Rapport de TER

Interconnexion de réseaux radio
de niveau 2 et 3

A l’attention de :
Laurent Guerby
Philippe Latu

Rédacteurs :
Alioune KASSE
Cheikh SALL

2012-2013
SOMMAIRE

REMERCIEMENTS .................................................................................................................................5

RESUME ..................................................................................................................................................6

I. PRESENTATION DE L'ASSOCIATION ...........................................................................................................7

II. PRESENTATION DU PROJET .......................................................................................................................9

   1. PROBLEMATIQUE ...............................................................................................................................9

   2. OBJECTIFS ...........................................................................................................................................9

   3. PLANIFICATION ...................................................................................................................................9

III. OUTILS ET RESSOURCES INFORMATIQUES .............................................................................................10

   1. Chiliproject ..........................................................................................................................................10

   2. Equipements .........................................................................................................................................11

       a. Equipements radio ...............................................................................................................................11

       b. Equipements réseau ............................................................................................................................17

   3. Outils de test ......................................................................................................................................18

   4. Stockage des fichiers ............................................................................................................................19

IV. TRAVAUX REALISES ...................................................................................................................................19

   1. Rappels ...............................................................................................................................................19

   2. Documentation .....................................................................................................................................21

   3. Familiarisation avec les équipements ....................................................................................................21

   4. Tests et améliorations de performances ...............................................................................................28

       a. Entre 2 Ubiquity NanoStation M5 ......................................................................................................28

       b. Entre 2 Mikrotik CPE SXT .................................................................................................................32
c. Entre Mikrotik 433L et 433UAHL .................................................................................. 39

d. Entre NanoStation Ubiquity et Mikrotik CPE SXT .................................................... 42

e. Entre NanoStation Ubiquity et Mikrotik 433 UAHL/433L ........................................... 46

5. Etude sur le protocole STP .......................................................................................... 48

6. Mise en place de réseaux virtuels : VLAN .................................................................. 68

CONCLUSION .................................................................................................................. 85

REFERENCES BIBLIOGRAPHIQUES ........................................................................ 86

GLOSSAIRE ...................................................................................................................... 87
REMERCIEMENTS

Nous tenons à remercier M. Laurent Guerby maître de stage et président de l’association teteneutral.net, pour nous avoir fait confiance et permis d’effectuer ce stage.

Nous remercions également M. Philippe Latu, enseignant tuteur du stage pour sa disponibilité, son encadrement et qui, grâce à ses compétences techniques sur les différents outils utilisés, nous ont permis de mener à bien notre stage et notre soutenance.

Merci à tout le personnel, enseignant ou non, du département informatique Réseaux Télécom de l’IUP STRI de Toulouse.
RESUME

Nous avons effectué notre stage dans le cadre de la validation de notre formation Master 2 STRI au sein de l’association Tetaneutral.net.

Cette association est une organisation récente qui a pour objectif principal de militer pour la neutralité de l’accès au réseau.

La réduction de la dépense énergétique étant un enjeu majeur pour le développement durable, il est primordial pour l’association Tetaneutral.net de disposer des équipements à basse consommation électrique.

La mission qui nous a été confiée fut celle de faire une étude entre des équipements existants de type Ubiquity avec des équipements Mikrotik dont la consommation est moindre.

Une grande partie du projet a été des tests de performances et d’interopérabilité entre des équipements.

Ce stage nous a été précieux car il nous a permis de travailler en total autonomie dans un cadre professionnel.

De plus, nous avons pu perfectionner nos connaissances en interconnexion radio.

Enfin, nous avons pu mettre en application les enseignements reçus au cours de nos années universitaires, tel que la configuration de switches CISCO, le protocole STP et la mise en place de réseaux virtuels.
I. PRESENTATION DE L'ASSOCIATION

L'internet est un réseau informatique mondial, souvent appelé le réseau des réseaux. Il est un enjeu social et politique majeur avec près de deux milliards d’utilisateurs dans le monde et il met en œuvre des sciences et techniques à un niveau avancé.

L’internet est un réseau décentralisé composé d’opérateurs qui acceptent de s’échanger des données en suivant le standard IP, « le protocole internet ».

Pour promouvoir la compréhension de l’internet et de ses enjeux par un large public, l’association Tetaneutral.net a décidé de devenir membre à part entière de ce réseau en exerçant les fonctions de Fournisseur d’Accès à Internet (FAI), d’hébergeur internet et d’opérateur sous forme associative, sans but lucratif et exigeant la neutralité du réseau.

Neutralité du réseau :

Les fournisseurs d’accès à internet, les hébergeurs et les opérateurs relient les utilisateurs du réseau entre eux et avec des fournisseurs de services. Ces intermédiaires ont techniquement la capacité de discriminer à l’égard de la source, de la destination ou du contenu de l’information transmise sur le réseau. Or pour le bon fonctionnement de l’internet, il est important que ces acteurs respectent la « neutralité du réseau » et s’interdisent de telles discriminations. De puissants intérêts commerciaux et politiques sont en jeu derrière cette simple notion.

Tetaneutral.net explique et défend la neutralité du réseau internet.

Services

Pour couvrir ses frais d’infrastructure, l’association propose à ses membres un certain nombre de services payants. Le principe de tarification appliqué est celui de Mix’Art Myrys : la participation libre est nécessaire. L’association donne une grille de tarif du normal au réduit et les membres contribuent selon leurs moyens et leur conscience et cela sans justificatif.

- Hébergement de machine virtuelle : tarif normal 10 euros/mois, suggéré de 5 à 15 euros/mois,
- Hébergement de machine physique au format libre : suivant la consommation électrique. 5 à 10 euros/mois pour une petite machine comme Netbook, Laptop, Nettop, NAS, Sheevaplug. 15 à 25 euros/mois pour un PC avec une référence à 20 euros pour une consommation de 100 Watt. Prévoir un onduleur. IP supplémentaires sur demande,
- Certificat OpenVPN : tarif normal 10 euros/mois, suggéré de 5 à 15 euros/mois,
**Moyens techniques**

Tetaneutral.net utilisera tous les moyens à sa disposition pour faire passer l’internet. Via French Data Network, l’association peut offrir un accès ADSL en dégroupage partiel. Entre son local et le centre réseau, une fibre optique a été posée. Du local au réseau des utilisateurs, une liaison radio en réseau redondant est déployée basée sur les travaux de Toulouse Sans Fil. Et enfin, dans le cadre des évolutions réglementaires et tarifaires l’association regarde s’il est possible de mettre en place de la fibre chez ses membres.

**Administratif**

Tetaneutral.net est une association loi du 1 er Juillet 901 déclarée à la préfecture de Haute-Garonne.

