La métrologie

- Métrologie : science de la mesure au sens le plus large. Mesure : opération qui consiste à donner une valeur à une observation.

- Métrologie réseau : mesure des performances du réseau :
  - Instrumenter le réseau et mesurer des caractéristiques du réseau
  - Analyser les mesures collectées
  - Repérer des comportements normaux/anormaux

- Supervision « classique/historique » (monitoring) informe en temps réel de l'état des équipements, par contre ne permet pas de savoir si le réseau assure parfaitement le service pour lequel il a été conçu.

- Métrologie : notion de qualité de service / Supervision : avant tout disponibilité.

- Monitoring : lancer un nombre élevé de vérifications sur les hôtes distants. La métrologie doit conserver un nombre plus restreints d'éléments mais sur une durée assez longue.

Métrologie et qualité de service

- Réseau est partagé par différentes applications qui ont des besoins (latence, variation de délai, débit) contradictoires.

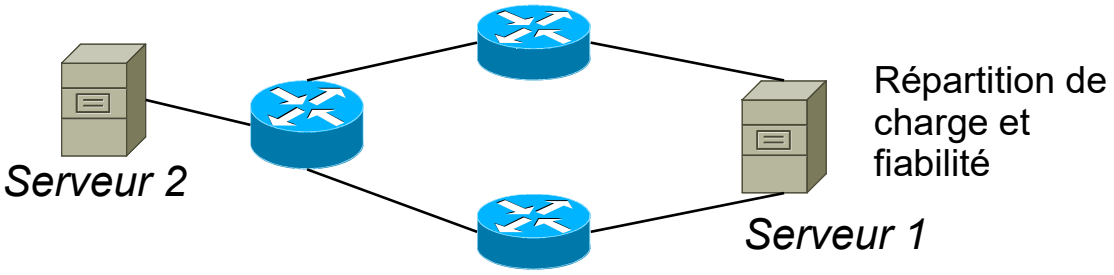
- Certaines applications sont « nativement » respectueuses des autres flux d'autres non. *Citez lesquelles et pourquoi ?*

- Des mesures (passives et actives) permettent de vérifier le bon fonctionnement du réseau et le respect du niveau de service.

- *Comment diagnostiquer un problème de performances qui se caractérise par une dégradation de service sans coupure ?*

Importance de la métrologie dans les réseaux actuels

- Algorithme de répartition de charges (ECMP) type round robin ==> nécessite parfois un ré-ordonnancement des paquets sur le serveur ==> consomme du temps CPU.



  - Comment savoir où passent les paquets d'une connexion ?

- Sécurité : attaque DoS, DDOS, détection de signaux « faibles », évasion de données.

- Complexification des protocoles de transport (IPSec, vpn tls).

- Forte augmentation du trafic UDP.

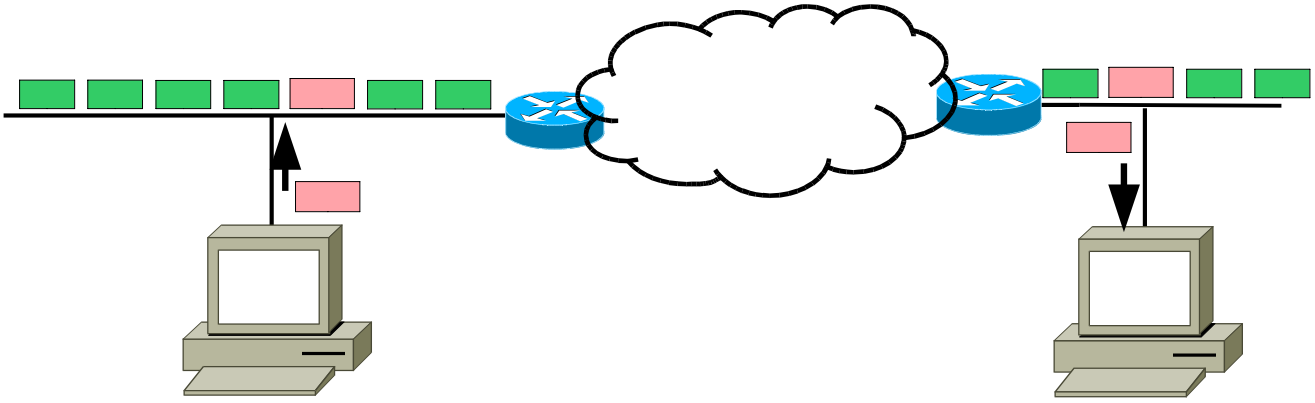
- Externalisation des services : Cloud (IaaS, PaaS, SaaS), Centrex IP.

