KONE ABDOUL AZIZ

BAMBA ALLASSANE

DIAKITE ABDOUL JUNIOR

TOURE SAMUEL

SILUE FRANCK HAMED

EHUI CHRISTIAN

AHOUSSY JAYSON

SAGBO ROSARIO

JEUDI 24 FEVRIER 2022

TD RESEAU ET SERVICES 2

NOTE	OBSERVATIONS

PROTOCOLE OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de type protocole route-link (que l'on pourrait traduire par protocole d'état des liens), cela signifie que, contrairement a RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné.

De plus, ce protocole évite aux routeurs intermédiaires d'avoir a incrémenter le nombre de sauts, ce qui se traduit par une information beaucoup moins abondante, ce qui permet d'avoir une meilleure bande passante utile qu'avec RIP.

FONCTIONNEMENT

1) Analyse en continue des connexions vers les éléments proches
   - Message hello envoyé à intervalles réguliers
2) Calcul du plus court chemin vers les routeurs voisins
3) Diffusion de la liste des routes connectées et des états de liens
   - Propage de proche en proche
   - Toutes les 30 min (intégralité des LSAs)
     . Et à chaque changement (LSA modifies uniquement)
   - LSA (Link State Advertisement)
     . L'ensemble des LSAs d'une aire formant la LSDB (Link State Data Base)
4) Détermine enfin la route la plus courte pour chaque réseau de la LSDB

AVANTAGES :

- Le protocole de routage OSPF à une connaissance complète de la topologie du réseau, ce qui permet au routeur de calculer les routes en fonction des demandes entrantes.
- Le protocole OSPF n'est pas limité dans le nombre de sauts, contrairement au protocole RIP qui ne compte que 15 sauts au maximum. Ainsi, OSPF converge plus rapidement que rip et offre un meilleur équilibrage de la charge.
- OSPF multidiffuse les mises à jour de l'état de lien et envoie des mises à jour uniquement lorsqu'il y a un changement dans le réseau

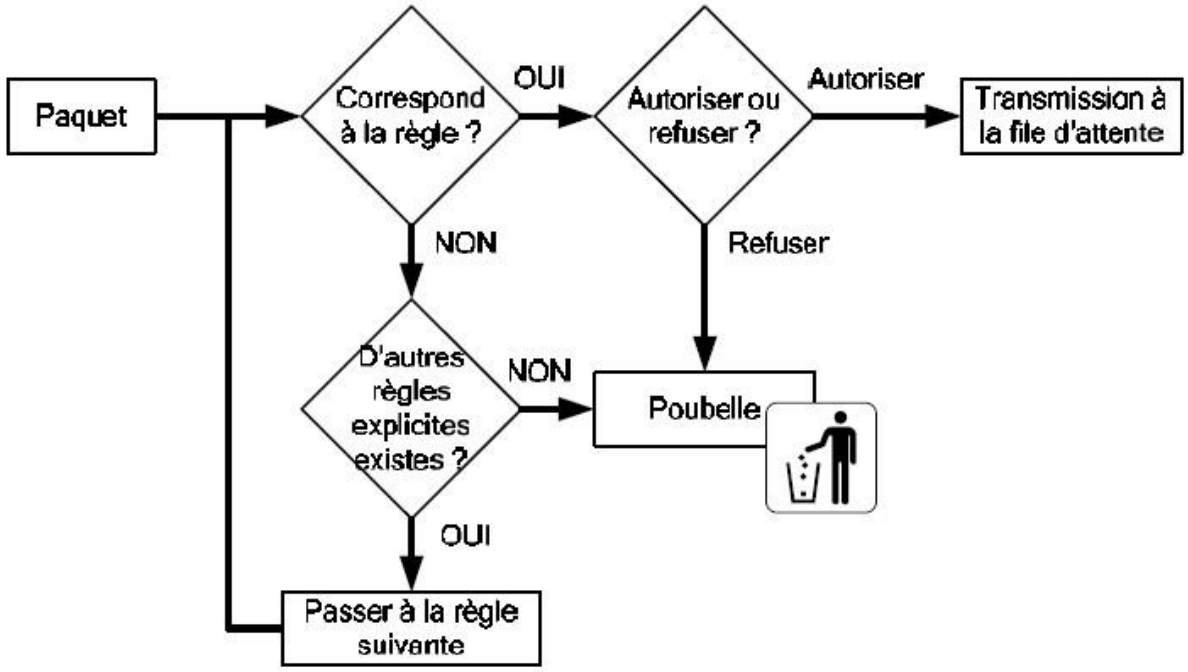
INCONVÉNIENTS :