Récépissé de déclaration de création de l’association numéro W313015266
Date de déclaration : 3 Janvier 2011

Siège Social :

Association Tetanueutral.net  
c/o Laurent GUERBY  
10, Chemin Tricou  
31200 TOULOUSE

Tetaneutral.net est inscrite dans la base SIRENE de l’INSEE :

- SIREN : 529 558 710
- SIRET du siège : 529 558 710 00016
- Désignation : TETANEUTRAL.NET
- Catégorie juridique 9220 Association déclarée
- APE 6209Z Autres activités informatiques
- Date de prise d’activité 03/01/2011

Tetaneutral.net est opérateur déclaré auprès de l’ARCEP depuis le 20 Janvier 2011 :

ASSOCIATION TETANEUTRAL  
Récipissé de déclaration numéro 11/0092  
Services autres que téléphonique réseau ouvert au public.

Ses membres fondateurs sont :

Pierre-Guy BAREGES,  
Mar BRUYERE (secrétaire),  
Laurent GUERBY (président),  
Alexandre GUY (trésorier),  
Arne STOLCK

Kassé- Sall
II. PRESENTATION DU PROJET

1. PROBLEMATIQUE

Dans le but de diversifier les équipements utilisés et d’avoir une large gamme de produits, l’association souhaite introduire dans son réseau de nouvelles installations radio du constructeur Mikrotik. Ces dernières présentent l’avantage principal de consommer moins d’énergie et présente un large éventail de fonctionnalités.

Une étude aux préalables de ce matériel ainsi que son interopérabilité avec le système existant est nécessaire avec son introduction sur le réseau de l’association.

2. OBJECTIFS

Le but principal de cette étude est de réaliser des tests d’interopérabilité et de performances entre les équipements radio déjà existants c’est-à-dire les Ubiquity NanoStation et les nouveaux équipements, les Mikrotik.

D’autre part, notre deuxième objectif était de faire une étude sur le protocol spanning tree.

Ces études sont fortement axées sur les niveaux 2 et 3 du modèle OSI.

3. PLANIFICATION

Le projet a duré 2 mois. Il a été découpé en trois grandes phases :

- Une première partie basée sur la documentation et la découverte des équipements,
- Une deuxième partie sur les tests de performance entre les équipements,
- Une dernière partie de mise en place du protocole STP et de réseaux virtuels.

Plannings prévisionnel et réel (voir Annexes)

Des réunions ont eu lieu tous les jeudis en fonction des disponibilités de nos responsables pour faire le point sur l’état d’avancement du projet.
III. OUTILS ET RESSOURCES INFORMATIQUES

1. Chiliproject

Tout au long de ce stage, nous avons utilisé l’outil de travail collaboratif Chiliproject, système web de gestion de projet. Une page web nous a été octroyé, accessible via le lien suivant:

http://chiliproject.tetaneutral.net/projects/tetaneutral/wiki/StageAirOSRouterOS

Ce wiki prend en charge toutes les personnes impliquées tout au long du cycle de vie du projet et permet de mettre en place et de discuter d’un plan de projet sur les questions de suivi et de reporting d’avancement des travaux à la connaissance collaborative de partage.

Ce wiki nous a permis durant tout le projet de reporter nos résultats intermédiaires obtenus, des liens utiles... permettant ainsi à nos tuteurs de suivre l’avancement de nos travaux et d’amener éventuellement des correctifs, remarques et suggestions.

Des notifications de mise à jour de la page sont envoyées à chaque observateur ajouté sur cette dernière dès qu’un utilisateur effectue des modifications. Parmi les observateurs, figurent nos 2 tuteurs (Philippe Latu et Laurent Guerby).

Observateurs de notre wiki Chiliproject
2. **Equipements**

   a. **Equipements radio**

**Ubiquity NanoStation M5**

Point d’accès extérieur 5GHz N avec antenne intégrée. Elle intègre la technologie AirMax permettant d'obtenir des débits de données jusqu'à 150Mbps LAN. L'antenne intégrée à double polarisation bénéficie d'un nouveau design qui porte son gain à 16dBi. La NanostationM5 intègre également un second port Ethernet avec possibilité d’activer l'alimentation PoE via l'interface d'administration.

Il est recommandé de l’utiliser avec un câble réseau de catégorie 5, spécialement conçu pour l’extérieur.

**Principales caractéristiques :**

- Réseau sans fil haut débit 802.11n
- Puissance de sortie jusqu’à 27 dBm +/-2dB
- Sensibilité en réception -96 dBm +/--2dB
- Antenne panneau jusqu’à 16 dBi à double polarisation intégrée (angle H/V 43°/41°)
- Fréquences : 4.9-5.9 GHz
- Technologie AAP (Adaptive Antenna Polarity) pour le choix automatique de la polarisation de l’antenne
- Température de fonctionnement extrême de -30° à +80°
- Plate-forme ouverte compatible avec d’autres firmwares
Watchdog soft et hard : redémarre automatiquement en cas de dysfonctionnement interne (ex. plantage après orage)
Facilité d'installation grâce à son alimentation PoE passif 24V, 0.5A (inclue)
Sécurité sans fil optimale grâce au cryptage WPA et WPA2
Chipset Atheros MIPS 24KC, 400MHz, 32Mo SDRAM, 8Mo Flash
Modes WiFi : Point d'accès, Client, Point d'accès + WDS, Client + WDS
Modes réseaux : Routeur, NAT, Client PPPoE, QoS, Serveur DHCP
Gestion de la bande passante (limitation en up et en down)
Indication du niveau de réception avec des diodes
Consommation max : 8W
Dimensions 29.4 cm x 8 cm x 3cm
Masse : 0,4 kg (hors accessoires)

Prix sur le marché = 89€ TTC / 74,41 € HT

CPE extérieur MikroTik RouterBoard SXT 5HnD

Le MikroTik RouterBoard SXT 5HnD est un CPE 5GHz spécialement conçu pour réaliser des liens point-à-point ou point-à-multipoint*. Ces antennes ont une double polarisation 802.11n avec la technologie Nv2 TDMA permettent d'atteindre un débit réel de 200 Mbps.

Désigné compact tout-en-un : installation facile et rapide
Compatible 802.11a/n
Antenne double polarité 16 dBi intégrée
LEDs d'indication de niveau de signal
Port USB 2.0 pour monitoring de tension et température

* le point-à-multipoint nécessite l'achat d'une licence RouterOS niveau 4.

**Principales caractéristiques :**

- Réseau sans fil haut débit 802.11 a/n
- Puissance de sortie jusqu'à 26 dBm +/-2dB
- Antenne panneau jusqu'à 16 dBi à double polarisation intégrée (angle H/V 25°/25°)
- Fréquences : 5.17-5.825 GHz
- Température de fonctionnement extrême de -30° à +80°
- Facilité d'installation grâce à son alimentation PoE passif 24V , 0.5A (inclue)
- OS : MikroTik RouterOS v4, licence Niveau3
- Indication du niveau de réception avec des diodes
- Consommation max : 7W
- Dimensions 140 cm x 140 cm x 56 cm
- Masse : 0,4 kg

**Prix sur le marché = 100,66€ TTC / 83,19 HT**
RouterBOARD 433UAHL

Cette carte dispose de trois emplacements miniPCI et de trois ports Ethernet. Elle est équipé d’un CPU Atheros cadencé à la vitesse de 680MHz, un slot pour carte microSD et deux ports USB 2.0, ce qui en fait le choix idéal universel pour les réseaux graves.