- Effacement de la frontière entre LAN, MAN et WAN. Pourtant ce n'est techniquement pas la même chose :
  - Latence et nombre d'équipements traversés (files d'attentes)
  - Partage de l'infrastructure
  - Le WAN n'est pas supervisé par l'entreprise.

Les outils pour la métrologie

- Métrologie **passive** :
  - Capture et analyse du trafic généré par des utilisateurs.
  - Permet d'avoir une bonne vision du trafic utilisateurs (pic de trafic dans la journée ou dans la nuit lors des sauvegardes, applications générant le plus de trafic ....).
  - Par contre certaines caractéristiques sont inconnues :
    - date d'émission du paquet,
    - nombre de saut franchis par un paquet,
    - ce paquet correspond-t-il à une retransmission ?
  - Impossible de vérifier (avant mais aussi en temps réel) si un service peut être rendu.
  - Outils utilisés : SNMP, Wireshark, Netflow,

- Métrologie **active** :
  - générer du trafic (dont on connaît forcément la nature) et étudier le comportement (pertes, délai, débit) de ce trafic lorsqu'il traverse le réseau.



Machine 1 : génère des paquets « sonde » et les envoie dans le réseau

Machine 2 : (sonde) récupère les paquets générés par machine 1 et les analyse (durée de traversée du réseau, nombre de bits faux ...)

Métrologie – mesure active

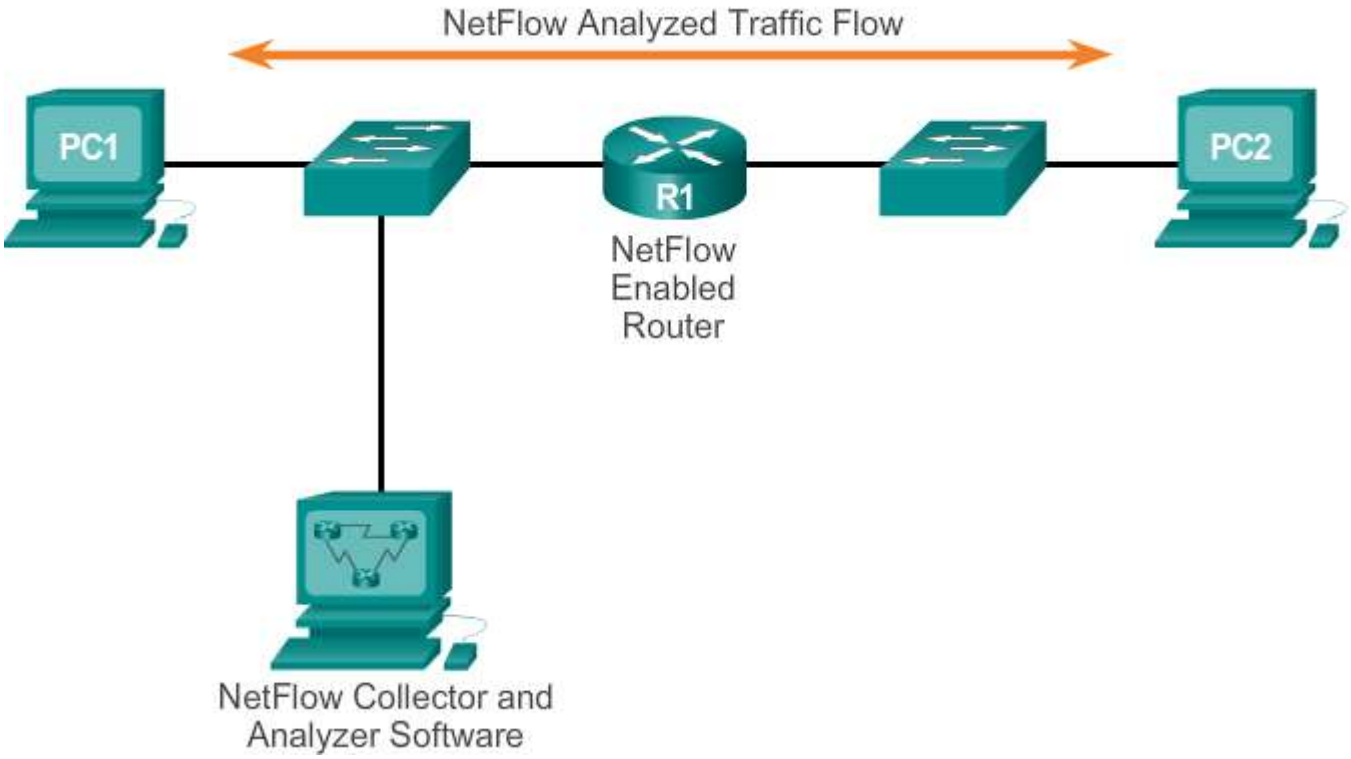
- Possibilité ainsi de :
  - Vérifier le bon fonctionnement du réseau (pertes, délai, bande passante ...),
  - Vérifier aux extrémités qu'un service fonctionne correctement (qualité de la voix dans une application ToIP, temps de réponse d'une base de données ...)
  - Reproduire un problème et mieux le diagnostiquer

