Ministère de l'enseignement supérieur et de la recherche scientifique
Institut Supérieur des Études Technologiques de Zaghouan
Département Technologies de l'Informatique

Module
Réseaux Locaux d'Entreprises & Architecture TCP/IP
Chapitre 8
Le protocole IP

Elaboré par
Rim BRAHMI

Public cible
2ème année Licence Appliquée en Réseaux et Services Informatiques

Année universitaire 2019-2020

Table de matières

Chapitre 8 : Protocole IPv4

Vue d'ensemble

Ce chapitre présente le protocole IP de la couche Internet de la pile protocolaire TCP/IP en introduisant le concept d'interconnexion des réseaux internet, la notion d'adressage, la création des sous réseaux ainsi que les concepts routage et les fonctions NAT et PAT.

Objectifs

- Décrire la structure d'une adresse IPv4
- Identifier les différents champs du paquet IPv4
- Comparer les caractéristiques et les utilisations des adresses de monodiffusion (unicast), de diffusion (broadcast) et de multidiffusion (multicast) IPv4

Prérequis

U.E Fondement réseaux, U.E Architecture et système I

Durée de déroulement

- 6h de Cours
- 2 séance (2h) de TD

Elements de contenu

- Adressage IPv4
- Création des sous réseaux
- Routage et les fonctions NAT et PAT

Leçon1 : Adressage IPv4

Objectif général	• Connaître le principe de l'adressage du protocole IPv4.
Objectifs spécifiques	• Décrire la structure d'une adresse IPv4 • Identifier les différents champs du paquet IPv4. • Comparer les caractéristiques et les utilisations des adresses de monodiffusion (unicast), de diffusion (broadcast) et de multidiffusion (multicast) IPv4
Volume horaire	• Cours : 1,5h
Mots clés	• IPv4, la couche réseaux, les classes d'adresses, CIDR, adresses réservées …

Introduction

Le but de l'adressage est de fournir un service de communication universel permettant a tout hôte de communiquer avec tout autre hôte de l'interconnexion. En fait, un hôte doit être accessible (par des humains ou d'autres hôtes) et par la suite, cet hôte doit être reconnu par

- Un nom,
- Une adresse qui doit être un identificateur universel sur l'hôte.
- Une route précisant comment la machine peut être atteinte.

Nous détaillerons le protocole IP dans cette leçon qui assure les fonctionnalités suivantes :

- Définir le format du datagramme IP qui est l'unité de base des données circulant sur internet
- Définir le routage sur Internet
- Définir la gestion de la remise non fiable des datagrammes.

I. Format de l'adresse IPv4

I.1. Structure d'une adresse IPv4

Les adresses IPv4 sont composées de 4 octets. Par convention, une adresse IPv4 est codée sur 32 bits. Elle est représentée en format décimal: 4 octets séparés de «. » : 192.168.10.10

L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte est unique à l'intérieur d'un même réseau.

I.2. Exemples

10.10.200.20 : Partie réseau :10.0.0.0 partie hôte 0.10.200.20

192.168.10.2 : Partie réseau : 192.168.10.0 partie hôte 0.0.0.2

172.172.10.2 : Partie réseau :172.172.0.0 partie hôte 0.0.10.2

I.3. Application

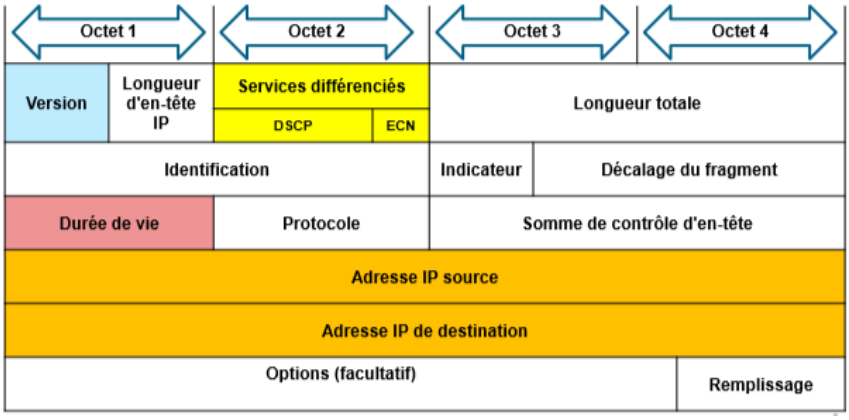
1. convertir les adresses suivantes en binaire

- 192.168.10.1
- 10.10.0.33
- 223.20.4.9

II. Format de l'entête IPv4

Le paquet IP est formé de deux grandes parties :

- **Entête du paquet**, généralement d'une taille de 20 octets, constitue le PCI du protocole. C'est là que sont inscrites toutes les informations du protocole (adresse, segmentation, options, etc.).
- **Partie « data », ou champ de données**, d'une taille maximum de : (65536 octets) – (les octets d'entête et d'options). Elle véhicule la PDU de couche supérieure (généralement un segment TCP ou UDP).



Entête IP (source : https://openclassrooms.com/fr/courses/2340511)

Après la valeur 4, pour le numéro de version, est indiquée la longueur de l'entête, qui permet de connaitre l'emplacement du début des données du fragment IP. Le champ suivant (type of service), précise le type de service des informations transportées dans le corps du paquet. Vient ensuite la longueur totale. Le champ suivant identifie le message auquel le paquet appartient.

Le drapeau porte plusieurs notifications. Il précise, en particulier, si une segmentation a été effectuée. Si oui, l'emplacement du fragment transporté dans le message TCP est indiqué dans le champ « emplacement du segment ». Le temps de vie spécifie le temps après lequel le paquet est détruit. Dans la réalité cette zone contient une valeur entière,

indiquant le nombre de nœuds qui peuvent être traversées avant une destruction du paquet. La valeur 16 est utilisée sur Internet, si un paquet IP a traversée plus de 15 routeurs, ce paquet soit détruit.