Les deux ports USB 2.0 peut être utilisé pour étendre le stockage, l’ajout d’un modem sans fil pour la connexion 3G de sauvegarde ou à une installation mobile, ou tous ensemble.

Principales caractéristiques :

- CPU speed 680MHz
- 1 Memory Cards
- RAM: 128MB
- Memory card type: microSD
- Architecture : MIPS-BE
- LAN ports: 3
MiniPCI : 3
USB : 2
PoE : 1 0-28V
Voltage Monitor : OUI
RouterOS License : Level5

Prix sur le marché = 140,53€ TTC / 117,50€ HT

**RouterBoard 433L**

Le RB433L dispose de trois emplacements miniPCI et trois ports Ethernet.

Trois ports vous donner beaucoup d'options de configuration pour de nombreux scénarios sans fil. Utilisez cet appareil dans une affaire en plein air pour une installation du secteur AP ou pour une liaison sans fil.
Il est propulsé par un processeur 300MHz et possède Atheros 64 Mo de RAM et une licence Niveau4 RouterOS.

**Principales caractéristiques :**

- CPU speed : Atheros AR7130 300MHZ
- RAM: 64MB
- LAN ports: 3
- MiniPCI : 3
- USB : 2
- PoE : 1 0-28V
- RouterOS License : Level4

**Prix sur le marché = 96,88 € TTC / 81 € HT**

**AntBox-56019-DP-MMCX**
ANT-BOX-56014-DP-MMCX intégré panneau 5GHz polarisation de l'antenne double dispose sommet de 14 dBi de gain et ROS faible <1,8

La glande à la base protège l'antenne de l'eau et de conditions météorologiques rigoureuses. Matériel de montage inclus

**Caractéristiques:**

- double polarisation
- Gain 14 dBi
- ROS <1,8
- 2x connecteurs RP-SMA
- 2x tresses MMCX

**Prix sur le marché** = 16,79 € TTC

Ces antennes peuvent accompagner les cartes RouterBOARD 433UAHL et 433L vu qu’elles sont dépourvues d’antennes.

b. **Equipements réseau**

En plus des équipements radio, nous avons eu à notre disposition des machines de la salle de travaux pratiques 212 du Bâtiment U2 de l’université et 2 switchs Cisco 3650.
Switchs 3650 Cisco

Salle de travaux pratiques

Grâce à ces ressources, nos travaux ont pu être effectués dans de bonnes conditions.

3. Outils de test

Ping

La commande ping permet d'envoyer une requête ICMP Echo d'un ordinateur à un autre pour tester si cet ordinateur hôte est accessible par le réseau;

Nous avons utilisé cette commande pour vérifier l'établissement d'une connexion entre des équipements.
Iperf

Iperf est un logiciel informatique permettant la mesure de différentes variables d'une connexion réseau IP par exemple la bande passante d'une liaison. Il est basé sur une architecture client/serveur et disponible sur différents systèmes d'exploitation.

Iperf nous a été utile pour les tests de performances.

Wireshark

Wireshark est un analyseur de paquets libre utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles.

4. Stockage des fichiers

Le wiki Chiliproject sert également de stockage des fichiers que nous souhaitons partager avec nos tuteurs.

Exemple de fichiers du wiki

Nous avons aussi utilisé le stockage en ligne Dropbox. Ceci nous a permis d'avoir nos fichiers personnels à tout moment et n'importe où et ce de manière sécurisée. Son contenu est juste disponible pour les stagiaires. Il nous a permis de préparer de préparer les documents avant leur upload sur le wiki.

IV. TRAVAUX REALISES

1. Rappels

L'architecture du modèle de référence d'interconnexion des systèmes ouverts (ou modèle de référence OSI) est hiérarchisée en sept couches. Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de constructeurs différents.
Les 2 couches qui vont nous intéresser dans ce projet sont :

- La **couche liaison** de données fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités du réseau. Elle détecte et corrige, si possible, les erreurs dûes au support physique et signale à la couche réseau les erreurs irrécupérables. Elle supervise le fonctionnement de la transmission et définit la structure syntaxique des messages, la manière d'enchaîner les échanges selon un protocole normalisé ou non.

- La **couche réseau** assure toutes les fonctionnalités de relai et d'amélioration de services entre entité de réseau, à savoir : l'adressage, le routage, le contrôle de flux et la détection et correction d'erreurs non réglées par la couche 2.
2. Documentation

Au début du projet, nous nous sommes beaucoup focalisés sur des recherches d’informations pour la bonne prise en main de l’étude.

Ces recherches se sont articulées sur les travaux effectués auparavant par des membres de l’association et disponibles dans leur wiki (voir liens en annexes).

Nous avons aussi recueilli des informations sur les forums, des tutoriels et sur les sites constructeurs notamment ceux de Mikrokit et Ubiquity.

3. Familiarisation avec les équipements

La familiarisation avec les équipements nous a permis de découvrir l’installation des équipements, la mise à jour et l’administration.

Les équipements sont alimentés en POE ( issu de la norme IEEE 802.3af ), technologie permettant de véhiculer des données et l’alimentation électrique dans le même câble Ethernet. Ceci est utile et est souvent utilisé dans des zones dépourvues de prise électrique.

a. Installation

Introduire un fil sur le connecteur marqué Main.

Ensuite brancher l’adaptateur sur un courant secteur et raccorder l’autre bout du fil sur le connecteur où est inscrit POE.
Brancher un autre fil sur le connecteur de l’adaptateur LAN et brancher l’autre bout directement au niveau de la carte réseau d’une machine ou un port lan d’un hub ou le port WLAN d’un routeur (avec ou sans fil).
Pour notre cas, ce sera la carte réseau d’une machine.

Les LEDs power et lan devraient s’allumer si tout fonctionne bien pour les NanoStation comme sur l’image suivante :
Contrairement aux NanoStation Ubiquity, les antennes Mikrotik eux ne présentent pas ces leds confirmant le bon câblage de l’équipement. Seul un bruit sonore se faire entendre.

b. Configuration

NanoStation Ubiquity

Les adresses par défaut des antennes sont 192.168.1.20/24. Pour relier cette antenne à une machine, il faut que cette dernière soit dans le même réseau que l’antenne. Donc, il faut choisir une adresse IP 192.168.1.X/24 avec X différente de 20 car elle est déjà attribuée à l’antenne sinon il risque d’y avoir des conflits d’adresses.

Mikrotik

Les adresses par défaut des antennes sont 192.168.88.1/24. Pour relier cette antenne à une machine, il faut que cette dernière soit dans le même réseau que l’antenne. Donc, il faut choisir une adresse IP 192.168.88.X/24 avec X différente de 1 car elle est déjà attribuée à l’antenne sinon il risque d’y avoir des conflits d’adresses.

