

Transition de IPv4 à IPv6

Objectifs:

Décrire les mécanismes de transition et
les cas d'utilisation

Généralités

- Pas de jour J
- Nécessité de la transition
 - Pénurie d'adresse (Chine et Inde en particulier)
 - Téléphonie mobile (3GPP)
 - Réseaux domotiques et personnels
 - Applications de type peer-to-peer
 - Connexions permanentes
 - Killer application, qualité de service ?
- Plusieurs mécanismes
 - Double pile
 - Tunnels
 - ...

IETF Working Groups

- Working groups ipng et ngtrans
 - Années 90s
 - IP nouvelle génération et transition à la nouvelle génération
 - Approche “Boite à outils”
 - Beaucoup d'outils sans mode d'emploi
- Working group IPv6ops
 - Créé en 2002
 - Déploiement opérationnel
 - **De la transition à la coexistence**
 - Approche en scenarii d'intégration :
 - Réseaux de mobiles (UMTS, 3GPP)
 - Réseaux d'ISP
 - Réseaux d'entreprise
 - Réseaux SOHO/domestiques

Mécanismes de transition

Mécanismes de transition

Mécanismes de transition	Coeur de réseau	ISP	Entreprises	Particuliers
Double pile	X	X	X	X
6PE (MPLS)	X	X	X	
6to4		X	X	X
Tunnel Broker		X	X	X
Tunnels configurés	?	X	X	X
TSP		X	X	X
ISATAP			X	
TEREDO		X	X	X
Relais applicatifs		X	X	X
NAT-PT		X	X	X
DSTM		X	X	X
SOCKS			X	X
VPN		X	X	X
L2TP		X	X	X

Source: IPv6 Théorie et Pratique, 4e Ed., O'Reilly

Déploiement d'IPv6 dans le coeur du réseau

- Double Pile
 - Dual Stack IPv4 et IPv6
- 6PE, Provider Edge IPv6
 - Equipements de périphérie, routeurs de bordure

Double pile (Dual Stack)

- Doter chaque équipement de réseau d'une double pile protocolaire, en privilégiant la pile IPv6
 - Affecter une adresse IPv4 et une adresse IPv6 à chaque interface
 - Coeur de réseau
 - En cas de déploiement partiel, attention au protocole de routage (IS-IS)
 - Equipement terminaux
 - Utilisation des adresses IPv4 mappées
- Inconvénients
 - Ne résoud pas le problème de pénurie des adresses
 - Routeurs doivent pouvoir acheminer les deux types de paquets
 - Applications doivent être recompilés
- Avantages
 - Mécanisme de transition le plus simple et le plus souple

6PE (MPLS)

- IPv6 Provider Edge
 - Les équipements de périphérie attribuent une étiquette à chaque paquet IPv6
- MPLS
 - Multi Protocol Label Switching
 - Protocole de routage de niveau 3
 - Coeur du réseau reste inchangé

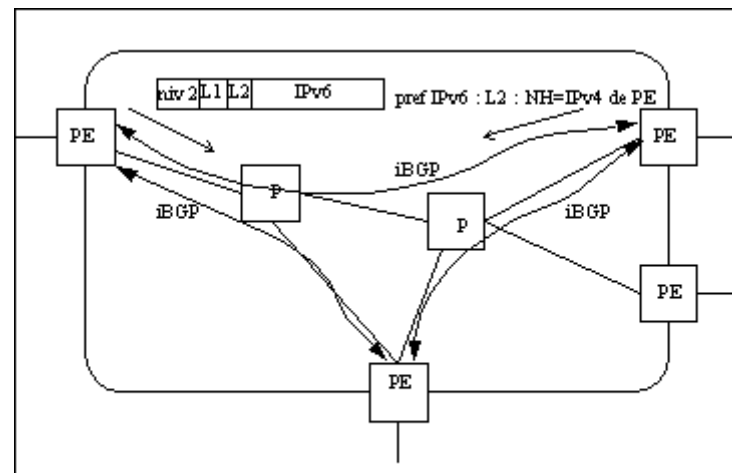


Figure 14-3. Architecture d'un réseau MPLS

Source: IPv6 Théorie et Pratique, 4e Ed., O'Reilly, Fig. 14-3

Déploiement d'IPv6 des FAI (ISP)

