Rapport scientifique du projet SwissQuantum (10 mars 2010 / G Litzistorf)

Executive summary

Des établissements (FR-GE-VD) de la HES-SO ont collaboré avec la société IdQuantique[1] pour valider dans la durée des échanges chiffrés entre 3 sites (hepia-CERN-UniGE) du canton de Genève. Rappelons que la confidentialité obtenue lors d'un payement sécurisé est basée sur le chiffrement des données à partir d'un secret partagé par les 2 extrémités que nous appellerons Alice et Bob. Il existe diverses méthodes plus ou moins sûres pour permettre à Alice de transmettre ce secret à Bob. La technologie développée par l'équipe du professeur Nicolas Gisin (UniGE) et commercialisée par IdQuantique utilise les lois de la physique quantique pour générer aux deux extrémités ce secret sans qu'il ne soit transmis sur la fibre optique reliant Alice et Bob.
Le travail de l'éventuel espion appelé Charly, consistant à écouter le flux de données chiffrées pour le décrypter, est rendu encore plus difficile si ce secret change fréquemment (chaque minute).
La HESSO a d'abord défini un contexte applicatif qui simule les besoins d'un client potentiel tel qu'une banque répartie sur 3 sites pour proposer une architecture redondante capable de faire face à la panne d'un lien intersites tout en garantissant certaines classes de trafic. Cette validation avait aussi comme objectifs de montrer que les opérations de chiffrement (Alice) et de déchiffrement (Bob) ne pénalisaient pas des paramètres tels que temps de latence ou débit utile. Le côté innovant de ce projet a été apporté par l'adaptation du système Linux (IPSec) à être compatible avec les clés (secrets) générés périodiquement.

Objectifs et structure du document

Ce document donne une synthèse des travaux scientifiques réalisés dans le cadre de ce financement. Destiné à un large public (étudiants, professionnels, curieux, …), son contenu se veut compréhensible et évite ainsi d'entrer dans le niveau de détails exigé par la configuration des divers équipements.

L'objectif de ce document est aussi de susciter l'intérêt du lecteur pour qu'il n'hésite pas à aller poser ses questions aux personnes qui ont participé à ce projet.

	Structure du rapport	Auteur
1.	Quels sont les principaux objectifs du projet définis dans la demande ?	Litzistorf
2.	Qui a participé a ce projet ?	Tous
3.	Calendrier : quelles sont les principales dates ?	Litzistorf
4.	WP1 : contexte applicatif	Litzistorf
5.	WP2 : architecture réseau, priorités des flux et redondance	Litzistorf
6.	WP3 : mesure de la qualité de service	Buntschu
7.	WP4 : adaptation du code IPSec-Linux au système quantique de distribution des clés	Junod
8.	WP5 : résultats	Ribordy-Trinkler
9.	Valorisation, conclusion et suite	Tous

Site du projet : http://www.swissquantum.com/

[1] http://www.idquantique.com/

1 Quels sont les principaux objectifs du projet définis dans la demande ?

Ce projet comprend 5 *Work Packages* (WP)

- 3 établissements (FR-GE-VD) de la HESSO participent à ce projet
- Chaque WP est sous la responsabilité d'un établissement
- GE a la responsabilité globale (requérant principal)
- Cette étude a été financée par le réseau de compétence en TIC (RCSO-TIC[2]) de la HESSO

WP1 (GE)
Définir un contexte applicatif d'échange qui simule les besoins d'un client potentiel tel qu'une banque (applications critiques au temps, applications qui exigent de la qualité de service, …)

WP2 (GE)
Proposer une architecture réseau capable d'effectuer les opérations de routage , de gestion des priorités des flux et de redondance

WP3 (FR)
Générer les divers flux définis au §1 et mesurer les paramètres tels que temps de réponse, débit utile, perte de paquets, taux de disponibilité, …

WP4 (VD)
Adapter la partie IPSec du noyau Linux 2.6 au système quantique de génération des clés.

WP5 (GE)
Afficher les résultats aux visiteurs de Telecom 2009 (5-9 oct 2009)

Commentaires :

- **Réseau privé réparti sur 3 sites**
  Le scénario proposé par la société Id Quantique comprend 3 sites (hepia – UniDufour – CERN) situés dans le canton de Genève

Fibre optique CERN-hepia : 17 km
Fibre optique CERN-UniGE : 14 km
Fibre optique hepia-UniGE : 3 km

[2] http://tic.rcso.ch/

2 Qui a participé à ce projet ?

Pour http://hepia.hesge.ch/

- Gérald Litzistorf, professeur, responsable du projet — gerald.litzistorf@hesge.ch
- José Tavares, ingénieur HES, assistant de recherche — jose.tavares@hesge.ch

Pour http://www.eia-fr.ch/

- François Buntschu, professeur — francois.buntschu@hefr.ch
- Didier Perroud, ingénieur HES, assistant de recherche — didier.perroud@hefr.ch

Pour http://www.heig-vd.ch/

- Pascal Junod, professeur — pascal.junod@heig-vd.ch
- Stefano Ventura, professeur, directeur www.iict.ch — stefano.ventura@heig-vd-ch
- Raphael Voirol — raphael.voirol@heig-vd.ch
- Patrick Monbaron — patrick.monbaron@heig-vd.ch

Pour http://www.idquantique.com/

- Grégoire Ribordy, directeur — gregoire.ribordy@idquantique.com
- Patrick Trinkler — patrick.trinkler@idquantique.com
- Samuel Robyr — samuel.robyr@idquantique.com
- Laurent Monat — laurent.monat@idquantique.com
- Jean-Benoît Page — jeanbenoit.page@idquantique.com
- Matthieu Legré — matthieu.legre@idquantique.com

Pour http://www.gap-optique.unige.ch/

- Nicolas Gisin, professeur, directeur — nicolas.gisin@unige.ch
- Robert Thew — robert.thew@unige.ch

Pour http://www.pictet.com

- Juan Garrido, — jgarrido@pictet.com

3 Calendrier : quelles sont les principales dates ?

11 mars 2008	Réunion de travail chez Id Quantique
26 mars 2008	Réunion de travail chez Id Quantique
31 mars 2008	Formation dispensée chez ID Quantique par spécialiste Senetas (participation de José Tavares)
3 avril 2008	Réunion de travail à UniGE-GAP pour le montage d'une demande nano-tera
10 avril 2008	Réunion de travail chez Id Quantique
22 mai 2008	Réunion de travail avec J. Garrido
29 mai 2008	**Décision du financement par le Comité scientifique du RCSO-TIC**
16 juin 2008	Présentation des buts du projet au Comité scientifique du réseau national ICTnet
1 juillet 2008	Séance préparatoire à EIG
Sept 2008	Début du travail de diplôme de Luis Couso (Prof. Fabien Vanel) en collaboration avec Id Quantique
15 octobre 2008	Séance de démarrage du projet à EIG
12 novembre 2008	Réunion de travail chez Id Quantique
Décembre 2008	Défense de diplôme
16 janvier 2009	Réunion de travail chez Id Quantique
29 janvier 2009	Réunion de travail HESSO à Lausanne
18 février 2009	Réunion de travail à hepia
25 mars 2009	Formation *Introduction à la virtualisation* dispensée à 10 personnes de l'économie
Fin mars 2009	Mise en service de la couche quantique
12 avril 2009	Indisponibilité de G. Litzistorf pour 4 semaines
7 mai 2009	Réunion de travail chez Id Quantique
26 juin 2009	Réunion de travail à hepia
19 août 2009	Réunion de travail à hepia
5-9 octobre 2009	**Exposition Telecom 2009 à Genève-Palexpo**
8 octobre 2009	Evénement *A Quantum Leap for Telecommunications, Today and Tomorrow* organisé par les pôles QP (EPFL), MaNEP (UniGE) et MICS (EPFL).

