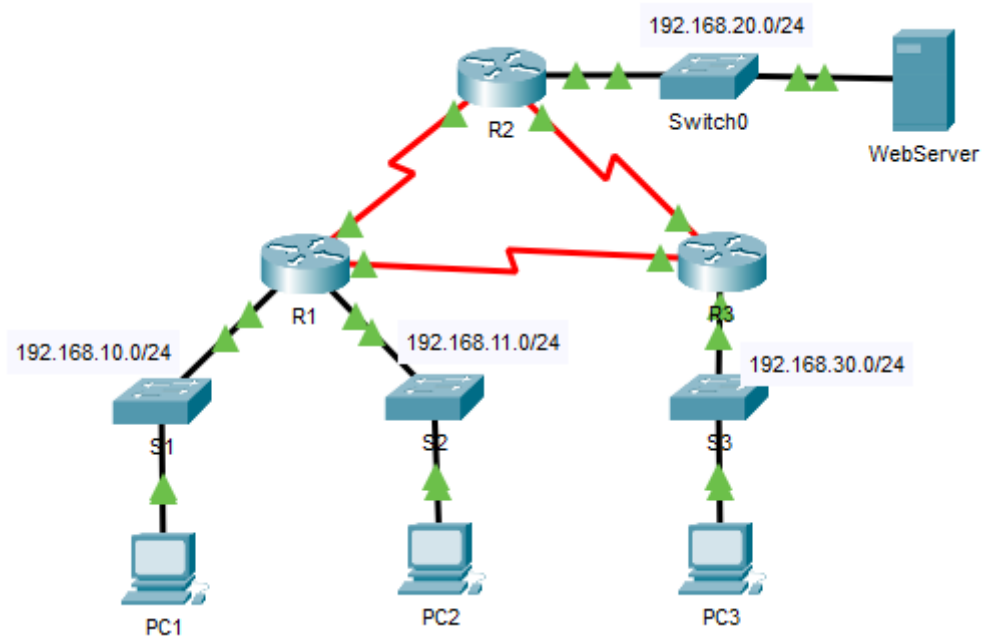


TP - ACL Cisco

Galiegue Enzo - 20/03/2023

Voici l'infrastructure Packet Tracer:



Et Voici le plan d'adressage:

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.10.1	255.255.255.0	N/A
R1	G0/1	192.168.11.1	255.255.255.0	N/A
R1	S0/0/0	10.1.1.1	255.255.255.252	N/A
R1	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192.168.20.1	255.255.255.0	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
R3	S0/0/0	10.3.3.2	255.255.255.252	N/A
R3	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC2	Carte réseau	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Carte réseau	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	Carte réseau	192.168.20.254	255.255.255.0	192.168.20.1

Partie 1 : Planification d'une implémentation de liste de contrôle d'accès.

Étudiez la configuration réseau actuelle.

PING	R1	R2	R3	PC1	PC2	PC3	WebServer
R1	✓	✓	✓	✓	✓	✓	✓
R2	✓	✓	✓	✓	✓	✓	✓
R3	✓	✓	✓	✓	✓	✓	✓
PC1	✓	✓	✓	✓	✓	✓	✓
PC2	✓	✓	✓	✓	✓	✓	✓
PC3	✓	✓	✓	✓	✓	✓	✓
WebServer	✓	✓	✓	✓	✓	✓	✓

Tout les pings effectués ont aboutis, donc tout les éléments peuvent communiquer entre eux. On peut alors conclure qu'il y a une connectivité complète.

Évaluez deux stratégies réseau et planifiez les implémentations de liste de contrôle d'accès.

Voici les stratégies sur les Routers:

- Les deux stratégies réseau sur R2 sont:
 - de ne pas autoriser le réseau 192.168.11.0/24 à accéder à WebServer
 - d'autoriser tout les autres accès
- Les deux stratégies réseau sur R3 sont:
 - de ne pas autoriser le réseau 192.168.10.0/24 à communiquer avec le réseau 192.168.30.0/24
 - d'autoriser tout les autres accès

Partie 2: Configuration, application et vérification d'une liste de contrôle d'accès standard.

Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R2.