Le numéro de protocole indique quel est le protocole encapsulé à l'intérieur du paquet.

La zone de détection d'erreur permet de déterminer si la transmission du paquet s'est effectuée correctement ou non.

Enfin, les adresses de l'émetteur et du récepteur sont précisées dans la dernière partie de l'entête, chacune sur 4 octets.

III. Types des adresses IPv4

III.1. Les types de transmission dans IPV4

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

III.1.1. Monodiffusion

C'est un processus consistant à envoyer un paquet d'un hôte à un autre hôte spécifique.

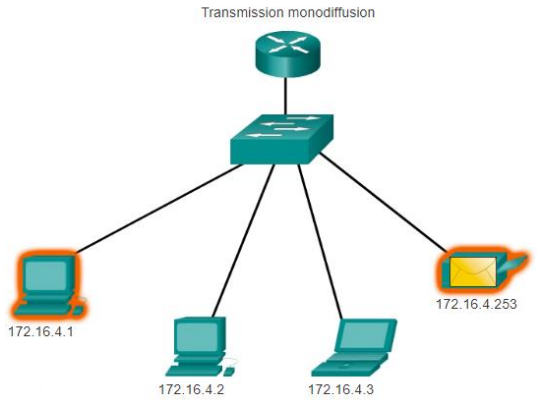


Figure 8.1. 1 : Monodiffusion

Les adresses d'hôte IPv4 sont des adresses de monodiffusion et se trouvent dans la plage d'adresses 0.0.0.0 à 223.255.255.255. Toutefois, dans cette plage, de nombreuses adresses sont réservées à un usage spécifique.

III.1.2. Diffusion

C'est un processus consistant à envoyer un paquet d'un hôte à tous les hôtes du réseau.

Puisque le trafic de diffusion est utilisé pour envoyer des paquets à tous les hôtes du réseau, les paquets utilisent des adresses de diffusion spécifiques. Lorsqu'un hôte reçoit un paquet avec comme destination une adresse de diffusion, il traite le paquet comme s'il était adressé à son adresse monodiffusion. La transmission de diffusion permet de localiser des services et périphériques spéciaux pour lesquels l'adresse n'est pas connue, ou lorsqu'un hôte doit fournir des informations à tous les hôtes sur le réseau.

Voici quelques cas d'utilisation des transmissions de diffusion :

- Mappage des adresses d'une couche supérieure à des adresses d'une couche inférieure
- Demande d'une adresse
- Échange d'informations de routage entre des protocoles de routage

Il y a deux types de diffusion : dirigée et limitée.

- **Diffusion dirigée**

  Une diffusion dirigée est envoyée à tous les hôtes d'un réseau particulier. Ce type de diffusion permet l'envoi d'une diffusion à tous les hôtes d'un réseau qui n'est pas local. Par exemple, pour qu'un hôte, situé en dehors du réseau, puisse communiquer avec les hôtes du réseau 172.16.4.0 /24,

- **Diffusion limitée**

  La diffusion limitée permet une transmission qui est limitée aux hôtes du réseau local. Ces paquets utilisent l'adresse IPv4 de destination 255.255.255.255. Les routeurs ne transmettent pas cette diffusion. Les paquets adressés à une adresse de diffusion limitée ne sont visibles que sur le réseau local. C'est la raison pour laquelle un réseau IPv4 est également appelé « domaine de diffusion ». Les routeurs forment les limites d'un domaine de diffusion.

  Par exemple, un hôte du réseau 172.16.4.0 /24 envoie une diffusion à tous les hôtes de son réseau à l'aide d'un paquet dont l'adresse de destination est 255.255.255.255

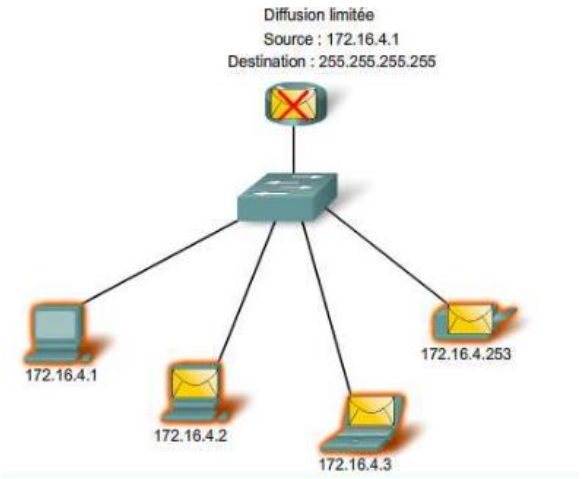


Figure 8.1. 2 : Diffusion (broadcast)

III.1.3. Multidiffusion

C'est un processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier (qui peuvent se trouver sur différents réseaux).

La transmission multidiffusion permet de conserver la bande passante du réseau IPv4. Elle réduit le volume de trafic en permettant à un hôte d'envoyer un seul paquet à un groupe d'hôtes désigné.