Remarque : l'établissement EIG (Ecole d'ingénieurs de Genève) s'appelle hepia (haute école du paysage, d'ingénierie et d'architecture) depuis le 1er jan 2009

Commentaires :

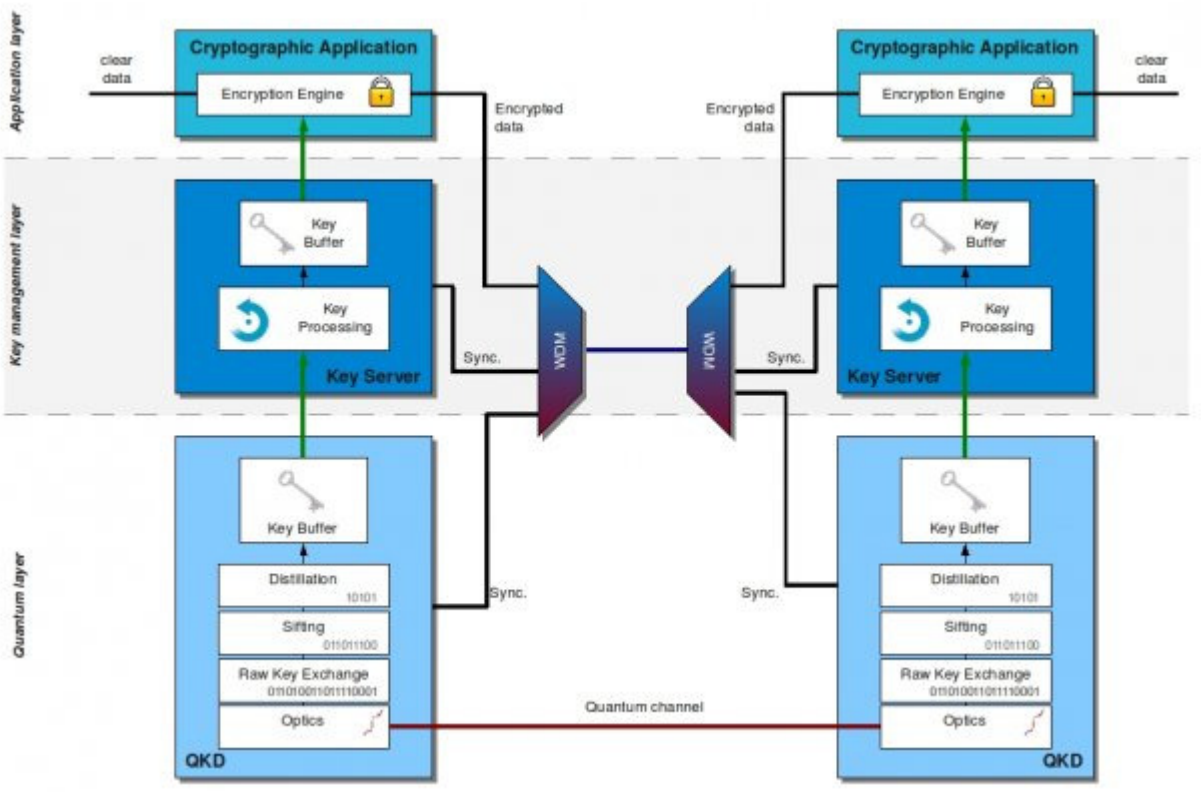
- Le financement de ce projet a porté sur une durée de 12 mois
- La fin du projet a coïncidé avec l'exposition Telecom 2009 à Genève-Palexpo

4 WP1 : contexte applicatif

4.1 Quelle sécurité voulons-nous démontrer ?

- La **disponibilité** (couche quantique, couche utilisateurs) est un des critères de sécurité que nous devons démontrer. Elle tirera profit de la topologie en triangle des 3 sites. Un des objectifs pour l'exposition Telecom 2009, consiste à valider la disponibilité de la couche quantique sur une durée de 6 mois.

- **Modèle en couches**
  La figure ci-dessous décrit les principales entités



Application layer qui chiffre et déchiffre selon des algorithmes éprouvée comme AES (en bleu clair sur l'image)

Quantum layer basé sur la technologie développé à UniGE-GAP par l'équipe du Dr Nicolas Gisin et commercialisé par la société Id Quantique (équipement foncé du bas)

- **La confidentialité** offerte par ce système utilise donc un chiffrement symétrique AES qui dispose en permanence de secrets partagés produits par les lois de la physique quantique.

  - Le canal des données chiffrées est donc susceptible d'être écouté alors que l'écoute du canal quantique va le perturber et donc le rendre inutilisable. En l'absence de clé quantique, les équipements AES utilisent leur propre mécanisme de secret partagé.

  - Il n'est pas prévu dans ce projet d'évaluer l'intégrité des données.

  - Le scénario type s'apparente à la constitution d'un réseau privé virtuel composé de 3 sites distants protégés chacun par une sécurité physique approprié.

4.2 Débit binaire, priorité des flux et qualité de service

L'utilisateur disposera de 3 canaux sécurisés offrant chacun un débit binaire de 1 Gbit/s.

Nous estimons que la gestion de cette bande passante ne constitue pas un domaine de recherche particulier puisque les méthodes existent et ont été validées.

Nous mettrons donc en œuvre **2 variantes** capables de faire face à une demande supérieure :
- La première sera basée sur le modèle *Differentiated Services* ou *Controlled Load Services* (rfc 2211[3]) en définissant des niveaux de priorité *(high – medium – low)*
- La seconde va réserver des ressources selon le modèle *Integrated Services* ou *Guaranted Services* (rfc 2212[4])

4.3 Classification des flux et qualité de service

Ce projet doit contrôler que les principales applications sont compatibles avec les caractéristiques du canal chiffré.
Il s'agit donc d'identifier les **applications critiques** et de mesurer l'influence du chiffrement sur les paramètres de transmission (taux d'erreur, temps de latence,)

Ces flux sont généralement du type ***elastic traffic*** ou ***inelastic traffic*** *(real time)* :
- La première catégorie *(elastic traffic)* regroupe des applications traditionnelles client - serveur (telnet, www, …) pourvues de mécanismes de contrôles d'erreur et de flux. Elles peuvent donc utiliser un canal qui présente un certain taux d'erreur et des variations du temps de latence.
- La seconde catégorie *(inelastic traffic)* concerne des **applications critiques aux temps**, telles la vidéo ou la téléphonie, sensibles au temps de transit (latence), à la gigue ainsi qu'à la bande passante

4.4 Quelles sont les applications critiques ?

Les applications critiques au temps comme la voix et la vidéo vont rapidement signaler des problèmes (craquement de la voix, arrêt de la vidéo) en cas de performances insuffisantes.

La voix sur IP (VoIP) devient inconfortable avec un temps de transit supérieur à 70-80 ms.
Il convient aussi de prendre en compte la variation (gigue) du temps de latence.

Technologies envisagées : http://www.videolan.org/vlc/, VoIP

Les applications synchrones de type SAN *(fiber channel)* sont sensibles au temps de latence (30 ms)

Il est également prévu de contrôler la compatibilité des trames Ethernet dites Jumbo

Ne pouvant pas tester toutes ces applications, nous préférons mettre l'accent sur la mesure de ces paramètres (voir §6)

---

[3] RFC 2211, Specification of the Controlled-Load Network Element Service, http://www.ietf.org/rfc/rfc2211.txt

[4] RFC 2212, Specification of Guaranteed Quality of Service, http://www.ietf.org/rfc/rfc2212.txt

5 WP2 : architecture réseau, priorités des flux, redondance et infrastructure

5.1 *Backbone* de niveau 2 ou de niveau 3 ?

Les choix opérés doivent simuler au mieux le réseau informatique d'une entité répartit sur 3 sites.

Après analyse, le *backbone* de niveau 2 semble représentatif. Il allie simplicité, performance, redondance, transparence et maturité :

- Simplicité au niveau du plan d'adressage, des VLANs et des configurations des équipements
- Performances des commutateurs sans surcoût dû aux protocoles grâce à une technologie évolutive (100 Mbit/s, 1 Gbit/s, 10 Gbit/s, …)
- Redondance du type *Fast Spanning Tree Protocol*
- Transparence pour les couches supérieures
- Maturité avec des technologies largement déployées

D'un point de vue fonctionnel, ce réseau sera vu comme un réseau Ethernet unique réparti dans un bâtiment sur 3 étages alors qu'il sera déployé sur 3 sites distants.

5.2 Equipements utilisés

Les 6 commutateurs Extreme Summit[5], offerts par la banque Pictet&Cie à hepia, semblent parfaitement convenir pour construire ce réseau.

Les 2 variantes (niveau 2 ou niveau 3) ont été configurée pour des tests en interne à hepia.

5.3 Conception du réseau

Chaque site (hepia-Uni-CERN) disposera d'un **commutateur Extreme Summit**
Les locaux mis à disposition sont fermés à clé
Il n'est pas prévu d'activer les systèmes redondants d'alimentation car chaque commutateur ne dispose pas de cet accessoire et l'échange d'un commutateur devrait être possible dans l'heure

Il n'est pas prévu de prendre en compte des attaques classiques de niveau 2 telles que *MAC flooding*, *ARP poisoning*, *VLAN attack*, … car les méthodes correctives sont connues.

