

Subnetting – Translation d'adresses

- Intérêt du subnetting
- Principe de fonctionnement du subnetting et exemples
- Translation d'adresses – NAT
- Port Forwarding (à faire après les prochains modules)

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Origine

- A l'origine
 - Dans la plupart des entreprises, les trames sont transmises en mode diffusion (broadcast). Dans ce type de transmission, les trames sont diffusées sur le support et sont donc visibles de toutes les stations.
- Qu'est-ce que le subnetting (segmentation en sous-réseaux) ?
 - Subdivision d'un réseau en plusieurs réseaux = extension du plan d'adressage initial
 - Segmentation en plusieurs domaines de broadcast

2

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Objectif et intérêt

■ Intérêt

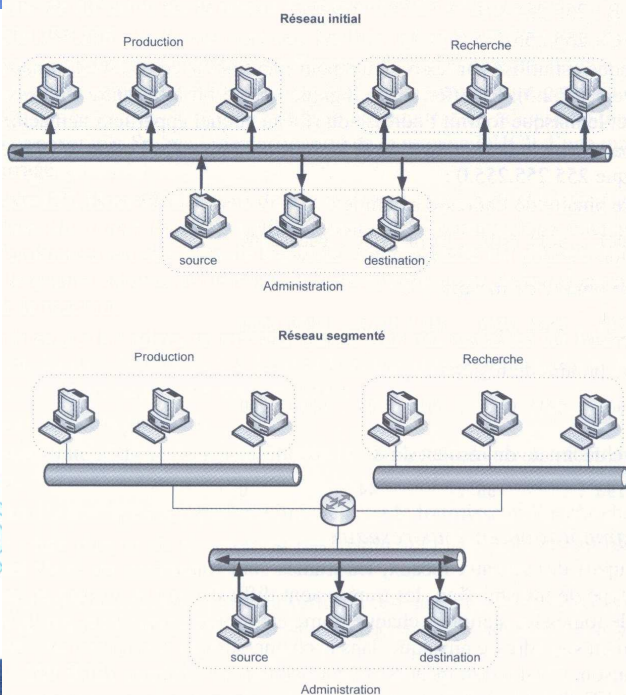
- Une meilleure gestion de l'espace d'adressage disponible
 - Structurer son réseau à l'image de l'organisation de l'entreprise (Production, R&D, ...)
- Dans un réseau local Ethernet TCP/IP il peut y avoir des problèmes de charge de réseau qui apparaissent pour plusieurs raisons :
 - diffusion trop importante (broadcast)
 - trop grande quantité de machines sur un seul réseau logique d'où un trafic trop important.
- Interconnexion de réseaux hétérogènes : Ethernet, Wifi
- Dans un réseau local, par sécurité, on peut vouloir isoler certains utilisateurs de certaines ressources.

Pour tout ces cas de figure, tout en gardant les mêmes adresses TCP/IP, la segmentation en sous-réseaux (subnetting) associé à l'utilisation de routeurs peut être une solution.

3

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Illustration

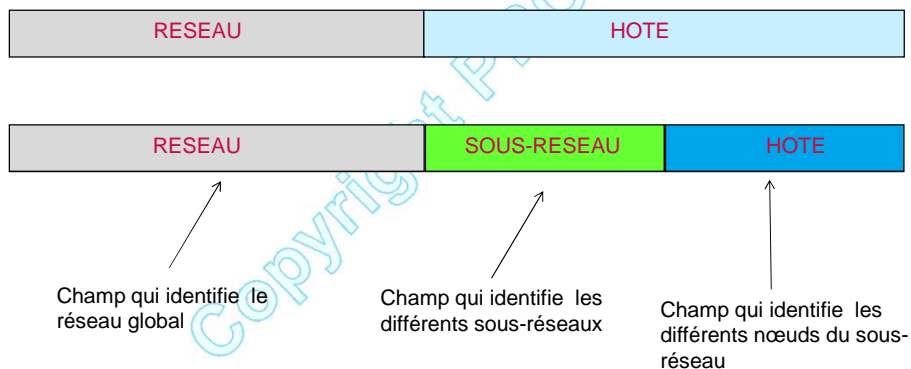


4

PRONETIS©20

Subnetting : Principe

- La technique de subnetting décompose l'adresse IP en 3 champs
- La partie HOTE dans le plan d'adressage initial est subdivisée en "*partie SOUS-RESEAU*" + "identification HOTE sur ce sous-réseau" :



