

RÉSEAUX INFORMATIQUES

Master 1

Dr. Alassane Diop

Ph. D. Télématiques et Réseaux Informatique

UFR SATIC
Université Alioune Diop de Bambe

Module 9 : Pile de protocoles TCP/IP et adressage IP

FIGURES

1

2

3

4

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :

9.1 Présentation du protocole TCP/IP

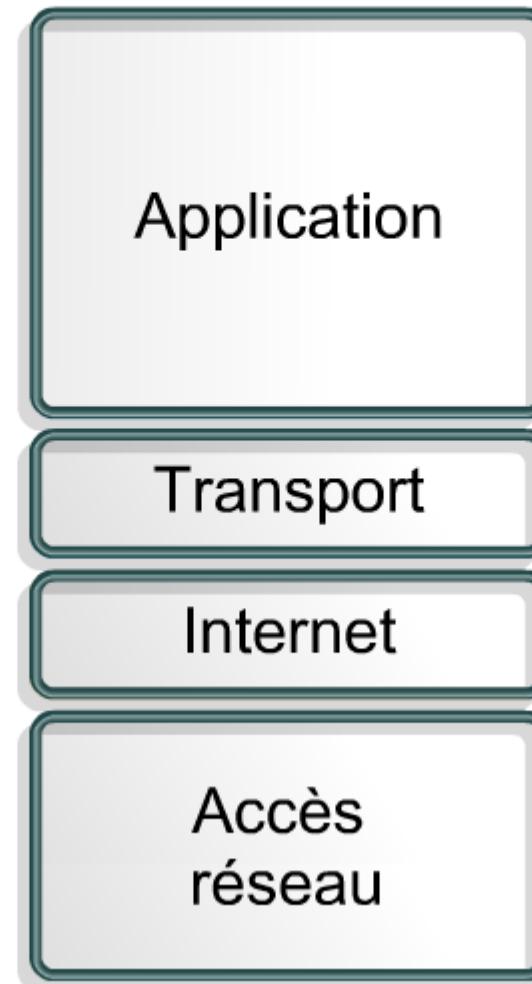
9.2 Adresses Internet

9.3 Obtention d'une adresse IP

Modèle TCP/IP

FIGURE

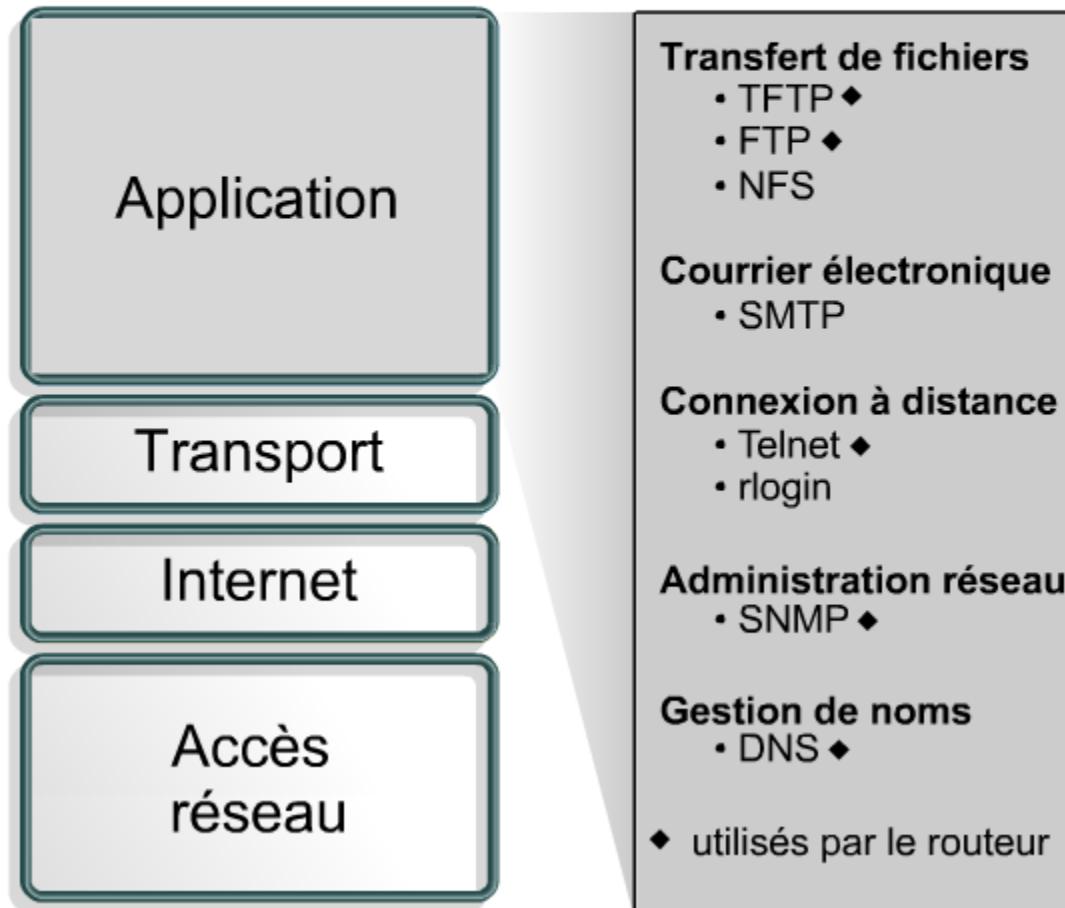
1



Applications TCP/IP

FIGURE

1

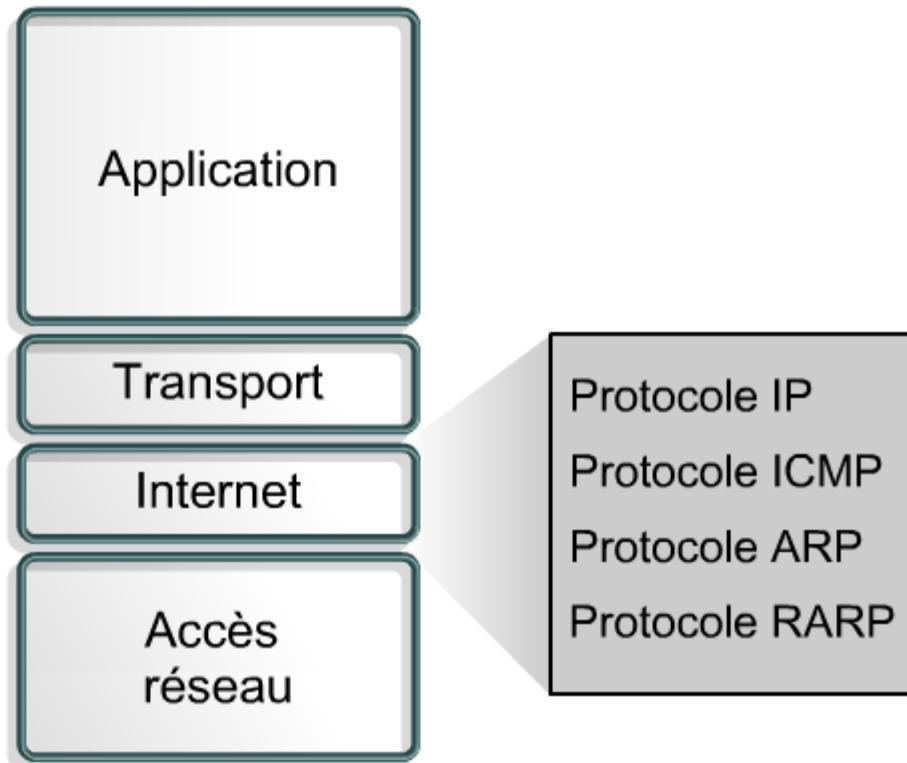


Protocoles de la couche Internet

FIGURES

1

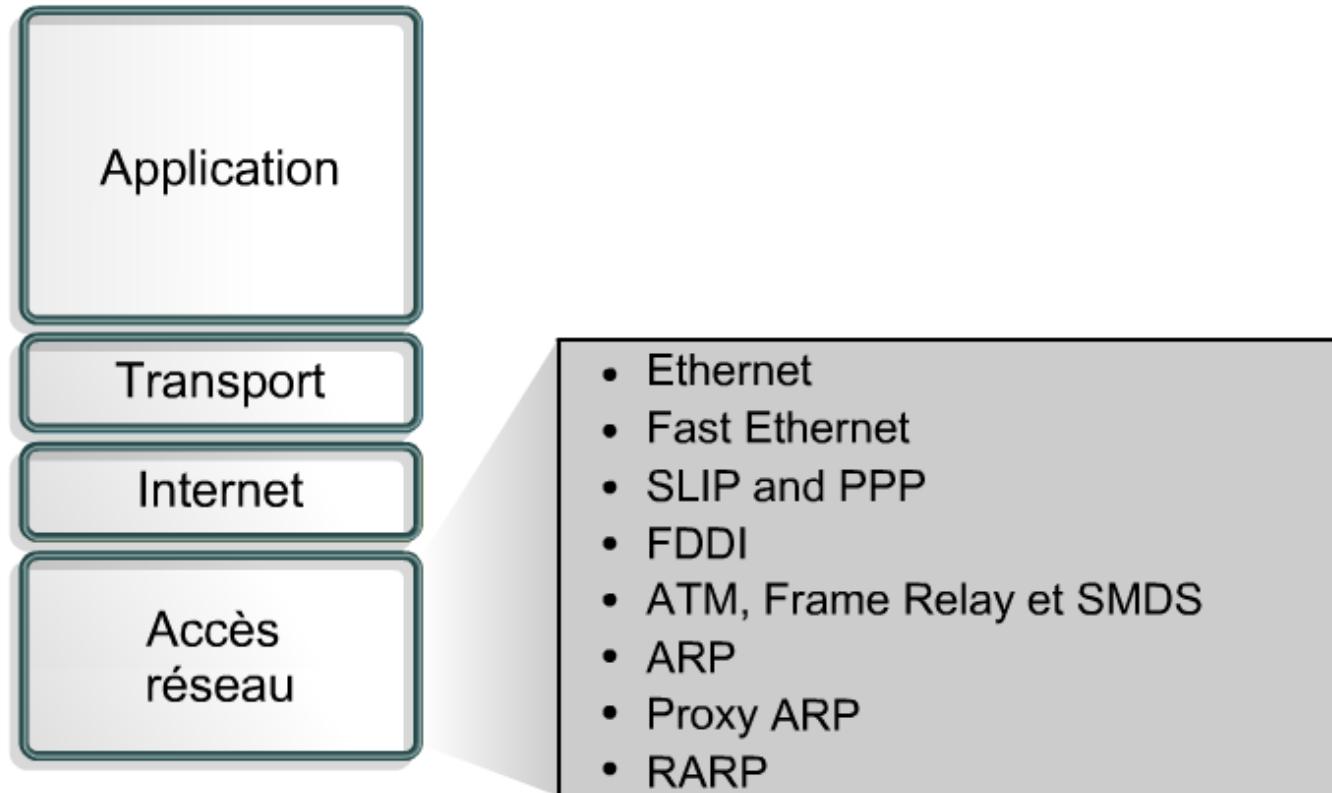
2



Protocoles d'accès au réseau

FIGURE

1



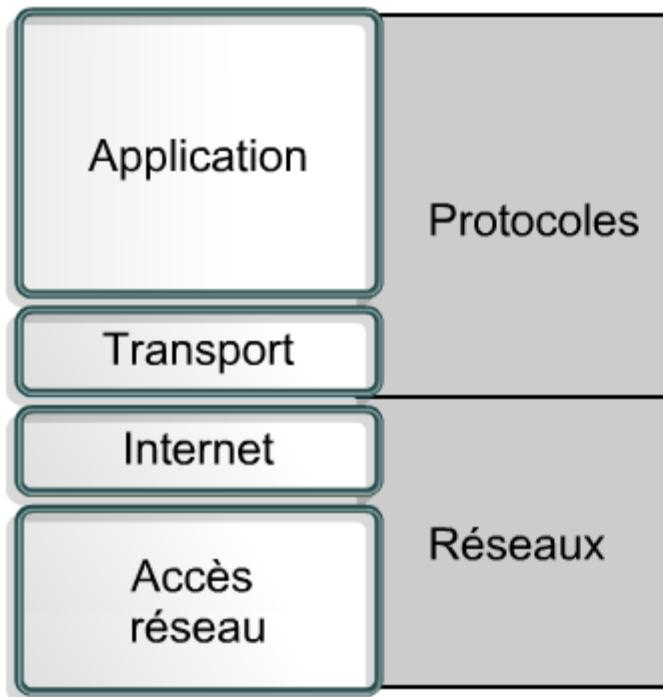
Les protocoles ARP et RARP se situent au niveau des couches d'accès réseau et Internet.

Comparaison du modèle TCP/IP et du modèle OSI

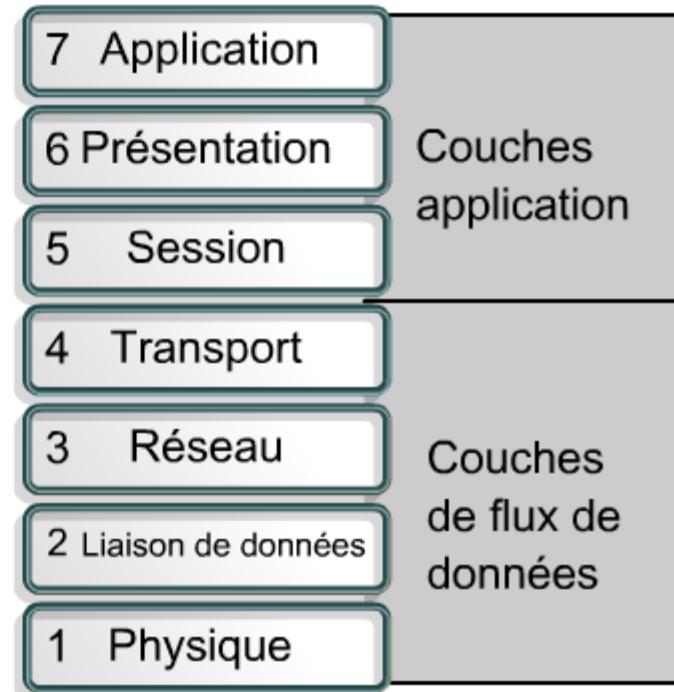
FIGURE

1

TCP/IP Modèle



OSI Modèle



Le routeur relie deux réseaux.

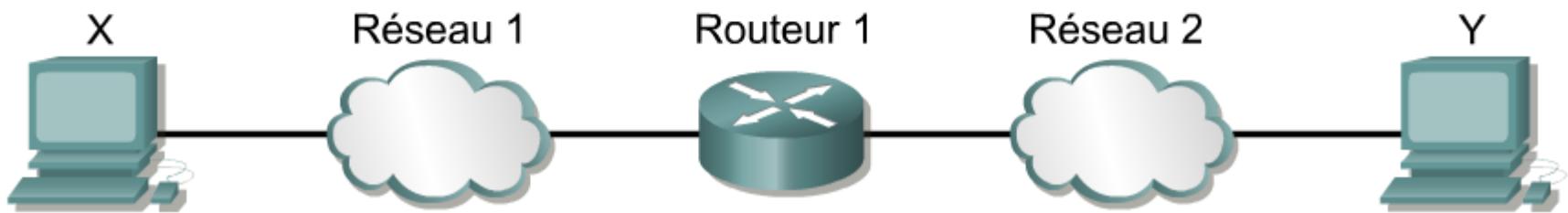
FIGURES

1

2

3

4



Les routeurs relient les réseaux locaux et distants.

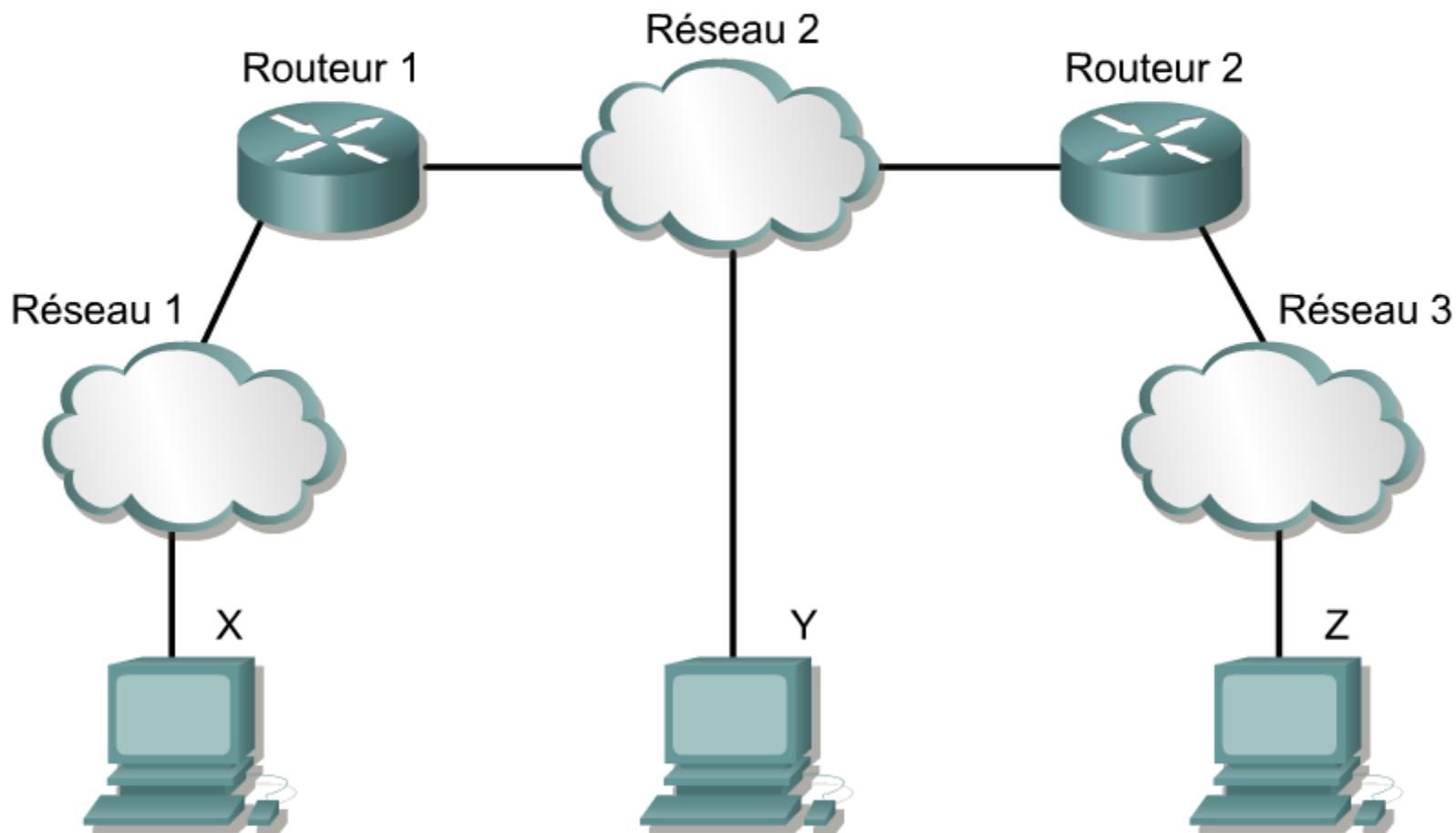
FIGURES

1

2

3

4



Les utilisateurs peuvent afficher le nuage TCP/IP.

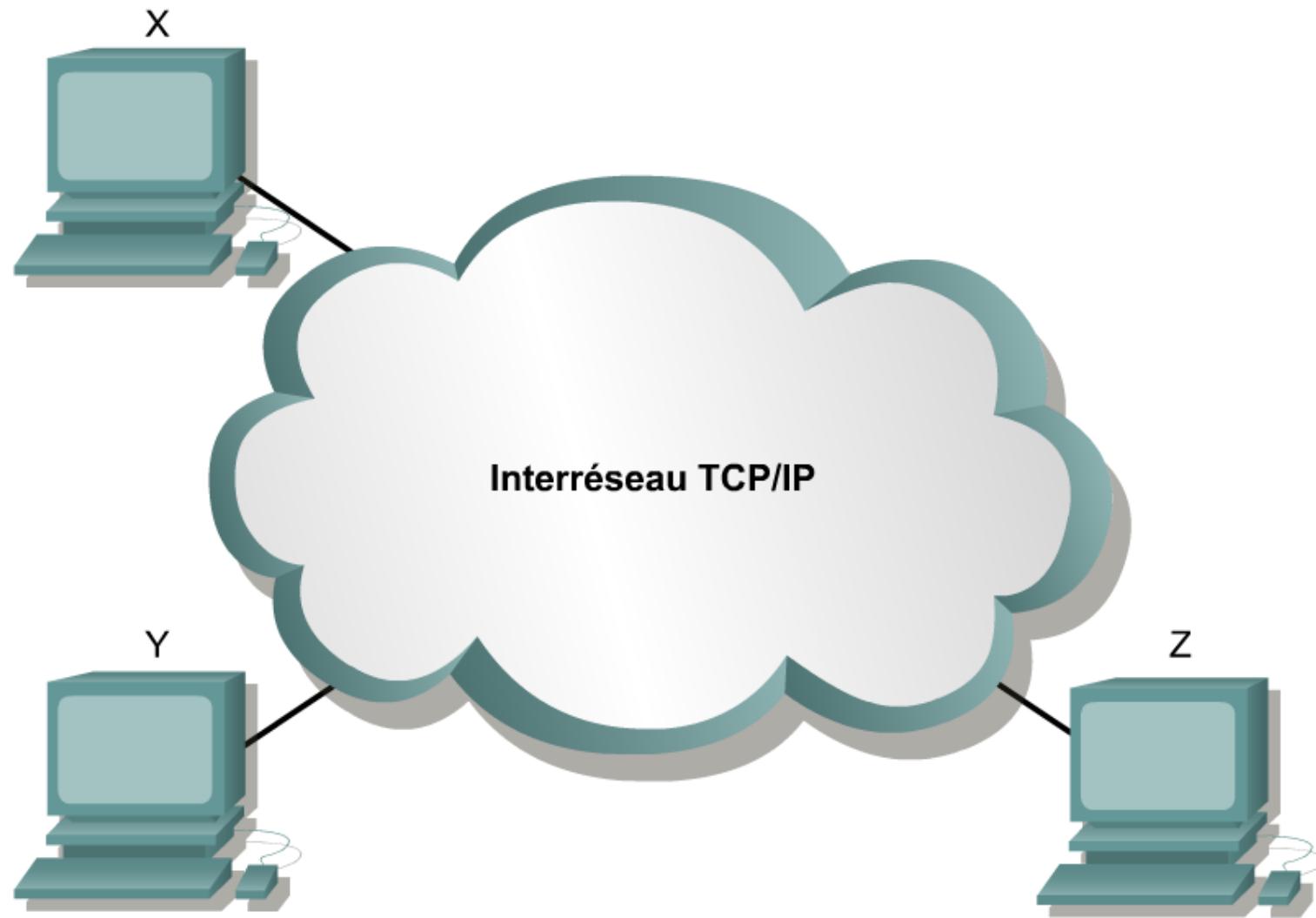
FIGURES

1

2

3

4



Détails physiques non visibles pour les utilisateurs

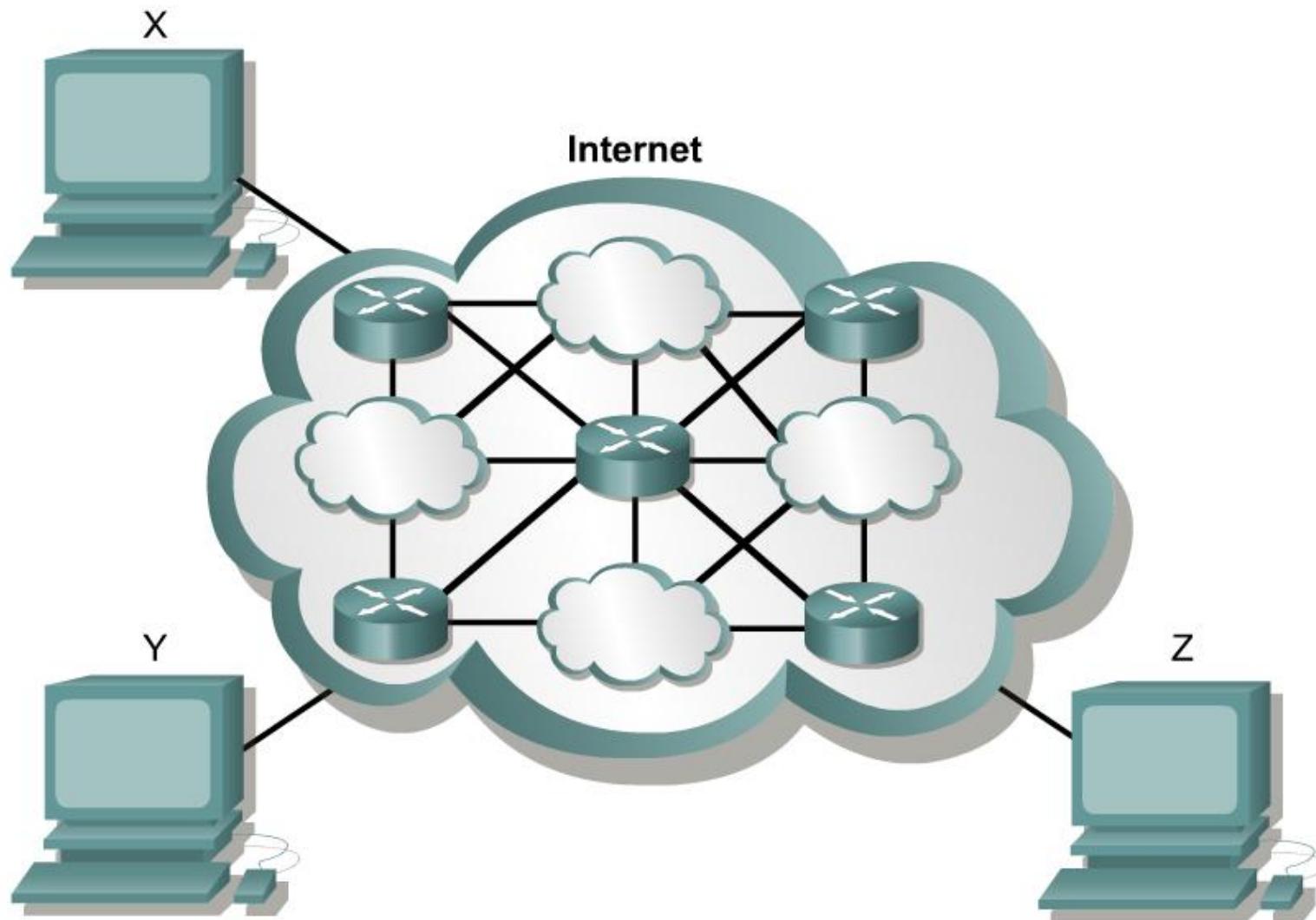
FIGURES

1

2

3

4



Adresses hôte

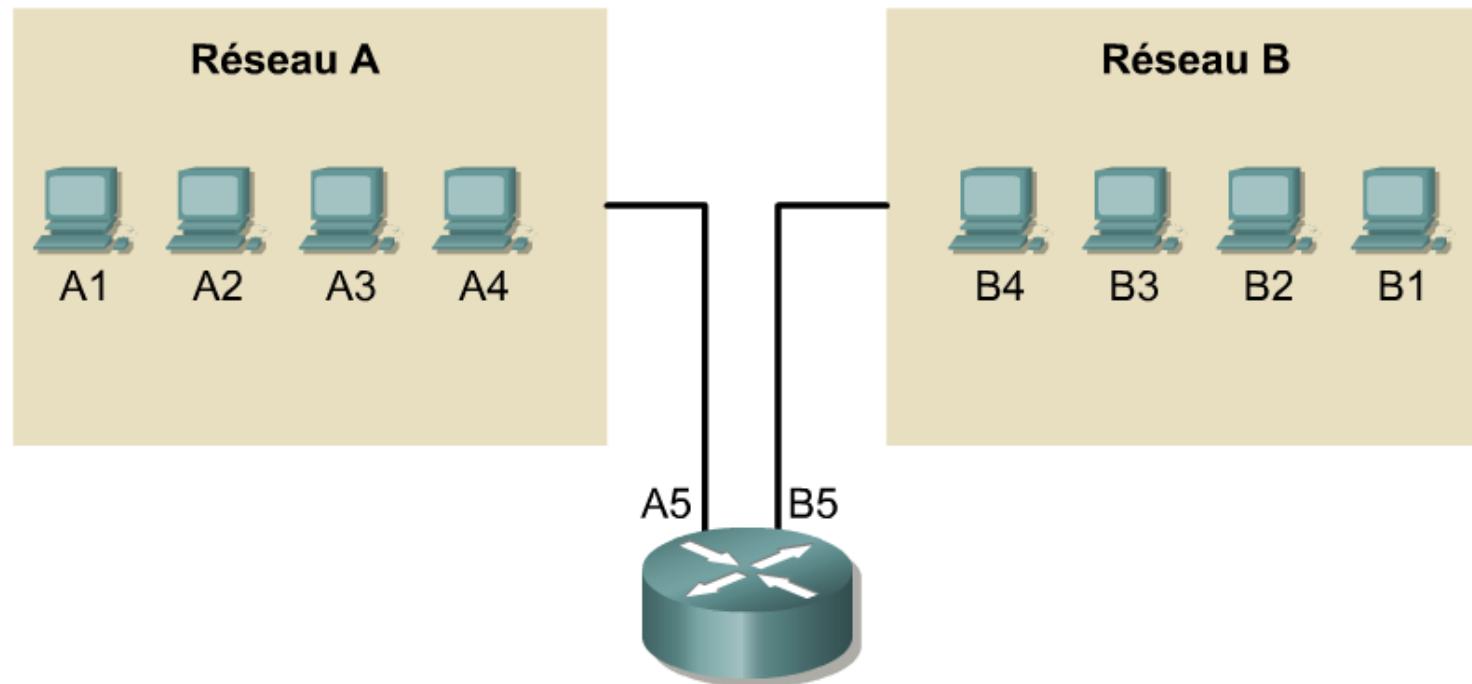
FIGURES

1

2

3

4



Ces adresses ne correspondent pas à des adresses réseau réelles, mais elles illustrent le concept du regroupement d'adresses. Dans ce concept, les lettres A ou B identifient le réseau, et la séquence de nombres désigne l'hôte correspondant. La combinaison d'une lettre (adresse réseau) et d'un numéro (adresse hôte) crée une adresse unique pour chaque unité du réseau.

