élasticité: Ajustement dynamique des ressources en fonction des besoins.

- Gestion centralisée: Administration centralisée des données et des applications.
- Services variés: Disponibilité de divers services (SaaS, PaaS, IaaS).
- Mises à jour automatisées : Gestion des mises à jour de manière centralisée.

Avantages du Cloud Computing:

- Scalabilité : Les ressources peuvent être augmentées ou réduites selon les besoins.
- Coûts réduits : Pas besoin d'investissements lourds en infrastructure.
- Accès global : Les ressources sont accessibles de n'importe où via Internet.
- Maintenance réduite : Les fournisseurs de cloud s'occupent de la maintenance des infrastructures.

Risques du Cloud Computing:

- Sécurité des données : Risque de perte de données et violations de confidentialité.
- Attaques informatiques : Menace constante de cyberattaques.
- Interruptions de service : Risque d'indisponibilité des services.

Composants Fondamentaux de l'Architecture Cloud :

1. **Virtualisation:** Virtualisation des serveurs, du stockage et des réseaux pour une utilisation efficace des ressources.
2. **Infrastructure:** Comprend les serveurs physiques, le stockage persistant et les équipements réseau.
3. **Middleware:** Composants logiciels permettant la communication entre applications et systèmes.
4. **Gestion:** Outils de surveillance et de gestion des performances et capacités de l'environnement cloud.
5. **Automatisation:** Outils pour automatiser les tâches de gestion et d'exploitation des ressources cloud, permettant des déploiements rapides et une gestion efficace

la virtualisation

La virtualisation est une technologie clé dans le cloud computing, offrant divers avantages en termes de gestion et d'efficacité des ressources :Simulation, émulation et virtualisation : Création d'environnements simulés pour différentes applications.

Types de virtualisation :

- **Virtualisation de serveur :** Partage des ressources d'un serveur physique entre plusieurs systèmes d'exploitation.
- **Virtualisation de poste de travail :** Exécution de plusieurs systèmes d'exploitation sur un seul ordinateur.
- **Virtualisation de stockage :** Gestion centralisée des ressources de stockage.
- **Virtualisation de réseau :** Création de réseaux virtuels indépendants des infrastructures physiques.
- **Virtualisation d'application :** Exécution d'applications sur des systèmes d'exploitation différents de ceux pour lesquels elles ont été conçues.
- **Virtualisation de données :** Abstraction des détails techniques pour une meilleure accessibilité et résilience des données.

Virtualisation vs Conteneurisation

- **Virtualisation :** Crée des environnements virtuels complets qui imitent des systèmes informatiques entiers. Consomme plus de ressources.
- **Conteneurisation :** Emballe une application et ses dépendances dans un conteneur léger qui partage le noyau de l'hôte. Plus efficace en termes de ressources et plus rapide à déployer

Modèles IaaS, PaaS et SaaS

- **IaaS (Infrastructure as a Service) :** Offre des ressources informatiques telles que des serveurs virtuels, du stockage et des réseaux. Exemples : AWS, Microsoft Azure.
- **PaaS (Platform as a Service) :** Fournit une plateforme pour développer, tester et déployer des applications. Exemples : Heroku, Google App Engine.
- **SaaS (Software as a Service) :** Fournit des applications hébergées accessibles via Internet. Exemples : Salesforce, Office 365.

Types de Services en Cloud Computing

- **Infrastructure en tant que Service (IaaS) :**Fournit des ressources informatiques telles que des serveurs virtuels, du stockage et des réseaux.Exemple : Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform.
- **Plateforme en tant que Service (PaaS) :**Offre des plateformes de développement et de déploiement pour les applications, comprenant des bases de données et des outils de développement. Exemple : Heroku, OpenShift, Google App Engine.
- **Logiciel en tant que Service (SaaS) :**Propose des applications logicielles en ligne accessibles via Internet.Exemple : Salesforce, Office 365, Gmail.
- **Stockage et Sauvegarde en Ligne:**Services de stockage de données en ligne, incluant sauvegarde et synchronisation de fichiers. Exemple : Dropbox, Google Drive, Amazon S3.
- **Analyse en Ligne:** Services d'analyse de données comme la Business Intelligence (BI) et le Machine Learning (ML).Exemple : Google BigQuery, AWS SageMaker, Microsoft Power BI.