	Mesures actives	**Mesures passives**
Principe	Générer du trafic dans le réseau pour en observer les caractéristiques : délai, taux de pertes, gigue …	Obtenir des informations sur le trafic utilisateur en un ou plusieurs points du réseau.
Avantages	On obtient des métriques (débit, latence…) sur un service que l'on utilise ou que l'on veut garantir.	Avoir une bonne vision de l'utilisation du réseau sans être trop intrusif. Assez facile à mettre en place (SNMP).
Inconvénients	Perturbations possibles introduites par le trafic de mesure. Nécessite des outils spécifiques.	Ne permet pas de déterminer si un service peut être garanti.
Exemples d'utilisation	Garantir l'utilisation d'applications temps réel : ToIP, visioconférence. Tests de fonctionnalités de QoS déployées.	Détecter des goulots d'étranglements, de dépassement de débit, d'attaques DOS, de virus …
Outils	ping, iperf, netperf, owamp, curl	SNMP, Netflow, Wireshark

Outils de mesures passives

- **SNMP**
  - Quels objets sont intéressants pour la métrologie réseau ?

- **Netflow - sflow**
  - Netflow : à l'origine développé par Cisco s'appuyant sur la notion de flux pour effectuer ses mesures ==> analyse de trafic.
  - Export d'informations vers un collecteur. Mécanisme Push contrairement à SNMP.
  - La version 9 est standardisée : RFC 3954.



Métrologie : outils de mesures passives

- L'agent Netflow (dans le routeur) maintient en mémoire une table des flux actifs (le cache netflow) à un instant t et compte le nombre de paquets et d'octets reçus pour chaque flux.

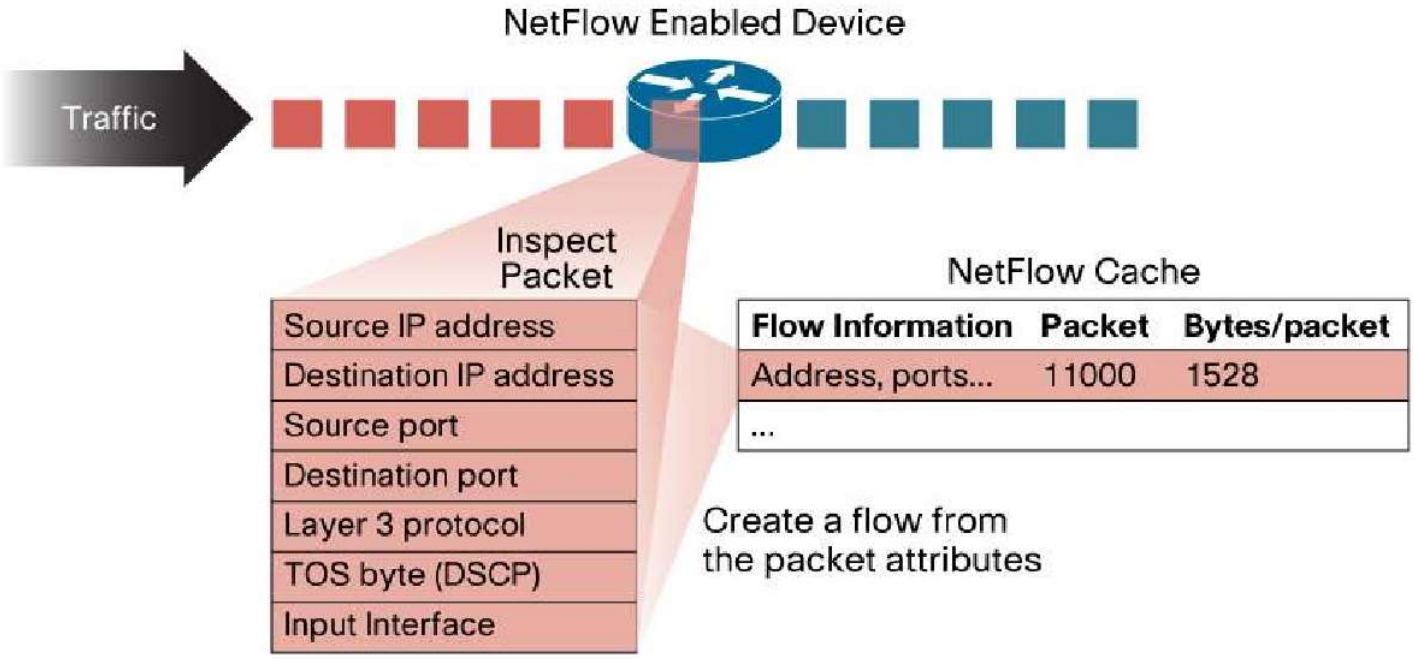
- Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes. IP Packet attributes used by NetFlow :
  - IP source address
  - IP destination address
  - Source port
  - Destination port
  - Layer 3 protocol type
  - Class of Service (DSCP)
  - Router or switch interface