Ordinateur à liaison double

FIGURES

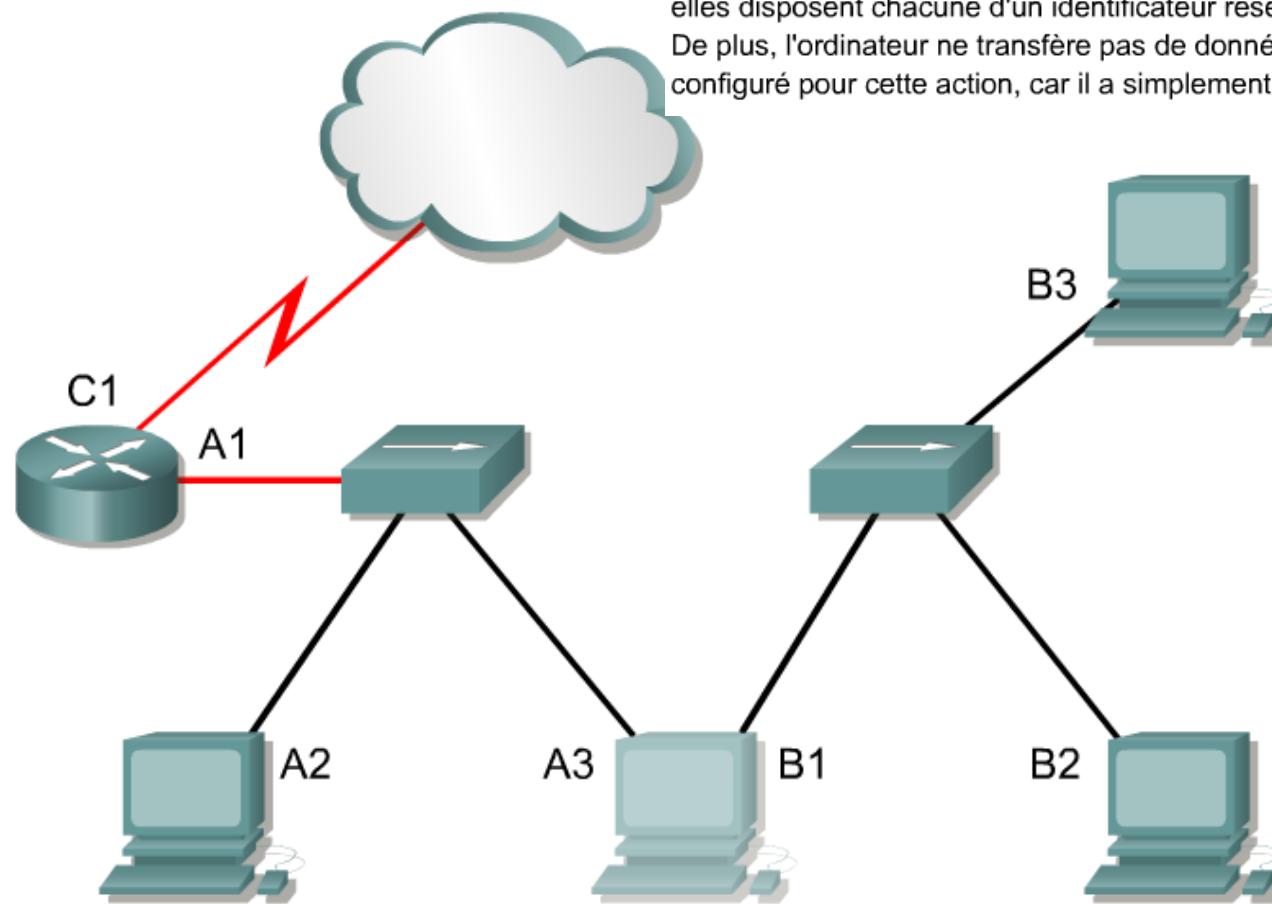
1

2

3

4

Voici l'exemple d'un ordinateur connecté à deux réseaux différents. Pour cela, il dispose de deux cartes réseau. Il est alors désigné sous le nom d'unité à liaison double. Il est important de retenir que les deux interfaces de l'ordinateur se trouvant sur des réseaux totalement différents, elles disposent chacune d'un identificateur réseau distinct pour l'adresse. De plus, l'ordinateur ne transfère pas de données, à moins qu'il n'ait été configuré pour cette action, car il a simplement accès aux deux réseaux.



Structure d'adressage IP

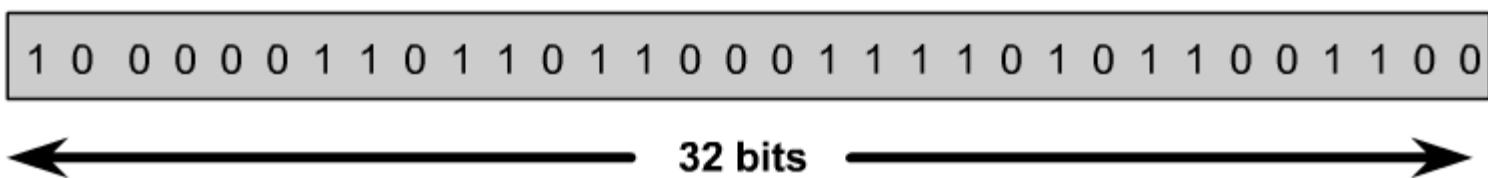
FIGURES

1

2

3

4



Valeurs binaires et décimales consécutives

FIGURES

1

2

3

4

Binaire : 11000000.10101000.00000001.00001000 et 11000000.10101000.00000001.00001001

Décimale : 192.168.1.8 et 192.168.1.9

Les nombres binaires et décimaux représentent les mêmes valeurs, mais les valeurs décimales permettent une meilleure visibilité. Il s'agit d'un des problèmes les plus fréquemment rencontrés lorsque des nombres binaires sont directement utilisés. La longue chaîne de 1 et de 0 répétés est propice aux omissions et aux transpositions.

Deux octets (nombre de 16 bits)

FIGURES

1

2

3

4

5

6

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Deux octets (nombre de 16 bits)

FIGURES

1

2

3

4

5

6

Puissance de la position	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7
Valeur décimale	6783	6783	6783	6783	2687	639	639	127	127
Valeur de la position	32768	16384	8192	4096	2048	1024	512	256	128
Compte binaire	0	0	0	1	1	0	1	0	0
Reste	6783	6783	6783	2687	639	639	127	127	127

← || →

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
127	127	63	31	15	7	3	1
128	64	32	16	8	4	2	1
0	1	1	1	1	1	1	1
127	63	31	15	7	3	1	0

|| →

Conversion du nombre décimal 6783 en nombre binaire 000110100

Un octet (nombre de 8 bits)

FIGURES

1

2

3

4

5

6

Puissance de la position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valeur décimale	104	104	40	8	8	0	0	0
Valeur de la position	128	64	32	16	8	4	2	1
Compte binaire	0	1	1	0	1	0	0	0
Reste	104	40	8	8	0	0	0	0

Conversion du nombre décimal 104 en nombre binaire 01101000.

Conversion de nombres décimaux en nombres binaires

FIGURES

1

2

3

4

5

6

Nombre décimal	Nombre binaire
244	
Essayez un autre nombre.	Vérifiez votre réponse.

Conversion de nombres décimaux en nombres binaires

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6

Nombre décimal	Nombre binaire
244	11110100
Essayez un autre nombre.	Vérifiez votre réponse.

Conversion de nombres binaires en nombres décimaux

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6

Nombre binaire	Nombre decimal
10110100	
Essayez un autre nombre.	Vérifiez votre réponse.

Conversion de nombres binaires en nombres décimaux

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6

Nombre binaire	Nombre decimal
10110100	180
Essayez un autre nombre.	Vérifiez votre réponse.

Chemin de communication de la couche réseau

FIGURES

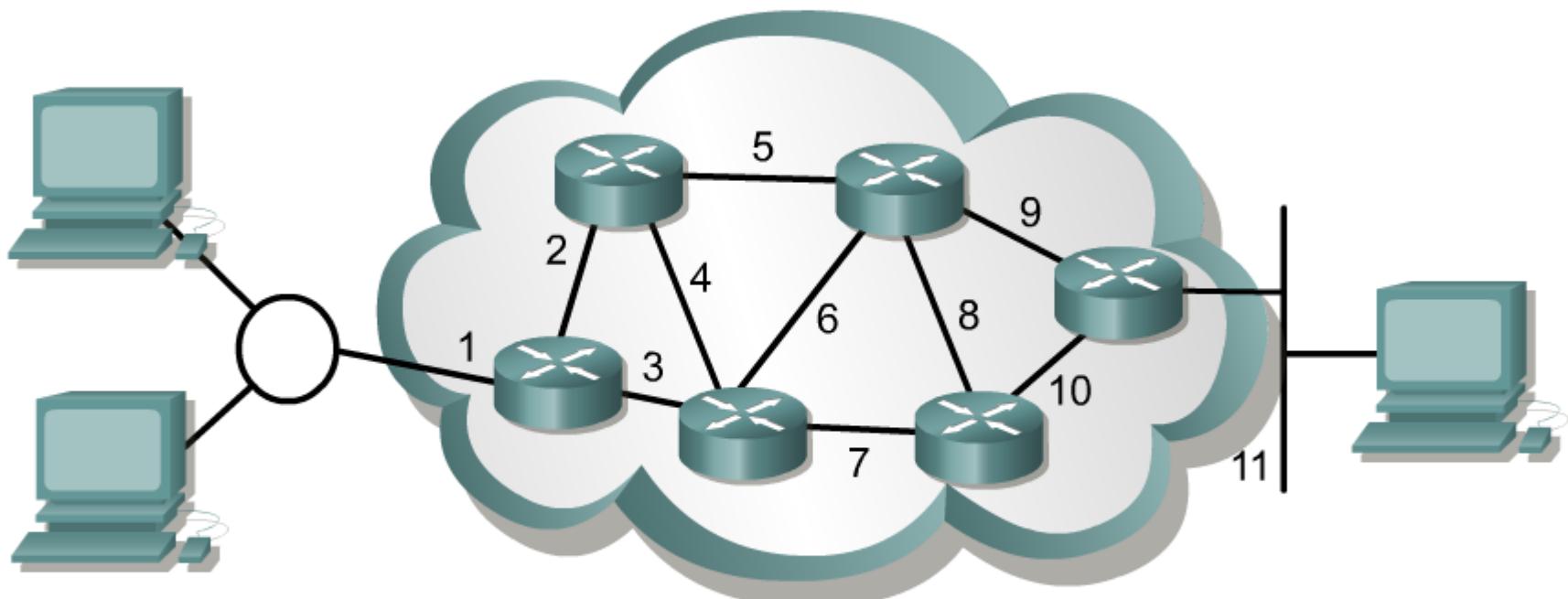
1

2

3

4

5



Les adresses représentent le chemin des connexions média.

Adressage des réseaux et des hôtes

FIGURES

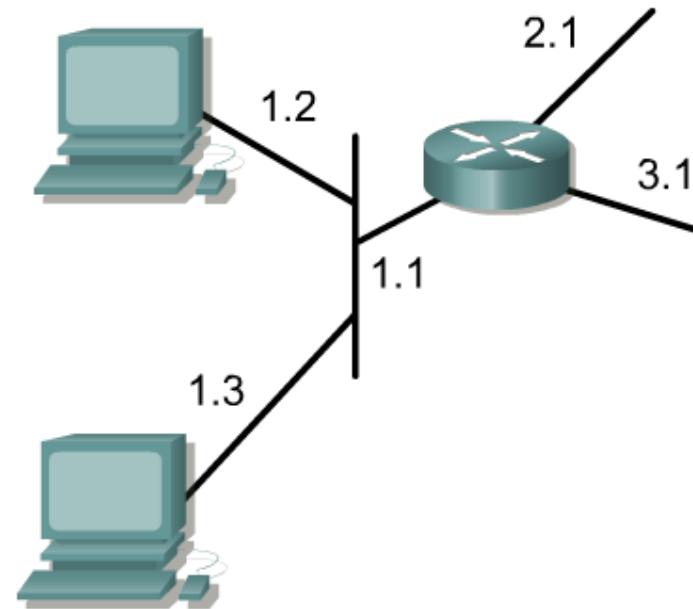
1

2

3

4

5



Réseau	Hôte
1	1 2 3
2	1
3	1

Adresses Internet

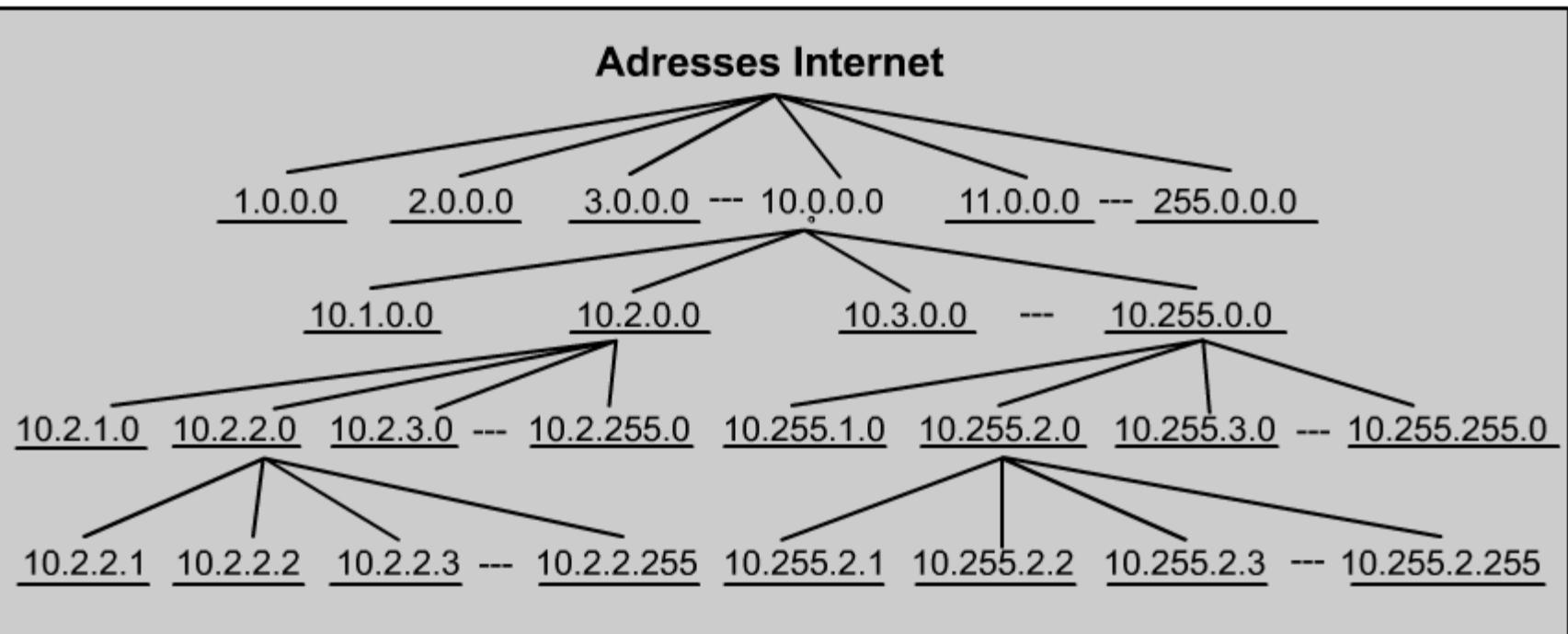
FIGURES

1
2

3

4

5



Classes d'adresses IP

FIGURES

1

2

3

4

5

Classe de l'adresse	Nombre de réseaux	Nombre d'hôtes par réseau
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (multicast)	S.O.	S.O.

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

Identification des classes d'adresses

FIGURES

- 1
- 2
- 3
- 4
- 5

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
----------------------	---------------------------	-----------------------------------	------------------------------------

Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

Préfixes des classes d'adresses

FIGURES

1

2

3

4

5

6

7

8

Classe A	Réseau	Hôte		
Octet	1	2	3	4

Classe B :	Réseau	Hôte		
Octet	1	2	3	4

Classe C	Réseau	Hôte		
Octet	1	2	3	4

Classe D	Hôte			
Octet	1	2	3	4

Les adresses de classe D sont utilisées pour les groupes de multicast. Il n'est pas nécessaire d'allouer des octets ou des bits pour séparer les adresses réseau et hôte. Les adresses de classe E sont réservées à la recherche.

Division du réseau et de l'hôte

FIGURES

1

2

3

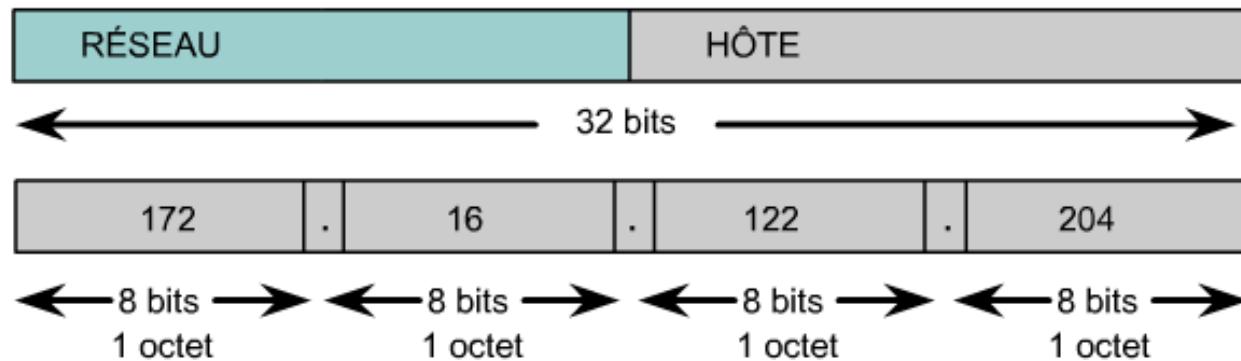
4

5

6

7

8

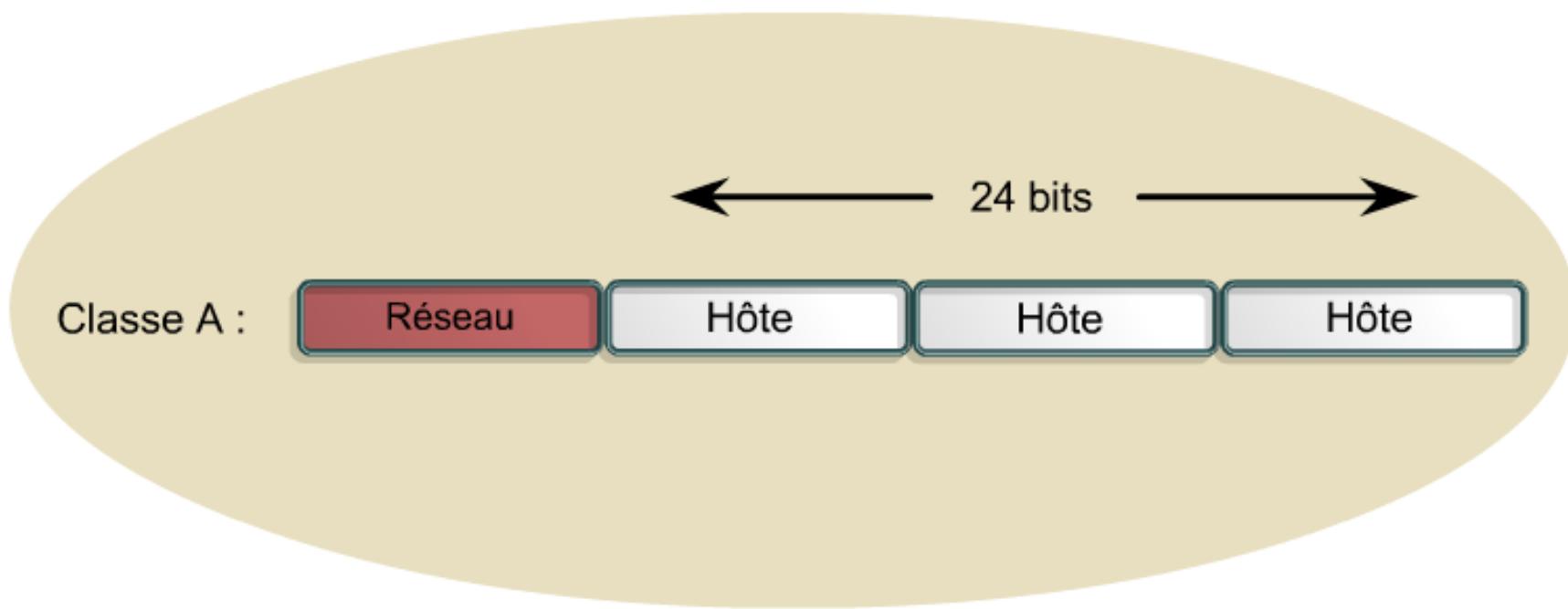


Une adresse IP comporte toujours une partie réseau et une partie hôte. Dans un modèle d'adressage par classe, cette distinction est effectuée au niveau des frontières entre les octets.

Adresse de classe A

FIGURES

1
2
3
4
5
6
7
8



Adresse de classe B

FIGURES

1
2
3
4
5
6
7
8

Classe B :



Adresse de classe C

FIGURES

1
2
3
4
5
6
7
8

Classe C :

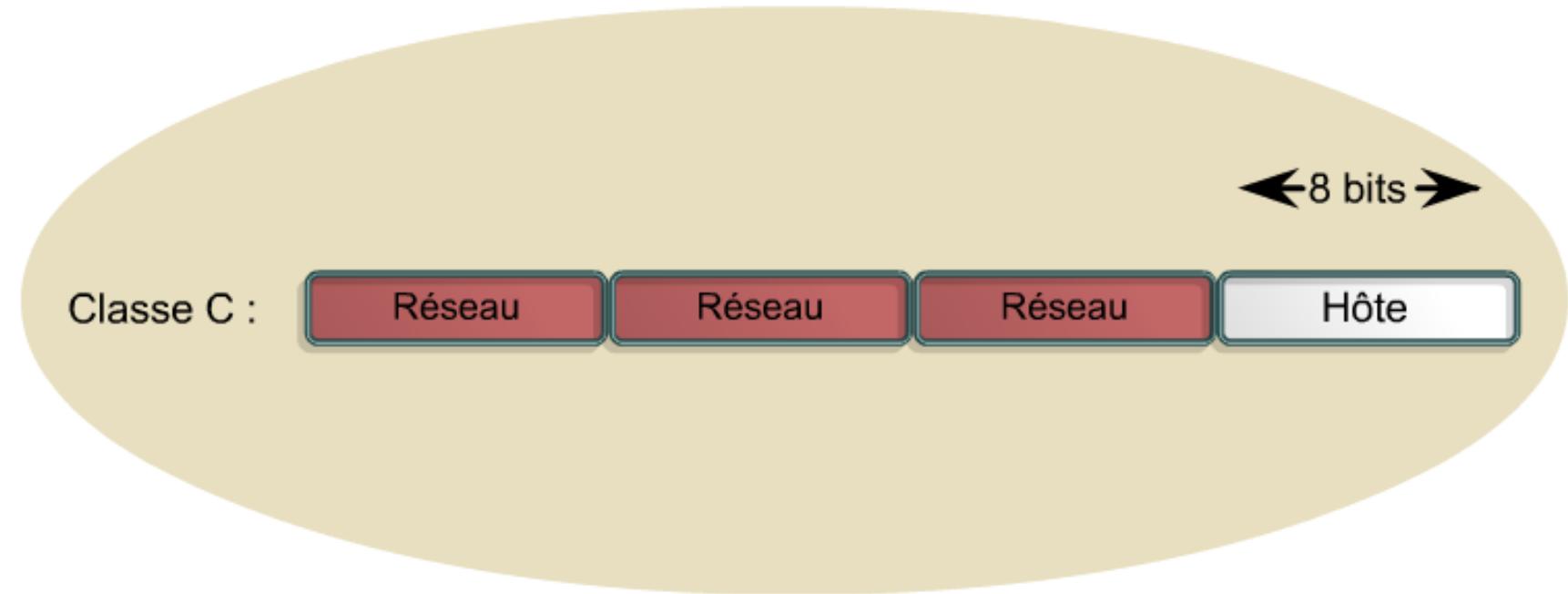
Réseau

Réseau

Réseau

Hôte

←8 bits→



Architecture de l'adresse de classe D

FIGURES

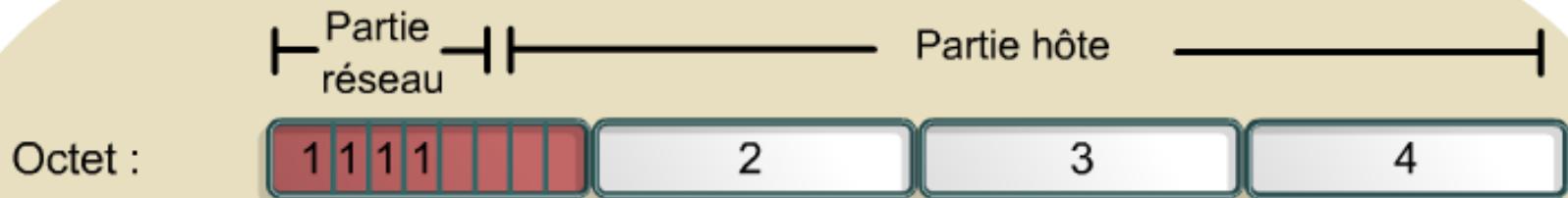
1
2
3
4
5
6
7
8



Architecture de l'adresse de classe E

FIGURES

1
2
3
4
5
6
7
8



Plage d'adresses IP

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Classe d'adresses IP

Plage d'adresses IP (premier octet)

Classe A	1-126 (00000001-01111110) *
Classe B :	128-191 (10000000-10111111)
Classe C	192-223 (11000000-11011111)
Classe D	224-239 (11100000-11101111)
Classe E	240-255 (11110000-11111111)

Déterminez la classe d'après le premier octet.

* 127 (01111111) est une adresse de classe A réservée aux tests en mode bouclé et elle ne peut pas être attribuée à un réseau.