- Le protocole OSPF exige des connaissances avancées sur les réseaux complexe ce qui en fait un protocole moins facile à apprendre que d'autres.
- Le routage OSPF ne peut être adapté lorsque des routeurs supplémentaires sont ajoutés au réseau. Le manque d'évolutivité du protocole OSPF le rend inadapté au routage sur internet
- Le protocole OSPF conserve plusieurs copies des informations de routage ce qui augmente la quantité de mémoire nécessaires.

ACL

Une ACL (Access Control List) est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d’autoriser ou d’interdire des paquets, que ce soit en entrée ou en sortie.

Il ne peut y avoir qu’une seule ACL par protocole, par interface et par direction (entrée/sortie).



LES ACCESS-LISTS (FONCTIONNEMENT ACL)

Fonctionnement ACL : Dans un monde parfait où nous pourrions avoir confiance en n'importe qui ou personne ne se tromperait, et bien nous n'aurions pas besoin de sécurité.

Mais dans la vraie vie, de mauvaises choses peuvent arriver à notre réseau, c'est pour ça que nous devons le protéger.

Par défaut, tous les paquets IP sur un routeur sont routés, il n'y a pas de restrictions.

Grâce aux access-lists, il sera possible d'empêcher certains paquets IP d'entrer ou de quitter nos routeurs !

Les listes d'accès fonctionnent sur la couche réseau, la couche3, et la couche transport, la couche 4.

Une ACL est une liste de règles qui permet de filtrer ou d'autoriser du trafic sur un réseau en fonction de plusieurs critères, par exemple de l'adresse IP, du port, ou même en fonction du protocole !

Elle permet de soit autoriser le trafic, dans ce cas l'ACL commencera par le mot « Permit », ou bien de le bloquer, avec le mot « deny ».

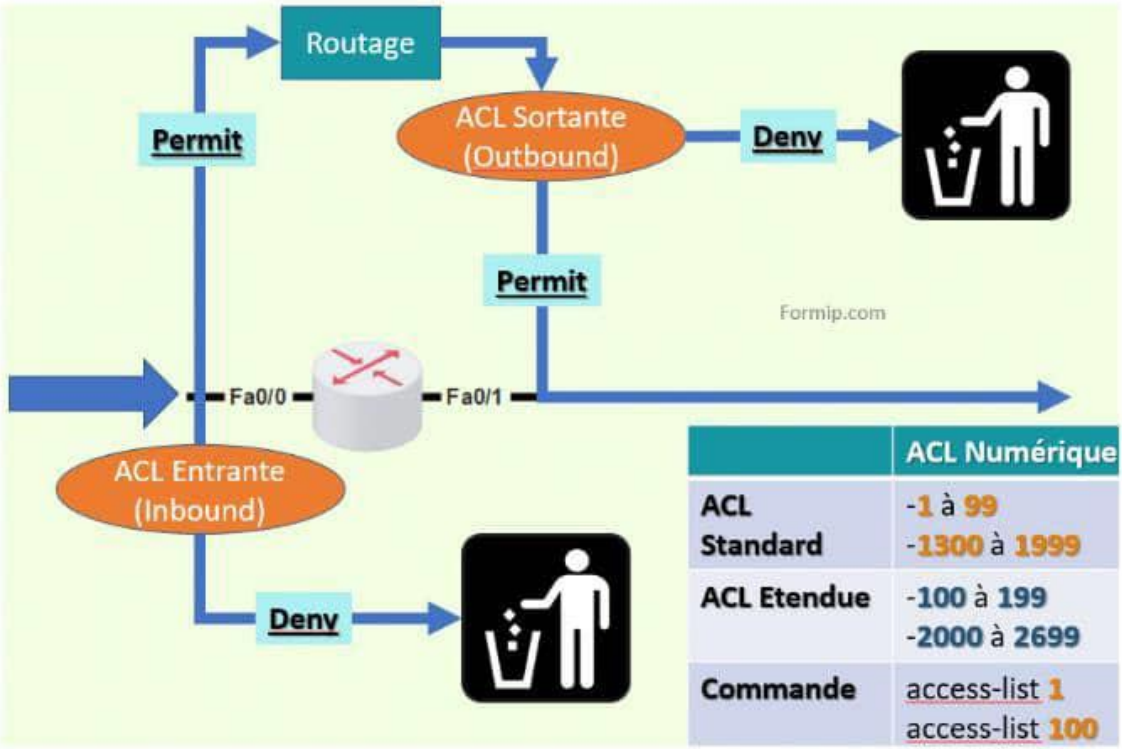
Il est possible d'appliquer au maximum une ACL par interface et par sens, c'est-à-dire soit en entrant ou soit en sortant, avec les mots input et output !

