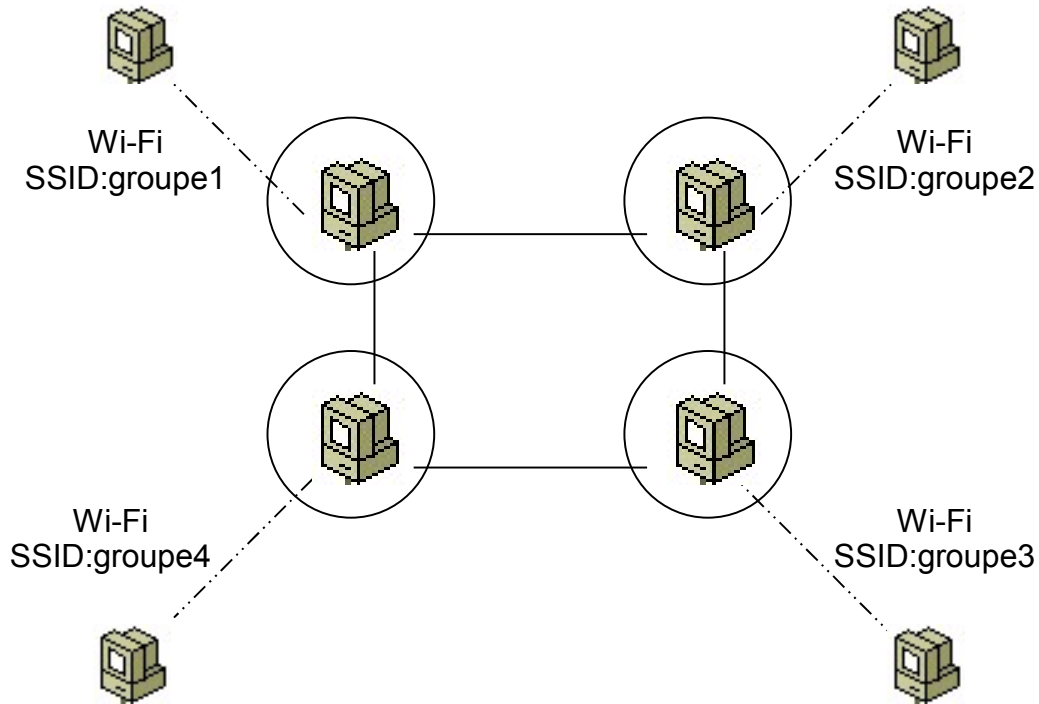


Lab 5: Déploiement

Objectif:

Réseau d'entreprise: transition de IPv4 à IPv6

Transition de IPv4 à IPv6



- **Instructions**

- 1) Lire les exemples suivants
- 2) Les adapter à l'environnement du lab
- 3) Tester et documenter les configurations

- **Objectifs**

Configurer un tunnel 6to4

Configurer un tunnel avec ISATAP, Intrasite
Automatic Tunnel Addressing Protocol

Méthodes de communication IPv6 et IPv4

Le protocole IPv6 de Windows XP fournit les méthodes suivantes pour la communication entre les noeuds IPv6 de différents sous-réseaux d'un réseau d'interconnexion IPv4 :

- Utilisation d'adresses compatibles IPv4
- Utilisation d'adresses ISATAP (Intrasite Automatic Tunnel Addressing Protocol)
- Utilisation de 6over4

6over4 requiert que le réseau d'interconnexion IPv4 soit compatible avec la multidiffusion. Étant donné que la plupart des réseaux IPv4 ne sont pas compatibles avec la multidiffusion, 6over4 est rarement utilisé. Pour plus d'informations sur 6over4, consultez [Fonctionnalités du protocole IPv6 pour Windows XP](#) et le document RFC 2529.

