Recommandations pour les sites et réseaux de collecte de la communauté académique RENATER :

La supervision des réseaux IPv6

Sommaire :

1 – La supervision IPv6 : Généralités 3
1.1 – Comment superviser notre réseau IPv6 3
1.1.1 – La supervision d'un réseau en Dual Stack IPv4/IPv6 3
1.1.2 – La supervision d'un réseau IPv6 only 3

1.2 – Les standards de la supervision en IPv6 : 3
1.2.1 – SSH/TELNET/TFTP 3
1.2.2 – SNMP 3
1.2.3 – Les MIBs 4
1.2.4 – L'export des flux IPv6 5

2 – Les plateformes et outils disponibles 6
2.1 – Les plateformes 6

2.2 - Quelques outils 6
2.2.1 - Pour un LAN, Laboratoires, petits sites 7
2.2.2 - Pour un MAN, Réseau de collecte, campus 8

2.3 – Les outils "faits maison": 12

Conclusion : 12

Références: 12

L'objectif de ce document est de guider **les sites** et **réseaux de collecte** dans la mise en place d'outils permettant de superviser leur réseau IPv6.

1 – La supervision IPv6 : Généralités

1.1 – Comment superviser notre réseau IPv6

De nos jours, un grand nombre de réseaux IPv6 ont été déployés. Même si la plupart sont double pile (« Dual Stack »), certains ne communiquent qu'avec la pile IPv6 (« IPv6 only »).

1.1.1 – La supervision d'un réseau en Dual Stack IPv4/IPv6

Le fait d'administrer des réseaux IPv6 ne se traduit pas toujours par l'emploi d'outils qui transportent l'information en IPv6. En effet, la plupart des équipements sur le réseau étant en Dual Stack (IPv4 – IPv6), l'accès peut se faire en IPv4 puis les informations concernant la supervision IPv6 sont récupérées. Cette solution peut être retenue quand les applications de supervision ne supportent pas transport en IPv6.
Cela permet aussi aux NOC (Network Operations Center) n'ayant pas déployé encore un plan d'adressage IPv6 pour la supervision, d'administrer aussi bien des réseaux IPv4 qu'IPv6 avec un seul plan d'adressage IPv4.

1.1.2 – La supervision d'un réseau IPv6 only

L'administration d'un réseau « IPv6 only » est différente de l'administration d'un réseau Dual Stack. En effet, du fait que les équipements ne sont accessibles qu'en IPv6, toute l'information de supervision doit être récupérée via un transport IPv6. Il est donc indispensable **dans ce cas** que toutes les applications utilisées pour l'administration du réseau supportent le transport IPv6.

1.2 – Les standards de la supervision en IPv6 :

Il existe un ensemble de méthodes qui permettent d'administrer convenablement un réseau IPv4. Nous allons voir par la suite si ces éléments sont disponibles en IPv6.

1.2.1 – SSH/TELNET/TFTP

- Pratiquement la totalité des équipements réseau supporte les connexions SSH et Telnet IPv6. L'administration à distance peut se faire en IPv6 sans aucune difficulté.
- De même, le protocole TFTP est supporté en IPv6 par les équipements réseau. Les images des systèmes d'exploitation peuvent être ainsi téléchargées en IPv6.

1.2.2 – SNMP

Un des modèles les plus utilisés dans la supervision des réseaux est SNMP. Ce protocole étant indépendant de l'architecture du protocole IP, son évolution vers IPv6 n'a pas représenté un

problème majeur. Plusieurs implémentations de SNMP pour le protocole IPv6 ont été réalisées (NET-SNMP, …).
D'autre part, la majorité des constructeurs supportent le transport IPv6 de ce protocole. En voici quelques uns :

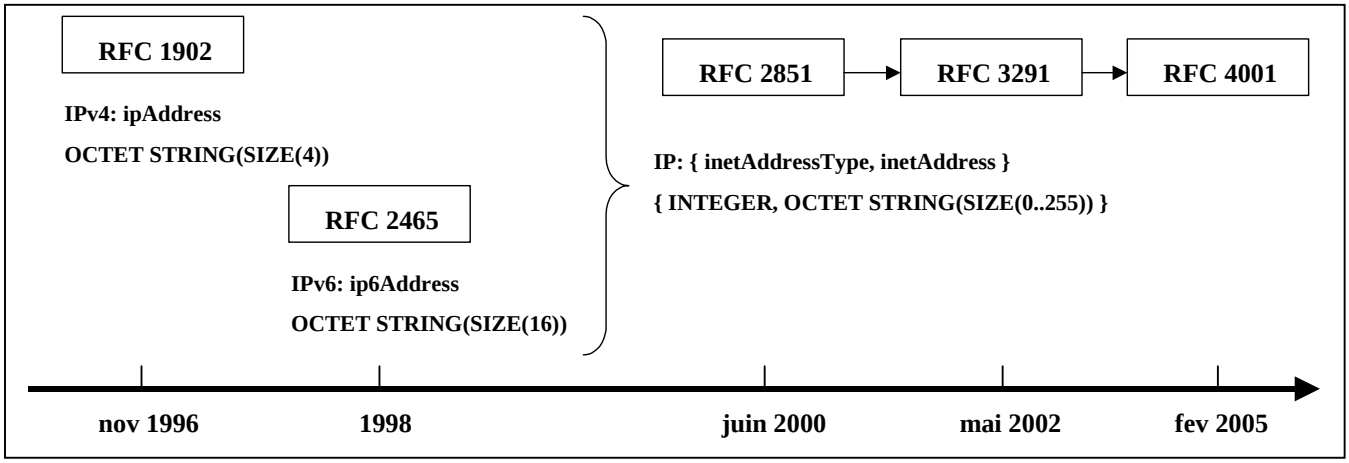
Constructeur	Cisco	Juniper	Hitachi	6wind
Disponibilité	A partir de : 12.0(27)S et 12.3(14)T	Ok	Ok	Ok

