Configuration de base d'un routeur

Passer à la mode privilégié :
R1> enable
pour régler la date et l'heur
Router #clock set 12 :30 :00 11 sept 2015
Configurez le nom d'hote
R1(config)# hostname name
Désactivez la recherche DNS
R1(config)# no ip domain-lookup
Désactivez le service HTTP
R1(config)# no ip http server
Attribuer le mot de passe à l'accés par console
R1(config)# line console 0
R1(config-line)# password password
R1(config-line)# login
Éviter les messages d'état d'interrompre
les entrées de ligne de commande
R1(config-line)# logging synchronous
Attribuer le mot de passe à l'accés par Telnet
R1(config)# line vty 0 4
R1(config-line)# password password
R1(config-line)# login
Utilisez un mot de passe au mode d'éxécution privilégié
R1(config)# enable password password
Attribuer le mot de passe par mode privilégié (crypté)
R1(config)# Enable secret password
Attribuer le mot de passe à l'accés par auxiliaire
R1(config)# line aux 0
R1(config-line)# password password
R1(config-line)# login
Chiffrez tous les mots de passe en texte claire
R1(config)# service password-encryption
Incluez un message dans la banniére MOTD
R1(config)# banner motd # message #
pour redémarrer un routeur
Router # reload
afficher les informations de dépannage du routage
R1 #debug ip routing
Enregistrez vos configuration :
R1# copy running-config startup-config

Configuration de SSH

Définissez un nom de domain
R1(config)# ip domaine-name domain.com
Générez la clé RSA
R1(config)# crypto key generate RSA
Créez un utilisateur local avec un mot de passe
R1(config)# username admin password password
Paramétrez toutes les lignes pour utilizer SSH et
un login local pour les connexions à distance
R1(config)# line vty 0 4
R1(config-line)# transport input SSH
R1(config-line)# login local

Activez SSH version 2

R1(config)# ip SSH version 2
Modifier la tentatives d'authentification SSH
R1(config)# ip SSH authentication-retries 3
Modifier la valeur du délai d'attente de SSH
R1(config)# ip SSH time-out 60
Supprimer la paire de clés RSA et désactivé le serveur SSH
R1(config)# crypto key zeroize rsa

RIP :

Activez et passer en mode de configuration RIP
R1(config)# router rip
Activez la version 2 du protocole RIP
R1(config-router)# version 2
Annoncez les réseaux RIP
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
Désactive la récapitulation automatique
R1(config-router)# no auto-summary
(Empêche l'interface indiquée d'envoyer de mises à jour)
R1(config-router)# passive-interface Fa0/1
(Propage le réseau candidat par défaut aux autres routeurs RIP du système autonome)
R1(config-router)# default-information originate
(Injecte les routes statiques locales et les propagent dans les mises à jour RIP)
R1(config-router)# redistribute static

Déclarer l'utilisation de clé sur interface :

R1(config-if)# ip rip authentification key-chain nom
R1(config-if)# ip rip authentification mode md5
Commandes show :
R1# show ip protocols (Parametres de Rip
R1#show ip route (Vérifier les routes)
R1# show ip route rip (Vérifier les routes rip)

Ipv6 :

Activer le Routage Rip V2 :
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 rip process1 enable
Maximum Path (pour la repartions de la charge) :
R1(config-if)# ipv6 rip process1 enable
R1(config-router)# maximum-paths 1
Activation de Ripng IPV6 :
R1(config)# interface S0/0/0
R1(config-if)# ipv6 rip RIP-AS enable
R1(config-if)# no shut

EIGRP:

Activez et passer en mode de configuration EIGRP
R1(config)# routeur eigrp 1
Configurer l'ID de routeur
R1(config-router) eigrp router-id 1.1.1.1
Annoncez les reseaux EIGRP
R1(config-router)# network 192.168.1.0 0.0.0.3

R1(config-router)# network 192.168.2.0 0.0.0.3
(Empêche l'interface indiquée d'envoyer des mises à jour)
R1(config-router)# passive-interface Fa0/1
Configurer la métrique :
R1(config-router)# metric weights tos k1 k2 k3 k4 k5
Modification de la bande passante d'interface
R1(config)# interface S0/0/0

R1(config-if)# bandwidth 64
Activez la récapitulation automatique

Les Access liste IPv4:

@S da2iman kanconfiguwrha f router li 9rib man @D
Une access liste standard numéroté
R1(config)# access-list [1-99] [permit/deny] [@IPsrc MG/any]
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
da2iman kanconfiguwrha f router li 9rib man @S
Une access liste étendues numerate
R1(config)# access-list [100-199] [permit/deny] [protocole] [@IPsrc MG/any] [@IPdst MG/any] [eq N°]
R1(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
Une access liste standard nommée
R1(config)# ip access-list standard name
R1(config-std-nacl)# [permit/deny] [@IPsrc MG/any]
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
Une access liste étendues nommée
R1(config)# ip access-list extended name
R1(config-ext-nacl)# [permit/deny]
[protocole] [@IPsrc MG/any] [@IPdst MG/any] [eq N°]
R1(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
Appliquer une liste de controle d'accés sur interface
R1(config)# interface g0/1
R1(config-if)# ip access-group [N°/name] [in/out]
R1(config-if)# ip access-group 100 in
Appliquer une liste de controle d'accés sur une ligne
R1(config)# line vty 0 4
R1(config-line)# access-class [N°/name] [in/out]
R1(config-line)# access-class 100 in

Configuration aggregation entre les switch

S1(config)# interface F 0/1
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk native vlan 99 Indique la liste des VLAN autorisés sur la liaison trunk
S1(config-if)# swichtport trunk allowed vlan 10,20,70,99
Configurez la fonction périphérie PVLAN et protégé le port
S1(config)# interface F0/3
S1(config-if)# switchport protected
Empéche l'interface de générer des trames DTP
S1(config)#interface F0/4
S1(config-if)# switchport nonegotiate

EIGRP:

Activez et passer en mode de configuration EIGRP
R1(config)# routeur eigrp 1
Configurer l'ID de routeur :
R1(config-router)# router-id 1.1.1.1
Affectation d'interface à une zone OSPF :
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
Configurer une interface de boucl age pour l'utiliser comme ID :
R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
Annoncez les réseaux OSPF
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
Propagation d'une route par défaut :
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R1(config)# router ospf 10
R1(config-router)# default-information originate
R1(config-router)# end
information originate
Redistribution des routes statiques
R1(config-router)# redistribute static
Configuration l'interface passive
R1(config-router)# passive-interface G0/1
Modification de la bande passante de réferance
R1(config-router)# auto-cost reference-bandwidth 1000
Modification de la bande passante d'interface
R1(config)# interface S0/0/0
R1(config-if)# bandwidth 64
Indique le nombre maximum de sauts (diamètre du système autonome)
R1(config-router)# metric maximum-hops {valeur}
Réglage manuel du cout OSPF
R1(config)# interface S0/0/0
R1(config-if)# ip ospf cost 15625
Modification de la priority
R1(config)# interface S0/0/0
R1(config-if)# ip ospf priority 255
Suppression du processus OSPF
R1# clear ip ospf process
Modification des intervalles
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
Activation de l'authentification MD5 OSPF globalement
R1(config)#router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-if)# end
R1(config)# interface G0/0
R1(config-if)# ip ospf message-digest-key 1 md5 name
Réglage manuel de cout (commande alternative à BP) :
R1(config)# interface s0/0/1
R1(config-if)# ip ospf cost 15625
Changer la réference de la BP :
R1(config-router)# auto-cost reference -bandwith 1000
Afficher la table de voisinage :
R1# show ip ospf neighbors
Vérifier le processus OSPF :
R1# show ip ospf
Vérifier les paramètres OSPF d'une interface :
R1# show ip ospf interface brief
Activation de l'authentification MD5 OSPF sur les interfaces
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 name
Récapituler les routes pour une zone
R1(config-router) # area 0 range 10.10.0.0 255.255.252.0

IPV6

OSPF Multizone.
R1(config-router)# network 10.1.1.0 0.0.0.255 area 1
R1(config-router)# network 10.1.2.0 0.0.0.255 area 1
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
Configurer les adresses link-local :
R1(config)# interface g0/0
R1(config-if)# ipv6 adresse fe80::1 link-local
R1(config)# exit

Configuration de SSH

Définissez un nom de domain
S1(config)# ip domaine-name domain.com
Générez la clé RSA
S1(config)# crypto key generate RSA
Créez un utilisateur local avec un mot de passe
S1(config)# username admin password password
Paramétrez toutes les lignes pour utilizer SSH et un login local pour les connexions à distance
S1(config)# line vty 0 15
S1(config-line)# transport input SSH
S1(config-line)# login local

Activez SSH version 2

S1(config)# ip SSH version 2
Modifier la tentatives d'authentification SSH
S1(config)# ip SSH authentication-retries 3
Modifier la valeur du délai d'attente de SSH
S1(config)# ip SSH time-out 60
Supprimer la paire de clés RSA et désactivé le serveur SSH
S1(config)# crypto key zeroize rsa

SSH

SH (Secure SHell), il fonctionne avec TCP/22, c'est un protocole de communication sécurisé, ainsi qu'il paermet d'ouvrir une session à distante mais plus sécurisé.

1-Installation des packages :

[root@user]# rpm -ivh openssh-...
[root@user]# rpm -ivh openssh-server-...