L’ACL est analysée par l’IOS de haut en bas.

Dès qu’une règle matche avec le paquet, il est soit autorisé ou soit supprimé !

Et le reste de l’ACL ne sera pas analysé.

Toute ACL dispose d’une dernière ligne par défaut qui bloque tout le trafic qui n’aurait pas matché avec l’une des ACLs.



Par exemple sur ce routeur, un paquet IP arrive sur l’interface Fa 0/0.

- Le paquet sera analysé par l’ACL entrante.
- Si le paquet matche avec une règle Deny, alors il sera supprimé.
- S’il matche avec une règle permit, alors il pourra passer et le routeur le prendra en charge !
- Le routeur décide de router ce paquet vers l’interface Fa0/1.
- Là aussi il y’a une ACL, mais cette fois-ci, elle est placée en sortie !
- Si le paquet est autorisé alors il continuera son chemin.
- Sinon il sera supprimé !

Il existe deux types d’ACL :

- L’ACL Standard qui permet d’analyser le trafic qu’en fonction de l’adresse IP source

- L’ACL étendu qui lui, permet d’analyser le trafic en fonction de plusieurs critères !

Les ACLs standard sont à appliquer le plus proche possible de la destination, en raison de leur faible précision.

Et Les ACLs étendues sont à appliquer le plus proche possible de la source.

Dans la configuration d’une ACL, il est possible de l’identifier par un nombre ou bien par un nom sous la forme d’une chaine de caractères alphanumériques.

Si on souhaite lui attribuer un numéro, alors la commande sera « access-list », et si on souhaite la nommer, alors ce sera « IP access-list » !

Lorsqu’une ACL contient plusieurs règles, il faut placer les règles les plus précises en début de liste, et les plus génériques en fin de liste.

Le plus simple est de créer son ACL dans un éditeur de texte et de la configurer par un copié/coller pour éviter les erreurs.

INCONVÉNIENTS :

Si les techniques de filtrages mises en œuvre dans les routeurs d’accès peuvent s’avérer un outil de sécurité indispensable, ces mécanismes souffrent toutefois de limitations et de contraintes particulières :

· Si les ACLs sont longues et complexes, il peut en résulter une baisse notable de performances du fait du balayage des règles de filtrage pour tous les paquets reçus, · L’interface d’administration de tels mécanismes, même s’il existe désormais des interfaces graphiques à ces systèmes, se révèle bien souvent assez lourde à l’emploi et peu ergonomique,

· Le contenu protocolaire n’est pas traité par ces règles : un routeur filtrant ne saura pas détecter qu’un segment TCP à destination du port 25 n’est pas du SMTP mais, par exemple, du HTTP puisque seul le port de service est reconnu, pas le protocole qui l’utilise,

· Il n’existe pas de notion de « contexte de session », qui permettrait de rejeter un paquet à priori valide éventuellement injecté dans un flot de communication entre deux machines par un pirate, ou qui permettrait d’identifier une session TCP en tant que telle. Le filtrage est ici réalisé paquet par paquet, indépendamment de la communication en elle-même.