- All packets with the same source/destination IP address, source/destination ports, protocol interface and class of service are grouped into a flow and then packets and bytes are tallied.

- Lorsqu'un flux a expiré, il est
  - supprimé du cache Netflow
  - exporté vers une machine de collecte au moyen de messages Netflow

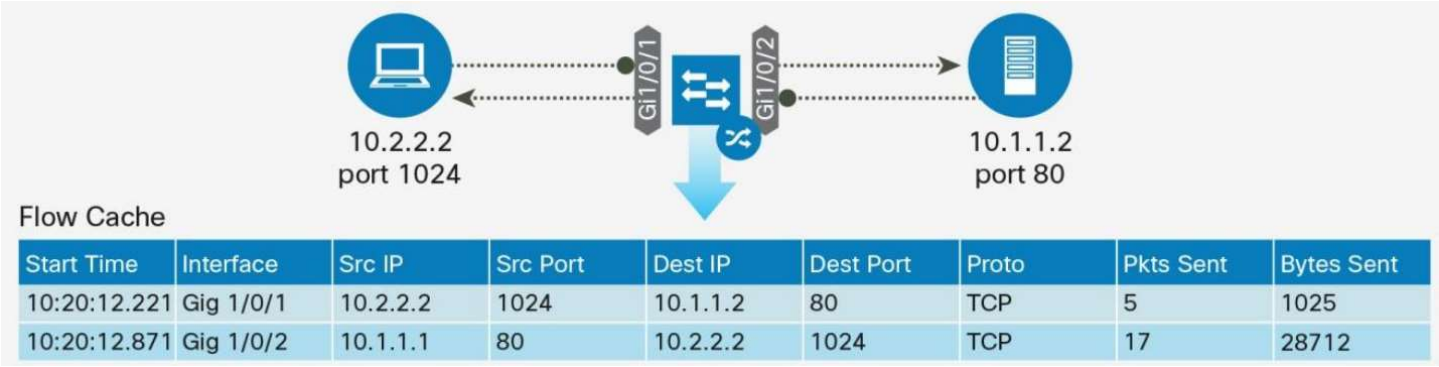
Outils de mesures passives - Netflow

- Rules for expiring NetFlow cache entries include:
  - Flows which have been idle for a specified time are expired and removed from the cache.
  - Long lived flows are expired and removed from the cache. (Flows are not allowed to live more than 30 minutes by default; the underlying packet conversation remains undisturbed.)
  - As the cache becomes full a number of heuristics are applied to aggressively age groups of flows simultaneously.
  - TCP connections which have reached the end of byte stream (FIN) or which have been reset (RST) are expired with small delay.