2-Configuration du fichier :

[root@user]# vi /etc/ssh/sshd_config

Port 22		(Num de port)
Protocole 2	(Version)	
ListenAddress 192.168.10.15		(l'@ de serveur)
PermitRootLogin yes	(autoriser l'accès Root)	
PermitEmptyPasswords no		(autoriser ou non mot d passe vide)
PasswordAuthentication yes		(s'authentifier ou non)

3-Démarrer le service SSH :

[root@user]# service sshd restart

4-sur la machine client on utilise le logiciel Putty :

Host name = @IP_du_serveur
root +mot de passe de root

HSRP,GLBP

Configurez HSRP sur R1 :
R1(config)# interface g0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
Configurez HSRP sur R3:
R3(config)# interface g0/1
R3(config-if)# standby 1 ip 192.168.1.254
Vérifiez le protocole HSRP.
R1# show standby
R1# show standby brief
Désactivez HSRP :
R1(config)# interface g0/1
R1(config-if)# no standby 1
Configurez le protocole GLBP sur R1.
R1(config)# interface g0/1
R1(config-if)# glbp 1 ip 192.168.1.254
R1(config-if)# glbp 1 preempt
R1(config-if)# glbp 1 priority 150
R1(config-if)# glbp 1 load-balancing round-robin
Configurez le protocole GLBP sur R3.
R3(config)# interface g0/1
R3(config-if)# glbp 1 ip 192.168.1.254
R3(config-if)# glbp 1 load-balancing round-robin
R1(config-router)# auto-summary
(Propage le réseau candidat par défaut aux autres routeurs EIGRP du système autonome)
R1(config-router)# default-information originate
(Propages les routes statiques locales dans les mises à jour EIGRP)
R1(config-router)# redistribute static
Configurez d'une route récapitulative manuelle
R1(config)# interface S0/0/0
R1(config-if)# ip summary-address eigrp 1 192.168.0.0255.255.255. 0
Configurez le pourcentage de bande passante utilisé par EIGRP
R1(config-if)# ip bandwidth-percent eigrp 1 40
Modification des intervalles hello
R1(config-if)# ip hello-interval eigrp 1 50
tempt d'attent
R1(config-if)# ip hold-time eigrp 1 150
Modifiée la valeur de paths
R1(config-router)# maximum-paths 8
(Indique le nombre maximum de sauts)
R1(config-router)# metric maximum-hops 60

OSPF:

Activez et passer en mode de configuration OSPF
R1(config)# router ospf 1
Configurer l'ID de routeur :
R1(config-router)# router-id 1.1.1.1
Affectation d'interface à une zone OSPF :
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
Configurer une interface de boucl age pour l'utiliser comme ID :
R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
Annoncez les réseaux OSPF
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
Propagation d'une route par défaut :
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R1(config)# router ospf 10
R1(config-router)# default-information originate
R1(config-router)# end
information originate
Redistribution des routes statiques
R1(config-router)# redistribute static
Configuration l'interface passive
R1(config-router)# passive-interface G0/1
Modification de la bande passante de réferance
R1(config-router)# auto-cost reference-bandwidth 1000
Modification de la bande passante d'interface
R1(config)# interface S0/0/0
R1(config-if)# bandwidth 64
Indique le nombre maximum de sauts (diamètre du système autonome)
R1(config-router)# metric maximum-hops {valeur}
Réglage manuel du cout OSPF
R1(config)# interface S0/0/0
R1(config-if)# ip ospf cost 15625
Modification de la priority
R1(config)# interface S0/0/0
R1(config-if)# ip ospf priority 255
Suppression du processus OSPF
R1# clear ip ospf process
Modification des intervalles
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
Activation de l'authentification MD5 OSPF globalement
R1(config)#router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-if)# end
R1(config)# interface G0/0
R1(config-if)# ip ospf message-digest-key 1 md5 name
Réglage manuel de cout (commande alternative à BP) :
R1(config)# interface s0/0/1
R1(config-if)# ip ospf cost 15625
Changer la réference de la BP :
R1(config-router)# auto-cost reference -bandwith 1000
Afficher la table de voisinage :
R1# show ip ospf neighbors
Vérifier le processus OSPF :
R1# show ip ospf
Vérifier les paramètres OSPF d'une interface :
R1# show ip ospf interface brief
Activation de l'authentification MD5 OSPF sur les interfaces
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 name
Récapituler les routes pour une zone
R1(config-router) # area 0 range 10.10.0.0 255.255.252.0

NAT – PAT

Configuration de la fonction NAT statique
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#interface Serial 0/0//0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config_if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial 0/1//0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
R2(config_if)# ip nat outside
R2(config-if)# exit

Configuration de la fonction NAT Dynamique :

R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config_if)# ip nat inside source list 1 pool NAT-POOL1
R2(config-if)# exit
R2(config)# interface Serial 0/0//0
R2(config_if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial 0/1//0
R2(config_if)# ip nat outside
R2(config-if)# exit
Vérification des traductions NAT statique :
R2# show ip nat translations
Effacer les statistiques des traductions passées :
R2# clear ip nat statics
Configuration de la fonction PAT
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload

STP :

Configurer le cout de port
S1(config)# interface F0/1
S1(config-if)# spanning-tree cost 5
Définir S1 en tant que pont racine principal
S1(config)# spanning-tree vlan 1 root primary
Définir S2 en tant que pont racine secondaire
S2(config)# spanning-tree vlan 1 root secondary
Modifier la priorité de pont
S1(config)# spanning-tree vlan 1 priority '0-61440'
Changer la priorité d'un port :
S1 (config)# interface fastEthernet 'FA0/0'
S1 (config-if)# spanning-tree vlan 1 port-priority '0-240'
S1(config-if)# exit
Configurez portfast sur une interface
S1(config)# interface F0/1
S1(config-if)# spanning-tree portfast
Configurez portfast sur tout les interfaces non-trunk
S1(config)# spanning-tree portfast default
Configurez la protection BPDU sur une interface
S1(config-if)# spanning-tree bpduguard enable
Configurez la protection BPDU sur tout les interface qui utilise portfast
S1(config)# spanning-tree bdpuguard default
Configurez root guard sur une interface
S1(config-if)# spanning-tree guard root
Configurez Rapid PVST+
S1(config)# spanning-tree mode rapid-pvst
Specifies le type de liaison pour une interface
S1(config-if)# spanning-tree link-type point-to-point

Routage inter-VLAN :

Affectez l'interface au VLAN 10 et donnez lui une addresse
R1(config)# interface fa0/0.10
R1(config-subif)#encapsulation dot1q 10 R1(config-subif)# ip address 192.168.10.1 255.255.255.0
Affectez l'interface au VLAN 20 et donnez lui une addresse
R1(config)# interface fa0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
Affectez l'interface au VLAN native et donnez-lui une addresse
R1(config)# interface fa0/0.70
R1(config-subif)#encapsulation dot1q 70 native
R1(config-subif)# ip address 192.168.70.1 255.255.255.0
Activez tous les sous interfaces précedant
R1(config)# interface fa0/0
R1(config-if)# no shutdown

Protocol vtp

Définissez le serveur VTP
S1(config)# vtp mode server
S1(config)# version 1/2
Définissez le domain VTP
S1(config)# vtp domain cisco.com
Définissez le mot de passe VTP
S1(config)# vtp password password
Définissez le serveur VTP
S2(config)# vtp mode transparent
S2(config)# version 1/2
Définissez le domain VTP
S2(config)# vtp domain cisco.com
Définissez le mot de passe VTP
S2(config)# vtp password password
Définissez le client VTP
S3(config)# vtp mode client
S3(config)# version 1/2
Définissez le domain VTP
S3(config)# vtp domain cisco.com
Définissez le mot de passe VTP
S3(config)# vtp password password

Configuration de sécurité des ports :

Configuration de la sécurité des ports selon les @ MAC des post connecter (statique)
Définissez le mode d'interfce sur le mode d'accés
S1 (config)# interface F0/1
S1 (config-if)# switchport mode access
Activez la sécurité des ports
S1(config-if)#switchport port-security
@mac du poste et entrer manuellement
S1(config-if)#switchport port-security macaddress @Mac de pc
un seul a@ mac et autorisé sur ce port
S1(config-if)#switchport port-security maximum 1
Modifier le mode de violation d'un port
S1(config-if)#switchport port-security violation [restrict/protect/shutdown]

Routage statique:

Configuration d'une route statique de tronçon suivant
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 S0/0/0
Configuration d'une route statique entièrement spécifiée
R1(config)# ip route 192.168.1.0 255.255.255.0 G0/1 172.16.2.2
Configuration d'une route statique par défaut
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/0

DHCP:

Activer le service DHCP
R1(config) # service dhcp
Excludes une plage d'adresses L'adresse IP à ne pas attribuer aux clients
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
Configurez un pool DHCP
R1(config)# ip dhcp pool name
Configurez le réseau du pool (@réseaux a attribuer au clients)
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
Configurez l'addresse de la passerelle par défaut
R1(dhcp-config)# default-router 192.168.10.1
Configurez l'addresse du serveur DNS
R1(dhcp-config)# dns-server 192.168.10.5
configurez le nom de domaine
R1(dhcp-config)# domain-name domain.com
Durée de bail dhcp
R1(dhcp-config)# lease 7
Adress service wins
R1(dhcp-config)#netbios-name-server 192.168.1.5
Configurez une interface pour obtenir une addresse Auprès du serveur DHCP
R2(config)# interface G0/1
R2(config-if)# ip address dhcp
Configurez le relais DHCP sur une interface
R2(config)# interface G0/2
R2(config-if)# ip helper-address 192.168.10.5
Commandes Show :
Les commandes DHCPv4 configurées sur R1 :
R1# show running-config | section dhcp
Afficher la liste de toutes les liaisons entre adresse IPv4 et adresse MAC / Clients :
R1# show ip dhcp binding
Afficher les statistiques :
R1# show ip dhcp server statistics
Afficher les conflits :
R1# show ip dhcp server conflict
Activation de routage ipv6 :
R1(config)# ipv6 unicast-routing
Configuration en tant que serveur sans etat :
Configuration d'un pool :
R1(config)# ipv6 dhcp pool pool-name
Définir les parametres de Pool :
R1(dhcpv6-config)# dns-server ServeurDNS
R1(dhcpv6-config)# domain-name ServeurDNS
Configuration de l'interface DHCPv6 :
R1(config)# interface type-name
R1(config-if)# ipv6 dhcp server pool-name
R1(config-if)#ipv6 nd other-config-flag
Verification d'un serveur sans etat :
R1# show ipv6 dhcp pool
Configuration en tant que client sans etat :
R1(config)# interface g0/1
R1(config-if)# ipv6 enable
R1(config-if)#ipv6 address autoconfig
Verification d'un client sans etat :
R1# show ipv6 dhcp pool
Configuration en tant que serveur avec etat :
Configuration d'un pool :
R1(config)# ipv6 dhcp pool pool-name
Définir les parametres de Pool :
R1(dhcpv6-config)#address prefix 2001:DB8:CAFE:1::/64 lifetime infinite
R1(dhcpv6-config)# domain-name tri2a.ma
R1(dhcpv6-config)# dns-server 192.168.10.22

Commande de Relais de DHCPv6 :

R(config)# interface g0/0
R(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6

Configuration de la surveillance DHCP:

Activez la serveillance DHCP

S1(config)# ip dhcp snooping

Activez la serveillance DHCP pour les VLAN

S1(config)# ip dhcp snooping vlan 10,20

Définissez les ports fiables

S1(config)#interface F0/1
S1(config-if)# ip dhcp snooping trust
Limiter la fréquence de fausse requites dhcp
S1(config)#interface F0/2
S1(config-if)# ip dhcp snooping limit rate 5

DHCP

Dynamic Host Configuration Protocol, il fonctionne avec UDP/67 pour le serveur et UDP/68 pour le client, il permet de configurer dynamiquement les hôtes (Attribution d'@IP, Masque, Durée de bail, plage d'exclure,DNS, WINS, NomNB..)

