

INSTITUT UNIVERSITAIRE DES SCIENCES
IUS

Faculté des Sciences et technologies
FST

Projet #3 Étude et Configuration de IGMP et ICMP dans Cisco Packet Tracer

Présentation du projet #3 dans le cadre du cours de Réseau 1

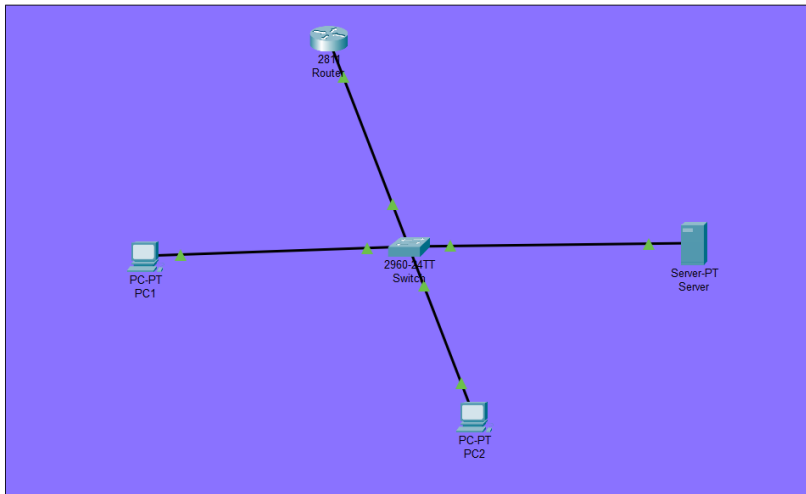
Niveau L3 Sciences Informatiques

Soumis au chargé de Cours **Ismaël SAINT – AMOUR**

Préparé par **Robaldo BADIO**

Date Le 28 / 02 / 2025

Topologie



Analyse des Protocoles IGMP et ICMP

Configuration de ICMP

Router

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
```

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface F0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#
Router(config)#

```

Configuration IGMP

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#
Router#enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip multicast-routing
Router(config)#^
% Invalid input detected at '^' marker.

Router(config)#?
Configure commands:
aaa                Authentication, Authorization and Accounting.
access-list        Add an access list entry
banner             Define a login banner
bba-group          Configure BBA Group
boot               Modify system boot parameters
cdp                Global CDP configuration subcommands
class-map          Configure Class Map
clock              Configure time-of-day clock
config-register    Define the configuration register
crypto             Encryption module
default            Set a command to its defaults
dial-peer          Dial Map (Peer) configuration commands
do                To run exec commands in config mode
dot11              IEEE 802.11 config commands
enable            Modify enable password parameters
end               Exit from configure mode
ephone            define ethernet phone
ephone-dn          Configure ephone phone lines (Directory Numbers)
exit              Exit from configure mode
flow              Global Flow configuration subcommands
hostname           Set system's network name
--More--

```

Pour la configuration de IGMP, les commandes ne passent pas.

1. Dans le TD 6, le TD qui avait rapport sur IGMP et ICMP, il y avait des erreurs dans ces commandes ;
2. J'utilise une version gratuite de Cisco, je pense que c'est la raison pour laquelle ces commandes ne passent pas.

```

Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip multicast-routing
      ^
% Invalid input detected at '^' marker.

Router(config)#interface f0/1
Router(config-if)#ip pim sparse-mode
      ^
% Invalid input detected at '^' marker.

Router(config-if)#ip igmp version 3
      ^
% Invalid input detected at '^' marker.

Router(config-if)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#

```

28 Device Name: Router
 Router Custom Device Model: 2811 IOS15
 Hostname: Router

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Down	--	192.168.1.1/24	<not set>	0040.0B51.D401
FastEthernet0/1	Down	--	<not set>	<not set>	0040.0B51.D402
Vlan1	Down	1	<not set>	<not set>	0001.962E.E15C

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router

Switch

```

Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#interface f0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#

```

IGMP

Il y a des commandes qui ne passent pas encore.

```
Switch>
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip igmp snooping
      ^
% Invalid input detected at '^' marker.