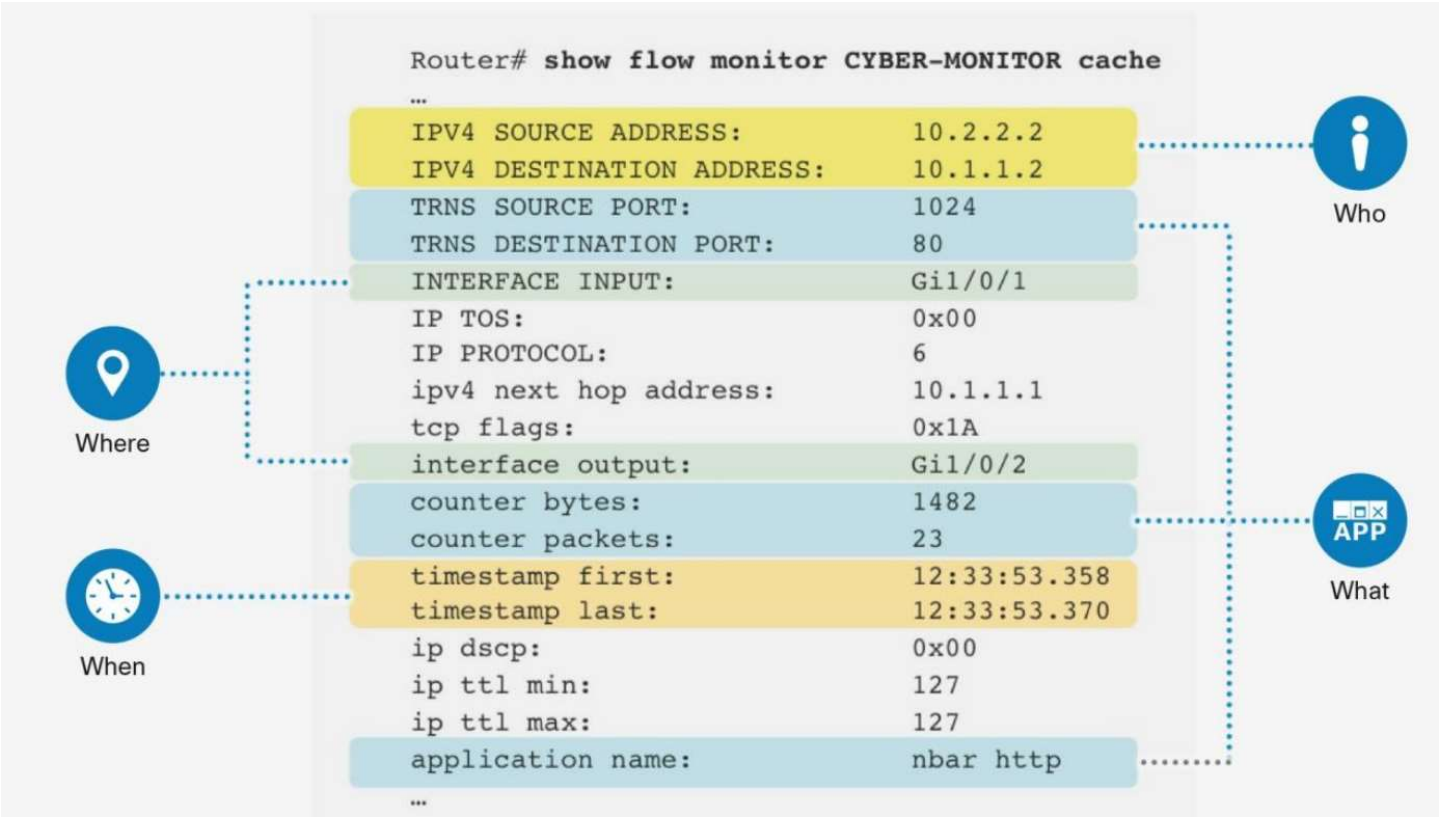
Outils de mesures passives - Netflow

Exemples de cache Netflow



Flow Cache

Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent
10:20:12.221	Gig 1/0/1	10.2.2.2	1024	10.1.1.2	80	TCP	5	1025
10:20:12.871	Gig 1/0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712



Outils de mesures passives - Netflow

- Différences Netflow – sflow :
  - Netflow : le collecteur ne reçoit que les informations générales sur le flux (metadata). Tous les paquets traversant l'équipement peuvent être analysés ou on analyse par exemple qu'un paquet sur 10.
  - Sflow (sampled flow) : l'équipement prélève aléatoirement des trames circulant et les renvoie à un collecteur dans un paquet UDP.
    - C'est le collecteur qui analyse par la suite les trames : retrouve IP-sce, IP-Dest, Ports... et compte les octets / paquets.
    - A 1 Gbit/S le rythme d'échantillonage est de une trame toutes les 1000 trames.

Métrologie active - Métrique réseau

Qu'est ce qu'une métrique ?