1- Tester le ping entre les différents machines

2- Installer les packages :

[root@user]# rpm -ivh dhcpd-...

3- Configurer le fichier de configuration :

[root@user]# vi /etc/dhcp/dhcpd.conf
options domain-name "2triLan";
option domain-name-servers serv1.2tri.lan;
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.1 192.168.1.100;}

4- Démarrer le service DHCP :

[root@user]# service dhcpd start

5- Si on veut réserver une adresse IP pour une machine :

[root@user]# vim /etc/dhcp/dhcpd.conf
host pc1 {hardware ethernet 08:00:27:B7:AA:01;
fixed-address 192.168.1.10;}

6- Redémarrer le service DHCP :

[root@user]# service dhcpd restart

7- Afficher les baux attribué (Vérification):

[root@user]# cat /var/lib/dhcp/dhcpd.leases

STP :

Configurer le cout de port

S1(config)# interface F0/1
S1(config-if)# spanning-tree cost 5

Définir S1 en tant que pont racine principal

S1(config)# spanning-tree vlan 1 root primary

Définir S2 en tant que pont racine secondaire

S2(config)# spanning-tree vlan 1 root secondary

Modifier la priorité de pont

S1(config)# spanning-tree vlan 1 priority '0-61440'

Changer la priorité d'un port :

S1 (config)# interface fastEthernet 'FA0/0'
S1 (config-if)# spanning-tree vlan 1 port-priority '0-240'
S1(config-if)# exit

Configurez portfast sur une interface

S1(config)# interface F0/1
S1(config-if)# spanning-tree portfast

Configurez portfast sur tout les interfaces non-trunk

S1(config)# spanning-tree portfast default
Configurez la protection BPDU sur une interface
S1(config-if)# spanning-tree bpduguard enable Configurez la protection BPDU sur tout les interface qui utilise portfast
S1(config)# spanning-tree bdpuguard default
Configurez root guard sur une interface
S1(config-if)# spanning-tree guard root
Configurez Rapid PVST+
S1(config)# spanning-tree mode rapid-pvst Specifies le type de liaison pour une interface
S1(config-if)# spanning-tree link-type point-to-point

VTP

VTP serveur : c'est le mode VTP par defeaut les Vlan peut etre modifier

VTP client : -impossible de créer ou modifier ou supprimé de vlan

-les MSJ sont recu de la part de VTP serveur

-les Vlan sont stocké seulement dans la RAM

VTP transparent :-les commutateur écoute pas les annance VTP mais il transmet ou commutateur voisin par le lien trunk

Configuration de base d'un Switch

Passer à la mode privilégié :
S1> **enable**
pour régler la date et l'heur
S1 #**clock set** 12 :30 :00 11 sept 2015
Configurez le nom d'hote
S1(config)# **hostname** name
Désactivez la recherche DNS
S1(config)# **no ip domain-lookup**
Attribuer le mot de passe à l'accés par console
S1(config)# **line console 0**
S1(config-line)# **password** password
S1(config-line)# **login**
Éviter les messages d'état d'interrompre les entrées de ligne de commande
S1(config-line)# **logging synchronos**
Attribuer le mot de passe à l'accés par Telnet
S1(config)# **line vty 0 15**
S1(config-line)# **password** password
S1(config-line)# **login**
Utilisez un mot de passe au mode d'éxécution privilégié
S1(config)# **enable password** password
S1(config)# **enable secret** password
Les (nombre de line) dernier commandes sont enregistrer dans l'historique
S1#**terminal history size** 20
Chiffrez tous les mots de passe en texte claire
S1(config)# **service password-encryption Incluez un message dans la banniére MOTD**
S1(config)# **banner motd #** message **#**
Configurer l'interface de VLAN
S1(config)# **interface vlan 1**
S1(config-if)# **ip address** 192.168.1.10 255.255.255.0
configurer passerelle par défaut
S1(config)# **ip default-gateway** 192.168.1.1
pour redémarrer un routeur
S1 # **reload**
Enregistrez vos configuration
S1# **copy running-config startup-config**

Définir les adresses IP au VLANS :

Switch(config)# **interface vlan 10**
Switch(config-if)# **ip address** 10.0.0.2 255.255.255.0
Switch(config-if)# **no shutdown**

Creations des VLAN

S1(config)# **vlan** 99
S1(config-vlan)# **name gestion**
S1(config)# **vlan** 10
S1(config-vlan)# **name clients**

Affectation des ports

S1(config)# **interface** F0/1
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan** 99
S1(config)# **interface range** F0/2-15
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan** 10

1 - Configuration du service réseau :

Statiquement :
[root@user]# ifconfig eth0 192.168.1.254
netmask 255.255.255.0 up
ou par le fichier de configuration :
[root@user]# vi etc/sysconfig/network-scripts/ifcfg-eth0
# Nom de la carte réseau
DEVICE=eth0
# L'adresse de réseau
NETWORK=192.168.1.0
# L'adresse de broadcast
BROADCAST=192.168.1.255
# Démarrer l'interface au démarrage (yes/no)
ONBOOT=YES
# Le nom de la connexion
NAME=lan
# Le type de connexion
TYPE=Ethernet
# Protocole de configuration réseau (dhcp/none)
BOOTPROTO=none
# L'adresse IP statique
IPADDR0=192.168.1.254
# Le masque de sous-réseau (24 = 255.255.255.0)
PREFIX0=24
# La passerelle par défaut
GATEWAY0=192.168.1.1
# Le serveur DNS primaire
DNS1=192.168.1.1
#Redémarrer le service réseau
[root@user]# service Network restart
Arrêt du démon NetworkManager : [OK]
Configuration des paramètres réseau... [OK]
Démarrage du démon NetworkManager : [OK]

NFS

1-Installation des packages portmap :
[root@user]# rpm -ivh portmap-....
2-création d'un répertoire :
[root@user]# mkdir /root/2tri
[root@user]# chmod 777 /root/2tri
3-fichier de configuration /etc/exports :
[root@user]# vi /etc/exports
/root/2tri *(rw)
4-démarrage des services :
[root@user]# service nfs start
[root@user]# service portmap start
5-sous la machine client :
[root@user]# mount -t nfs l'@_du_serveur:/root/2tri /root/partage1
(monter le dossier /root/2tri sur cette machine)
6-création des fichiers sous la machine serveur
(/root/2tri/fich)
7-sur la machine client :
ls /root/partage1.

TELNET

Telnet (TErminal NETwork ou TELecommunication NETwork),
il fonctionne avec 23/tcp, il permet de créer ou d'accéder une session Telnet sur une machine distante.

1-Installation des packages :
[root@user]# rpm -ivh telnet-...
2-Configuration du fichier :
[root@user]# vi /etc/xinetd.d/telnet :
service telnet
{ flags = REUSE
socket_type = stream
wait = no
user = root
server = /usr/sbin/in.telnetd
log_on_failure += USERID
disable = no
port = 23}
3-Créer un utilisateur :
[root@user]# useradd client-telnet
[root@user]# passwd client-telnet
4-démarrer le service telnet :
[root@user]# service xinetd start
5-Au niveau client XP :
(sous l'invite de commande)
telnet
open
l'@_IP_du_serveur
login+password_of_client

BIND-DNS

(Domain Name Service) il fonctionne avec 'TCP-UDP'/53, c'est un service TCP/IP permettant la correspondance entre un nom de domaine qualifié (FQDN : Fully Qualified Domain Name) et une adresse IP.BIND (Berkley Internet Naming Daemon) le serveur DNS est le plus utilisé sur Internet.

1- Installer les packages :
[root@user]# rpm -ivh bind-...
2- Configurer le service DNS :
[root@user]# vi /etc/named.conf
3- Configurer les fichiers des zones :
[root@user]# vi /var/named/2tri.lan.zone
5- Configurer le fichier resolv.conf :
[root@user]# vi /etc/resolv.conf
6- Créer un lien symbolique entre les fichiers zones :
[root@user]# ln -s 2tri.lan.zone /var/named
[root@user]# ln -s 2tri.lan.rev /var/named
7- Changer les propriétaires des fichiers de zone :
[root@user]# chown named:named 2tri.lan.*
9- Démarrer le service BIND :
[root@user]# service named start

Les protocole de redondance est :

HSRP

HSRP definit un group de routeur Pour verifier l'etat HSRP utilisez la commande show standby

VRRPv2

un routeur VRRP est configuré pour executer le protocole VRRP conjointement à un ou plusieurs autres routeurs associes a un vlan

GLBP

Protocole FHRP proprietaire CISCO qui protege le trafic de données en provanace d'un routeur ou d'un cercuit defailant 'telque HSRP et VRRP ,tout en permettent un equilibrage de la charge (egalement appele partage de charge) au sein d'un groupe de routeur redondants

Etherchannel

Une thechnique de ressau local entre deux commutation permettent de regouper plusieurs port fast ethernet ou gigabite ethernet ou un seul canal logique

Les avantage etherchannel

-la plupart des taches de configuration peuvent etre realisees sur l'interface etherchannel
-offre d'aventage de bande passante en reposant sur port existant
-equilibrage de change

PAGP :

le Protocole PAGP est un protocole FHRP proprietaire de cisco qui facilite la creation automatique de liaison etherchannel

SAMBA

SAMBA fonctionne par un protocole SMB ((Server Message Block) avec un numéro de port 445,
c'est un service qui permet de partager les ressources (imprimante, Scanner, Dossier ...)
entre les systèmes Windows/Linux.