5

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Rappel sur les masques de classes A,B,C

Réseau

Hôte

- Classe A
 - 8 bits partie réseau, 24 bits partie hôte
 - Masque par défaut : 255.0.0.0
- Classe B
 - 16 bits partie réseau, 16 bits partie hôte
 - Masque par défaut : 255.255.0.0
- Classe C
 - 24 bits partie réseau, 8 bits partie hôte
 - Masque par défaut : 255.255.255.0

6

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : méthode de calcul

- Le choix du découpage dépend des perspectives d'évolution du site :
 - nombre de postes de travail connectés au site
 - nombre de sous-réseaux nécessaires
- Méthode classique
 1. Empruntez le nombre de bits suffisants en fonction des contraintes (nombre de postes de travail ou nombre de sous-réseaux)
 2. Calculez le nouveau masque de sous réseau
 3. Identifiez les différentes plages d'adresses IP
 4. Identifiez les plages d'adresses non utilisables
 5. Identifiez les adresses de réseau et de broadcast
 6. Déterminez les plages d'adresses utilisables par les hôtes

7

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Illustration

- Calcul du nombre d'hôtes
 - Calcul du nombre de bits nécessaires pour coder le nombre d'hôtes souhaités

Réseau

Sous-réseaux

Hôte

- Exemple
 - On cherche à obtenir des sous-réseaux comportant 12 hôtes
 - 12 en binaire donne: 0000 1100, il faut donc 4 bits (16 possibilités) pour coder les hôtes demandés

8

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Illustration

- Calcul du nombre de bits nécessaires pour coder le nombre de SR souhaités

Réseau	Sous-réseaux	Hôte
--------	--------------	------

■ Exemple

- On cherche à obtenir 9 sous-réseaux
- 9 en binaire donne: 0000 1001, il faut donc 4 bits (16 possibilités) pour coder les sous-réseaux demandés

9

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Illustration

- On souhaite subdiviser la Classe C suivante :
192.168.10.0 en 9 sous-réseaux de 12 hôtes chacun

Masque	Réseau	Sous-réseaux	Hôte
32 bits	24 bits	+ 4 bits	+ 4bits
	[1111 1111 . 1111 1111 . 1111 1111] . [1111] [0000]		

- Le nouveau masque de sous-réseau correspondant à nos attentes est donc le 255.255.255.240

10

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous réseau

- Adresse IP : 160.55.12.120
- Masque de sous-réseau : 255.255.255.128
- A quelle classe appartient l'adresse IP ?
 - A la classe B , avec un masque de réseau par défaut à 255.255.0.0
- Quelle est l'adresse réseau ?
 - Il s'agit d'une adresse de classe B, l'adresse du réseau est donc donnée par les deux premiers octets de l'adresse, complétée par des « 0 », soit 160.55.0.0.
 - Opération booléenne « ET logique » entre l'adresse IP et le masque de réseau de la classe associée

11

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous réseau

- Quelle est l'adresse étendue du réseau ?
 - L'adresse étendue du réseau s'obtient avec le masque de sous-réseau défini. Le masque de sous-réseau dans cet exemple est : 255.255.255.128.
 - Opération booléenne « ET logique » entre l'adresse IP et le masque de sous-réseau
 - Identifiant du réseau étendu : 160.55.12.0
 - Numéro du sous-réseau : 0.0.12.0
- Quelle est l'adresse de l'hôte ?
 - L'adresse de l'hôte au sein du sous-réseau est donnée par la partie restante.
 - Opération booléenne « ET logique » entre l'adresse IP et le complément à un du masque
 - Le numéro de l'hôte est 0.0.0.120 dans le sous-réseau numéro 0.0.12