- Architecture client/serveur
 - Mécanismes automatiques
- 6to4
- Tunnel Broker
- TSP
 - Tunnel Setup Protocol

6to4

- Permet d'interconnecter des sites IPv6 isolés en créant des tunnels automatiques IPv6 dans IPv4 en fonction du destinataire des données
 - Machine terminale 6to4
 - Routeur de bordure encapsule paquets IPv6 dans IPv4
 - Relais 6to4
- Inconvénients
 - Routage peut être asymétrique
 - Délais peuvent être élevés à cause des tunnels
- Avantages
 - Permet de router du trafic IPv6 même si l'ISP est IPv4

Adresses 6to4

- Préfixe alloué par IANA
 - 2002::/16

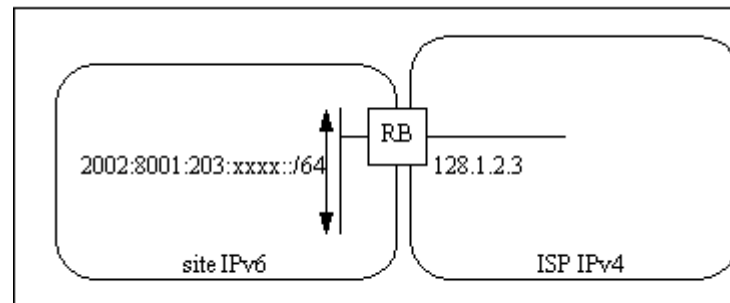
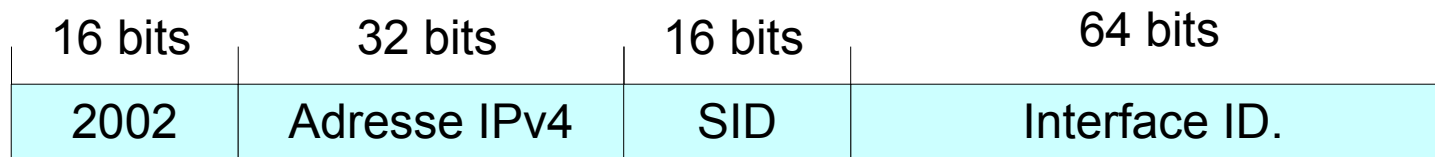


Figure 14-5 . Exemple de numérotation en utilisant le préfixe de 6to4

Exemple de routage des paquets

- A utilise DNS pour trouver l'adresse IPv6 de B
 - Par exemple 2002:c0c0:c0c0:...
- Paquets dont l'adresse de destination commence par préfixe 2002::/16 sont routés vers un routeur tunnelier 6to4
- Routeur tunnelier peut extraire adresse IPv4 de l'autre extrémité du tunnel
 - Dans cette exemple 192.192.192.192

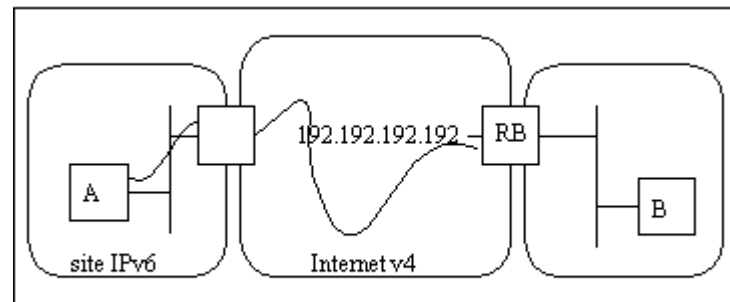


Figure 14-6. Exemple de routage des paquets

Tunnel Broker

- Serveur de tunnels (IPv6 dans IPv4)
- Permet de fournir la connectivité IPv6 à des équipements/réseaux locaux isolés dans Internetv4
 - Architecture client/serveur
 - Protocole TSP
 - Connexion au broker
 - Configuration du tunnel Tunnel Server / Terminal
 - Envoi du script configuration du tunnel Terminal / Tunnel Server
 - Communication IPv6