- Utilisation de 6to4

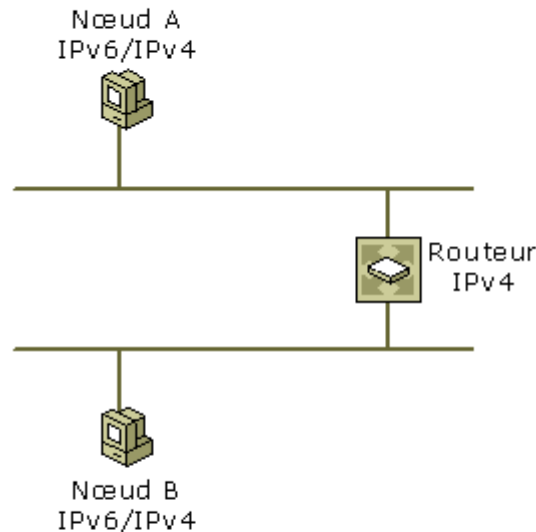
Bien que 6to4 soit essentiellement conçu pour permettre la communication entre sites 6to4 compatibles IPv6 distincts, les hôtes 6to4 qui utilisent le protocole IPv6 de Windows XP peuvent également utiliser les adresses 6to4 et le tunneling 6to4 pour communiquer via un intranet IPv4 ou Internet. Pour plus d'informations, consultez [Trafic IPv6 entre nœuds dans des sites différents par Internet \(6to4\)](#).

Dans tous les cas ci-dessus, bien que le trafic IPv6 soit traité comme la charge utile d'un paquet IPv4 (l'infrastructure IPv4 étant considérée comme une couche liaison IPv6), il conserve sa qualité de trafic IPv6. Les applications qui utilisent les adresses associées à ces méthodes recourent aux mêmes fonctions de sockets Windows que si des adresses IPv6 globales et une infrastructure IPv6 étaient utilisées. Vous pouvez utiliser ces méthodes afin de tester les fonctionnalités IPv6 pour vos applications sans déployer de routeurs IPv6 au sein de votre entreprise.

Utilisation d'adresses compatibles IPv4

Les adresses compatibles IPv4 dérivées des adresses IPv4 publiques permettent de connecter des sites ou hôtes IPv6 via l'infrastructure Internet IPv4 existante. Lorsque le trafic IPv6 est associé à des adresses compatibles IPv4, il n'est pas nécessaire d'ajouter des routeurs IPv6. Le trafic est encapsulé avec un en-tête IPv4.

L'illustration suivante montre la configuration de deux noeuds sur des sous-réseaux distincts utilisant des adresses compatibles IPv4 pour communiquer via un routeur IPv4.



Par défaut, le protocole IPv6 de Windows XP configure automatiquement des adresses compatibles IPv4 pour les adresses IPv4 publiques sur la pseudo-interface de tunneling automatique (ID d'interface 2). Une adresse compatible IPv4 prend la forme `::w.x.y.z`, où `w.x.y.z` représente une adresse IPv4 publique affectée à une interface de l'ordinateur. À titre d'exemple, consultez le résultat de la commande `ipv6 if` dans la rubrique [Sous-réseau unique avec adresses lien-local](#) ;

En outre, le protocole IPv6 de Windows XP crée automatiquement un itinéraire `::/96` qui transmet tout le trafic utilisant des adresses compatibles IPv4 avec la pseudo-interface de tunneling automatique (ID d'interface 2). Tout le trafic transmis par cet hôte aux destinations compatibles IPv4 est encapsulé avec un en-tête IPv4.

Lorsque vous envoyez du trafic à une adresse compatible IPv4, il part d'une adresse compatible IPv4 puis est encapsulé avec un en-tête IPv4. Le champ Protocole de l'en-tête IPv4 a pour valeur 41, indiquant que la charge utile est un paquet IPv6. L'en-tête IPv4 permet au trafic de parcourir une infrastructure IPv4. Les adresses IPv4 incorporées dans les adresses compatibles IPv4 source et de destination d'un en-tête IPv6 deviennent les adresses IPv4 source et de destination dans l'en-tête IPv4.

Configuration et test de connectivité

Supposons que l'hôte A (configuré avec l'adresse IPv4 131.107.41.17) utilise des adresses compatibles IPv4 pour envoyer du trafic IPv6 à l'hôte B (configuré avec l'adresse IPv4 157.60.15.93). Les adresses source et de destination des en-têtes IPv4 et IPv6 sont répertoriées dans le tableau ci-dessous.

Champ	Valeur
Adresse source dans l'en-tête IPv6	::131.107.41.17
Adresse de destination dans l'en-tête IPv6	::157.60.15.93
Adresse source dans l'en-tête IPv4	131.107.41.17
Adresse de destination dans l'en-tête IPv4	157.60.15.93

L'infrastructure de routage IPv4 transmet le paquet depuis l'hôte A vers l'hôte B, en fonction de l'adresse de destination IPv4 157.60.15.93. Une fois reçue par l'hôte B, la charge utile du paquet IPv4 (le paquet IPv6) est transmise au protocole IPv6.