La **redondance des liens** permettra de garantir qu'un site A peut toujours atteindre les sites B et C si un des 3 liens est en panne.

Nous renonçons d'utiliser le *Spanning Tree Protocol* qui présente quelques défauts majeurs :

- Temps de convergence (30 s) élevé
- Indisponibilité du réseau pendant le temps de convergence
- Difficulté de dépanner lorsque la convergence n'est pas obtenue

En remplacement, Extreme Networks propose *Ethernet Automatic Protection Switching* (EAPS) décrit dans un *white paper* [6] :
The networking industry has relied on the Spanning Tree Protocol (STP) in large Layer 2 networks to provide a certain level of redundancy. However, STP has proven inadequate to provide the level of resiliency required for real-time and mission critical applications. It is important to note that the entire industry has recognized that a new technology is needed to replace STP and many vendors are in the process of developing pre-standard technologies to meet that requirement. Ethernet Automatic Protection Switching (EAPS) is Extreme Networks' solution for fault-tolerant Layer 2 ring topologies. EAPS is responsible for a loop-free operation and a sub-second ring recovery. This revolutionary technology provides end users with a continuous operation usually only available in voice networks and does so with radical simplicity.

EAPS est décrit dans la rfc 3619 [7] (octobre 2003)

---

5 Summit 48SI , http://www.extremenetworks.com/products/summit-48si.aspx
6 http://www.extremenetworks.com/libraries/whitepapers/WEAPS_1293.pdf
7 http://www.faqs.org/rfcs/rfc3619.html

La segmentation d'un réseau local en VLAN *(Virtual LAN)* fait partie des bonnes pratiques *(best practices)* d'un réseau d'entreprise.
Voir document "Virtual LAN Security Best Practices" [8]
4 VLANs *(magament – high – medium – low)* sont ainsi créés selon une attribution par port

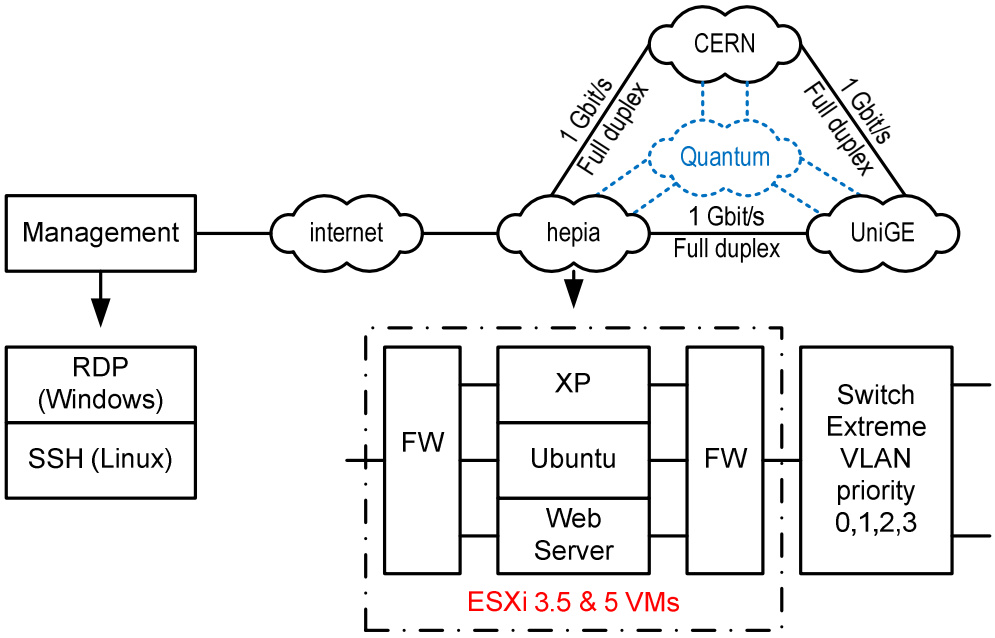
5.4 Tests unitaires

Les tests unitaires suivants ont été réussis avec succès :

- Contrôler que les ports d'interconnexion sont bien configurés pour un débit binaire de 1 Gbit/s et pour le mode *full duplex*
- Contrôler l'excellente disponibilité des sites grâce à l'efficacité du protocole EAPS
- Contrôler le bon fonctionnement du mécanisme de mise en priorité des flux à partir des VLANs.
  En cas de congestion (surcharge), les paquets générés sur le VLAN-low sont perdus

5.5 Infrastructure pour administrer et valider la couche quantique

La figure ci-dessous illustre l'infrastructure mise à disposition de UniGE-GAP et Id Quantique via *internet* pour administrer et valider la couche quantique :



- Accès à un système Windows XP depuis un client distant RDP
- Accès à un système Ubuntu Desktop depuis un client SSH
- *Firewall* (FW) côté *internet* pour n'autoriser que les flux légitimes
- *Firewall* (FW) côté *intranet* pour limiter les accès au réseau de gestion (défense en profondeur)
- *Web Server* décrit dans §8

Nous disposions de matériel PC *(low cost)* [9] et avons profité d'utiliser la virtualisation gratuite que VMware propose avec son *hyperviseur* ESXi [10].

8 http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf
9 http://www.tdeig.ch/vmware/Montage_PC_Gigabyte.pdf
10 http://www.vmware.com/products/esxi/

Le bilan, après plus de 6 mois d'exploitation, est très positif :

- Réelle économie de PC
- Facilité d'utilisation avec l'outil Virtual Infrastructure Client [11] (GUI sous Windows)
- Très bonne stabilité
- Bonne performance
- Simplicité des sauvegardes

La décision a été prise de privilégier cette virtualisation ESXi dans les activités du laboratoire avec un certain succès puisque 26 personnes (payantes) ont suivi notre formation d'un jour "Introduction à la virtualisation" en 2009.

Pour plus de détail, consulter la rubrique VMware du site www.tdeig.ch

5.6 Documentation interne produite (non publiée)

§2.4	Configuration des commutateurs	Activer EAPS 3 VLANs applicatifs + VLAN dedié à EAPS + VLAN hepia Associer des priorités à chaque VLAN Autoriser l'administration à distance
§2.2	Liste des adresses IP	
§2.3.1	Configuration PC-ESXi Management	Voir §5.5
§2.3.2	Configuration PC-ESXi de mesure	Voir §6
§2.3.3	Configuration PC Manager	Voir §6.5
§2.3.4	Configuration PC IPSec	Voir §7