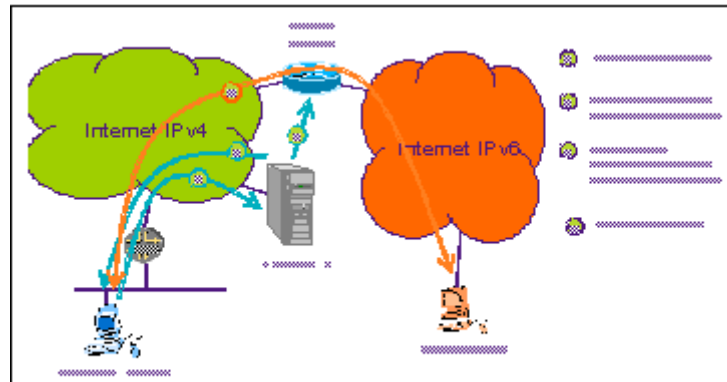


Figure 14-7. Configuration d'un Tunnel Broker avec TSP

TSP

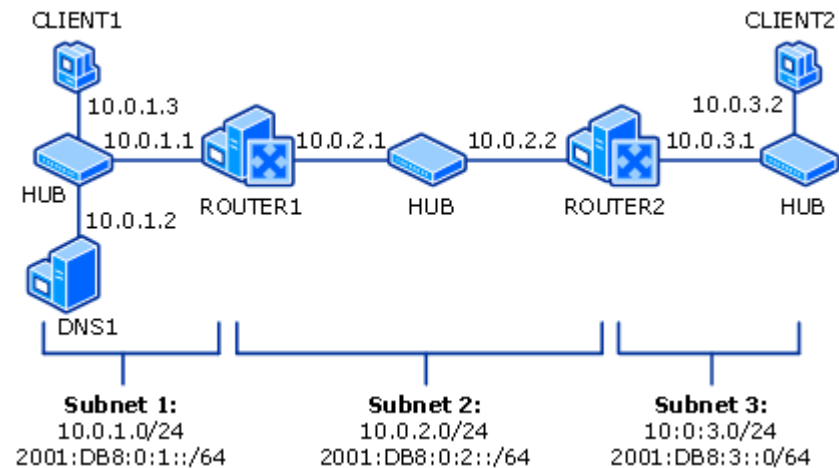
- Tunnel Setup Protocol
- Permet la négociation automatique et transparente
 - mécanisme d'authentification utilisateur utilisé
 - type d'encapsulation utilisée :
 - IPv4 dans IPv6, IPv6 dans IPv4, IPv6 dans UDP IPv4
 - Traversée de NAT
 - Découverte de NAT
 - Envoi de message UDP avec adresse du terminal
 - Si différente de l'adresse source > NAT
 - adresse IPv6 assignée lorsque le client TSP est un terminal
 - préfixe IPv6 alloué lorsque le client TSP est un routeur
 - l'enregistrement DNS dans le cas d'un terminal
 - la résolution DNS inverse dans le cas d'un routeur

Déploiement d'IPv6 dans les entreprises

- ISATAP
 - Intra-Site Automatic Tunnel Addressing Protocol
- Teredo
 - Tunneling IPv6 over UDP through NAT

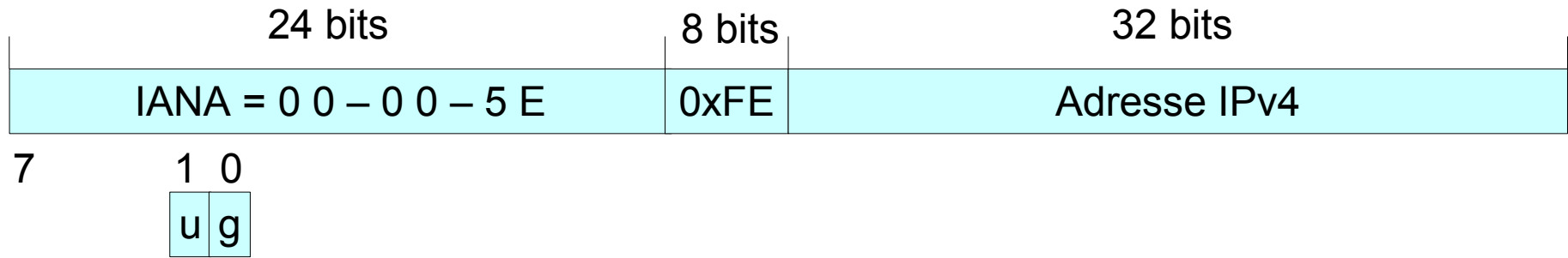
ISATAP

- Intra-Site Automatic Tunnel Addressing Protocol
 - Similaire à 6to4 dans un réseau privé