Une fois cette configuration effectuée, la machine pourra accéder à l’interface web d’administration de l’antenne.

c. Interface d’administration Web:

Ubiquity
Chacune des pages web de gestion (ci-dessous) contient des paramètres qui affectent un aspect spécifique de l'appareil:

**MAIN**

Il affiche l’état actuel de l’appareil et les informations statistiques

**WIRELESS**

Cette page contient les commandes pour la configuration du réseau sans fil, tout en couvrant les paramètres de base sans fil qui définissent le mode de fonctionnement (Point d’accès ou Station simple), la puissance de sortie, associant les détails et les options de sécurité des données.

**NETWORK**

Elle couvre la configuration du mode de fonctionnement du réseau, les paramètres IP, les paramètres de filtrage de paquets et les services réseau (par exemple un serveur DHCP).

**ADVANCED**

Cette page contient des paramètres qui sont dédiés à la commande sans fil d’interface plus précis. Il comprend également la polarité antenne, régulation de trafic et les paramètres de qualité de service.

**SERVICES**

Cette page décrit la configuration des services de gestion du système (c.-à-SNMP, NTP, Journal du système, chien de garde Ping et SSH / Telnet du serveur).

**SYSTEME**

Cette page contient des contrôles pour les paramètres de maintenance du système, la gestion du compte administrateur, la personnalisation du dispositif, la langue d’interface, la mise à jour du firmware, et de sauvegardes de configurations.
Mikrokit

L’interface web est à peu près similaire à celle d’Ubiquity mais présente l’avantage d’avoir plus d’options et de fonctionnalités. Contrairement à Ubiquity, il existe différents modes de configuration possibles pour la station.

**Mode Station**

Il s’agit du mode standard qui ne prend pas en charge la liaison de niveau 2. Ainsi, une tentative de mettre un pont ne produira pas les résultats escomptés. D’autre part, ce mode peut être considéré comme le plus efficace et ne devrait donc être utilisée que si le pont L2 station n’est pas nécessaire comme dans le cas du réseau routé ou MPLS. Ce mode est supporté par tous les protocoles sans fil.

**Mode Station Bridge**

Ce mode fonctionne uniquement avec des points d'accès RouterOS et fournit un support pour transparent indépendante du protocole de liaison L2 sur le périphérique station. Le point d'accès(AP) RouterOS accepte des clients dans le mode station bridge lorsqu'ils ont activé leur mode bridge dans leur paramétrage. Dans ce mode de transmission l'AP maintient une table avec des informations sur les adresses MAC accessibles.

Ce mode est propriétaire et ne peut pas être utilisé pour connecter des appareils d'autres marques. Ce mode permet d’utiliser un pont de niveau 2.
**Mode station-pseudobridge**

Ce mode de connexion sans fil du point de vue est le même que le mode de station standard. Il a un support limité pour pont L2 par l'intermédiaire de certains services mis en place dans la station:

- Traduction d'adresses MAC pour les paquets IPv4 - station conserve table de mappage IPv4-to-MAC et remplace adresse MAC source avec sa propre adresse lors de l'envoi cadre d'AP (afin d'être en mesure d'utiliser 3 format de trame adresse), et remplace adresse MAC de destination avec adresse de table de mappage pour les trames reçues de l'AP. IPv4-to-MAC mappages sont construits également pour le VLAN des trames encapsulé.
- simple traduction d'adresse MAC pour le reste de protocoles - station apprend adresse MAC source de la première transmis non IPv4 cadre et l'utilise comme valeur par défaut pour la traduction inverse - l'adresse MAC est utilisé pour remplacer l'adresse MAC de destination pour les trames reçues de l'AP si IPv4 à -MAC mappage ne peut pas être exécutée (par exemple - non-IPv4 cadre ou la cartographie manquant).

Ce mode est disponible pour tous les protocoles sauf NV2 et doit être évitée autant que possible.

**Mode de station-pseudobridge-clone**

Ce mode est le même que la station-pseudobridge mode, sauf qu'il se connecte au point d’accès "cloné" adresse MAC qui est soit l'adresse configurée dans les paramètre de la station-clone-mac (s'il est configuré) ou l'adresse source de la première trame transmise. Cela semble essentiellement sur le point d'accès comme si l'appareil de l'utilisateur final est relié au poste connecté au point d'accès.

**Mode station-wds**

Ce mode fonctionne uniquement avec des points d'accès RouterOS. À la suite de la négociation de connexion, une interface WDS séparée est créée sur l'AP pour la station donnée. Cette interface peut être considérée comme point-à-point entre AP et la station donnée. Tout ce qui est envoyé sur l'interface WDS est livré à la station (et seulement à station en particulier) et quelle que soit la station envoie à l'AP WDS est reçu de l’interface WDS.

Ce mode est supporté pour tous les protocoles sans fil, sauf lorsque le protocole 802.11 est utilisé dans le cadre de la non utilisation de dispositif RouterOS. Le mode utilise une trame de 4 adresses lorsqu'il est utilisé avec protocole 802.11, pour les autres protocoles (comme nstreme ou NV2), le protocole interne est utilisé.
Ce mode utilise le pont de niveau 2 et permet un contrôle plus administratif sur le point d'accès par l'intermédiaire de l'interface WDS séparée, par exemple l'utilisation d'un pont pare-feu, RSTP pour détecter et éviter les boucles.

La configuration de la station doit respecter la matrice d’applicabilité des protocoles sans fil ci-dessus :

<table>
<thead>
<tr>
<th></th>
<th>802.11</th>
<th>ROS 802.11</th>
<th>nstreme</th>
<th>nv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>station</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-wds</td>
<td>V</td>
<td></td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-pseudobridge</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>station-pseudobridge-clone</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>station-bridge</td>
<td>V</td>
<td></td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>

**Matrice d’applicabilité des protocoles sans fil**
4. **Tests et améliorations de performances**

a. **Entre 2 Ubiquity NanoStation M5**

**Architecture réseau et adressage équipements**

Tous les équipements appartiennent au même réseau 192.168.1.0/24. Les antennes sont configurés en mode bridge pour assurer la transition entre le lien Ethernet et radio.

**NB : Cette même architecture sera déployée par la suite pour les tests des autres antennes.**

Pour tester les débits, nous allons utiliser **iperf** de bout en bout au niveau des 2 postes de travail. Il nous permet de mesurer la bande passante et d’évaluer la qualité du lien réseau.
Nous avons fait les tests en disposant les antennes sur une distance d’environ 2 mètres.

Configuration :

- **Point d’accès**
1 : Antenne configurée en Point d'accès.

2 : Station raccordée au point d'accès

### Station

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Name client</th>
<th>Network Mode</th>
<th>Wireless Mode</th>
<th>AP MAC</th>
<th>Signal Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Bridge</td>
<td>Station</td>
<td>DC:8F:DB:2F:24:4F</td>
<td><img src="image" alt="Signal Strength" /></td>
</tr>
</tbody>
</table>

- Channel/Frequency: 64 / 5220 MHz
- Channel Width: 40 MHz (Lower)
- Distance: 0.1 mile (0.2 km)
- TX/RX: 2x2
- WLAN MAC: DC:8F:DB:2F:24:64
- LAN0 MAC: DC:8F:DB:2F:12:64
- LAN1 MAC: DC:8F:DB:2F:24:64
- LAN0/LAN1: 1000Mbps Full Unplugged

3 : Antenne configurée en mode Station

4 : Connexion au point d'accès établie

**Test de la bande passante**

Nous avons mis en place utilisé l’outil intégré Speedtest pour mesurer la bande passante entre les 2 antennes.
Résultat du Speedtest

Le débit que nous obtenons avoisine les **150 Mbits/s** correspondant à une bonne qualité de liaison.