1.2.3 – Les MIBs

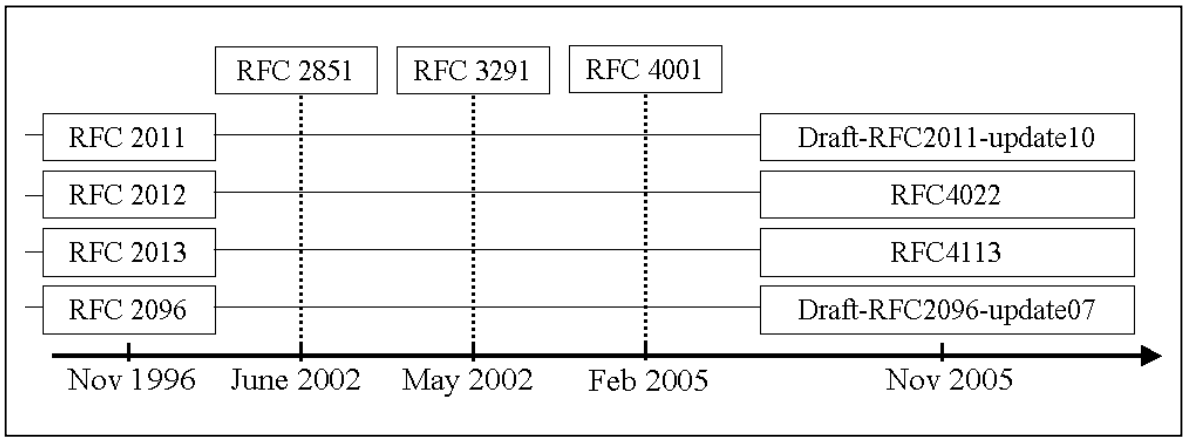
Le modèle SNMP repose sur l'interrogation des MIBs. Or, la standardisation des MIBs contenant les informations sur IPv6 a beaucoup évolué dans les dernières années et elle n'est pas complètement achevée.

- Standardisation :

Voici un schéma résumant cette évolution dans les dix dernières années :



Dans un premier temps, l'approche de l'IETF a été d'avoir des MIBs IPv4 et IPv6 indépendantes. Cependant, cette approche implique une gestion indépendante des protocoles IPv4 et IPv6 et donc la création d'un nombre inconsidéré de MIBs faisant référence à IPv6. Ainsi, l'IETF a décidé de définir une MIB-2 unifiée, permettant de superviser les réseaux IPv4 et IPv6 (RFC 2851 – Juin 2000).
Afin d'améliorer la description de la RFC 2851, sont apparues successivement les RFC 3291 et RFC 4001. Des informations supplémentaires sont décrites comme le préfixe réseau, le numéro de port utilisé par la couche transport ou le numéro d'AS (Autonomous System) correspondant à l'adresse IPv4 ou IPv6.
Cette volonté d'avoir des MIBs unifiées entraîne aussi la mise à jour de MIBs déjà existantes :



En raison de toutes ces modifications, les MIBs ne sont pas complètement disponibles aujourd'hui en IPv6. En effet, les seules réalisations effectuées par les constructeurs portent principalement sur des MIBs obsolètes ou des drafts.

- Implémentation par les constructeurs :

Un certain nombre d'informations concernant IPv6 peut être récupéré au travers des MIBs. Cependant, celles qui permettent de mesurer le trafic IPv6 ne sont pas disponibles sur la plupart des équipements réseaux.