Identifiant d'interface

- Identifiant d'interface 64 bit IEEE dérivé de l'adresse IPv4
 - OUI de l'IANA: 00-00-5e
 - 00-00-5E-FE + 32 bit adresse IPv4

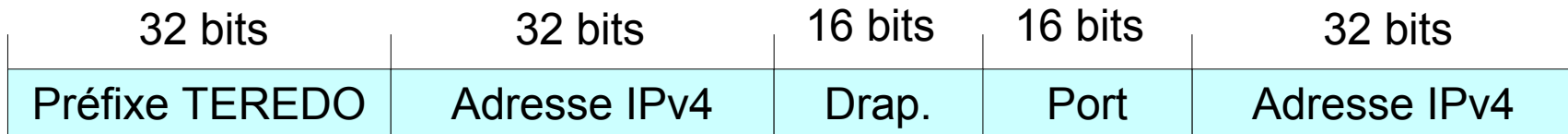


Algorithme de configuration

- Equipement doit connaître l'adresse IPv4 du routeur gérant ISATAP
 - En utilisant DNS (ou une adresse anycast IPv4)
- Equipement envoie un message IPv6 Router Solicitation
 - Adresse source fe80::5e:fe:IPv4
 - Adresse destination ff02::02 (adresse multicast des routeurs)
 - Message encapsulé dans un paquet IPv4 dont l'adresse de destination est l'adresse IPv4 du routeur
- Routeur renvoie un message IPv6 Router Advertisement
 - en point à point, toujours encapsulé dans un paquet IPv4, la liste des préfixes IPv6 utilisés pour joindre les équipements isolés
- ISATAP est compatible avec 6to4

TEREDO

- Permet de fournir automatiquement la connectivité IPv6 à un terminal situé derrière un NAT
 - RFC 4380 (Christian Huitéma, INRIA dans les années 80s)
 - <http://www.ietf.org/rfc/rfc4380.txt>
- Format des adresses
 - Préfixe (de test pour le moment):
 - 3FFE:831F::/32 + adresse IPv4 du serveur Teredo
 - Identifiant:
 - adresse IPv4 et numéro de port (en sortie de NAT) du client Teredo



Partie obscurcie

Architecture Teredo

- Architecture client, serveur et relais
 - Déterminer le type de NAT traversé et assigner une adresse IPv6 au client Teredo
 - Fonctionne uniquement avec les cone NATs
 - http://en.wikipedia.org/wiki/Full_cone_NAT#Different_types_of_NAT
 - Maintenir ouvert dans le NAT, l'association entre adresse/port interne et adresse/port externes
 - Envoi périodique d'un message spécifique vers le serveur Teredo qui a pour effet de ré-initialiser le time-out d'inactivité du NAT

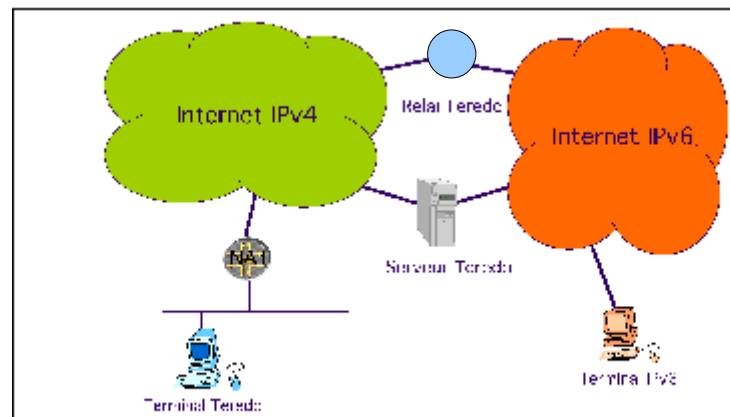


Figure 14-10. architecture Teredo

Relais

- Application Level Gateways (ALG)
 - Serveurs de courrier électronique
 - Spoolers d'impression
 - Serveurs DNS
 - Proxies et caches web
- Relais TCP/UDP
 - SOCKS
 - Extension du RFC 1928 par le RFC 3089
- DSTM
 - Dual Stack Transition Mechanism
 - Dynamic Tunneling Interface (DTI)
 - Routeur Tunnel End Point (TEP)