· Ce type de filtrage nécessite que l'on connaisse précisément les ports de services TCP qui seront utilisés entre les machines, or certains protocoles fonctionnent sur un mécanisme d'allocation dynamique des ports (cas de H323 par exemple qui écoute sur un numéro de port précis, mais qui négocie les ports TCP des communications ultérieures)

· Dans les situations où l'on dispose de nombreuses règles de filtrage, il devient impératif de bien les organiser. Il se peut en effet qu'une règle sensée interdire un service soit sans effet, si une règle précédente, plus générale, a déjà autorisée le service et ce en raison du mécanisme de « first match »

QUESTIONS

1) lorsqu'on empêche à une machine d'accéder à un réseau pas le protocole ACL, est-ce possible que les machines de ce réseau puis communiqué avec cette machine

2) existe-t-il d'autres moyens de pouvoir empêcher une machine de communiquer ou d'accéder à un réseau bien précisa

3) à quoi peut nous servir ACL en sécurité

Deny FTP Host xxxx gt 23

Explication

4) au niveau des couches 3 et 4 comment le protocole ACL fonctionne

Propositions de réponses

Fonctionnement du protocole ACL au niveau des couches 3 et 4

Lorsque la ligne de liste de contrôle d'accès contient des informations de couche 3 et de couche 4 et que le mot clé fragments est présent, l'action de la liste de contrôle d'accès est conservatrice pour les actions d'autorisation et de refuser. Les actions sont conservatrices car vous ne voulez pas refuser accidentellement une partie fragmentée d'un flux, car les fragments ne contiennent pas suffisamment d'informations pour correspondre à tous les attributs de filtre. Dans le cas de refus, au lieu de refuser un fragment non initial, l'entrée de liste de contrôle d'accès suivante est traitée. Dans le cas de l'autorisation, on suppose que les informations de couche 4 du paquet, si elles sont disponibles, correspondent aux informations de couche 4 de la ligne de liste de contrôle d'accès.

Autoriser la ligne ACL avec les informations de couche 3 uniquement

1. Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, elles sont autorisées.

2. Si les informations de couche 3 d'un paquet ne correspondent pas aux informations de couche 3 de la ligne de liste de contrôle d'accès, l'entrée de liste de contrôle d'accès suivante est traitée.

Refuser la ligne ACL avec les informations de couche 3 uniquement

1. Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, elles sont refusées.

2. Si les informations de couche 3 d'un paquet ne correspondent pas aux informations de couche 3 de la ligne de liste de contrôle d'accès, l'entrée de liste de contrôle d'accès suivante est traitée.

Autoriser la ligne ACL avec les informations de couche 3 uniquement, et le mot clé fragments est présent

Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, le décalage de fragment du paquet est vérifié.

1. Si FO > 0 d'un paquet, le paquet est autorisé.

2. Si FO = 0 d'un paquet, l'entrée de liste de contrôle d'accès suivante est traitée.

Refuser la ligne ACL avec les informations de couche 3 uniquement, et le mot clé fragments est présent

Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, le décalage de fragment du paquet est vérifié.

1. Si le FO > 0 d'un paquet est refusé.

2. Si FO = 0 d'un paquet, la ligne de liste de contrôle d'accès suivante est traitée.

Autoriser la ligne ACL avec les informations L3 et L4

1. Si les informations de couche 3 et de couche 4 d'un paquet correspondent à la ligne ACL et à FO = 0, le paquet est autorisé.

2. Si les informations de couche 3 d'un paquet correspondent à la ligne de la liste de contrôle d'accès et à FO > 0, le paquet est autorisé.

