HackerSpace / Breizh-Entropy / Elaboratoires / 48

SIMONNEAU Marc - PASTOL Joël - CARIOU Morgane

16 mars 2012

Contexte

L'ELABORATOIRE, association Loi 1901 existe depuis 1997 dans une friche industrielle à 5 minutes du centre ville de rennes. (http ://elaboratoire.free.fr)

L'Elaboratoire défend la création artistique alternative, l'autogestion, le lieu de vie sur le lieu de travail, une escale pour les nomades, et revendique haut et fort une zone libre de résistance aux pouvoirs marchands. Chacun apporte son art, son idée, son savoir-faire, son matériel, ses outils, ses principes alternatifs.

Ils ont intégré la liste européenne des friches artistiques, ou autrement dit « les nouveaux territoires de l'art ». C'est un lieu d'accueil de chapiteaux, un lieu de répétition d'arts gestuels (danse, theatre, cirque), un bureau avec accès internet, presque deux hectares pour les maisons roulantes ou autres, un bâtiment couvert de 1000 m2 ou s'enchevêtrent moultes ateliers de bidouille, bricolage, sculpture, couture, bois, métal, sérigraphie, un garage avec pont poids-lourds.

Depuis bientot 15 ans, le lieu a beaucoup évolué : un deuxième site géographique à environ 500 mètres (« le 48 »), avec de nouveaux ateliers de créations mécaniques, métallurgiques, salle d'exposition, cuisine collective pour les résidents, salle d'expression multimédias ...

Il s'est donc avéré pertinent de repenser le réseau numérique, (qui s'était construit par petits bouts en fonction des besoins et possibilités du moment), afin d'en améliorer l'architecture, réduire son instabilité, rationaliser les échanges de flux, et d'y déployer des serveurs de services (mail, web, monitoring, ...)

C'est au sein de cette association qu'est accueilli le Hackerspace de rennes créé suite au Breizh-Entropy Congress, évènement inter-disciplinaire ayant pour thème la création et les cultures libres. (http ://hackerspaces.org/wiki/Breizh_Entropy_Congress)

Les membres du Hackerspace, soucieux du partage des savoirs, ont accepté de nous superviser sur cette tâche donnant ainsi au projet un enjeu à la fois pratique (obligation de résultat) et social (nous participons à l'évolution du Hackerspace et de l'Elaboratoire).

C'est dans ce cadre que se déroule notre projet tutoré.

Définition du terme Hackerspace :

> "Les hackerspaces sont des lieux protéiformes regroupant des personnes d'horizons différents dans l'objectif de produire des projets, de nouvelles idées et de les partager. Les technologies et le numérique sont utilisés comme levier. Les activités liées aux différents hackerspaces peuvent varier par rapport aux lieux, aux cultures, aux personnes qui portent le hackerspace."
>
> (sources : http ://fablabsquared.org/ ?Qu-est-ce-qu-un-Hackerspace)

Encadrement In Situ

- Mathieu Goessens, mathieu.goessens@inria.fr
- Lucien Loiseau, lucien.loiseau@telecom-bretagne.eu
- Emmanuel Thierry, emmanuel.thierry@telecom-bretagne.eu

Objectifs/Directives (1er cahier des charges)

L'objectif du projet est d'améliorer, simplifier l'architecture réseau existante. Cela a pour but d'améliorer la maîtrise de l'architecture ainsi que de son potentiel évolutif.

La simplification de l'architecture doit permettre une meilleure vision du réseau. Une organisation améliorée qui permettra une gestion plus efficiente. Cette simplification doit également mettre en œuvre des capacités d'évolution. L'amélioration de l'architecture réseau passe par l'interconnexion des deux sites, « 48 » et Elaboratoire, la déverse des différents sites de production et de vie du lieu (ateliers, cuisines, zone résidentielle), la sécurité des données privées, le principe d' « anonymat sur internet » (valeur partagée par le Hackerspace et L'Elaboratoire).

Le réseau du hackerspace était géré par une Freebox. Cela posait des problèmes de fléxibilités, comme l'impossibilité de modifier des règles de firewall sans redémarrage.

Travaux à réaliser :

- Installation et configuration du routeur firebox sous PFSense
- Serveur DHCP (sur le Firebox)
- Resolveur DNS (bind9 sur le Firebox)
- Routage NAT Firewall (sur le Firebox)
- Gestion QoS Monitoring (munin sur le Firebox)
- Firewall (sur le Firebox)
- Configuration de la freebox en mode « bridge »
- Uniformisation configurations WRTs (sous OpenWRT)
- Mise en place noc (Munin)
- Mise en place d'un noeud DN42
- Mise en place d'un noeud TOR
- Mise en place double VLAN/SSID : L'un normal, l'autre anonyme, pour accèder au réseau tor.

Choix techniques

Nous avons orienté tous nos choix techniques vers des solutions libres en accord avec les valeurs des Hackerspaces et de l'Elaboratoire, valeurs défendues par Richard Stallman et la Free Software Foundation : basées sur la liberté, l'égalité et la fraternité :

- la liberté d'exécuter le programme, pour tous les usages
- la liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins
- la liberté de redistribuer des copies du programme (ce qui implique la possibilité aussi bien de donner que de vendre des copies)
- la liberté d'améliorer le programme et de distribuer ces améliorations au public, pour en faire profiter toute la communauté

Pour les points d'accès wifi (linksys wrt54gl), la distribution OpenWRT à été choisie.

L'O.S. privilégié est Debian pour son aspect libre et réputé, ainsi que sa communauté trés active. Ces aspects nous ont conforté dans notre choix par rapport à d'autre : Red Hat ou Suse sont des solutions plutot orientées Entreprise, bien qu'elle soit réputées et utilisées, elles ne sont pas libres strico sensu. Leurs clones libres (respectivement : CentOS et OpenSuse) sont quant à eux libres mais ne jouissent pas d'une communauté aussi forte que Debian.

En terme d'outil de monitoring, nous avons tous d'abord pensé à Nagios (car étudié en cours). Il represente une solution complète et flexible. Cependant ces deux points l'amènent à être complexe à configurer et mettre en place. Nous nous sommes donc résolus à trouver une alternative, plus simple à mettre en oeuvre. Munin est semble-t-il un outil moins complet mais permettant nativement de faire des graphiques. Son installation, à contrario de Nagios, est simple. Nous en avons conclu que la mise en place du serveur de supervision se ferait via cette solution.

Pour ce qui est du serveur de résolution de noms, le service Bind a été préféré. Il permet la résolution de noms ainsi que la gestion de zones en un seul et même service, contrairement au couple NSD/Unbound. Djbdns ne respectant pas les normes de résolution DNS, nous ne nous somme pas attardé sur celui-ci.

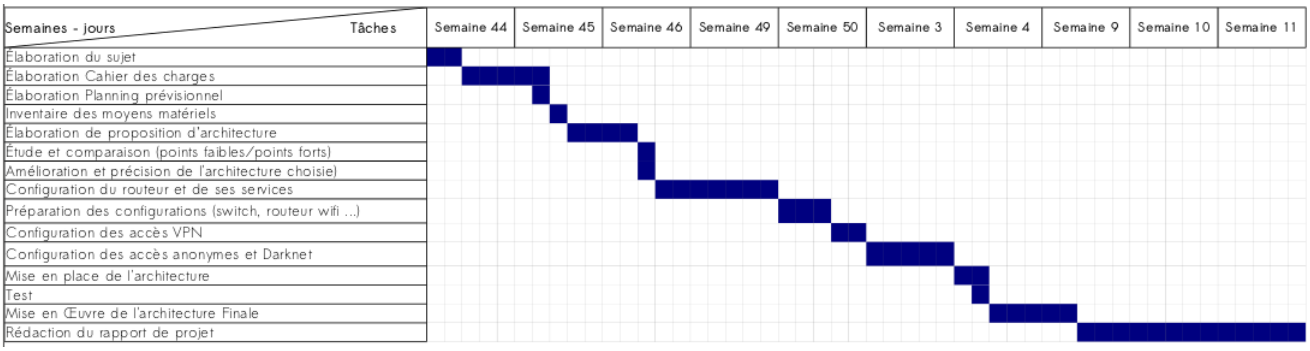
La solution de gestion du protocole BGP a été décidée rapidement. En effet Quagga est le service le plus utilisé face à Bird ou encore OpenBGP.

OpenVpn a été choisi comme service pour gérer les réseaux privés virtuels. Quicktun, un autre outil du même type, est par rapport à ce dernier, moins utilisé et reste peu vérifié au niveau chiffrement.