Relais IP

- SIIT
 - Stateless IP/ICMP Translation Algorithm
 - RFC 2765
- NAT-PT
 - Network Address Translator with Protocol Translator
 - RFC 3234
 - <http://www.google.fr/url?sa=X&start=0&oi=define&q=http://community.roxen.com/developers/>
 - Routeur NAT-PT
 - Traduit adresse et protocole IPv6 en IPv4

Fonctionnalités protocole IPv6 sous Windows XP

Fonctionnalités du protocole IPv6 pour Windows XP

Le protocole IPv6 de Windows XP comprend les fonctionnalités suivantes :

- Tunneling 6to4
- Protocole ISATAP
- Tunneling 6over4
- Adresses anonymes
- Préfixes de site dans les annonces de routeur
- Prise en charge de DNS
- Prise en charge d'IPSec
- Prise en charge des applications
- Prise en charge des fonctions RPC
- Prise en charge des routeurs statiques

Les sections suivantes décrivent chacune de ces fonctionnalités.

Tunneling 6to4

6to4 est une technique de tunneling décrite dans le document RFC 3056. Les hôtes 6to4 ne requièrent aucune configuration manuelle et créent les adresses 6to4 par le biais d'une configuration automatique standard. 6to4 utilise le préfixe d'adresse global 2002:WWXX:YYZZ::/48, où WWXX:YYZZ représente la forme hexadécimale à deux-points d'une adresse IPv4 publique (w.x.y.z) affectée à un site ou hôte. WWXX:YYZZ représente la partie NLA (Next Level Aggregator) d'une adresse 6to4.

6to4 permet aux sites et hôtes compatibles IPv6 de communiquer au moyen du protocole IPv6 via une infrastructure IPv4 (par exemple, Internet). Les sites et hôtes IPv6 peuvent utiliser leur préfixe d'adresse 6to4 et Internet pour communiquer sans obtenir de préfixe d'adresse global IPv6 auprès d'un fournisseur de services Internet ni se connecter à 6bone (portion IPv6 d'Internet).

Pour plus d'informations, consultez

[Trafic IPv6 entre nœuds dans des sites différents par Internet \(6to4\)](#).

Protocole ISATAP

Protocole ISATAP

ISATAP (Intrasite Automatic Tunnel Addressing Protocol) est un mécanisme d'affectation d'adresses et de tunneling utilisable pour la communication entre nœuds IPv6/IPv4 au sein d'un réseau IPv4. Il est décrit dans le document d'assistance en ligne « Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) » (draft-ietf-ngtrans-isatap-00.txt). Pour plus d'informations, consultez [Trafic IPv6 entre nœuds de sous-réseaux différents d'une interconnexion IPv4](#).

Tunneling 6over4

6over4, également appelé tunneling multidiffusion IPv4, est une technique de tunneling décrite dans le document RFC 2529. 6over4 permet aux nœuds IPv6 et IPv4 de communiquer au moyen du protocole IPv6 via une infrastructure IPv4. 6over4 utilise l'infrastructure IPv4 comme liaison compatible avec la multidiffusion. Pour que 6over4 fonctionne correctement, l'infrastructure IPv4 doit être en mesure de prendre en charge la multidiffusion IPv4.

Pour plus d'informations sur la configuration d'une interface 6over4, consultez [Utilitaires IPv6](#).

Adresses anonymes (ou temporaires)

Pour que l'accès aux ressources Internet bénéficie d'un certain degré d'anonymat, l'identificateur d'interface 64 bits d'une adresse IPv6 globale est dérivé à partir de nombres aléatoires afin de créer une adresse globale anonyme.

Pour plus d'informations, consultez [Identificateurs d'interface IPv6](#).