Switch(config)#vlan 101
Switch(config-vlan)#ip igmp snooping
      ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#
```

Vérification de la configuration

Router

```
Router>show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.168.1.1    YES manual up          up
FastEthernet0/1 unassigned      YES unset  administratively down down
Vlan1          unassigned      YES unset  administratively down down
Router>
```

Switch

```
Switch>show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                           Gig0/2
101  VLAN0101                active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
Switch>
```

Configuration des appareils :

Server

The screenshot shows a configuration window for a server. The 'Desktop' tab is selected. Under 'IP Configuration', the 'DHCP' radio button is selected, and a message states 'DHCP request successful.' The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are populated with values. Under 'IPv6 Configuration', the 'Static' radio button is selected, and fields for IPv6 Address, Link Local Address, Default Gateway, and DNS Server are present. Under '802.1X', the 'Use 802.1X Security' checkbox is unchecked, and the 'Authentication' dropdown is set to 'MD5'.

IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
DHCP request successful.	
IPv4 Address	192.168.1.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	/
Link Local Address	FE80::2D0:58FF:FE3B:270E
Default Gateway	
DNS Server	

802.1X	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

PC1

```
Device Name: PC1
Device Model: PC-PT

Port      Link  IP Address      IPv6 Address      MAC Address
FastEthernet0  Up    192.168.1.3/24  <not set>         000C.850C.3DA3
Bluetooth    Down  <not set>       <not set>         0002.4A53.442E

Gateway: 192.168.1.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC1
```

PC2

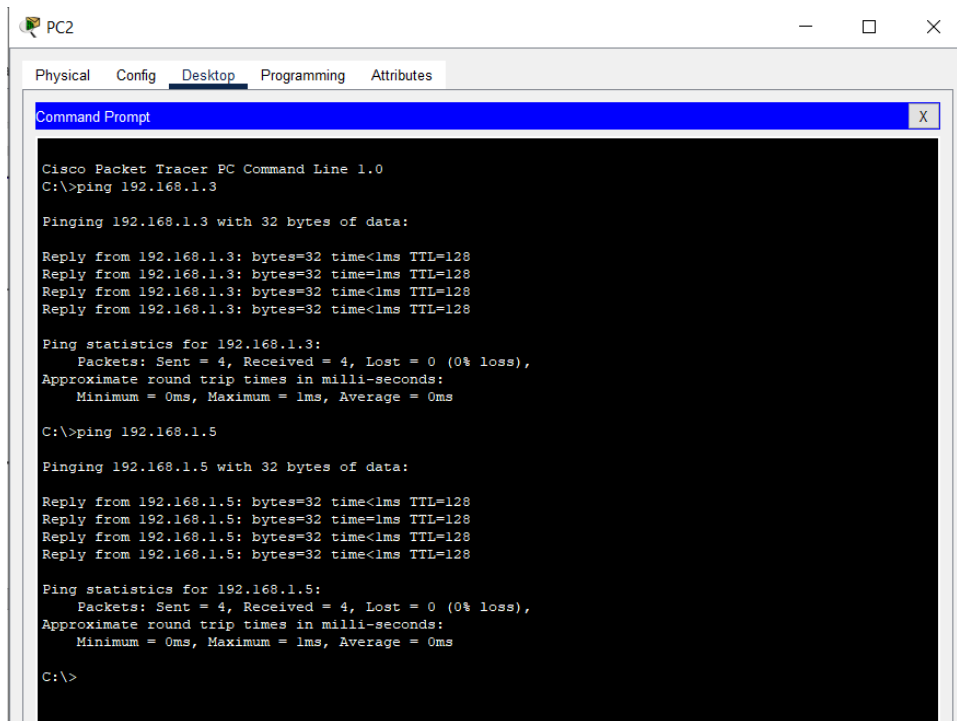
```
Device Name: PC2
Device Model: PC-PT

Port      Link  IP Address      IPv6 Address      MAC Address
FastEthernet0  Up    192.168.1.4/24  <not set>         0060.3ECD.0A04
Bluetooth    Down  <not set>       <not set>         0050.0FB2.548B