Pour tester la connectivité, utilisez la commande **ping6**. Par exemple, vous utiliseriez la syntaxe suivante sur l'hôte A pour adresser une commande ping à l'hôte B à partir de son adresse compatible IPv4 :

```
ping6 ::157.60.15.93
```

Intrasite Automatic Tunnel Addressing Protocol

ISATAP

Un autre mécanisme d'affectation d'adresses et de tunneling utilisable pour la communication entre noeuds IPv6/IPv4 d'un réseau IPv4 est décrit dans le document d'assistance en ligne « Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) » (draft-ietf-ngtrans-isatap-00.txt). Ces adresses sont appelées adresses ISATAP (Intrasite Automatic Tunnel Addressing Protocol). Elles présentent la forme *Préfixe64Bits:200:5EFE:w.x.y.z* où :

- la partie *Préfixe64Bits* représente tout préfixe 64 bits valide pour les adresses de monodiffusion IPv6. Cela englobe le préfixe d'adresse lien-local (FE80::/64), les préfixes site-local et les préfixes globaux ;
- la partie 200:5EFE représente l'identificateur d'interface 64 bits global unique résultant de la combinaison de l'identificateur d'unité d'organisation (Organizational Unit Identifier, OUI) affecté à l'IANA (Internet Assigned Numbers Authority) (00-00-5E) et d'un type indiquant une adresse IPv4 incorporée (FE) ;
- la partie *w.x.y.z* représente toute adresse IPv4 monodiffusion (publique ou privée).

À l'image des adresses 6over4, 6to4 et compatibles IPv4, les adresses ISATAP possèdent une adresse IPv4 incorporée permettant de déterminer les adresses IPv4 source ou de destination dans l'en-tête IPv4 lorsque du trafic IPv6 utilisant des adresses ISATAP est envoyé via un réseau IPv4.

Par défaut, le protocole IPv6 de Windows XP configure automatiquement l'adresse ISATAP FE80::200:5EFE:w.x.y.z sur la pseudo-interface de tunneling automatique pour chaque adresse IPv4 affectée au noeud. Cette adresse ISATAP lien-local permet à deux hôtes de communiquer via un réseau IPv4 en utilisant leurs adresses ISATAP mutuelles.

Configuration ISATAP et test de connectivité

Par exemple, l'hôte A est configuré avec l'adresse IPv4 10.40.1.29 et l'hôte B avec l'adresse IPv4 192.168.41.30.

Lorsque le protocole IPv6 de Windows XP est exécuté, l'hôte A est automatiquement configuré à partir de l'adresse ISATAP FE80::200:5EFE:10.40.1.29 et l'hôte B est automatiquement configuré à partir de l'adresse ISATAP FE80::200:5EFE:192.168.41.30. Le tableau suivant répertorie les adresses source et de destination des en-têtes IPv4 et IPv6 impliquées lorsque l'hôte A envoie du trafic IPv6 à l'hôte B en utilisant l'adresse ISATAP de celui-ci :

Champ	Valeur
Adresse source dans l'en-tête IPv6	FE80::200:5EFE:10.40.1.29
Adresse de destination dans l'en-tête IPv6	FE80::200:5EFE:192.168.41.30
Adresse source dans l'en-tête IPv4	10.40.1.29
Adresse de destination dans l'en-tête IPv4	192.168.41.30

Pour tester la connectivité, utilisez la commande **ping6**.

Par exemple, vous utiliseriez la syntaxe suivante sur l'hôte A pour adresser une commande ping à l'hôte B à partir de son adresse ISATAP lien-local :

```
ping6 FE80::200:5EFE:192.168.41.30%2
```

La partie *%IDÉtendue* de la commande permet de spécifier l'index de l'interface à partir de laquelle le trafic est envoyé.

Dans ce cas, **%2** spécifie l'interface 2, qui correspond à l'ID d'interface affecté à la pseudo-interface de tunneling automatique sur l'hôte A.

Communication hors site

L'utilisation d'adresses ISATAP lien-local permet aux hôtes IPv6/IPv4 d'un intranet IPv4 de communiquer entre eux mais pas avec les hôtes IPv6 situés hors du site. La communication hors site requiert la configuration suivante supplémentaire :

- Un hôte doit recevoir du routeur situé à la limite du site une annonce contenant un préfixe d'adresse global. Le routeur situé à la limite du site sépare l'intranet d'Internet (ou de 6bone). Il s'agit le plus souvent d'un routeur 6to4 connecté à Internet. Dès réception de l'annonce de routeur, des adresses ISATAP supplémentaires basées sur le préfixe global sont automatiquement ajoutées.