5.7 Schéma réseau

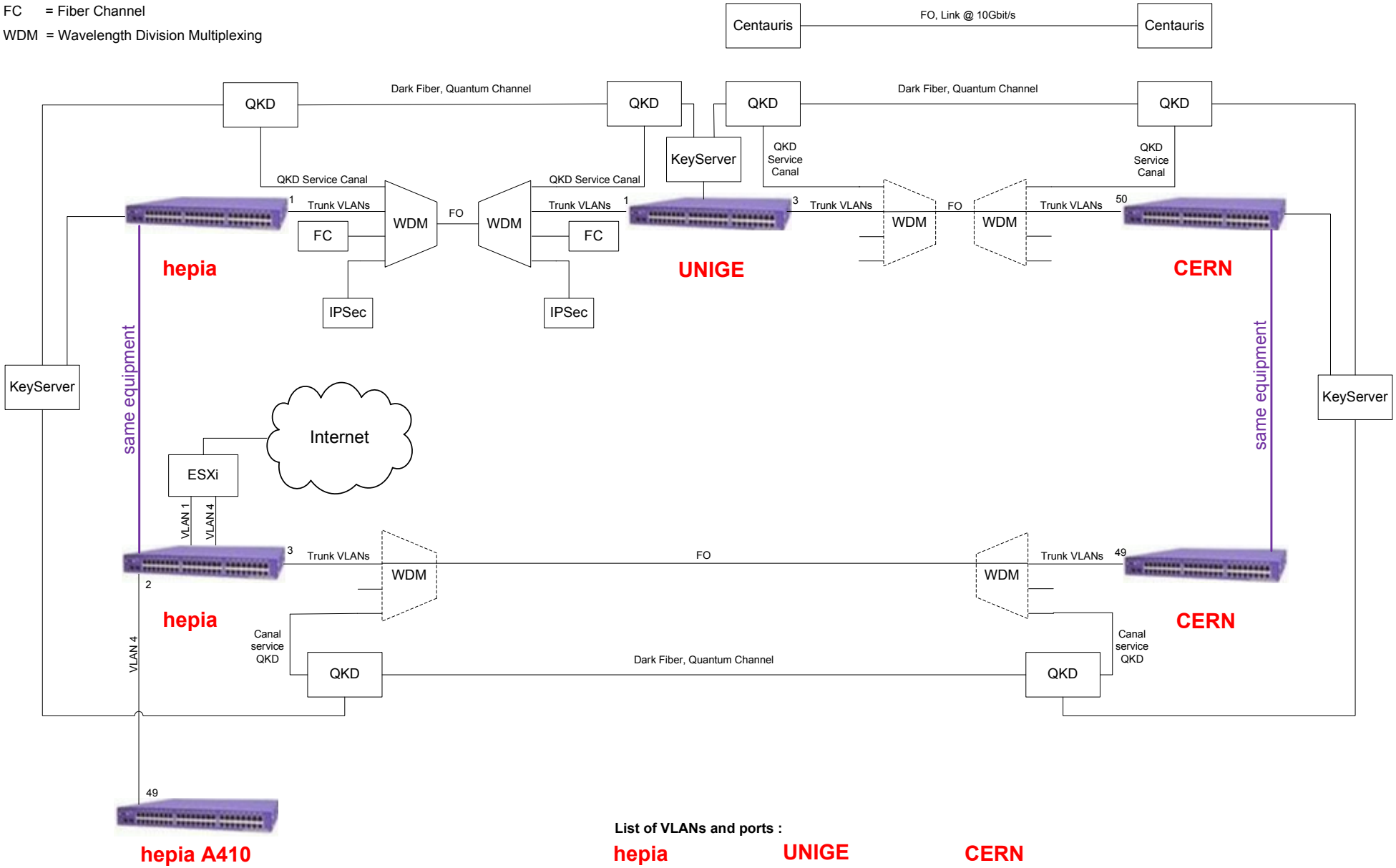
Voir page suivante

[11] http://www.vmware.com/pdf/vi3_301_201_admin_guide.pdf

QKD = Quantum Key Distribution

FC = Fiber Channel

WDM = Wavelength Division Multiplexing



List of VLANs and ports :

hepia	UNIGE	CERN
VLAN1 ports 4-16	VLAN1 ports 2,4-16	VLAN1 ports 2, 4-16
VLAN2 ports 17-32	VLAN2 ports 17-32	VLAN2 ports 17-32
VLAN3 ports 33-47	VLAN3 ports 33-48	VLAN3 ports 33-48
VLAN4 ports 2,49		

- Internet allowed only for SwissQuantum administration, via VLAN1
- VLAN4 only used to fully administrate ESXi, only via hepia A410 Switch

26.08.2009)

6 WP3 : qualité de service

6.1 Introduction

Ce chapitre a pour but de décrire l'infrastructure de génération de trafic et de mesure déployée à Genève. Nous allons aussi définir ici les tests qui ont été effectués et quelles sont les valeurs à disposition au travers des mesures.

Les tests effectués sur la liaison entre les deux sites nous ont permit de démontrer l'aboutissement du développement par l'EIA-FR de l'outil '**QoS Test Software Suite**', ainsi que son utilité dans la démarche du contrôle de qualité d'une infrastructure sur le long terme.

6.2 Objectifs des mesures

Plusieurs flux de trafic ont été générés entre les deux sites au travers de générateurs. Les différents flux de trafic sont une modélisation de ce que l'on rencontre dans un réseau d'entreprise. Différents tests de génération de trafic au moyen de l'outil D-ITG[12] et de capture de trafic au moyen de la librairie **libpcap**[13] ont permit de déterminer les limites de l'utilisation d'outils Open-Source. Les résultats ci-dessous nous ont ainsi permit de générer les flux supportés par nos équipements.

Flux¤	Moyenne· trames/secondes¤	Moyenne¶ de·taille·de·trame¶ [Bytes]¤	Moyenne¶ de·débit·théorique· [Mbits/s]¤
TCP¤	1000¤	512¤	4¤
RTP¤	1300¤	64¤	0.6¤
UDP¤	8000¤	512¤	32¤
Total·unidirectionnel¤	¤	¤	36.6¤
Total·bidirectionnel¤	¤	¤	73.2¤

Figure 1 : Flux de trafic générés

Les outils de mesures fonctionnant sur des machines virtuelles (cf WP2), les flux ont été diminués pour permettre leur génération sans problèmes de performances:

Flux¤	Moyenne· trames/secondes¤	Moyenne¶ de·taille·de·trame¶ [Bytes]¤	Moyenne¶ de·débit·théorique· [Mbits/s]¤
TCP¤	500¤	512¤	2¤
RTP¤	1300¤	64¤	0.6¤
UDP¤	1500¤	512¤	6¤
Total·unidirectionnel¤	¤	¤	8.6¤
Total·bidirectionnel¤	¤	¤	17.2¤

Figure 2: Flux de trafic générés par les machines virtuelles

Les objectifs des mesures sur ces flux sont de :

→ démontrer la stabilité de l'infrastructure en terme de QoS
→ mesurer & visualiser les différents paramètres (métriques) représentatifs de la QoS, soit :
- la latence
- la perte de paquet
- le débit
- la gigue

[12] http://www.grid.unina.it/software/ITG/
[13] http://www.tcpdump.org/

Ces mesures seront effectuées en pseudo-temps réel, soit par échantillonnage du trafic à intervalles réguliers et par la mise à disposition sous forme de MIB SNMP[14] de ces valeurs.

Ces valeurs pourront ensuite être récupérées à intervalle régulier par un outil de gestion de réseau du type Cacti [15], MRTG[16] ou encore Nagios[17]

6.3 Définition de la QoS

La QoS peut se définir de différentes manières, comme étant par exemple:

« *La capacité d'offrir différentes priorités à différentes applications, utilisateurs, ou flux de donnée ou de garantir un certain niveau de performance à un flux de données*. »

Selon **ISO 8402:1994**[18]: "*la totalité des caractéristiques d 'une entité qui portent sur sa capacité à satisfaires des besoins formulés et supposés »*

Selon **ISO 9001:2000**[19]: définit la qualité comme le "*degré auquel un ensemble de caractéristiques inhérentes respectent des exigences. »*

Selon l'**ITU-T E.800** (et **ETSI ETR003**): "*Ensemble des caractéristiques d'un service de télécommunication qui lui permettent de satisfaire aux besoins explicites et aux besoins implicites de l'utilisateur du service*."

Selon **IETF**[20] : l'IETF se focalise plutôt sur la notion intrinsèque de la QoS et ne traite pas les aspects de perception. Sa définition est la suivante : "*Un ensemble de service prérequis a remplir par le réseau lors du transport d'un flux* ."

6.3.1 Métriques pour la mesure de la QoS

Pour quantifier la perception de la qualité de service d'un réseau hétérogène, plusieurs organismes ont tenté de définir différents métriques représentatifs de la qualité d'un flux de donnée.

a) IETF : IPPM

Plusieurs standards définissent la QoS d'un réseau de téléinformatique :

RFC 2330	Framework for IP Performance Metric (IPPM)
RFC 2697	A One-Way Delay Metric for IPPM
RFC 2680	A One-way Packet Loss Metric for IPPM
RFC 2681	A Round-trip Delay Metric for IPPM
RFC 3357	One-way Loss Pattern Sample Metrics
RFC 3393	IP Packet Delay Variation Metric for IPPM

[14] Management Information Base (MIB), Simple Network Management Protocol (SNMP)
[15] Cacti, http://www.cacti.net/
[16] MRTG, http://oss.oetiker.ch/mrtg/
[17] Nagios, http://www.nagios.org/
[18] ISO 8402 :1994 : Quality management and quality assurance -- Vocabulary
[19] ISO 9000 :2000 : Quality management principle
[20] RFC 2386, E. Crawley *et al.,* "A Framework for QoS-Based Routing in the Internet", Aug. 1998.

b) IETF : RFC 2544 / RFC 1242

Le RFC 1242 défini les métriques utilisés par le RFC 2544 pour le benchmarking d'un réseau, avec entre autre (extrait du RFC):