1-Installation des packages :
[root@user]# rpm -ivh samba-...
2-Fichier de configuration "/etc/samba/smb.conf" :
[root@user]# vi /etc/samba/smb.conf
[global]
workgroup = 2tri
encrypt passwords = yes
wins support = yes
log level = 1
max log size = 1000
read only = no
public = yes
[partage1]
comment = Répertoire partagé 1
path = /home/partage1
browseable =yes
public = no
writable = yes
printable = no
group = partage
[Bureau150]
comment = Laserjet 2100
printer = lj2100
valid users = user1 user2 user3
path = /var/spool/lj2100
public = no
writable = no
printable = yes
browseable = yes
guest ok = yes # guest OK
guest only = yes # guest only
create mode = 0777 # fully accessed
directory mode = 0777 # fully accessed
share modes = yes # warn if some people access to a file

3-Ajouter un utilisateur :
[root@user]# useradd samba-1
[root@user]# smbpasswd -a samba-1

4-Démarrage du service :
[root@user]# service smb start
5-Sur la machine cliente :
Démarrer> Exécuter> \\l'@IP_du_serveur

Configuration d'un serveur APPATCH

1. installer le paquage : yum install httpd
2. configuration APPATCH cd /var/www/html
creel une page HTML
nano /etc/conf/httpd.conf
3. Démarrage de http : désactiver le parfeu
démmarer la carte réseau: service network retstart
démarrer le service : service httpd restart ou cd /etc/rc.d/init.d/httpd restart
4. Accéder au serveur http trois maniéres pour accéder au serveur Apache :
http:\\localhost\ - http:\\172.0.0.1 - l'adresse su serveur depuis le naviguateur
5. Sécuriser Apache avec TLS (SSL)
Nous allons ensuite nous placer dans le répertoire d'Apache 2 (/etc/apache2)
pour générer lecertificat au bon endroit : #cd /etc/apache2
Création de la clé privée RSA :
Cette commande va vous permettre de générer une clé RSA :
openssl genrsa -out server.key 1024
A partir de la clé de tout à l'heure, vous allez pouvoir créer un certificat générique pour votre organisme :
#openssl req -new -key server.key -out server.csr

FTP

« File Transfer Protocol » C'est un protocole qui permet de partager des ressources (dossier et fichier). Il fonctionne avec TCP/21.
Donner une address statique :
ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up
Installation des packeges :
rpm –ivh /root/.gnome-desktop/RPMS/vsftpd-1.1.3-8.i386.rpm
Modifier le fichier de configuration:
vi /etc/vsftpd/vsftpd.conf
Assurer que vsftpd est exécuté au démarrage :
# chkconfig vsftpd on
# Port d'ecoute
listen_port=21
# Banniere de bienvenue
ftpd_banner=Bienvenue sur mon ftp perso
# Fichier de config PAM
pam_service_name=vsftpd
# Mode "standalone"
listen=YES
Pour plus de sécurité, on réduit les droits sur le fichier de configuration :
chmod 600 /etc/vsftpd/vsftpd.conf
CRÉATION DE L'UTILISATEUR SYSTÈME
Cet utilisateur sera le propriétaire des fichiers et dossiers que les utilisateurs virtuels vont créer.
groupadd ftpclient
useradd -g ftpclient -d /home/ftpclient ftpclient
passwd ftpclient
chown ftpclient:ftpclient /home/ftpclient
chmod 700 /home/ftpclient
DÉMARRER LE SERVICE VSFTPD
Une fois le fichier de configuration remplacé, on relance le serveur FTP en tapant en root :
/etc/init.d/vsftpd start
Pour démarrer, redémarrer et stopper le service, les commandes respectives sont (toujours en super utilisateur) :
service vsftpd start
service vsftpd restart
service vsftpd stop
TEST DE SERVEUR
Commande
1-Ouvrez l'invite de
2-Type -> ftp targetMachineIP
J'utilise ftp 192.168.1.5 dans ce cas,
3-Type de nom d'utilisateur et mot de passe
J'utilise racine et root123

EIGRP

Formile de calcule de la metrique
M = [K1*bande passante+K3*delai]
K1(Bp)=1
K2(charge)=0
K3(delai)=1
K4(fiabilite)=0
K5(fiabilite)=0

Configuration de la sécurité des ports avec apprentissage des @mac dynamic
S1 (config)# **interface** F0/2-5
S1(config-if)#**switchport port-security**
S1(config-if)#**switchport port-security dynamic** 3 **@mac diffirent sont autorisé dynamic**
S1(config-if)#**switchport port-security maximum** 3
S1(config-if)#**switchport port-security violation** [restrict/protect/shutdown]
Configuration de la sécurité des ports Rémanents (sticky)
S1 (config)# **interface** F0/5-6
S1(config-if)#**switchport port-security**
S1(config-if)#**switchport port-security sticky**
S1(config-if)#**switchport port-security maximum** 2
S1(config-if)#**switchport port-security violation** [restrict/protect/shutdown]

OPENLDAP

OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur (Comme AD sous windows), c'est une implémentation libre du protocole LDAP (LDAP = Lightweight Directory Access Protocol, il fonctionne avec 389/tcp).
##################**Au niveau du serveur**#####################

1- Installation et configuration de DNS :
rpm -ivh --replacepkgs bind-9...
rpm -ivh --replacepkgs bind-chroot....
•1- Configuration du fichier /etc/named.conf
-Création des zones : Zone directe et Zone inversé
-Configuration des fichiers des zones
•2- Configuration de fichier /etc/resolv.conf
search 2tri.lan
nameserver 192.168.1.254
•3- Démarrage de service BIND
service named restart

2-- Installation des packages nécessaires pour LDAP :
rpm -ivh ...
•Openldap-...
•Openldap-servers-...
•Openldap-clients-...
•Openldap-devel-...
•Cyrus-...

3- Fixer un mot de passe pour le root LDAP
slappasswd
copier (SSHA)....

4- Editer le fichier /etc/openldap/slapd.conf
suffix "dc=2tri, dc=lan"
rootdn "cn=manager,dc=2tri,dc=lan"
rootpw Coller (SSHA)...

5- Démarrer le service ldap
service slapd start

6- Créer des utilisateurs (les informations des utilisateurs sont stocké dans un fichier .ldif (format texte clair):
useradd user1
passwd user1
grep user1 /etc/passwd
user1:x:501:501::/home/user1/:bin/bash
grep user1 /etc/passwd > users.passwd
ls

7- Utilisation du fichier "/usr/share/openldap/migration/migrate_passwd.p1 :
>>script <fichier source (/etc/passwd)> <fichier destination .ldif>
/usr/share/openldap/migration/migrate_passwd.p1 users.passwd users.ldif
ls
vim users.ldif
(changer le nom de domaine)
dn: uid=user1,ou=People,dc=2tri,dc=lan
uid: user1
cn: user1
ObjectClass:

8- Créer un autre fichier .ldif qui contient le domaine et les unités d'organisation :
vim 2tri.lan.ldif
dn: dc=2tri,dc=lan
dc: 2tri
objectClass: dcObject
objectClass: organizationalUnit
ou: rootobject
dn: ou=People,dc=2tri,dc=lan
ou: People
description: utilisateurs
objectClass: organizationalUnit

9- Ajouter les informations sous les fichiers .ldif à la base de données LDAP
ldapadd -xW -D "cn=Manager,dc=2tri,dc=lan" -f 2tri.lan.ldif
Entrer la mot de passe de ldap
ldapadd -xW -D "cn=Manager,dc=2tri,dc=lan" -f users.ldif
Entrer la mot de passe de ldap

10- Partager /home avec tous les utilisateurs clients on utilisant NFS :
vim /etc/exports
/home 192.168.1.0/24(rw,sync)
exportfs -a

11- Démarrer les services nfs et portmap :
service portmap start
service nfs start
chkconfig portmap on
chkconfig nfs on
>>chkconfig permet de gérer les services (commande d'admin).
##################**Au niveau du client**#####################

1- Installation des packages nécessaires pour LDAP :
rpm -ivh ...
•Openldap-...
•Openldap-clients-...
•Openldap-devel-...

2- Renommer le /home par /home.local (on va monter le /home du serveur donc il faut séparer les 2 homes)
mv /home /home.local

3- Créer un nouveau /home :
mkdir /home

4- monter le home partagé :
mount 192.168.1.254:/home /home

5-- Activer ldap : (on va rendre la machine membre au domaine)
authconfig --enableldap --enableldapauth --ldapserver=192.168.1.254 --ldapbasedn="dc=2tri,dc=lan" --enablemd5 --enabeshadow (MD5 algorithme de cryptage)
>>on ouvrir une fenêtre bleue de configuration de l'authentification (dans cette fenêtre on va cocher : Utiliser LDAP + Utiliser les mot de passe MD5 + Utiliser les mots de passe masqués + Utiliser l'authentification LDAP + suivant + ok)

6- Redémarrer la machine et ouvrir la session avec l'utilisateur user1 qu'on déjà créer sur le serveur

Problemes lies à une implémentation OSPF à zone agrand taille :

Taille excessive de la base de données de lien (LSDB)
Taille excessive de la table de routage de grande taille
Frequence elevee des calculs de l'algorithme SPF
ZONE Federatrices
La conception herarchique du reseau definit au quel toutes les autres zones sont connectés directement
ROUTEUR interne :toutes les interfeace se situent dans le meme zone
ROUTEUR federateur :
ROUTEUR ABR (area border router) :routeur possedant des interfaces dans differentes zones
ROUTEUR ASBR (autonomous system boundary routeur) routeur possedant au moins une interface associe a un interreseau externe (autre système autonome)

3 problemes stp

1- Instabilite de la base des données MAC
2- Tempete de diffusion
3- Trames de monodiffusion en double

Les type de paquet (MESSAGE OSPF)

1- Hello
2- DBD
3- LSR
4- LSU
5- LSACK

Les avantege multizone
ABR : Rolie deux zone OSPF
ASBR : rolie deux deffirence (Ex :rip-ospf)

EtherChannel avec LACP :

Créez l'interface de canal de port(les ports regrouper dans le même lien)
S1 (config)# **interface range** f0/1-2
N attribuer on lien logique etherchannel avec le mode du lien active .passive.ON
S1 (config-if)# **channel-group** 1 **mode** active
Configurez port channel 1 en tant que trunk
S1(config-if)# **interface port-channel** 1
S1(config-if)# **switchport mode trunk**

EtherChannel avec PAGP:

Créez l'interface de canal de port(les ports regrouper dans le même lien)
S1(config)# **interface range** f0/1-2
N attribuer on lien logique etherchannel avec le mode du lien Désirable .AUTO.ON
S1(config-if)# **channel-group** 1 **mode** ON
Configurez port channel 1 en tant que trunk
S1(config)# **interface port-channel** 1
S1(config-if)# **switchport mode trunk**