12

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous réseau

- Identification de l'adresse de Broadcast dirigé
 - L'adresse de diffusion dirigée, s'obtient en mettant tous les bits à 1 de la partie Hôte
 - L'adresse de diffusion dans ce sous-réseau est : 160.55.12.127
- Décompte des hôtes et des sous-réseaux
 - Le nombre d'hôtes par sous-réseau est : $2^7 - 2 = 126$
 - Le nombre de sous-réseau est : $2^9 = 512$ sous-réseaux

13

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

	160	55	12	120
Adresse IP (classe B) =	1 0 1 0 0 0 0 0	0 0 1 1 0 1 1 1	0 0 0 0 1 1 0 0	0 1 1 1 1 0 0 0
Préfixe réseau /25 =	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 0 0 0 0 0 0 0
Numéro de sous-réseau =	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 0	0 0 0 0 0 0 0 0
Numéro d'hôte =	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 1 1 1 1 0 0 0
Adresse de diffusion =	1 0 1 0 0 0 0 0	0 0 1 1 0 1 1 1	0 0 0 0 1 1 0 0	0 1 1 1 1 1 1 1
ID sous-réseau du sous-réseau =	1 0 1 0 0 0 0 0	0 0 1 1 0 1 1 1	0 0 0 0 1 1 0 0	0 1 1 1 0 0 0 0

Diagram annotations: A red box highlights the '00001100' bits in the 'Numéro de sous-réseau' row. A red arrow points from this box to the '12' value below it. A vertical dashed line separates the '12' and '120' columns. A horizontal double-headed arrow labeled 'Numéro sous-réseau' spans the '12' column. Another horizontal double-headed arrow labeled 'Num hôte' spans the '120' column. A vertical double-headed arrow labeled 'Préfixe réseau' spans the first three columns.

14

Exemple détaillé – Utilisation d'un masque de sous réseau

- Voici les 512 sous-réseaux possibles :
 - Identifiant de sous-réseau – Pool d'adresses IP disponibles - Adresse de broadcast
 - SR N°1 : **160.55.12.0** [160.55.12.1 à 160.55.12.126] et **160.55.12.127**
 - SR N°2 : **160.55.12.128** [160.55.12.129 à 160.55.12.254] et **160.55.12.255**
 - SR N°3 : **160.55.13.0** [160.55.13.1 à 160.55.13.126] et **160.55.13.127**
 - SR N°4 : **160.55.13.128** [160.55.13.129 à 160.55.13.254] et **160.55.13.255**
 -
 -
 - SR N°512 : **160.55.255.128** [160.55.255.129 à 160.55.255.254] et **160.55.255.255**

15

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous réseau

- Adresse **91.198.174.2** et un masque de **255.255.224.0 (19 bits)**
- Il s'agit d'une classe A - l'identifiant de réseau est 91.0.0.0
01011011.11000110.10101110.00000010 (91.198.174.2)
AND 11111111.00000000.00000000.00000000 (255.0.0.0)
= 01011011.00000000.00000000.00000000 (91.0.0.0)

Identifiant du réseau : 91.0.0.0

- L'adresse étendue du réseau est : 91.198.160.0
01011011.11000110.10101110.00000010 (91.198.174.2)
AND 11111111.11111111.11100000.00000000 (255.255.240.0)
= 01011011.11000110.10100000.00000000 (91.198.160.0)

Identifiant de sous-réseau : 91.198.160.0

16

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous réseau

- L'adresse de l'hôte au sein du sous-réseau est 0.0.14.2
 01011011.11000110.10101110.00000010
 AND 00000000.00000000.00011111.11111111 (complément à un du masque de sous-réseau)
 = 00000000.00000000.00001110.00000010