Métrique	Définition	Unité de mesure
Frame Loss Rate	Percentage of frames that should have been forwarded by a network device under steady state (constant) load that were not forwarded due to lack of resources.	Percentage of N-octet offered frames that are dropped. To be reported as a graph of offered load vs frame loss.
Latency	**For store and forward devices:** The time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port. **For bit forwarding devices:** The time interval starting when the end of the first bit of the input frame reaches the input port and ending when the start of the first bit of the output frame is seen on the output port.	Time with fine enough units to distinguish between 2 events.
Throughput	The maximum rate at which none of the offered frames are dropped by the device.	N-octet input frames per second input bits per second

c) ITU L.359 et Y.1540

La norme Y.1540 défini les métriques suivants pour l'environnement IP :

IPLR	IP Packet Loss Ratio
IPTD	IP Packet Transfer Delay
IPDV	IP Packet Delay Variation (Jitter)
IPER	IP Packer Error Ratio

Des exemples de valeur pour les réseaux IP publiques sont donné par la norme Y.1541 :

QoS Class	Charateristics	IPTD	IPDV	IPLR	IPER
0	Real time, jitter sensitive, highly interactive	100 ms	50 ms	10^{-3}	10^{-4}
1	Real time, jitter sensitive, interactive	400 ms	50 ms	10^{-3}	10^{-4}
2	Transaction data, highly interactive	100 ms	-	10^{-3}	10^{-4}
3	Transaction data, interactive	400 ms	-	10^{-3}	10^{-4}
4	Low loss only (short transaction, bulk data, video streaming)	1 s		10^{-3}	10^{-4}
5	Traditional applications of default IP networks	-	-	-	-

De plus, la norme Y.1541 donne des exemples de prérequis pour diverses applications multimedia :

Applications	IPTD	IPDV	IPLR	IPER
Data acquisition from sensors	100 ms	50 ms	0	10^{-4}
Radar Traces	20 ms	1-3 ms	10^{-3}	10^{-4}
Weapon control	20 ms	10 ms	0	10^{-4}
Sensor control	20 ms	10 ms	0	10^{-4}
Voice	250 ms	30 ms	10^{-2}	10^{-4}
Video streaming	5 – 10 s	-	$2x10^{-2}$	10^{-4}

Les métriques utilisées dans le cadre de ce projet sont:

- Délai moyen et déviation standard
- Gigue moyenne et déviation standard
- Débit effectif moyen
- Perte de paquet

6.3.2 Méthodologie de mesure

Il existe plusieurs méthodes pour la mesure de la QoS :

- Les mesures aller/retour (de type RTT, Round Trip Time)
- Les mesures unidirectionnelles (avec synchronisation)

De plus, il existe plusieurs types d'architectures pour effectuer ces mesures :

- architecture passive (écoute uniquement)
- architecture active (génération et écoute)

L'outil développé par l'EIA-FR dans le cadre de ce projet utilise une architecture passive. De plus, pour permettre aux sondes de mesurer des lignes à haut débit, la méthodologie de mesure utilisée est basée sur un échantillonage temporelle et sur le filtrage de trafic. Cette méthode est basée sur le draft IETF 'draft-ietf-psamp-sample-tech-04.txt' par Zseby, Molina, Raspall et Duffield.

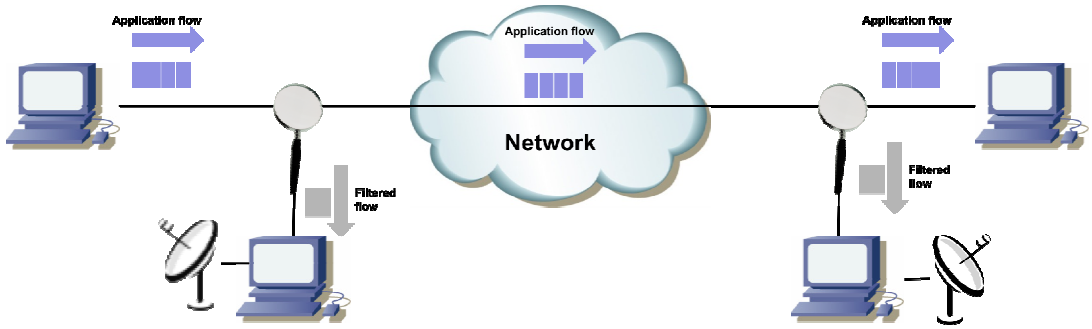


Figure 3: Achitecture et méthodologie de mesure de la QOS

6.4 Outils

Dans le cadre de ce projet, l'EIA-FR à développer l'outil 'QoS Test Software Suite' composé des éléments suivants :

- Deux sondes de mesure en **temps réel** (fonctionnant selon la méthodologie décrite précédement)
- L'outil de calcul de la QoS

Tous le développement a été fait en langage C et déployé sur des machines Linux (avec une distribution Ubuntu).

Pour la mesure de la QoS, il est nécessaire que les sondes soient synchronisées pour permettre le calcul des différentes valeurs liées au temps, telles que le délai ou encore la gigue. Cette synchronisation est possible grâce à l'utilisation du protocole NTP (Network Time Protocol).
Différents tests de précisions réalisé dans le cadre de ce projet, nous indique que NTP nous permet d'obtenir une synchronisation de l'ordre de 100µs et que le temps qu'il faut pour que les deux sondes soient synchronisée est de l'ordre de 30 minutes.

L'outil de calcul de la QoS fournit les métriques suivantes sous forme de MIB :

- Délai moyen et déviation standard
- Gigue moyenne et déviation standard
- Débit effectif moyen
- Perte de paquet

Les caractéristiques générales de l'outil sont les suivantes:

- Basé sur des librairies Open Source (libpcap)
- Synchronisation des sondes au travers de NTP
- Mesure de flux UDP avec des débits jusqu'à 80 Mb/s sur des machines "réelles" (avec Linux)
- Mesure de flux UDP avec des débits jusqu'à 15 Mb/s sur des machines "virtuelles" (VMWare ESXi)

Plus d'informations sont disponibles sur le site http://swissquantum.project.eia-fr.ch sur la configuration et la précision NTP, l'implémentation de MIB propriétaire et le fonctionnement de l'application.

6.5 Implémentation sur site

Une fois l'infrastructure optique et réseau en place, l'outil 'QoS Test Software Suite' a été déployé entre l'hépia et l'Université de Genève. Le détail de l'installation se trouve dans la figure suivante :