Voici quelques exemples de transmission multidiffusion :

- Une visioconférence
- Échange d'informations de routage entre des protocoles de routage dynamique
- Distribution de logiciels

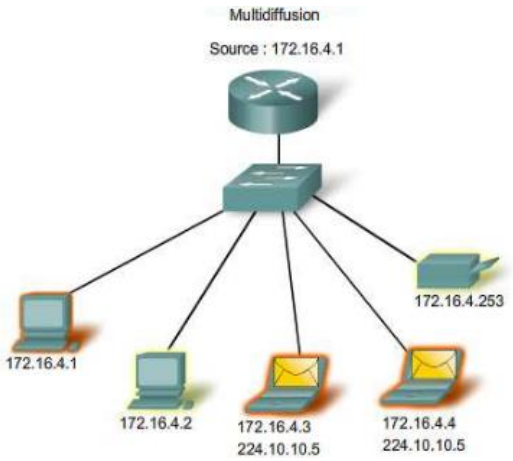


Figure 8.1. 3: Multidiffusion

III.2. Les classes des adresses IPv4

A l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement des paquets entre differents réseaux. Ces groupes ont été baptises classes d'adresses IP. Ces classes correspondent à des groupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum. Il existe quatre classes d'adresses, chacune permettant de coder un nombre différent de réseaux et de machines :

- **Classe A** : 128 réseaux et 16 777 216 hôtes (7 bits pour les réseaux et 24 bits pour les hôtes) Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

- **Classe B** : 16 384 réseaux et 65 535 hôtes (14 bits pour les réseaux et 16 bits pour les hôtes) Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.
- **Classe C** : 2 097 152 réseaux et 256 hôtes (21 bits pour les réseaux et 8 bits pour les hôtes) Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.
- **Classe D** : adresse de groupes (128 bits pour les hôtes appartenant à un même groupe) Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 1. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Figure 8.1. 4 : Les classes d'adresses (source : wapiti.enic.fr)

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	Adresses uniques	Adresses uniques
E	Non défini	240.0.0.0 - 255.255.255.255	Adresses uniques	Adresses uniques

Tableau 8.1. 1 : Espace d'adressage

III.3. Types d'adresse IPv4

- **Adresse réseau** : bits de la partie hôte mis à 0 (192.168.10.0)
- **Adresse machine** : bits de la partie hôte non tous à 0, non tous à 1 (192.168.10.1 à 192.168.10.254) Adresse diffusion : correspond à tous les hôtes du réseau. Bits de la partie hôte tous à 1 (192.168.10.255)
- **Les adresses IPv4 réservées** :
  - **Adresses réseau et de diffusion** : dans chaque réseau, les première et dernière adresse ne peuvent pas être attribuées à des hôtes
  - **Adresse de bouclage** : 127.0.0.1 est une adresse spéciale utilisée par les hôtes pour diriger le trafic vers eux-mêmes (les adresses de 127.0.0.0 à 127.255.255.255 sont réservées)

- **Adresse link-local** : les adresses de 169.254.0.0 à 169.254.255.255 (169.254.0.0/16) peuvent être automatiquement attribuées à l'hôte local
- **Adresses TEST-NET** : les adresses de 192.0.2.0 à 192.0.2.255 (192.0.2.0/24) sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau
- **Adresses expérimentales** : les adresses de 240.0.0.0 à 255.255.255.254 sont indiquées comme étant réservées

- **Les adresses IPv4 privées**

  Il existe trois blocs d'adresses IPv4 privées qui ont été réservés par Internet Assigned Numbers Authority (IANA). Ces adresses sont définies dans le document RFC 1918, Address Allocation for Private Internet. Les entreprises utilisent ces adresses sur leurs réseaux privés qui ne sont pas valides sur Internet (non routables) et ne sont pas utilisées sur des systèmes devant communiquer hors du réseau local.

Les trois blocs des adresses IPv4 privées sont décrit dans le tableau suivant

Classe d'adresses IPv4	Plage d'adresses IPv4	Masque de réseau
Classe A	10.0.0.0 - 10.255.255.255	10.0.0.0
Classe B	172.16.0.0 - 172.31.255.255	172.16.0.0
Classe C	192.168.0.0 - 192.168.255.255	192.168.0.0

Tableau 8.1. 2 : Les blocs des adresses IPv4 privées

IV. Résumé des adresses (CIDR)

Le problème de système d'adressage par classe est que le pourcentage de perte d'adresses est assez élevé. Prenons la classe A, par exemple, nous permettre d'obtenir 16 777 214 adresses IP par réseau en utilisant les masques par défaut. Si une entreprise voulait une adresse IP pour un réseau de 10 000 hôtes aurait quand même 16 767 214 d'adresses en surplus.

C'est pourquoi un nouveau système d'adressage, capable de réduire au minimum le gaspillage d'adresses IP et de faciliter considérablement le routage, a été mis en place. C'est l'adressage sans classe ou adressage CIDR.

IV.1. Présentation

CIDR est l'acronyme de *Classless Inter Domain Routing* (« routage sans classes entre domaines »). La notation CIDR a été introduite en 1993 par l'IETF (RFC 1338) et elle a été conçue pour remplacer l'adressage par classes.

Elle correspond au nombre de bit à 1 du masque de sous-réseau. Elle permet de l'aggrégation d'adresses et ainsi l'allégement de la charge de travail des routeurs d'Internet. Nous ne parlons plus de la notion des classes c'est pourquoi un masque ne peut plus être déduit d'une adresse IP unicast. Par conséquent, les protocoles de routages "classless" doivent obligatoirement accompagner les adresses IP de masque.

Les objectifs de ce nouveau système sont :

- Économiser les adresses IP.
- Faciliter le routage.

IV.2. Exemple

Prenons l'adresse machine 192.168.1.13 et le masque 255.255.255.248, nous voulons déterminer l'adresse réseau.