Voici un tableau récapitulatif des MIBs implémentées par les principaux constructeurs :

	RFC/draft de référence	**Nom de la MIB**
Cisco	draft-ietf-ipngwg-rfc2011-update-00.txt	cisco-ietf-ip-mib (privé)
	draft-ietf-ipngwg-rfc2096-update-00.txt	cisco-ietf-ip-forwarding-mib (privé)
Juniper	RFC 2465 (obsolète)	`mib-jnx-ipv6.txt (privé)`
	RFC 2466 (obsolète)	`mib-jnx-ipv6.txt (privé)`
	draft ietf-idr-bgp4-mibv2-03	`mib-jnx-bgpmib2.txt (privé)`
Hitachi	RFC 2452 RFC 2454 (obsolètes) RFC 2465 RFC 2466	MIBs standard implémentées
6wind	RFC 2465 (obsolètes) RFC 2466	MIBs standard implémentées

Remarque : Il est possible sur les équipements Juniper d'obtenir le trafic IPv6 au travers des MIBs en associant des compteurs à des règles de filtrages IPv6 (firewall-filter inet6).

1.2.4 – L'export des flux IPv6

Un autre élément très important de nos jours dans la supervision des réseaux est l'export des flux. En effet, les flux permettent de caractériser le trafic acheminé sur le réseau. Il est donc essentiel de disposer au niveau des équipements réseau de cette fonctionnalité pour les flux IPv6.
Le groupe de travail IPFIX de l'IETF travaille pour définir un format standard pour l'export des flux. Cependant, aujourd'hui chaque constructeur a développé sa propre technologie.
Voici un tableau indiquant les différentes technologies utilisées par quelques constructeurs et si elles supportent l'export de flux IPv6 :

Constructeur	**technologie employée pour l'export des flux**	**Export des flux IPv6**
Cisco	Netflow (version 9)	A partir de la version d'IOS 12.3(7)T. Non disponible pour les Cisco GSR
Juniper	Cflowd	Non disponible
Hitachi	sflow	Disponible
6wind	Non disponible	Non disponible

2 – Les plateformes et outils disponibles

2.1 – Les plateformes

Les plateformes de supervision disponibles dans le marché visent à intégrer un ensemble d'outils permettant d'administrer de façon globale le réseau. Vu que tous les éléments de base ne sont pas disponibles, il est difficile de trouver aujourd'hui une plateforme qui permette de superviser un réseau IPv6 de la même façon qu'IPv4. Cependant, certaines versions de ces plateformes disposent de quelques fonctionnalités de supervision IPv6.
Voici un tableau récapitulant les fonctionnalités IPv6 de quelques plateformes d'administration.

Plateforme	**outil**	**Fonctionnalités disponibles**
HP OpenView	Network Node Manager (NMM 7.5)	Implémentation de MIBs IPv6 standard Découverte de réseau IPv6
CiscoWorks	Campus manager 4.0	Transport IPv6 : trace d'équipements terminaux IPv6 En phase de test
	Resource Manager Essentials (RME)	Inventaire et configuration d'équipements En phase de test
	Cisco View	En cours de développement
Tivoli-Netview		Pas de fonctionnalité IPv6 disponible
Infovista		Pas de fonctionnalité IPv6 disponible et aucune prévision d'en intégrer.

Aujourd'hui, les plateformes de supervision ne sont pas suffisamment avancées pour superviser entièrement un réseau IPv6.

2.2 - Quelques outils

Plutôt que d'utiliser les plateformes de supervision, il est souvent plus simple de mettre en place un outil pour superviser un besoin spécifique. Des outils sont disponibles aussi bien pour les petits sites et laboratoires que pour les campus universitaires ou réseaux de collecte.
Voici un tableau qui résume les outils disponibles qui supportent le protocole IPv6. :