Par exemple, si le site est connecté à 6bone et que l'hôte A reçoit le préfixe global 3000::/64 dans une annonce de routeur, l'adresse ISATAP 3000::200:5EFE:10.40.1.29 est automatiquement configurée. Sans préfixe d'adresse global et connexion à 6bone, un site peut utiliser un préfixe d'adresse global 6to4 et se connecter à d'autres sites 6to4, à des hôtes 6to4 et à 6bone en utilisant l'infrastructure Internet IPv4. Si le site utilise le préfixe d'adresse 6to4 2002:836B:1:5::/64 (basé sur l'adresse publique 131.107.0.1 et sur un SLA ID égal à 5), l'adresse ISATAP 2002:836B:1:5:200:5EFE:10.40.1.29 est automatiquement configurée.

Toutefois, aucun mécanisme ne prend actuellement en charge la propagation de l'annonce de routeur entre le routeur situé à la limite du site et les hôtes ISATAP via un réseau IPv4.

Le protocole IPv6 de Windows XP doit être configuré manuellement pour l'adresse ISATAP globale sur la pseudo-interface de tunneling automatique (ID d'interface 2) au moyen de la commande **ipv6 adu**. Dans l'exemple de préfixe 6to4 ci-dessus, la commande à partir de l'hôte A est **ipv6 adu 2/2002:836B:1:5:200:5EFE:10.40.1.29**. Pour plus d'informations, consultez [Pour configurer le protocole IPv6 avec des adresses manuelles](#). Le préfixe global 64 bits, qui utilise la pseudo-interface de tunneling automatique (ID d'interface 2), doit être ajouté manuellement à la table de routage IPv6 au moyen de la commande **ipv6 rtu**. Dans l'exemple de préfixe 6to4 ci-dessus, la commande à partir de l'hôte A est **ipv6 rtu 2002:836B:1:5::/64 2**. Pour plus d'informations, consultez [Ajouter un itinéraire IPv6](#).

Itinéraire par défaut (default route)

Un hôte doit posséder un itinéraire par défaut pointant vers une adresse ISATAP qui correspond à l'interface intranet du routeur situé à la limite du site.

Par exemple, si l'interface intranet du routeur situé à la limite du site est configurée avec l'adresse IPv4 172.16.0.1, l'hôte A doit être configuré avec un itinéraire par défaut (::/0) qui utilise l'adresse ISATAP FE80::200:5EFE:172.16.0.1 comme adresse de tronçon suivant. Tout le trafic IPv6 qui correspond à cet itinéraire par défaut en tant qu'itinéraire le plus proche est ensuite encapsulé et transmis au routeur situé à la limite du site. Le routeur situé à la limite du site transmet ensuite le trafic. Si le routeur situé à la limite du site est un routeur 6to4, il encapsule le trafic IPv6 et le transmet sur Internet.

Le protocole IPv6 de Windows XP doit être configuré manuellement à l'aide de la commande **ipv6 rtu** pour obtenir un itinéraire par défaut (::/0) qui utilise la pseudo-interface de tunneling automatique (ID d'interface 2) et possède une adresse de tronçon suivant définie d'après une adresse ISATAP correspondant à l'interface intranet du routeur situé à la limite du site. Dans l'exemple ci-dessus, la commande à partir de l'hôte A est **ipv6 rtu ::/0 2/FE80::200:5EFE:172.16.0.1**.

Pour plus d'informations, consultez [Ajouter un itinéraire IPv6](#).

Ajouter une adresse manuelle

Pour configurer le protocole IPv6 avec des adresses manuelles

À l'invite de commandes, tapez :

```
ipv6 if
```

pour obtenir l'index de l'interface pour laquelle une adresse manuelle est ajoutée.

À l'invite de commandes, tapez :

```
ipv6 adu [IndexInterface][Adresse]
```

où *IndexInterface* représente le numéro de l'interface et *Adresse* désigne l'adresse IPv6. D'autres paramètres de ligne de commande sont disponibles.

Ajouter un itinéraire (route) IPv6

À l'invite de commandes, tapez :

ipv6 if

pour obtenir l'index de l'interface qui permet d'accéder aux adresses du préfixe d'itinéraire.