Types de Ressources en Cloud Computing

- **Serveurs Virtuels:** Fournissent des machines virtuelles (VM) pour exécuter des applications et des services. Exemple : EC2 (AWS), Virtual Machines (Azure).
- **Mémoire:** Ressources de mémoire pour le stockage temporaire des données utilisées par les applications. Exemple : RAM allouée à une VM.
- **Stockage:** Divers types de stockage comme les disques SSD et HDD pour les données persistantes. Exemple : Amazon EBS, Azure Blob Storage.
- **Bases de Données:** Services de bases de données gérées pour stocker et accéder aux données structurées et non structurées. Exemple : Amazon RDS, Azure SQL Database, Google Firestore.
- **Réseaux:** Fournit des services de mise en réseau comme les Virtual Private Clouds (VPC) et les Content Delivery Networks (CDN).Exemple : AWS VPC, Azure Virtual Network.
- **Applications:** Applications logicielles accessibles via Internet. Exemple : Google Workspace, Microsoft Office 365.
- **Services et Fonctionnalités:** Inclut des services divers comme l'authentification, l'analyse, et la sécurité. Exemple : AWS Lambda (serverless computing), Azure Active Directory.

Facturation Pay-as-You-Go

La facturation "Pay-as-You-Go" (PAYG) permet de payer uniquement pour les services utilisés. Cela offre des avantages comme :

- Flexibilité des coûts : Les utilisateurs paient pour ce qu'ils consomment, sans frais fixes mensuels.
- Efficacité économique : Réduction des coûts pour les utilisateurs qui n'ont pas besoin d'un usage constant.

Organisation des Ressources et Comptes d'Administration

Les Abonnements Azure

- Libre : Accès gratuit avec un crédit initial pour tester les services.
- Pay-As-You-Go : Facturation mensuelle basée sur la consommation.
- Entreprise : Contrats pour des achats groupés avec des remises.
- Étudiant : Offres spéciales sans carte de crédit avec crédits limités.

Les Types de Comptes Azure :

- Administrateur de Comptes : Responsable de l'abonnement et de la facturation.
- Administrateur de Services : Gère les ressources mais sans responsabilité de facturation.
- Co-Administrateur : Partage les privilèges de gestion des ressources avec l'administrateur de services.

Abonnement et Accès AWS :

- Toutes les ressources créées sous le compte AWS sont liées au compte d'administration, avec des contrôles d'accès gérés par AWS Identity and Access Management (IAM).

Abonnement et Accès Google Cloud :

- Nécessite un compte de facturation séparé du compte d'administration.

Gérer les Ressources Matérielles et Logicielle

Exploitation des VM et Conteneurs :

- VM : Machines virtuelles pour exécuter des applications et des services.
- Conteneurs : Environnements légers pour exécuter des applications isolées, utilisant des orchestrateurs comme Kubernetes.

Réseaux Virtuels:

- NSG (Network Security Group) : Définit des règles de sécurité pour filtrer le trafic réseau.
- NVA (Network Virtual Appliance) : Machines virtuelles exécutant des fonctions réseau spécialisées.
- Load Balancer : Assure la répartition du trafic réseau pour optimiser la disponibilité et les performances.
- Peering : Connecte des réseaux virtuels pour permettre la communication entre eux.
- Hub and Spoke : Architecture réseau pour gérer des connexions complexes entre plusieurs réseaux.
- Service Endpoints : Offre une connectivité sécurisée aux services Azure.
- ExpressRoute : Connexion privée directe aux réseaux virtuels Azure, offrant une fiabilité et une sécurité accrues.