L’activation AIRMAX n’influe en rien sur le débit mais il est conseillé de l’activer **uniquement** entre des équipements de type Ubiquity.

**Important :** L’activation d’Airmax empêche à l’antenne de se connecter avec une antenne d’un autre constructeur. Il est juste recommandé de l’activer entre des équipements Ubiquity.

La technologie AIRMAX est issue du développement du WIFI 802.11an et utilise une technologie TDMA (Time Division Multiple Access) qui permet de transmettre plusieurs signaux sur un seul canal. Par ce moyen, une fréquence peut être utilisée par plusieurs abonnés simultanément. En d'autre terme, la technologie AIRMAX est l'alliance des technologies MIMO issues des développements 802.11n du WIFI et de la norme TDMA (en remplacement du CSMA/CA du WIFI).

Pour augmenter les performances, nous avons pensé à réduire les puissances d’émission des antennes à leur plus basse valeur (-4dbm) vu que les antennes sont proches de 2 mètres.
Synthèse :

- **Station**
  - Bande de fréquence 20/40 Mhz
  - Désactivation de AirMax
  - Puissance d’émission réduite -4dBm

- **Point d’accès**
  - Bande de fréquence 40 Mhz
  - Débit relevé 148 Mbits/s
  - Activation de AirMax
  - Débit relevé 145 Mbits/s

b. **Entre 2 Mikrotik CPE SXT**

- **Lien ethernet**
  - IP: 192.168.1.1
  - IP: 192.168.1.2

- **Lien radio**
  - IP: 192.168.1.22
  - IP: 192.168.1.23

**Architecture réseau et adressage équipements**
Configuration :

Nous n'avons pas eu activé la fonction Point d’accès à cause d’un niveau de licence insuffisant. Le niveau de licence est de 3 alors qu’il est possible de mettre en place un point d’accès à partir du niveau 4 qui est tarifié à 45 $. 

<table>
<thead>
<tr>
<th>Software ID</th>
<th>Z4RL-DHV.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgradable To</td>
<td>y7.x</td>
</tr>
<tr>
<td>Level</td>
<td>3</td>
</tr>
<tr>
<td>Features</td>
<td>extra-channels</td>
</tr>
<tr>
<td>Expires In</td>
<td></td>
</tr>
</tbody>
</table>

Niveau de License actuel

Couldn't change Interface <wlan1-gateway> - license does not allow AP mode (6)

Message d’erreur lors d’une tentative d’activation de la fonction AP (Point d’accès)
Niveaux de licence des équipements Mikrotik

Donc, il n’est possible de faire que du **point à point** en mode bridge entre ces deux équipements. Ce qui n’est pas avantageux.

**Bridge**

Configuration en mode bridge avec la fréquence fixée à 5180 Mhz.

```
Mode: bridge
Band: 5GHz-AN
Channel Width: 20/40MHz HT Above
Frequency: 5180 MHz
SSID: Mikrotik
Scan List: default
Wireless Protocol: 802.11
Security Profile: default
Bridge Mode: enabled
```

**Station**

Nous avons procédé à plusieurs tests en modifiant le mode de la station (station simple, station bridge, station WDS...) tout en respectant leur compatibilité des protocoles sans fil (cf matrice d’applicabilité des protocoles sans fil)
Test de la bande passante

Voici les résultats de débits obtenus avec l’outil intégré Bandwidth Test entre les deux stations en TCP et UDP:
### Résultat du test de bande passante en TCP

<table>
<thead>
<tr>
<th>Test To</th>
<th>192.168.1.22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>tcp</td>
</tr>
<tr>
<td>Local UDP Tx Size</td>
<td>1500</td>
</tr>
<tr>
<td>Remote UDP Tx Size</td>
<td>1500</td>
</tr>
<tr>
<td>Direction</td>
<td>receive</td>
</tr>
<tr>
<td>TCP Connection Count</td>
<td>20</td>
</tr>
<tr>
<td>Local Tx Speed</td>
<td></td>
</tr>
<tr>
<td>Remote Tx Speed</td>
<td></td>
</tr>
<tr>
<td>Random Data</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>***</td>
</tr>
</tbody>
</table>

| Lost Packets | 0            |
| Tx/Rx Current | 0 bps/42.8 Kbps |
| Tx/Rx 10s Average | 0 bps/40.7 Kbps |
| Tx/Rx Total Average | 0 bps/31.0 Kbps |
On constate un bon débit (supérieur à 100 Mbits/s) en UDP avec des pertes de paquets considérables (1861 paquets) ce qui explique les faible obtenu en TCP. Cela peut être dû à la réfraction et à la réflexion des antennes dans la salle ou nous avons effectué les tests.

**Remarque:**

Le mode station permet la connexion avec l’antenne en mode bridge. Cependant, nous avons remarqué qu’on pouvait plus aller au-delà de l’antenne c’est-à-dire que les 2 postes de travail ne peuvent plus communiquer.
Ceci est dû au fait qu’il ne prend pas en compte le niveau 2 (Liaison).

**Synthèse :**

<table>
<thead>
<tr>
<th>Station</th>
<th>Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bande de fréquence 20/40 Mhz</td>
<td></td>
</tr>
<tr>
<td>Fréquence fixée à 5180 Mhz</td>
<td></td>
</tr>
<tr>
<td>Débit relevé en TCP = 40 Mbits/s</td>
<td></td>
</tr>
<tr>
<td>Débit relevé en UDP &gt; 100 Mbits/s</td>
<td></td>
</tr>
</tbody>
</table>
c. Entre Mikrotik 433L et 433UAHL

**Architecture réseau et adressage équipements**

![Network Architecture Diagram](image)

**Configuration :**

Nous avons configuré une carte en AP et une autre en station vice versa en variant les différents types de stations possibles

**Test de la bande passante**

On retrouve des résultats similaires aux tests entres mikrotik SXT car ils sont issus du même constructeur.
Voici les résultats de débits obtenus avec l'outil intégré **Bandwidth Test** entre les deux stations en TCP et UDP:

<table>
<thead>
<tr>
<th><strong>Test To</strong></th>
<th>192.168.1.24</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
<td>tcp</td>
</tr>
<tr>
<td><strong>Local UDP Tx Size</strong></td>
<td>1500</td>
</tr>
<tr>
<td><strong>Remote UDP Tx Size</strong></td>
<td>1500</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>receive</td>
</tr>
<tr>
<td><strong>TCP Connection Count</strong></td>
<td>20</td>
</tr>
</tbody>
</table>