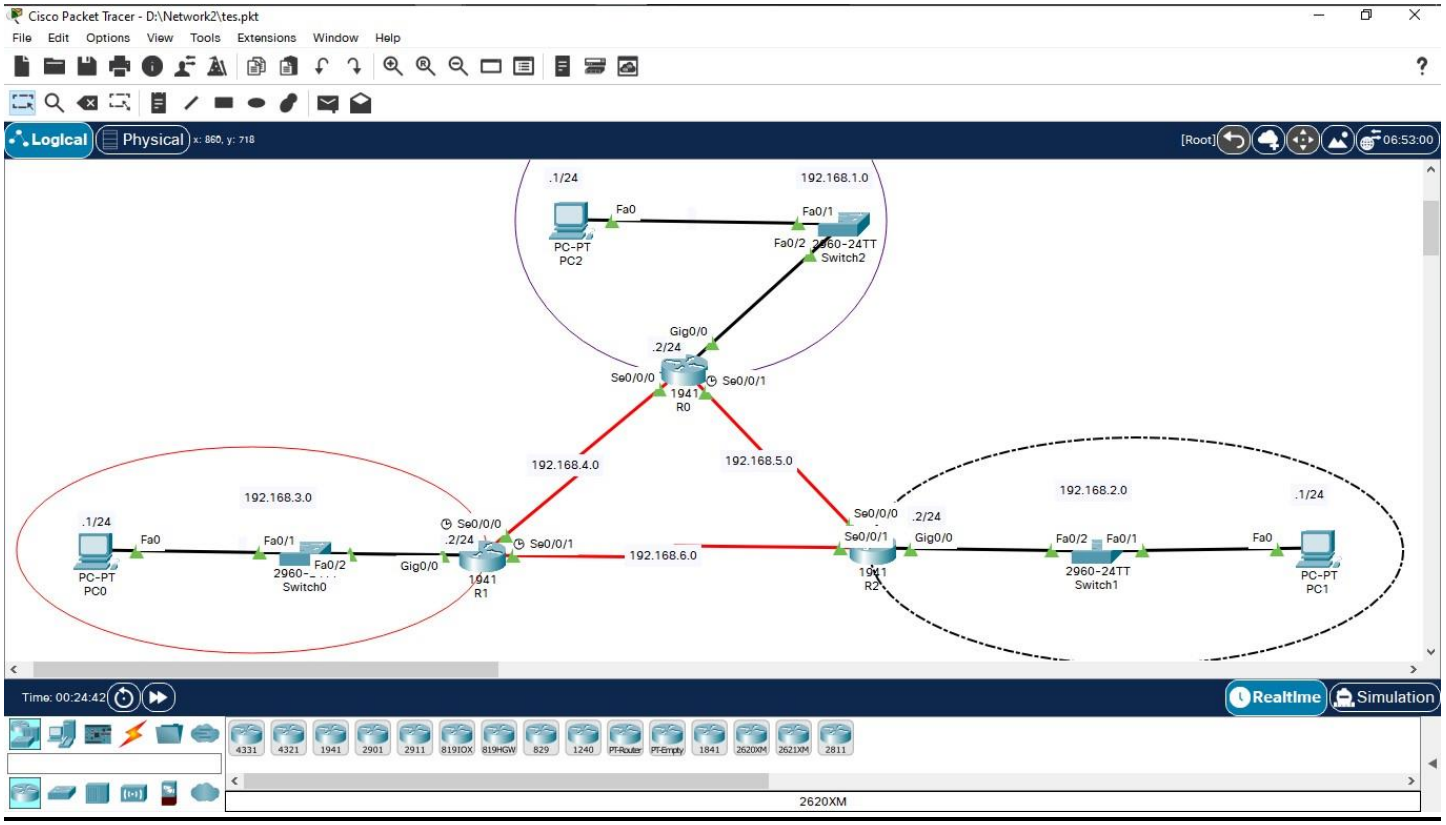
Refuser la ligne ACL avec les informations L3 et L4

1. Si les informations de couche 3 et de couche 4 d'un paquet correspondent à l'entrée de la liste de contrôle d'accès et à FO = 0, le paquet est refusé.

2. Si les informations de couche 3 d'un paquet correspondent à la ligne de liste de contrôle d'accès et à FO > 0, l'entrée de liste de contrôle d'accès suivante est traitée.

Remarque : Les fragments non initiaux eux- mêmes contiennent uniquement des informations de couche 3, jamais de couche 4, bien que la liste de contrôle d'accès puisse contenir des informations de couche 3 et de couche 4.