- Caractéristique du comportement d'un réseau.
- Elle sert à qualifier une situation (normale /anormale)
- Elle est exprimée dans une unité standard et permet de faire des comparaisons :
  - dans le temps :
    - Après un changement de configurations
    - Après une panne, un changement de route
  - dans l'espace
    - Entre un poste et deux autres postes (comparaison des situations)
    - Entre deux réseaux dont les topologies sont proches mais les performances différentes
- Les métriques sont utiles :
  - pour les fournisseurs d'accès
  - pour les utilisateurs
  - afin qu'ils comprennent les performances qu'ils fournissent ou qu'ils perçoivent.
- Les métriques IPPM IP Performance Metrics (RFC 2330, RFC 4148, RFC 6248...). Cf IP performance metrics working group.
  - Connectivity (ping)
  - One-way delay
  - One-way Packet Loss
  - Delay Variation (Gigue-Jitter)
  - Bulk Transfer Capacity (Bande passante disponible à un moment donné)
  - ...

Métrologie active - Métrique IPPM

Métrique IPPM Wire Time

- Inadéquat que les mesures soient faites au niveau du système ou au niveau applicatif :
  - interruptions matérielles introduisent des délais inacceptables
  - gestion du temps partagé entre les applications

- RFC recommande que la mesure du temps de réception ou d'émission d'un paquet soit réalisée le « plus près possible du fil ».

Mesure du délai

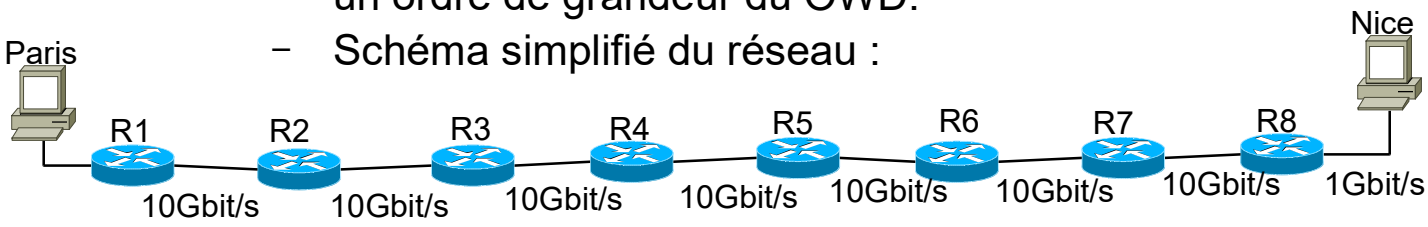
- One Way Delay.
  - Quel autre terme est généralement utilisé pour le OWD ?
  - Expliquer une méthode permettant de mesurer le OWD. Justifier qu'il est plus simple de mesurer le RTT.
  - Quelle est la difficulté associée à la mesure du OWD ?
  - Par quels moyens techniques cette difficulté peut-elle être gérée ?
  - Pourquoi mesurer OWD et ne pas se contenter de RTT ?

Métrologie active- Métrique IPPM - OWD

- Composition du OWD sur une liaison point à point :
  - OWD = Σ (sur chaque lien)
    - Temps de propagation (la plupart du temps dans la fibre)
    - Temps d'insertion d'un paquet sur une ligne physique (Serialization Delay)
    - Temps de traitement dans les organes intermédiaires (Queuing delay).
  - On considère deux machines reliées par une fibre optique de 200km (vitesse de propagation 0,7c) à 1Gbit/s. Calculer les temps de propagation et d'insertion et le OWD.

➢ Exercice

- On considère une liaison Paris → Nice, on souhaite avoir un ordre de grandeur du OWD.
- Schéma simplifié du réseau :



- Entre Paris et Nice au total 1200 km de fibre. On considère : vitesse de propagation dans une fibre : environ 0,66c.
  - Calculer le temps de propagation total dans la fibre.
- On considère que R1 et R8 fonctionne en mode store and Forward. R2 à R7 fonctionnent en mode Cut through.
  - Calculer le temps d'insertion (serialization delay) pour une trame de 1450 octets, pour A, R1 et R8.
- On mesure un OWD de 8,97 ms.
  - Sachant que l'on a 8 routeurs, calculer le queuing delay moyen par routeur.

  Que peut-on déduire si cette valeur de OWD varie ?

Métrologie active - Métriques IPPM - Suite

- Autres métriques IPPM :
  - One Way Packet Loss
  - Connectivity
  - Delay variation (Gigue – Jitter). Pour applications temps réel : voip , visio conf.