Organisation

Diagramme de Gant prévisionnel

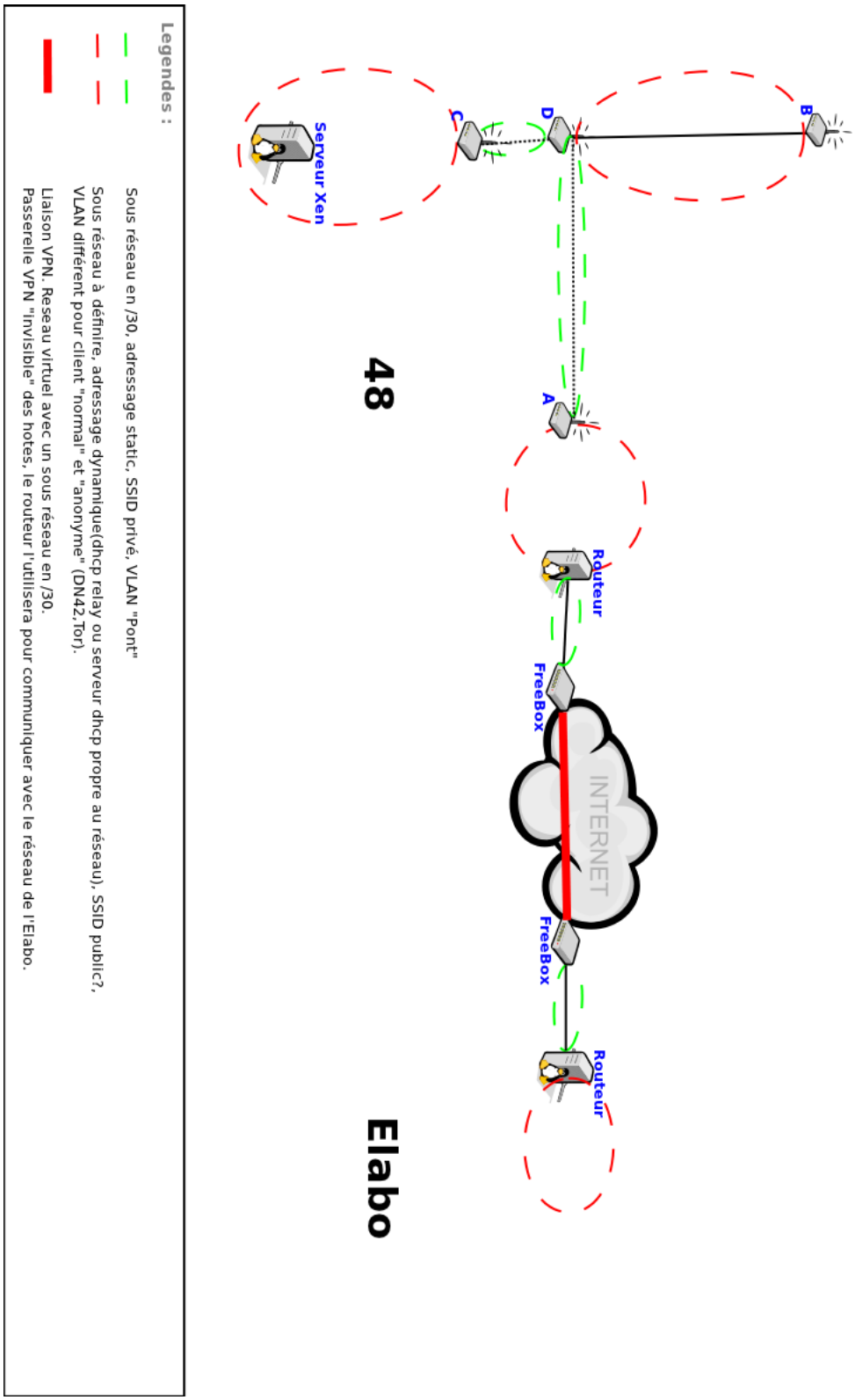
Le diagramme ci dessous nous a servi de base pour projeter nos différentes étapes dans le temps au départ du projet. Ainsi nous avons pu voir à quels moment nous étions en avance et en retard par rapport au déroulement initialement prévu.



Déroulement

Le groupe a fonctionné en autonomie. Des points réguliers ont eu lieu, une à deux fois par mois, avec l'encadrement in situ afin de suivre l'évolution du projet, de cerner certaines problématiques, et de discuter de certains choix techniques. De plus, nous avons envoyé un rapport hebdomadaire d'activité à la personne en charge de notre suivi à l'IUT.

Proposition d'architecture réseau



La solution proposée veut joindre deux entités via internet. Une connexion VPN entre le 48 et l'Elabo permettra d'etablir un pont virtuel entre ces deux lieux. Par cet accès, les hôtes de ces deux batiments pourront communiquer ensemble de façon transparente. La configuration du VPN rendra transparente la communication inter-réseaux du 48 et de l'Elabo. Cette connection site à site utilisant internet, le debit est basé sur les accés respectifs des deux batiments. Les connexions à internet n'étant pas symetriques, le débit descendant et montant ne sont pas similaires. Le pont virtuel créé entre ces deux batiments n'aura donc pas un débit élevé.

Un pont wifi avait été pensé pour apporter une reponse à l'aspect du débit, le vpn aurait joué le role de "backup" en cas de chute du pont wifi. Les batiments de l'elabo et du 48 étant éloignés d'au moins 500 métres, il aurait fallu des antennes et des acces-points puissants. Le budjet n'étant pas au rendez vous, et le site de l'Elabo étant en passe de devoir être évacué d'un moment à l'autre (et possiblement dans l'urgence), l'idée à finalement été abandonnée.

Architecure Wifi sur le site du 48

Prise en main des Linksys

Pour une meilleure gestion du réseau et avoir un accès à plus d'options, nous avons choisi de changer le firmware des linksys wrt54GL pour le passer en "OpenWrt". OpenWrt est une distribution GNU/Linux minimaliste pour matériel embarqué.

La derniére version (Backfire) a été choisie.

Solutions de mise en place de pont wifi inter-bâtiment

Architecture « routée » (relayd)

Le pont est situé sur un vlan particulier. Le plan d'adressage de celui-ci contient un masque très haut pour avoir peu d'adresses ip disponibles et ainsi n'autoriser que les connexions inter-routeurs créant le pont.

Architecture « switchée »

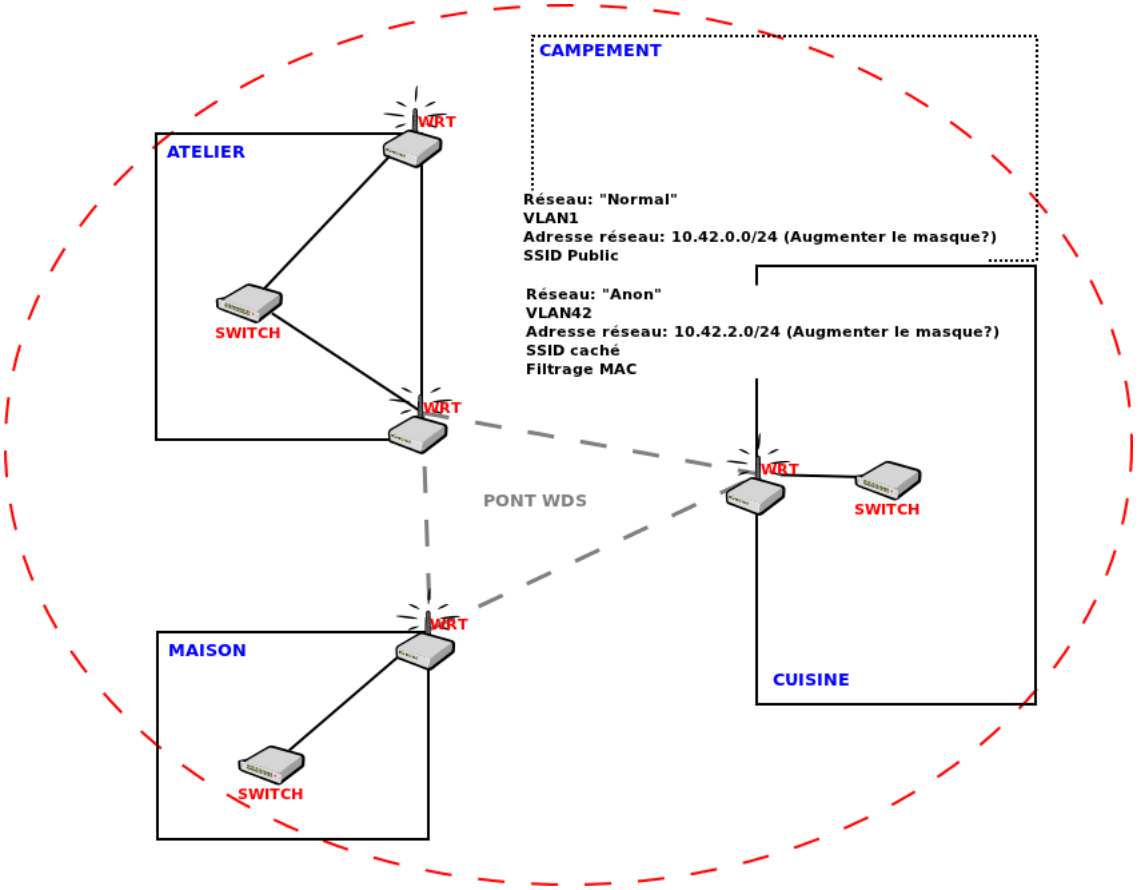
Le pont est formé par un protocole particulier :