Le masque en binaire est 11111111.11111111.11111111.11111000

Si nous comptons le nombre de bit à "1" nous obtenons un CIDR de 29. Donc, pour l'hôte 192.168.1.13/29 nous avons maintenant capable de dire que son masque est 255.255.255.248

IV.3. Application

1. Donner les notations CIDR des hôtes suivants :

- 10.10.126.200 / 255.255.0.0
- 192.168.10.12 / 255.255.255.0

2. Donner les masques des hôtes suivants :

- 9.9.0.10/8
- 192.168.200.1/24

V. Techniques et méthodes de fragmentation des paquets

Le protocole IP définit l'unité de données de protocole ainsi que le format exact de toutes données qui transitent dans le reseau. IP inclut également un ensemble de règles qui définissent comment traiter les paquets, gérer la fonction de routage et traiter certains cas d'erreurs.

Les datagrammes peuvent être de longueur quelconque. Cependant, comme ils doivent transiter de routeur en routeur, ils peuvent être fractionnées. De sorte à s'adapter à la structure de la trame sous-jacente, c'est l'encapsulation. Pour un sous reseau, un datagramme est une donnée comme une autre. Dans le meilleur des cas, le datagramme est contenu dans une seule trame, ce qui rend la transmission plus performance.

Le but de l'environnement Internet est de cacher les sous-réseaux. C'est pourquoi, au lieu de prévoir la taille des datagrammes en fonction des contraintes des sous-réseaux, nous leur choisissons une taille convenable, puis nous les découpons en fragments, de façon qu'ils soient transportés dans de petites trames puis réassemblées. Internet ne limite pas la taille des datagrammes mais suggère que les réseaux et les passerelles puissent supporter ceux de 576 octets sans les fragments.

La couche de accès reseau (Couche 2) définit une taille limite, le « Maximum Transfer Unit. Une trame Ethernet est de taille 1500, elle peut être de 256 avec SLIP (« Serial Line IP ») sur liaison série (RS232...).

Dans ces conditions, si la couche IP doit transmettre un bloc de données de taille supérieure au MTU à employer, il y a fragmentation.

Par exemple, un bloc de 1481 octets sur Ethernet sera décomposé en un datagramme de 1480

(1480 + 20 = 1500) et un datagramme de 1 octet

Il existe une exception à cette opération, due à la présence active du bit « Don't Fragment bit » du champ FLAGS de l'entête IP. La présence à 1 de ce bit interdit la fragmentation dudit datagramme par la couche IP qui en aurait besoin. C'est une situation de blocage, la couche émettrice est tenue au courant par un message ICMP (cf. paragraphe 4) « *Fragmentation needed but don't fragment bit set »* et bien sûr le datagramme n'est pas transmis plus loin.

V.1. Fragmentation

Quand un datagramme est fragmenté, il n'est réassemblé que par la couche IP destinatrice finale. Cela implique trois remarques :

- La taille des datagrammes reçus par le destinataire final est directement dépendante du plus petit MTU rencontré ;
- Les fragments deviennent des datagrammes à part entière ;
- Rien ne s'oppose à ce qu'un fragment soit à nouveau fragmenté.

Cette opération est absolument transparente pour les couches de transport qui utilisent IP.

Quand un datagramme est fragmenté, chaque fragment comporte la même valeur de champ IDENTIFICATION que le datagramme initial.

S'il y a encore des fragments, un des bits du champ FLAGS est positionné à 1 pour indiquer « More fragment » !

Ce champ a une longueur de trois bits.

FRAGMENT OFFSET contient l'offset du fragment, relativement au datagramme initial.

Cet offset est codé sur 13 bits.

V.2. Réassemblage

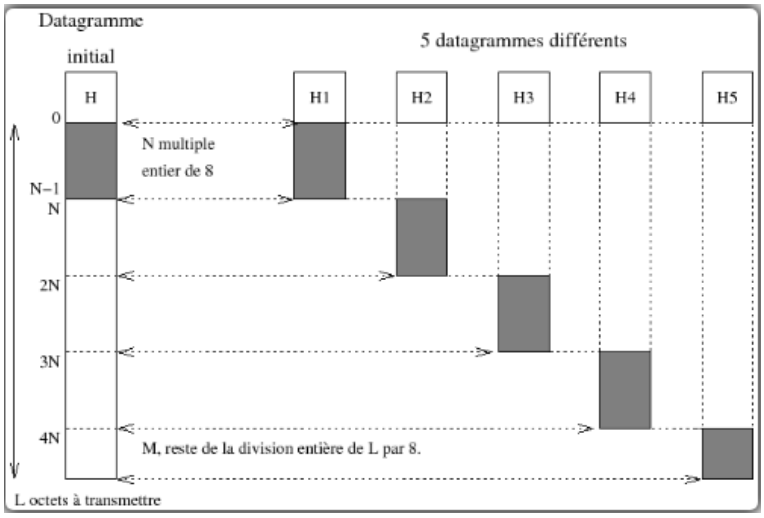
Pour tous les fragments :

- Les données doivent faire un multiple de huit octets, sauf pour le dernier fragment, évidemment ;
- Le champ TOTAL LENGTH change ;
- Chaque fragment est un datagramme indépendant, susceptible d'être à son tour fragmenté.

Pour le dernier fragment :

- FLAGS est remis à zéro ;
- Les données ont une taille quelconque.

V. 3. Exemple de fragmentation



	H1	H2	H3	H4	H5	
IDENTIFICATION	I	I	I	I	I	
FLAG	MF	MF	MF	MF	0	
OFFSET	0	N	2 x *N*	3 x *N*	4 x *N*	
TOTAL LENGTH	*H+N*	*H+N*	*H+N*	*H+N*	*H+M*	
HEADER CHECKSUM	C_1	C_2	C_3	C_4	C_5	

Figure 8.1. 5: Exemple de fragmentation

Conclusion

Nous concluons que le IPv4 possède des limites au niveau de l'espace de l'adressage qui nous a donné la nécessite de migrer vers IPv6 ainsi que des problèmes au niveau de l'entête de paquet IP à savoir :

- Son entête comporte deux problèmes, la somme de contrôle (checksum) doit être calculée à chaque traitement de datagramme, chaque routeur doit analyser le contenu du champ option.