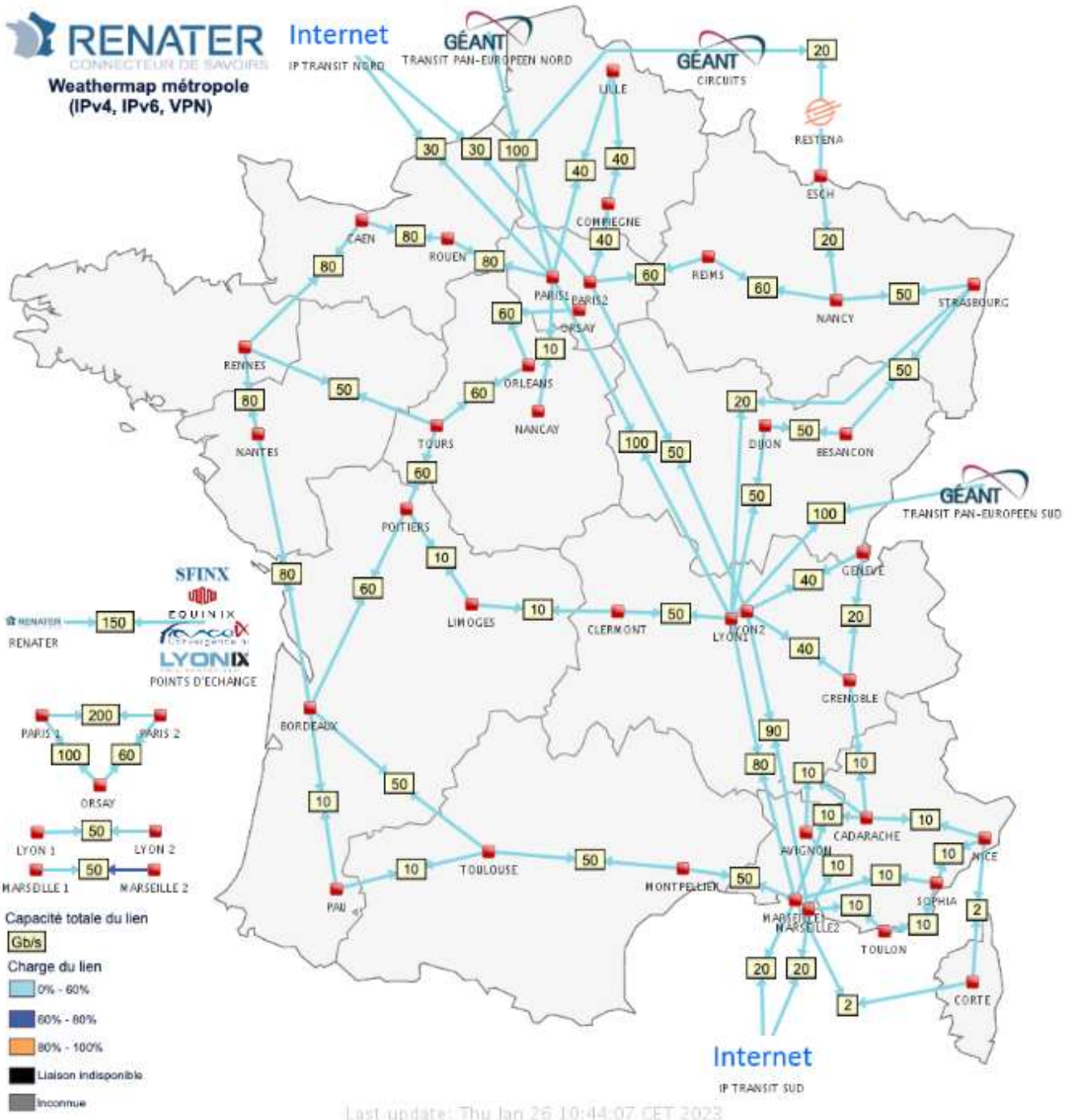
- Deux types de mesure :
  - Mesures au sein du réseau ==> superviser la santé du réseau
  - Mesures de bout en bout ==> Vision utilisateur final, supervision des applications.