- **Lost Packets**: 0
- **Tx/Rx Current**: 0 bps/57.8 Mbps
- **Tx/Rx 10s Average**: 0 bps/53.7 Mbps
- **Tx/Rx Total Average**: 0 bps/46.5 Mbps

**Résultat du test de bande passante en TCP**
### Résultat du test de bande passante en UDP

**Test To**: 192.168.1.24  
**Protocol**: udp  
**Local UDP Tx Size**: 1500  
**Remote UDP Tx Size**: 1500  
**Direction**: receive  
**TCP Connection Count**: 20

- **Local Tx Speed**:  
- **Remote Tx Speed**:  
- **Random Data**:  
- **User**: admin  
- **Password**: •••••  
- **Lost Packets**: 1656  
- **Tx/Rx Current**: 0 bps/109.7 Mbps  
- **Tx/Rx 10s Average**: 0 bps/110.3 Mbps  
- **Tx/Rx Total Average**: 0 bps/95.5 Mbps

![Graph]

---

**Graph**

<table>
<thead>
<tr>
<th>Speed</th>
<th>2 min ago</th>
<th>1 min ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>500.0 Mbps</td>
<td>![Graph Data]</td>
<td>![Graph Data]</td>
</tr>
<tr>
<td>400.0 Mbps</td>
<td>![Graph Data]</td>
<td>![Graph Data]</td>
</tr>
<tr>
<td>300.0 Mbps</td>
<td>![Graph Data]</td>
<td>![Graph Data]</td>
</tr>
<tr>
<td>200.0 Mbps</td>
<td>![Graph Data]</td>
<td>![Graph Data]</td>
</tr>
<tr>
<td>100.0 Mbps</td>
<td>![Graph Data]</td>
<td>![Graph Data]</td>
</tr>
</tbody>
</table>

**Legend**:  
- **Tx**: cur: 109.7 Mbps  
- **Rx**: cur: 95.5 Mbps  
- **avg:** max:
  - **max**: 113.5 Mbps
 Synthèse :

<table>
<thead>
<tr>
<th>Station</th>
<th>Point d’accès</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bande de fréquence 20/40 Mhz</td>
<td>Bande de fréquence 20/40 Mhz</td>
</tr>
<tr>
<td>Fréquence fixée à 5180 Mhz</td>
<td>Fréquence fixée à 5180 Mhz</td>
</tr>
<tr>
<td>Débit relevé en TCP ≈ 57,8 Mbits/s</td>
<td>Débit relevé en TCP ≈ 57,8 Mbits/s</td>
</tr>
<tr>
<td>Débit relevé en UDP &gt; 100 Mbits/s</td>
<td>Débit relevé en UDP &gt; 100 Mbits/s</td>
</tr>
</tbody>
</table>

d. Entre NanoStation Ubiquity et Mikrotik CPE SXT

Architecture réseau et adressage équipements
Configuration :

Etant donné que la fonctionnalité Point d’accès n’est pas disponible pour les antennes Mikrotik sxt, nous avons mis une antenne Mikrotik sxt en mode station et une autre antenne Ubiquity en mode Point d’accès.

Pour la configuration, voir configurations point d’accès Nanostation et Station Mikrokit SXT détaillées antérieurement.

Test de la bande passante

Station

Comme expliqué précédemment cette option ne gère pas le niveau 2 donc nous avons pas eu de lien entre les 2 postes de travail donc pas test de débit possible.

Station bridge

Cette option est propriétaire. Elle ne fonctionne qu’avec l’« écosystème mikrotik » or ici nous avons un point d’accès nanostation donc il est impossible d’avoir une interopérabilité avec ce mode.

Station wds

Ce mode ne fonctionne qu’avec les points d’accès de routerOs ce qui explique la non comptabilité avec l’antenne nanostation M5.
Station pseudobridge et pseudobridge clone

Voici les résultats obtenus en TCP:

Commandes iPerf :

Coté serveur : iperf –s

Coté client : iperf –c 192.168.1.1 –i 1

Ces commandes nous permettent d’avoir une estimation de la basse passante à des intervalles réguliers d’une seconde.

Client connecting to 192.168.1.1, TCP port 5001
TCP window size: 23.5 KByte (default)

| [ 3] local 192.168.1.2 port 58670 connected with 192.168.1.1 port 5001 |
| ID | Interval       | Transfer     | Bandwidth |
| [ 3] 0.0- 1.0 sec 6.62 MBytes 55.6 Mbits/sec |
| [ 3] 1.0- 2.0 sec 10.5 MBytes 88.1 Mbits/sec |
| [ 3] 2.0- 3.0 sec 9.00 MBytes 75.5 Mbits/sec |
| [ 3] 3.0- 4.0 sec 9.62 MBytes 80.7 Mbits/sec |
| [ 3] 4.0- 5.0 sec 9.75 MBytes 81.8 Mbits/sec |
| [ 3] 5.0- 6.0 sec 9.62 MBytes 80.7 Mbits/sec |
| [ 3] 6.0- 7.0 sec 9.00 MBytes 75.5 Mbits/sec |
| [ 3] 8.0- 9.0 sec 9.75 MBytes 81.8 Mbits/sec |
| [ 3] 9.0-10.0 sec 8.88 MBytes 74.4 Mbits/sec |
| [ 3] 0.0-10.1 sec 92.5 MBytes 77.2 Mbits/sec |

Le débit moyen est d’environ 75 Mbits/s

Voici les résultats obtenus en UDP :

Commandes iPerf :

Coté serveur : iperf –s –u –i 1

Coté client : iperf –c 192.168.1.1 –i -b 100M –i 1

Ces commandes nous permettent d’avoir une estimation de la basse passante avec un débit souhaité à 100 Mbits/s à des intervalles réguliers d’une seconde.

Client connecting to 192.168.1.1, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 224 KByte (default)

| [ 3] local 192.168.1.2 port 48037 connected with 192.168.1.1 port 5001 |
| ID | Interval | Transfer     | Bandwidth |
| [ 3] 0.0- 1.0 sec 11.5 MBytes 96.7 Mbits/sec |
Le débit moyen est d’environ 86,3 Mbits/s.

**Synthèse:**

<table>
<thead>
<tr>
<th>Station pseudobrigde/ pseudobrigde clone</th>
<th>Point d’accès</th>
</tr>
</thead>
<tbody>
<tr>
<td>Débit relevé en UDP environ 86 Mbits</td>
<td></td>
</tr>
<tr>
<td>Débit relevé en TCP environ 75 Mbits</td>
<td></td>
</tr>
<tr>
<td>Station WDS/Station brigde</td>
<td>Point d’accès</td>
</tr>
<tr>
<td>Incompatible</td>
<td></td>
</tr>
<tr>
<td>Station</td>
<td>Point d’accès</td>
</tr>
<tr>
<td>Niveau 2 non géré</td>
<td></td>
</tr>
</tbody>
</table>

Nous estimons que le débit est satisfaisant entre les deux équipements mais que les modes accessibles sont restreints à cause des constructeurs différents.
e. Entre NanoStation Ubiquity et Mikrotik 433 UAHL/433L

Architecture réseau et adressage équipements

Configuration :

Etant donné que la fonctionnalité Point d’accès est disponible pour les cartes Mikrotik (433UAHL et 433L), nous avons mis une carte Mikrotik en mode Point d’accès et une autre antenne Ubiquity en mode station et vice versa.
Pour la configuration, voir configurations point d’accès Nanostation et Station Mikrokit SXT détaillées antérieurement.