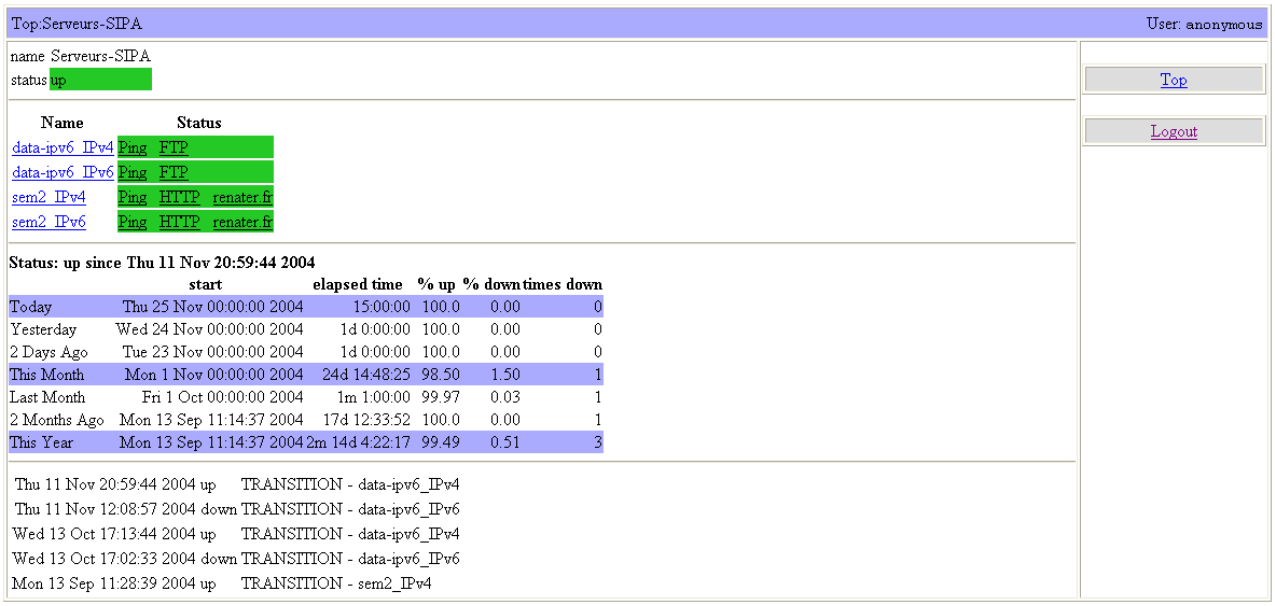
Supervision de :	Liens/Services	Analyse de flux Troubleshooting	Trafic	Routage	multicast
LAN	Argus	Ethereal	MRTG et Command Line Interface		dbeacon
MAN	Nagios	IPFlow, ReNetCol		AsPathTree/ Looking Glass	

Les outils développés en interne, ou outils faits maison restent un bon complément pour combler les manques existants dans les outils cités ci-dessus.

2.2.1 - Pour un LAN, Laboratoires, petits sites

- **Supervision des services : Argus**

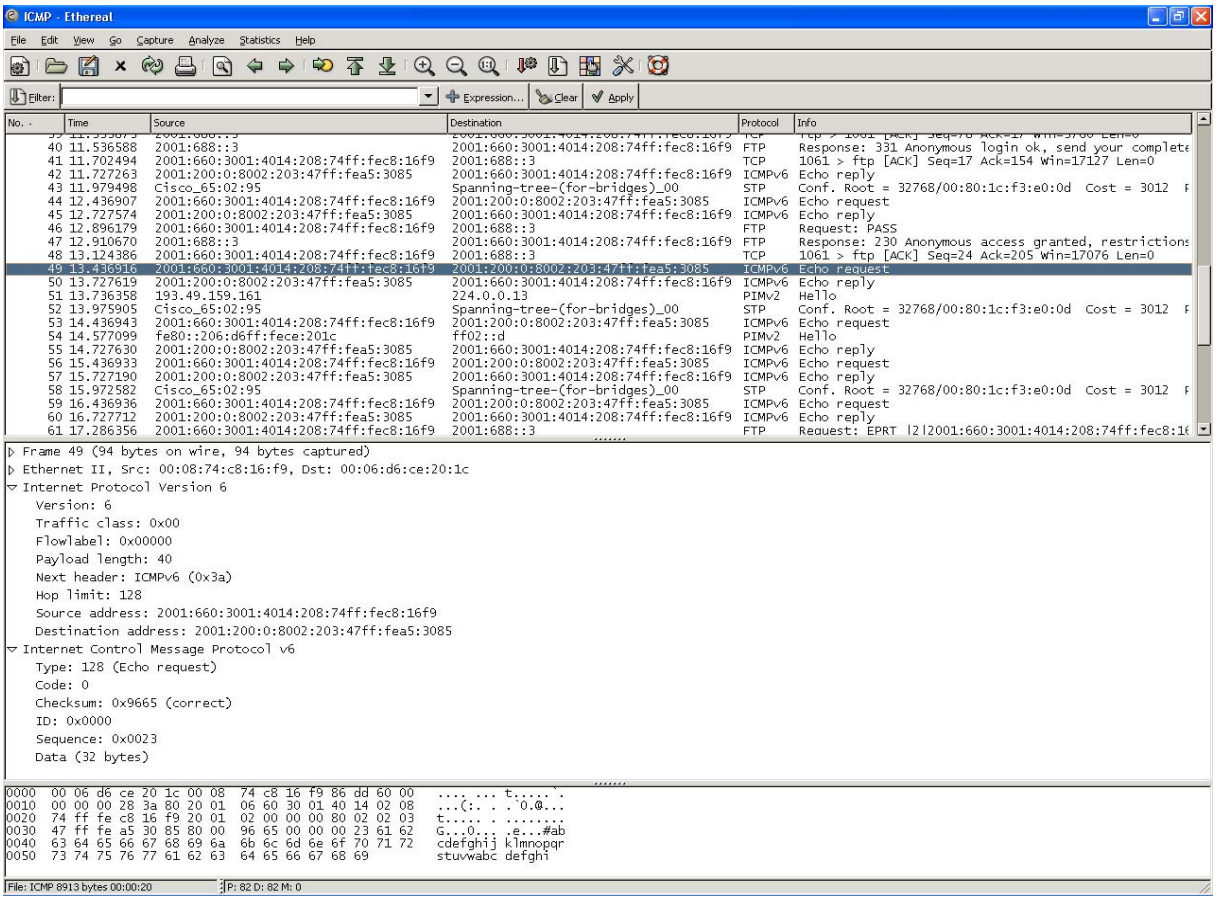
Argus est un logiciel libre permettant de superviser les différents équipements d'un réseau local (switch, routeurs, serveurs, stations de travail) ainsi que les applications associées (connectivité, applications TCP, UDP comme ping, ssh, ftp, http, dns,...) via une interface web. Ce logiciel supporte IPv6 depuis la version 3.2. Son fonctionnement modulaire permet à un administrateur d'ajouter des fonctionnalités qui ne seraient pas disponibles dans un premier temps. Le logiciel est aussi capable de générer des notifications d'alertes (mail, pager).