- "WDS"(+ spanning-tree), qui peut être sécurisé (psk, psk2) : Chiffrement et Clef déterminables. Le pont est effectué via un protocole et non par le biais d'un réseau adressable, ce qui accroit donc la sécurité.
- "OLSR", topologie dynamique, envoi d'un « hello » pour se placer par rapport aux autres matériels du réseau mesh. Cependant l'architecture visée n'est pas assez imposante pour avoir besoin de ce protocole.
- "BABEL", similaire à "OLSR", est quant à lui non pas basé sur le chemin le plus court, mais sur le chemin de meilleure qualité. Le même raisonement que précédement s'applique, l'architecture n'est pas assez importante.

Le 48 voulait avoir la visibilité du voisinage réseau. Il était donc impossible d'opter pour l'architecture routée. La topologie switchée via le protocol "wds" à ainsi été préférée.

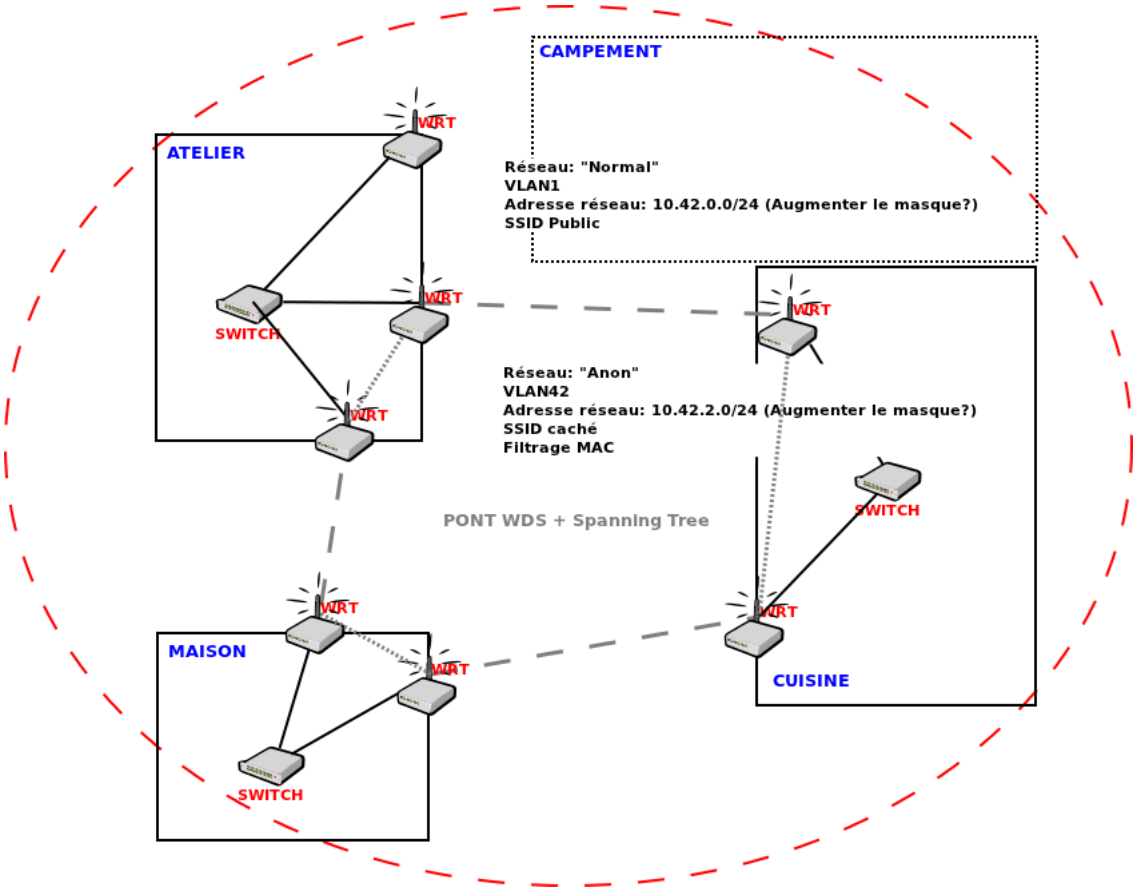
Architectures switchées proposées

Première architecture proposée :



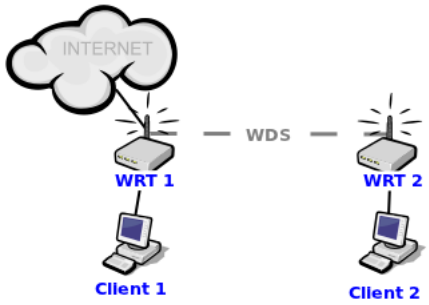
Cette première approche est basée sur un pontage « WDS » via 3 « WRT ». En sachant que les WRT utilisés pour les ponts servent uniquement à cet effet et ne peuvent recevoir de connections d'autres types. Le principal point fort de cette solution est le faible nombre de points d'accès wifi utilisés. Le point faible, quant à lui, se situe au niveau de la continuité de service. En effet si l'un des ponts tombe, la partie du réseau derriére celui-ci devient innaccessible. De plus chacun des points d'accès doit gérer deux pont différents. Les echanges sur un pont peuvent donc impacter un autre pont.

Deuxième architecture proposée :



La deuxiéme approche développée apporte une solution avec un pontage “WDS” via 6 “WRT” (Les pointillés gris materialisent des pont WDS intermediaires en option). En prennant les point faibles de la topologye précédente, cette alternative isole chacun des ponts sur des WRT différents. Ainsi plusieurs chemins peuvent être empruntés par les trames pour communiquer avec les differentes parties du réseau. Donc si un des chemins tombe par un dysfonctionnement d’un point d’accès, l’architecture réseau reste viable et les échanges peuvent continuer. La continuité de service est alors assuréé. Cependant, au contraire de l’architecture précédente, celle-ci intègre un plus grand nombre de linksys.

Test de mise en place d’un pont « wds »



Ce test a été réalisé pour verifier la viabilité des ponts wifi utilisant le protocol “WDS”. Le schéma représente une architecture utilisant un pont “WDS” dans le but de faire communiquer le “client 1” avec le “client 2”. Le linksys “WRT1” pointe vers l’adresse mac du linksys “WRT2” et inversement. Le ssid du pont est caché (BSSID) et il est égal à l’adresse MAC du partenaire du pont. Le Spanning Tree est utilisé pour former un arbre de priorités et éviter les boucles dans la topologie. Sur cet exemple un seul chemin est possible, ce protocole n’est donc pas utile sur une si petite installation. Cependant pour des mesures de test, il est utile de voir le comportement du spannig tree sur un pont wifi : Dans cette situation les interfaces wifi de nos deux point d’accès sont reservés pour former le pont, le passage de l’interface lan au pont wifi est transparent.

Ce test à été concluant, les deux clients ont pu communiquer entre eux. Il reste cependant des inconnues, comme le comportement de ces ponts avec un nombre important de clients, ainsi que des échanges spanning tree soutenus. La porté wifi ne sera une variable importante que lors de la mise en place effective.

TOR

The Onion Router (Tor) (littéralement : le routage en oignon) est une solution libre, constituant un réseau mondial décentralisé de routeurs organisés en couches (d'où l'onion routing, comme les différentes couche d'un oignon), appelés "nœuds de l'oignon", dont la tâche est de transmettre de manière anonyme des paquets TCP. C'est ainsi que tout échange Internet basé sur TCP peut être rendu anonyme en utilisant Tor. En effet, cela permet de se protéger contre certaines formes de surveillance de réseau menacant les libértés individuelles (exemple : DPI, voir plus bas).