**Test de la bande passante**

*Station pseudobridge et pseudobridge clone*

*Voici les résultats obtenus en TCP:*

**Commandes iperf :**

Côté serveur : `iperf –s`

Côté client : `iperf –c 192.168.1.1 –i 1`

Ces commandes nous permettent d’avoir une estimation de la basse passante à des intervalles réguliers d’une seconde.

Nous retrouvons des résultats similaires aux tests entre Ubiquity nano M5 et MiKrotik SXT 5HND

*Voici les résultats obtenus en UDP:*

**Commandes iperf :**

Côté serveur : `iperf –s –u –i 1`

Côté client : `iperf –c 192.168.1.1 –i –b 100M –i 1`

Ces commandes nous permettent d’avoir une estimation de la basse passante avec un débit souhaité à 100 Mbits/s à des intervalles réguliers d’une seconde.

Nous retrouvons des résultats similaires aux tests entre Ubiquity nano M5 et MiKrotik SXT 5HND
**Synthèse :**

<table>
<thead>
<tr>
<th>Station pseudobrigde/ pseudobrigde clone</th>
<th>Point d’accès</th>
</tr>
</thead>
<tbody>
<tr>
<td>Débit relevé en UDP environ Mbits</td>
<td></td>
</tr>
<tr>
<td>Débit relevé en TCP environ Mbits</td>
<td></td>
</tr>
<tr>
<td><strong>Station WDS/Station brigde</strong></td>
<td><strong>Point d’accès</strong></td>
</tr>
<tr>
<td>Incompatible</td>
<td></td>
</tr>
<tr>
<td><strong>Station</strong></td>
<td><strong>Point d’accès</strong></td>
</tr>
<tr>
<td><strong>Niveau 2 non géré</strong></td>
<td></td>
</tr>
</tbody>
</table>

**5. Etude sur le protocole STP**

Les réseaux commutés de type Ethernet doivent avoir un chemin unique entre deux points, cela s'appelle une topologie sans boucle. En effet, la présence de boucle génère des tempêtes de diffusion qui paralysent le réseau : tous les liens sont saturés de trames de diffusion qui tournent en rond dans les boucles et les tables d'apprentissage des commutateurs deviennent instables.

Une solution serait de ne pas tirer les câbles en surnombre de manière à ne pas avoir de boucles dans le réseau. Néanmoins, un bon réseau doit aussi offrir de la redondance pour proposer un chemin alternatif en cas de panne d’une liaison ou d’un commutateur.

L'algorithme de « *spanning tree minimum* » garantit l’unicité du chemin entre deux points du réseau tout en n’interdisant pas les câbles en surnombre. Pour cela, il bloque administrativement certains ports des commutateurs (ponts).

Le *Spanning Tree Protocol* (algorithme de l’arbre recouvrant, aussi appelé *STP*) est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau *sans boucle* (appelée arbre) dans les LAN avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985.
Le but de ce travail pratique suivant est d’abord de mettre en œuvre le protocole STP au sein des antennes. Ce protocole permet de détecter et de désactiver les boucles de réseau. Nous allons aussi faire participer les antennes à l’élection du commutateur racine (root). Nous observerons également les changements lors des modifications de la topologie.

a. Architecture

Notre réseau est constitué de :

- 2 postes de travail d’adresses IP 192.168.1.1/24 et 192.168.1.2/24
- 2 Switchs Cisco 3950
- 2 antennes. Nous allons, tour à tour, placer les antennes NanoStation et Mikrotik.

Les 2 postes de travail peuvent communiquer via le lien filaire et le lien radio. Ils nous permettront de voir d’analyser la communication suite à un changement de la topologie réseau.

Cette architecture nous permettra de faire participer les antennes à l’élection du commutateur racine.
b. Configuration des switchs Cisco 3950

Tout d’abord, nous avons réinitialisé la configuration des Switchs sur leurs paramètres d’origine.

<table>
<thead>
<tr>
<th>Equipement</th>
<th>Port</th>
<th>Equipement</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1</td>
<td>FastEthernet 0/1</td>
<td>PC2</td>
<td>FastEthernet 0/1</td>
</tr>
<tr>
<td>Antenne 1</td>
<td>FastEthernet 0/2</td>
<td>Antenne 2</td>
<td>FastEthernet 0/2</td>
</tr>
<tr>
<td>Trunk (lien filaire)</td>
<td>FastEthernet 0/11</td>
<td>Trunk (lien filaire)</td>
<td>FastEthernet 0/11</td>
</tr>
</tbody>
</table>

Les 2 Switchs sont configurés de la même manière.

Un trunk est établi entre les 2 Switchs pour permettre la communication entre les 2 machines sur le lien filaire à travers la commande suivante :

```
sw1#conf t
sw1(conf-if)# int fa0/11
sw1(conf-if)#switchport mode trunk
An interface whose trunk encapsulation is Auto can not be configured to trunk mode
sw1(conf-if)#switchport trunk encapsulation dot1q
sw1(conf-if)#switchport mode trunk
```

Mise en place du trunk sur l’interface FastEthernet 0/11
au niveau des 2 Switchs

c. Activation du protocole Spanning Tree

Par défaut, cette fonctionnalité est activée nativement sur les équipements Cisco. Cependant, nous aurions pu le faire à travers la commande suivante si ce n’était pas le cas :

```
sw1#conf t
sw1(config)#spanning-tree vlan 1
sw1(config)#spanning-tree mode pvst
sw1(config)#exit
```

Nous venons d’activer le protocole STP sur le VLAN 1 par défaut où nous travaillons (antenne, poste de travail, trunk).

d. Installation des antennes NanoStation et Observations
Pour nos premières observations, nous avons placé des antennes NanoStation M5.

- Antenne 1 = NanoStation M5
- Antenne 2 = NanoStation M5

Les 2 antennes sont configurées en **Station** et **Point d’accès**. Le bridge permettant de faire le lien entre le réseau filaire et le réseau radio est le bridge0 (bridge par défaut). Pour activer le protocole STP sur ce dernier, il suffit de cocher la case STP (Aller dans l’onglet **Network** ➔ Changer le mode configuration de **Simple** à **Avancé** ➔ Accéder à la partie **Bridge Network** et cocher la case STP).

**Inconvénient** : Nous n’avons pas trop d’options sur le protocole STP avec les NanoStation en configuration graphique par exemple la priorité qui est fondamentale pour l’élection du commutateur racine. Malgré les recherches qui ont été effectuées, nous n’avons pas pu trouver un moyen pour extraire la priorité même en ligne de commande.