- Recherche d'outils sur Internet (mots clés à utiliser) :
  - Network monitoring tools open source
  - Speed network measurement
  - bandwidth speed test tools open source
  - benchmarking network monitoring throughput
  - One way delay

- A One-way Active Measurement Protocol (OWAMP).
  - https://github.com/perfsonar/owamp

Mesures actives – outils et méthodes

Exemple Weathermap Renater



Mesures actives – Outils bout en bout

Mesures de bout en bout et QoE

- QoE : Quality of Experience :
  - mesurer le ressenti utilisateur
  - établir des références
  - diagnostiquer un problème ou surveiller des applications.

- Outils dans les OS pour mesurer de bout en bout : ping, traceroute
  - Ces outils présentent des limites ==> attention à l'interprétation des résultats :
    - Les chemins aller et retour peuvent être différents.
    - Paquets ICMP pas traités dans les routeurs comme les autres paquets (souvent traités en CPU)

- Préférer l'utilisation d'outils simulant des requêtes applicatives :
  - les outils se comportent en tant que client et interrogent les applications que l'on veut superviser
  - Exemple :
    - curl -o /dev/null -s -w 'Total: %{time_total}s\n' https://www.univ-smb.Fr/lorawan
    - disponibilité de l'application
  - temps de réponse applicatif

- Pour de la QoE on instrumente directement l'application de l'utilisateur (téléphone, client lourd, client web).

- Les mesures doivent absolument être corrélées à des mesures réseau pour pouvoir différencier des problèmes réseaux de problèmes applicatifs.

Résolution des problèmes de performance de bout en bout

Qu'est ce qu'un problème de performance ?

- Problème de performance : dégradation sans coupure du service
  - problème généralement non permanent : des fois ça fonctionne, des fois ça ne fonctionne pas. Exemples :
    - voix saccadée
    - temps de réponse d'un serveur plus élevé que d'habitude

- Difficultés :
  - les dégradations perçues au niveau applicatif, donc par l'utilisateur final.
  - c'est souvent lui qui signale les problèmes de performances.
  - Déploiement d'outils de QoE

- Nécessité d'avoir mis en place des outils pour :
  - Comparer des situations
  - Être proactif : anticiper sur le problème ou à minima déceler les problèmes de performances avant l'utilisateur final
  - Faciliter la résolution du problème

- Pendant la résolution du problème, les utilisateurs doivent être informés que le service est dégradé

Résolution des problèmes de performance de bout en bout

Démarche pour résoudre un problème de performance

- Collecte d'informations :
  - Auprès de l'utilisateur final
    - Attention : informations à prendre au conditionnel
    - Les performances perçues par l'utilisateur sont différentes des performances réseau: performances perçues par l'utilisateur dépendent de l'application.
    - Utilisation de métriques applicative ex VoIP: MOS (Mean Opinion Score)
  - Sur son propre réseau
  - Informations mises à disposition par les autres réseaux
  - Vérifier qu'il s'agit d'un problème réseau, d'un problème applicatif, ou autres : Base de données, CPU/mémoire de la machine, etc

- Investigation/mesures/tests :
  - Faire des tests de bout en bout avec les machines impliquées
  - Faire des tests à partir de systèmes dédiés

- Vérification des informations aux extrémités :
  - Le type d'application/logiciel et son mode de fonctionnement
  - Les systèmes d'exploitation (version, noyau, etc.)
  - Cartes réseau, processeur, disque dur, mémoire vive

Haute disponibilité - Introduction

Introduction

- Définition : *Disponibilité* :
  - Probabilité qu'un service fonctionne lorsque l'on en a besoin.
  - Pourcentage de temps pendant lequel un service est accessible.
  - Sous forme d'équation : MTBF= MTTF + MTTR
    - Mean Time Between Failure
    - Mean Time To Failure
    - Mean Time To Repair

- Règle des 9 :
  - 2 neuf : 99 % → arrêt du service ~ 4 jours par an
  - 3 neuf : 99,9 % → arrêt du service ~ 9 heures par an
  - 4 neuf : 99,99 % → arrêt du service ~ 1 heure par an
  - 5 neuf : 99,999 % → arrêt du service ~ 5 minutes par an

- Nécessité de la haute disponibilité :
  - Dépendance par rapport aux services ==> Impacts en cas d'indisponibilité
  - Palier les arrêts planifiés et non planifiés
  - Pas de système 100% fiable

- Complexité (et donc les coûts) dépendront des objectifs S'assurer de ses besoins réels.

Le maillon faible (Single Point Of Failure)

  - Définir la chaîne complexe assurant le service
  - Identifier les «points durs» (SPOF)

- Disponibilité du service = disponibilité du SPOF le plus faible