Ce logiciel est basé sur un système de connexions "anonymes", au sens d"'impersonnelles", entre les acteurs du réseau TOR : Tor n'encrypte pas les communications sur internet. Par l'intermediaire d'un systéme de sauts, il permet à des données de sortir sur internet à la suite de plusieurs "hop" suivant un nombre aléatoire de serveurs Tor.

La communication est encryptée entre le client et les differents serveurs, hormis le dernier noeud servant de passerelle vers internet : à partir de celui-ci la communication sort normalement (pas d'encryption) afin d'être lisible et permet ainsi son interprétation sur internet. Les données de réponses reviennent par le serveur Tor d'où l'initialisation de la communication sortie. Cependant, le retour "intra-Tor" peut prendre un tout autre chemin vers la source initiale de la communication (asymétrie). Ainsi les paquets transmis par le client sont lus comme étant été envoyés par le serveur Tor de sortie sur internet. Le client reste donc anonyme vis-à-vis de son interlocuteur sur internet.

Fontionnement

Routage

Chaque noeud par lequel passe les paquets ne connait l'adresse IP que du noeud précédent et celle du suivant (n-1 / n+1). Le serveur de sortie connait l'adresse IP du dernier routeur par lequel sont passés les paquets mais ne connaitra pas l'adresse de l'internaute qui a émis la demande.

Chiffrement

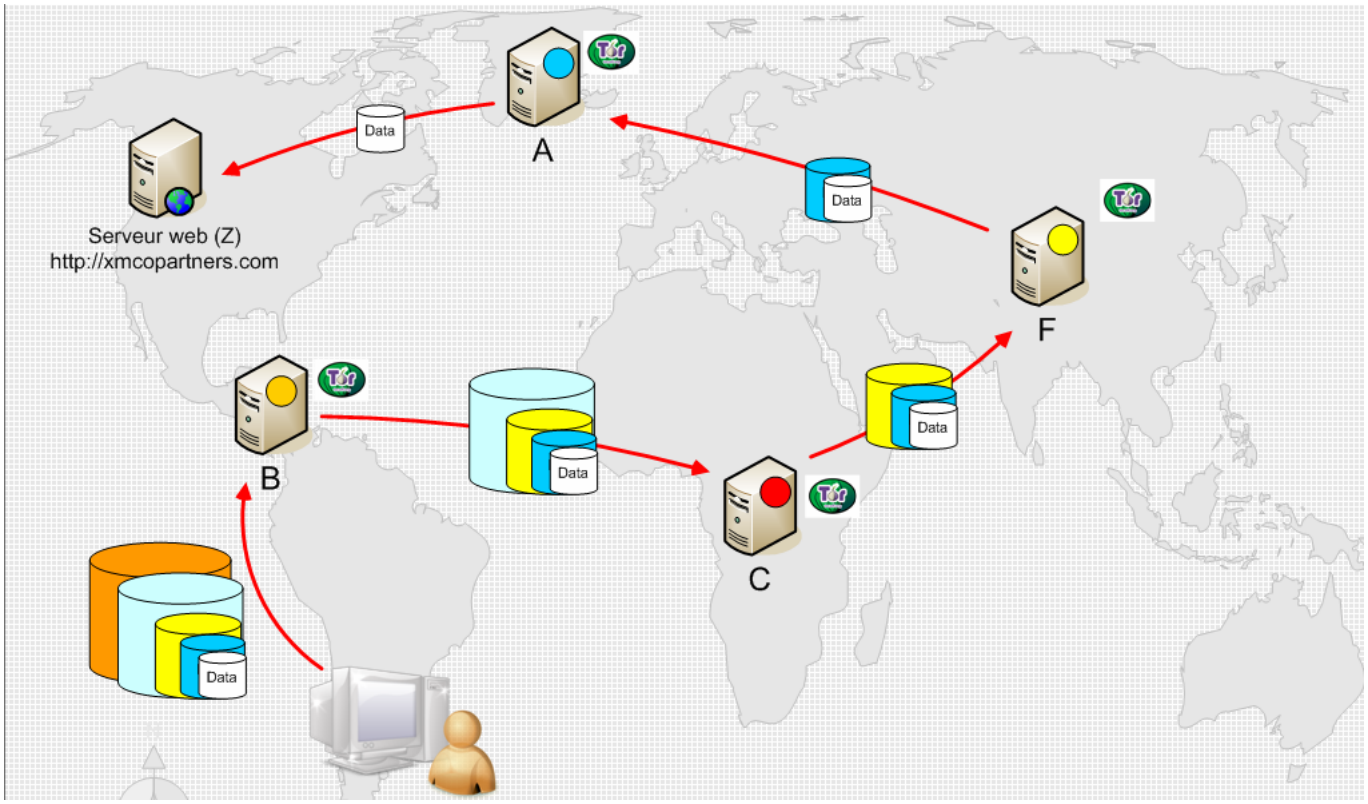
Après la phase de construction du circuit, chaque nœud a une clef secrète qui lui est propre et ne connaît que son prédécesseur et son successeur au sein du circuit. Avant que le paquet ne soit envoyé, le client Tor récupère chacune des clefs publiques des relais du circuit et chiffre les données de la manière suivante, le paquet sera chiffré de nombreuses fois :

la première fois, le client chiffre son paquet TCP avec la clef publique correspondant au dernier nœud, numéroté "n"
la deuxième fois, avec celle de l'avant-dernier nœud, numéroté "n-1"
la troisième fois, avec celle de "n-2"
la dernière fois, avec celle du premier nœud, numéroté "1".

Chaque noeud va ensuite déchiffrer partiellement le paquet avec sa clef :

le premier serveur du circuit déchiffre le paquet avec la clef "1" et l'envoie au deuxième serveur
le deuxième serveur déchiffre ce paquet avec la clef "2", etc...
le dernier serveur déchiffre ce paquet avec sa propre clef privée "n" et obtient le paquet original.

Cette méthode de chiffrement permet d'éviter qu'un élément du circuit puisse déchiffrer le message transmis. Le contenu du paquet reste inaccessible tant qu'il n'a pas atteint le dernier serveur car les données sont encapsulées.



(ci dessus, chaque cylindre de couleur représente une des “couches de l’oignon”)

Inconvenient

A première vue, Tor apparaît comme un réseau fiable et sécurisé.

Seulement si on l’étudie en profondeur, on peut s’apercevoir qu’il n’assure pas la stricte confidentialité des données :

Le réseau connait un problème majeur. Lorsque le dernier routeur du réseau (appelé noeud de sortie) a déchiffré les paquets, ceux-ci sont en clair. Il est donc en mesure de lire les données. En 2007, un pirate suédois nommé Dan Erstad divulgue de nombreux mots de passe appartenant à de nombreuses ambassades, ministères et agences gouvernementales. Pour obtenir ces mots de passe, le pirate avait positionné des noeuds Tor dans les 4 coins du monde et écouté leur trafic en sortie.

Tor propose principalement l’anonymat. Tout est pensé en ce sens, c’est pour cela que la sortie n’est pas chiffrée.

Le réseau TOR ne doit donc pas être utilisé pour envoyer des données sensibles ou alors il serait nécessaire d’utiliser HTTPS ou un chiffrement final similaire et des mécanismes d’authentification.

Mise en place d’un relay ou d’un exit server

L’installation d’un serveur TOR permet de contribuer à la qualité du réseau. La lenteur inhérente au principe de fonctionnement de Tor peut être en effet améliorée, dans une certaine mesure, en multipliant les serveurs présents sur le réseau. TOR va consommer de la bande passante sur la connexion internet, et même si le débit alloué à TOR est paramétrable, ne laisser que quelques Ko/s au nœud n’est pas d’une grande aide pour le réseau. Il faut donc être prêt à offrir de la bande passante pour TOR sur votre connexion. Les recommandations du projet TOR indiquent 20 Ko/s minimum dans les deux sens : il s’agit là d’un strict minimum...

Serveur mode relay :

Un serveur Tor configuré en mode « relay » forme un point de passage pour le trafic du réseau Tor.

Les connexions passant par ce point sont cryptées. L'adresse ip du serveur est exclusivement utilisée pour transmettre les paquets à un autre serveur du réseau Tor.