Mode LACP

;W1	SW2	ETABLISMENT
)N	ON	OUI
\CTIVE	ACTIVE	OUI
PASSIVE	ACTIVE	OUI
ON /AC/PA	NO CONFIGUER	NON
ON/PASSIVE	PASSIVE	NON
ON	ACTIVE	NON

Mode PagP

;W1	SW2	:TABLISMENT
)N	ON	OUI
\U/DESI	DESIRABLE	OUI
ON /AU/DE	NO CONFIGUER	NON
ON/AU	ON	NON
ON	DESIRABLE	NON

Routage inter-VLAN :

Affectez l'interface au VLAN 10 et donnez lui une addresse
R1(config)# **interface** fa0/0.10
R1(config-subif)#**encapsulation dot1q** 10
R1(config-subif)# **ip address** 192.168.10.1 255.255.255.0
Affectez l'interface au VLAN 20 et donnez lui une addresse
R1(config)# **interface** fa0/0.20
R1(config-subif)#**encapsulation dot1q** 20
R1(config-subif)# **ip address** 192.168.20.1 255.255.255.0
Affectez l'interface au VLAN native et donnez-lui une addresse
R1(config)# **interface** fa0/0.70
R1(config-subif)#**encapsulation dot1q** 70 **native**
R1(config-subif)# **ip address** 192.168.70.1 255.255.255.0
Activez tous les sous interfaces précedant
R1(config)# **interface** fa0/0
R1(config-if)# **no shutdown**

STP :

Configurer le cout de port
S1(config)# **interface** F0/1
S1(config-if)# **spanning-tree cost** 5
Définir S1 en tant que pont racine principal
S1(config)# **spanning-tree vlan** 1 **root primary**
Définir S2 en tant que pont racine secondaire
S2(config)# **spanning-tree vlan** 1 **root secondary**
Modifier la priorité de pont
S1(config)# **spanning-tree vlan** 1 **priority** '0-61440'
Changer la priorité d'un port :
S1 (config)# **interface fastEthernet** 'FA0/0'
S1 (config-if)# **spanning-tree vlan** 1 **port-priority** '0-240'
S1(config-if)# **exit**
Configurez portfast sur une interface
S1(config)# **interface** F0/1
S1(config-if)# **spanning-tree portfast**
Configurez portfast sur tout les interfaces non-trunk
S1(config)# **spanning-tree portfast default**
Configurez la protection BPDU sur une interface
S1(config-if)# **spanning-tree bpduguard enable Configurez la protection BPDU sur tout les interface qui utilise portfast**
S1(config)# **spanning-tree bdpuguard default**
Configurez root guard sur une interface
S1(config-if)# **spanning-tree guard root**
Configurez Rapid PVST+
S1(config)# **spanning-tree mode rapid-pvst Specifies le type de liaison pour une interface**
S1(config-if)# **spanning-tree link-type point-to-point**

Protocole RIP

RIPv1

RIPv1 est un protocole de routage intérieur classful, à vecteur de distance qui base ses décisions d'acheminement sur une métrique qui emploie essentiellement le nombre de saut. Le nombre maximum de saut est de 15.
- Il transmet des mises à jour de routage complètes toutes les 30 secondes.
- RIPv1 est un protocole de routage intérieur (IGP).
- C'est est un protocole de routage à vecteur de distance

• Il utilise une métrique basée sur le nombre de saut.
- RIPv1 a une convergence lente.
- RIPv1 est un protocole de routage classful et par conséquent ne supporte pas VLSM et CIDR. RIPv2

•
RIPv2 apporte également des fonctionnalités supplémentaires tels que :
- Le support du routage classless.
- La diffusion du masque réseau dans les mises à jour de routage.
- Le support de VLSM.
- La diffusion des mises à jour de routage par multicast avec l'adresse de classe D 224.0.0.9.

• L'authentification de la source de la mise à jour de routage par un texte en clair ou un texte crypté suivant l'algorithme MD5

PPDM : (protocole dependant module)
-creation le traduction des paquet specifique du protocole pour dual
-les paquet EIGRP de multidiffusion pour IPv4 utilise L'@ de multidiffusion ipv4 reserve 224.0.0.10

Type paquet EIGRP

1- Hello
2- Accuse de reception
3- Mise a jour
4- Requete
5- ICMP

La methode router-on-a-stick

Est un type de configuration de routeur dans la quelle une seule interface physique achemine le traffic entre plusieurs VLAN d'un reseau
Finite state Machine (FSM) :
Toute la logique utilisé pour calculer et comparer les routes dans un reseau EIGRP

Avantage vlan
- **Securite optimisé**
- **Cout reduit**
- **Meilleurs performances**
- **Domaines de diffusion plus peties**
- **Efficacité**
- **Efficacité de gestion**

1. La table filter
Iptables fonctionne selon un système de tables, ces tables sont composées de chaîne. Dans le cadre de la configuration et de l'utilisation de Netfilter comme pare-feu, c'est la table Filter qui est utile, elle permet de filtrer les paquets réseaux. Tout paquet entrant est analysé afin de déterminer notamment sa source et sa destination.
Elle est composée de trois sortes de chaîne :
☑ **INPUT** : Permet d'analyser les paquets entrants. Si le paquet est adressé au poste, il est confronté au filtre INPUT.
☑ **FORWARD** : Permet d'analyser et d'autoriser les trames à passer d'une interface à une autre, seulement dans le cadre d'une interface réseau servant de passerelle.
☑ **OUTPUT** : Permet d'analyser les paquets sortants. Si le paquet sort du poste, il passera par la chaîne OUTPUT

Frame Relay : La technologie Frame Relay dispose des caractéristiques suivantes :

• Destinée pour des équipements numériques haut de gamme et à haut débit.
• Fonctionne au niveau des couches 1 et 2 du modèle OSI.
• Utilise des circuits virtuels dans un environnement commuté.
• Technologie à commutation de paquets, et à accès multiples.
• L'ETTD et l'ETCD sont généralement généralement le routeur client et le commutateur de l'opérateur.
• Remplace des réseaux point-à-point, trop coûteux.
• Se base sur l'encapsulation HDLC.
• Utilise le multiplexage pour partager la bande passante totale du nuage Frame Relay.
Un réseau Frame Relay peut être conçu suivant deux topologies :
• Maillage global • Maillage partiel : Egalement appelé topologie en étoile ou "hub-and-spokes".

point-to-point :

```
Router1(config)# interface serial se 0/0
Router1(config-if)# no ip adresse
Router1(config-if)# no shutdown
Router1(config-if)# encapsulation frame-relay
Router1(config)# interface serial se 0/0.20  point-to-point
Router1(config-subif)# ip address 10.0.0.1 255.255.255.252
Router1(config-subif)# frame-relay interface-dlci 102
Router1(config)# interface serial se 0/0.30  point-to-point
Router1(config-subif)# ip address 20.0.0.1 255.255.255.252
Router1(config-subif)# frame-relay interface-dlci 103
```

Multi point

```
R1(config)# interface serial 0/0 multipoint
R1(config-if)# ip adresse 10.0.0.1 255.255.255.248
R1(config-if)# no shutdown
R1(config-if)# encapsulation frame-relay
R1(config-if)# frame-relay interface-dlci 102
R1(config-if)# frame-relay interface-dlci 103
R1(config-if)# Frame-relay map ip 10.0.0.2 102 broadcast
R1(config-if)# Frame-relay map ip 10.0.0.3 103 broadcast
R2(config-if)# interface serial 0/0 multipoint
R2(config-if)# ip adresse 10.0.0.2 255.255.255.248
R2(config-if)# no shutdown
R2(config-if)# encapsulation frame-relay
R1(config-if)# frame-relay interface-dlci 201
R1(config-if)# frame-relay interface-dlci 203
R2(config-if)# Frame-relay map ip 10.0.0.1 201 broadcast
R2(config-if)# Frame-relay map ip 10.0.0.3 203 broadcast
```

PPP : C'est le protocole de réseau WAN le plus répandu

permettant • Connexion entre routeurs ou entre un hôte et un routeur.
• Gestion des circuits synchrones et asynchrones.
• Contrôle de la configuration des liaisons.
• Possibilité d'attribution dynamique des adresses de couche 3.
• Multiplexage des protocoles réseau.
• Configuration des liaisons et vérification de leur qualité.
• Détection des erreurs.
• Négociation d'options (Adresses de couche 3, Compression .. Le protocole PPP peut prendre en charge plusieurs modes d'authentification : • Aucune authentification.
• Utilisation du protocole PAP : Mots de passe envoyés en clair.
• Utilisation du protocole CHAP.

```
R1(config)# username R1  password password 1111
R1(config) interface se 0/0
R1(config - if)# encapsulation ppp
R1(config - if)# ppp authentication pap
R1 (config - if)# ppp pap se nt-username R2 password 222
```

• RNIS : Ensemble de services numériques pour la voix et les données sur le réseau commuté classique. Technologies RNIS Il existe deux types de services RNIS :
• BRI : Accès de base.
• PRI : Accès primaire (fonctionnant sur des lignes dédiées).

creation d'user useradd -c "Abdo" -f 0 -G eleves –m –d /home/repAbdo -k /etc/skel –s /bin/bash –p password abdo Les fichiers initile /etc/group, /etc/passwd et /etc/shadow/ grep expression /répertoire/fichier grep "\$" *.txt

NetFlow est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco. NetFlow est la norme pour la collecte de données opérationnelles IP à partir de réseaux IP. Deux critères principaux sont à la base de la création du protocole NetFlow par Cisco :
• Le protocole NetFlow devait être complètement transparent pour les applications et les périphériques du réseau.
• Le protocole NetFlow ne devait pas obligatoirement être pris en charge et en cours d'exécution sur l'ensemble des périphériques réseau pour fonctionner.

Syslog est un utilitaire de consignation d'évènements Cisco basé sur l'utilitaire Syslog d'Unix. A l'origine, Syslog avait été développé pour le logiciel Sendmail uniquement. Mais l'utilité de ce dernier était telle que beaucoup d'autres applications se sont mises à l'utiliser. Syslog fonctionne sur un modèle client - serveur.