Adresse réseau

FIGURES

1

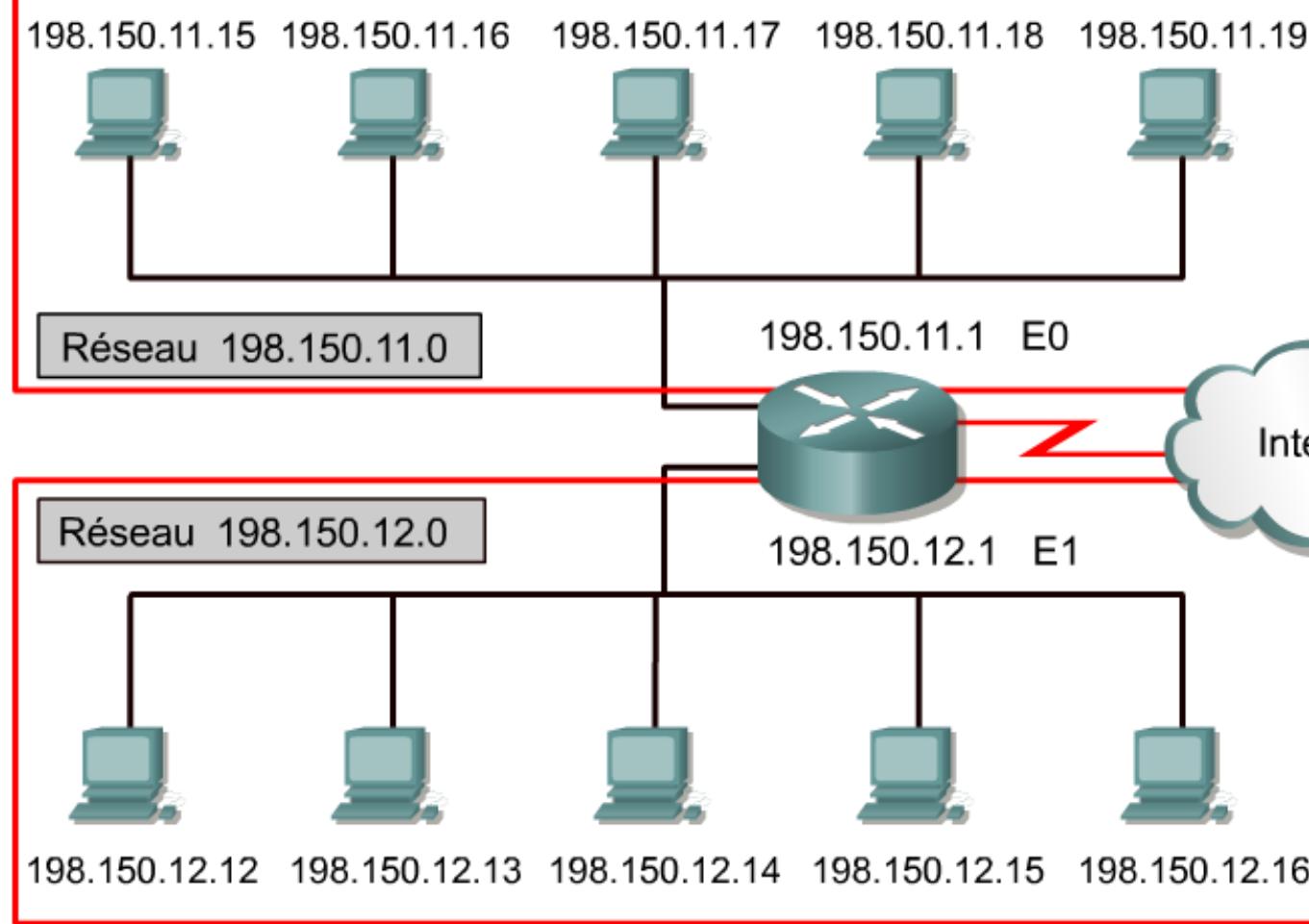
2

3

4

5

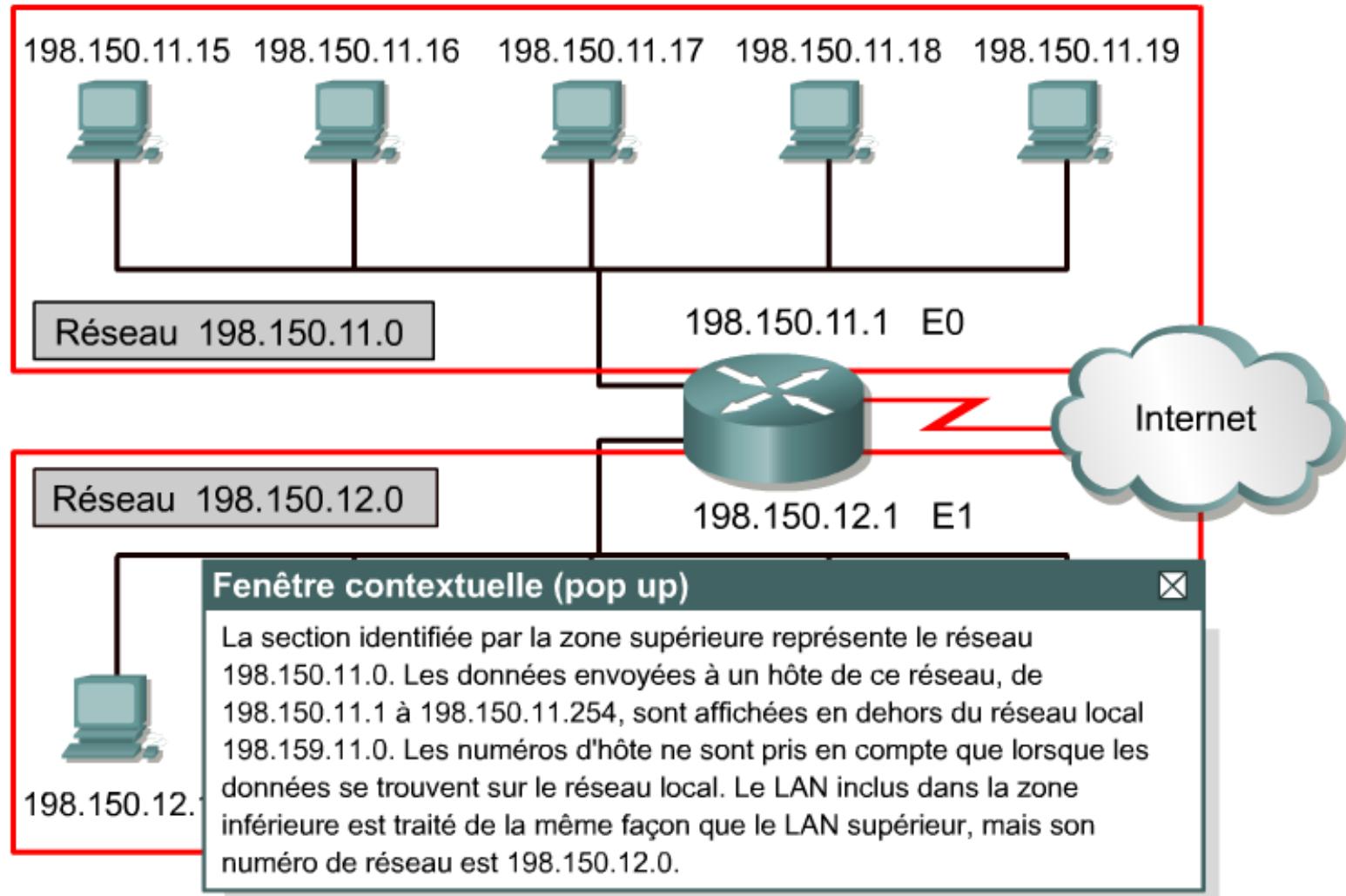
6



Adresse réseau

FIGURES

1
2
3
4
5
6



Adresse de broadcast

FIGURES

1

2

3

4

5

6

198.150.11.15 198.150.11.16 198.150.11.17 198.150.11.18 198.150.11.19



Adresse 198.150.11.255

198.150.11.1 E0

Adresse 198.150.12.255

198.150.12.1 E1

Internet



198.150.12.12 198.150.12.13 198.150.12.14 198.150.12.15 198.150.12.16

Adresse de broadcast

FIGURES

1

2

3

4

5

6

198.150.11.15 198.150.11.16 198.150.11.17 198.150.11.18 198.150.11.19



198.150.11.1 E0

Adresse 198.150.11.255



Adresse 198.150.12.255

198.150.12.1 E1



198.150.1

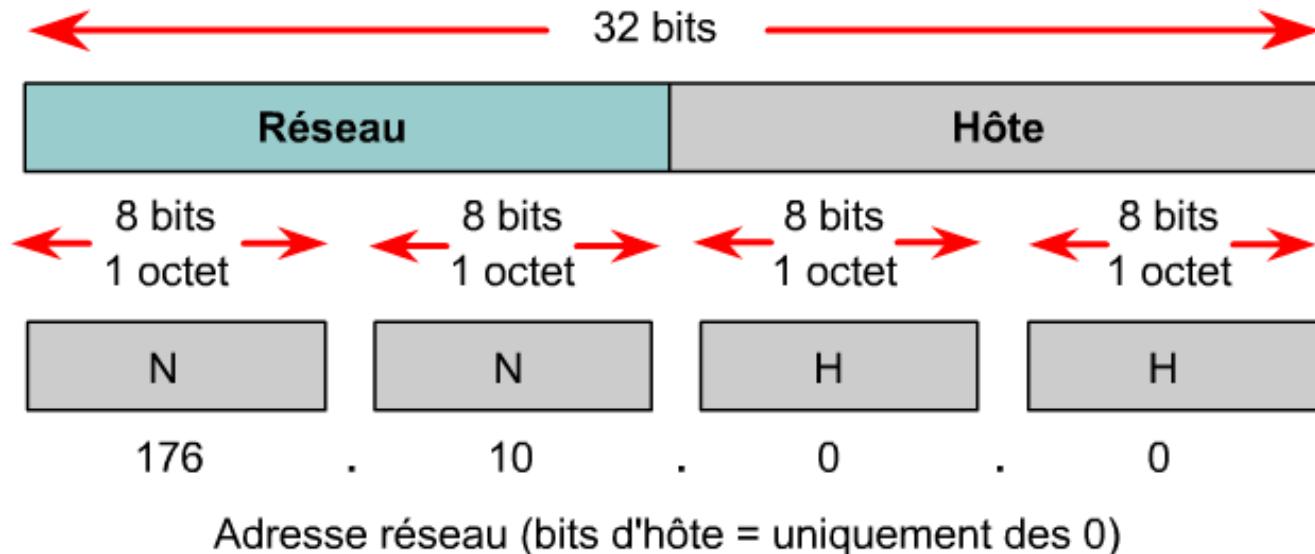
Fenêtre contextuelle (pop up)

La section identifiée par la zone supérieure représente l'adresse de broadcast 198.150.11.255. Les données envoyées à l'adresse de broadcast seront lues par un hôte du réseau, de 198.150.11.1 à 198.150.11.254. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son adresse de broadcast est 198.150.12.255.

Adresses réseau

FIGURES

1
2
3
4
5
6

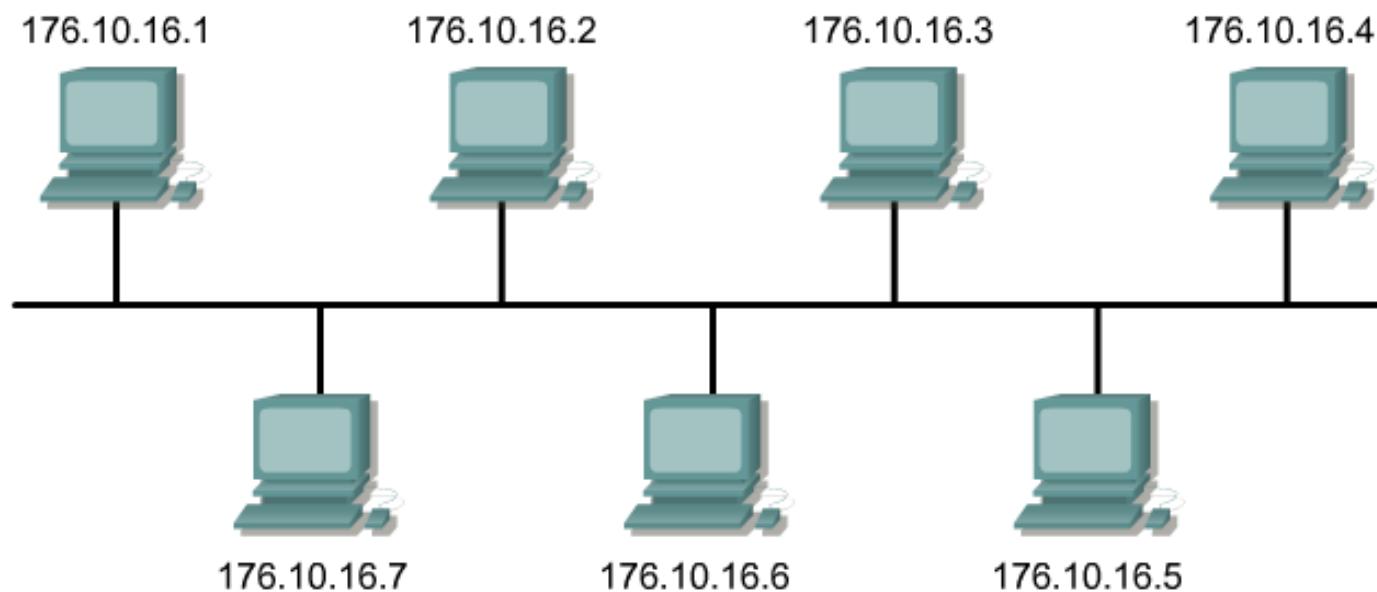


Cette adresse de classe B ne comporte que des bits définis sur 0.
C'est pourquoi elle est identifiée en tant qu'adresse réseau.

Transmission Unicast

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6



Transmission Unicast

FIGURES

1

2

3

4

5

6

176.

Fenêtre contextuelle (pop up)

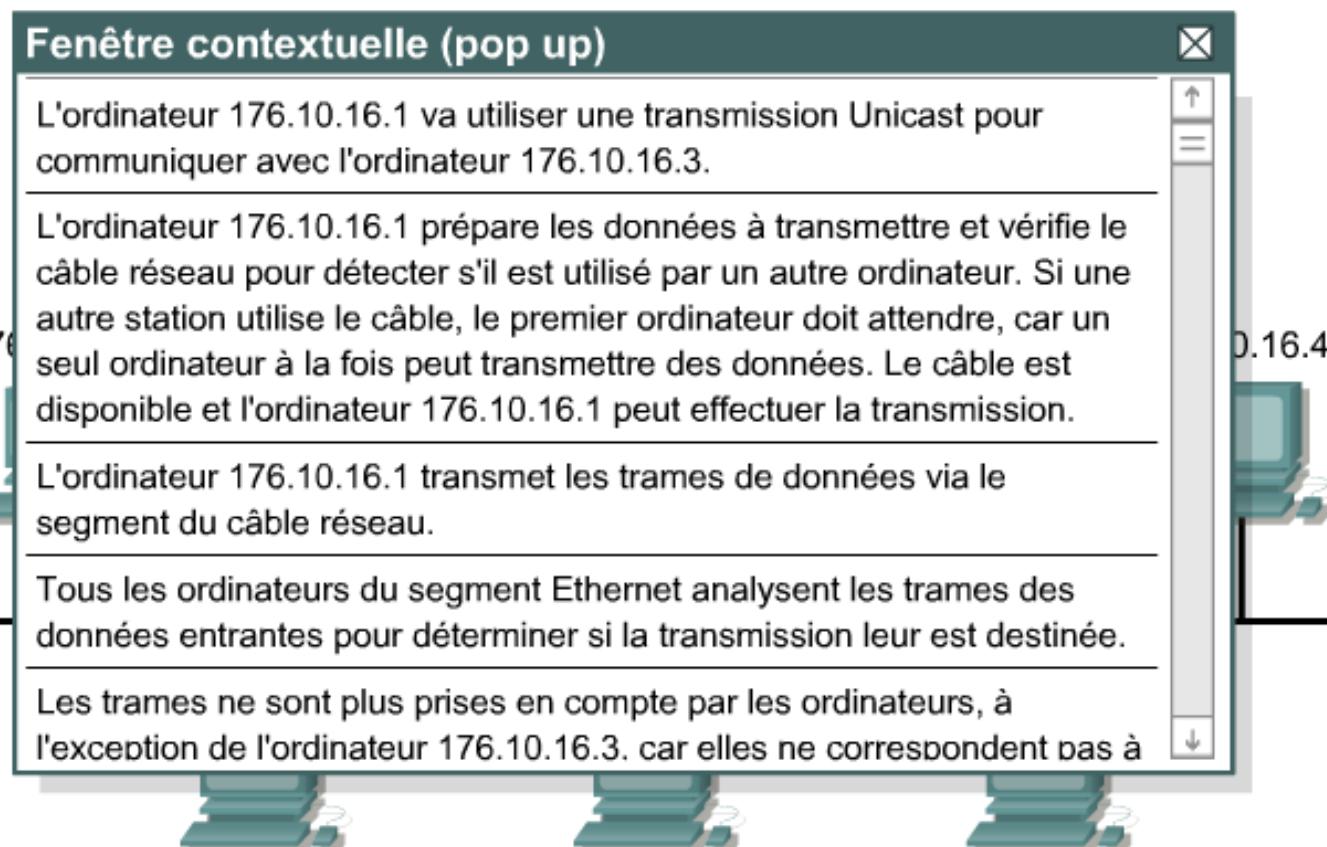
L'ordinateur 176.10.16.1 va utiliser une transmission Unicast pour communiquer avec l'ordinateur 176.10.16.3.

L'ordinateur 176.10.16.1 prépare les données à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Les trames ne sont plus prises en compte par les ordinateurs, à l'exception de l'ordinateur 176.10.16.3. car elles ne correspondent pas à



176.10.16.7

176.10.16.6

176.10.16.5

Transmission Unicast

FIGURES

1

2

3

4

5

6

Fenêtre contextuelle (pop up)

Les trames ne sont plus prises en compte par les ordinateurs, à l'exception de l'ordinateur 176.10.16.3, car elles ne correspondent pas à l'adresse MAC de destination des trames entrantes. C'est pourquoi cette transmission est appelée transmission Unicast. Seul l'ordinateur dont l'adresse correspond continue à traiter la trame, et chaque adresse IP étant unique, un seul ordinateur va accepter les données.

L'ordinateur 176.10.16.3 traite les données provenant des trames de données de l'ordinateur 176.10.16.1 et prépare une réponse pour l'ordinateur 176.10.16.1. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.

L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment envoient les trames.



Transmission Unicast

FIGURES

1

2

3

4

5

6

176.

Fenêtre contextuelle (pop up)

données de l'ordinateur 176.10.16.1 et prépare une réponse pour l'ordinateur 176.10.16.1. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.

L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment analysent les trames entrantes.

Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.



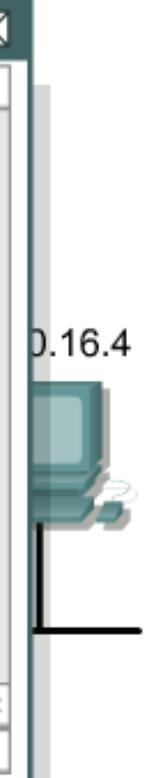
176.10.16.7



176.10.16.6



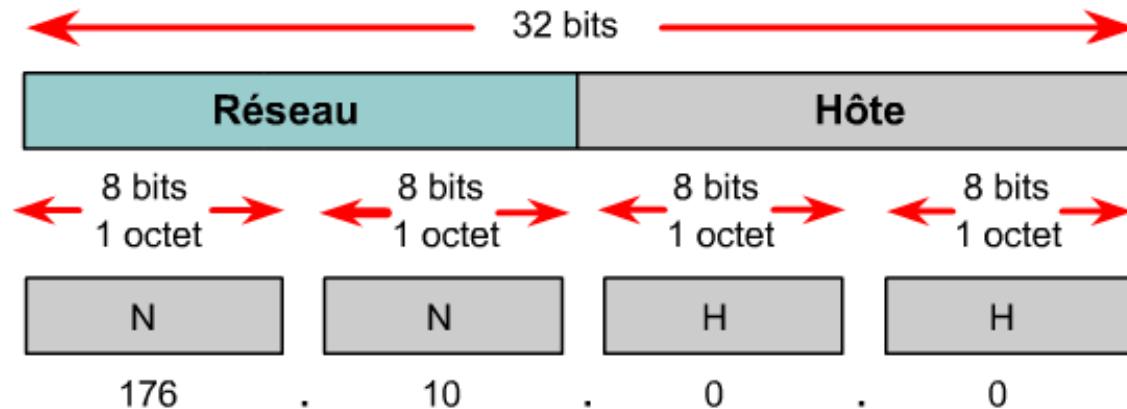
176.10.16.5



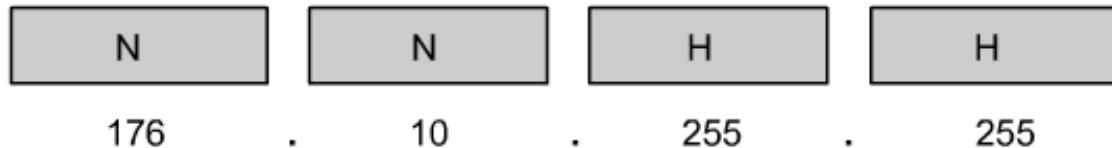
Adresse de broadcast

FIGURES

1
2
3
4
5
6



Adresse réseau (bits d'hôte = uniquement des 0)



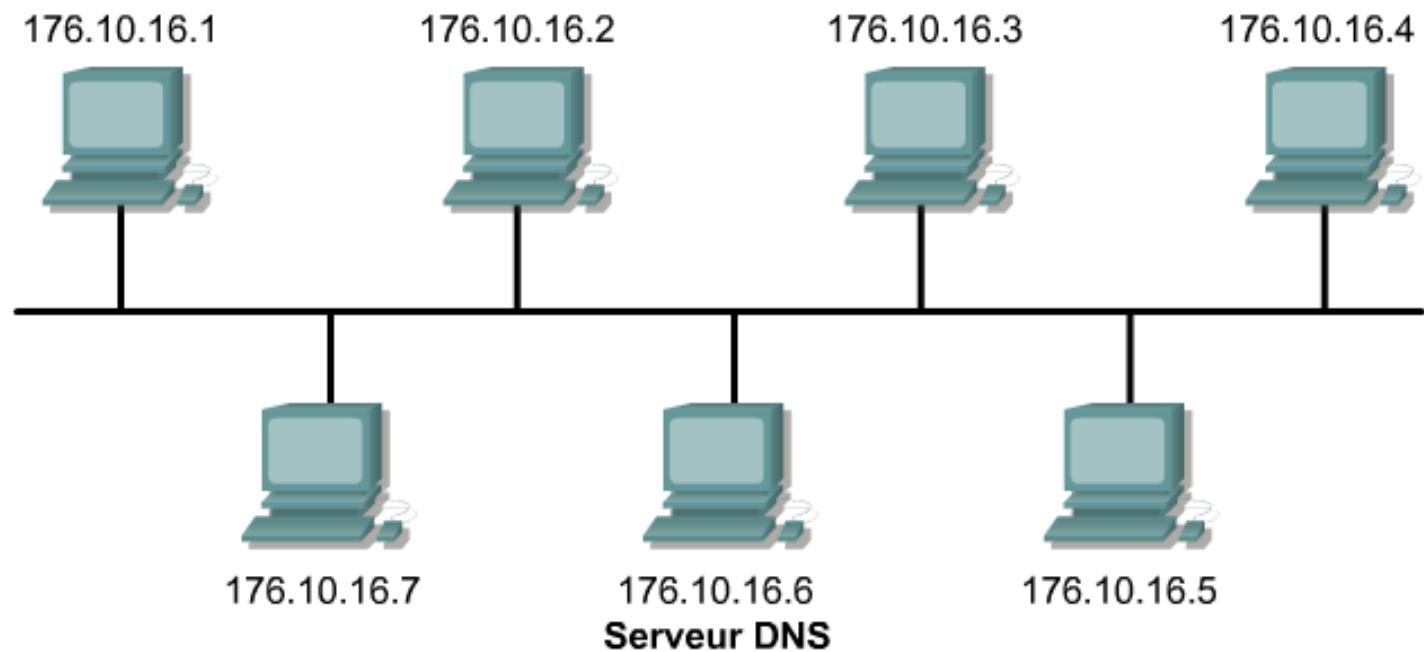
Adresse de broadcast (bits d'hôte = uniquement des 1)

Cette adresse de classe B est l'adresse de broadcast de ce réseau. Lorsque des paquets sont reçus avec cette adresse de destination, les données sont traitées par chaque ordinateur.

Transmission de broadcast

FIGURES

- 1
- 2
- 3
- 4
- 5
- 6



Transmission de broadcast

FIGURES

1

2

3

4

5

6

176

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 va utiliser une transmission de broadcast pour rechercher un serveur DNS. En général, un broadcast est utilisé pour localiser une unité ou un service spécifique. Il peut s'agir d'un serveur DNS, d'un serveur DHCP ou d'autres types d'unités.

L'ordinateur 176.10.16.1 prépare le paquet de broadcast à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des

176.10.16.7

176.10.16.6

176.10.16.5

Serveur DNS

Transmission de broadcast

FIGURES

1

2

3

4

5

6

176

Fenêtre contextuelle (pop up)

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Étant donné qu'il s'agit d'une transmission de broadcast, tous les ordinateurs acceptent la transmission et la traitent. La transmission de broadcast est utilisée afin que tous les hôtes du segment traitent les données. L'ordinateur qui procède au traitement décide également de la suite à donner à la transmission. Dans le cas présent, le broadcast recherchant un serveur DNS, seule cette unité va répondre. Si plusieurs serveurs DNS reçoivent ce broadcast, ils doivent tous répondre.

L'ordinateur 176.10.16.6 traite la requête provenant de la transmission de l'ordinateur 176.10.16.1 et prépare une réponse Unicast pour l'ordinateur 176.10.16.1. L'adresse de l'unité à l'origine de la requête étant connue, la réponse peut être envoyée directement à cette unité. Elle vérifie le câble Ethernet pour détecter si des données sont

176.10.16.7

176.10.16.6

176.10.16.5

Serveur DNS

Transmission de broadcast

FIGURES

1

2

3

4

5

6

176

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1. L'adresse de l'unité à l'origine de la requête étant connue, la réponse peut être envoyée directement à cette unité. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.

L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment analysent les trames entrantes.

Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.

176.10.16.7

176.10.16.6

176.10.16.5

Serveur DNS

Adresses uniques requises

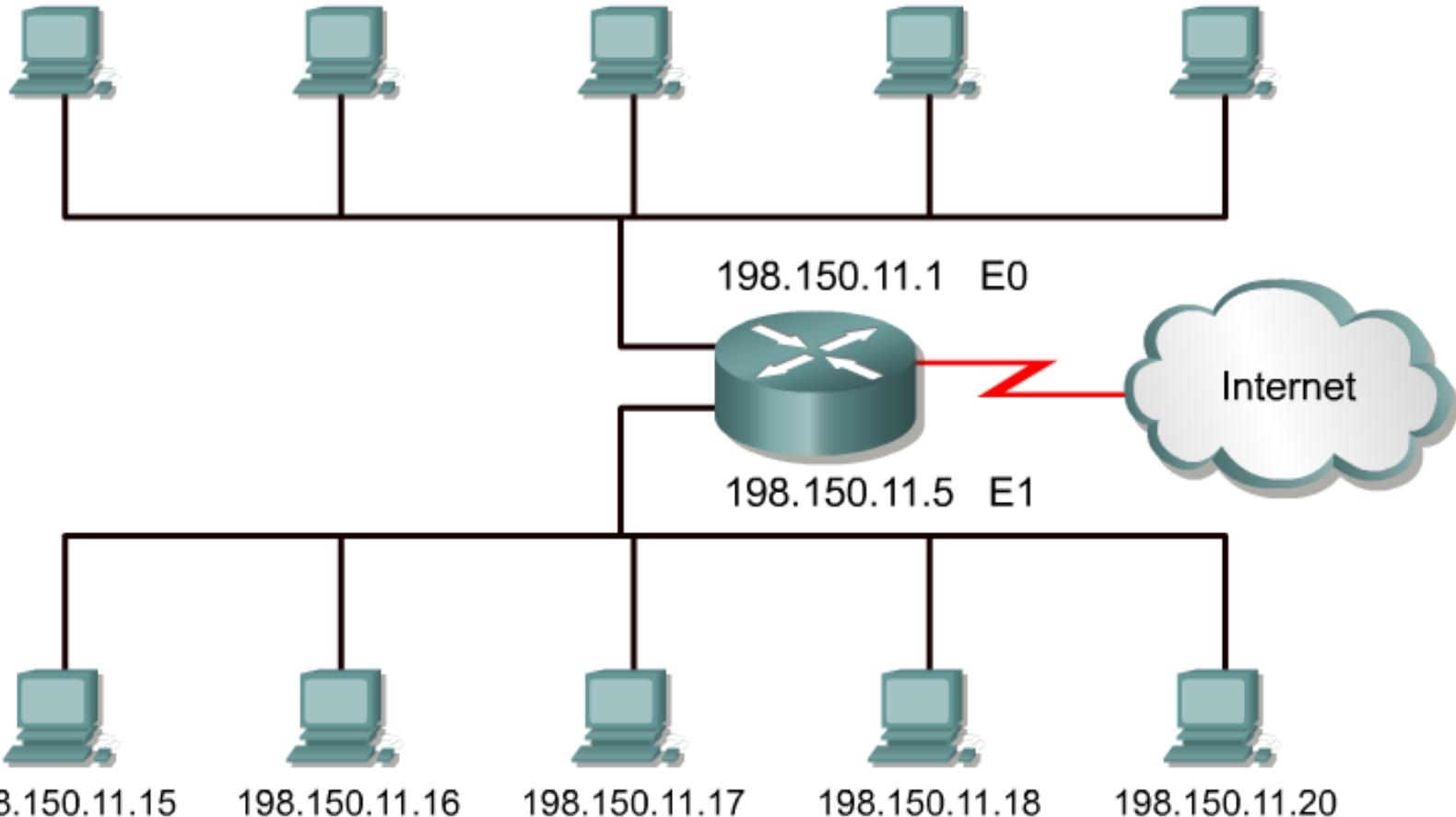
FIGURES

1

2

3

198.150.11.15 198.150.11.16 198.150.11.17 198.150.11.18 198.150.11.19



Adresses uniques requises

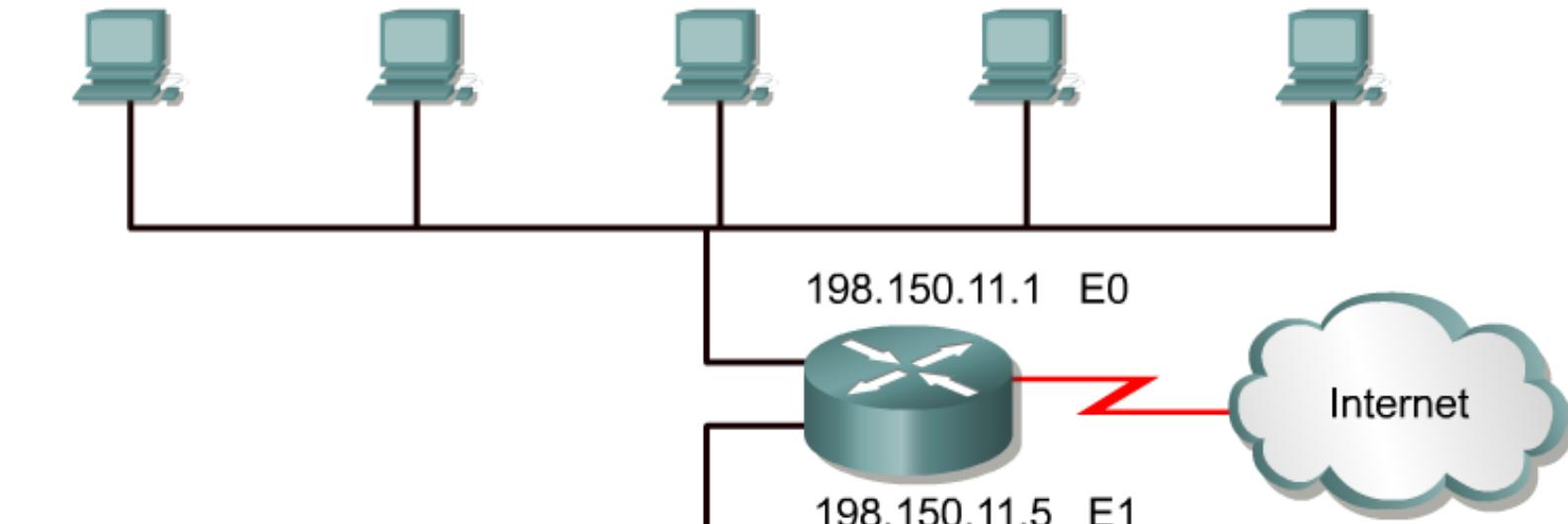
FIGURES

1

2

3

198.150.11.15 198.150.11.16 198.150.11.17 198.150.11.18 198.150.11.19



Fenêtre contextuelle (pop up)

Le modèle d'adressage réseau est incorrect. L'adresse réseau des deux réseaux est 198.150.11.0. Dans cet exemple, lorsque les transmissions de données atteignent le routeur, comment ce dernier doit-il les orienter ? Si cette action était autorisée, le trafic du réseau serait considérablement plus important et irait à l'encontre de la fonction de base du routeur. L'adresse de chaque unité d'un réseau doit être unique.