Serveur mode exit :

A contrario un serveur en mode exit, est utilisé sur le réseau Tor pour la sortie vers internet. Étant le dernier point de passage, un paquet utilisant Tor n'est plus chiffré à ce moment précis. Une écoute du réseau sur ce point peut donc être effectuée (cf « Hack of the year »). En outre l'adresse ip utilisée pour sortir sur internet est donc celle de ce serveur. Si le trafic Tor utilisant ce serveur, est utilisé de façon illégal (navigation sur des sites répertoriés comme illégaux, téléchargement d'oeuvres privatrices...), l'adresse ip incriminée sera celle du serveur. Un compromis peut être trouvé, en spécifiant les services autorisés à utiliser le serveur d'exit. Ainsi le reste du trafic sera passé à un autre serveur du réseau Tor par le mode relay du serveur. Quelque soit le mode utilisé pour participer au réseau Tor, la bande passante du serveur sera utilisée pour ce réseau. Il est possible de la limiter.

Mise en place d'une passerelle d'accès Tor

Cette utilisation permet de centraliser un client Tor. Sur un réseau local, il n'y a alors plus besoin que tous les hôtes aient un client Tor chacun, ils passent par la passerelle qui les redirige directement sur internet via Tor.

Concrètement Tor se comporte comme un proxy socks, il est donc nécessaire de configurer les applications pour l'utiliser :

- Soit dans l'application (on définit l'adresse et le port du proxy dans les paramètres du navigateur)

- Soit via une commande (exécuter dans un terminal : "~/emplacement_dossier_du_bundle_tor-browser/App/Firefox/firefox -no-remote -profile ~/emplacement_dossier_bundle_tor_browser/Data/profil

- Soit via un firewall/NAT qui redirige toutes les communications venant du réseau sur le socks tor.

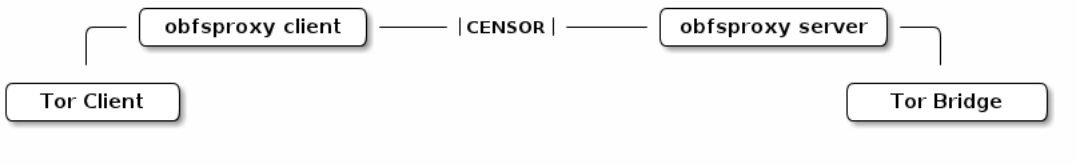
Recherche pour l'établissement des connexions clientes :

Une des propositions, pour activer ou non l'accès au réseau Tor, est la mise en place d'une passerelle VPN. L'hôte du réseau local, s'il veut utiliser Tor, se connectera à la passerelle VPN qui redirigera automatiquement ses requêtes via le réseau Tor.

Mise en place de Obfsproxy

Cet outil permet, entre autre, de mettre en place un contournement face à un Deep Packet Inspection (DPI) qui interdirait les communications chiffrées. Les communication entre les clients et les relais Tor étant chiffrées, elles sont soumises à ce type de filtrage. Obfsproxy permet alors la pérénité des connections Tor chiffrées se heurtant au DPI.

Par l'intermediaire d'un "proxy furtif" (obfuscated proxy), il permet de transformer le trafic entre un client Tor et un des relais du réseau Tor prenant en charge Obfsproxy (comme indiqué ci dessous).



Le directeur exécutif du projet, Andrew Lewman, explique que "l'idée est de faire en sorte que votre Ferrari ressemble à une Toyota en mettant la carosserie d'une Toyota sur une Ferrari, où la Toyota serait une communication normale sur Internet et la Ferrari en dessous serait la communication chiffrée".

Les dispositifs de filtrage mis en place sur internet, comme le dispositif "eagle" vendu par Amesys (filiale de Bull) dans des pays du magreb et moyen-orientaux, ne voient pas de traffic considéré comme "suspect" par le DPI grâce à ce procédé.

DN42

"Decentralized Network 42", ou DN42, est un réseau pair à pair basé sur l'utilisation de vpn. La volonté de rejoindre ce réseau vient du fait qu'il relie différents Hackerspaces autour de la planète.

Il applique une architecture similaire à internet (protocole BGP). Chaque noeud au réseau a un numero d'identification unique (AS-Number). Ce numéro est attribué via le site du projet.

L'AS-Number entre en action quand les differents noeuds du réseau DN42 communiquent entre eux : Il permet l'identifcation simple du noeud et les différents chemins qu'il connait sur le réseau. Ainsi chacun des serveur-noeuds s'echangent la table de routage pour que les paquets puissent arriver à destination.

Pour rentrer sur ce "dark internet" il faut :

un AS number

connaitre au moins un autre noeud

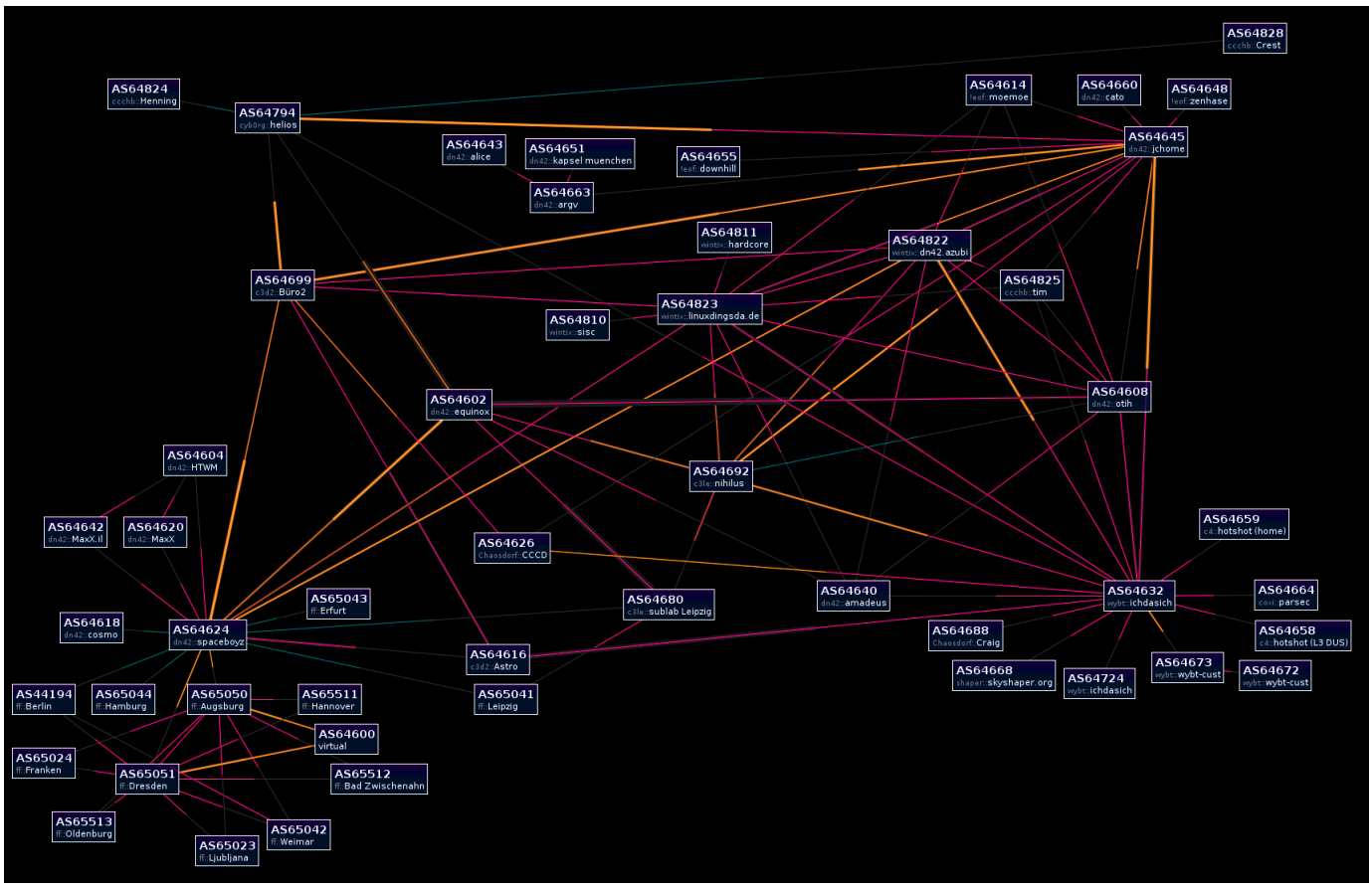
Etre relié permet la communication de l'architecture réseau, les différents chemins possibles entre deux pairs mais donne également les renseignements nécessaires quant au sous-réseau(x) géré(s) par le nouveau noeud auprès des différents acteurs du réseau DN42.

Pour un client souhaitant rejoindre ce réseau, la mise en relation à celui-ci s'effectue par l'intermédiaire d'une connexion à un des serveurs (dit "noeud") présent sur DN42.

DN42 utilise ses propres services comme BGP, DNS, IRC, ...