Pour configurer cela on se dirige vers le CLI de R2.

```
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip access-group 1 out
```

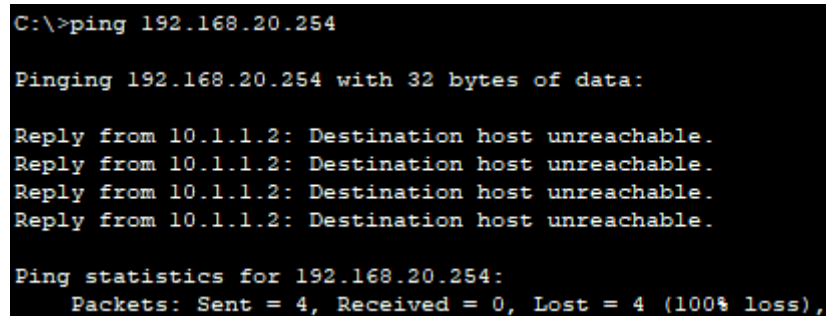
Ligne 1: Nous créons une liste de contrôle d'accès en utilisant le numéro 1, il va permettre de refuser l'accès vers le réseau 192.168.20.0/24 à partir du réseau 192.168.11.0/24

Ligne 2: Nous allons autoriser tout le reste, car par défaut c'est l'inverse

Ligne 3: On se dirige sur l'interface sortante

Ligne 4: Puis nous allons lui appliquer la liste de contrôle d'accès que nous venons de créer.

On peut tester simplement en effectuant un `ping` du **PC2** à **WebServer**:



```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R3.

Pour configurer cela on se dirige vers le CLI de R3.

```
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 1 out
```

Ligne 1: Nous créons une liste de contrôle d'accès en utilisant le numéro 1, il va permettre de refuser l'accès vers le réseau 192.168.30.0/24 à partir du réseau 192.168.11.0/24

Ligne 2: Nous allons autoriser tout le reste, car par défaut c'est l'inverse

Ligne 3: On se dirige sur l'interface sortante

Ligne 4: Puis nous allons lui appliquer la liste de contrôle d'accès que nous venons de créer.

On peut tester simplement en effectuant un `ping` du **PC1** à **PC3**:

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.

Ping statistics for 192.168.30.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Vérifiez la configuration et le fonctionnement des listes de contrôle d'accès.

Configuration des listes ACL sur R2:

```
R2#show access-lists
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255 (4 match(es))
 20 permit any
```

Configuration des listes ACL sur R3:

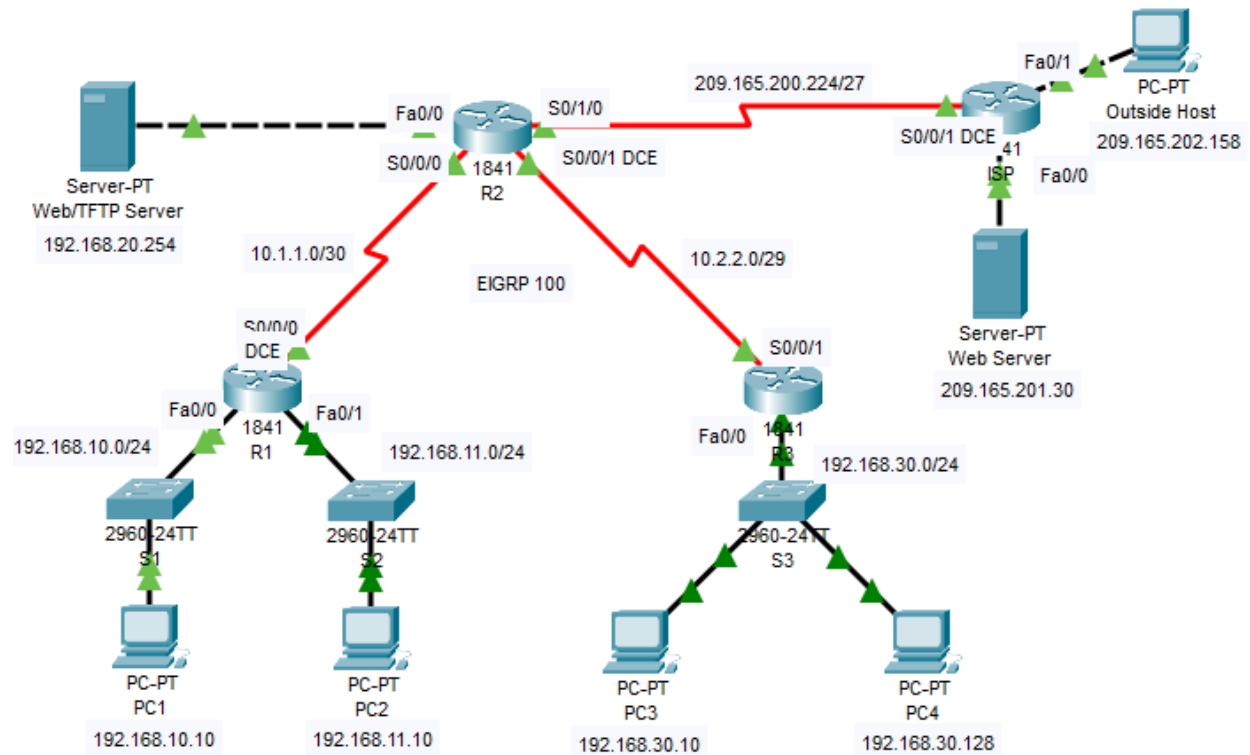
```
R3#show access-lists
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255 (4 match(es))
 20 permit any
```

Lors des vérifications des implémentations de listes de contrôle, les deux seuls test via un ping qui échouent sont au dessus, le reste à abouti.

TP - ACL 2

Galiegue Enzo - 20/03/2023

Voici l'infrastructure Packet Tracer:



Et Voici le plan d'adressage:

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0	10.1.1.1	255.255.255.252
R1	Fa0/0	192.168.10.1	255.255.255.0
R1	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
R2	S0/0/1	10.2.2.1	255.255.255.252
R2	S0/1/0	209.165.200.225	255.255.255.224
R2	Fa0/0	192.168.20.1	255.255.255.0
R3	S0/0/1	10.2.2.2	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
FAI	S0/0/1	209.165.200.226	255.255.255.224
FAI	Fa0/0	209.165.201.1	255.255.255.224

Périphérique	Interface	Adresse IP	Masque de sous-réseau
FAI	Fa0/1	209.165.202.129	255.255.255.224
PC1	Carte réseau	192.168.10.10	255.255.255.0
PC2	Carte réseau	192.168.11.10	255.255.255.0
PC3	Carte réseau	192.168.30.10	255.255.255.0
PC4	Carte réseau	192.168.30.128	255.255.255.0
Serveur TFTP/Web	Carte réseau	192.168.20.254	255.255.255.0
Serveur Web	Carte réseau	209.165.201.30	255.255.255.224
Hôte externe	Carte réseau	209.165.202.158	255.255.255.224

Tâche 1 : étude de la configuration actuelle du réseau

Étape 1. Affichage de la configuration en cours sur les routeurs

Voici les différentes configurations en cours sur les routeurs.

R1:

```

interface FastEthernet0/0
  description R1 LAN
  ip address 192.168.10.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.11.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  description Link to R2
  ip address 10.1.1.1 255.255.255.252
  encapsulation ppp
  ppp authentication pap
  ppp pap sent-username R1 password 0 cisco123
  clock rate 64000
!
```

R2:

```

interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description Link to R1
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password 0 cisco123
!
interface Serial0/0/1
 description Link to R3
 ip address 10.2.2.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 clock rate 64000
!
interface Serial0/1/0
 description Link to ISP
 ip address 209.165.200.225 255.255.255.224
,

```

R3:

```

interface FastEthernet0/0
 description R3 LAN
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 description Link to R2
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!

```

Chaque configuration router est en correspondance avec le plan d'adressage.

Étape 2. Vérification que tous les périphériques ont accès à tous les autres emplacements

En faisant un `show ip route` sur chacun des router, on peut voir que chacuns sont configurés, comme celui ci par exemple, le R3:

```
R3#sh ip route
Codes: C - connected, S - static, I - IGRP, 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 0.0.0.0 to network 0.0.0.0

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D    10.1.1.0/30 [90/2681856] via 10.2.2.1, 00:54:11, Serial0/0/1
C    10.2.2.0/30 is directly connected, Serial0/0/1
C    10.2.2.1/32 is directly connected, Serial0/0/1
D    192.168.10.0/24 [90/2684416] via 10.2.2.1, 00:54:11, Serial0/0/1
D    192.168.11.0/24 [90/2684416] via 10.2.2.1, 00:54:11, Serial0/0/1
D    192.168.20.0/24 [90/2172416] via 10.2.2.1, 00:54:11, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

On peut quand même tester quelques ping:

- À partir de PC1, envoyez une requête ping à PC2
- À partir de PC2, envoyez une requête ping à Hôte externe
- À partir de PC4, envoyez une requête ping au serveur Web/TFTP

<pre>C:\>ping 192.168.11.10 Pinging 192.168.11.10 with 32 bytes of data: Reply from 192.168.11.10: bytes=32 time<1ms TTL=127 Reply from 192.168.11.10: bytes=32 time<1ms TTL=127 Reply from 192.168.11.10: bytes=32 time<1ms TTL=127 Reply from 192.168.11.10: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.11.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>	<pre>C:\>ping 209.165.202.158 Pinging 209.165.202.158 with 32 bytes of data: Reply from 209.165.202.158: bytes=32 time=16ms TTL=125 Reply from 209.165.202.158: bytes=32 time=13ms TTL=125 Reply from 209.165.202.158: bytes=32 time=10ms TTL=125 Reply from 209.165.202.158: bytes=32 time=12ms TTL=125 Ping statistics for 209.165.202.158: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 10ms, Maximum = 16ms, Average = 12ms</pre>	<pre>C:\>ping 192.168.20.254 Pinging 192.168.20.254 with 32 bytes of data: Reply from 192.168.20.254: bytes=32 time=8ms TTL=126 Reply from 192.168.20.254: bytes=32 time=4ms TTL=126 Reply from 192.168.20.254: bytes=32 time=3ms TTL=126 Reply from 192.168.20.254: bytes=32 time=10ms TTL=126 Ping statistics for 192.168.20.254: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 10ms, Average = 6ms</pre>
---	--	--