198.150.11.15

20

Adresses IP privées

FIGURES

1

2

3

Classe Plage d'adresses internes RFC 1918

A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

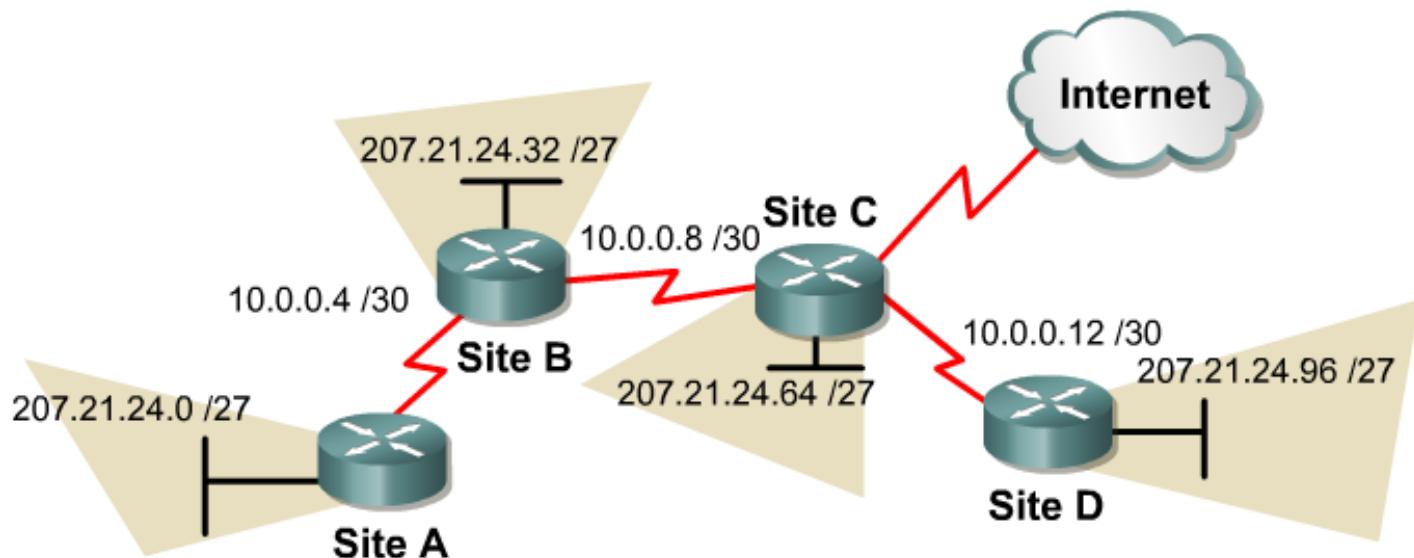
Utilisation des adresses privées dans le WAN

FIGURES

1

2

3



Les adresses privées peuvent être utilisées pour prendre en charge les liaisons série point-à-point sans gaspiller les adresses IP réelles.

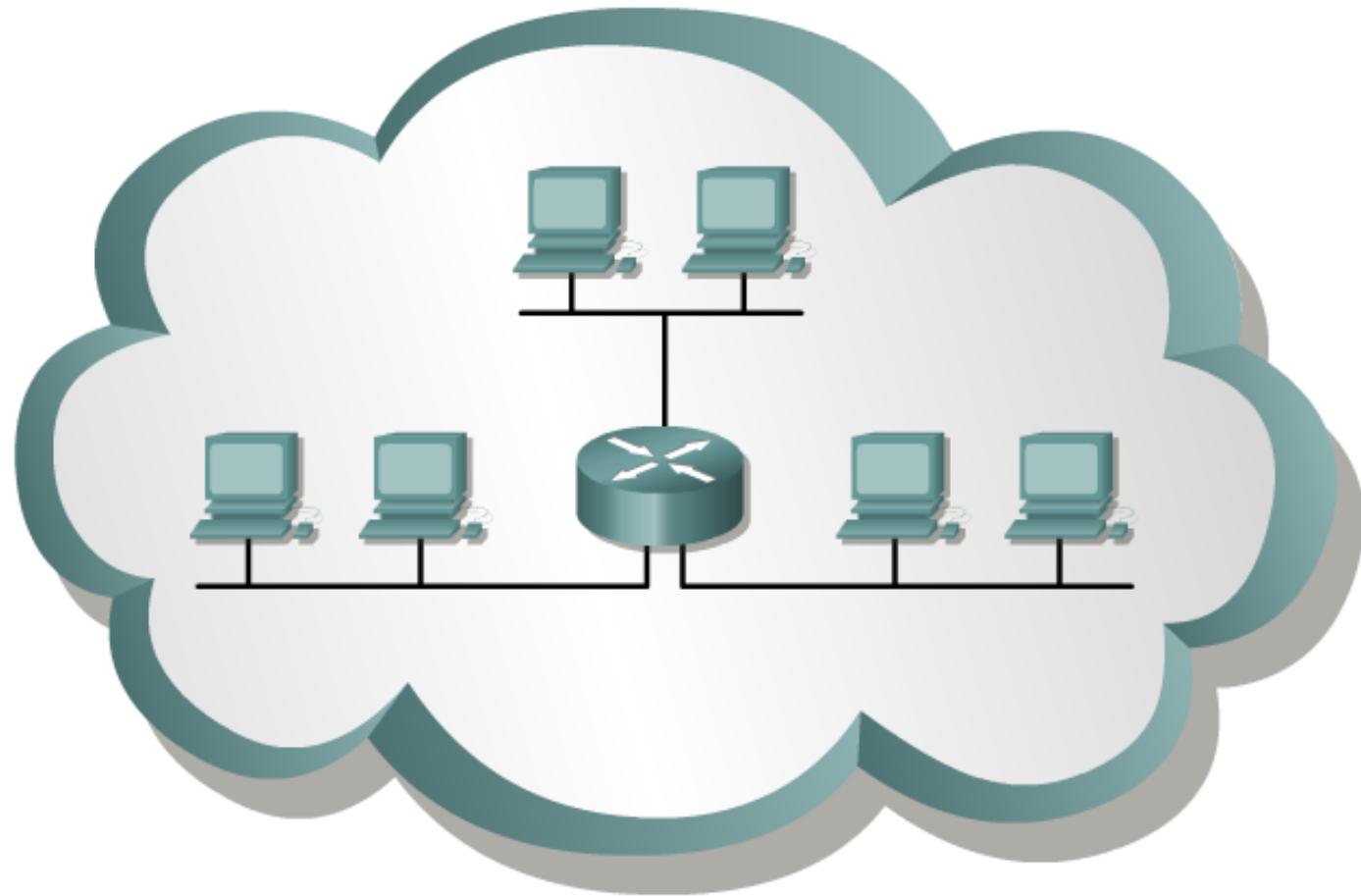
Adressage avec sous-réseaux

FIGURES

1

2

3



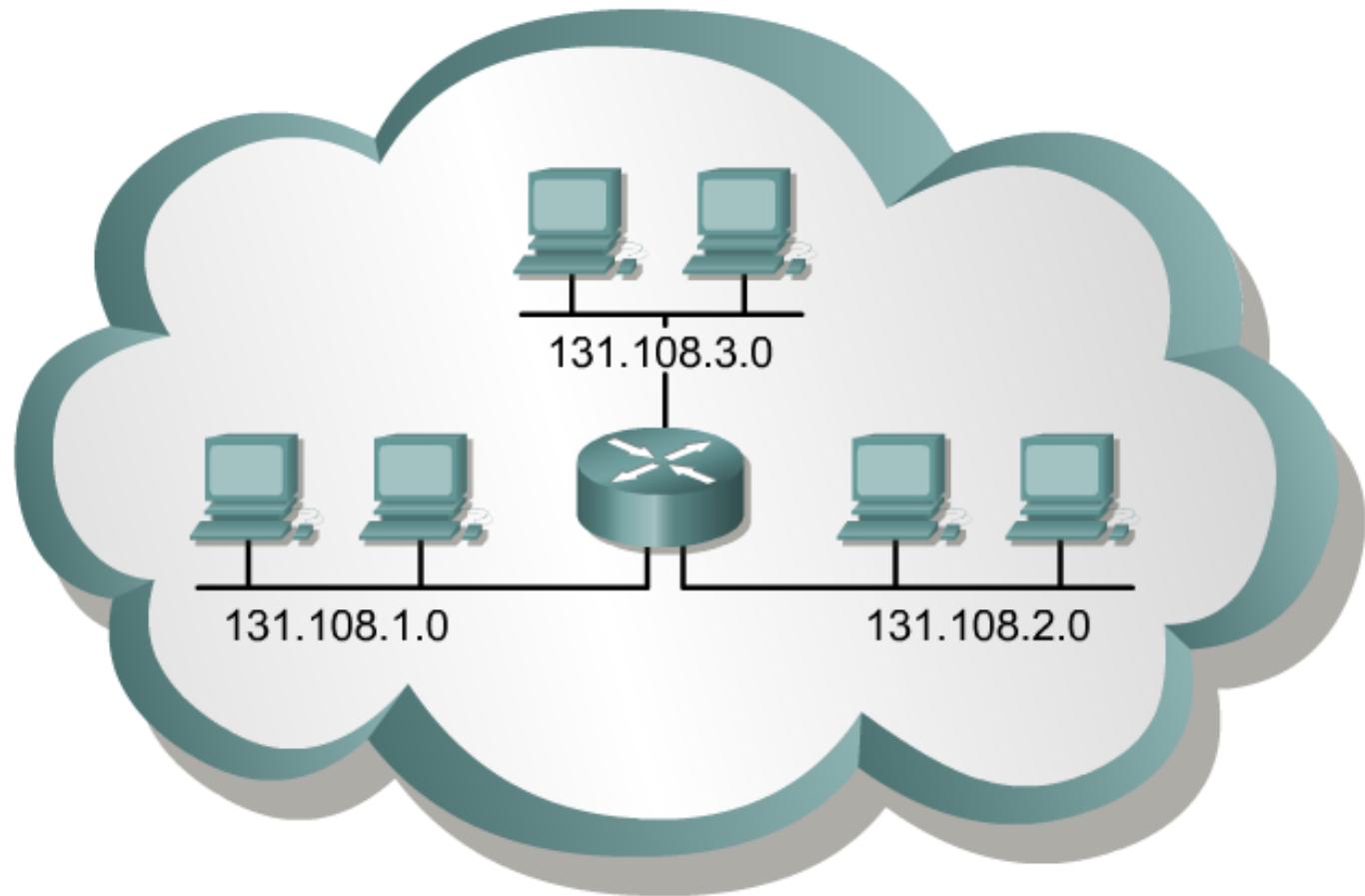
Adressage avec sous-réseaux

FIGURES

1

2

3



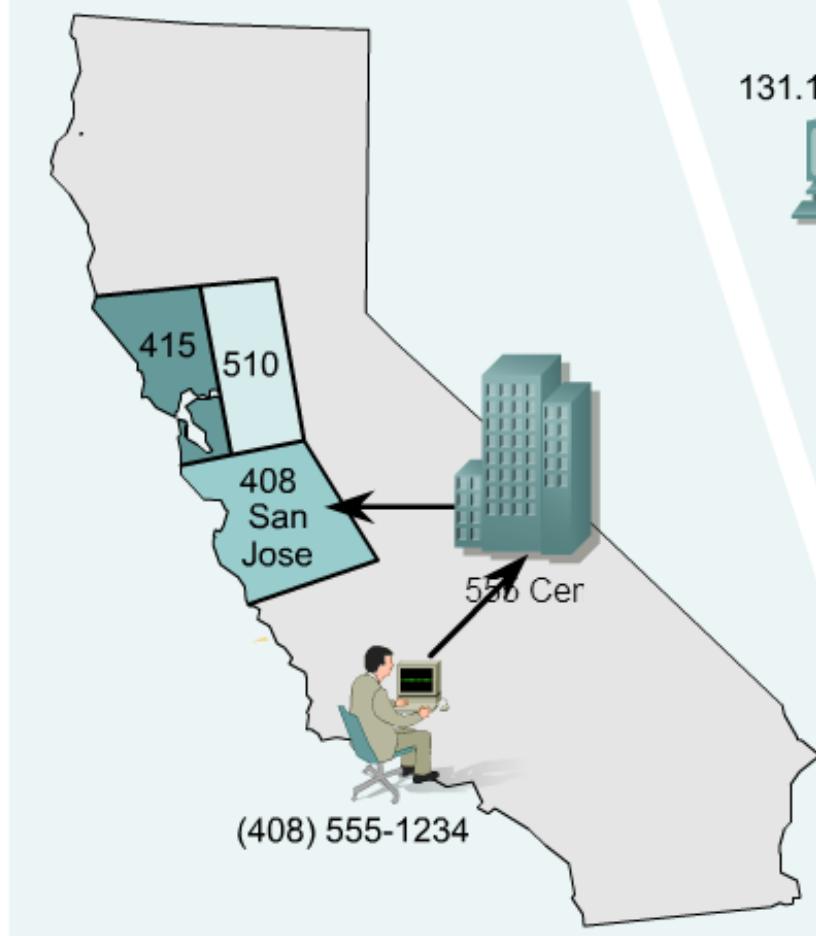
Adresses de sous-réseau

FIGURES

1

2

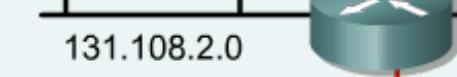
3



131.108.2.15



131.108.2.0



131.108.0.0



Table de référence des sous-réseaux

FIGURES

1

2

3

Nombre de bits emprunté au champ hôte pour créer des sous-réseaux	Nombre de sous-réseaux	Nombre d'hôtes de classe A par sous-réseau	Nombre d'hôtes de classe B par sous-réseau	Nombre d'hôtes de classe C par sous-réseau
2	2	4,194,302	16,382	62
3	6	2,097,150	8,190	30
4	14	1,048,574	4,094	14
5	30	524,286	2,046	6
6	62	262,142	1,022	2
7	126	131,070	510	-
8	254	65,534	254	-

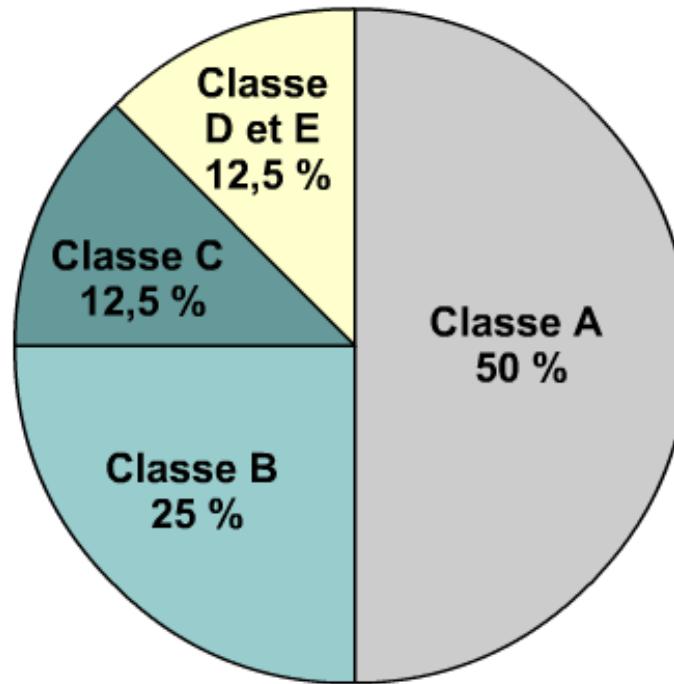
Attribution d'adresses IPv4

FIGURES

1

2

3



Les adresses de classe A et B étant pratiquement toutes utilisées, les adresses de classe C (12,5 % de l'espace total) peuvent être attribuées aux nouveaux réseaux.

IPv4 et IPv6

FIGURES

1

2

3

Version 4 du protocole IP (IPv4) 4 octets

11010001.11011100.11001001.01110001

209.156.201.113

4 294 467 295 adresses IP

Version 6 du protocole IP (IPv6) 16 octets

11010001.11011100.11001001.01110001.11010001.11011100

110011001.01110001.11010001.11011100.11001001

01110001.11010001.11011100.11001001.01110001

A524:72D3:2C80:DD02:0029:EC7A:002B:EA73

$3,4 \times 10^{38}$ adresses IP

Adresses IPv4 et IPv6

FIGURES

1

2

3

0 0 1 0 0 0 0 1 . 1 0 0 0 0 1 1 0 . 1 1 0 0 0 0 0 1 . 0 0 0 0 0 0 0 1 1

33

134

193

3

0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 : 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0

3ffe

1900

0 1 1 0 0 1 0 1 0 1 0 1 0 0 0 1 0 1 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1

6545

3

0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 : 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 1 0 0

230

f804

0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 : 0 0 0 1 0 0 1 0 1 1 1 0 0 0 0 1 0

7ebf

12c2

3ffe : 1900 : 6545 : 3 : 230 : f804 : 7ebf : 12c2

Adresses IPv4 et IPv6

FIGURES

1

2

3

0 0 1 0 0 0 0 1 . 1 0 0 0 0 1 1 0 . 1 1 0 0 0 0 0 1 . 0 0 0 0 0 0 1 1

33

134

193

3

0 0 1 1 1 1 1 1 1 1 1 1 1 1 0 : 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0

3ffe

1900

:

0 1 1 0 0 1 0 1 0 1 0 0 0 1 0 1 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1

6545

3

:

0 0 0 0 0 0 1 0 0 0 1 1 0 0 0 0 : 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 1 0 0

Fenêtre contextuelle (pop up)

0 1 1

Les adresses IPv4, qui sont les plus fréquentes, ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Toutefois, les adresses IPv6 ont une longueur de 128 bits et sont exprimées au format hexadécimal avec deux-points de séparation. Les deux-points séparent les champs de 16 bits. Les zéros de tête peuvent être omis dans chaque champ, comme dans l'exemple ci-dessus, où " 0003 " est écrit " 3 ".

0 1 0

Attribution d'adresses IP

FIGURES

1

2

Adresse IP source
Adresse ?



Adresse MAC
02-60-8C-01-02-03

Adresse IP source
Adresse ?



Adresse MAC
00-00-A2-05-09-89

Adresse IP source
Adresse ?



Adresse MAC
08-00-02-90-90-90

Serveur RARP
Adresse IP source
197.15.22.126



Adresse MAC
08-00-02-89-90-81

Adresse IP source
Adresse ?



Adresse MAC
02-08-BB-03-74-30

Adresse IP source
Adresse ?



Adresse MAC
02-00-A2-04-09-89

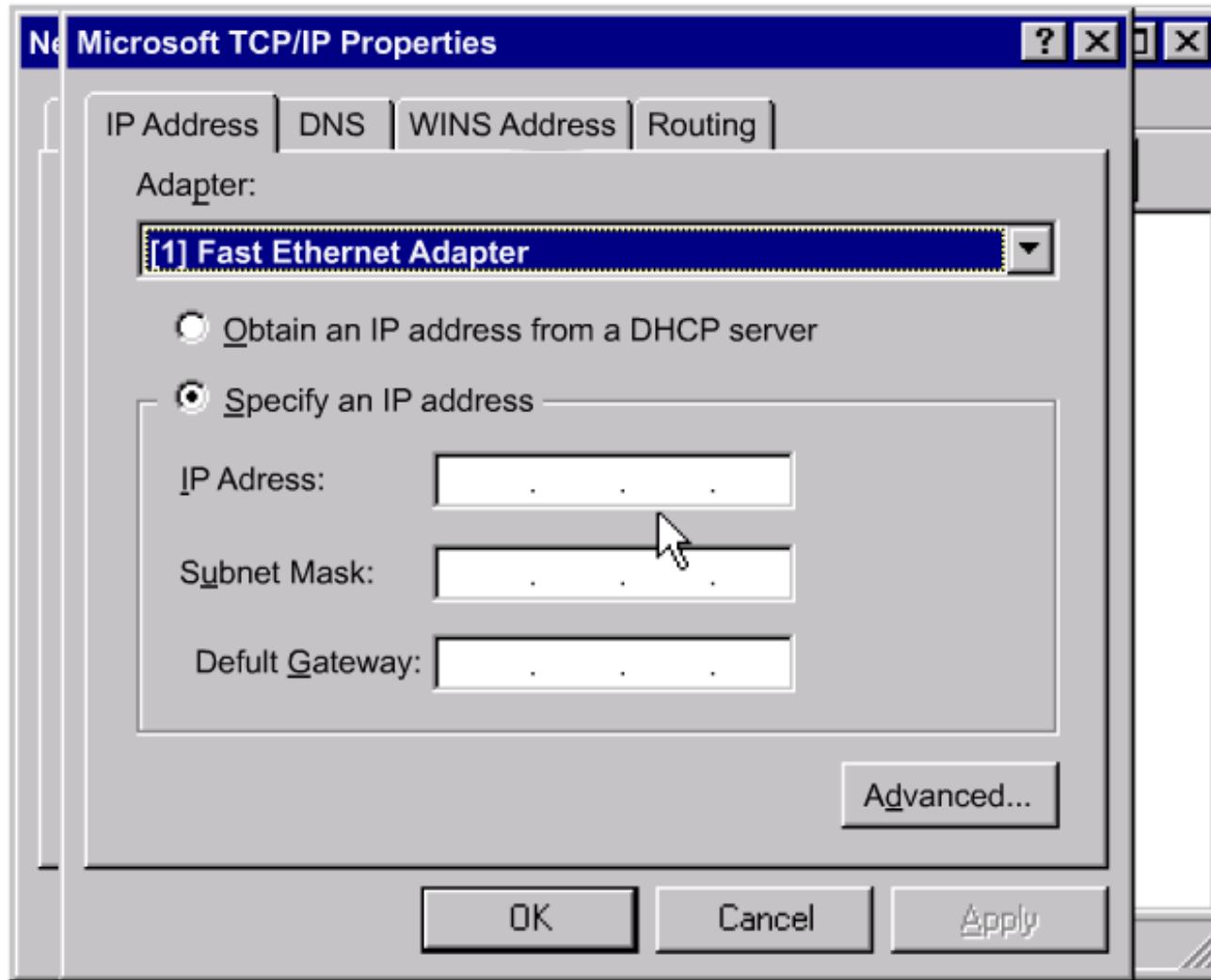
Les hôtes bénéficient d'une adresse physique car ils comportent une carte réseau qui permet d'accéder au média physique. Les adresses IP doivent être attribuées à l'hôte selon l'une des méthodes possibles. L'attribution des adresses IP peut être statique ou dynamique.

Configuration TCP/IP de Windows 98

FIGURES

1

2



Adresse IP

FIGURES

1

2

Academy Connection - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address Go

CISCO SYSTEMS

Contacts & Feedback | Site Help

ACADEMY CONNECTION Academy Connection Home GO

ACADEMY CONNECTION

Home

- Networking Academy +
- Global Learning Network +
- Workforce Development +
- Digital Divide +
- Newsroom +

Welcome to the Cisco Networking Academy Program web site. Our comprehensive, global e-learning program offers students an opportunity to pursue IT curricula through online instructor-led training and hands-on laboratory exercises. As a result, students can apply classroom learnings to actual technology challenges, which ultimately prepares tomorrow's workforce for life-long learning opportunities.

Cisco Networking Academy Program

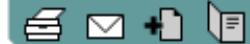
 [Networking Academy Program Overview](#)
The Cisco Networking Academy Program is a comprehensive program designed to teach students Internet technology skills.

 [Global Learning Network](#)
GLN is an AVVID-based comprehensive e-learning solution proven in the Academy Program.

Search GO

Search All Cisco.com

Toolkit: roll over tools below



Academy Users Login

Instructors: [CCNA](#) | [CCNP](#) | [New Curriculum](#)
[Forgot Username/Password?](#)
[Initial Registration](#)
[Get a Serial Number](#)
Students: [Student Login](#)
[Login help](#)
Alumni Connection

Academy Locator

[Find an Academy near you.](#)

International Related Sites

[Asia Pacific](#) | [Canada](#) | [EMEA](#)
[Japan](#) | [Latin America](#)

News and Events

Structure du message ARP/RARP

FIGURES

1

2

3

4

5

6

7

8

9

10

0 - 15 bits		16 - 31 bits
Type de matériel		Type de protocole
HLen (1 octet)	PLen (1 octet)	Opération
AM expéditeur (octets 1 - 4)		
AM expéditeur (octets 5 - 6)		AP expéditeur (octets 1 - 2)
AP expéditeur (octets 3 - 4)		AM cible (octets 1 - 2)
AM cible (octets 3 - 6)		
AP cible (octets 1 - 4)		
Structure de l'en-tête RARP		

Description des champs de la structure du message ARP/RARP

FIGURES

1

2

3

4

5

6

7

8

9

10

Champ	Description
Type de matériel	Spécifie un type d'interface matérielle pour lequel l'expéditeur attend une réponse.
Type de protocole	Spécifie le type d'adresse de protocole de haut niveau fourni par l'expéditeur.
HLen	Longueur de l'adresse matérielle.
PLen	Longueur de l'adresse de protocole.
Opération	Les valeurs sont les suivantes : 1 Requête ARP 2 Réponse ARP 3 Requête RARP 4 Réponse RARP 5 Requête RARP dynamique 6 Réponse RARP dynamique 7 Erreur RARP dynamique 8 Requête InARP 9 Réponse InARP
Adresse matérielle (AM) de l'expéditeur	Longueur en octets HLen.
Adresse de protocole (AP) de l'expéditeur	Longueur en octets PLen.
Adresse matérielle (AM) de la cible	Longueur en octets HLen.
Adresse de protocole (AP) de la cible	Longueur en octets PLen.

Processus RARP : segment de réseau

FIGURES

1

2

3 Station de travail
sans disque dur local

4

5

6

7

8

9

10

Station de travail
sans disque dur local

192.168.10.34

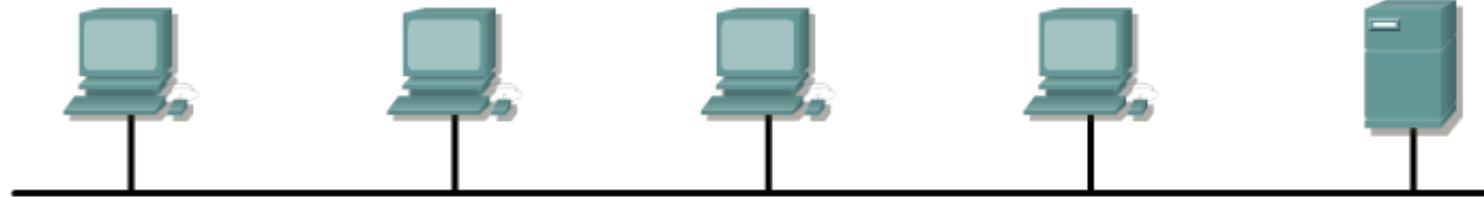
192.168.10.91

192.168.10.97

192.168.10.98

Serveur
RARP

FE:ED:F9:23:44:EF FE:ED:F9:44:45:66 DD:EC:BC:AB:04:AC DD:EC:BC:00:94:D4 FE:ED:F9:65:33:3A



L'ordinateur FE:ED:F9:23:44:EF doit obtenir son adresse IP pour utiliser un intranet.