L'outil est disponible sur http://argus.tcp4me.com

- **Analyse de trafic, troubleshooting : Ethereal**

Ethereal est un logiciel libre qui permet d'analyser le trafic en temps réel en distinguant le trafic IPv4 et IPv6 sur une interface. Il intègre un grand nombre de protocoles des couches réseau et transport mais aussi des couches applicatives.



L'outil est disponible sur http://www.ethereal.com

- **Supervision du Multicast : dbeacon :**

dbeacon est une application client/serveur donnant des matrices de mesures sur le trafic Multicast en IPv4 et IPv6.
Chaque client possède un démon beacon. Le démon envoie un message périodiquement aux autres membres du groupe multicast pour mesurer les pertes, le délai, la gigue, les doublons et le mauvais séquencement des paquets. Ces informations sont envoyées au serveur beacon qui peut afficher ces informations dans une table.

L'outil est disponible sur http://artemis.av.it.pt/~hsantos/dbeacon/

2.2.2 - Pour un MAN, Réseau de collecte, campus

- **Etat des liens, supervision des services : Nagios**

Nagios est un logiciel couvrant les mêmes besoins qu'Argus (voir plus haut). Il offre cependant plus de fonctionnalités et peut être employé à grande échelle. Il est donc plutôt adapté aux réseaux de campus et réseaux de collecte. Il dispose de plus de vues graphiques entre autres.

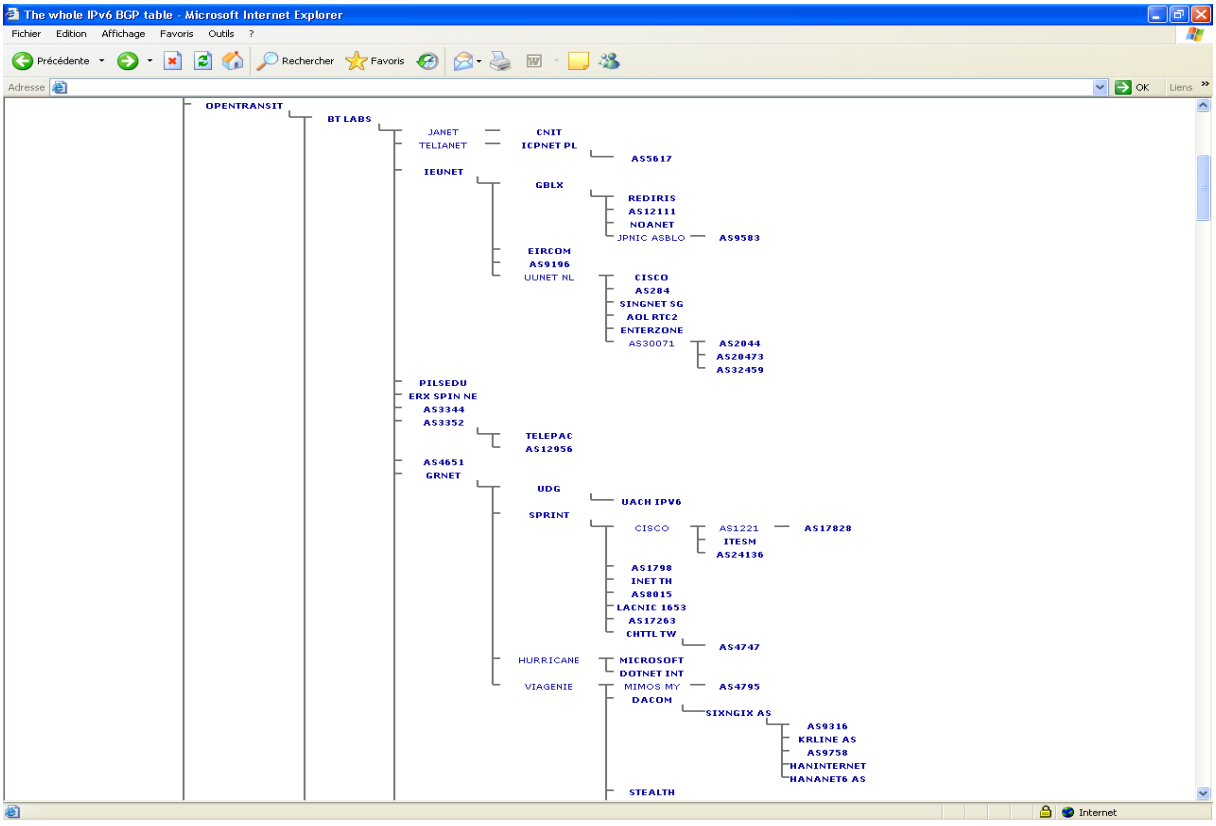
L'outil est disponible sur http://www.nagios.org .