Numéro de l'hôte : 0.0.14.2

- En résumé

	Notation décimale	Notation binaire
Adresse IPv4	91.198.174.2	01011011.11000110.10101110.00000010
Masque par défaut (classe A)	255.0.0.0	11111111.00000000.00000000.00000000
Adresse du réseau	91.0.0.0	01011011.00000000.00000000.00000000
Masque de sous-réseau	255.255.224.0	11111111.11111111.11100000.00000000
Adresse de réseau étendue	91.198.160.0	01011011.11000110.10100000.00000000
Adresse du sous-réseau	0.198.160.0	00000000.11000110.10100000.00000000
Adresse de l'hôte	0.0.14.2	00000000.00000000.00001110.00000010

17

Subnetting : Espace de numérotation d'un masque

- **Pratique conseillée selon la RFC 950*** :
 - Ne pas utiliser le premier et le dernier sous-réseaux - **Nb sous-réseau = $2^n - 2$**
 - L'utilisation des valeurs tout à <0> ou tout à <1> du champ « sous-réseau » est déconseillée .
 - Risque de dysfonctionnement

RESEAU	SOUS-RESEAU	HOTE
--------	-------------	------

- Espace de numérotation d'un masque de sous-réseau de « n » bits
 - **Nb sous-réseau = $2^n - 2$** (n = bits défini par le masque de sous-réseau)

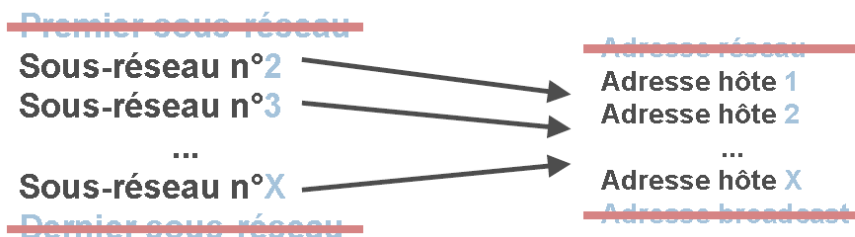
*Même si la RFC 950 a été déclarée obsolète dans la RFC 1878, il est fortement conseillé de la respecter.

18

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Subnetting : Unicité du masque sur un même réseau

- Ne pas utiliser le premier ni le dernier sous-réseau



19

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Exemple détaillé – Utilisation d'un masque de sous-réseau

- Dans l'exemple précédent : 160.55.12.0 / 255.255.255.128
Le nombre de sous-réseau est : $2^9 = 512$ sous-réseaux
Après rectification de la RFC950 : $2^9 - 2 = 510$ sous-réseaux
- Voici les 512 sous-réseaux possibles :
 - Identifiant de sous-réseau – Pool d'adresses IP disponibles - Adresse de broadcast
 - SR N°1 : **160.55.12.0** [160.55.12.1 à 160.55.12.126] et **160.55.12.127**
 - SR N°2 : **160.55.12.128** [160.55.12.129 à 160.55.12.254] et **160.55.12.255**
 - SR N°3 : **160.55.13.0** [160.55.13.1 à 160.55.13.126] et **160.55.13.127**
 - SR N°4 : **160.55.13.128** [160.55.13.129 à 160.55.13.254] et **160.55.13.255**
 - - - - -
 - - - - -
 - SR N°512 : **160.55.255.128** [160.55.255.129 à 160.55.255.254] et **160.55.255.255**

20

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Masque de sous-réseau par défaut – Valeurs de préfixes

Préfixe réseau	Masque de sous-réseau
/1	128.0.0.0
/2	192.0.0.0
/3	224.0.0.0
/4	240.0.0.0
/5	248.0.0.0
/6	252.0.0.0
/7	254.0.0.0
/8	255.0.0.0
/9	255.128.0.0
/10	255.192.0.0
/11	255.224.0.0
/12	255.240.0.0
/13	255.248.0.0
/14	255.252.0.0
/15	255.254.0.0
/16	255.255.0.0
/17	255.255.128.0
/18	255.255.192.0
/19	255.255.224.0

21

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Masque de sous-réseau par défaut – Valeurs de préfixes (suite)

Préfixe réseau	Masque de sous-réseau
/20	255.255.240.0
/21	255.255.248.0
/22	255.255.252.0
/23	255.255.254.0
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252
/31	255.255.255.254
/32	255.255.255.255

22

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Mémo

Pour convertir en binaire les masques qui ne correspondent pas à des frontières d'octet, vous pouvez utiliser la table suivante

Valeur décimale	Représentation binaire
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Translation d'adresse - NAT

NAT - Network Address Translation

- La translation d'adresse (ou NAT) est nécessaire lorsqu'un réseau utilise une adresse privée non routable sur Internet. Cela nécessite l'utilisation d'un équipement dédié : routeur ou pare-feu (firewall).