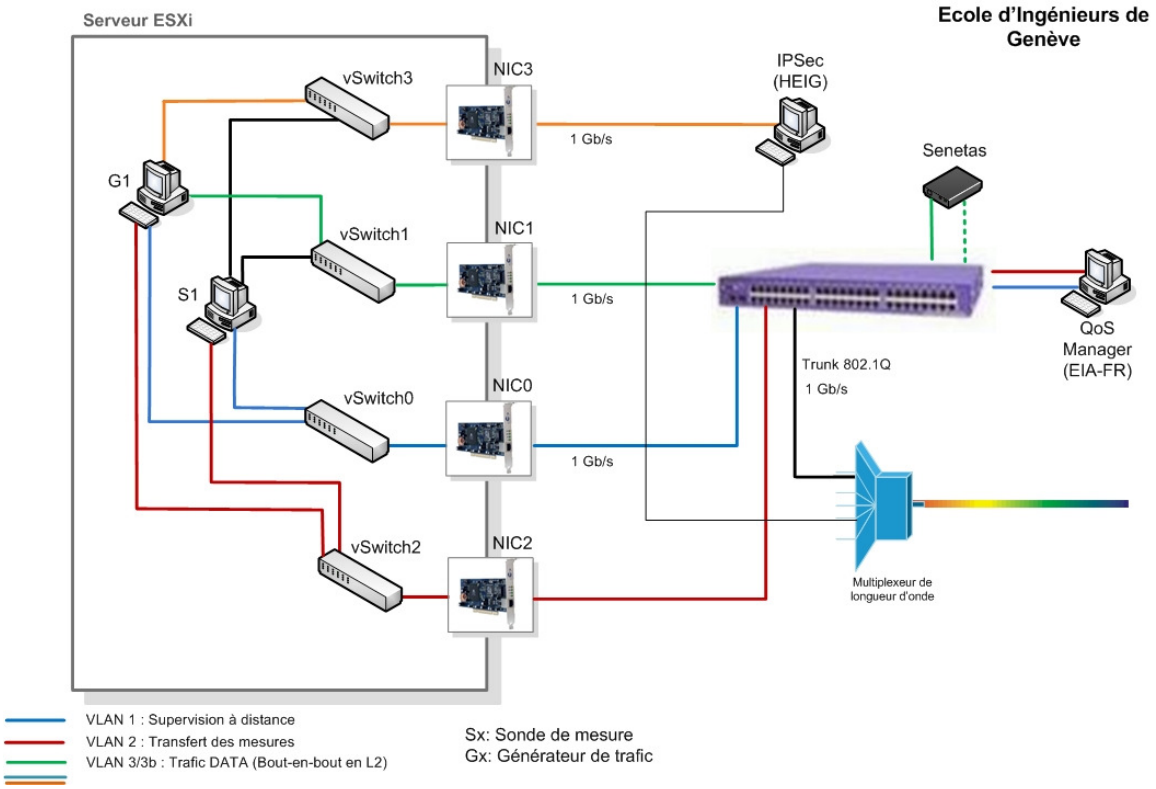


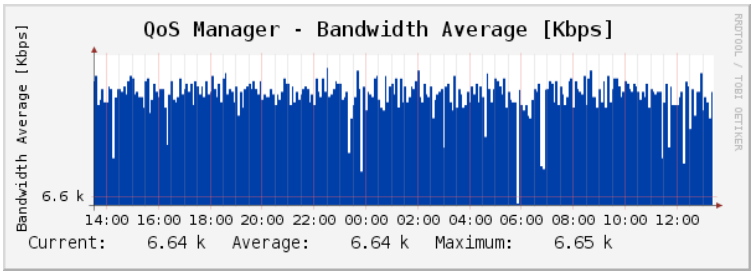
Figure 4 : QoS Test Software Suite et générateur de trafic - hepia

Comme on peut le constater, l'outil de mesure de la QoS est déployé sur des machines virtuelles (sous VMWare ESXi). Plusieurs interfaces par machine permettent de séparer le flux de supervision à distance (VLAN1) du flux de mesure (VLAN2) et des flux produits par les générateurs de trafic fonctionnant avec D-ITG[21].
Le flux généré est par la suite encrypté au moyen du protocole IPSec utilisant des clés générées par les équipements de la société idQuantique, pour plus de détails, se référer au WP4.

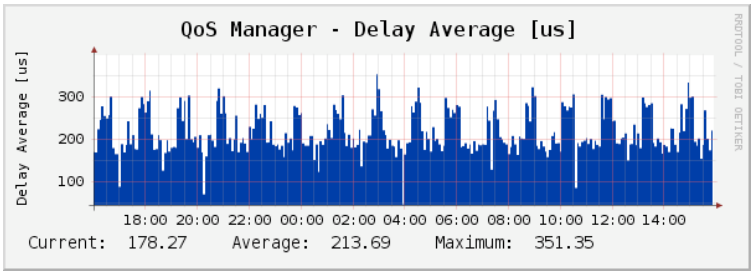
6.6 Résultats obtenus

[21] http://www.grid.unina.it/software/ITG/

Les outils (sondes et générateurs) ont été installés au mois d'avril 2009 et ont fonctionnés sans interruption jusqu'à la fin de l'année 2009. Le flux de référence est un flux UDP (cf. Chapitre 6.2). Un exemple des résultats fournits se trouve dans les figures ci-dessous :



6.6 Mb/s en moyenne



214 ms en moyenne

Les résultats sont visibles sur le site dédié au projet Swissquantum, au travers de l'URL suivant :
http://www.swissquantum.com/?IPsec-QoS-live-performance

Le bilan, après plus de 6 mois d'exploitation, est très positif :

- Validation du concept de sondes de mesure par mesure passive et synchronisée
- Stabilité éprouvées des sondes
- Utilisation d'outils open-source
- Divers mandats possibles avec des entreprises pour de la qualification de réseau en terme de QoS

7 WP4 : adaptation du code IPSec-Linux au système quantique de distribution des clés

7.1 Aperçu

Le but de cette partie consistait à concevoir, implémenter et tester un couplage entre le système quantique de distribution des clefs et une pile IPSec standard tournant sous Linux. Même si cette association peut sembler peu naturelle au premier abord en termes de sécurité (le protocole IPSec ne possédant pas de propriétés de sécurité inconditionnellement sûre au sens de la théorie de l'information), ce mariage a néanmoins permis de démontrer de nombreux avantages techniques :

- Le protocole IPSec permet de prendre la relève en cas d'indisponibilité passagère du lien quantique ainsi que de garantir une sécurité plus que raisonnable dans ces moments-là.
- La technologie de mise au point quantique de clefs peut être intégrée sans problème avec le protocole IPSec, et ceci de manière simple et sûre.
- Les modifications requises de la pile IPSec sont réduites au strict nécessaire.
- Les performances obtenues sur du matériel d'entrée de gamme (tel qu'un PC standard utilisé comme routeur) sont plus que suffisantes pour la majorité des scénarios.

7.2 Implémentation et résultats

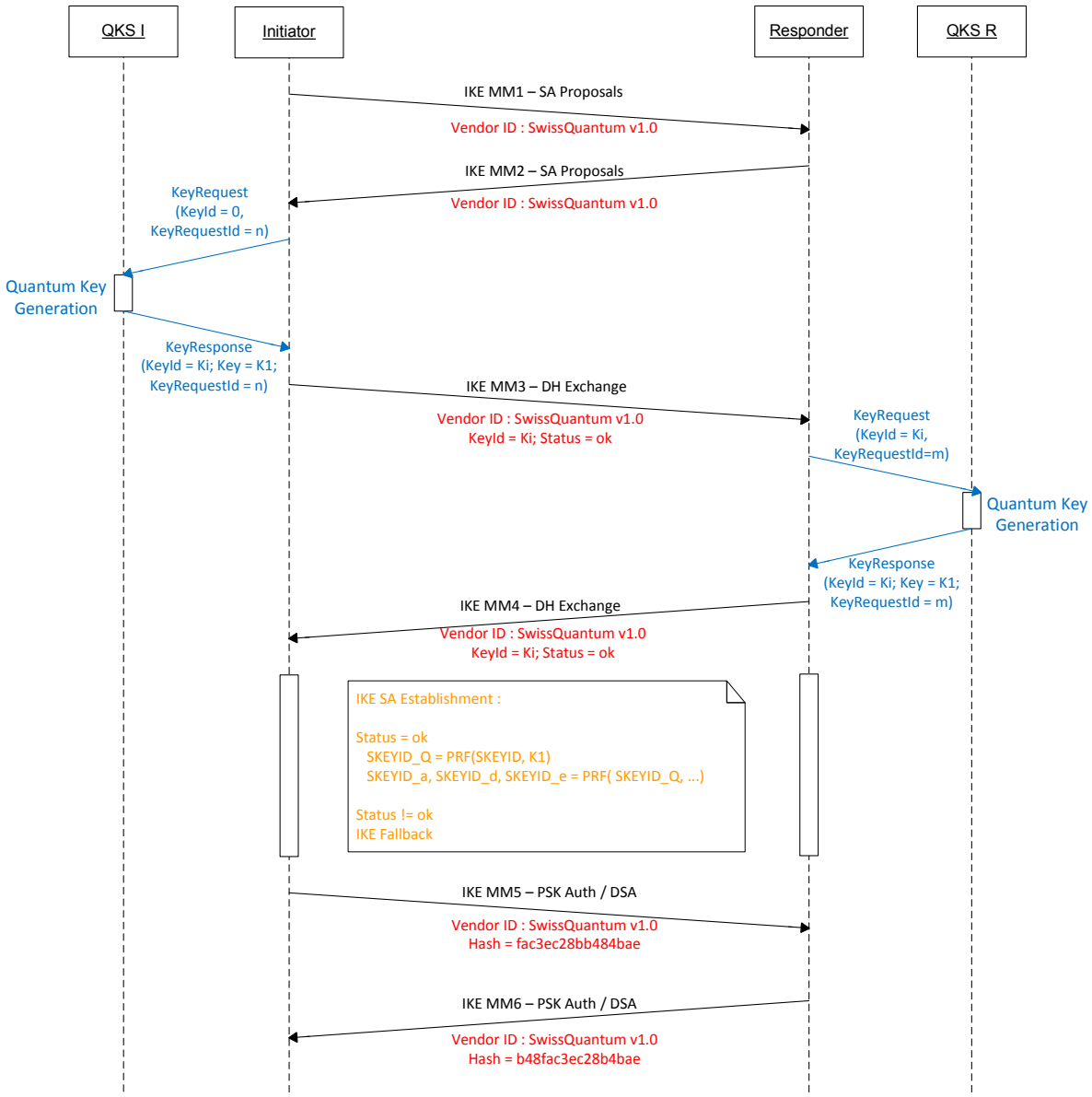
Les principaux défis à relever étaient les suivants :

- Le système se devait de coller au mieux à la philosophie du protocole IPSec, notamment dans sa partie de mise au point de clefs de sessions.
- Le système se devait d'être capable de détecter un problème vis-à-vis du lien quantique dans un premier temps, puis de basculer dans un mode IPSec classique de manière transparente, sans perte de paquets et avec un temps de latence acceptable.
- Les modifications du code de la pile IPSec se devaient d'être aussi légères que possible, dans le but d'une sécurité maximale ainsi que d'une intégration facilitée avec les futures versions du logiciel.
- La procédure de combinaison des clefs classiques et quantiques se devait d'être résiliente à la compromission d'une des deux clefs et se devait d'atteindre un niveau maximal de sécurité.