PRATIQUES(OSPF)




```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 0
                           ^
% Invalid input detected at '^' marker.

Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
Router(config-router)#
```

```
Router>enable
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.4.2, 00:06:06, Serial0/0/0
O    192.168.2.0/24 [110/65] via 192.168.6.2, 00:02:49, Serial0/0/1
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.2/32 is directly connected, GigabitEthernet0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, Serial0/0/0
L       192.168.4.1/32 is directly connected, Serial0/0/0
O    192.168.5.0/24 [110/128] via 192.168.4.2, 00:03:12, Serial0/0/0
                    [110/128] via 192.168.6.2, 00:03:12, Serial0/0/1
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, Serial0/0/1
L       192.168.6.1/32 is directly connected, Serial0/0/1

Router#
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 2
Router(config-router)#network 192.168.4.0 0.0.0.255 area 0
Router(config-router)#network 192.168
00:15:19: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.6.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

                              ^
% Invalid input detected at '^' marker.

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
Router>enable
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.2/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.5.2, 00:01:59, Serial0/0/1
O    192.168.3.0/24 [110/65] via 192.168.4.1, 00:05:42, Serial0/0/0
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, Serial0/0/0
L       192.168.4.2/32 is directly connected, Serial0/0/0
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, Serial0/0/1
L       192.168.5.1/32 is directly connected, Serial0/0/1
O    192.168.6.0/24 [110/128] via 192.168.4.1, 00:02:22, Serial0/0/0
 --More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 2
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#
00:18:07: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.5.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
Router(config-router)#ne
00:18:34: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.6.1 on Serial0/0/1 from LOADING to FULL,
Loading Done

% Ambiguous command: "ne"
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#
```

```
Router>enable
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.1.0/24 [110/65] via 192.168.5.1, 00:01:52, Serial0/0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.2/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/65] via 192.168.6.1, 00:01:25, Serial0/0/1
O    192.168.4.0/24 [110/128] via 192.168.5.1, 00:01:25, Serial0/0/0
                    [110/128] via 192.168.6.1, 00:01:25, Serial0/0/1
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, Serial0/0/0
L       192.168.5.2/32 is directly connected, Serial0/0/0
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, Serial0/0/1
 --More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

PRATIQUES(ACL)

Router8

Physical | Config | CLI | Attributes

IOS Comm

```
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#no ip address
Router(config-if)#int s0/0/1
Router(config-if)#ip addr 192.168.10.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#no shutdown
% 192.168.10.0 overlaps with Serial0/0/1
Serial0/0/0: incorrect IP address assignment
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended reseau-upb
Router(config-ext-nacl)#permit tcp host 192.168.30.1 gt 1023 192.168.20.0 0.0.0.255 eq 22
Router(config-ext-nacl)#permit udp host 192.168.30.3 eq 53 192.168.20.0 0.0.0.255 gt 1023
Router(config-ext-nacl)#permit tcp any any established
Router(config-ext-nacl)#deny ip any any log
                                ^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#
```

Ctrl+F6 to exit CLI focus

Top

Router8

Physical | Config | CLI | Attributes

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Router>enable
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#exit
Router(config)#ip route 192.168.20.0 s0/0/0
                                     ^
% Invalid input detected at '^' marker.

Router(config)#ip route 192.168.20.0 255.255.255.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.10.1
%Invalid next hop address (it's this router)
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.10.2
%Invalid next hop address (it's this router)
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.10.1
%Invalid next hop address (it's this router)
Router(config)#
Router(config)#
Router(config)#
Router(config)#ip access-list extended reseau-expose-CCNA2
Router(config-ext-nacl)#exit
Router(config)#int g0/1
Router(config-if)#int fa0/3
%Invalid interface type and number
Router(config)#int g0/1
Router(config-if)#permit 192.168.30.1 0.0.0.255 192.168.20.3
                   ^
% Invalid input detected at '^' marker.

Router(config-if)#permit tcp 192.168.30.1 0.0.0.255 192.168.20.3
                   ^
% Invalid input detected at '^' marker.

Router(config-if)#permit 192.168.20. 0.0.0.255
                   ^
% Invalid input detected at '^' marker.

Router(config-if)#permit 192.168.20.3 0.0.0.255
                   ^
% Invalid input detected at '^' marker.

Router(config-if)#access-list 1 permit 192.168.20.3 0.0.0.255
Router(config)#
```

Ctrl+F6 to exit CLI focus

Top

PC0

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.7

Pinging 192.168.20.7 with 32 bytes of data:

Reply from 192.168.20.7: bytes=32 time=1ms TTL=126
Reply from 192.168.20.7: bytes=32 time=11ms TTL=126
Reply from 192.168.20.7: bytes=32 time=11ms TTL=126
Reply from 192.168.20.7: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```