Stockage Virtuel:

- Comptes de Stockage : Conteneurs pour les services de stockage Azure.
- Types de Comptes de Stockage : Standard et Premium, avec différentes options de redondance (LRS, ZRS, GRS, GZRS)

Configuration des Services de Stockage et Applications Virtuelles dans Azure :

Configuration du Service de Stockage :

Après la création d'un compte de stockage dans Azure, vous pouvez configurer différents types de services de stockage en fonction de vos besoins.

1. Créer un compte de stockage :

- Accédez au portail Azure et créez un compte de stockage.
- Sélectionnez le type de stockage (Standard/Premium, V2/BlobStorage).

2. Configurer le service de stockage de fichiers :

- Dans le compte de stockage, choisissez
- Créez un nouveau partage de fichiers et définissez les quotas et permissions nécessaires.
- Vous pouvez ensuite créer des dossiers et configurer les autorisations d'accès.

Applications Virtuelles avec Azure App Service :

Azure App Service permet de créer et d'héberger des applications web, des back-ends mobiles et des API RESTful. Les avantages incluent une mise à l'échelle automatique, une haute disponibilité, et la compatibilité avec divers langages de programmation. Voici comment configurer un App Service :

1. Créer une nouvelle application :
   - Accédez au portail Azure et sélectionnez App Services.
   - Cliquez sur Créer une ressource et choisissez App Service.
   - Remplissez les informations nécessaires (nom de l'application, abonnement, groupe de ressources, système d'exploitation).
2. Configurer l'application :
   - Choisissez le plan App Service qui convient à vos besoins (Windows/Linux, Basic/Standard/Premium).
   - Déployez votre application à partir de sources telles que GitHub, Azure DevOps ou un dépôt Git local.

Bases de Données dans Azure :

Pour Azure SQL Database, il existe trois modèles de déploiement et deux modes d'approvisionnement :

1. Modèles de déploiement :
   - Unique Database: Base de données unique avec une gamme complète de fonctionnalités.
   - Elastic Pool: Regroupe plusieurs bases de données avec des ressources partagées.
   - Managed Instance: Offre une compatibilité étendue avec SQL Server et des fonctionnalités de gestion simplifiées.
2. Modes d'approvisionnement :
   - DTU (Data Transaction Unit) : Mesure combinée du processeur, de la mémoire, des lectures et des écritures.
   - vCore (Virtual Core) : Permet de choisir les caractéristiques physiques du matériel (nombre de cœurs, mémoire, taille du stockage). Inclut le mode Serverlesspour une scalabilité automatique.
3. Configuration de la sécurité :
   - Ajoutez une autorisation pour l'adresse IP du poste client dans les paramètres du pare-feu.
   - Utilisez SQL Server Management Studio pour se connecter au serveur de base de données en utilisant le compte administrateur.

Gestion des Données en Cloud

Contrat de Niveau de Service (SLA)

Les SLA définissent les engagements du prestataire cloud en termes de disponibilité et de connectivité. Chaque service Azure possède son propre contrat SLA avec des termes, des limitations et des crédits de service associés

Récupération et Redondance des Données :

1. **Techniques de redondance :**
   - Réplication : Utilisation de ZRS (Zone-Redundant Storage) et GZRS (Geo-Zone-Redundant Storage) pour assurer la redondance des données.
   - Équilibreur de charg: Utiliser plusieurs machines virtuelles derrière un équilibreur de charge pour assurer la disponibilité.
   - Partitionnement: Diviser les bases de données pour optimiser l'extensibilité et la disponibilité.
   - Déploiement multi-région: Utiliser Azure Traffic Manager pour gérer le basculement entre les régions.
   - Récupération des données :
   - Configurez les options de sauvegarde, planification et rétention selon les besoins spécifiques.
   - Sécurisation des Données

1. **Chiffrement et Protection des Accès :**
   - Chiffrement : Utilisation d'AIP pour chiffrer les messages et documents.
   - Access Keys : Utilisez les clés d'accès pour authentifier les demandes. Conservez-les dans Azure Key Vault et remplacez-les régulièrement.

- Signature d'Accès Partagée (SAS) : Contrôlez granulairement l'accès aux ressources de stockage.