- Sa configuration nécessite au moins trois informations que sont l'adresse, le masque de sous-réseau et la route par défaut.
- Son absence de sécurité est insupportable. Issu d'un monde fermé où la sécurité n'était pas un problème, le datagramme de base n'offre aucun service de confidentialité, d'intégrité et d'authentification.
- Son absence de qualité de service ne répond pas aux exigences des protocoles applicatifs modernes (téléphonie, vidéo, jeux interactifs en réseau...). Le champ TOS n'est pas suffisant et surtout est interprété de manière inconsistante par les équipements

Leçon 2 : Création des sous réseaux

Objectif général	• Connaitre les principes de segmentation d'un réseau IPv4 en sous réseaux
Objectifs spécifiques	• À l'aide d'un réseau et d'un masque de sous-réseau, calculer le nombre d'adresses d'hôte disponibles • Décrire les avantages des masques de sous-réseau de longueur variable (VLSM) • Calculer le masque de sous-réseau nécessaire pour répondre aux besoins d'un réseau
Volume horaire	• Cours : 1,5h
Mots clés	• Découpage classique, VLSM, masque sous réseau…

Introduction

La segmentation d'un réseau local en sous réseaux permet d'optimiser l'espace d'adressage IPv4 32 bits qui est déjà limité et de réduire la taille des tables de routage d'un inter réseau étendu.

Pour la création des sous-réseaux, l'administrateur réseau alloue (emprunte) des bits de la partie ID_HOST pour la partie ID_NET afin d'utiliser des réseaux supplémentaires. Les bits alloués de la partie ID_HOST aux nouvelles adresses réseau sont appelés **numéro de sous-réseau**.

I. La segmentation des réseaux

La création des sous réseaux est une technique qui permet de diviser un réseau local d'une entreprise comportant un nombre élevé d'hôtes en des sous-réseaux plus petits selon les besoins de l'entreprise en personnalisant les masques de sous-réseaux.

Prenons l'exemple d'une entreprise, son réseau local comporte 500 hôtes, nous pourrons le segmenter en 4 sous-réseaux de 125 hôtes.

I.1. Besoin de création des sous réseaux

Les réseaux locaux de taille important devraient être segmentés en sous-réseaux plus petits en créant des groupes de périphériques et de services pour une bonne surveillance du trafic notamment le trafic de diffusion dans les sous réseaux créés. La création des sous réseaux au sein d'une entreprise nous permet de réduire le trafic total et par suite nous aurons une amélioration des performances de ce dernier.

I.2. Notions de bases sur les sous réseaux

La création des sous-réseaux consiste à segmenter un réseau local en segments plus petits appelés sous-réseaux. Chaque sous réseau est considéré comme un réseau à part. Un routeur est nécessaire pour que les périphériques des différents réseaux et sous-réseaux puissent communiquer. Chaque interface de routeur doit comporter une adresse d'hôte IPv4 qui appartient au réseau ou au sous-réseau auquel elle est connectée. Les périphériques d'un réseau et d'un sous-réseau utilisent l'interface de routeur associée à son réseau local (LAN) comme passerelle par défaut.

I.3. Application

Soit la topologie suivante

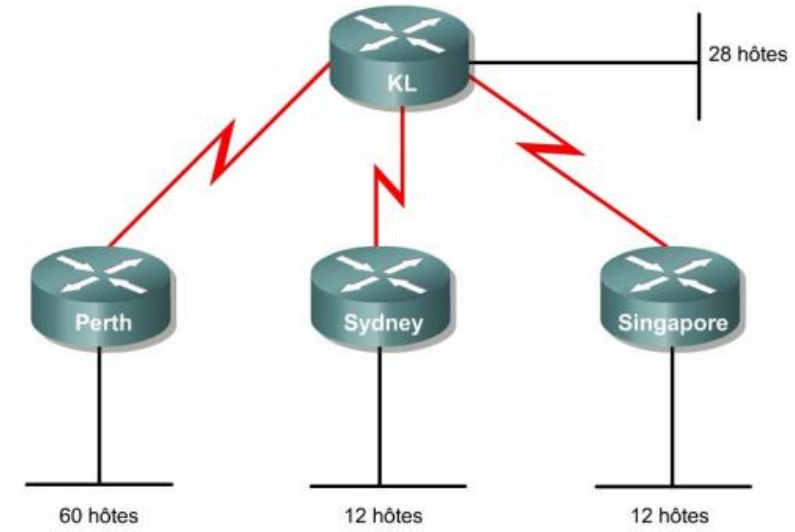


Figure 8.2. 1 : Topologie réseau

Combien de sous réseaux créés dans cette topologie ?

I.3. Les formules de calcul des sous réseaux

Deux considérations sont à prendre en compte lors de la planification des sous-réseaux :

- Nombre de sous-réseaux nécessaires
- Nombre d'adresses d'hôtes nécessaires

Pour déterminer le nombre de sous réseaux

- Soit **n** le nombre de bits empruntés de la partie ID_HOST
- Nombre de sous réseaux = $\mathbf{2^n}$

Pour déterminer le nombre d'hôtes par sous réseaux

- Soit **n** le nombre de bits de la partie ID_HOST
- Nombre d'hôtes par sous réseaux = $\mathbf{2^n - 2}$

La première et la dernière adresse des adresses disponibles présentent l'adresse réseau et adresse de diffusion.

I.4. Exemple

Une entreprise veut créer 3 sous réseaux. L'adresse réseau utilisée au sein du réseau est 192.168.20.0

Le nombre de bits empruntées : $\mathbf{2^n = 3}$ d'où **n= 2**, nous empruntons 2 bits de la partie ID_HOST.