- **Politique de routage : ASPath-Tree :**

Basé sur des captures régulières de la table BGP IPv6, ASpath-tree génère automatiquement un ensemble de pages HTML fournissant une vue graphique des chemins pour atteindre les autres AS sous forme d'arbre.
A la base conçu pour être employé par des sites IPv6 impliqués dans l'expérimentation du protocole BGP à l'intérieur du 6Bone, il peut être aujourd'hui utilisé dans n'importe quel réseau IPv6 opérationnel qui utilise BGP comme protocole de routage.
De plus, il permet la détection des entrées anormales de routes annoncées par BGP (les préfixes interdits ou non agrégés), des numéros d'AS erronés (réservés ou privés) et fournit un ensemble d'information complémentaire comme :

- le nombre de routes (valid/total/suppressed/damped/history)
- le nombre d'AS dans la table (total, originating only, originating/transit, transit only, private and reserved)
- le nombre de voisins actifs BGP (c'est à dire annonçant des routes)
- une analyse de la taille de réseau, en termes de distance inter-AS
- le nombre de préfixes circulant dans le réseau (total, 6Bone pTLAs, sTLAs, 6to4, autres).

Un des grands avantages d'ASPath-Tree est qu'il permet de connaître rapidement les chemins empruntés par les paquets pour atteindre un AS en se basant uniquement sur un routeur du réseau (même AS). Ceci simplifie beaucoup la mise en place de l'outil.
ASPath-tree facilite donc la mise en place d'une politique de routage au niveau d'un backbone. Ce n'est pas un outil de supervision de l'état des peerings BGP.