25

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- Contexte – Adresses publiques et Adresses privées **RFC 1918**
 - Pour permettre l'interconnexion de réseau, il faut garantir l'unicité des adresses
 - L'IANA attribue à chaque réseau un identifiant unique : une plage d'adresses publiques
 - Mais tous les réseaux n'ont pas besoin d'interconnexion via un réseau public, dans ce cas, l'unicité des d'adresses au plan mondial n'est pas nécessaire.
 - Par conséquent, les entreprises et les particuliers qui disposent de leur propre réseau (réseau privé) sans aucun besoin d'interconnexion vers l'extérieur peuvent utiliser n'importe quelle adresse IP.
 - Afin de prévenir dans les réseaux privés, une éventuelle utilisation anarchique des adresses, il a été envisagé de réserver des plages d'adresse à ces réseaux **RFC1918**

26

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

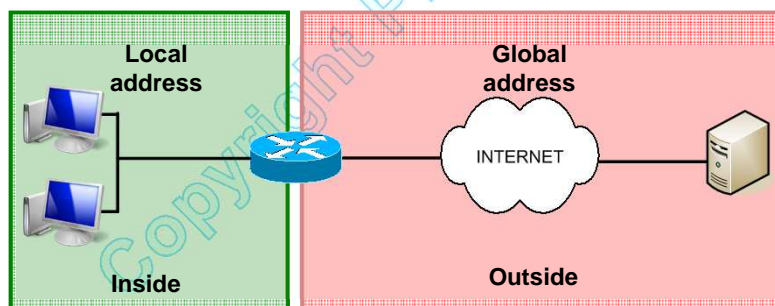
- Plages d'adresses privées RFC 1918
 - 10.0.0.0 à 10.255.255.255 – 1 réseau
 - 172.16.0.0 à 172.31.255.255 – 16 réseaux
 - 192.168.0.0 à 192.168.255.255 – 256 réseaux
- Que faire lorsque un réseau privé a des besoins d'accès à un réseau public (Internet par exemple) ?
 - Renommer toutes les stations avec des adresses publiques ?
 - Réaliser une conversion d'adresse, c'est-à-dire de mettre en œuvre un mécanisme qui établit une correspondance entre une adresse privée et une adresse publique ?

27

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- **Local address** : adresse privée utilisée dans la partie interne (inside) du réseau.
 - Ex : LAN de l'entreprise
- **Global Address** : adresse publique utilisée dans la partie externe du réseau (outside)
 - Ex : Internet



28

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- Il y a deux types de NAT
 - Statique
 - Dynamique

29

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

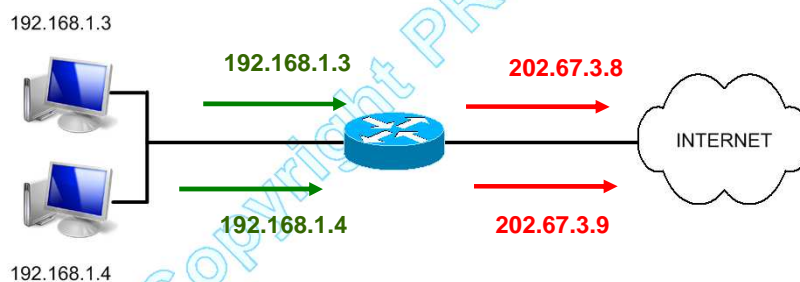
- NAT statique
 - Le principe du **NAT statique** consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.
- **Exemple d'utilisation** : hébergement d'un serveur WEB local qui doit être visible à partir d'Internet.