Gateway: 192.168.1.1
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC2
```

Vérification de la connectivité pour les appareils :



PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

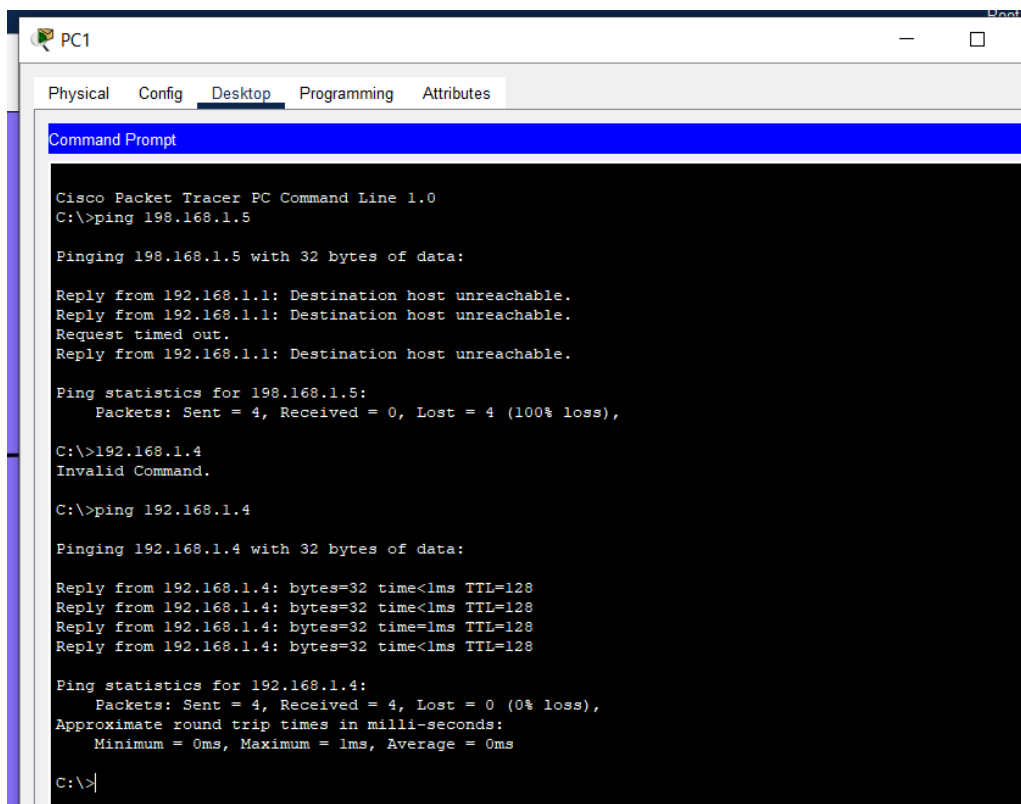
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 198.168.1.5

Pinging 198.168.1.5 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 198.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>192.168.1.4
Invalid Command.

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

Conclusion et Recommandations

- **Importance de ICMP :** Illustrer pourquoi ICMP est essentiel pour la connectivité réseau et le diagnostic des pannes.

Le protocole ICMP (Internet Control Message Protocol) est essentiel pour la connectivité réseau car il permet de détecter et de signaler les erreurs dans les communications réseau. Par exemple, lorsqu'un paquet de données ne parvient pas à atteindre sa destination, ICMP envoie des messages d'erreur pour informer les équipements réseau, tels que les routeurs et les switches, de l'échec de livraison. Cela permet une gestion proactive des réseaux en signalant les points de défaillance et en aidant à réacheminer le trafic, ce qui assure une communication plus fiable et efficace. De plus, ICMP est utilisé pour les fonctions de gestion du réseau, comme la vérification de l'accessibilité des hôtes et la mesure des temps de transit des paquets, ce qui est crucial pour maintenir la performance et la sécurité des réseaux.

En ce qui concerne le diagnostic des pannes, ICMP est un outil précieux pour les administrateurs réseau. Des commandes courantes comme "ping" et "tracert" s'appuient sur ICMP pour tester la connectivité et identifier les points de défaillance sur le chemin réseau entre deux hôtes. Le "ping" envoie des paquets ICMP Echo Request à une destination et attend des réponses Echo Reply, ce qui permet de vérifier si l'hôte est joignable et de mesurer le délai de communication. "Tracert" utilise les messages ICMP Time Exceeded pour tracer le chemin des paquets à travers un réseau, en identifiant chaque nœud intermédiaire et en fournissant des informations détaillées sur les éventuels points de congestion ou de panne. Grâce à ces outils, ICMP facilite la résolution rapide des problèmes et améliore la maintenance proactive des réseaux.

- **Importance de IGMP :** Montrer comment IGMP optimise l'efficacité du réseau pour les applications multicast.

L'IGMP (Internet Group Management Protocol) joue un rôle crucial dans l'optimisation de l'efficacité du réseau pour les applications multicast. Il permet aux routeurs et aux commutateurs

de gérer de manière efficace les abonnements aux groupes multicast, en s'assurant que les paquets de données multicast ne sont envoyés qu'aux hôtes qui en ont fait la demande. Cela réduit considérablement le trafic inutile sur le réseau, car seuls les hôtes intéressés reçoivent les flux de données multicast. Par exemple, dans une application de streaming vidéo en direct, IGMP garantit que le contenu vidéo est acheminé uniquement vers les appareils des utilisateurs qui regardent le flux, évitant ainsi la surcharge du réseau et améliorant la qualité du service.

En outre, IGMP permet aux réseaux de s'adapter dynamiquement aux changements dans les abonnements des hôtes aux groupes multicast. Lorsqu'un hôte rejoint ou quitte un groupe multicast, IGMP envoie des messages de rapport ou de départ aux routeurs, qui ajustent ensuite leur table de routage multicast en conséquence. Cette capacité à réagir rapidement aux changements d'abonnement assure une distribution efficace des données, minimisant la latence et maximisant la bande passante disponible pour d'autres applications. En somme, IGMP améliore la performance et la scalabilité des réseaux multicast en gérant intelligemment la distribution des flux de données vers les hôtes concernés.