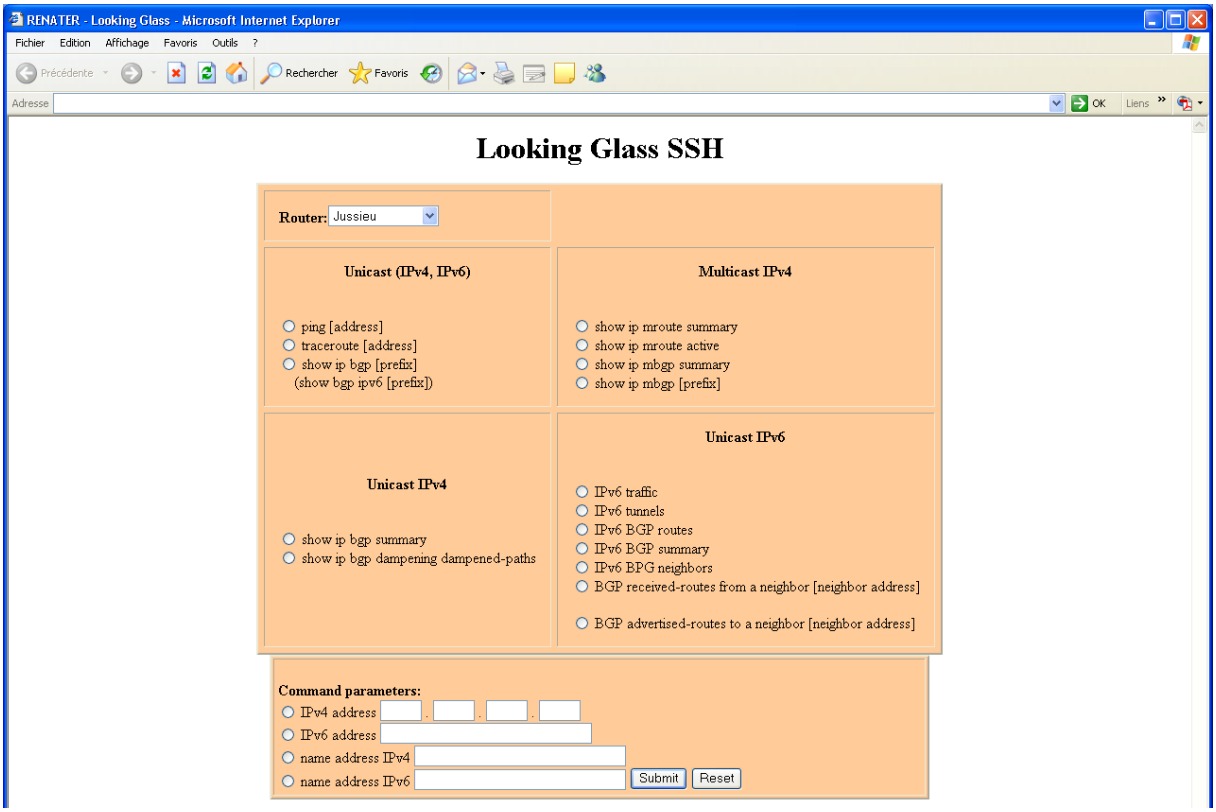


L'outil est disponible sur http://carmen.ipv6.tilab.com/ipv6/tools/ASpath-tree/

Remarque : Cet outil est spécifique à IPv6. En effet, le nombre de routes présentes dans les tables de routage en IPv6 est de l'ordre de 700 alors qu'en IPv4 ce nombre dépasse 120 000, ce qui rendrait le traitement beaucoup plus lourd.

- **Looking Glass**

Cet outil permet, à travers une interface WEB, d'avoir un accès direct sur les routeurs ou switchs. L'utilisateur dispose d'une liste de commandes qui peuvent être exécutées. Des scripts CGI permettant la connexion Telnet ou SSH (en IPv4 ou IPv6) récupèrent l'information désirée et l'affichent sur une page WEB.
Son grand avantage est qu'il permet d'obtenir des informations directement sur des équipements réseaux en temps réel sans avoir un compte dédié sur ces équipements. L'administrateur peut ainsi donner une vision de son réseau aux administrateurs d'autres réseaux et aux utilisateurs finaux. Cependant, le fait de donner des informations sur les équipements réseaux oblige à mettre en place un certain nombre de mesures de sécurité pour préserver la confidentialité des informations (accès restreint au serveur web…).