Processus RARP : génération des requêtes

FIGURES

1

2

3

Station de travail
sans disque dur local

4

Station de travail
sans disque dur local

5

192.168.10.34

6

FE:ED:F9:44:45:66

192.168.10.91

7

DD:EC:BC:AB:04:AC

8

192.168.10.97

9

DD:EC:BC:00:94:D4

10

Serveur
RARP

192.168.10.98

FE:ED:F9:65:33:3A



En-tête de trame	1	0800 ₁₆
Adresse MAC source	06 04	3
FE:ED:F9:23:44:EF		FE:ED:F9:23:
Adresse MAC de destination	44:EF	non défini
FF:FF:FF:FF:FF:FF	non défini	FF:FF:
Champ Type		FF:FF:FF:FF
0X8035 (Ethernet)		non défini

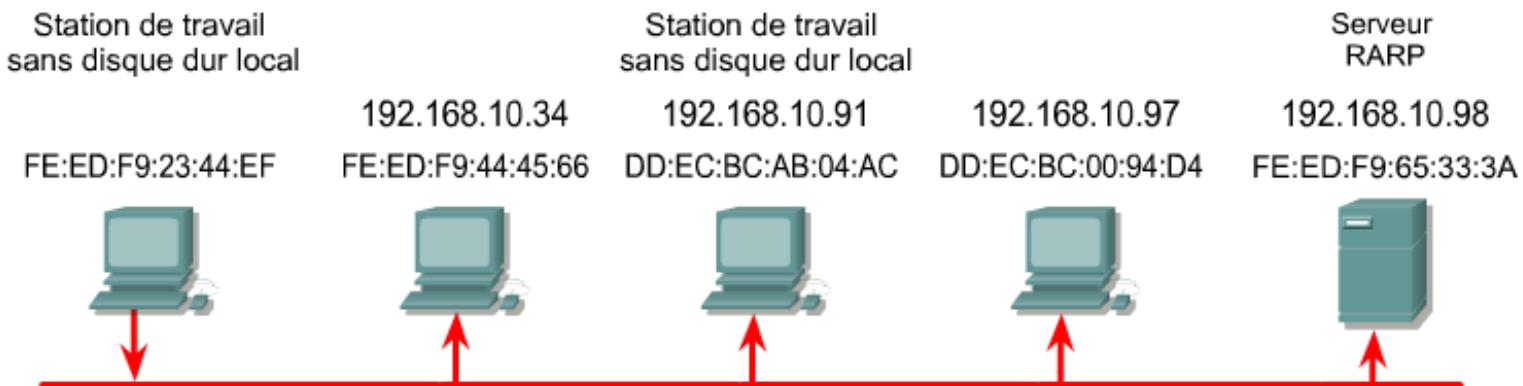
Fenêtre contextuelle (pop up)

L'ordinateur FE:ED:F9:23:44:EF génère une requête RARP.

Processus RARP : transmission des requêtes

FIGURES

1
2
3
4
5
6
7
8
9
10



En-tête de trame	1	0800 ₁₆
Adresse MAC source	06 04	3
FE:ED:F9:23:44:EF		FE:ED:F9:23:
Adresse MAC de destination	44:EF	non défini
FF:FF:FF:FF:FF:FF	non défini	FF:FF:
Champ Type		FF:FF:FF:FF
0X8035 (Ethernet)		non défini

Fenêtre contextuelle (pop up)

L'ordinateur FE:ED:F9:23:44:EF transmet une requête RARP.

Processus RARP : vérification des requêtes

FIGURES

1

2

3

Station de travail
sans disque dur local



Serveur
RARP

4

5

6

192.168.10.34
FE:ED:F9:23:44:EF

192.168.10.91
FE:ED:F9:44:45:66

192.168.10.97
DD:EC:BC:AB:04:AC

192.168.10.98
DD:EC:BC:00:94:D4

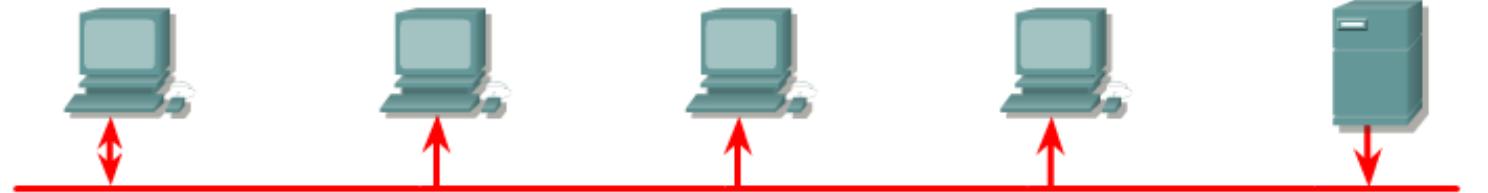
FE:ED:F9:65:33:3A

7

8

9

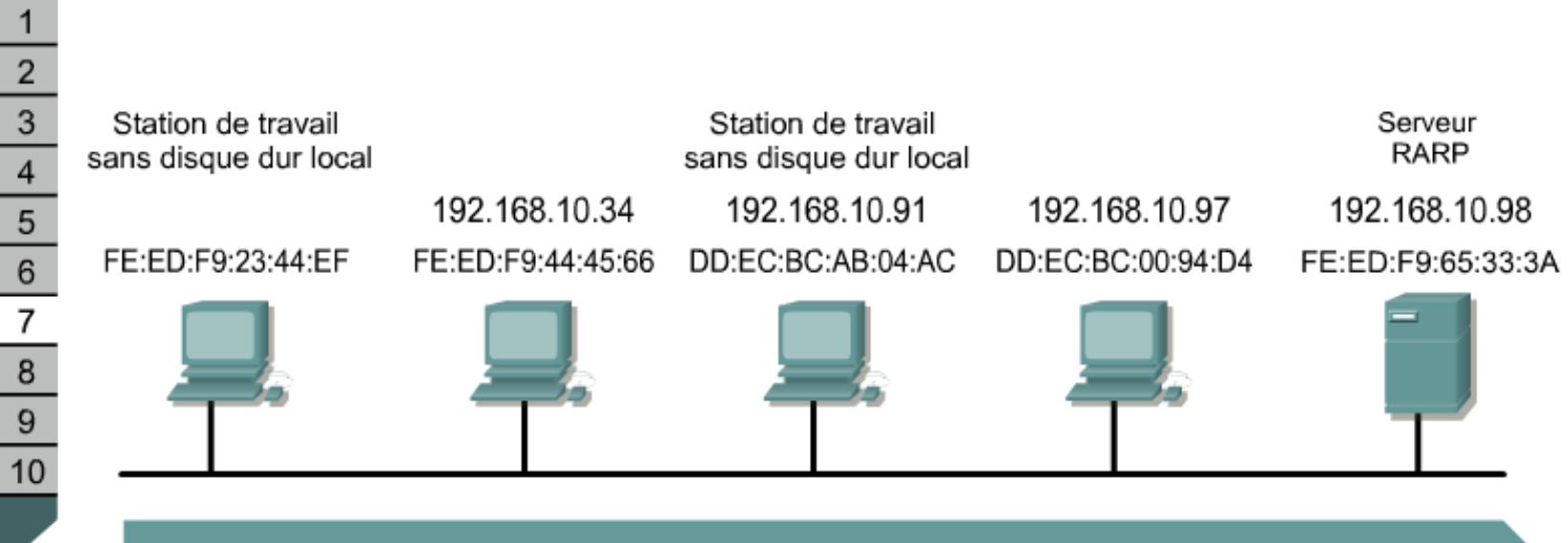
10



En-tête de trame	1		0800 ₁₆
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23:		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF:
Champ de demande RARP	Fenêtre contextuelle (pop up)		
0X803	Tous les ordinateurs transmettent le paquet à la couche réseau. Si les numéros IP ne correspondent pas, le paquet est supprimé, sauf sur le serveur RARP, qui détecte le champ de requête RARP.		

Processus RARP : génération des réponses

FIGURES



En-tête de trame	1	0800 ₁₆
Adresse MAC source	06 04	4
FE:ED:F9:65:33:3A		FE:ED:F9:23:
Adresse MAC de destination	44:EF	192.168.
FE:ED:F9:23:44:EF	10.36	FE:ED:
Champ Type	F9:65:33:3A	
0x8	Fenêtre contextuelle (pop up)	☒

Le serveur RARP crée un message de réponse RARP pour le client à l'origine de la demande.

Processus RARP : transmission des réponses

FIGURES

1

2

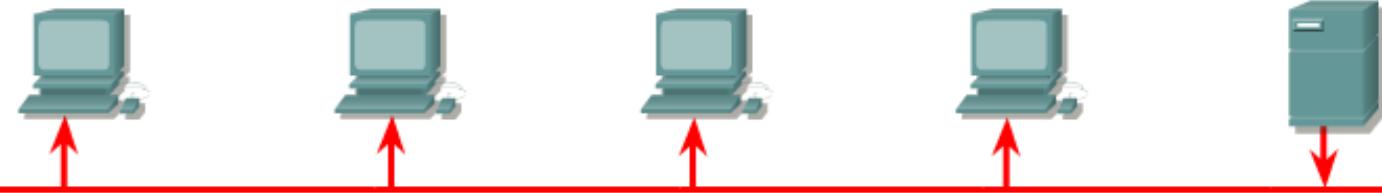
3

4

5

6

192.168.10.34 192.168.10.91 192.168.10.97 192.168.10.98
FE:ED:F9:23:44:EF FE:ED:F9:44:45:66 DD:EC:BC:AB:04:AC DD:EC:BC:00:94:D4 FE:ED:F9:65:33:3A



En-tête de trame	1	0800 ₁₆
Adresse MAC source	06 04	4
FE:ED:F9:65:33:3A		FE:ED:F9:23:
Adresse MAC de destination	44:EF	192.168.
FE:ED:F9:23:44:EF	10.36	FE:ED:
Champ Type		F9:65:33:3A
0X8035 (Ethernet)		192.168.10.98

Fenêtre contextuelle (pop up)

Tous les ordinateurs copient la trame et l'examinent.

Processus RARP : évaluation des réponses

FIGURES

1

2

3

4

5

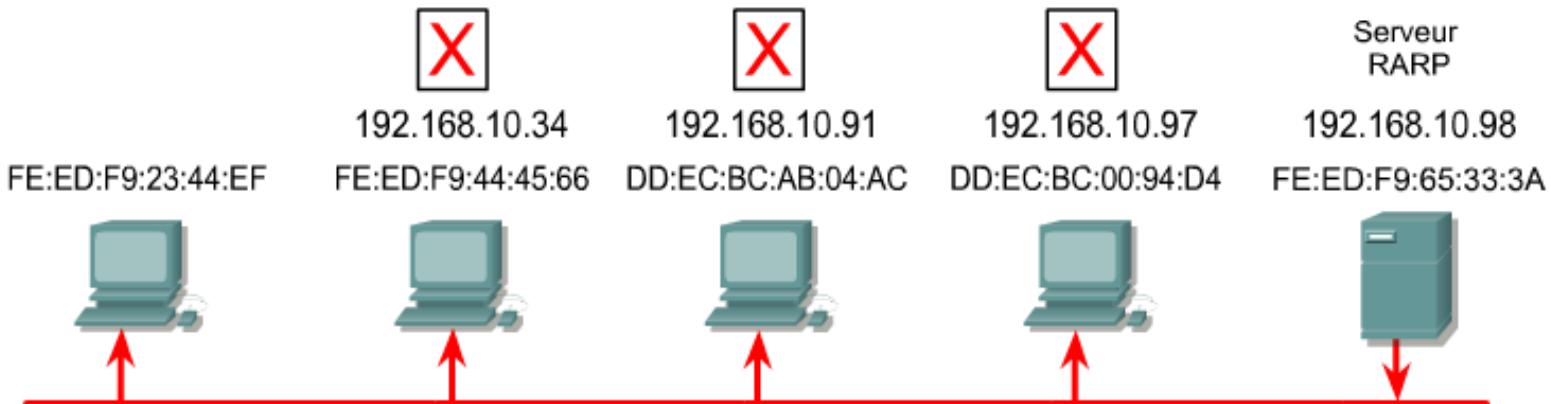
6

7

8

9

10



En-tête de trame	1	0800 ₁₆
Adresse MAC source	06	04
	FE:ED:F9:65:33:3A	FE:ED:F9:23:
Adresse MAC de destination	44:EF	192.168.
FE:ED:F9:23:44:EF	10.36	FE:ED:
Champ Type	F9:65:33:3A	
0X8035 (Ethernet)	192.168.10.98	

Fenêtre contextuelle (pop up)

Si les adresses MAC ne correspondent pas, le paquet est supprimé.

Processus RARP : stockage des données

FIGURES

1

2

3

Station de travail
sans disque dur local

4

192.168.10.36

FE:ED:F9:23:44:EF

5

192.168.10.34

FE:ED:F9:44:45:66

6

Station de travail
sans disque dur local

7

192.168.10.91

DD:EC:BC:AB:04:AC

8

192.168.10.97

DD:EC:BC:00:94:D4

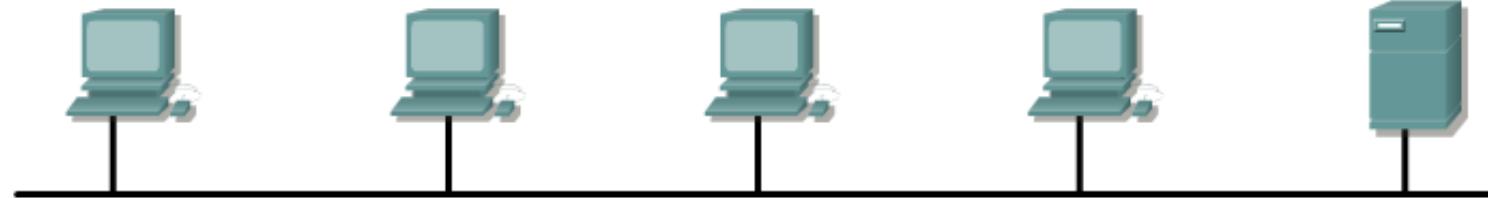
9

Serveur
RARP

192.168.10.98

FE:ED:F9:65:33:3A

10



L'ordinateur FE:ED:F9:23:44:EF conserve l'adresse IP reçue dans la réponse RARP pour l'utiliser ultérieurement.

Structure des messages BOOTP

FIGURES

1

2

3

4

5

6

7

8

9

10

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits		
Op (1)	Htype (1)	HLen (1)	Hops (1)		
Xid (4 octets)					
Secondes (2 octets)		Non utilisé			
Ciaddr (4 octets)					
Yiaddr (4 octets)					
Siaddr (4 octets)					
Giaddr (4 octets)					
Chaddr (16 octets)					
Nom d'hôte du serveur (64 octets)					
Nom du fichier de démarrage (128 octets)					
Zone spécifique du fournisseur (64 octets)					
Structure des messages BOOTP					

Description des champs de la structure du message BOOTP

FIGURES

1

2

3

4

5

6

7

8

9

10

Champ	Description
Op	Code de fonctionnement des messages. Les messages peuvent être de type BOOTREQUEST ou BOOTREPLY.
Htype	Type d'adresse matérielle
HLen	Longueur de l'adresse matérielle
Hops	Le client ajoute un zéro ; ce champ est utilisé par le serveur BOOTP pour envoyer des requêtes à un autre réseau.
Xid	ID de la transaction
Secs	Secondes écoulées depuis le début du processus de renouvellement ou de l'acquisition de l'adresse par le client.
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (client)
Siaddr	Adresse IP du serveur suivant à utiliser dans le bootstrap
Giaddr	Adresse IP de l'agent de relais utilisée pour l'amorçage via un agent de relais
Chaddr	Adresse matérielle du client
Server Host Name	Spécifie le serveur qui doit fournir les informations BOOTP.
Boot File Name	Permet d'utiliser plusieurs fichiers de démarrage ; les hôtes peuvent alors exécuter différents systèmes d'exploitation

Description des champs de la structure du message BOOTP

FIGURES

1

2

3

Champ	Description	
Boot File Name	Permet d'utiliser plusieurs fichiers de démarrage ; les hôtes peuvent alors exécuter différents systèmes d'exploitation.	 
Vendor Specific Area	Contient des informations facultatives propres au fournisseur qui peuvent être transmises à l'hôte.	 

Protocole BOOTP : segment de réseau

FIGURES

1

2

Station de travail sans disque dur local

3

4

FE:ED:F9:23:44:EF 192.168.10.34 FE:ED:F9:44:45:66

5

6



7

8

9

10

Station de travail sans disque dur local

DD:EC:BC:AB:04:AC 192.168.10.91

Serveur TFTP

DD:EC:BC:00:94:D4 192.168.10.97

Serveur

192.168.10.98 FE:ED:F9:65:33:3A



Internet

198.1.10.2



192.168.10.1
FE:ED:F9:FA:33:AA

L'ordinateur FE:ED:F9:23:44:EF doit obtenir son adresse IP pour les opérations effectuées sur l'intranet et Internet.

Protocole BOOTP : création d'une requête

FIGURES

1
2
3
4
5
6
7
8
9
10

Station de travail sans disque dur local

Station de travail sans disque dur local

Serveur TFTP

Serveur

Internet

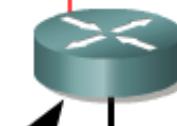
FE:ED:F9:23:44:EF

192.168.10.34
FE:ED:F9:44:45:66

192.168.10.91
DD:EC:BC:AB:04:AC

192.168.10.97
DD:EC:BC:00:94:D4

192.168.10.98
FE:ED:F9:65:33:3A



198.1.10.2

198.1.10.2

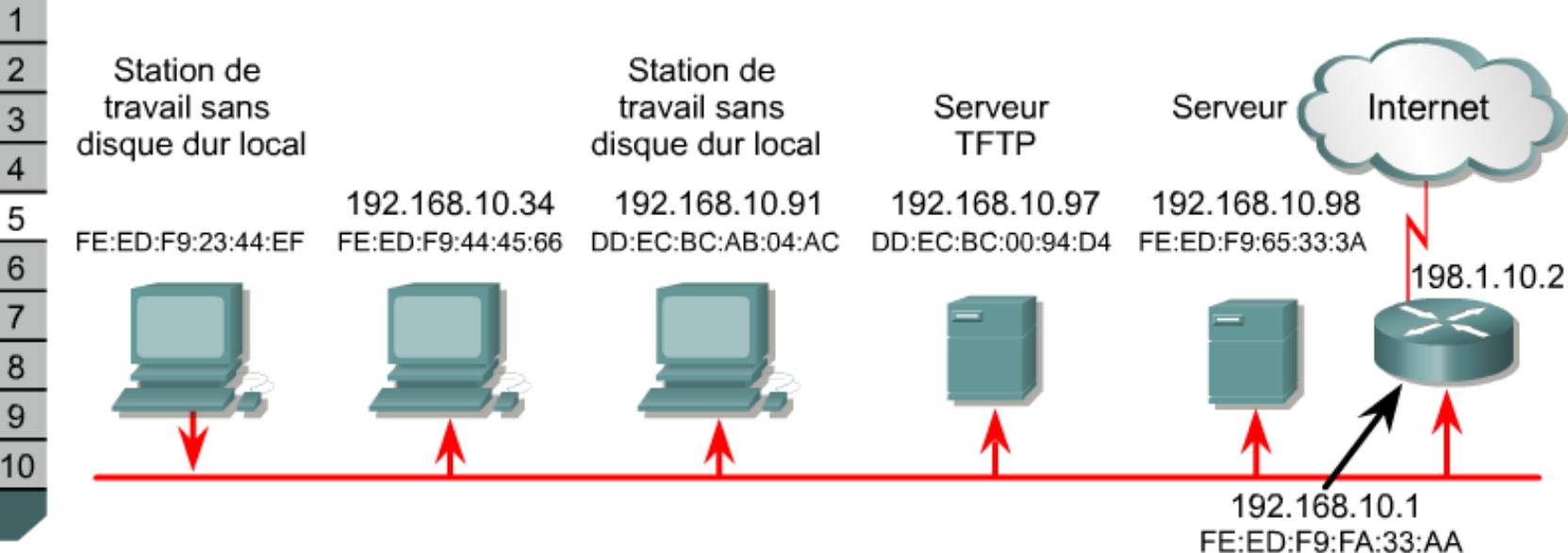
Fenêtre contextuelle (pop up)

L'ordinateur FE:ED:F9:23:44:EF génère une requête BOOTP.

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source		221			du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination		0			
FF:FF:FF:FF:FF:FF	225.225.225.225		0			
Champ Type			0			
0X8035 (Ethernet)			0			
		FE:ED:F9:23:44:EF				

Transmission d'une requête BOOTP

FIGURES



En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source		221			du CRC
FE:ED: Adress FF:FF: Champ 0X803	Fenêtre contextuelle (pop up)					
	La station de travail FE:ED:F9:23:44:EF encapsule la requête dans l'en-tête d'un paquet. L'en-tête contient une adresse IP source inconnue et une adresse IP de destination de broadcast. Pour l'en-tête de la trame, la station de travail utilise son adresse MAC en tant que source et un broadcast pour la destination car elle ne connaît pas l'adresse du serveur BOOTP. La station de travail transmet alors une trame de requête BOOTP.					

Protocole BOOTP : vérification des requêtes

FIGURES

1
2
3
4
5
6
7
8
9
10

Station de travail sans disque dur local



FE:ED:F9:23:44:EF 192.168.10.34 FE:ED:F9:44:45:66

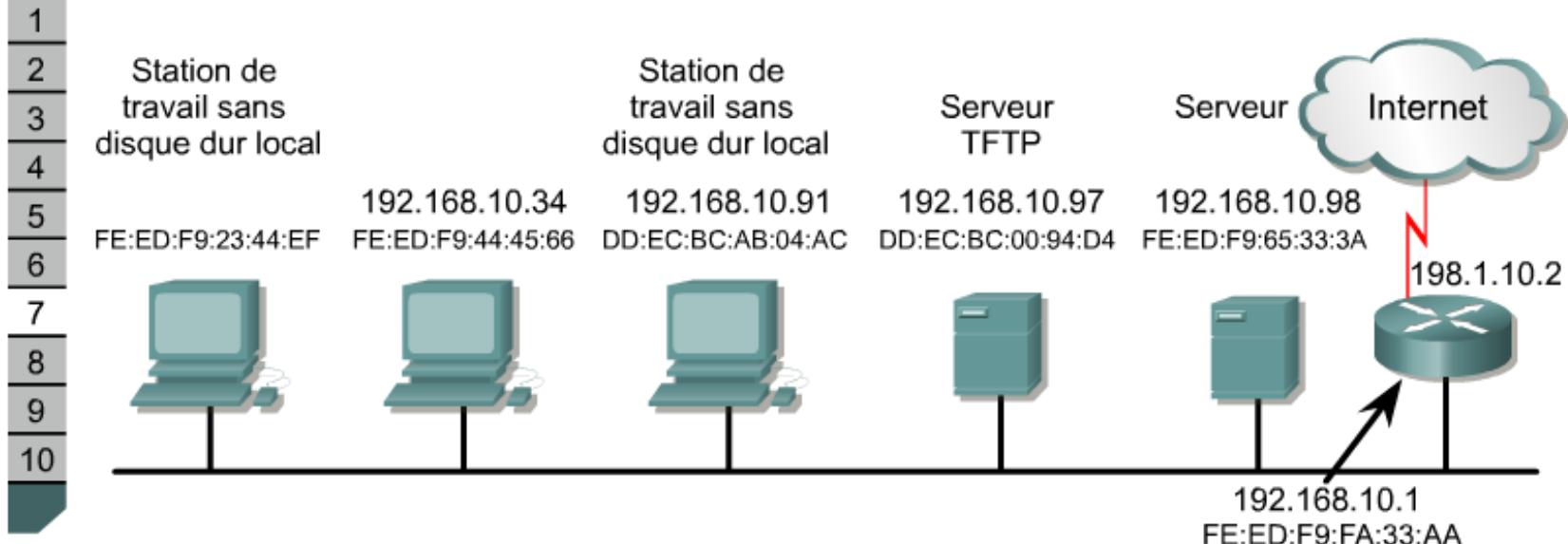
192.168.10.91

192.168.10.97 DD:EC:BC:AB:04:AC

192.168.10.98 FE:ED:F9:65:33:3A

Création d'une réponse

FIGURES



Fenêtre contextuelle (pop up)

À partir de sa base de données, le serveur prépare une réponse BOOTP destinée à l'unité qui est à l'origine de la demande. Cette réponse inclut l'adresse IP du client, l'adresse du serveur TFTP et l'adresse de la passerelle par défaut (les autres champs sont omis pour cet exemple). Dans l'en-tête de la trame, les adresses source et de destination sont inversées. Dans l'en-tête du paquet, le serveur BOOTP place son adresse IP dans le champ source et une adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse BOOTP au niveau de la couche transport en vue de son traitement. Seul un broadcast sera acheminé puisque le client ne connaît pas son adresse IP.



Édition
Vérification
CRC

Protocole BOOTP : transmission des réponses

FIGURES

1
2
3
4
5
6
7
8
9
10

Station de travail sans disque dur local

Station de travail sans disque dur local

Serveur TFTP

Serveur

Internet

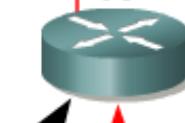
192.168.10.34
FE:ED:F9:23:44:EF

192.168.10.91
FE:ED:F9:44:45:66

192.168.10.97
DD:EC:BC:AB:04:AC

192.168.10.98
DD:EC:BC:00:94:D4

198.1.10.2



Fenêtre contextuelle (pop up)

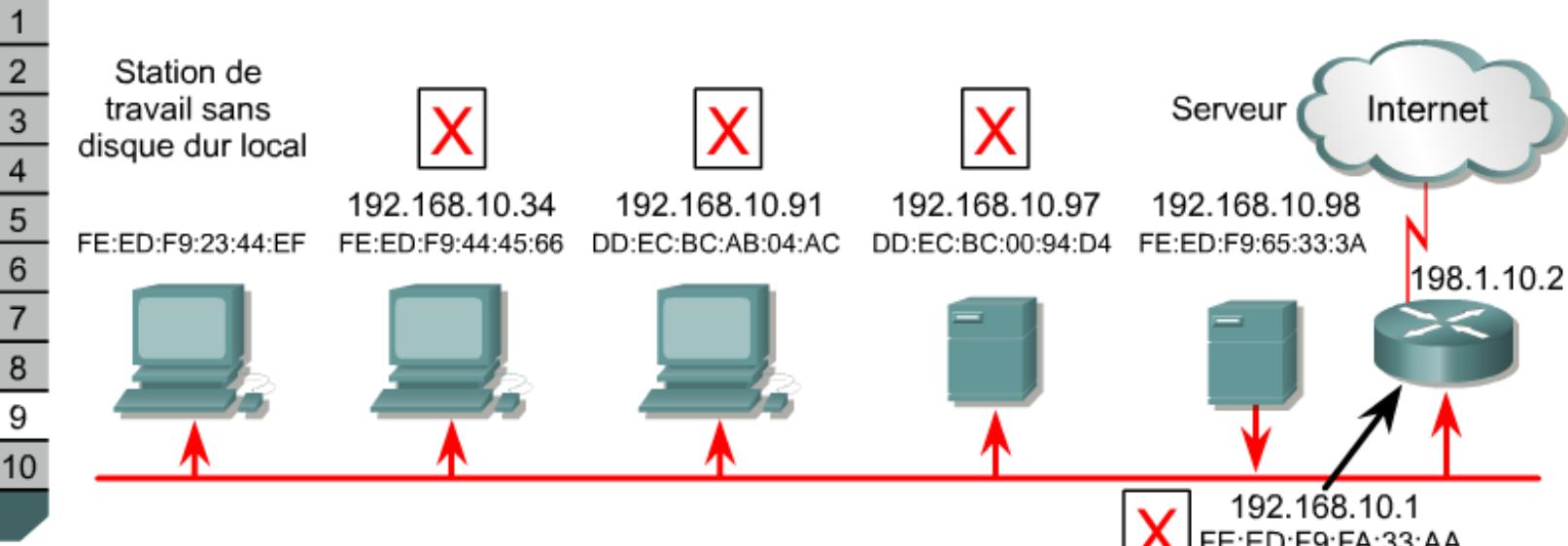
Le serveur BOOTP renvoie alors la trame de la réponse BOOTP à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.