Préfixes dans les annonces de routeur

Préfixes de site dans les annonces de routeur

Les préfixes sur liaison publiés peuvent être configurés avec une longueur de préfixe de site, comme le décrit le document d'assistance en ligne « Site prefixes in Neighbor Discovery » (draft-ietf-ipngwg-site-prefixes-0x.txt). Vous pouvez utiliser la commande **ipv6 rtu** pour associer une longueur de préfixe de site au préfixe d'adresse. Pour plus d'informations, consultez [Utilitaires IPv6](#).

Lorsqu'une option d'informations de préfixe spécifiant un préfixe de site est reçue, une entrée est créée dans la table de préfixes de site. Vous pouvez afficher cette table à l'aide de la commande **ipv6 spt**. La table de préfixes de site permet de supprimer les adresses site-local inappropriées parmi celles renvoyées par la fonction Windows Sockets **getaddrinfo()**.

Autres fonctionnalités

Prise en charge de DNS

Le traitement des enregistrements d'hôtes IPv6 DNS (Domain Name System), appelés enregistrements de ressources AAAA ou quadruple A, tel que défini dans le document RFC 1886, « DNS Extensions to support IP version 6 », est pris en charge par la résolution DNS (client) dans Windows XP et dans le service Serveur DNS dans Windows 2000. Tout le trafic DNS est envoyé via IPv4.

Pour plus d'informations, consultez [Résolution de noms](#).

Prise en charge d'IPSec

Le traitement de l'en-tête d'authentification (AH, *Authentication Header*) à l'aide du hachage MD5 (Message Digest 5), et d'ESP (Encapsulating Security Payload) à l'aide de l'en-tête NULL ESP et du hachage MD5, est pris en charge. Le cryptage de données ESP n'est pas pris en charge.

Pour un exemple de configuration, consultez [Utilisation de IPSec entre deux hôtes locaux de liaison](#).

Prise en charge des applications

Les applications prenant en charge l'utilisation du protocole IPv6, qui sont fournies avec Windows XP, comprennent Internet Explorer, le client Telnet (Telnet.exe) et le client FTP (Ftp.exe).

Pour plus d'informations, consultez [Applications IPv6](#).

Prise en charge des fonctions RPC

Les fonctions RPC (Remote Procedure Call), qui permettent de transmettre par le réseau des appels de fonction d'application à un système distant, peuvent être utilisées via IPv6. L'administration à distance recourt couramment aux fonctions RPC.

Routage statique

Prise en charge des routeurs statiques

Un ordinateur exécutant Windows XP peut faire office de routeur IPv6 statique qui transmet les paquets IPv6 entre les interfaces en fonction du contenu de la table de routage IPv6. Vous pouvez configurer des itinéraires statiques à l'aide de la commande **ipv6 rtu**. Les protocoles de routage IPv6 ne sont actuellement pas pris en charge.

Un ordinateur exécutant Windows XP peut envoyer des annonces de routeur. Le contenu des annonces de routeur est automatiquement dérivé des itinéraires publiés dans la table de routage. Les itinéraires non publiés sont utilisés pour le routage mais ne sont pas envoyés dans les annonces de routeur. Les annonces de routeur contiennent toujours une option d'adresse source de couche liaison et une option d'unité de transmission maximale. La valeur de l'option d'unité de transmission maximale est tirée de l'unité de transmission maximale de liaison en cours de l'interface émettrice. Vous pouvez modifier cette valeur à l'aide de la commande **ipv6 ifc mtu**. Si un itinéraire par défaut est configuré pour être publié, un ordinateur exécutant Windows XP n'annonce que lui-même comme routeur par défaut (par le biais d'une annonce de routeur avec une durée de vie de routeur différente de zéro).

Pour des exemples, consultez

[Trafic IPv6 entre nœuds de sous-réseaux différents d'une interconnexion IPv6](#) et
[Tâches de l'atelier de test IPv6](#).

Références

- IPv6 Théorie et Pratique, Chapitre Intégration d'IPv6 et des applications
 - http://livre.point6.net/index.php/Int%C3%A9gration_d%27IPv6_et_des_applications
- IPv6 Day
 - <http://www.ipv6day.org/action.php?n=En.IPv6day>
- Wanadoo
 - <http://www.ipv6.wanadoo.fr/mxBB/>
- RFC 1933