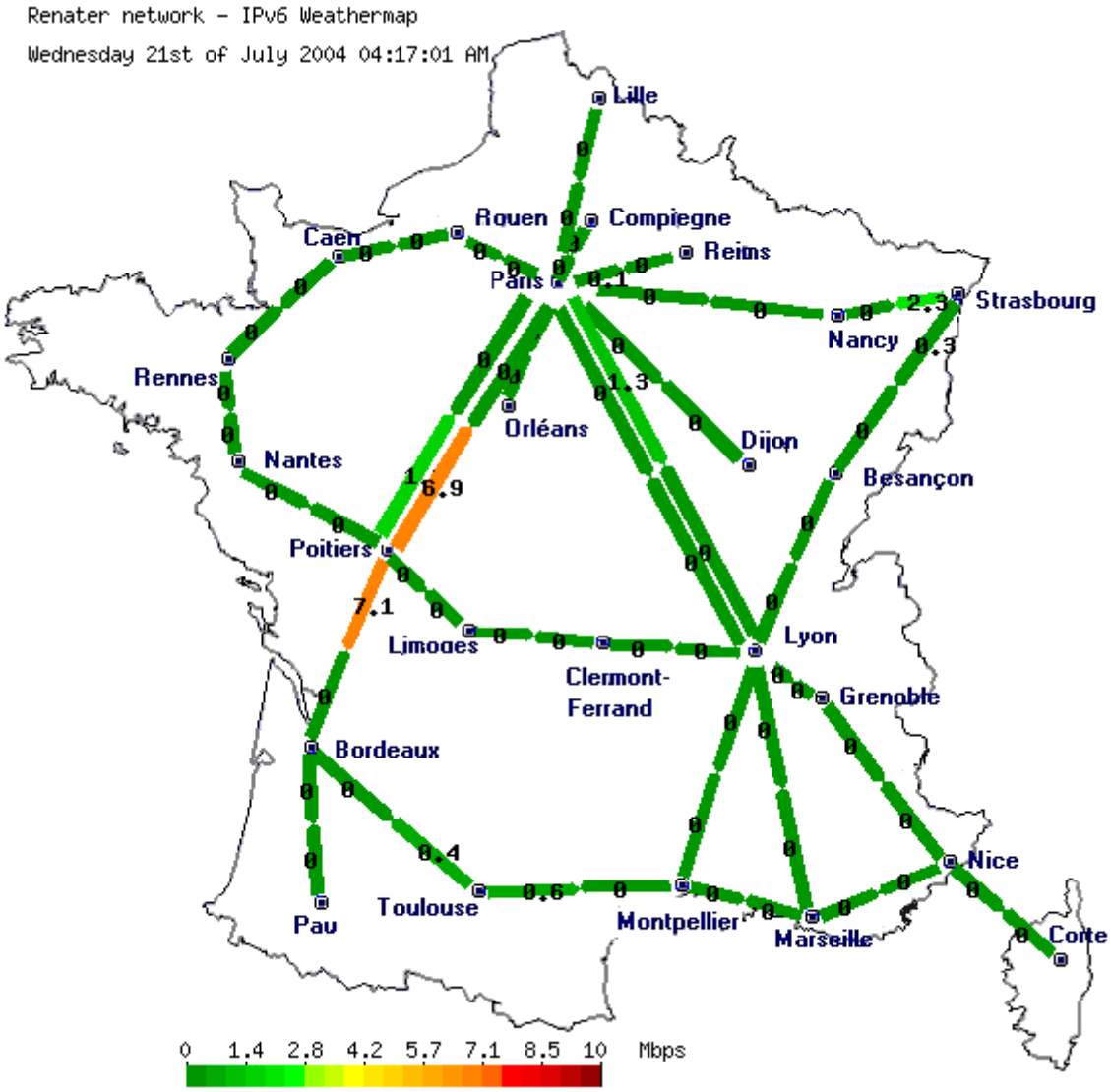
- **Trafic : MRTG**

MRTG permet de générer des graphes sur le trafic réseau. Une version IPv6 de MRTG a été développée par l'université de Rome-3. Elle permet d'interroger les équipements via SNMP sur un transport IPv6.
L'outil est disponible sur http://www.uniroma3.6net.garr.it/mrtg

Remarque : Cet outil ne résout pas le problème de la disponibilité des MIBs IPv6 au niveau des équipements réseau.

- **Trafic : Weather Map :**

Un Weather Map permet de présenter une carte topologique du réseau avec son trafic actuel. Il se base généralement sur des applications comme MRTG pour récupérer les données et afficher les graphes de trafic entre deux liens du réseau. Si nous voulons avoir un weather map représentant le trafic IPv6 uniquement, il est nécessaire que les MIB des routeurs distinguent bien le trafic IPv4 et IPv6. Or, actuellement, tous les constructeurs ne proposent pas cela. Si l'on dispose d'interfaces dédiées pour IPv6 (VLAN, etc), il est possible de différencier le trafic IPv6 du trafic IPv4 et de faire de la métrologie « standard ».



- **Analyse des flux :**

L'export des flux IPv6 étant possible sur certains équipements, des outils pour collecter ces flux ont été déployés :

  - Cisco propose l'outil NFC v5.0 qui est capable de collecter les flux netflow v9 (supportant IPv6)
  - IPFlow développé par l'UTC (http://www.ipflow.utc.fr/index.php/IPFlow) permet également de collecter des flux netflow au format v9 ainsi que le standard IETF IPFix.
  - Le collecteur RENETCOL développé par le GIP RENATER supporte également les flux netflow v9. Les premières versions avec quelques fonctionnalités sont disponibles sur http://pasillo.renater.fr/renetcol

2.3 – Les outils "faits maison":

La plupart des constructeurs n'ayant implémenté qu'une partie des MIBs définis par l'IETF et les plateformes de supervision n'ayant pas encore intégré la totalité des fonctionnalités nécessaires pour administrer convenablement un réseau IPv6, la supervision de certains services restent impossible avec les applications existantes. Aujourd'hui, pratiquement tous les langages de programmation supportent la pile IPv6, il est donc facile de développer ses propres scripts pour répondre à ces besoins.
Par exemple, nous pouvons avoir le besoin suivant : Connaître à intervalle régulier le nombre de routes IPv6 reçus sur les peerings BGP d'un équipement. Vu que les MIBs BGP4+ ne sont quasiment pas implémentées par les constructeurs, il est difficile de récupérer cette information via SNMP. Une façon de palier ce manque est de mettre en place un script qui se connecte régulièrement sur l'équipement en Telnet ou SSH et via des CLI (Command Line Interface) récupère cette information (par exemple, « show ipv6 bgp summary »). Il est clair que cette méthode est moins optimale qu'une simple récupération par SNMP (charge de la CPU plus importante, temps de réponse plus lent avec SSH ou Telnet que SNMP) mais elle permet cependant d'obtenir l'information souhaitée dans un premier temps.

Conclusion :

Aujourd'hui, un administrateur dispose d'un ensemble d'outils permettant d'administrer des réseaux IPv6. Cependant, un effort reste à faire pour atteindre le même niveau de supervision qu'en IPv4. Les récentes normalisations réalisées par des organismes comme l'IETF commencent à être mises en œuvre par les constructeurs d'équipements et par les éditeurs de logiciels de supervision. Ceci permet de se rapprocher d'un modèle de supervision standard.

Références:

Management IPv6 et CISCO
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65f3.html