30

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- NAT statique : (1 -> 1)
 - L'ordinateur avec l'adresse IP 192.168.1.3 sera traduit en 202.67.3.8 de manière permanente.
 - L'ordinateur avec l'adresse IP 192.168.1.4 sera traduit en 202.67.3.9 de manière permanente.



NAT remplace l'adresse locale du champ adresse source de l'en-tête IP par l'adresse globale de son interface

31

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

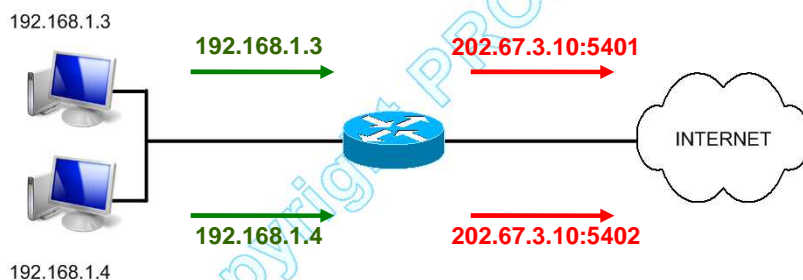
- NAT Dynamique – ou appelé *NAPT (Network Address Port Translation)*
 - Chaque utilisateur du LAN aura une seule adresse globale dans un pool d'adresses IP globales disponibles. La correspondance est automatique.
 - Le PAT (Port Address Translation) peut attribuer à plusieurs utilisateurs la même adresse IP globale grâce à la numérotation des ports.
 - Seulement une seule adresse globale assignée pour plusieurs utilisateurs
 - 64511 (65535 – 1024) adresses IP locales peuvent être en théorie attribuées à une seule adresse IP globale.

32

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- NAT Dynamique

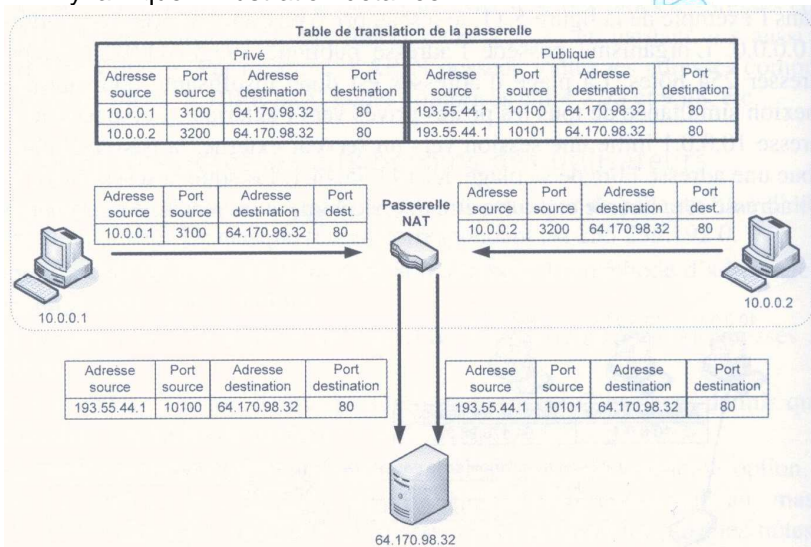


33

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

NAT - Network Address Translation

- NAT Dynamique – Illustration détaillée



34

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Port Forwarding

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Port Forwarding

- **Objectif** : Le port Forwarding redirige les flux qui arrivent sur un port TCP ou UDP donné et une adresse IP, en général une adresse IP publique, vers une autre adresse IP, en général une adresse IP privée et si besoin sur un autre port.
- Cela se configure donc sur un routeur. Le paramétrage consiste à indiquer au routeur de retransmettre les paquets qui arrivent sur son interface publique (désignée interface WAN) et sur un port ou une plage de ports spécifiés vers une machine dans son réseau local, sur une adresse IP désignée.