Tâche 2 : évaluation d'une stratégie de réseau et planification de la mise en œuvre de listes de contrôle d'accès

Étape 1. Évaluation de la stratégie pour les réseaux locaux de R1

Les stratégies pour les réseaux locaux de R1 sont:

- d'autoriser tout les autres accès du réseau 192.168.30.0/24
- de ne pas autoriser l'hôte 192.168.30.128 à accéder hors du réseau local

Étape 3. Évaluation de la stratégie pour le réseau local de R3

Les stratégies pour les réseaux locaux de R3 sont:

- de ne pas autoriser le réseau 192.168.10.0/24 à accéder au réseau 192.168.11.0/24
- d'autoriser tout les autres accès du réseau 192.168.10.0/24
- de ne pas autoriser le réseau 192.168.11.0/24 à accéder à FAI
- d'autoriser tout les autres accès du réseau 192.168.11.0/24

Tâche 3 : configuration de listes de contrôle d'accès standard numérotées

Étape 1. Définition du masque générique

Le masque inversé (0.0.0.255) sert à identifier un réseau entier, alors il convient parfaitement dans ce cas d'utilisation.

Étape 2. Définition des instructions

Avec les commandes suivantes nous allons configurer R1 afin de restreindre l'accès comme demandé:

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Faisons pareil sur R2:

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Étape 3. Application des instructions aux interfaces

Continuons les commandes sur R1 en configurant l'ACL sur l'interface voulue:

```
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip access-group 10 out
```

Puis R2:

```
R2(config)#interface serial 0/1/0
R2(config-if)#ip access-group 11 out
```

Étape 4. Vérification et test des listes de contrôle d'accès

Après ces configurations, on peut les tester simplement en faisant des simples ping:

- PC1 à PC2 (192.168.11.10)
- PC2 à Hôte externe (209.165.202.158)

```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.11.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 209.165.202.158

Pinging 209.165.202.158 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.

Ping statistics for 209.165.202.158:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Étape 5. Vérification des résultats

On peut vérifier que je suis bien arrivé à 66% ~ 67%:

Tâche 4 : configuration d'une liste de contrôle d'accès standard nommée

Étape 1. Définition du masque générique

`host` permet contrairement au masque inversé (0.0.0.255) de ne sélectionner qu'un hôte

Étape 2. Définition des instructions

On va créer une liste de contrôle nommée `NO_ACCESS`, puis refuser le trafic arrivant de l'hôte `192.168.30.128` et autoriser tout le reste.

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Étape 3. Application des instructions à l'interface correcte

On va ensuite appliquer ce que l'on vient de configurer sur l'interface F0/0.

```
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip access-group NO_ACCESS in
```

Étape 4. Vérification et test des listes de contrôle d'accès

En cliquant sur `Check Result`, et dans `Connectivity Tests`, on peut s'apercevoir que 4 tests échouent:

- PC1 vers PC2
- PC2 vers Hôte externe
- PC2 vers Serveur Web
- Toutes les requêtes ping en provenance de/vers PC4, sauf entre PC3 et PC4.

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Below are the results of your connectivity tests:

	Status	Test Condition	Points	Source	Destination	Type
1	Correct	Fail	0	PC1	PC2 : 192.168.11.10	ICMP
2	Correct	Fail	0	PC2	Outside Host : 209.165.202.158	ICMP
3	Correct	Fail	0	PC2	Web Server : 209.165.201.30	ICMP
4	Correct	Fail	0	PC2	PC4 : 192.168.30.128	ICMP
5	Correct	Successful	0	PC3	PC4 : 192.168.30.128	ICMP

Étape 5. Vérification des résultats

Le taux de réalisation est à 100%

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All

Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
[-] Network				
[-] R1				
[-] ACL		0	ACL	
✓ 10	Correct	0	ACL	
[-] Ports		0	Other	
[-] FastEthernet0/1		0	Other	
✓ Access-group Out	Correct	0	ACL	
[-] R2				
[-] ACL		0	ACL	
✓ 11	Correct	0	ACL	
[-] Ports		0	Other	
[-] Serial0/1/0		0	Other	
✓ Access-group Out	Correct	0	ACL	
[-] R3				
[-] ACL		0	ACL	
✓ NO_ACCESS	Correct	0	ACL	
[-] Ports		0	Other	
[-] FastEthernet0/0		0	Other	
✓ Access-group In	Correct	0	ACL	