Configuration Syslog :

```
Router(config)#  logging on
Router(config)# logging 'nom d'hôte'/'adresse IP de la station
Router(config)# logging trap
Router(config)#  service timestamps log datetim
```

NAT statique : Translate une adresse IP privé avec toujours la même adresse IP publique globale.

```
R1(config)# ip nat inside source static @IP privé @IP public
R1(config)# interface fa 0/0
 R1(config-if)# ip nat inside
R1(config)# interface se  1/1
R1(config-if)# ip nat  outside
```

Nat dynamique : translate une/des adresses IP privés avec une adresse IP publique appartenant à une plage des adresses IP publique. R1(config)# ip nat pool tri 22.2.2.2 3.3.3.3 255.255.255.0

```
R1(config)# access-list  1 permit 10.0.0.0 255.255.255.0
R1(config)#   ip nat inside source list 1 pool tri
R1(config)# interface fa 0/0
R1(config-if)# ip nat inside
R1(config)# interface se  1/1
R1(config-if)# ip nat  outside
```

Pat : permet à plusieurs adresse IP de se connectés en même temps en utilisant le numéro de port pour distinguer leurs messages.

```
R1(config)#   ip nat inside source list 1 pool tri  overload
```

DHCP

La configuration d'un client avec le protocole DHCP :

1) DHCP DISCOVER : Lorsqu'une configuration DHCP cliente est présente sur un poste utilisateur, celui-ci envoie une requête en broadcast aux serveurs DHCP, appelée DHCP DISCOVER.
2) DHCP OFFER : Les serveurs DHCP recevant le broadcast et pouvant répondre à la demande, envoient une requête en unicast au client. Ce DHCP OFFER contient toutes les informations nécessaires au client (IP, adresse de passerelle, durée du bail, serveur DNS, WINS, etc.).
3) DHCP REQUEST : Le client émet ensuite une requête en broadcast afin de confirmer l'offre qu'il a sélectionnée • S'il y avait plusieurs serveurs DHCP, tous sont alors au courant et peuvent libérer leur offre en conséquence. • S'il s'agit d'un renouvellement de bail, le client propose au serveur l'IP qu'il veut se voir réattribuer.
4) DHCP ACK : Cette confirmation est envoyée en unicast par le serveur DHCP au client. Une fois le DHCP ACK reçu, le client peut alors utiliser l'adresse IP ainsi que le reste de la configuration attribuée.
5) DHCP DECLINE : Si le client détecte l'IP qu'on lui a proposée sur le même segment réseau, il envoie cette requête au serveur. Le processus redémarre alors.
6) DHCP NACK : Lorsqu'un serveur détecte que l'IP pour laquelle il doit renvoyer un ACK est déjà présente sur le réseau, il envoie un DHCP NACK. Le processus doit alors redémarrer pour le client concerné
7) DHCP RELEASE : Lorsqu'un client veut annuler le bail (arrêt du système, commande ipconfig /release sous Windows), cette requête est envoyée au serveur afin qu'il libère la réservation d'adresse

Relais DHCP : Les serveurs DHCP font partie des serveurs d'entreprise. Il est possible d'éviter ce problème en appliquant la commande ip helper-address sur l'interface d'un routeur. Celle-ci permet de relayer les broadcast UDP vers une adresse unicast définie

Qu'est-ce qu'un espace de nom de domaine DNS ?

La structure hiérarchique de l'espace de noms de domaines est telle que :
• **Domaine Racine** : qui se trouve en haut de la structure du noms de domaine, représente par point.
• **Domaine de niveau supérieur** : représente les TLDs (on a 224 TLD=Top Level Domain, comme : com, fr, ma...)
• **Domaine de niveau second** : est un nom unique de logueur variable, il est enregistré directement auprès des entreprises.
• **Sous-domaines** : permet à une organisation de subdiviser son nom de domainepar département ou service Ex microsof.s.com

1- Les composants de serveur DNS :
- **Serveur DNS** : Ordinateur exécute le serveur DNS
- **Client DNS** : Ordinateur exécute le service client DNS
- **Enregistrement de ressources DNS** : entrée de base de données DNS qui mappe les noms d'hôtes à des ressources.

2- Les requêtes DNS : Une requête est une demande de résolution des noms envoyée à un serveur DNS.
Il existe 2 types de requête :
récursive et itérative. La requête peut être lancé par client/serv
- **Requête récursive :** est un requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur DNS de fournir une réponse complète.
- **Requête itérative** : est un requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur DNS de fournir une meilleure réponse.

3- Les indications de racine : Les indications de racine sont des enregistrements de ressource DNS stocké sur un serveur DNS qui répertorient les adresse IP des serveurs racines du système DNS. Ils sont trouvés dans 'cache.dsn' qui se trouve dans le dossier '%systemroot%\system32\dns\'.

4- Les redirecteurs : Un redirecteur est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution des noms de domaines externes ou hors sites.

5- La mise en cache de serveur DNS : La mise en cache est le processus qui consiste à stocker temporairement (durant le TTC de la réponse) dans un sous système de mémoire spéciale des informations ayant fait l'objet d'un accès récent pour y accéder plus rapidement ensuite

Les enregistrements et les zones DNS : Un enregistrement de ressource est une structure de base de données DNS standard qui contient des informations utilisées pour traiter les requêtes DNS. Il existe plusieurs types des enregistrements de ressources :
- **A (Host)** : résous un nom d'hôte en adresse IP.
- **PTR (Pointeur) :** résous un adresse IP en nom d'hôte.
- **SOA** (Start Of Autority) : Premier enregistrement dans tout les fichiers de la zone.
- **SRV** (Service) : Résoud les noms des serveurs qui fournissent des services.
- **NS** Name Server Identifie le serveur DNS associé à chaque zon
- **MX (Mail eXchange** : Chemin pour messagerie) : Identifie le serveur de messagerie à chaque zone.
- **CNAME** (Canonical NAME : Nom officiel) : Un nom d'hôte qui fait la référence d'un autre nom d'hôte.

2- **Les types des zones** : Une zone est un ensemble des mappages de noms d'hôtes à adresses IP. Il existe différents types de la zone :
- **Zone Principale Standard** : (Lecture/Ecriture) : Doit toujours être crée en premier pour une nouvelle zone.
- **Zone Secondaire Standard** : (Lecture seule) : Contient toutes les modifications effectuées sur le fichier de la zone principale. On utilise la zone secondaire pour avoir une tolérance en panne et pour réduire les charges pour la zone principale.
- **Zone de Stub** : contient uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant l'autorité pour la zone.

3- La zone de recherche directe et la zone inversée :
- **Zone de recherche directe** : c'est une zone utilisée pour résoudre les noms d'hôtes en adresses IP.
- **Zone de recherche inversée** : c'est une zone utilisée pour résoudre les adresses IP en noms d'hôtes.

Réplication et transfert de zones Réplication La présence de serveurs de noms de domaine secondaires DNS permet la réplication des fichiers de zones. Cette pratique se justifie dans les cas suivants :
** Offrir une redondance en cas de panne du serveur DNS principal.
** Réduire le trafic lorsque le domaine est dans des sites différents reliés par des liaisons WAN.
** Réduire la charge du serveur de noms DNS principal.

Transfert de zone La réplication des fichiers de zones se fait au cours d'une opération appelée transfert de zone.Transfert de zone complet.Il y a un transfert complet du fichier de zone lorsqu'un nouveau serveur de noms DNS secondaire est installé. On parle de transfert de zone complet (AXFR)
Transfert de zone incrémentiel
Une fois le transfert de zone complet effectué, il se fait une mise à jour des fichiers de zones dans les serveurs de noms secondaire au cours d'une opération nommée transfert de zone incrémentiel (IXFR)

DDNS Dynamic Domain Name System. Dès qu'un nouvel ordinateur apparaît dans le domaine, le serveur DNS ajoute automatiquement un enregistrement A avec son nom et son adresse IP dans le fichier de zone. Ce service s'appuie sur le service DHCP
La création d'un fichier de zone : /etc/bind/db.isgim.tri

Les messages SNMP : Il existe 4 types de requêtes SNMP :
• **get-request** : Le Manager SNMP demande une information à un agent SNMP
• **get-next-request** : Le Manager SNMP demande l'information suivante à l'agent SNMP
• **set-request** : Le Manager SNMP met à jour une information sur un agent SNMP
• **trap** : L'agent SNMP envoie une alerte au Manager . Configuration SNMP :

```
Router(config)# snmp-server  community Com1 ro/rw
Router(config)# snmp-server  location 'Emplacement du R1
Router(config)# snmp-server  contact informations personnes
Router(config)# snmp-server  host 'IP de la NMS'
Router(config)# snmp-server enable traps snmp
```

Équipement et dispositifs des réseaux WAN :
- Routeur
- Serveur de communication
- Commutateur WAN
- Modem
- Unité CSU/DSU
- CPE :
- Point de démarcation de service
- Boucle locale
- Commutateur du central téléphonique
- Réseau interurbain

Normes WAN :
Il existe deux types de circuits :
• Circuit point-à-point
* Circuit virtue

Les types de commutation :
• commutation de circuits :
• commutation de paquets/cellules
• Liaisons dédiées (lignes louées)

Établissement de la communication :
• Aussi appelé signalisation, ce service permet d'établir ou de mettre fin à la communication entre les utilisateurs du système téléphonique.

Transit des données :
• **Multiplexage temporel :** Principe simple qui permet d'allouer l'intégralité de la bande passante disponible d'une liaison par tranche de temps fixe, affectée à chaque utilisateur.
Active Directory :
1 - Définition : L'Active Directory est un service qui permet de stocker des informations sur les ressources de tout le réseau et permet aux utilisateurs de localiser, gérer et utiliser ces ressources. Il utilise le protocole LDAP (Lightweight Directory Acces Protocole), son numéro de port 389/TCP.
2- Les objets Active Directory : Serveurs, domaines, sites, utilisateurs, ordinateurs, groupe, lien de site, imprimantes, dossier partagé...
3- Schéma Active Directory : Le schéma Active Directory stocke la définition de tous les objets d'Active Directory (ex : nom, prénom pour l'objet utilisateur). Le schéma comprend deux types de définitions : les classes d'objets et les attributs.
4- Le catalogue global : Le catalogue global contient une partie des attributs les plus utilisés de tous les objets Active Directory. Il contient les informations nécessaires pour déterminer l'emplacement de tout objet de l'annuaire
. **5- Le protocole LDAP :** LDAP (Lightweight Directory Access Protocol) est un protocole du service d'annuaire utilisé pour interroger et mettre à jour Active Directory. Chaque objet de l'annuaire est identifié par une série de composants :
• **DC : (Domain Controller)** Composant de domaine.
• **OU : (Organizational Unit)** Unité d'organisation.
• **CN : (Common Name)** Nom usuel.
Les composants logiques de la structure d'Active Directory sont les suivants :
1- Domaine : est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base-d-don d'annuaire. Un domaine a un nom unique sur le réseau.
2- Unité d'organisation : est un objet conteneur utilisé pour organiser les objets au sein du domaine.
3- Arborescence : est un ensemble de domaines partageant un nom commun.
4- Forêt: est un ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun.
5- Rôles de maîtres d'opération : - Contrôleur de schéma : sert à modifier et à mettre à jour le schéma.
- **Maître d'attribution des noms de domaine :** permet d'ajouter ou de supprimer un domaine dans une forêt.
- **Émulateur PDC :** permet le support des clients (changement des mots de passes
- **Maître RID :** distribue des plages d'identificateurs relatifs (RID) à tous les contrôleurs de domaine pour éviter que deux objets différents possèdent le même RID.