2. Classification :

- Les administrateurs définissent des règles pour protéger les données sensibles. Les utilisateurs peuvent appliquer des étiquettes de classification pour sécuriser les documents**.**

supervision et Optimisation des Coûts

1. Supervision :

- Surveillez les journaux d'activités et les métriques (CPU, mémoire, I/O réseau).
- Utilisez des outils comme Azure Monitor pour suivre l'utilisation des ressources.

2. Optimisation des coûts :

- Utilisez des outils comme le TCO (Total Cost of Ownership) pour comparer les coûts d'exploitation des infrastructures existantes par rapport au cloud.
- Adoptez des bonnes pratiques pour réduire les coûts, comme la localisation des services dans des régions moins coûteuses et l'optimisation des services activés.

Gestion de la Continuité du Service

1. **Résilience :**

- Utilisez des zones de disponibilité pour garantir que les applications peuvent basculer automatiquement d'une zone à l'autre sans interruption.
- Employez des couplages de réplication inter-région pour augmenter la résilience.

2. Azure Site Recovery :

- Assurez la continuité des activités en répliquant les charges de travail vers un emplacement secondaire. Utilisez Site Recovery pour basculer et revenir aux emplacements primaires lors des pannes.

Présentation des Plateformes de Cloud

Microsoft Azure :

- **Azure** est une plateforme complète offrant des services pour gérer toutes les opérations informatiques.
- **Utilisateurs :** Utilisé par 85% des entreprises du Fortune 500.
- **Stockage des données:** Stockées dans des centres de données Microsoft à travers le monde.
- **Part de marché:** 20% au premier trimestre 2021.

Amazon AWS :

- **AWS:** Leader du marché avec une large gamme de services cloud.
- **Fonctionnalités:** Offre Amazon EC2 pour les VM, et des services de réseau de pointe.
-**Part de marché:** Contrôle plus de 50% des dépenses mondiales en services d'infrastructure cloud avec Azure.

Google Cloud Platform (GCP)

-**GCP:** Offre des services cloud complets avec une évolution rapide pour devenir compétitif.
- **Historique :** Lancé avec Google App Engine, devenu GCP en 2013

Autres Acteurs du Marché :

- **Alibaba Cloud :** Fournisseur chinois offrant des services de cloud computing.
- **Salesforce :** CRM basé sur le cloud.
- **OVH Cloud:** Fournisseur français de solutions cloud.
- **IBM Cloud:** Offre combinée de PaaS et IaaS.
- **DigitalOcean:** Fournit des plateformes d'infrastructure cloud pour les développeurs, startups et PME.

Cloud au Maroc :

Atlas Cloud Services : Initiative marocaine pour promouvoir la souveraineté digitale et la transformation digitale des entreprises locales, fruit d'un partenariat entre l'OCP et l'Université Mohammed VI Polytechnique.

Mise en place d'une Plateforme Open Source : OpenStack

OpenStack est une plateforme open source de cloud computing fondée en 2010 par la NASA et Rackspace. Conçue pour permettre la mise en place flexible et temporaire de réseaux informatiques, elle a attiré des entreprises telles qu'AT&T,

RedHat, Canonical (développeur d'Ubuntu), Intel, IBM et Huawei, qui ont contribué à son développement. OpenStack fonctionne exclusivement sur Linux et est publié sous une licence Apache, garantissant un accès libre au code source et une utilisation gratuite.
La dernière version d'OpenStack, nommée "Yoga", a été publiée en mars 2022. OpenStack permet de créer et gérer des clouds privés et publics à partir de pools de ressources virtuelles.