Les implémentations d'IPSec sous Linux sont normalement constituées de deux parties distinctes, à savoir un démon tournant en mode utilisateur et responsable d'implémenter le protocole IKE (Internet Key Exchange), donc de gérer les associations de sécurité IPSec, tandis que du code noyau implémente le chiffrement et l'authentification des données à proprement parler (en utilisant soit les sous-protocoles ESP ou AH), et ceci, en fonction des clefs de sessions négociées via IKE.

Le moment le plus naturel pour intégrer une clef quantique se situe évidemment lors de la négociation des associations de sécurité au moyen du protocole IKE. Nous avons ainsi choisi de modifier le démon open source `racoon`[22] pour y intégrer la communication avec le serveur de clefs quantiques (QKD) ainsi que l'intégration de la clef quantique lors de la négociation de clefs. Le flux de message est illustré sur la figure suivante (« Main mode » modifié) :

[22] http://ipsec-tools.sourceforge.net



La communication entre le QKD et le démon IKE est sécurisé via un réseau virtuel privé (VPN) implémenté au moyen du logiciel open-source `OpenVPN`[23], ce qui permet de garantir une authentification mutuelle des deux nœuds ainsi que la confidentialité de la clef de session quantique échangée entre le QKD et le démon IKE.

Le système décrit a été implémenté, testé et mis en charge pendant plus de 12'000 heures sans aucun problème notable, démontrant ainsi sa stabilité. Une bande passante utile de plus de 400 Mbps a été atteinte en pic, et ceci en utilisant uniquement des PCs standard[24], comme matériel.

23 http://www.openvpn.net

24 http://www.tdeig.ch/vmware/Montage_PC_Gigabyte.pdf

8 WP5 : résultats

Le taux d'erreurs quantiques (QBER) des trois systèmes SwissQuantum à partir du 1er avril 2009 jusqu'au le 4 février 2010 est montré dans la Fig. QBER. Ce taux reste constant pendant presque tout le temps de fonctionnement du réseau quantique. Pendant la période mi-avril / mi-mai, nous pouvons observer que le QBER a un comportement assez différent de celui qu'il a pendant le reste du test. Nous soupçonnons que cette différence est liée aux aménagements effectués dans la salle des serveurs du CERN pour améliorer son système de refroidissement. Les forts changements de température de la salle au cours de cette période de temps expliquent le comportement du QBER.
Dans la Fig. RSK, nous pouvons voir le taux clés secrètes des trois systèmes. Il est assez stable pendant toute la période du projet SwissQuantum, bien qu'il y ait périodiquement des réductions ou des interruptions de la création de clés secrètes sur les liens SQ2 et SQ3. Le système de refroidissement interne d'un des systèmes du lien quantique SQ2 a eu un dysfonctionnement à partir du mois de juillet 2009. Cela a provoqué une réduction de son taux de clé secrète. Nous avons pu définitivement résoudre ce problème en Novembre 2009. Il y a eu aussi des problèmes avec le refroidissement du système SQ3 à partis de juin 2009 aussi. Ce dysfonctionnement est à lier avec une panne du système d'air conditionné à l'Université de Genève. Le système air conditionné a été réparé en juillet 2009.
A la fin d'août 2009, lors de la mise en fonction des serveurs de clé entre les systèmes de distribution des clés quantiques et les encrypteurs, de fortes perturbations sur le lien SQ3 sont apparues. Ceci à réduit fortement le taux de la clé secrète du système jusqu'à ce que nous résolvions le problème des serveurs de clés.

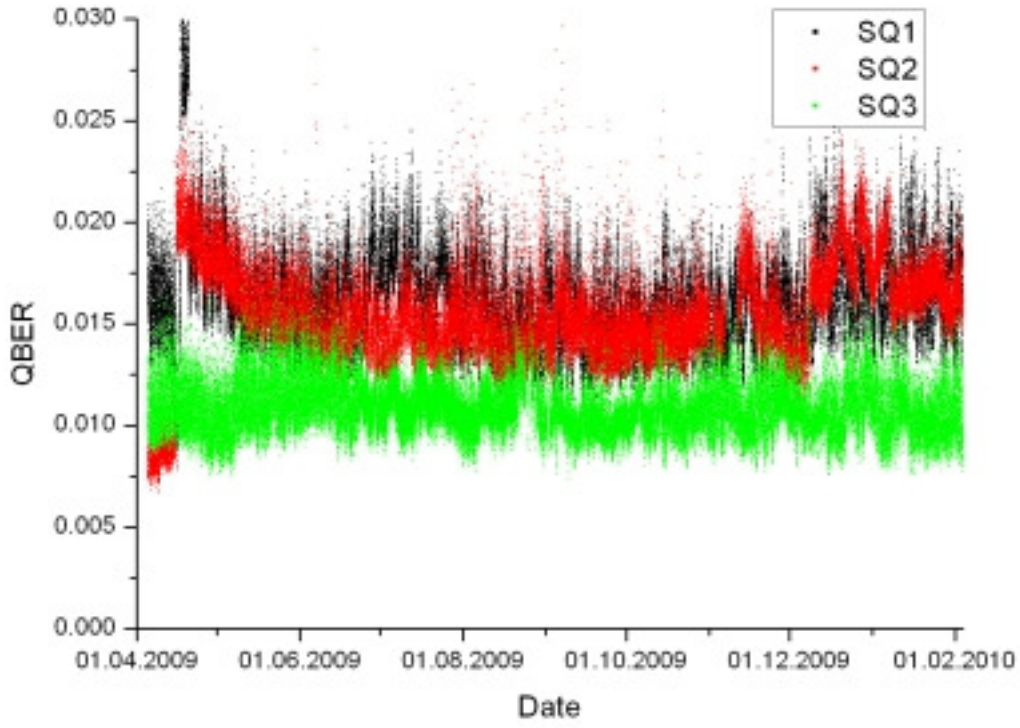


Fig. QBER : le taux de Quantum Bit Error en fonction du temps

Taux de Quantum Bit Error : Le taux d'erreur bit quantique (QBER) est la mesure de référence de la performance du système de distribution de clés quantique.

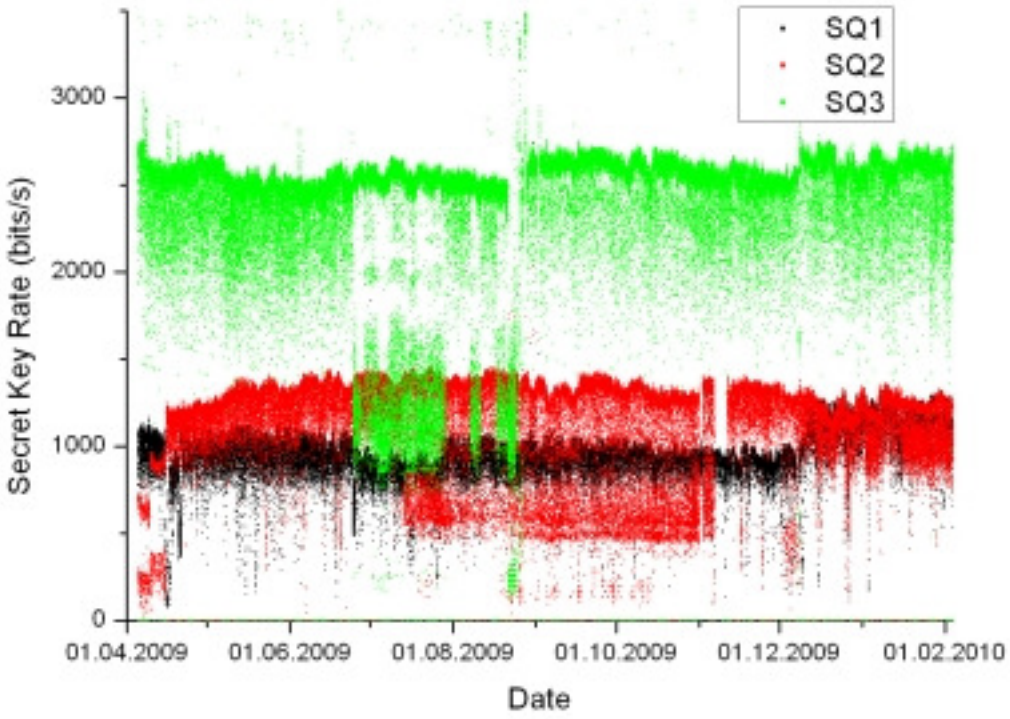


Fig. Rsk : le taux de clés secrètes en fonction du temps

Remarques :

- SQ1: Lien entre Université de Genève et le CERN (14,4 km de fibre).
- SQ2: Lien entre le CERN et l'hepia (17,1 km de fibre).
- SQ3: Lien entre l'hepia et l'Université de Genève (3,7 km de fibre).