À l'invite de commandes, tapez :

ipv6 rtu *Préfixe IndexInterface/AdresseTronçonSuivant*

où :

- *Préfixe* représente le préfixe d'itinéraire.
- *IndexInterface* représente le numéro d'interface.
- *AdresseTronçonSuivant* représente l'adresse d'un routeur local.

D'autres paramètres de ligne de commande sont disponibles.

Commande ipv6 if : information interface

- **ipv6 [-v] if [*IndexIf*]**
- Affiche des informations sur les interfaces. Si un numéro d'index d'interface est spécifié, les informations affichées ne concernent que cette interface. Sinon, elles portent sur toutes les interfaces. Le résultat de la commande comprend l'adresse de la couche liaison de l'interface et la liste des adresses IPv6 affectées à l'interface. Il comprend également l'unité de transmission maximale actuelle de l'interface et celle qu'elle peut effectivement prendre en charge. Le paramètre **-v** permet d'afficher des informations supplémentaires sur l'interface.
- L'interface 1 est une pseudo-interface utilisée pour le bouclage (pseudo-interface de bouclage). L'interface 2 est une pseudo-interface utilisée pour le tunneling automatique (pseudo-interface de tunneling automatique). L'interface 3 est généralement une pseudo-interface utilisée pour le tunneling 6to4 (pseudo-interface de tunneling 6to4). Les autres interfaces sont numérotées de façon séquentielle au fur et à mesure de leur création. Cet ordre varie d'un ordinateur à l'autre.
- Si l'adresse de la couche liaison présente la forme *aa-bb-cc-dd-ee-ff*, elle désigne une interface FDDI (Fiber Distributed Data Interface) ou Ethernet.
- Les pseudo-interfaces de bouclage, de tunneling automatique et de tunneling 6to4 n'utilisent pas la fonctionnalité de découverte du voisinage IPv6.

Commande ipv6 adu : address update

- **ipv6 adu** *IndexIf/Adresse* [**life** *DuréeVieValide*[/*DuréeViePréférée*]] [**anycast**] [**unicast**]
- Ajoute ou supprime sur une interface une affectation d'adresse monodiffusion ou diffusion aléatoire (l'option « unicast » est appliquée par défaut si l'option « anycast » n'est pas spécifiée).
- Si la durée de vie n'est pas spécifiée, elle est infinie. Si seule une durée de vie valide est spécifiée, la durée de vie préférée est égale à la durée de vie valide. Vous pouvez spécifier une durée de vie infinie ou une durée de vie spécifique en secondes. La durée de vie préférée doit être inférieure ou égale à la durée de vie valide. La spécification d'une durée de vie égale à zéro génère la suppression de l'adresse.
- Vous pouvez exprimer l'option **lifetime** par sa forme abrégée **life**.
- Pour toute adresse diffusion aléatoire, les seules valeurs de durée de vie valides sont zéro et infini.

Commande ipv6 rtu : route update

ipv6 rtu *Préfixe* *IndexIf*[*Adresse*] [*life* *Valide*[*Préférée*]] [*preference* *P*] [*publish*] [*age*] [*spl* *LongueurPréfixeSite*]

Ajoute ou supprime un itinéraire dans la table de routage. Le préfixe de l'itinéraire est obligatoire. Les préfixes de liaison requièrent une interface. Les préfixes hors liaison requièrent une interface et une adresse de saut suivant. L'itinéraire peut avoir une durée de vie en secondes (infinie par défaut) et une préférence (zéro par défaut, si possible). La spécification d'une durée de vie égale à zéro génère la suppression de l'itinéraire.

Si l'itinéraire est spécifié en tant qu'itinéraire publié (utilisé dans l'élaboration des annonces de routeurs), par défaut, il ne vieillit pas. La durée de vie de l'itinéraire ne diminue pas et est donc infinie. Lorsque l'itinéraire figure dans les messages d'annonce de routeurs, la durée de vie est utilisée. Vous avez également la possibilité de spécifier un itinéraire en tant qu'itinéraire publié qui vieillit. Un itinéraire non publié vieillit toujours par défaut.

Le paramètre **spl** permet d'associer une longueur de préfixe de site à l'itinéraire. La longueur de préfixe de site est uniquement utilisée lors de l'envoi d'annonces de routeurs.

Vous pouvez exprimer les options **lifetime**, **preference** et **publish** par leur forme abrégée respective **life**, **pref** et **pub**.