Architecture et Composants d'OpenStack :

OpenStack se compose de plusieurs outils, ou "projets", qui assurent les principaux services de cloud computing :

- Nova : Composant de calcul responsable de la gestion des instances de machines virtuelles (VM) et de l'équilibrage de charge.
- Cinder : Fournit un stockage en bloc persistant pour les instances de VM, permettant de créer et gérer des volumes de stockage qui peuvent être attachés et détachés.
- Neutron : Service de réseau qui gère les réseaux virtuels, les sous-réseaux et les connexions entre les instances de VM.
- Glance : Permet de stocker et de récupérer des images de machines virtuelles, utilisées pour créer de nouvelles instances de VM.
- Keystone : Service d'authentification et d'autorisation qui gère l'authentification des utilisateurs et des services, ainsi que l'autorisation des actions qu'ils peuvent effectuer.
- Heat : Service d'orchestration permettant de déployer et de gérer des applications complexes en utilisant des modèles définis par l'utilisateur.
- Horizon : Interface utilisateur web officielle d'OpenStack, offrant un tableau de bord pour gérer et surveiller l'infrastructure cloud.

Les principaux services du cloud OpenStack comprennent :

- Horizon (Dashboard)
- Nova (Compute Service)
- Keystone (Identity Service)
- Glance (Image Service)
- Neutron (Networking)
- Cinder (Block Storage)
- Swift (Object Storage)

Automatisation et Orchestration du Cloud

L'automatisation consiste à remplacer une tâche manuelle par une tâche automatique et planifiée. Elle permet de minimiser les processus manuels, augmenter l'efficacité et la fiabilité, et gérer une quantité croissante de données, d'applications et de systèmes.

L'orchestration relie des tâches automatisées en un workflow homogène pour réaliser un objectif, en supervisant les autorisations et en appliquant des règles. Elle est utilisée pour le provisioning, le déploiement ou le démarrage de serveurs, l'acquisition et l'affectation de capacité de stockage, la gestion de réseau, la création de VM, et l'accès à des logiciels spécifiques dans le cadre de services cloud.

L'orchestration du cloud est particulièrement utile pour les services informatiques et les adeptes de DevOps, car elle permet de fournir des ressources cloud aux clients et utilisateurs selon un modèle de libre-service. Parmi les solutions d'orchestration, on peut citer :

- Apache AirFlow
- Kubernetes
- Microsoft Azure Automation
- OpenStack Heat

M206 – SÉCURISER UNE INFRASTRUCTURE DIGITALE

La sécurité

La sécurité : est protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les menaces, les atteintes à la confidentialité, les attaques malveillantes et les perturbations.
les principaux objectifs de la sécurité :

- **La disponibilité :** S'assurer qu'une donnée ou service soit toujours disponible aux personnes autorisées.
- **La confidentialité :** S'assurer que les données ne sont accessibles que par les personnes autorisées.
- Définir l'intégrité et donner un exemple de mise en place ?
- **L'intégrité :** S'assurer que les données n'ont pas été modifiées pendant le traitement, stockage et transfert.
- **Authentification :** vérifier l'identité des utilisateurs avant l'accès aux systèmes ou aux données sensibles.
- **Non-répudiation** : Ce principe assure qu'une action ne peut pas être niée par la suite.
- **Contrôle d'accès:** Gérer les droits d'accès des utilisateurs et des systèmes
- **Traçabilité:** exige de suivre les actions exécutées par une entité durant son accès à un actif

les classes de la sécurité :

- La sécurité de l'information
- La sécurité physique
- La sécurité de l'informatique
- La sécurité de communication
- La sécurité opérationnelle.

Un actif :se réfère à tout ce qui a de la valeur pour une entité (une organisation ou une personne) et qui nécessite donc d'être protégé par des mesures de sécurité.

les actifs d'une entreprise :

- Actifs matériels
- Actifs logiciels
- Actifs informationnels
- Actifs commerciaux.