9 Valorisation, conclusion et suite

La fin du projet a été fixée en fonction de l'exposition Telecom 2009 à Genève-Palexpo qui se déroulait du 5 au 9 octobre 2009.
A cette occasion, HESSO s'est associé à l'événement *A Quantum Leap for Telecommunications, Today and Tomorrow* organisé par les pôles QP (EPFL), MaNEP (UniGE) et MICS (EPFL) le 8 octobre 2009.

Les 3 établissements HESSO concernés avaient des missions différentes :

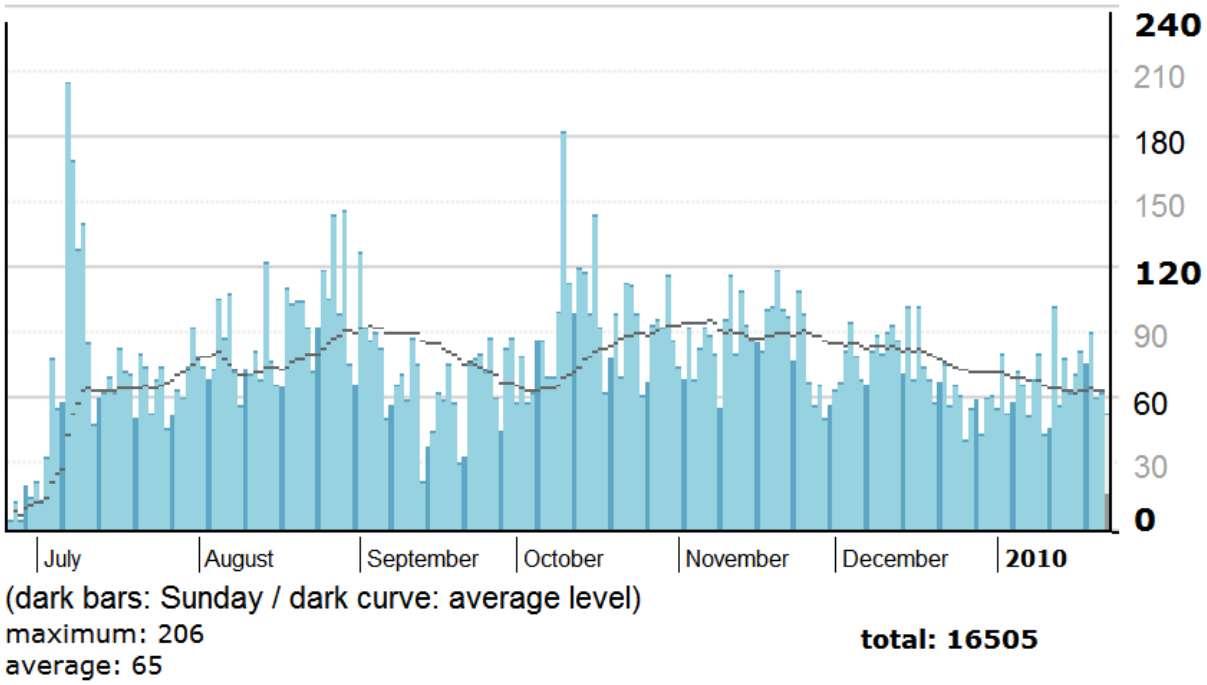
- GE a profité de ce projet pour acquérir des compétences dans les architectures virtualisées avec le produit ESXi qui semblent faciles à utiliser pour réunir plusieurs serveurs. L'expérience acquise montre que la virtualisation ajoute une couche de complexité et que sa parfaite maitrise demande des compétences pointues dans l'optimisation des ressources CPU & RAM ainsi que l'utilisation appropriée des VMWare Tools.
  Ainsi 26 personnes ont suivi la formation *Introduction à la virtualisation*[25] d'un jour en 2009 et nous pensons pouvoir proposer une suite avec *Bonne gestion d'une architecture virtualisée avec vSphere & ESXi (version 4)* [26]

- FR a profité de ce projet pour étendre le concept de mesure en temps réel de la QoS (Quality of Service) de flux de donnée. Les connaissances acquises on permit d'étoffer le contenu des cours Réseaux & Service donnés dans le cadre de la formation Bachelor. De plus, divers mandats ont découlé de ce projet pour la qualification en terme de QoS d'équipement réseau.

- VD a adapté avec succès une pile IPSec Linux au système quantique de distribution des clefs. De plus, les performances obtenues *(thoughtput)* sur une base matérielle *low cost* sont intéressantes.

- ID quantique

  Statistiques du site web www.swissquantum.com :



  Statistiques de la conférence au salon ITU Telecom 2009 :

[25] http://www.tdeig.ch/vmware/Flyer_2009.pdf
[26] http://www.tdeig.ch/vmware/flyer2.pdf

Nombre de flyers ***envoyés*** : 1230 (550 par la poste, 680 par email). A cela il faut ajouter l'article dans la e-newsletter de la Promotion Economique, qui atteint 4'000 personnes.
Nombre de ***réponses*** (inscriptions) : 145.
Nombre de personnes ***présentes*** à l'événement : 100 (environ).

- Conclusions

Le projet SwissQuantum est un succès, autant en termes de développement technologique que de sensibilisation du public. Tous les objectifs du projet ont été atteints. Le principal but, l'essai à long terme d'une plate-forme QKD, a été atteint avec de bons résultats. Le réseau SwissQuantum est encore en service. Les données et résultats liés à l'exploitation du réseau et le statut sont encore accessibles à tous via le site web www.swissquantum.com. Les autres objectifs qui mettent l'accent sur l'innovation, ont également été remplis au cours de ce projet. D'une part, les plates-formes de chiffrement classique ont été développées et testées avec succès. Elles utilisent des clés secrètes produites avec la technologie de distribution de clés quantiques pour sécuriser le trafic de données. D'autre part, la gestion des clés quantiques est en exploitation depuis une longue période (août 2009) et elle est intégrée dans une topologie de réseau conventionnel, avec des données réelles et des applications éprouvées (encrypteur 10G Ethernet). Cette application de gestion de clés secrètes est une partie très innovante du projet SwissQuantum.
Par ailleurs, du point de vue de la visibilité, le projet SwissQuantum a suscité un fort intérêt médiatique adressé aussi bien aux spécialistes qu'au grand public. La conférence publique organisée dans le cadre de l'exposition ITU Telecom a rassemblé plus de 100 personnes. Le site Web a été une fenêtre ouverte sur le projet. On peut y voir les performances du réseau en «temps réel». Grâce à son succès, le site a permis à la cryptographie quantique d'être connue et comprise par un public plus large.

- Publications

1. UNIGE Presse, 3 juillet 2009, Un triangle d'or pour crypter l'information - L'UNIGE déploie le premier réseau quantique durable.
2. futurezone.ORF, 6 juillet 2009, Schweizer starten Quantenkryptographie-Netz.
3. NZZ Online, 6 juillet 2009, Ein abhörsicheres Netz im Langzeittest.
4. RSR.ch, 9 juillet 2009, Cryptage quantique.
5. PR NewsWire, SYS-CON Australia, Pressportal , ICT Journal, 9 octobre 2009, Quantum Cryptography Network Up and Running for 12,000 Hours.
6. ICTjournal, septembre 2009, Le chiffrement quantique est-il invulnérable.
7. IT-Security, novembre 2009, Quanten-Verschlüsselung das SwissQuantum Project.