192.168.10.1
FE:ED:F9:FA:33:AA

En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source		221			du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination		0			
FE:ED:F9:23:44:EF	225.225.225.225		192.168.10.36			
Champ Type			192.168.10.97			
0X8035 (Ethernet)			192.168.10.97			
			FE:ED:F9:23:44:EF			

Protocole BOOTP : réponse vérifiée

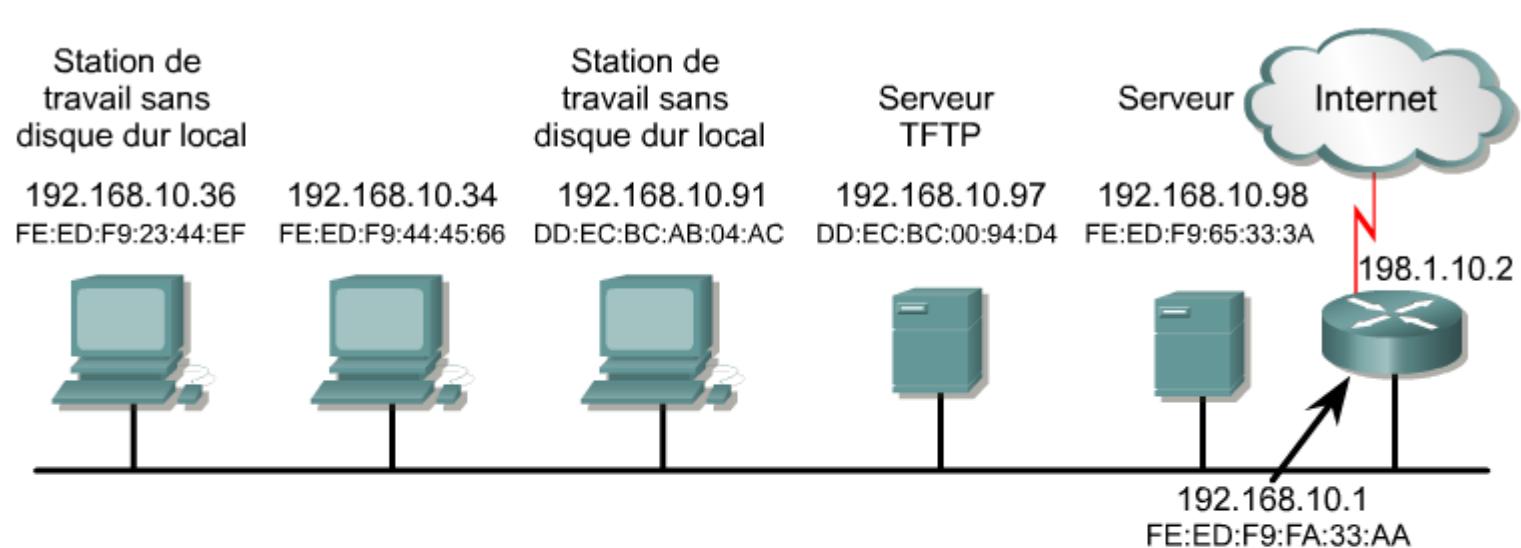
FIGURES



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source		221			du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse	Fenêtre contextuelle (pop up)					
FE:ED:F9:65:33:3A	L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur BOOTP sont alors stockées dans la table ARP de la station de travail sans disque dur local. L'en-tête de la trame est retiré et ignoré.					
Champ T						
0X8035 (

Protocole BOOTP : stockage des données

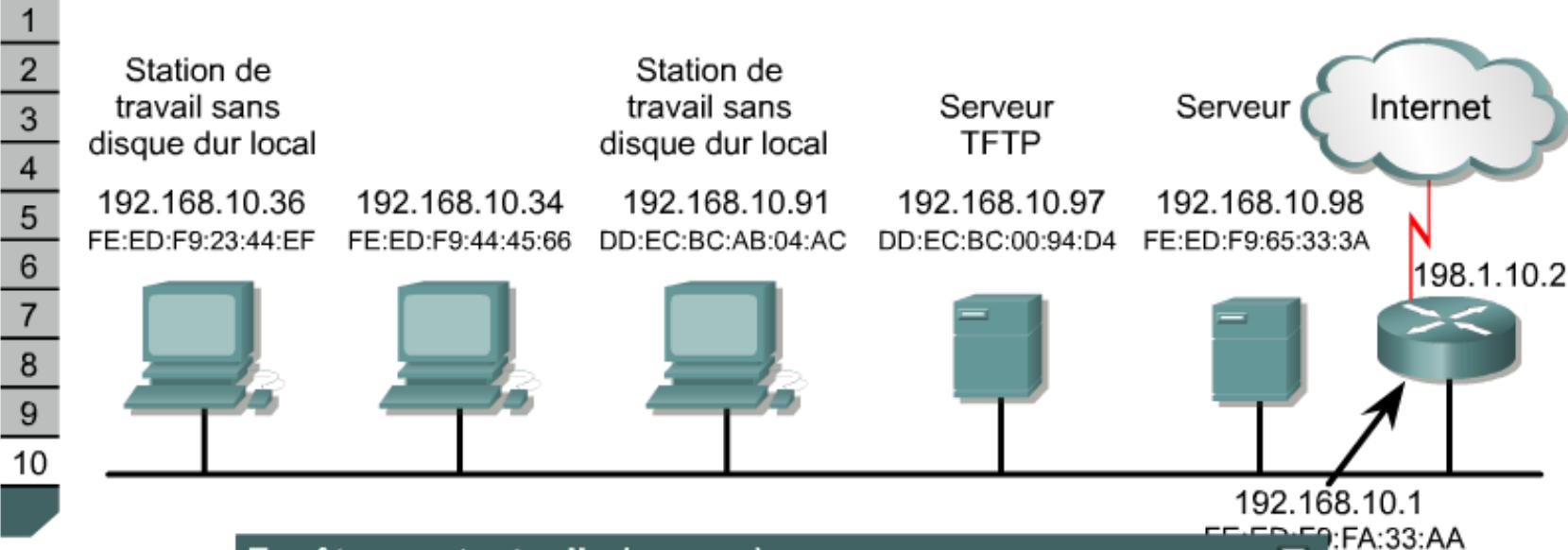
FIGURES



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source		221			du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination		0			
FE:ED:F9:23:44:EF	225.225.225.225		192.168.10.36			
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Protocole BOOTP : stockage des données

FIGURES



Fenêtre contextuelle (pop up)

L'adresse IP de destination du paquet étant un broadcast, l'en-tête du paquet est retiré et les données de la réponse BOOTP sont transmises à la couche transport, dans laquelle les données du champ OP indiquent qu'il s'agit d'une réponse BOOTP. Les données de la réponse sont stockées dans les emplacements de mémoire appropriés de la station de travail. La station de travail a maintenant accès au serveur TFTP, pour télécharger d'autres systèmes d'exploitation, et à la passerelle par défaut. Elle dispose également de sa propre adresse IP. Elle peut donc être utilisée avec le réseau et Internet.

Vérification du CRC

En-tête		
Adresse		
FE:ED:		
Adresse		
FE:ED:		
Champ		
0X8035 (Ethernet)	192.168.10.97	
		FE:ED:F9:23:44:EF

Structure des messages DHCP

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits		
Op (1)	Htype (1)	HLen (1)	Hops (1)		
Xid (4 octets)					
Secondes (2 octets)		Indicateurs (2 octets)			
Ciaddr (4 octets)					
Yiaddr (4 octets)					
Siaddr (4 octets)					
Giaddr (4 octets)					
Chaddr (16 octets)					
Nom d'hôte du serveur (64 octets)					
Nom du fichier de démarrage (128 octets)					
Zone spécifique du fournisseur (variable)					
Structure des messages DHCP					

Description des champs de la structure du message DHCP

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

Op	Les messages des codes de fonctionnement des messages peuvent être de type BOOTREQUEST ou BOOTREPLY.
Htype	Type d'adresse matérielle
Hlen	Longueur de l'adresse matérielle
Hops	Le client ajoute un zéro ; ce champ est utilisé par le serveur BOOTP pour envoyer des requêtes à un autre réseau.
Xid	ID de la transaction
Secs	Secondes écoulées depuis le début du processus de renouvellement ou de l'acquisition de l'adresse par le client.
Indicateurs	Indicateurs
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (client)
Siaddr	Adresse IP du serveur suivant à utiliser dans le bootstrap
Giaddr	Adresse IP de l'agent de relais utilisée pour l'amorçage via un proxy
Chaddr	Adresse matérielle du client
Server Host Name	Spécifie le serveur qui doit fournir les informations BOOTP.

Description des champs de la structure du message DHCP

FIGURES

1

2

3

17

Server Host Name	Spécifie le serveur qui doit fournir les informations BOOTP.
Boot File Name	Permet d'utiliser plusieurs fichiers de démarrage ; les hôtes peuvent alors exécuter différents systèmes d'exploitation.
Vendor Specific Area	Contient des informations facultatives propres au fournisseur qui peuvent être transmises à l'hôte.

Protocole DHCP : amorçage de l'hôte

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

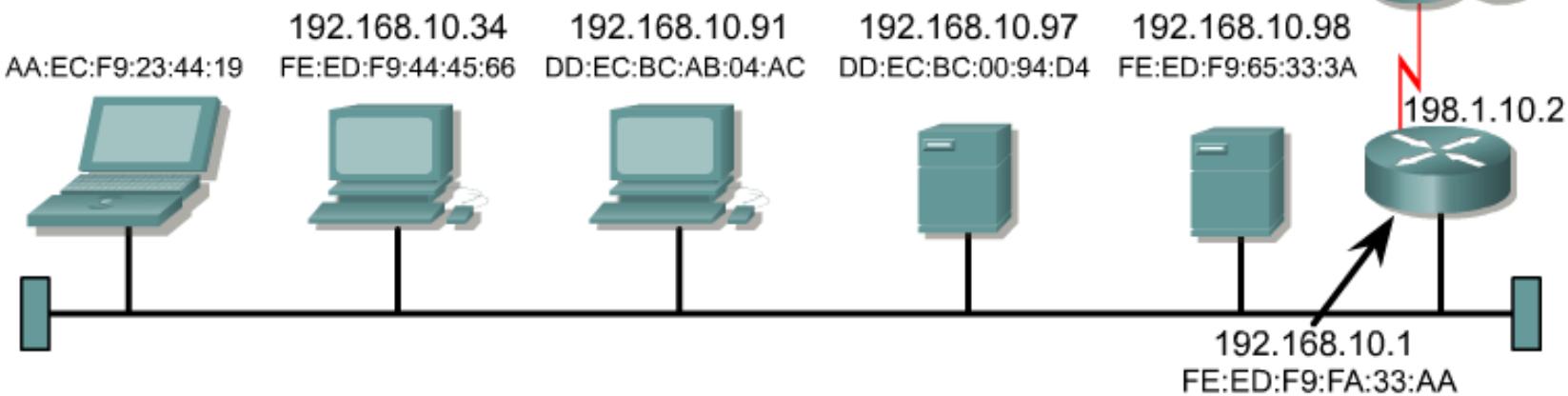
17

Station de travail sans disque dur local

Serveur DHCP

Serveur DHCP

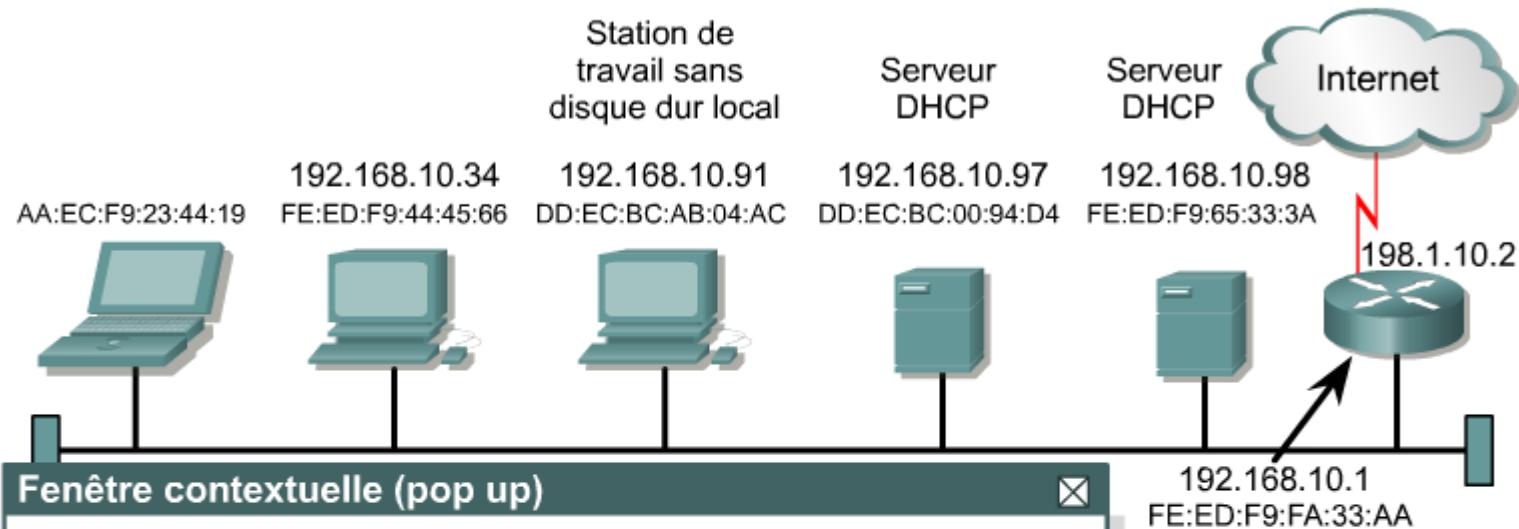
Internet



L'ordinateur portable AA:EC:F9:23:44:19 doit obtenir une adresse IP pour les opérations effectuées sur l'intranet et Internet.

Description des champs de la structure du message DHCP

FIGURES



Fenêtre contextuelle (pop up)

L'ordinateur portable AA:EC:F9:23:44:19 génère une requête DHCP.

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	221					
AA:EC:F9:23:44:19	192.168.10.98	2					
Adresse MAC de destination	Adresse IP de destination	0					
FF:FF:FF:FF:FF:FF	255.255.255.255	0					
Type de champ		0					
0X8035 (Ethernet)		AA:EC:F9:23:44:19					
		53	1	2			

Protocole DHCP : requête transmise

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

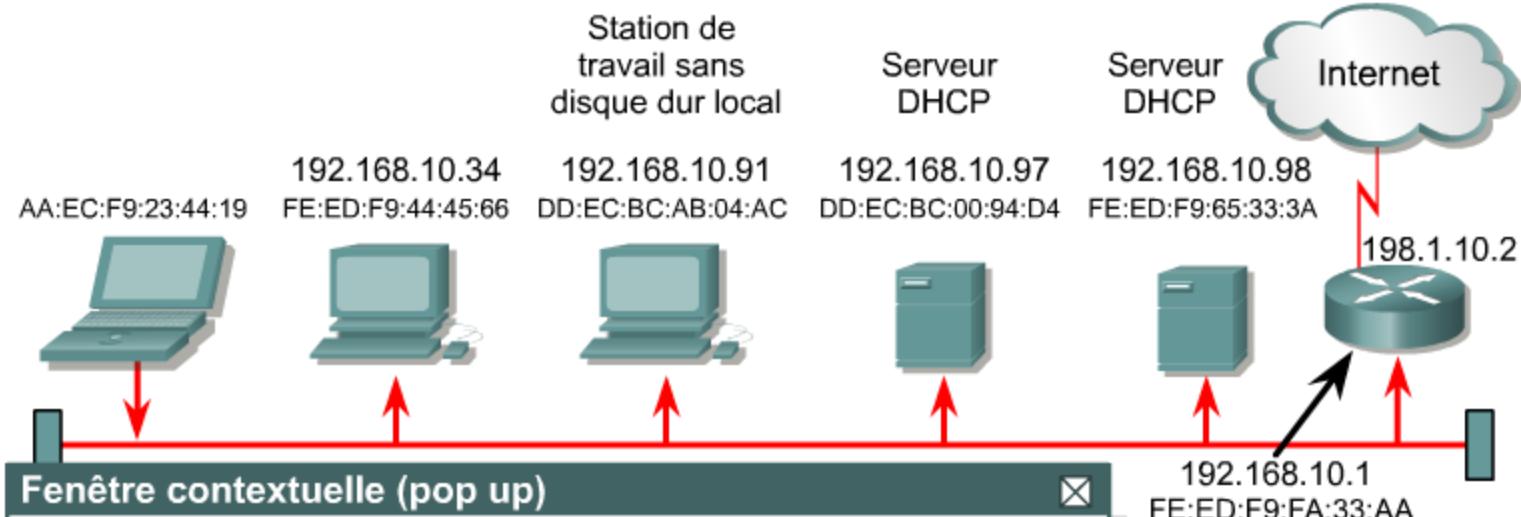
13

14

15

16

17



En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	221					
AA:EC:F9:23:44:19	192.168.10.98	2					
Adresse MAC de destination	Adresse IP de destination	0					
FF:FF:FF:FF:FF:FF	255.255.255.255	0					
Type de champ		0					
0X8035 (Ethernet)		AA:EC:F9:23:44:19					
		53	1	2			

Protocole DHCP : requête évaluée

FIGURES

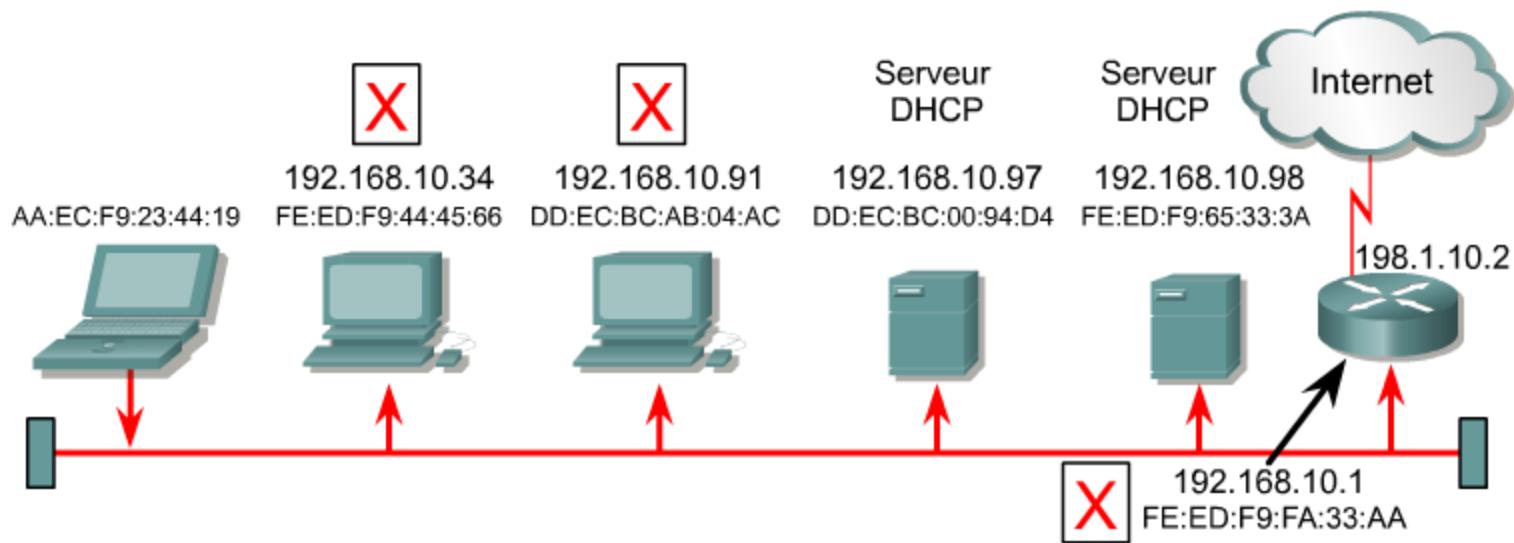
1

2

3

4

5



6

7

8

9

10

11

12

13

14

15

16

17

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC
Adresse M	Fenêtre contextuelle (pop up)					
AA:EC:F9:	Toutes les unités extraient une copie de la trame, détectent une adresse					
Adresse M	MAC de destination de broadcast, retirent l'en-tête et transmettent le					
FF:FF:FF:I	paquet à la couche réseau. Les unités détectent que l'adresse de					
Type de ch	destination IP est une adresse IP de broadcast, retirent l'en-tête du paquet					
0X8035 (E	et transmettent les données de la réponse à la couche transport. Toutes					
	les unités détectent le champ de requête DHCP en tant que requête					
	DHCP. Elle est alors ignorée par toutes les unités, à l'exception des					
	serveurs DHCP.					

Protocole DHCP : offre DHCP préparée

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

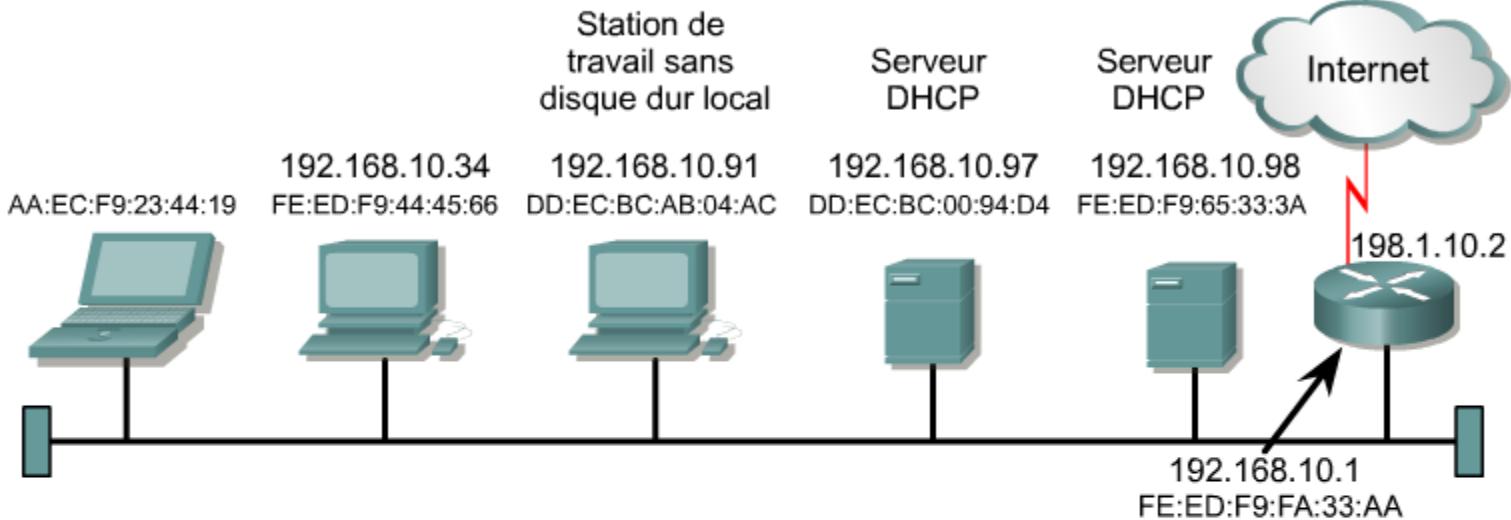
13

14

15

16

17



En-tête de

Fenêtre contextuelle (pop up)

Vérification
du CRC

Adresse M

Le serveur prépare une offre DHCP à renvoyer à l'unité qui est à l'origine de la demande. Elle inclut l'adresse IP du client, l'adresse du serveur DHCP et l'adresse de la passerelle par défaut. Dans l'en-tête de la trame, les

FE:ED:F9:

adresses source et de destination sont inversées. Dans l'en-tête du paquet, le serveur DHCP place son adresse IP dans le champ source et une

Adresse M

adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse DHCP au niveau de la couche transport en

AA:EC:F9:

vue de son traitement. Seul un broadcast sera acheminé puisque le client

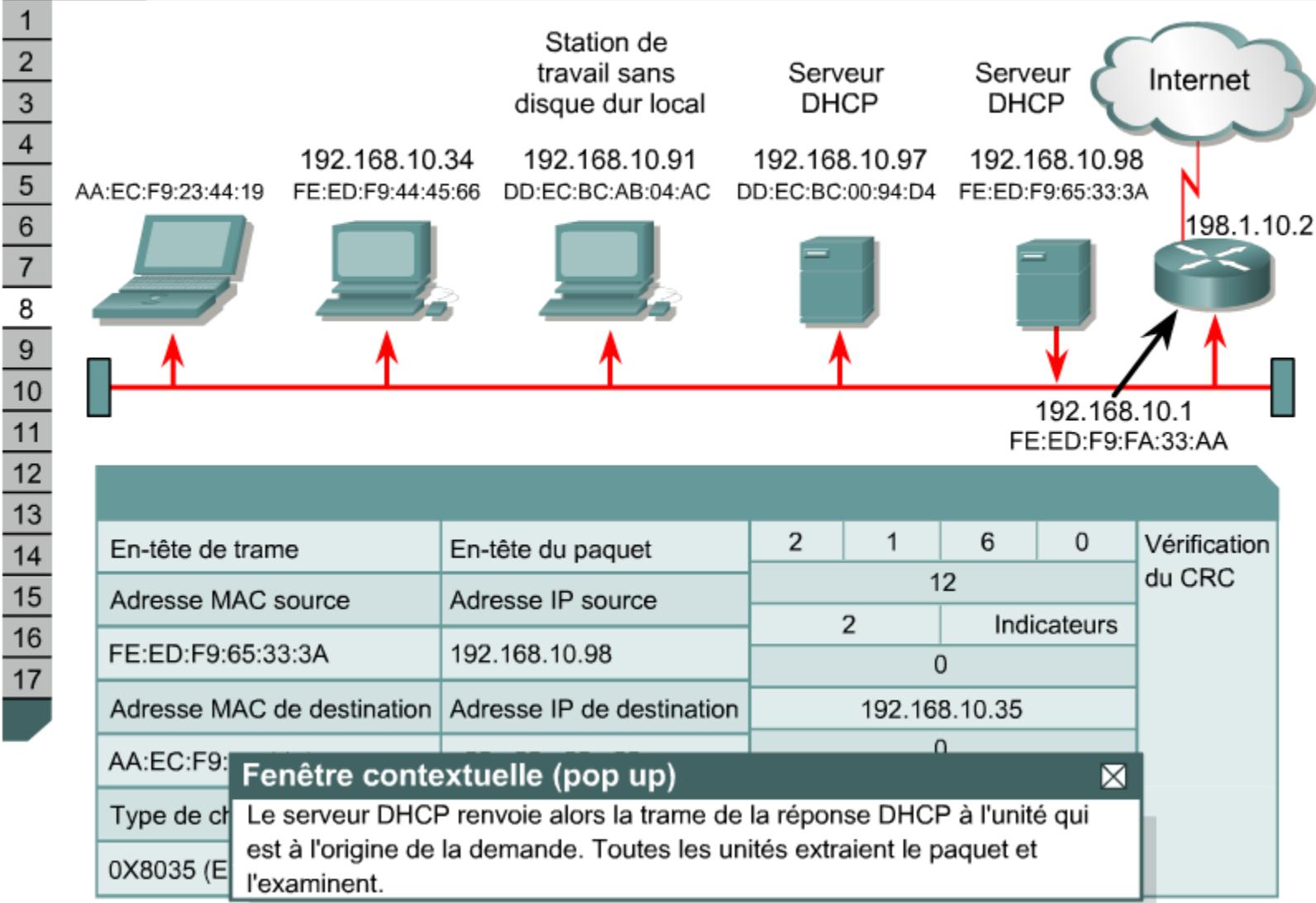
Type de ch

ne connaît pas son adresse IP.