Les Attaque informatique

Menace : Un potentiel de violation de la sécurité qui pourrait exploiter une ou plusieurs vulnérabilités d'un actif pour l'endommager. Ou bien un danger dans l'environnement de l'entreprise qui peut exploiter une vulnérabilité.
Victime : la cible d'une attaque de sécurité.
Risque : C'est la probabilité qu'une menace puisse exploiter une vulnérabilité.
Contre-mesure : C'est l'ensemble des méthodes, techniques et outils pour la protection contre les attaques de sécurité.
Vulnérabilité : La faiblesse d'un actif (ou d'une ressource) l'expose à des menaces
Attaque : Une action ou un évènement non autorisée délibérée sur un actif pour causer son dysfonctionnement ou l'altération de l'information qu'il stocke.
Acteur de menace (Agent de menace):Une entité qui exécute et réalise une action de menace
Risque: la probabilité qu'une menace particulière exploite une vulnérabilité donnée).
Les virus : Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.
les antivirus : est un programme capable de détecter la présence de virus sur un ordinateur. Il existe La suppression du code correspondant au virus dans le fichier infecté ou La suppression du fichier infecté.
DDoS : Une attaque par déni de service distribué est une forme d'attaque informatique, souvent compromis par des logiciels malveillants, sont utilisés pour saturer les ressources d'un serveur cible.

Flooding : Une attaque par déni de service DoS est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser
SYN : (SYN flood) est une forme spécifique d'attaque par déni de service (DoS)
l'attaque IP Spoofing : C'est la falsification (usurpation) de l'adresse IP d'une machine victime.
l'attaque de Pharming : C'est une attaque qui exploite une faille de DNS qui permet la redirection des internautes vers de faux sites web.
l'attaque phishing : Tentative de vol d'informations sensibles (mot de passe, informations bancaires, etc) en utilisant des emails ou des pages web.
les méthodes pour casser un mot de passe :

- Attaque par dictionnaire
- force brute
- Hybride
- keylogger
- phishing, ...

White Hat Hacker (Pirate chapeau blanc): C'est un type de pirate qui a pour objectif de découvrir les vulnérabilités afin de les corriger.
Black Hat Hacker (Pirate chapeau noir): C'est un type de pirate qui exploite les vulnérabilités à des fins nuisibles.
Cracker : C'est un type de pirate qui contourne la protection des logiciels payants illégalement.
Hacktiviste : C'est un type de pirate pour des raisons idéologiques.
Attaque passive : c'est une attaque pour la surveillance des données sans modification.
Attaque active : c'est une attaque pour manipuler les données. Exemples : déni de service, modification, rejeu, ...
Attaque interne : c'est une attaque réalisée par des personnes à l'intérieur de l'organisation ou ayant une relation avec elle.
Attaque externe : c'est une attaque réalisée qui n'ont aucune relation avec l'organisation.
L'ingénierie sociale : c'est une attaque qui vise à exploiter la naïveté des personnes pour avoir accès non autorisé aux système d'information.
Ransomware : c'est une attaque qui bloque l'accès aux ressources (par cryptage) pour demander de l'argent (rançon) pour le rétablir.

Cryptographie

Cryptographie : Est une des disciplines de la cryptologie, s'attachant à protéger des messages.
Chiffrement et déchiffrement : le chiffrement et la transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement.
Chiffrement symétrique : se basent sur une même clé pour chiffrer et déchiffré un message. On utilisés les algorithme: DES , AES ,RC4.
Chiffrement Asymétrique : Il se base sur le principe de deux clés : Une publique, permettant le chiffrement. Une privé, permettant le déchiffrement. on utilisés la algorithme: RSA
fonction de hachage : est un algorithme qui prend une entrée de données, comme un fichier ou un message, et génère une sortie de taille fixe, appelée hash ou empreinte. Cette sortie est unique pour chaque entrée de données et peut être utilisée pour vérifier l'intégrité des données On utilisés les algorithme: MD5, SHA.
La signature électronique : est un procédé permettent de garantir l'authenticité de l'expéditeur et de vérifier l'intégrité du message reçu. La signature électronique = hachage + clé privé.

Un certificat électronique : C'est une méthode cryptographique pour empêcher l'usurpation de l'identité. Il contient la clé publique de l'utilisateur, les informations sur l'utilisateur et les informations sur l'autorité de certification (CA). Exemple de certificat X.509

Les protocole de sécurité

le pare-feu : (firewall) est un dispositif de sécurité qui contrôle le trafic réseau entrant et sortant, en appliquant des règles prédéfinies pour autoriser ou bloquer les connexions. Il protège les réseaux internes contre les accès non autorisés et les attaques externes.