Ce projet ne m'a pas permis d'acquérir les connaissances souhaitées par ce qu'il y a des commandent qui n'a pas pu exécuter lors de quelques testent ou lors de quelques configurations. Mais, j'ai appris beaucoup de chose dans ce cours de Réseau 1, c'est pour cette raison que je mets un court résumé de ce projet à la fin du document.

COURTE RESUME ET PRESENTATION DU PROJET :

1 : Introduction

Titre : Protocole ICMP et IGMP **Sous-titre :** Importance et efficacité des protocoles réseau.

Le protocole ICMP (Internet Control Message Protocol) est essentiel pour la gestion des erreurs et la connectivité réseau, en permettant de signaler et de diagnostiquer les problèmes de communication, tandis que le protocole IGMP (Internet Group Management Protocol) optimise l'efficacité des applications multicast en gérant les abonnements aux groupes multicast afin de réduire le trafic inutile et d'améliorer la qualité du service ; ensemble, ces deux protocoles assurent des réseaux plus fiables, performants et adaptatifs.

2 : Protocole ICMP

Définition et rôle :

- ICMP permet de détecter et signaler les erreurs dans les communications réseau.
- Exemples : messages d'erreur pour les paquets non livrés, gestion proactive des réseaux.

3 : ICMP et la connectivité

Connectivité réseau :

- Fonction de gestion réseau : vérification de l'accessibilité des hôtes.
- Mesure des temps de transit des paquets pour maintenir la performance du réseau.

4 : ICMP et le diagnostic des pannes

Outils de diagnostic :

- **Ping :** Envoie des paquets Echo Request pour tester la connectivité et mesurer les délais.
- **Traceroute :** Utilise les messages Time Exceeded pour tracer le chemin des paquets à travers le réseau.

5 : Protocole IGMP

Définition et rôle :

- IGMP gère les abonnements aux groupes multicast, réduisant le trafic inutile.
- Optimisation du réseau : assure que seuls les hôtes intéressés reçoivent les flux multicast.

6 : IGMP et l'efficacité du réseau

Gestion dynamique :

- Messages de rapport et de départ pour ajuster les tables de routage multicast.
- Adaptation rapide aux changements d'abonnement, maximisant la bande passante disponible.

7 : Comparaison entre ICMP et IGMP

Le protocole ICMP (Internet Control Message Protocol) et le protocole IGMP (Internet Group Management Protocol) ont des fonctions distinctes mais essentielles dans la gestion des réseaux. ICMP est principalement utilisé pour la gestion des erreurs et le diagnostic des pannes dans les communications réseau. Il permet aux équipements réseau, comme les routeurs et les switches, de signaler les échecs de livraison des paquets de données et d'envoyer des messages d'erreur. Par exemple, des outils comme "ping" et "traceroute" s'appuient sur ICMP pour tester la connectivité et identifier les points de défaillance dans le réseau.

En revanche, IGMP est utilisé pour optimiser l'efficacité des réseaux pour les applications multicast. IGMP permet aux routeurs et switches de gérer les abonnements aux groupes multicast, ce qui assure que seuls les hôtes intéressés reçoivent les flux de données multicast. Cela réduit le trafic inutile sur le réseau et améliore la qualité du service. Par exemple, dans une application de streaming vidéo en direct, IGMP s'assure que le contenu vidéo est acheminé uniquement vers les utilisateurs qui regardent le flux. Ainsi, tandis qu'ICMP se concentre sur la communication et la gestion des erreurs, IGMP se concentre sur la distribution efficace des données multicast. Ensemble, ces protocoles contribuent à des réseaux plus fiables et performants.

Utilisations spécifiques :

- Différences clés entre les deux protocoles.
- Importance combinée pour une communication efficace et fiable.

8: Conclusion

Résumé:

- Points clés abordés : rôle et importance d'ICMP et IGMP.
- Impact sur la performance et la gestion des réseaux modernes.