Nous avons porté notre choix sur OpenVPN comme suite permettant l'établissement des connections aux différents Peers (principe de Tunnel VPN). Ce choix a été motivé par la simplicité d'installation ainsi que la notoriété d'OpenVPN quant à sa stabilité, et sa sécurité (le code source est régulièrement vérifié par la communauté OpenSource). Les autres alternatives étaient GRE, TINC, QuickTun.

Une fois relié, les routes du VPN (échangées via BGP), garantissent non pas l'anonymat du contenu échangé, mais l'anonymat geophysique des peers : les ip sont des ip locales de type 172.22.n.0/23 , avec un AS-Number de type 64600+n. Une table d'allocation autogérée est disponible sur le site du projet (https ://dn42.net).



Modification du cahier des charges

Dans le cahier des charges initial, il nous avait été demandé de penser une solution par ponts WIFI inter-batiments sur le site du 48, comme indiqué précédemment. Les batiments ayant finalement été reliés par cable éthernet, la demande a évolué au milieu du projet au profit d'un arrosage WIFI en bouts de lignes afin de couvrir la superficie du site et permettre aux résidents une connection mobile grâce à une SSID unique sur les différents WRT à poser.

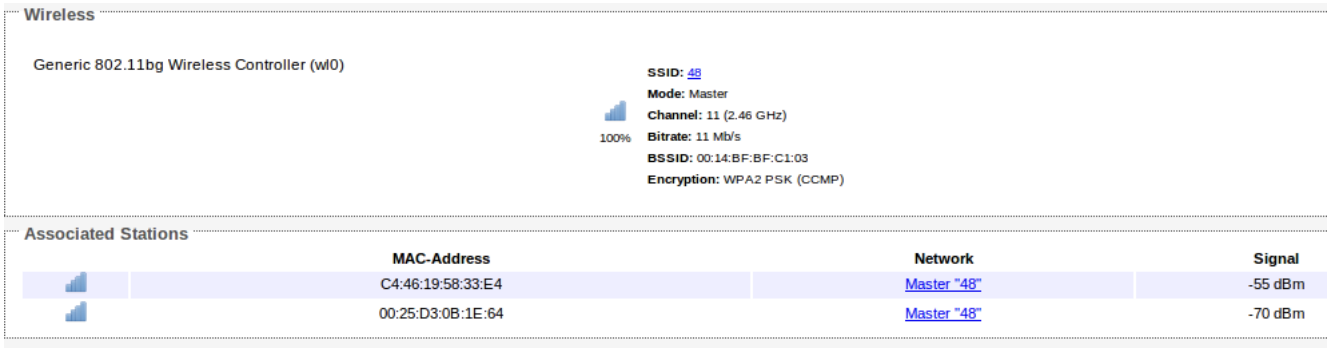
Il nous a donc fallu abandonner le fruit du travail de plusieurs semaines pour s'adapter à la nouvelle demande.

WRT d'Access-Point

Développement et mise en place d'une configuration TYPE

Suite aux directives du 48, nous avons fait plusieurs interventions pour remplacer des linksys WRT défectueux et également pour en installer de nouveaux. Pour que la configuration soit armonisée entre les différents équipements wifi, une configuration type à été mise en place, et est encore active à l'heure actuelle.

Celle-ci contient un SSID "48". Chaque routeur ayant le même SSID, un ordinateur peut changer d'acces-point automatiquement sans perte de connection.



Les interfaces Wifi et Lan des wrt sont bridgée. Ainsi le réseau complet forme un unique réseau niveau 2 (ethernet). Un réseau niveau 3 (IP) était envisageable, il aurait permis de réduire la charge potentielle du réseau (broadcast...) mais obligeait à modifier/configurer certaines applications reposant sur un réseau niveau 2 (netbios/samba/partage de fichiers windows). Cela reste néanmoins une évolution possible dans le futur.

Le service DHCP est désactivé sur chacun des points d'accès wifi pour centraliser ce service. Un DHCP sur chacune des AP aurait pu faire baisser la charge du DHCP principal en étant considéré comme plusieurs serveurs DHCP secondaires. Cependant le nombre de clients en DHCP n'étant pas important, il n'est pas primordial d'initialiser le service DHCP sur les WRT.

Chacun d'entre eux a une adresse ip configurée en statique. Une idée aurait été de les mettre eux aussi en client DHCP. La configuration aurait été la même sur chacun des linksys (si il n'y avait pas de changement de Hostname). Cependant pour l'administration, cela aurait posé un problème : l'adresse ip pouvant potentiellement changer à tout moment, retrouver la bonne ap à administrer serait devenu beaucoup plus long. Une adresse ip allouée en fonction de l'adresse MAC des différents AP aurait pu être mise en place pour pallier ce problème.

Le Serveur Passerelle

Ce serveur a plusieurs finalités :

- Firewall (Sécurité de l'accès et de l'utilisation du réseau)
- Serveur DHCP (Distribution de paramètres IP)
- Serveur DNS (Resolution de nom et gestion de zone locale)

Cependant il n'a pas été mis en place : La détermination de l'O.S. destiné à ce serveur n'est toujours pas fixé. Pfsense était une hypothèse de départ, mais il n'est pas assez modulable et n'a, à cette heure, pas été retenu sans pour autant que nous ayons eu le temps de nous accorder sur une alternative avec l'équipe du Hackerspace. Des problématiques techniques liées au matériel (un Firebox X550 réccupéré) ont egalement gelé les divers tests de configuration.

Cependant, nous avons évalué les besoins du réseau afin d'ébaucher une configuration à appliquer et adapter au serveur. Une telle configuration permettrait :

- la mise en place d'une zone dns specifique locale
- la mise en place d'un accès ipv6 via un tunnel 6in4 (méthode d'encapsulation d'IPv6 dans IPv4 utilisée dans un mécanisme de transition d'IPv4 vers IPv6)
- l'équilibrage de la bande passante entre les différents utilisateurs
- un équilibrage fin entre les protocoles (protocoles interactifs (web,dns,mail..) privilégié au détriment des protocoles faiblements intéractifs (téléchargement..)

Nous nous somme penchés particulièrement sur l'aspect Firewall :

Cette passerelle doit donner l'accès à internet, mais aussi rendre accessible quelques serveurs (Noeud Tor, DN42, Mail) depuis internet. Il faudra donc limiter les connexions entrantes à celles établies par les clients du réseaux local, et également autoriser celles communiquant avec Tor et Dn42.

Résultat (en cours de mise en place)

Le cahier des charges initial a évolué tout au long du projet, et ce pour plusieurs raisons :

- Nous avons évolué au sein d'un milieu associatif, impliquant le fait que les personnes sont des bénévoles. Par conséquent, leur temps de présence est fluctuant. De plus, les membres de l'Elabo/48 ont une méconnaissance technique en informatique et réseau. Il nous a donc été nécessaire de traduire les besoins exprimés, et parfois de les adapter à la réalité de terrain.
- Le Hackerspace est une "association de fait". C'est à dire qu'il n'y a pas de liste de membres, pas de bureau, pas de chaine de décisions. Les choix se discutent collégialement, avec le paradoxe inhérent que les participants vont et viennent en fonction de leur disponiblité et rythme de vie. Ainsi une décision nécessite un croisement de regards au sein d'un groupe fluctuant, impliquant que certaine inertie parfois dans la prise de décision, avec des position collectives pouvant varier en fonction de l'arrivée d'Untel qui ouvre une nouvelle perspective sur une problématique identifiée. C'est une richesse qui comporte intrinsèquement ses inconvénients par moments, mais une valeur fondamentale partagée au sein du lieu.
- Divers soucis techniques se sont imposés à nous. Comme dans tout Projet, il y a les impondérables auxquels il faut faire face au fur et à mesure qu'ils arrivent car on ne peut tous les anticiper. Ces nouvelles données remettent parfois en cause les choix établis, et/ou viennent perturber la linéarité temporelle du déroulement du projet initial. Par exemple, certains WRT sur lesquels ont comptait se sont trouvés être défectueux au final, réduisant notre champs d'action. De même, le Firebox devant nous servir de passerelle s'est trouvé avoir un fonctionnement aléatoire au niveau de sa fiabilité de service et demande à être révisé. Ceci nous a conduit à reporter la mise en place de la passerelle, élément clef de la mise en production de notre architecture.
- Sur la dernière partie du projet, la configuration d'un des batiments a été modifiée dans son utilisation, avec pour conséquence un des WRT qui a été supprimé. Le fait qu'il y ait beaucoup de projets en parallèle dans un même lieu fait que la communication est plus complexe à mettre en oeuvre.
- Tout au long du projet, nous sommes intervenus en maintenance sur le réseau WIFI en réponse aux sollicitations des membres du 48/Elaboratoire qui pensaient à une défection du réseau/installation/architecture. Or, bien souvent il s'agissait d'erreurs humaines n'ayant rien à voir avec notre installation : WRT débranchés pour une autre utilisation de la prise électrique, ... A contrario, cela nous a permis de faire de la pédagogie auprès des résidents et utilisateurs du lieu afin de qu'il comprennent mieux le fontionnement de l'architecture.