La structure physique permet d'optimiser les échanges d'informations entre les différentes machines en fonction des débits assurés par les réseaux qui les connectent. Les composants de la structure physique :
1- Contrôleurs de domaine : Un contrôleur de domaine est un ordinateur exécutant Windows Server qui stocke un réplique de l'annuaire. Il assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi les recherches dans l'annuaire.
2- Sites et liens des sites : Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Un lien de site est une liaison entre deux site. La réplication Active Directory peut utiliser les protocoles :
• IP pour les liaisons intra site.
• RPC pour les liaisons inter site.
• SMTP pour les liaisons inter site.
Les outils d'administration d'Active Directory :
• **Utilisateurs et ordinateurs Active Directory :** C'est le composant le plus utilisé pour accéder à l'annuaire. Il permet de gérer les comptes d'utilisateurs, les comptes d'ordinateurs, les fichiers et les imprimantes partagés, les unités d'organisaio
• **Sites et Services Active Directory :** Ce composant permet de définir des sites, des liens de sites et de paramétrer la réplication Active Directory.
• **Domaines et approbations Active Directory :** Ce composant permet de mettre en place les relations d'approbations et les suffixes UPN. Il propose aussi d'augmenter le niveau fonctionnel d'un domaine ou d'une forêt.
• **Schéma Active Directory :** Ce composant permet de visualiser les classes et les attributs de l'annuaire.
• **Gestion des Stratégies de Groupe :** Ce composant permet de centraliser l'administration des stratégies de groupe d'une forêt, de vérifier le résultat d'une stratégie de groupe ou bien encore de comparer les paramètres de deux stratégies de groupe. Ce composant n'est pas disponible sur le CD-ROM de Windows Server, il doit être téléchargé sur le site de Microsoft.
• **Dsadd, dsmod, dsrm, dsget, dsquery, dsmove :** Ces outils en ligne de commande permettent respectivement d'ajouter, de modifier, de supprimer, de lister ou de déplacer des objets dans l'annuaire.
• **Csvde** : L'outil en ligne de commande CSVDE est utilisé pour importer des comptes d'utilisateurs à partir d'un fichier texte vers Active Directory.

Le rôle du Système DNS dans Active Directory : Le système DNS fournit les principales fonctions ci-dessous sur un réseau exécutant Active Directory :
• Résolution de noms.
• Convention de dénomination.
• Localisation des composants physiques d'Active Directory. Les zones DNS intégrées à **Active Directory :** Les zones DNS intégrées à Active Directory stockent les enregistrements de ressources directement dans le service d'annuaire Active Directory. Elle p euvent être dupliquées sur tous les contrôleurs de domaine.

Les relations d'approbation
1- Transitivité de l'approbation : Le domaine A approuvé directement le domaine B. Le domaine B approuve directement le domaine C. Les deux relations d'approbations de A à B et de B à C sont transitives, alors le domaine A approuvé indirectement le do C.
2- Direction de l'approbation : Unidirectionnelle Bidirectionnelle
3- Approbation racine/arborescence :
4- Approbation parent-enfant :
5- Approbation raccourcie :
6- Approbation externe :
7- Approbation de forêt

Création des objets Active Directory en ligne de commande :
1- **Création d'un compte utilisateur** : dsadd user "cn='Abdo',ou='OU2',dc='tri',dc='com'" -pwd 'Mdp' -upn 'session'
2- Création d'un groupe : dsadd group "cn='Adminstration',ou= 'OU3 ,dc='tri',dc='com"
3- **Création d'un compte ordinateur** : dsadd computer "cn='Nom',ou='unité',dc='Domaine',dc='TLD'"
4 - **Création d'une unité d'organisation** : dsadd ou "cn='Materiel',ou= 'OU2 ,dc='tri',dc='com"
5- **Supprime compte utlisateur** dsrm " cn=post3ou=OU3, dc='tri',dc='com'"

Implémentation de comptes de groupe :
1- Le type de groupe :
• **Les groupes de sécurité** : permettent d'affecter des utilisateurs et des ordinateurs à des ressources.
• **Les groupes de distribution :** exploitables entre autres via un logiciel de messagerie.
2- L'Étendue de groupe :
• **Les groupes globaux :** Visibles dans leur domaine et dans tous les domaines approuvés, Membres des groupes locaux du même domaine, Autorisations pour Tous les domaines de la forêt
• **Les groupes locaux de domaine** : Visibles dans leur propre domaine, Membres d'aucun groupe, Autorisations pour Le domaine dans lequel le groupe local de domaine existe.
• **Les groupes universels** : Visibles dans tous les domaines de la forêt, Autorisations pour Tous les domaines de la forêt.

Les stratégies de groupe : Une stratégie de groupes est un objet Active Directory qui va contenir un ensemble de paramètres (Installation, Configuration, Suppression, Désinstallation, Ouverture, Fermeture, ...).
NTDS : L'explorateur de Windows s'ouvre et affiche le contenue du dossier Ntds qui doit comporter les fichiers suivants :
• **Ntds.dit** : il s'agit du fichier de base de données d'annuaire.
• **Edb.*** : il s'agit des journaux de transaction et des fichiers de points de vérification • Res
*.**log** : il s'agit des fichiers journaux réservés. NTDSUTIL permet de défragmenter la base de données

Restauration Active Directory :
• Une restauration forcée est utile dans le cas ou vous avez effacé des objets dans Active Directory par erreur.
• Une restauration non forcée, est une restauration dite normale toutes les modifications faites depuis la sauvegarde vont être récupérées lors de la prochaine réplication entre les DCs
• La restauration principale doit être utilisée uniquement lorsque les données contenues dans tous les contrôleurs de domaine du domaine sont perdues.

Résolution des noms NetBios Il est difficile pour un utilisateur de travailler avec des adresses IP. La résolution est le processus qui permet d'affecter automatiquement une traduction entre les noms alphanumériques et des adresses IP. Tous les ordinateurs possèdent deux identificateurs :
- Nom alphanumérique
- Adresse IP
Dans les systèmes Windows on trouve deux types de noms :
- Les noms NetBIOS
- Les noms d'hôtes

récupération de mot de passe pour les routeurs

1.Connectez votre PC sur le port console du cisco.
2. Une fois connecté, tapez : show version.
3. Redémarrez l'équipement. Dans les 30 secondes après allumage, tapez [CTRL] + C.
4. Tapez alors configreg 0x2102
5. Tapez ensuite reset
6. Au redémarrage du système, tapez no
7. Tapez enable
8. Faites copy startup-config running-config
10. Changez tranquillement votre mot de passe :
11. tapez config-register 0x2102

Mise à jour de l'IOS d'un Routeur :

```
Router#dir flash:
Router#delete flash:nom_du_fichier_IOS_actuel.bin (On supprime l'actuel IOS)
Router#copy tftp: flash:
Router#Address 192.168.1.10
Router#Source filename []?nom_du_fichier_IOS_New.bin
Router(config)#boot systemflash:nom_du_fichier_IOS
Router#wr
Router#reload
```

Les requêtes HTTP :

requête version HTTP description
GET HTTP/0.9 obtient un document
HEAD HTTP/1.0 obtient l'en-tête de la réponse
POST HTTP/1.0 envoie du contenu au serveur
PUT HTTP/1.1 demande au serveur d'enregistrer la ressource envoyée
DELETE HTTP/1.1 permet d'effacer un fichier sur le serveur
TRACE HTTP/1.1 permet de contrôler la requête reçue par le serveur
CONNECT HTTP/1.1 mot réservé pour les proxies permettant de créer des tunnels
OPTIONS HTTP/1.1 liste les options possibles pour une ressource donnée

Les authentifications HTTP :

• **Basique** : simple et facile à craquer les mots de passe envoyé pour cette méthode.
• **Digest** : basé sur le hachage des mots de passe, plus sécurisé que la méthode basique.
• **NTLD** : supporte les systèmes Win basé sur le protocole NTLD
Définition HTTP :HTTP (Hyper Text Transfer Protocol) un protocole de communication client-serveur développé pour le World Wide Web. permet la transmission des pages web et aussi d'autres fichiers (vidéo, audio, image...). HTTP est un protocole de la couche application Il utilise le protocole TCP et un numéro de port 80. Le répertoire de base / de publicité toutes les données qui seront publier doive obligatoire dans le sous répertoire de publicité + site web + page web Site web peut identifier par une @ip / n° de port / le nom d'entête d'hôte.

Définition SMTP : signifie Simple Message Transfert Protocole, ce protocole est utilisé pour transférer les messages électroniques sur les réseaux. Un serveur SMTP est un service qui écoute sur le port 25, son principal objectif est de router les mails à partir de l'adresse du destinataire.

Définition POP3 : signifie Post Office Protocol. Actuellement c'est la version 3 qui est utilisée. Le service POP écoute sur le port 110 d'un serveur. Le protocole POP a un objectif précis : permettre à l'utilisateur de relever son courrier depuis un hôte qui ne contient pas sa boîte aux lettres.En d'autres termes, POP établie un dialogue entre le logiciel de messagerie (MUA) et la boîte aux lettres de l'utilisateur sur le serveur.