L'adresse 192.168.20.0 fait partie de la classe C, l'ID_HOST s'écrit sur 8 bits.

Nombre d'hôtes par sous réseaux= $\mathbf{2^n - 2 = 2^{8-2} - 2}$

II. Les techniques de segmentation des réseaux

II.1. La segmentation traditionnelle

La méthode classique de segmentation crée des sous-réseaux de même taille. Chaque sous-réseau d'un schéma classique utilise le même masque de sous-réseau. Nous avons le même nombre d'adresses d'hôtes attribué à chaque sous-réseau.

II.2. Exemple

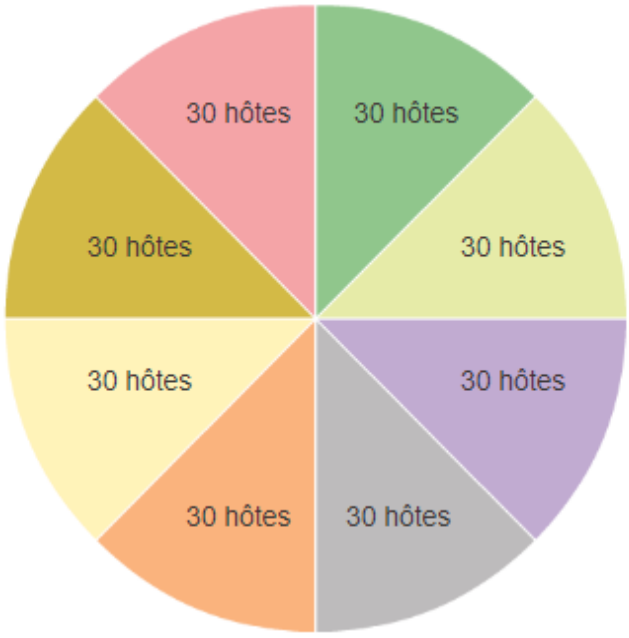


Figure 8.2. 2: découpage classique

La figure si dessus comporte 8 sous réseaux, chaque sous réseau supporte 30 hôtes.

Les sous-réseaux qui n'ont pas besoin de la totalité ont des adresses inutilisées. Par exemple, les liaisons WAN n'ont besoin que de 2 adresses. Les masques de sous-réseau de longueur

variable (VLSM, Variable Length Subnet Mask) ou la segmentation d'un sous-réseau optimisent l'utilisation des adresses.

II.3. Application découpage classique

Le *CCK* dont dépend votre institut vient de vous attribuer l'adresse IP 193.100.11.0. Vous devez créer 7 sous-réseaux distincts pour les 7 succursales de l'institut, à partir de cette adresse IP.

1. Quel masque de sous-réseau devez-vous utiliser ?
2. Combien d'adresses IP (machines ou routeurs) pourra recevoir chaque sous-réseau ?
3. Quelle est l'adresse de broadcast du 5ième sous-réseau utilisable ?

II.4. Les masques de sous-réseau de longueur variable (VLSM)

La méthode VLSM permet de diviser un réseau local d'une entreprise en parties inégales. Avec la méthode VLSM, le masque de sous-réseau varie selon le nombre de bits empruntés pour le sous-réseau, d'où la partie « variable » de cette méthode.

La création de sous-réseaux VLSM est similaire à la création de sous-réseaux classique car des bits de la partie ID_HOST sont empruntés pour créer des sous-réseaux. Les formules de calcul du nombre d'hôtes par sous-réseau et du nombre de sous-réseaux créés s'appliquent également. La différence réside dans le fait que la segmentation nécessite plus d'une opération. Avec le VLSM, **le réseau est divisé en sous-réseaux qui sont eux-mêmes divisés en sous-réseaux**. Ce processus peut être **répété plusieurs fois** de manière à créer des sous-réseaux de différentes tailles.

II.5. Application

Avec la même adresse IP attribuée que dans l'application précédente, vous désirez prendre en compte des exigences supplémentaires. En effet, sur les 7 succursales, 1 nécessitant 80 adresses IP, 3 nécessitent entre 25 et 30 adresses IP tandis que les 3 autres peuvent se contenter d'une dizaine d'adresses.

1. Détaillez les 7 adresses de sous-réseaux finalement choisies avec leurs masques respectifs.

2. Quel est le nombre total d'adresses pouvant être utilisées dans cette configuration ? Comparez avec la solution précédente.

Conclusion

La segmentation d'un réseau local consiste à le décomposer en sous-réseaux de petites tailles a fon d'améliorer les performances de ce dernier. La segmentation des sous-réseaux, ou l'utilisation des masques de sous-réseau de longueur variable (VLSM), permet d'éviter le gaspillage des adresses.

Leçon 3 : Le routage et les fonctions NAT & PAT

Objectif général	• Comprendre le routage IP. • Comprendre les connaissances de base sur les fonctions NAT et PAT
Objectifs spécifiques	• Acquérir les connaissances de base sur le routage statique. • Acquérir les connaissances de base sur le routage dynamique • Décrire les principales caractéristiques et fonctionnalités d'un routeur • Connaitre le processus d'encapsulation et de désencapsulation utilisé par les routeurs lors de la commutation des paquets entre les interfaces • Comprendre le principe de la NAT statique et dynamique • Comprendre le principe de la PAT
Volume horaire	• Cours : 1,5h
Mots clés	• Routage IP, routage direct, routage indirect, statique, dynamique, protocole de routage, NAT, PAT, adresse privée, adresse publique…

Introduction

Nous détaillons comment les informations transitent d'un réseau à un autre. Nous verrons notamment en premier lieu les divers types de routage, en deuxième lieu nous verrons comment les hôtes possédant des adresses privées peuvent également échanger des données avec d'autres hôtes font partie des réseaux distants.