Les types de pare-feu :

les pare-feu matériels : qui sont des dispositifs physiques dédiés,

les pare-feu logiciels :qui sont des programmes installés sur des ordinateurs ou des serveurs.

Une DMZ : (Zone Démilitarisée) est une zone de réseau isolée utilisée pour héberger des services accessibles depuis l'extérieur, tout en protégeant le réseau interne. Elle permet de limiter les risques en cas de compromission des serveurs publics.

proxy server: Le serveur proxy est une machine fonction d'intermédiaire entre les ordinateurs d'un réseau local et l'internet.

Les fonctionnalités d'un serveur proxy :

- La fonction de cache
- Reverse proxy
- Le filtrage.
- L'authentification.

IDS/ IPS : surveille et contrôle le trafic réseau, IDS identifiant les comportements malveillants, et IPS identifiant les comportements malveillants et bloquant les attaques

UTM : (Unified Threat Management) est un pare-feu réseau avancé qui regroupe plusieurs fonctionnalités de sécurité telles que le filtrage de URL en utilisé (IDS/IPS)

SIEM : (Security Information & Event Management) est une solution intégrée qui combine le SIM (gestion des informations de sécurité) et le SEM (gestion des événements de sécurité), offrant une vision centralisée des événements de sécurité et des informations sur les menaces, permettant une réponse rapide aux incidents.

DLP : (Data Loss Prevention) est un système de protection des données qui contrôle et bloque la transmission de données sensibles, prévenant ainsi la fuite d'informations confidentielles.

SEG : (Secure Email Gateway) est une passerelle de messagerie sécurisée qui analyse les e-mails entrants et sortants à la recherche de menaces potentielles, telles que les logiciels malveillants ou le phishing, avant qu'ils n'atteignent les systèmes de messagerie de l'entreprise

VPN: (Virtual Private Network) crée une connexion sécurisée et chiffrée sur un réseau public ou privé, permettant aux utilisateurs de protéger leurs données et de masquer leur adresse IP. Cela améliore la confidentialité en ligne et permet l'accès à des ressources réseau de manière sécurisée.

les types de VPN :

- VPN site à site : protocoles utilisées (IPSec).
- VPN accès distant : protocoles utilisées (IPSec et TLS).

types de protocoles de tunnuling de VPN :

- IPSec
- GRE
- PPTP
- L2TP

AH : implémente l'intégrité et l'authentification.

ESP : implémente l'intégrité et l'authentification et la confidentialité.

la différence entre les 2 méthodes IPsec :AH et ESP :ESP plus sécurisé que AH, car ESP implémente la confidentialité en plus de l'intégrité et l'authentification.

iptables : est un utilitaire en ligne de commande sous Linux permettant de configurer et de gérer les règles du pare-feu du noyau Linux pour filtrer et manipuler le trafic réseau. Il contrôle le flux des paquets de données en définissant des chaînes et des règles spécifiques pour autoriser, bloquer ou rediriger le trafic.

OpenSSL : est une bibliothèque logicielle robuste et complète pour la mise en œuvre des protocoles de sécurité SSL (Secure Sockets Layer) et TLS (Transport Layer Security). Elle fournit des outils de cryptographie pour chiffrer et déchiffrer les données, générer des certificats numériques, et gérer les clés cryptographiques.

Comment avoir un mot de passe fort

- Mélange entre les lettres minuscules et majuscules, chiffres et caractères spéciaux.
- Longueur minimal de 10 caractères.
- Difficile à deviner (Ne pas utiliser des mots dictionnaires).

les mesures de sécurités qu'on peut utiliser pour sécuriser notre système

- Sécurité physique (ex : caméra de surveillance) ;
- Pare-feu (firewall) ;
- Antivirus ;
- Mise à jour des SE ;
- Authentification à 2 facteurs ;
- Vigilance.