36

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Port forwarding – Illustration

Exemple de configuration sur un routeur

Port Forwarding Rules

WAN Interface: WAN 1

Default Server: 0 . 0 . 0 . 0

Go To Page 1

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	POP3	110 - 110	110 - 110	192 . 168 . 1 . 2
2	<input checked="" type="checkbox"/>	SMTP	25 - 25	25 - 25	192 . 168 . 1 . 2
3	<input checked="" type="checkbox"/>	IMAP	143 - 143	143 - 143	192 . 168 . 1 . 2

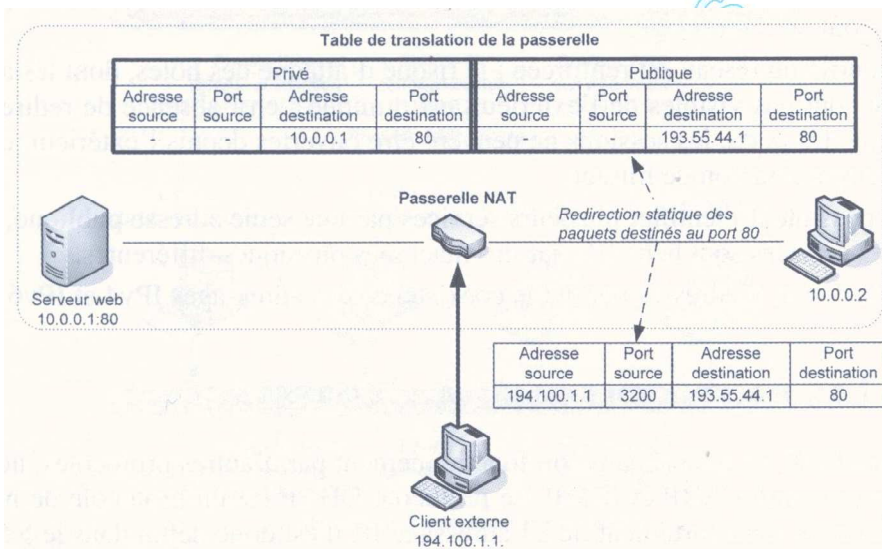
Exemple : Le flux IMAP (port TCP 143) de messagerie arrivant sur l'interface WAN du routeur se redirigé vers l'adresse 192.168.1.2 (machine interne du réseau Local).

Le port forwarding peut autoriser l'ouverture de connexion depuis l'extérieur à condition d'associer de manière statique le port d'un service défini à une adresse privée

37

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Port forwarding – Illustration



38

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Pause-réflexion

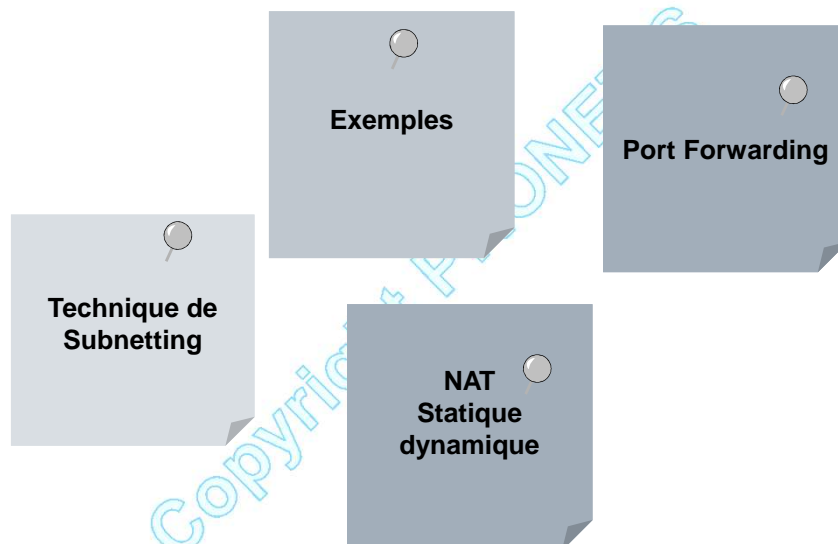
Avez-vous des questions ?



39

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

Résumé du module



40

PRONETIS©2011 - Philippe Prestigiacomo - Droits d'utilisation ou de reproduction réservés

FIN DU MODULE

Copyright PRONETIS