Difficultés rencontrées et surmontées :

- L'encadrement initiallement prévu a été plus léger en réel : Nous avons travaillé plus en autonomie, avec parfois de la perte de temps faute de recadrage rapide sur des choix. Néanmoins, cela nous a conduit à faire de nombreuses recherches afin de trouver des réponses à nos questions par nous même, puis de s'appuyer sur les "tuteurs" de terrain afin de vérifier nos recherches ou non. Cela nous a amené à devoir reformuler ce que nous pensions avoir compris par nous même, ce qui est un exercice fort intéressant et enrichissant.
- A l'origine nous étions en binôme, et l'arrivée d'une troisième personne en milieu de projet nous a conduit à réexpliquer notre démarche de projet, l'historique, les taches, et nous réorganiser pour faire un trio où chacun aurait sa place et trouverait son plaisir.
- De formation hétérogène, le déséquilibre des bases en informatique du binome initial aurait pu nuire à la construction du projet. Mais à contrario, cela nous a soudé et le partage des connaissances a été effectif, fructueux et plaisant.

Parties réalisées selon le dernier cahier des charges en date :

- Les WRT sont fonctionnels et en production depuis leur mise en place sur le site. Suite aux diverses discussions avec les membres de l'Élaboratoire/48 sur les raisons de baisses de signal en fonction de l'utilisation et horaires de pointe, il est en projet d'augmenter la puissance des antennes. Les discussions sont en cours.
- Les configurations DN42 et TOR sont prêtes à être mises en production.
- Une connexion vers le reseau DN42 a été montée. Elle permet de d'envisager de rejoindre celui ci pleinement en paticipant à la mise en place de nombreux services internes au reseau (DNS anycast, noeud irc...).
- Une solution TOR est également active mais hors zone de travail.

Projections :

Nous tenons à finir la mise en place prévue du projet et restons actifs au sein du Hackerspace qui a su nous accueillir avec bienveillance. Ainsi nous allons procéder à :

- la mise en place de Vlans : comme prévue dans le cahier des charges, un vlan pour la navigation normale sur internet, et un autre vlan pour la navigation anonyme.
- la mise en place d'un VPN afin d'avoir un accès extérieur pour les taches administratives sur les serveurs de production.
- Contribuer à la sensibilisation et l'élaboration d'une pédagogie à propos de l'usage de l'anonymat sur internet auprès des résidents du lieu et des personnes de passage (spectateurs, artistes en résidence ...)
- Nous impliquer dans la poursuite du cahier des charges évolutif : un réseau qui vit est un réseau qui évolue.

Expérience

Lors de ce projet, nous avons pu nous enrichir de diverses manières :

- la confrontation au réel : travailler en réel sur un projet qui doit être mis en production est plus motivant que rester dans une salle où le projet ne restera qu'au stade de projet. Ainsi l'engagement dans le réel est moteur, et l'apprentissage plus profond.
- le travail en équipe : travailler en équipe, expliquer ce que l'on sait, ce que l'on pense avoir compris, se confronter à l'autre de manière constructive et coopérative est une démarche ludique et aiguise la curiosité, la soif d'apprendre. L'émulsion du travail collaboratif est une force quand l'équilibre se trouve en sein du groupe.
- adaptation continuelle : les changements réguliers des conditions de déroulement du projet ont développé une aisance à l'adaptation, tant aux personnes qu'aux matériels et techniques.
- déchiffrage des demandes : le langage humain est parfois trouble et l'idée que l'on veut exprimer se perd parfois dans les mots. Ce phénomène est d'autant accentué si l'on est en contact avec des personnes ne maitrisant pas le même vocabulaire technique. Décrypter une idée chimérique afin d'expliquer son infaisabilité dans le réel est un exercice parfois hardu, mais c'est une gymnastique de l'esprit qu'il faut savoir garder si l'on veut continuer à inover dans la richesses des réponses que l'on pourra apporter aujourd'hui comme demain.
- études et comparaison de solutions : en informatique il y a souvent plusieurs solutions possible à apporter à une problématique donnée. Les rechercher, puis les comparer aide à les différencier et par conséquent à les intégrer avec plus de finesse.
- approfondissement des solutions libres : opérer au sein du Hackerspace et de l'Elaboratoire/48 nous a permis d'approfondir les enjeux induits par les solutions libres, tant au niveau technique que des relations humaines et postures éthiques.
- enrichissement du réseau de contacts : être au contact régulier des membres des lieux nous hébergeant pour le projet nous a également permis d'enrichir notre réseau social et professionnel : au sein du Hackerspace, on peut effectivement trouver des étudiants, des enseignant-chercheurs, et également des professionnels en poste en entreprise. L'environnement de contact interpersonnel dans lequel s'est déroulé le projet n'étant pas un milieu professionnel stricto sensu, les relations se nouent d'une autre manière, et le rapport de partage de connaissance et de techniques s'en est trouvé favorisé.

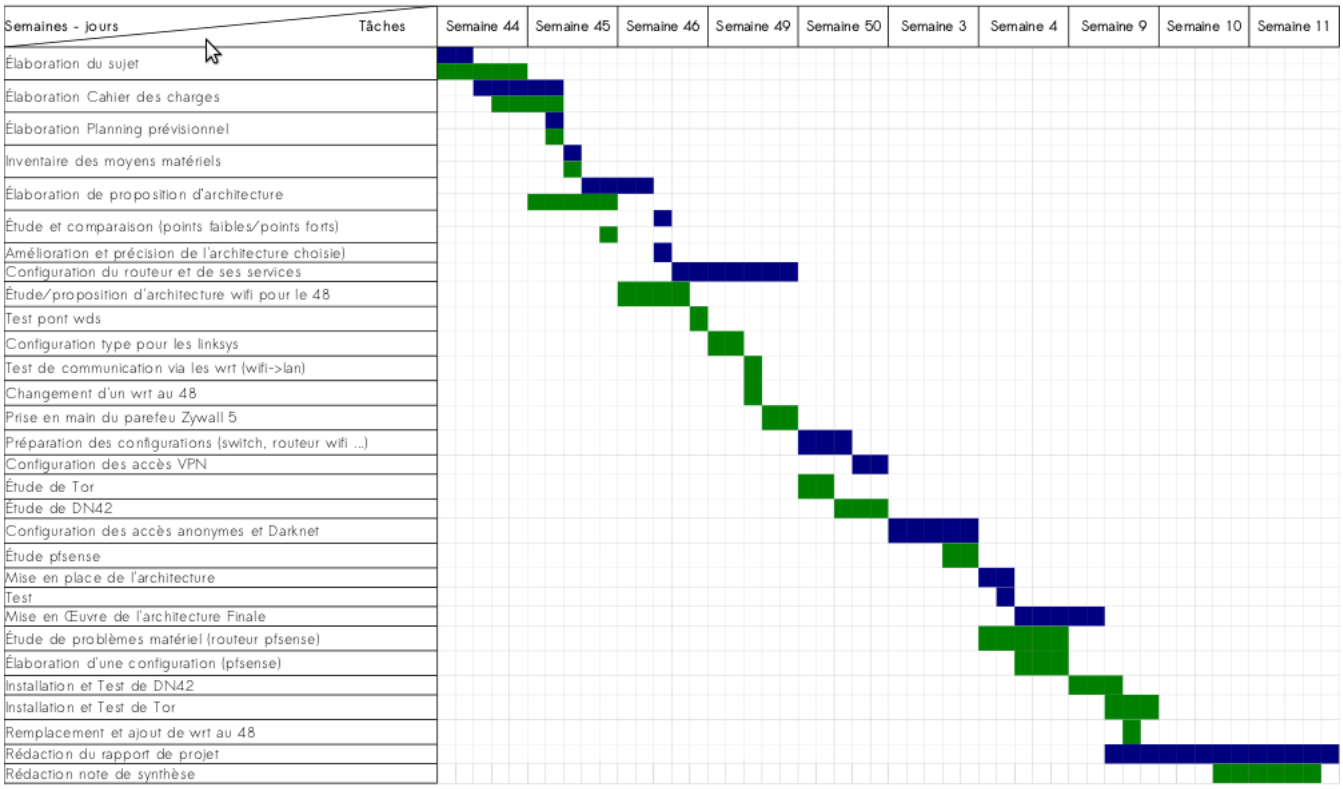


Diagramme de Gant Final prévisionnel (en bleu) et le réalisé (en vert)