I. Le routage IP

Les réseaux sont reliés les uns aux autres, et nous passons souvent par plusieurs réseaux pour en joindre un autre. Notamment, nous utilisons un équipement de couche 3 (Internet) pour interconnecter les divers réseaux. C'est le routeur qui se charge de bien acheminer les paquets de la source à la destination autrement dit de choisir le meilleur chemin existant entre l'émetteur et le récepteur.

I.1. Le routeur

Le routeur est un micro-ordinateur possédant des ressources pareillement comme l'ordinateur, des mémoires (ROM, RAM…) et un processeur qui sont utilisés dans les taches du routeur.

Les routeurs interconnectent plusieurs réseaux. Ils possèdent des interfaces, chacune définit un réseau IP différent. Ils déterminent le meilleur chemin pour l'envoi du paquet d'une source à une destination en utilisant leur **table de routage** qui est un fichier sauvegardé dans la mémoire RAM contenant des informations sur les éléments suivants

- Routes connectées directement
- Routes distantes
- Réseau ou tronçon suivant

Ils assurent l'encapsulation des paquets et ils les transmettent vers la destination.

Pour connecter un périphérique à un réseau, il fallait configurer ce dernier avec les informations IP suivantes :

- **Adresse IP** qui identifie l'hôte sur le réseau local
- **Masque de sous réseau** qui identifie le sous réseau de l'hôte
- **Passerelle par défaut** identifiant l'interface de routeur auquel un paquet est envoyé lorsque la destination n'est pas sur le même sous réseau.

Un équipement final sans passerelle par défaut ne peut pas communiquer avec d'autres équipements des sous réseaux différents.

Un routeur reliant deux segments peut atteindre chaque segment directement, c'est le **routage direct**.

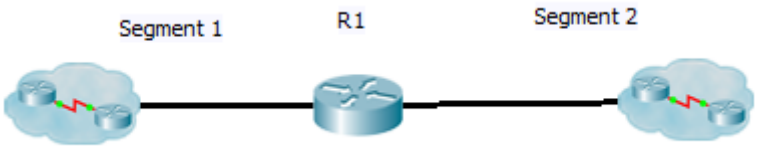


Figure 8.3. 1 : Routage direct

Un routeur doit utiliser le **routage indirect** s'il retransmet les datagrammes à un réseau auquel il n'est pas directement rattaché. Dans ce cas, les routeurs utilisent des routes statiques et des routes dynamiques pour atteindre des réseaux distants et remplir leurs tables de routages.

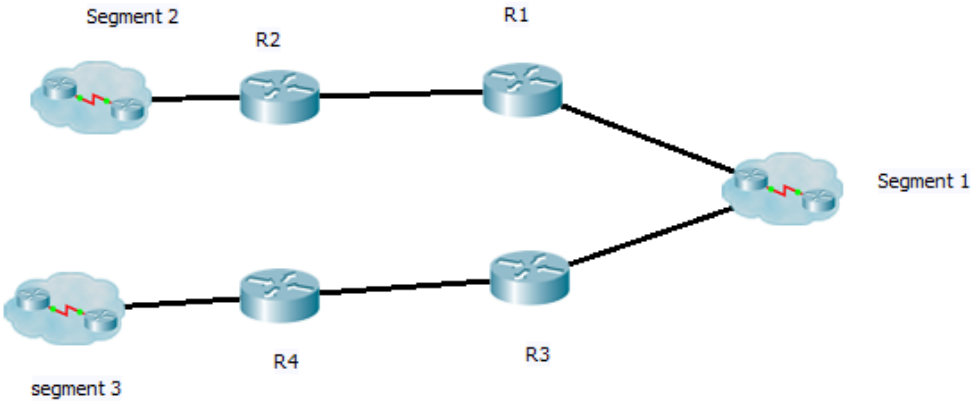


Figure 8.3. 2: Routage indirect

I.2. Le routage statique

Les routes sont configurées manuellement par l'administrateur reseau et qui définissent un chemin explicite entre deux périphériques reseau. En cas de modification de la topologie reseau, les routes (le contenu de la table de routage) sont mises à jour manuellement.

Cette méthode de routage est avantageuse dans le cas d'un réseau local de petite taille ou la sécurité est renforcée et les ressources sont contrôlées.

Cette méthode n'est pas convenable dans le cas d'un réseau de grandes tailles ou l'administrateur ne pourrait pas tout contrôler manuellement. Parlant de l'automatisation de la tache de routage.

I.3. Le routage dynamique

Dans le routage statique, l'administrateur réseau ajoute manuellement les routes (chemins) sur les routeurs. Ce type de routage n'est pas très efficace ou le risque d'omettre des erreurs est élevé ainsi qu'il ne convient qu'aux des réseaux de petites tailles. C'est pourquoi il est nécessaire d'automatiser cette tâche, c'est le rôle des protocoles de routage. L'ajout des routes dans la table de routage et la mise à jour sont automatiques.

Les objectifs des protocoles de routages dynamiques

- Le rôle principal est de découvrir dynamiquement les routes vers les réseaux d'un inter réseau et les inscrire dans la table de routage sur routeur.
- S'il existe plus d'une route vers un réseau, inscrire la meilleure route dans la table de routage.
- Détecter les routes qui ne sont plus valides et les supprimer de la table de routage.
- Ajouter le plus rapidement possible de nouvelles routes ou remplacer le plus rapidement les routes perdues par la meilleure route actuellement disponible.

Cette section sera détaillée dans le module routage au second semestre.