Détail du fonctionnement

Le service SMTP est divisé en plusieurs parties, chacune assurant une fonction spécifique :
• **MUA :** Mail User Agent, c'est le client de messagerie (KMail, Evolution, etc.).
• **MTA :** Mail Transfert Agent, c'est l'agent qui va transférer votre mail vers le serveur chargé de la gestion des emails de votre destinataire. Dans la pratique, le courrier peut transiter par plusieurs MTA.
• **MDA :** Mail Delivery Agent est le service de remise du courrier dans les boîtes aux lettres des destinataires. Donc si on résume, le MUA transfert l'email à un MTA qui le transfert au MTA du destinataire (ou à un MTA intermédiaire) qui le passe au MDA chargé de stocker l'email dans la boite aux lettres du destinataire. Dans la pratique le MUA établit une connexion SMTP avec un MTA qui contacte via SMTP le MTA du destinataire qui est aussi un MDA.
Fonctionnalités

POP est avant tout un protocole très simple, de ce fait il ne propose que des fonctionnalités basiques:
• Délimiter chaque message de la boite aux lettres, • Compter les messages disponibles,
• Calculer la taille des messages,
• Supprimer un message,
• Extraire chaque message de la boite aux lettres. telnet 192.168.1.20 110 USER nom_
PASS password
DELE numéro_du_mesg : efface le message spécifié ;
LIST : donne une liste des messages ainsi que la taille de
RETR numéro_du_msg : récupère le message indiqué ;
STAT : indique le nombre de messages et la taille occupée par l'ensemble des messages ;
TOP numéro_du_msg nombre_de_lignes

Définition IMAP : IMAP (Internet Message Access Protocol) c'est un protocole alternetive au POP3, il utilise le numéro de port 143. Il offre beaucoup d'avantage que POP3 :
• Manipulation des dossiers à distants ,Ajout des messages à un dossier distant..
• Support de dossier multiple (support de dossier hiérarchique, accès à des dossiers non email
• Optimise la performance en mode en ligne.
⁉ recopier sur le serveur des messages qui sont en local
Un serveur proxy (traduction française de «proxy server», appelé aussi «serveur mandataire») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et internet.
Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle- ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête.
Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.
Les fonctionnalités d'un serveur proxy
Désormais, avec l'utilisation de TCP/IP au sein des réseaux locaux , le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Pour autant, les serveurs proxy sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités.

Kerberos : C'est un protocole d'authentification des utilisateurs.
La politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer. La politique de sécurité permet d'assurer :
• **L'intégrité** : c'est-à-dire garantir que les données sont bien celles que l'on croit être, hachage, MD5, SHA-1
• **La confidentialité** : consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
Chiffrement/déchiffrement RSA
• **La disponibilité** : permettant de maintenir le bon fonctionnement du système d'information. Tolérance aux pann
• **La non répudiation** : permettant de garantir qu'une transaction ne peut être niée. Signature numérique/Empreinte
• **L'authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources. Non utilisateur/mot de passe
Cryptologie est : fonction mathématique utilisé dans le processus de chiffrement et déchiffrement, méthodes permettant de transmettre des données de manière nn sécurié
Cryptage symétrique est : Un type de chiffrement ou on crypte et on décrypte avec la même clé secrète .les Protocoles utiliser DES / AES /RC1
Cryptage asymétrique est : Un type de chiffrement ou on crypte et on décrypte avec deux clés différentes. Il utilise : une clé publique connue de tous et une clé privée connue seulement du destinataire du cryptogramme. Protocole utiliser RSA .

Les différents types de pirates :
• **white hat hackers** : hackers au sens noble du terme
• **black hat hackers** : hackers au sens nuisible
• **script kiddies** : sont de jeunes qui utilisent les scripts sur internet pour pirater leurs amis.
• **phreakers** : sont des pirates s'intéressant au réseau téléphonique commuté (RTC)
• **carders** :s'attaquent principalement aux systèmes de cartes à puces : cartes bancaires.
• **crackers** : sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants.
• **hacktivistes** : sont des hackers dont la motivation est principalement idéologique.

Vulnérabilité ou faille est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.
Menace est : Décrit un danger ou une vulnérabilité En termes de sécurité informatique les menaces peuvent être le résultat de diverses actions en provenance de plusieurs origines.
Système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions
• **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.
• **Vers (Worms)** : est un programme informatique nuisible. il génère les copies de lui-même jusqu'à l'infini. Il propage sont l'intervention humain
• **Cheval de trois (Trojan)** un programme informatique nuisible effectuant des opérations malicieuses à l'insu de l'utilisateur
Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier.
Un pare-feu est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Un système pare-feu contient un ensemble de règles prédéfinies permettant : D'autoriser la connexion (allow) De bloquer la connexion (deny) ; De rejeter la demande de connexion sans avertir l'émetteur (drop).
DMZ (Zone démilitarisée) : est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Les types d'attaque :

Déni de service est : une attaque informatique visant à rendre une machine inaccessible en la saturant Ping de la mort ping of death ou PoD : est une attaque historique de type déni de service réalisé par l'envoi de paquet ping malformé. Un ping a normalement une taille de 56 octets (soit 84 octets avec l'entête IP).
Flooding Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser
Architecture Exchange
Forêt Windows 2003
Groupes Administratifs Exchange 2003
Groupes deRoutage Exchange 2003
Site Windows 2003
Topologie Physique 1 Les fichiers de base de données EDB et STM : Tous les emails sont stockés dans une base de données, cette base de données adopte le moteur Extensible Storage Engaine basé sur les transactions ACID. Cette base de données est scindée en deux fichiers,
- le premier fichier porte l'extension EDB, ce fichier contient tous les mails et composant MAPI;
- le deuxième fichier porte l'extension STM, ce fichier contient toutes les informations non relatives à MAPI.
Les bases peuvent être monté ou démonter individuellement, ce qui empêche l'arrêt total en cas d'intervention sur une des bases de données; de ce fait seul une partie des utilisateurs n'auront pas accès temporairement à leur boite mail.
La commande STORE.EXE permet d'administrer en ligne de command es les fichiers de base de données et autres paramètres de stockage de fichiers Exchange.
2 Serveurs frontaux et dorsaux - Les serveurs frontaux exécutent Exchange 2003 mais n'hébergent ni les boîtes aux lettres ni les banques d'informations de dossiers publics. Ces serveurs transmettent les requêtes au service d'annuaire, via LDAP, afin de déterminé le serveur dorsal qui contient la boîte aux lettres de l'utilisateur
- Les serveurs dorsaux exécutent Exchange 2003 et contiennent les boîtes aux lettres ou une banque d'informations publiques.
- Il est possible de configurer le système DNS ou l'équilibrage de charge Windows 2003 pour n'avoir qu'un seul nom pour tous les serveurs frontaux .
- Les serveurs frontaux permettent aussi l'accès au contenu distribué du système de dossiers publics par des clients IMAP4 ils permettent aussi de sécuriser l'accès aux données car ils peuvent être placés sur un réseau intermédiaire entre l'Internet et l'intranet. Le processus d'authentification se passe en 6 phases :
- Le frontal reçoit une demande d'un utilisateur.
- Le frontal interroge Active Directory pour identifier le serveur de BAL de l'utilisateur.
- Le frontal envoie une demande au dorsal correspondant.
- Le dorsal authentifie l'utilisateur.
- Le dorsal envoie au frontal la réponse à la requête.
- Le frontal envoie au client le résultat.
Les certificats : ce sont des documents d'identification numériques qui permettent aux serveurs et aux clients de s'authentifier mutuellement. Certificats serveurs : Les certificats serveurs permettent aux utilisateurs de confirmer l'identité de votre site Web.
Certificats clients : Avec SSL, votre serveur Web a également la possibilité d'authentifier les utilisateurs en vérifiant le contenu de leur certificat client.
Un réseau sans fil (en anglais Wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux : ordinateur portable, PDA … peuvent Communiquer sans liaison filaire. Il existe deux modèles de déploiement :
• **Le mode infrastructure** : permet de connecter les ordinateurs équipés d'une carte réseau Wifi entre eux via un ou plusieurs points d'accès qui agissent comme des concentrateurs.
• **Le mode « Ad-Hoc »** : permet de connecter directement les ordinateurs équipés d'une carte réseau Wifi, sans utiliser un matériel tiers tel qu'un point d'accès.
Les normes de Wifi :
• **802.11a** : norme pour les réseaux locaux utilisant comme fréquence le 5 GHz pour des transferts jusqu'à 54 Mbps.
• **802.11b** : autre norme pour les réseaux locaux, utilisant le 2,4 GHz avec une bande passante maximale de 11 Mbps.
• **802.11g** : norme la plus aboutie pour les réseaux étendus, exploite le 2,4 GHz avec des débits maximums de 54 Mbps.

Les avantages de réseau sans fils (WIFI) :
• les coûts sont nettement plus réduits.
• l'installation d'un réseau câblé est un vrai casse-tête autant pour les bâtiments anciens.
• les clients vont apprécier la mobilité : la portée en plein air d'un réseau wifi est de 100 mètres.

Les équipements WIFI :
•**Linksys-WRT54G** : est un routeur Wifi produit par Linksys. Il permet de partager une con-nexion Internet vers des ordinate.
• **Hot spot** est un dispositif électronique servant à amplifier un signal numérique ainsi d'étendre la distance maximale entre l'émetteur et le récepteur.
• **CPL (courant porteur en ligne)** permet de se connecter à internet en utilisant le réseau électrique existant.

Sécurité d'un WIFI :
• **WEP :** consiste à définir une clé sécrète qui doit être déclarée au niveau de chaque adaptateur sans fil du réseau ainsi que sur le point d'accès. Cependant, le WEP possède un grand nombre de failles, le rendant vulnérable. En effet, le cryptage RC4 présente des faiblesses. La clé de session partagée par toutes les stations est- nous le savons - statique.
• **WPA** :protocole de sécurisation des réseaux sans fil offrant une meilleure sécurité que le WEP car il est destiné à en combler les faiblesses. Ainsi, le WPA permet d'utiliser une clé par station connectée à un réseau sans fil, alors que le WEP, lui, utilisait la même clé pour tout le réseau sans fil. Les clés WPA sont en effet générées et distribuées de façon automatique par le point d'accès sans fil - qui doit être compatible avec le WPA.
• **Le WAP2,** tout comme son prédécesseur - le WPA - assure le cryptage ainsi que l'intégrité des données mais offre de nouvelles fonctionnalités de sécurité telles que le « Key Caching » et la « Pré-Authentification ».
Définition HTTP :HTTP (Hyper Text Transfer Protocol) un protocole de communication client-serveur développé pour le World Wide Web. permet la transmission des pages web et aussi d'autres fichiers (vidéo, audio, image…). HTTP est un protocole de la couche application Il utilise le protocole TCP et un numéro de port 80. Le répertoire de base / de publicité toutes les données qui seront publier doive obligatoire dans le sous répertoire de publicité + site web + page web Site web peut identifier par une @ip / n° de port / le nom d'entête d'hôte.