0X8035 (E

Protocole DHCP : offre DHCP transmise

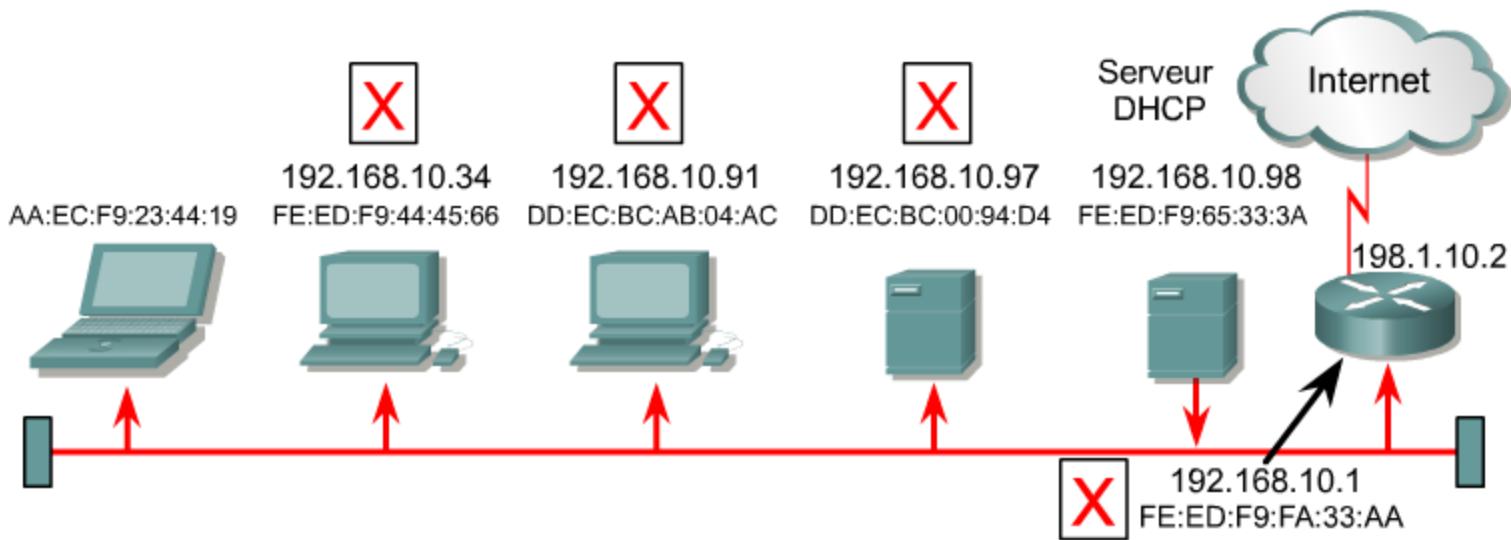
FIGURES



Protocole DHCP : offre DHCP évaluée

FIGURES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

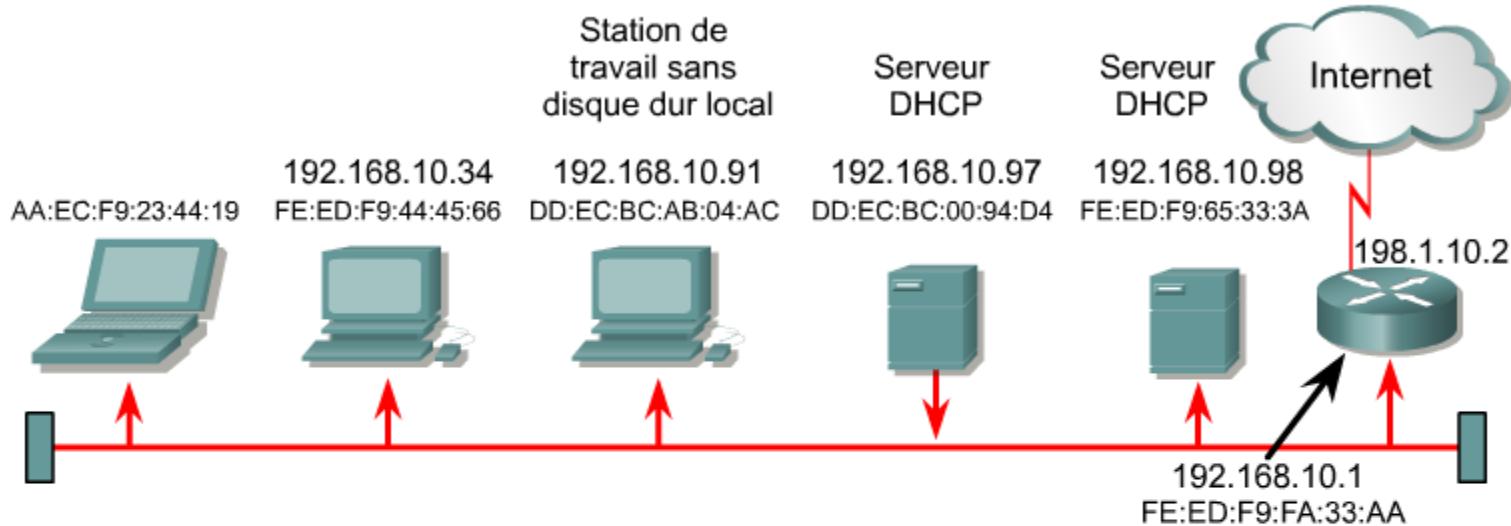


En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FE:ED:F9:	Fenêtre contextuelle (pop up)	2		Indicateurs		
Adresse M	L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré.					
AA:EC:F9:						
Type de ch						
0X8035 (E						

Protocole DHCP : offre DHCP transmise

FIGURES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

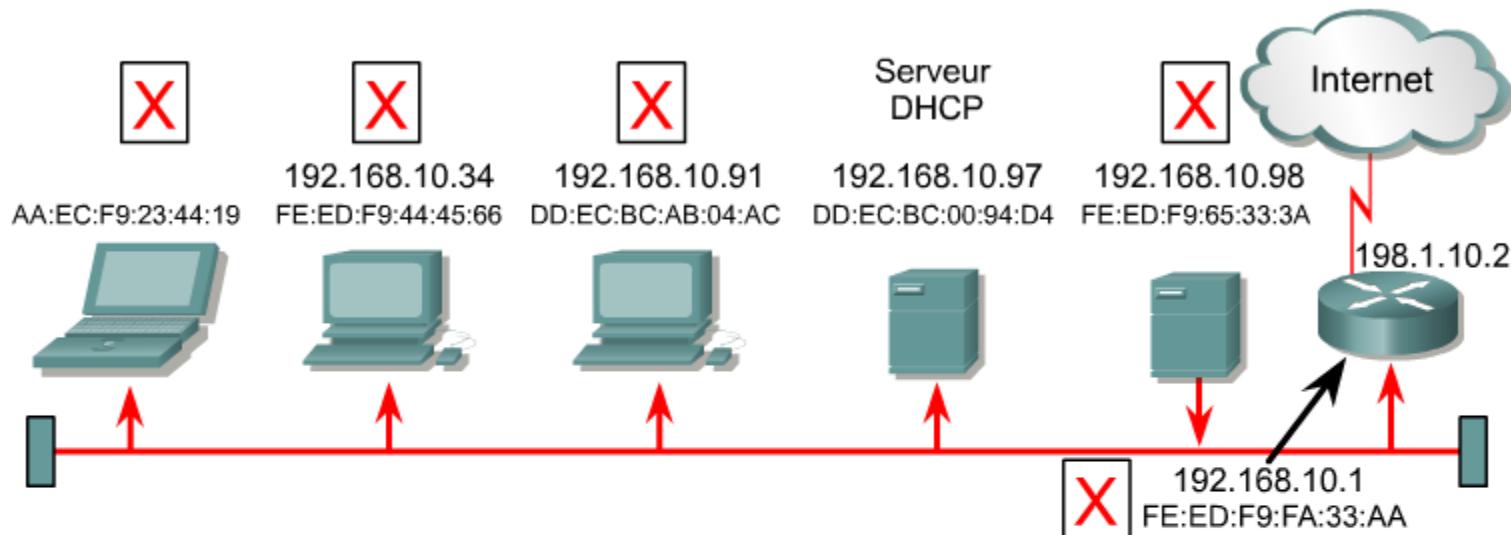


En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	12					
DD:EC:BC:00:94:D4	192.168.10.97	2					
Adresse MAC de destination	Adresse IP de destination	0					
AA:EC:F9:	Fenêtre contextuelle (pop up)	192.168.10.90					
Type de ch	Le deuxième serveur DHCP renvoie alors la trame de la réponse DHCP à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.						
0X8035 (E							

Protocole DHCP : offre DHCP évaluée

FIGURES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source			12		
DD:EC:BC:AB:04:AC						
Adresse MAC destination						
AA:EC:F9:23:44:19						
Type de chaîne						
0X8035 (E)						

Fenêtre contextuelle (pop up)

L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC est celle de l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré. L'ordinateur portable ayant déjà reçu une offre DHCP d'un autre serveur, l'offre est ignorée.

Protocole DHCP : requête DHCP générée

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

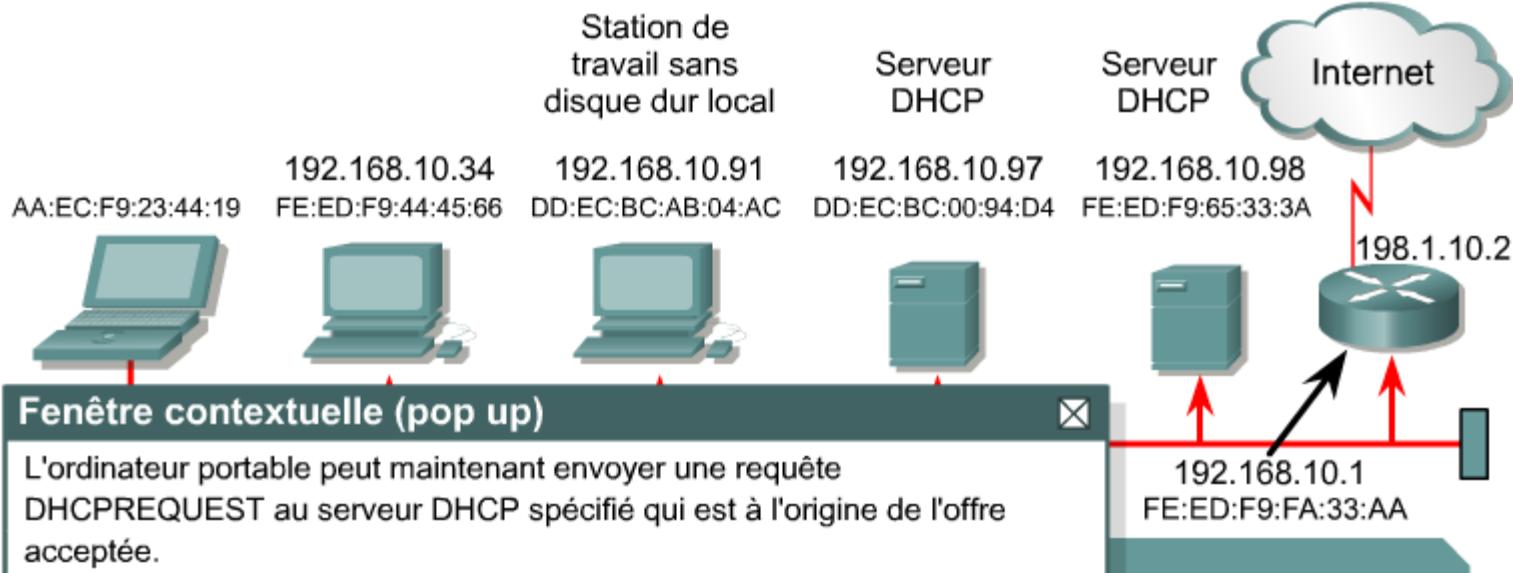
13

14

15

16

17



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	12					
FA:ED:F9:65:33:3A	192.168.10.98	2					
Adresse MAC de destination	Adresse IP de destination	0					
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35					
Type de champ		0					
0X8035 (Ethernet)		192.168.10.1					
		AA:EC:F9:23:44:19					
		53	1	5			

Protocole DHCP : requête DHCP transmise

FIGURES

1

2

3

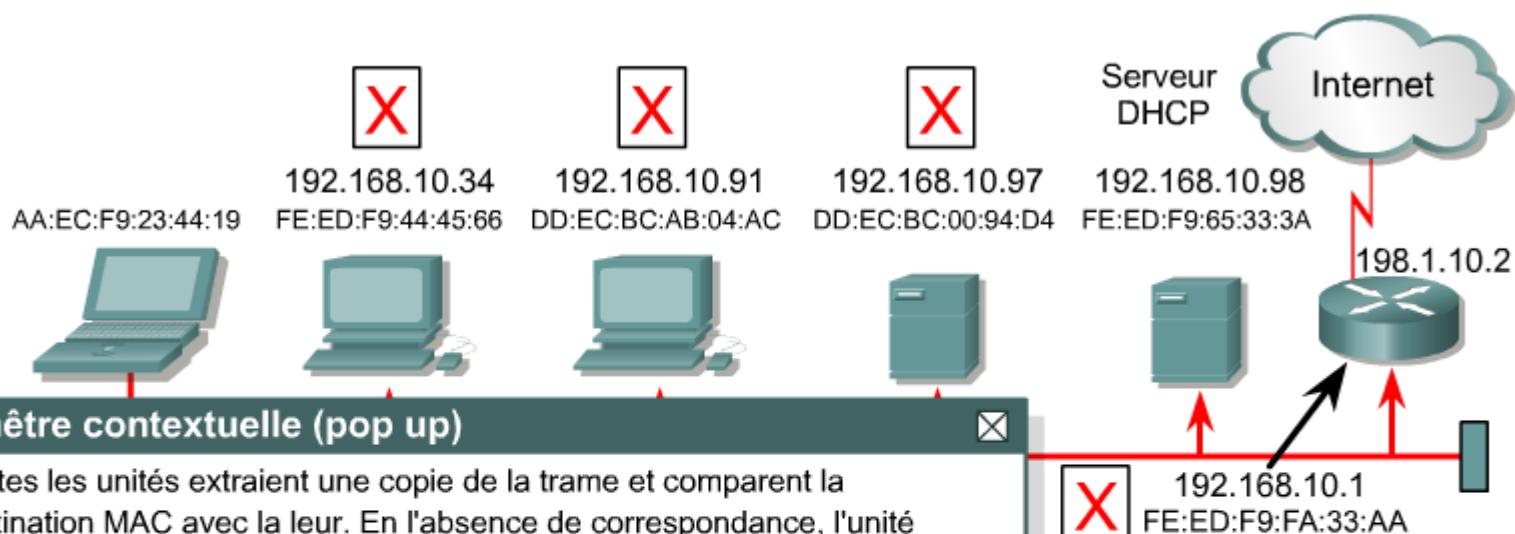
4

5

6

7

8

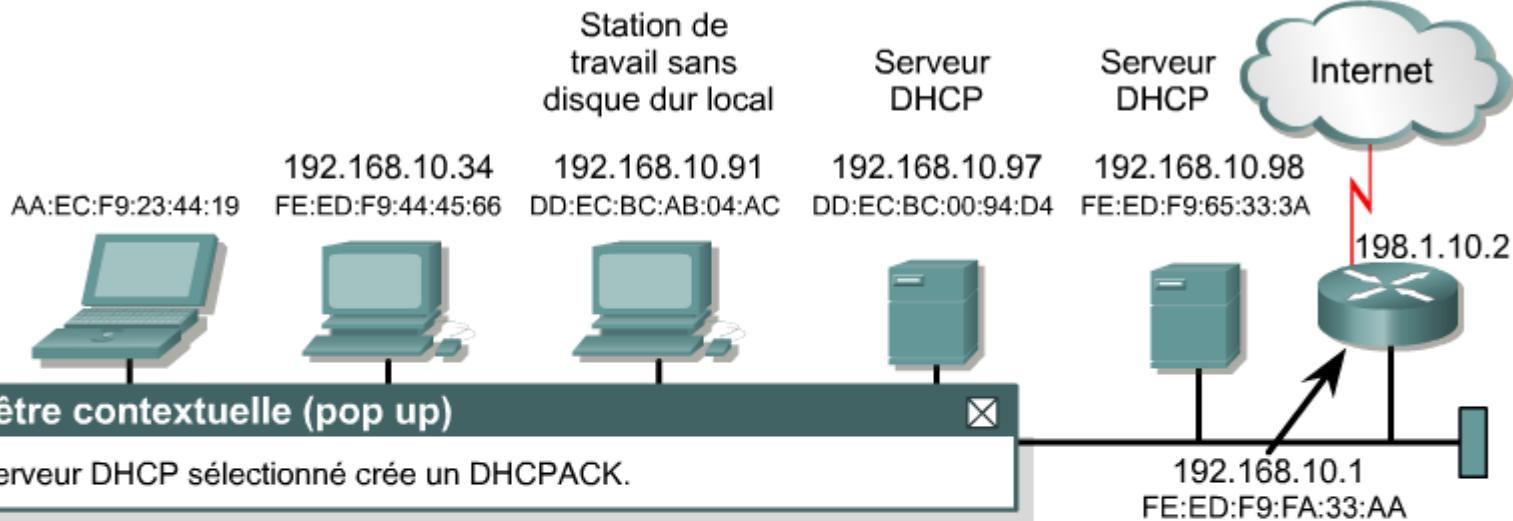


	En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC		
14	Adresse MAC source	Adresse IP source	12						
15	FA:ED:F9:65:33:3A	192.168.10.98	2						
16	Adresse MAC de destination	Adresse IP de destination	0						
17	AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35						
	Type de champ		0						
	0x8035 (Ethernet)		192.168.10.1						
			AA:EC:F9:23:44:19						
			53	1	5				

Protocole DHCP : DHCPACK créé

FIGURES

1
2
3
4
5
6
7
8

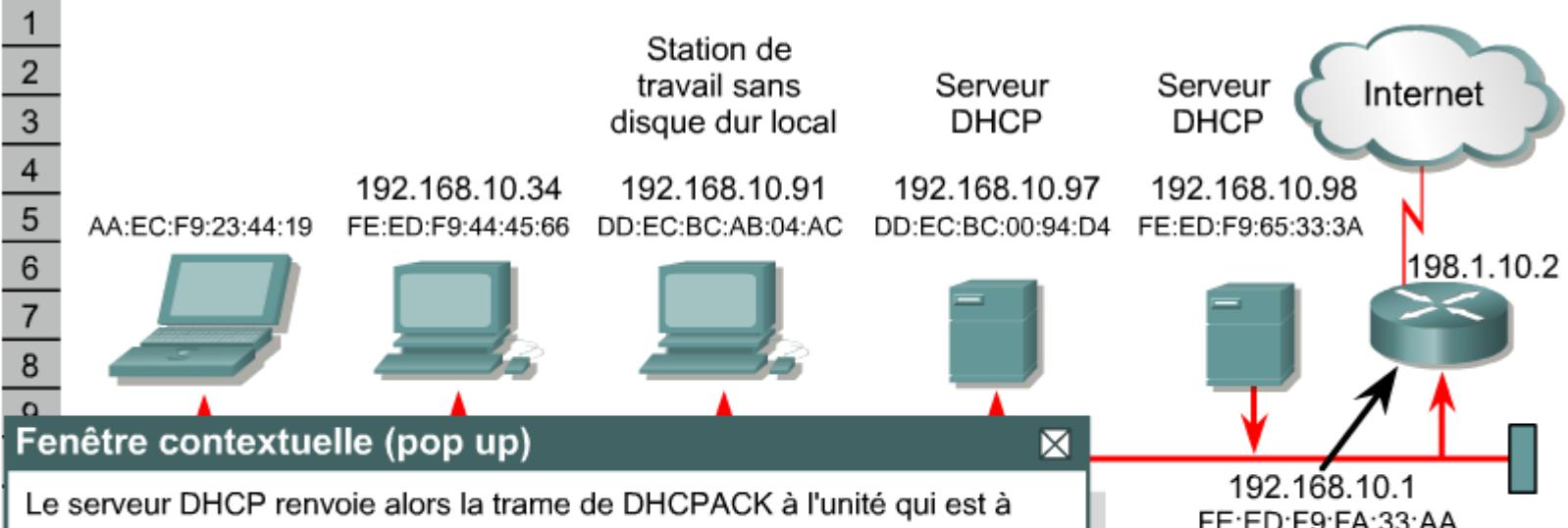


12
13
14
15
16
17

En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	12					
FA:ED:F9:65:33:3A	192.168.10.98	2					
Adresse MAC de destination	Adresse IP de destination	0					
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35					
Type de champ		0					
0X8035 (Ethernet)		192.168.10.1					
		AA:EC:F9:23:44:19					
		53	1	5			

Protocole DHCP : DHCPACK transmis

FIGURES



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC	
Adresse MAC source	Adresse IP source	12					
FA:ED:F9:65:33:3A	192.168.10.98	2					
Adresse MAC de destination	Adresse IP de destination	0					
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35					
Type de champ		0					
0X8035 (Ethernet)		192.168.10.1					
		AA:EC:F9:23:44:19	53	1	5		

Protocole DHCP : DHCPACK évalué

FIGURES

1

2

3

4

5

6

7

8

9

10

11

12

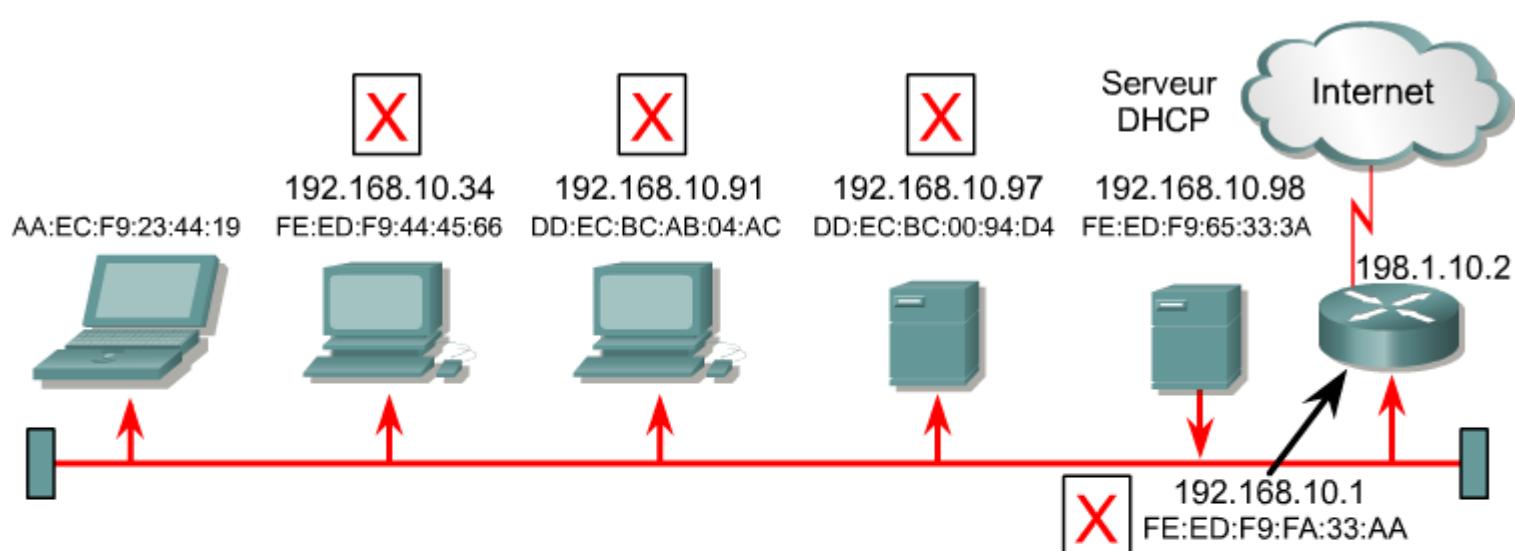
13

14

15

16

17



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC		
Adresse MAC source	Adresse IP source	12						
FA:ED:F9:		2		Indicateurs				
Adresse M	Fenêtre contextuelle (pop up)							
AA:EC:F9:	L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré.							
Type de ch								
0X8035 (E								

Protocole DHCP : DHCPACK créé

FIGURES

1

?

3

4

5

6

7

9

9

10

11

12

13

1

15

10

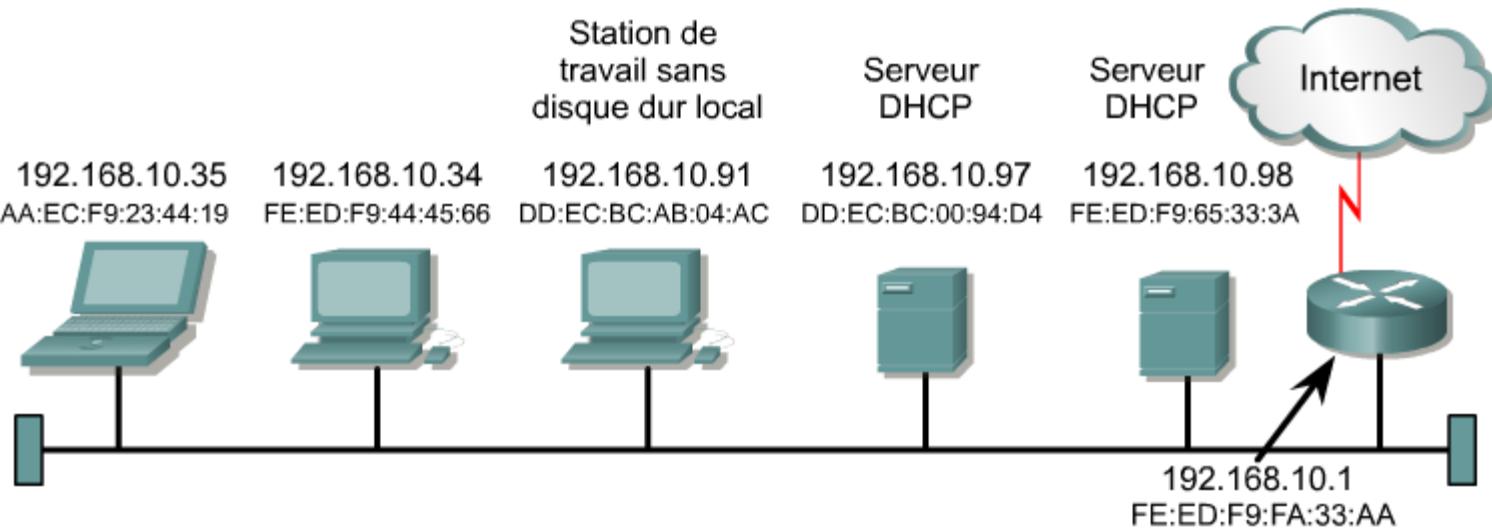
1

Station de travail sans disque dur local

Serveur DHCP

Serveur DHCP

Internet



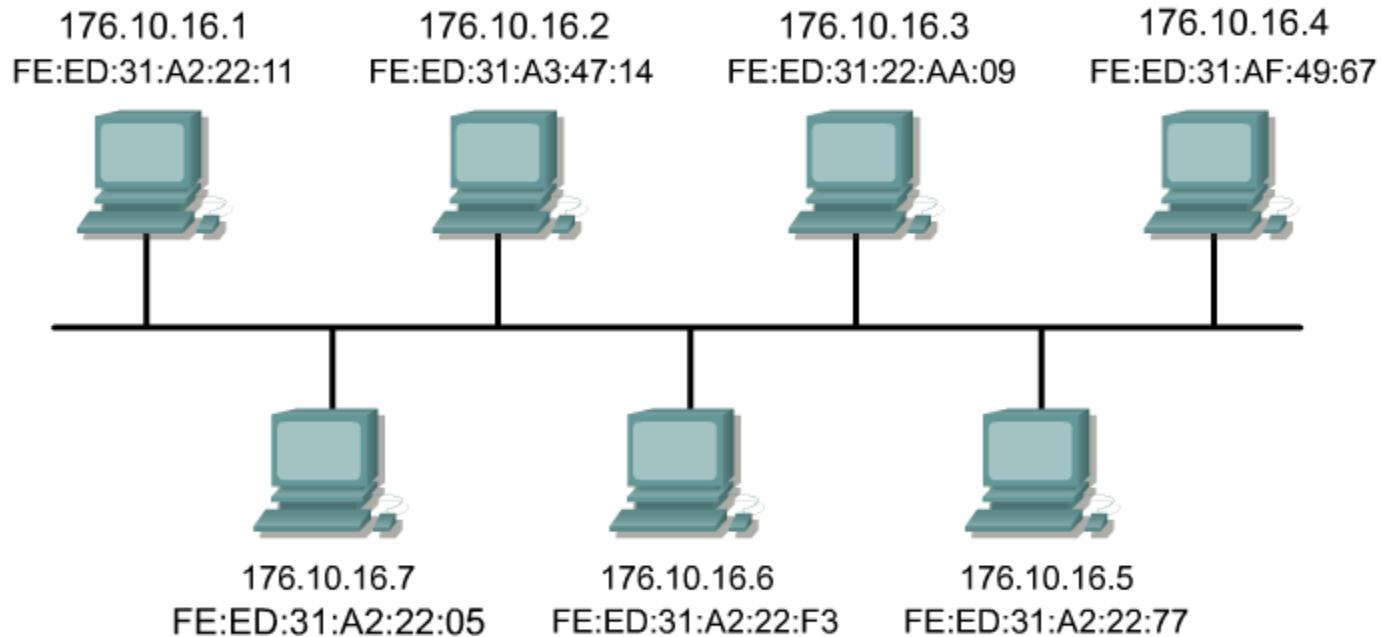
L'ordinateur portable passe alors en mode de liaison et commence à utiliser l'adresse IP attribuée ainsi que d'autres données transmises avec le message de l'offre DHCP.

Problèmes de résolution d'adresses en transmission LAN

FIGURES

1

2



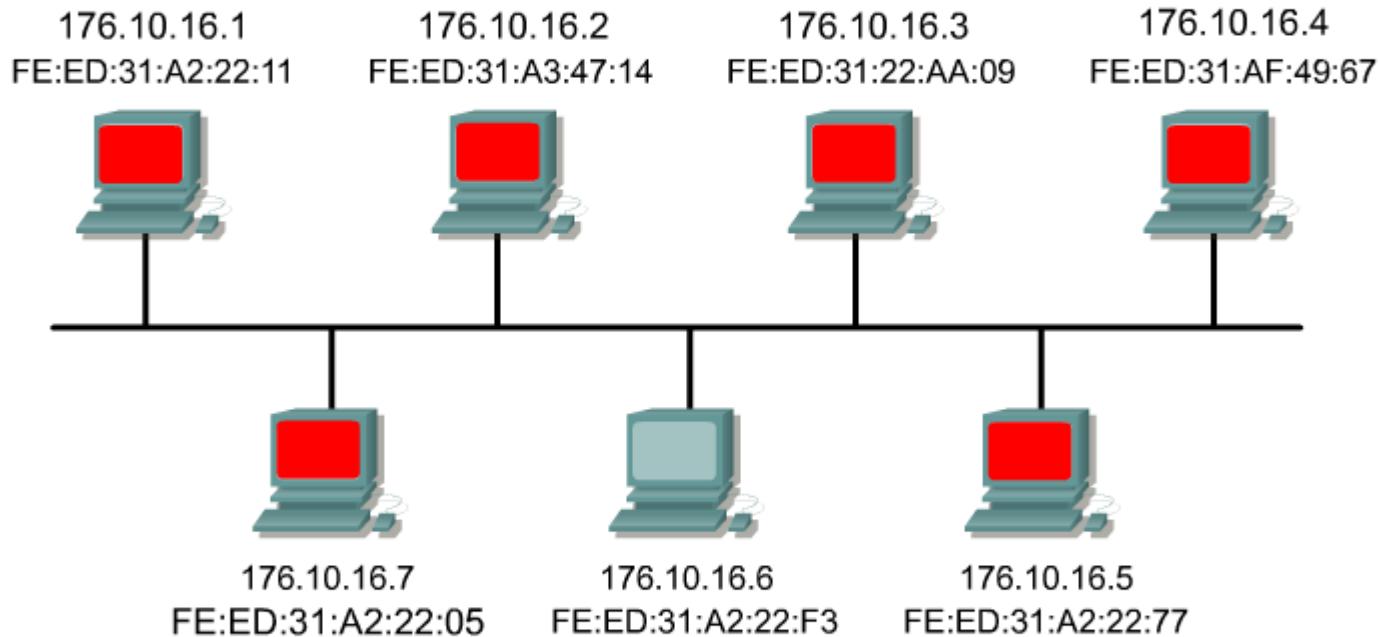
Adresse IP	Adresse MAC

Problèmes de résolution d'adresses en transmission LAN

FIGURES

1

2



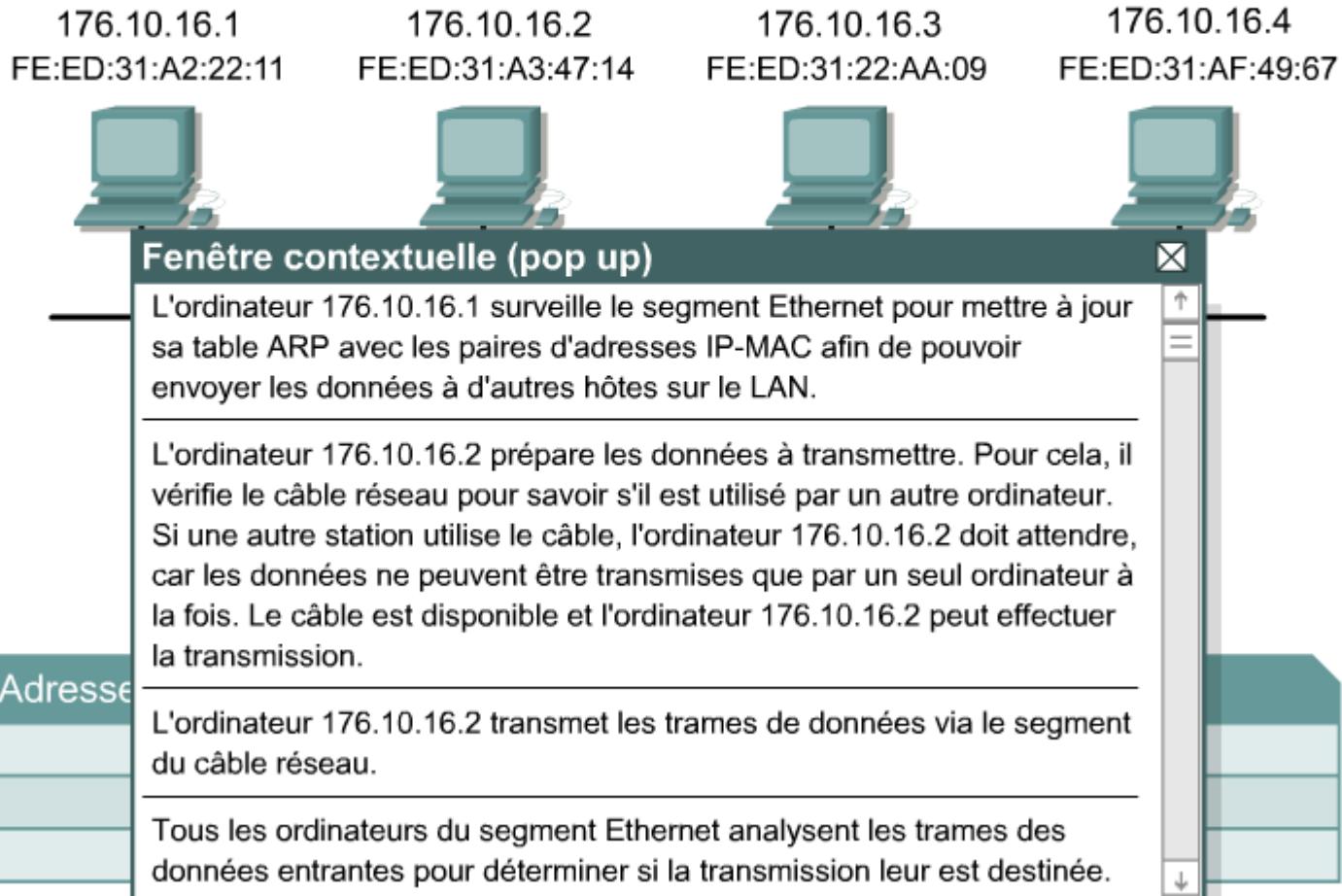
Adresse IP	Adresse MAC
176.10.16.2 FE:ED:31:A3:47:14	
176.10.16.3 FE:ED:31:22:AA:09	
176.10.16.6 FE:ED:31:A2:22:F3	

Problèmes de résolution d'adresses en transmission LAN

FIGURES

1

2



Problèmes de résolution d'adresses en transmission LAN

FIGURES

1

2

176.10.16.1 176.10.16.2 176.10.16.3 176.10.16.4
FE:ED:31:A2:22:11 FE:ED:31:A3:47:14 FE:ED:31:22:AA:09 FE:ED:31:AF:49:67



Fenêtre contextuelle (pop up)

Une partie de ce processus consiste à ajouter les adresses source IP-MAC à la table ARP. La trame des données est ignorée par toutes les unités, à l'exception de celle à laquelle les données ont été envoyées.