II. Translation des adresses

Nous utilisons le protocole IPv4 actuellement. Ce protocole offre un champ d'adressage limité et insuffisant pour permettre à tout terminal informatique de disposer d'une adresse IP. Pour faire face à cette pénurie d'adresses, et en attendant IPv6, qui offrira un nombre d'adresses beaucoup plus important sur 128 bits, il faut recourir à un partage de connexion en utilisant la translation d'adresse, ou NAT (Network Address Translation). Le NAT consiste à établir des relations entre les adresses privées dans un réseau et les adresses publiques pour se connecter à Internet. Ce mécanisme est utilisé fréquemment chez les entreprises et les particuliers.

II.1. NAT

Les adresses IP privées conviennent généralement pour couvrir un réseau privé, de particulier ou d'entreprise, mais pas pour communiquer directement avec les réseaux publics.

Pour résoudre ce problème et permettre à un terminal disposant d'une adresse IP privée de communiquer avec le réseau public, le processus de NAT fait intervenir une entité tierce entre un terminal, ayant une adresse IP privée, et tout autre terminal ayant une adresse IP publique. Cette translation d'adresse est effectuée principalement sur les routeurs de bordure d'une entreprise connectée à Internet. Le réseau utilisant les adresses IP privées est ainsi appelé le réseau interne (inside), tandis que la partie du réseau utilisant des adresses IP publiques (Internet) est appelé le réseau externe (outside).

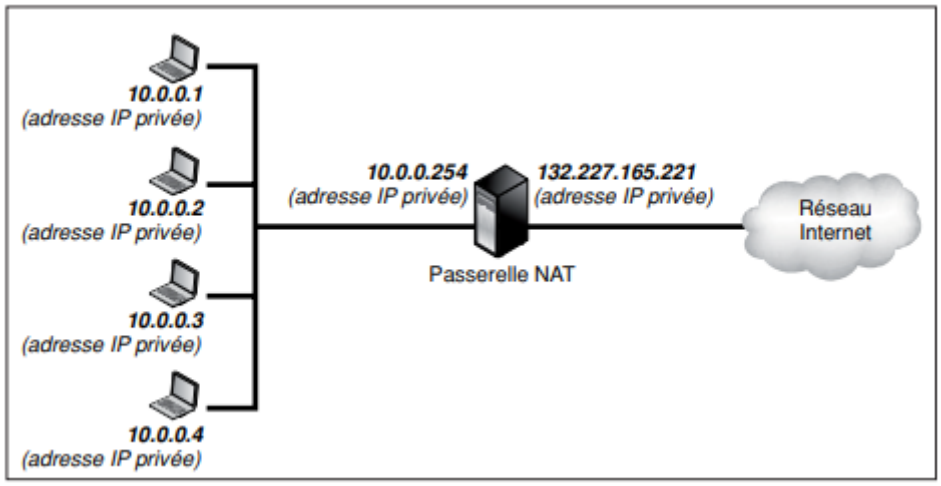


Figure 8.3. 3 : NAT

Quand un utilisateur du réseau interne (inside) souhaite communiquer avec un hôte du réseau externe (outside), le routeur reçoit le paquet avec l'adresse IP privée et réécrit le paquet en changeant l'adresse IP source avec l'adresse IP public du routeur (c'est l'opération de translation).

Le routeur consulte ensuite sa table de routage pour acheminer le paquet jusqu'à la bonne destination. Le destinataire recevra le paquet avec comme source l'adresse IP public du routeur et non l'adresse IP privée de l'hôte qui envoie le paquet dans le réseau interne.

Les traductions NAT peuvent avoir de nombreuses utilisations et peuvent indifféremment être attribuées de façon statique ou dynamique.

II.1.1. NAT statique

La NAT statique consiste à associer une adresse IP privée fixe et permanente à une adresse IP publique fixe et permanente. Ne pouvant se connecter sur internet avec une adresse IP privée, le routeur doit remplacer l'adresse IP source par l'adresse IP de l'interface publique donnée par le FAI.

Exemple

Gateway(config)#ip nat inside source static 10.10.10.10 199.99.9.33

II.1.2. NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local. Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique. Elle maintient cette correspondance pour une période fixe, mais renouvelable selon l'activité de l'utilisateur, qui assure le suivi des communications.

Exemple

Router(config)#ip nat pool public-access 199.99.9.40 199.99.9.62 netmask 255.255.255.224

Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255

Router(config)#ip nat inside source list 1 pool public-access

II.2. PAT

Le PAT (Port Address Translation) ou Overloading permet d'attribuer une seule adresse IP publique pour la translation de plusieurs adresses IP privées. Chaque utilisateur est différencié grâce à un numéro de port unique qui lui est attribué lorsqu'il souhaite communiquer.

Etant donné qu'il existe 65536 ports différents, un routeur pourrait translater jusqu'à 65536 adresses IP privées différentes. Cependant en réalité, un équipement ne peut gérer en moyenne que la translation d'environ 4000 ports par adresse IP publique.

Conclusion

Le rôle principal d'un routeur est d'interconnecter plusieurs réseaux et d'acheminer les paquets d'un réseau à l'autre. Il se base sur la table de routage qui est une liste de réseaux connus par le routeur. Ces réseaux sont ajoutés par deux manières, statiquement ou il n'y a pas de surcharge pour le routeur mais nécessitent de la maintenance si la topologie change. La deuxième méthode est d'une manière dynamique en consommant de la CPU, de la BP et de l'espace mémoire mais en prenant en charge les changements de la topologie. La translation des adresses NAT possède plusieurs atouts à savoir la gestion simplifiée du réseau en laissant l'administrateur libre d'adopter le plan d'adressage interne qu'il souhaite.