Documentation Technique

Tutoriel DN42 (à vérifier : adressage, nom de fichiers)

Adresse réseau reversée à Breizh-Entropy : 172.22.108.0/23

As Number réservé à Breizh Entropy : 64708

OpenVPN

Installation du paquet openvpn :

aptitude install openvpn

Configuration Coté Serveur

Génération de la clef à échanger avec les peers

openvpn –genkey –secret dn42-48.key

Fichier de configuration

***Pour respecter la nomenclature DN42, la syntaxe suivante est préférée : dn42-48.conf**

mode p2p # Mode PeerToPeer
remote @ip/nom_de_domaine(dydns) PORT # Adresse du Peer déjà rattaché à DN42
lport 50001 # Port local
rport 22200 # Port Distant
proto udp # Protocole UDP
dev tun # Mode Routé // Nom de l'interface
#tun-ipv6 # Utilisation de l'IPv6 si désiré
comp-lzo # Compression du flux
secret dn42-48.key # Le fichier clef
chroot /etc/openvpn/jail # Répertoire « prison » du service

user DN42 # Utilisateur pour le service openvpn
group openvpn # Groupe pour celui-ci
persist-key # Si interruption, on garde la clef.
Persist-tun # Si interruption, on garde le nom de l'interfaçe.
status /etc/openvpn/jail/log/dn42-48.log
log-append /etc/openvpn/jail/log/dn42-48.log
verb 2 # Taux de verbosité.
Ifconfig 172.22.108.1 172.22.108.2 # Adressage : 'ifconfig @ip_local @ip_distante'

Permission

Fichier de conf : 640
Fichier Clef : 400

Création du script d'init

cd /etc/init.d
ln -s openvpn dn42-48

Initialisation du script au démarrage

update-rc.d dn42-48 defaults

(« remove » pour une suppression du demarage)

Quagga

Installation

apt-get install quagga

Activation des services zebra et bgp

(/etc/quagga/daemons)

zebra=yes
bgpd=yes

Vérification de la conf des daemon, liés à la boucle local

(/etc/quagga/debian.conf)

zebra_options=" –daemon -A 127.0.0.1" bgpd_options=" –daemon -A 127.0.0.1"

Configuration basique de zebra

(/etc/quagga/zebra.conf)

hostname hostname-zebra
password mot_de_passe
log file /var/log/quagga/zebra.log
service advanced-vty
line vty exec-timeout 0 0

Configuration basique de bgpd

(/etc/quagga/bgpd.conf)

hostname hostname-bgp
password mot_de_passe
log file /var/log/quagga/bgp.log
service advanced-vty
line vty
exec-timeout 0 0

Lancement de quagga

/etc/init.d/quagga start

*Vérification du lancement de quagga par la commande « lsof -i »

Configuration de quaggga Connexion au service bgp

telnet localhost(@ip_serveur_bgp) 2605

Commandes basiques

show running-config //Voir la running config
configure terminal //Entrer dans le mode configuration
end //Quitter le mode configuration
write file //Sauvegarde des changements

Configuration du routeur bgp

router bgp AS_number //En mode configuration Assignation du As number
bgp router-id @adresseDN42_perso //Assignation d'un identifiant routeur
network @reseauDN42_perso/masque //Assignation du réseau

Sortir du mode configuration et sauvegarder.

Mise en place de la prefix-list

Liste : https ://dn42.net/trac/wiki/BGP_Filter
En mode configuration, rentrer les commandes de la liste souhaitée puis sauvegarder.

Mise en place du peering

En mode configuration, entrer la configuration du routeur :

routeur bgp 64708 //ASNumber

Ajout du peer

neighbor @ip_peer remote-as AS_number_peer
neighbor @ip_peer description peer_name
neighbor @ip_peer soft-reconfiguration inbound
neighbor @ip_peer prefix-list dn42
neighbor @ip_peer route-map dn42-out out

Sauvegarder et quitter

Configuration Coté Client

Coté client, on doit retrouver dans /etc/openvpn/ 4 fichiers :
– ca.crt
– $PEERNAME$.conf

client
dev tun
proto udp
remote $NOM_DU_SERVEUR_DISTANT$ 22200 //port distant
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert $PEERNAME$.crt
key $PEERNAME$.key
ns-cert-type server
comp-lzo
verb 3

- $PEERNAME$.crt // certificat donné par le serveur
- $PEERNAME$.key // clef donnée par le server

Commande de connection

openvpn –config /etc/openvpn/$PEERNAME$.conf

Configuration de Bind

/etc/bind/named.conf.local

```
zone "dn42" {
        type forward;
        forwarders { 172.22.0.53; };
};
zone "22.172.in-addr.arpa" {
        type forward;
        forwarders { 172.22.0.53; };
};
zone "23.172.in-addr.arpa" {
        type forward;
        forwarders { 172.22.0.53; };
};
```

Tutoriel TOR

Création d'une passerelle TOR

On installe les paquets TOR :

```
wget http://www.torproject.org/dist/tor-0.2.1.28.tar.gz
tar xzf tor-0.2.1.28.tar.gz && rm tor-0.2.1.28.tar.gz
cd tor-0.2.1.28
./configure
make
su -c 'make install'
```

Requirements: 'apt-get install build-essential' ; 'apt-get install libevent-dev' ; 'apt-get install libssl-dev'

Configuration de Tor comme simple point d'entrée dans le réseau TOR :

Emplacement: /etc/tor/torrc

Port et adresse d'écoute du démon Tor ORPort 9001
ORListenAddress 127.0.0.1

Port et adresse d'écoute pour les requêtes DNS DNSPort 53

Port et adresse d'écoute pour Tor en mode proxy transparent TransPort 8118
TransListenAddress 0.0.0.0

Lancement de Tor: invoke-rc.d tor start

Activation IP forward dans /etc/sysctl.conf net.ipv4.ip_forward=1

Configuration netfilter/iptables Afin de concentrer tout le trafic entrant vers le proxy transparent local, on configure quelques règles iptables simples:

Règles locales

iptables -t nat -A OUTPUT -p tcp -j REDIRECT –to-ports 8118 iptables -t nat -A OUTPUT -p udp -m udp –dport 53 -j REDIRECT –to-ports 53

Règles extérieures

iptables -t nat -A PREROUTING -p tcp -j REDIRECT –to-ports 8118 iptables -t nat -A PREROUTING -p udp -m udp –dport 53 -j REDIRECT –to-ports 53

Création d'un serveur TOR

Installation de TOR :

Ajouter le dépôt de torproject.org au fichier "/etc/apt/sources.list" deb http://deb.torproject.org/torproject.o karmic main

Décommenter la ligne deb http://deb.torproject.org/torproject.org experimental-karmic main

Importer la clé du dépôt gpg –keyserver keys.gnupg.net –recv 886DDD89
gpg –export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -

Installation des paquets TOR apt-get install tor tor-geoipdb

Configuration de polipo : La version actuelle de TOR utilise Polipo qui permet d'avoir des connexions SOCK. Tor lance un proxy supportant Socks5.

Configurer fichier /etc/polipo/config proxyAddress = "127.0.0.1"
proxyPort = 8118
allowedClients = 127.0.0.1
allowedPorts = 1-65535
proxyname = "localhost "
socksParentProxy = "localhost:9050"
socksProxyType = socks5
Configurer serveur tor
Configurer un client ntp
ntpdate pool.ntp.org

Editer fichier /etc/tor/torrc SocksPort 9050
SocksListenAddress 127.0.0.1
DataDirectory /var/lib/tor
Nickname pseudo-du-serveur
Address adresse_ip_fixe
ContactInfo votre_nom votre_@adresse.mail
ORPort 9001
BandwidthRate 20 KB #Bande passante allouée au minimum
RelayBandwidthBurst 80 KB # Bande passante allouée au maximum
BridgeRelay 1 ExitPolicy reject *:*
Pour ne pas être noeud de sortie L'option ExitPolicy est importante, puisqu'elle permet de déterminer le type de serveur (serveur relai ou de sortie).

Créer le répertoire référencé dans le paramètre DataDirectory et rendre l'utilisateur propriétaire de ce répertoire : chown debian-tor.debian-tor /var/lib/tor

Configurer pare-feu et le cas échéant le routeur pour accepter les connexions provenant de Tor

Redémarrer Tor