L'ordinateur 176.10.16.3 prépare les données à transmettre. Il effectue toutes les étapes de la préparation.

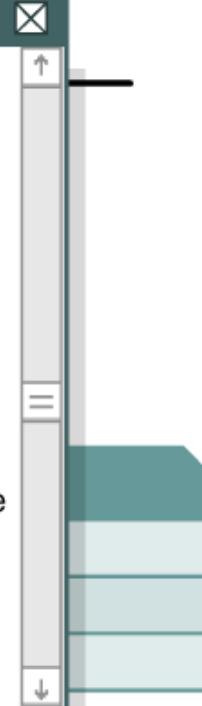
L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du même segment analysent les trames entrantes. Ils ajoutent les données à leurs tables ARP et ignorent la trame si les données ne leurs sont pas destinées.

L'ordinateur 176.10.16.6 prépare les données à transmettre.

L'ordinateur 176.10.16.6 transmet ses trames de données via le segment

Adresse



Problèmes de résolution d'adresses en transmission LAN

FIGURES

1

2

L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes. Ils ajoutent les données à leurs tables ARP et ignorent la trame si les données ne leur sont pas destinées. Cela correspond au processus automatique utilisé sur un LAN Ethernet normal pour gérer les associations d'adresses.

L'ordinateur 176.10.16.1 souhaite envoyer les données à l'ordinateur 176.10.16.4. Il dispose d'une adresse IP, mais la transmission des données nécessite aussi l'adresse MAC de l'ordinateur 176.10.16.4. Comment peut-il obtenir cette adresse MAC pour transmettre les données ?



Problèmes de résolution d'adresses non locales

FIGURES

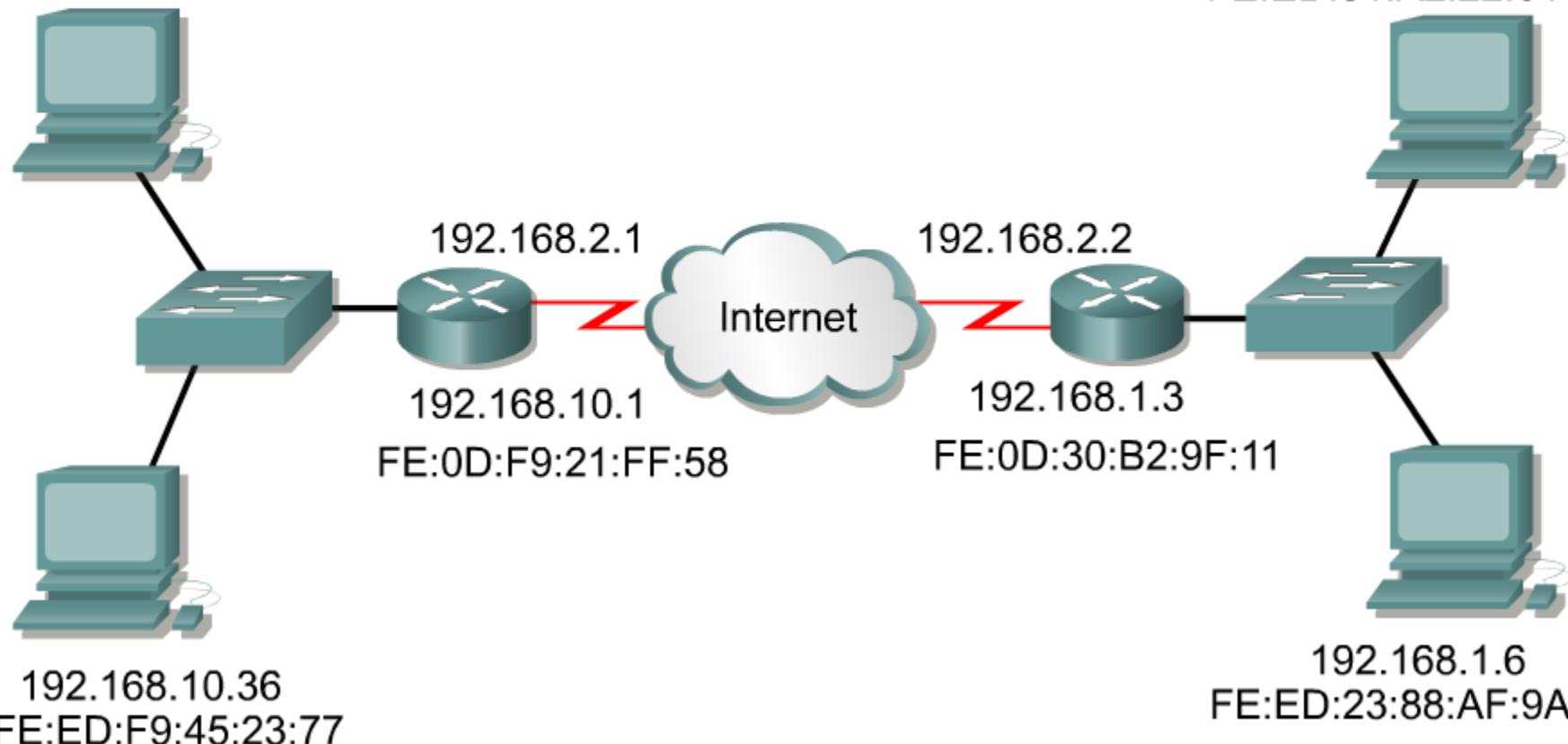
1

2

L'ordinateur 192.168.10.34 doit communiquer avec l'ordinateur 192.168.1.1. Comment obtient-il l'adresse MAC de l'ordinateur 192.168.1.1, et l'obtention de cette adresse présente-t-elle des avantages ? Les adresses MAC sont utiles uniquement dans un réseau local. Elles sont donc inutiles en dehors du réseau 192.168.10.0. Ainsi, l'adresse MAC du routeur est nécessaire pour extraire les données du LAN et les transférer au système WAN.

192.168.10.34
FE:ED:F9:44:45:66

192.168.1.1
FE:ED:31:A2:22:01



192.168.10.36
FE:ED:F9:45:23:77

192.168.1.6
FE:ED:23:88:AF:9A

Entrée de la table ARP

FIGURES

1
2
3
4
5
6

Entrée de la table ARP

Adresse Internet	Adresse physique	Type
68.2.168.1	00-50-57-00-76-84	Dynamique

Table ARP 198.150.11.36

MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Fonctions de la table ARP

FIGURES

1

2

FE:ED:31:A2:22:11

176.10.16.1



FE:ED:31:A3:47:14

176.10.16.2



FE:ED:31:22:AA:09

176.10.16.3



FE:ED:31:AF:49:67

176.10.16.4

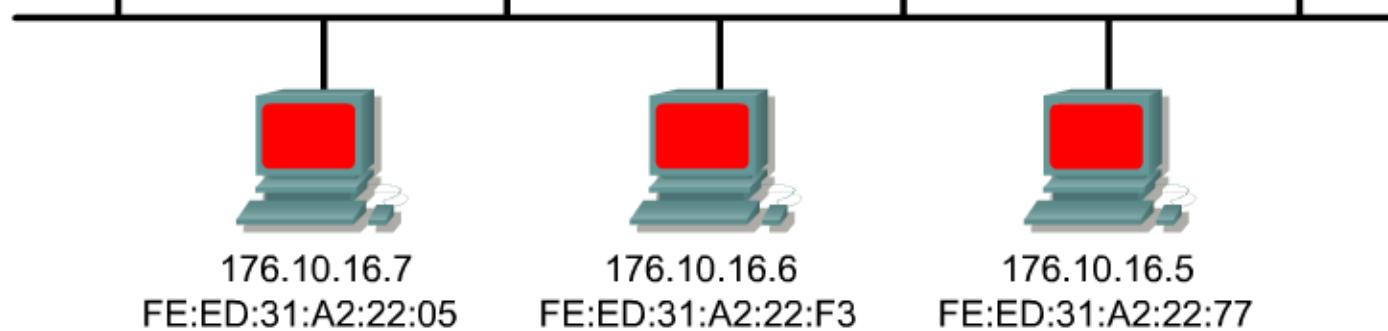


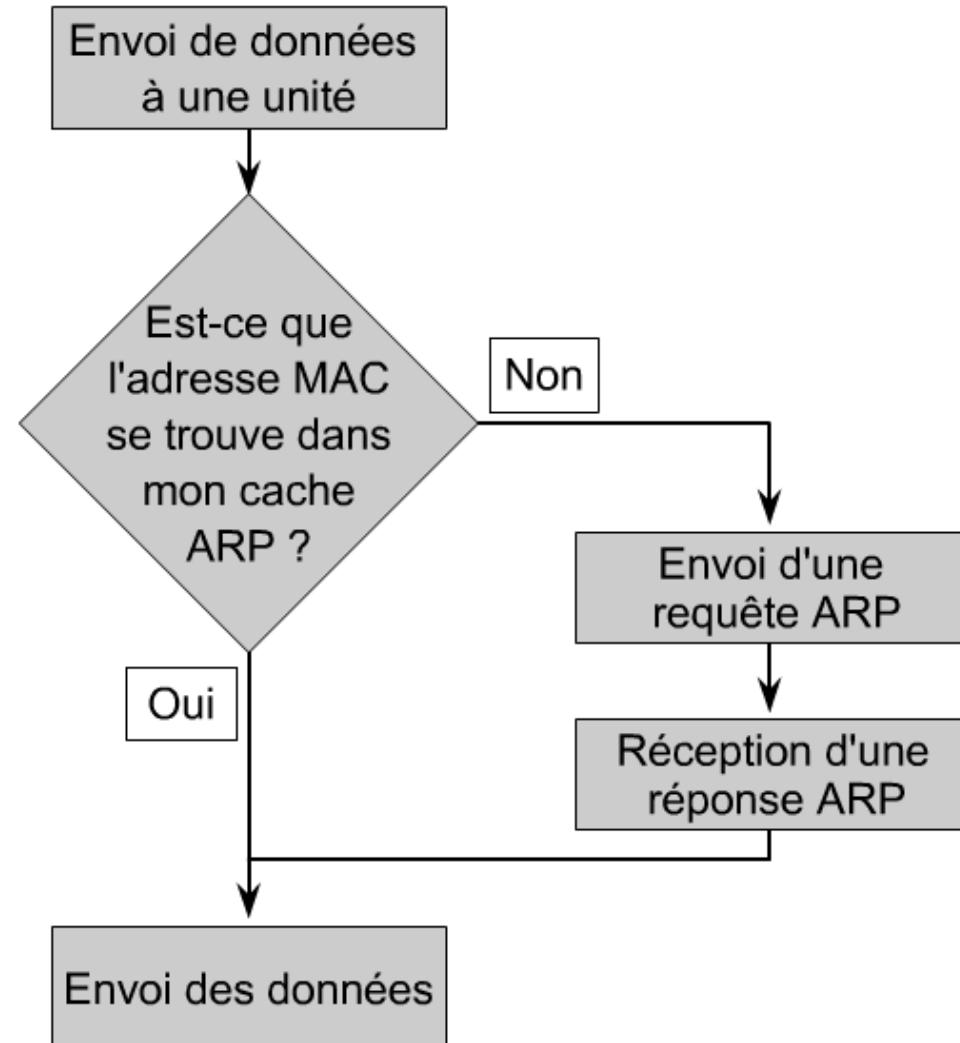
Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Processus ARP

FIGURES

1
2
3
4
5
6



Requête ARP

FIGURES

1

2

3

4

5

6

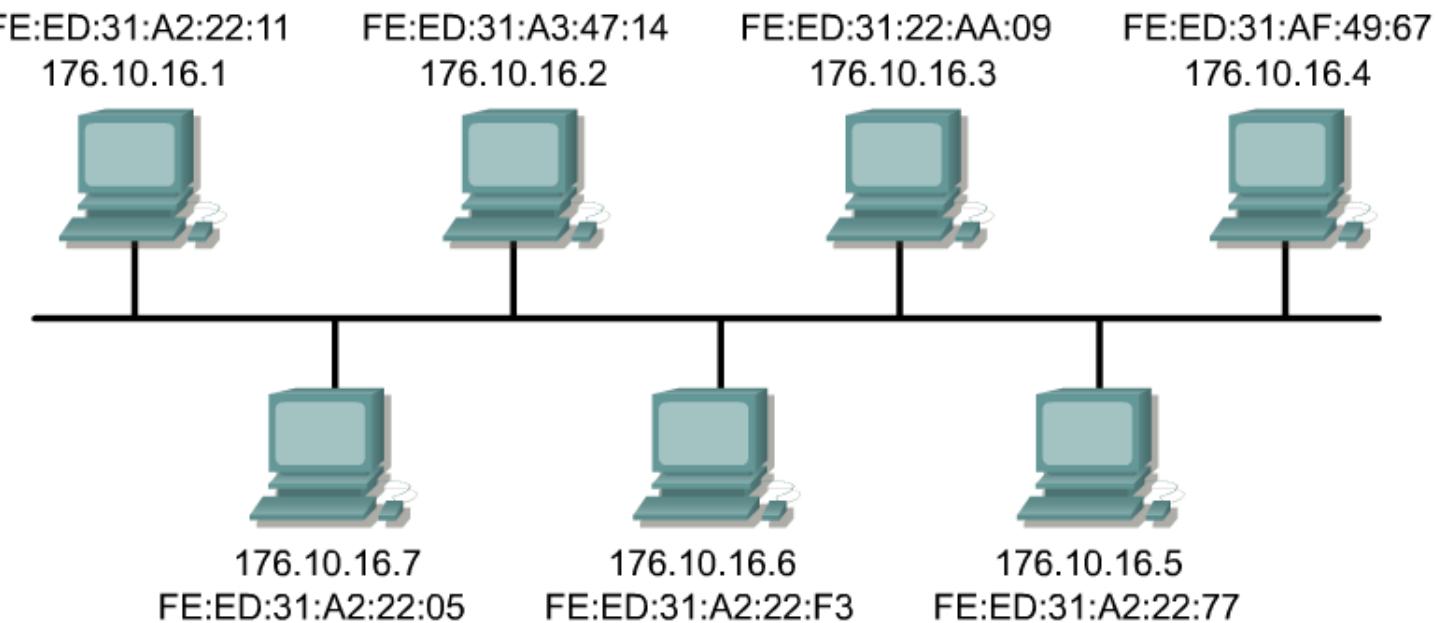


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Requête ARP

FIGURES

L'ordinateur 176.10.16.1 doit transmettre des données à l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 prépare les données à transmettre à l'ordinateur 176.10.16.4. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de l'ordinateur 176.10.16.4 ne se trouve pas dans sa table ARP. L'ordinateur 176.10.16.1 ayant besoin de cette paire, il doit émettre une requête ARP pour l'obtenir.

L'ordinateur 176.10.16.1 n'effectue pas le processus d'encapsulation pour la transmission des données mais crée une requête ARP pour obtenir l'adresse MAC de l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Requête ARP

FIGURES

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse IP de destination des trames entrantes.

L'ordinateur 176.10.16.4 prépare les données de réponse ARP à transmettre.

L'ordinateur 176.10.16.4 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du segment analysent les trames entrantes et ajoutent les données à leurs tables ARP.

Requête ARP

FIGURES

L'ordinateur 176.10.16.1 prépare les données à transmettre.

L'ordinateur 176.10.16.1 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

L'ordinateur 176.10.16.4 traite la transmission des données.

Requête Proxy ARP

FIGURES

1

2

3

4

5

6

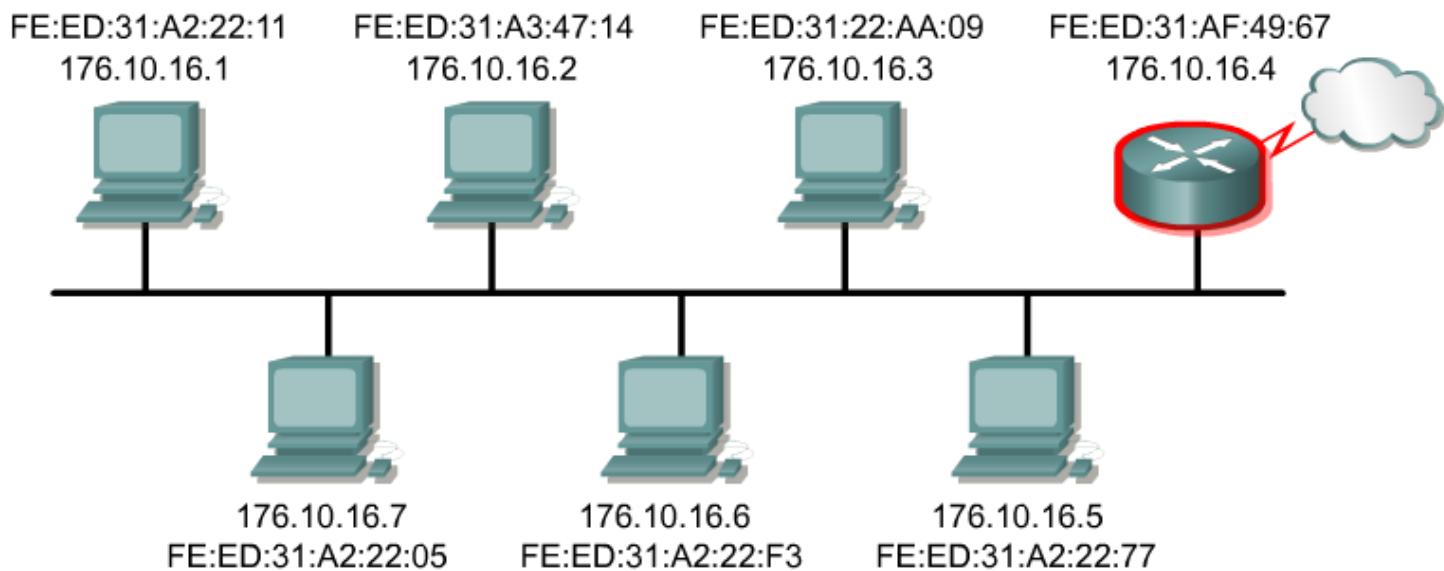


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

Requête Proxy ARP

FIGURES

L'ordinateur 176.10.16.1 doit transmettre des données à routeur 176.10.16.4.

L'ordinateur 176.10.16.1 prépare les données à transmettre à routeur 176.10.16.4. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de routeur 176.10.16.4 ne se trouve pas dans sa table ARP. L'ordinateur 176.10.16.1 ayant besoin de cette paire, il doit émettre une requête ARP pour l'obtenir.

L'ordinateur 176.10.16.1 n'effectue pas le processus d'encapsulation pour la transmission des données mais crée une requête ARP pour obtenir l'adresse MAC de l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Requête Proxy ARP

FIGURES

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Toutes les unités, à l'exception du routeur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse IP de destination des trames entrantes.

Le routeur 176.10.16.4 compare l'adresse avec son adresse IP de l'interface Ethernet. Grâce à cette opération, il constate que ce paquet est acheminé en dehors du LAN. Ce routeur étant compatible avec le protocole Proxy ARP, il prépare une réponse ARP à l'hôte demandeur avec son adresse MAC et l'adresse IP de l'unité de destination.

Le routeur 176.10.16.4 transmet ses trames de données via le segment Ethernet.

Requête Proxy ARP

FIGURES

À nouveau, tous les hôtes du segment analysent les trames entrantes et ajoutent les données à leurs tables ARP.

L'ordinateur 176.10.16.1 prépare les données à transmettre.

L'ordinateur 176.10.16.1 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

Le routeur 176.10.16.4 prend en charge la transmission des données vers le prochain saut du réseau.

Passerelle par défaut

FIGURES

1
2
3
4
5
6

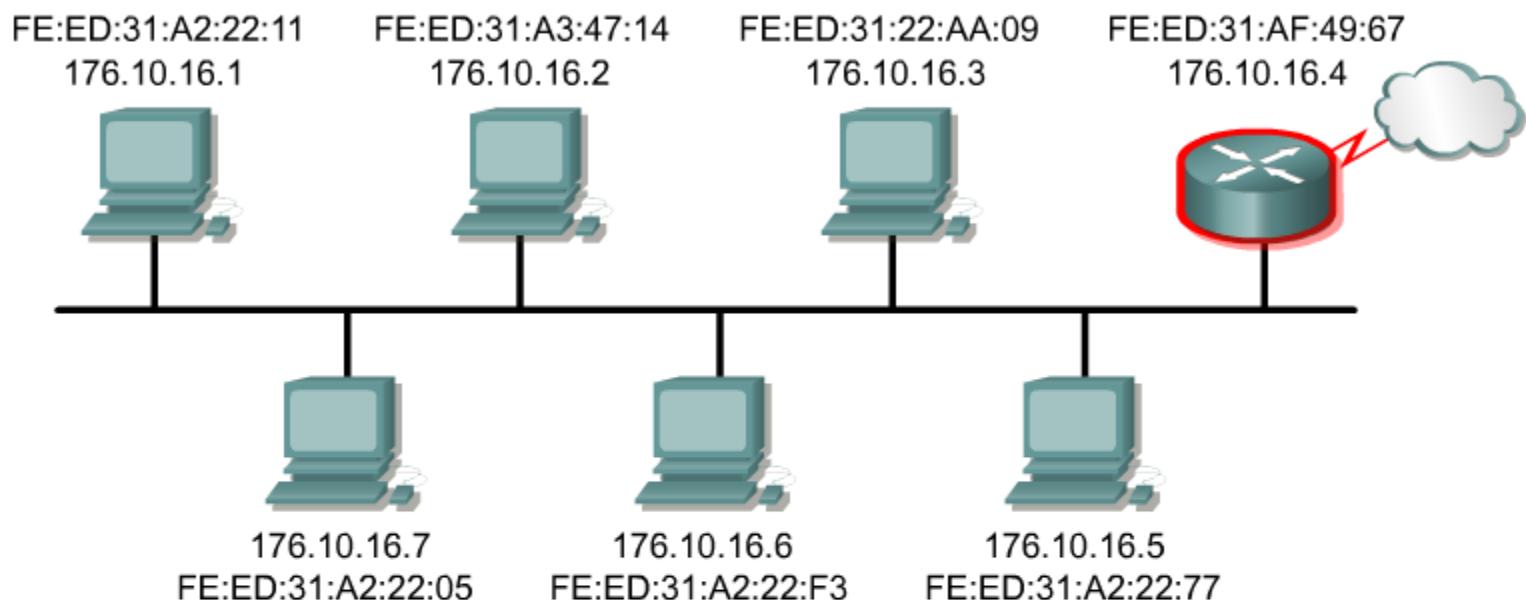


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut

176.10.16.4	FE:ED:31:AF:49:67

Passerelle par défaut

FIGURES

L'ordinateur 176.10.16.1 doit transmettre des données à l'ordinateur 199.11.20.5 l'adresse MAC de la passerelle par défaut.

L'ordinateur 176.10.16.1 prépare les données à transmettre à l'ordinateur 199.11.20.5. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de l'ordinateur 199.11.20.5 ne se trouve pas dans sa table ARP. Lorsque la passerelle par défaut est définie sur cet ordinateur, l'adresse de destination est comparée à l'adresse source des hôtes. Cette opération révèle que l'adresse de destination est située sur un autre réseau. L'hôte élabore alors la trame des données à l'aide de l'adresse IP de destination et de l'adresse MAC des passerelles par défaut.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les hôtes du même segment analysent les trames entrantes.

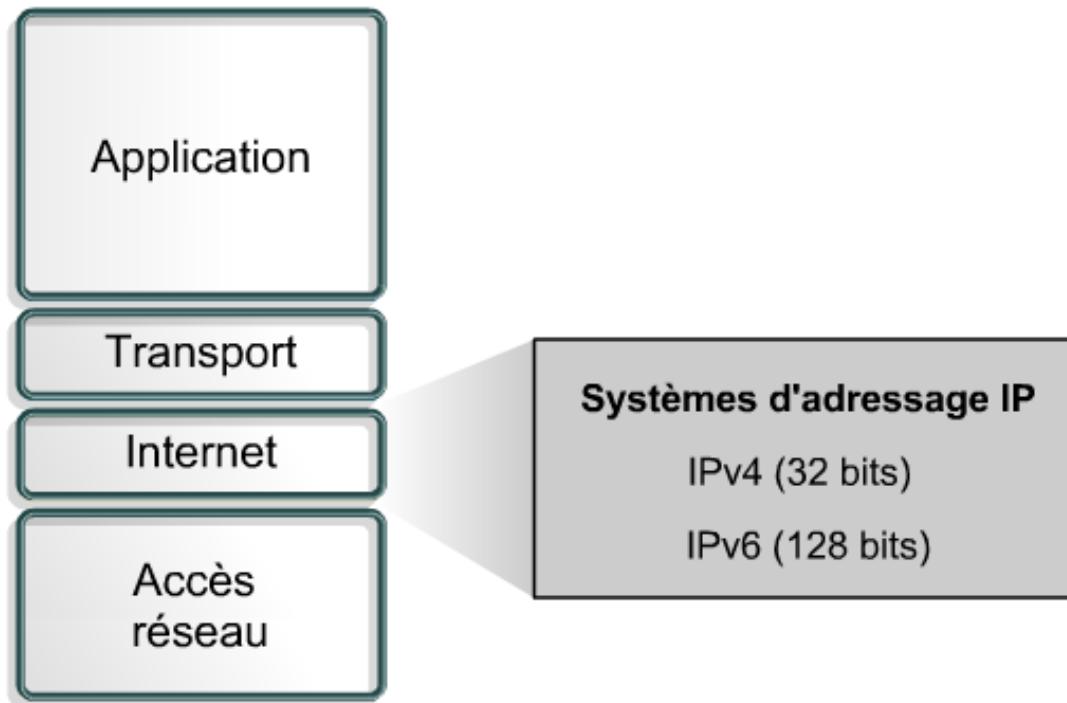
Tous les ordinateurs, à l'exception du routeur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

Module 9 : Résumé

FIGURE

1

Couches du modèle TCP/IP



Référence: Cisco CCNA 1

 Copyright sur l'intégralité du contenu © 2003 Cisco Systems, Inc. Tous droits réservés.