Ceci ne nous permet pas de faire participer les antennes NanoStation à l’élection du commutateur racine.
**Supposition** : Par la suite, nous avons supposé que la priorité est égale à **32768** (0x8000 en hexadécimal). Cette priorité est la priorité par défaut connu pour plusieurs équipements.

Les priorités des switchs Cisco sont à **32768**.

**Principe de fonctionnement du protocole STP** : Le commutateur avec la priorité la plus basse l'emporte, et en cas d'égalité, c'est l'adresse MAC la plus basse qui l'emporte.

Dans notre cas, tous les équipements ont la même priorité. L'élection du commutateur racine s'effectue sur l'équipement avec la plus petite adresse MAC.

Voici les adresses MAC de nos équipements :

Switch 1: **00:23:34:15:12:80**

Switch 2: **00:26:ca:a4:24:00**

NanoStation 1: **dc:9f:db:2f:f2:4f**

NanoStation 2: **dc:9f:db:2e:f2:64**

Nous constatons que le switch 1 a la plus petite adresse MAC (**00:23:34:15:12:80**) et doit normalement être élu commutateur racine.

**Vérification** :

```
sw1#sh spanning-tree

VLAN0001
Spanning tree enabled protocol iscc
Root ID 5276B
Priority 32768
Address 0023.3415.1280
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32768 (priority 32768 sys-id-ext 1)
Address 0023.3415.1280
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15 sec

Interface Role Sts Cost Frio.Nbr Type
------------------ --- ---- ----------
Fa0/1 Desg FWD 19 128.3 P2p
Fa0/2 Desg FWD 19 128.4 P2p
Fa0/11 Desg LRN 19 128.19 P2p
```

**Informations STP sur le switch 1**
Le switch 1 est bien le commutateur racine.

Les informations STP sur le switch 2 confirment bien que le switch 1 est le commutateur racine. Par ailleurs, nous en déduisons que le lien filaire est privilégié par rapport au lien radio des antennes car l’interface FastEthernet 0/11 joue le rôle de Root (voir configuration des Switchs et architecture réseau plus haut pour plus de compréhension).
Modification de la topologie

Jusque là, la communication entre les 2 postes de travail est fonctionnelle et passe par le trunk (lien filaire).

Nous allons forcer le trafic à passer par le lien radio c’est -à-dire le bridge STP établi entre les 2 antennes et voir la réaction des équipements. Pour ce faire, nous allons désactiver l’interface fa0/11 sur le switch 1 et évaluer le temps nécessaire pour le rétablissement de la communication entre les 2 postes de travail.

```
sw1#conf t
sw1(conf-if)# int fa0/11
sw1(conf-if)#shutdown
```

Désactivation de l’interface fa 0/11

Observations

Pour l’observation des événements STP au niveau des switchs, il est nécessaire d’utiliser la commande suivante :

```
sv2#debug spanning-tree events
Spanning Tree event debugging is on
```

Activation de l’affichage des événements STP

Au niveau du switch 2, nous avons reçu le message suivant indiquant que l’interface FastEthernet 0/2 sur lequel est connecté le lien radio devient prioritaire :
Avant de désactiver l’interface FastEthernet 0/11, nous avions lancé un ping entre les 2 postes de travail 192.168.1.1/24 et 192.168.1.2/24. Nous avons évalué le temps nécessaire au rétablissement du lien entre les 2 postes de travail suite à la désactivation de l’interface FastEthernet 0/11.

### Evaluation du temps de rétablissement

Pour évaluer le temps nécessaire au rétablissement du lien suite à la désactivation du lien entre les 2 Switchs, nous avons utilisé Wireshark pour recueillir les résultats du ping. Un filtrage sur la réponse du ping (réponse echo de type 0) nous permet d’être plus précis sur la durée de rétablissement du lien entre les 2 postes de travail.

#### Filtrage de la réponse ICMP suite au ping

![Filtrage de la réponse ICMP suite au ping](image)

- **Avant interruption du lien entre les 2 switchs**
- **Interruption du lien**
- **Rétablissement du lien**

---

Kassé- Sall  
TER Interconnexion réseaux radio  
Page 55/89
Nous constatons que l’interruption du lien s’est effectuée au bout d’un temps $t_1 = 11$ secondes et que le rétablissement s’est effectué au bout d’un temps $t_2 = 59$ secondes.

$t_1 - t_2 = 59$ secondes $- 11$ secondes $= 48$ secondes

Donc, il a fallu 48 secondes pour que le lien soit établi de nouveau entre les postes de travail, ce qui est non négligeable.

e. Installation des antennes Mikrokit et Observations

Après avoir travaillé avec les antennes NanoStation, nous allons maintenant refaire les mêmes tests sur les antennes Mikrotik.

- Antenne 1 = Mikrotik SXT 5Hnd
- Antenne 2 = Mikrotik SXT 5Hnd

Les 2 antennes sont configurées en Station bridge et Bridge. Le bridge permettant de faire le lien entre le réseau filaire et le réseau radio est le bridge1 (bridge par défaut). Pour activer le protocole STP sur ce dernier, il suffit de cocher la case STP (Aller dans l’onglet Bridge ➔ Double clic sur le bridge1 ➔ Modifier le mode de protocole du bridge à STP).
**Avantage des équipements Mikrotik** : L'avantage que présentent les antennes Mikrotik par rapport aux NanoStation est qu'il est possible de modifier la priorité du bridge. Par défaut, elle est fixée à 32768 (8000 en hexadécimal).

![Bridge configuration table](image)

Ce tableau montre les paramètres du bridge avec le nom `bridge1`, le type `Bridge`, la taille de la MTU `1500`, la taille de la L2 MTU `65535`, et l'adresse MAC `00:0c:42:f2:ac:a0`.

Cette possibilité de pouvoir modifier la priorité est utile dans la mesure où elle permet à un administrateur du réseau de s'influencer le résultat de l'élection pour que le commutateur racine soit choisi le plus près possible du cœur de réseau. Pour cela, il configure la priorité du commutateur racine le plus opportun en fonction de la topologie du réseau, ainsi que la priorité d'un autre commutateur qui deviendra commutateur racine en cas de défaillance du commutateur racine principal.

Vu que les switchs Cisco et les antennes Mikrotik ont les mêmes priorités de bridge (32768), l'élection du commutateur racine s'effectuera sur l'équipement avec la plus petite adresse MAC.

**Switch 1** : 00:23:34:15:12:80
**Switch 2** : 00:26:ca:a4:24:00
**Mikrotik SXT 1** : 00:0c:42:f2:ac:a0
**Mikrotik SXT 2** : 00:0c:42:f1:af:83
Nous constatons que l’antenne Mikrotik SXT 2 a la plus petite adresse MAC (00:0c:42:af:83) et doit normalement être élu commutateur racine.

Vérification :

Afficher spanning-tree

<table>
<thead>
<tr>
<th>VLAN0001</th>
<th>Spanning tree enabled protocol ieee</th>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Cost</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>32768</td>
<td>00:0c:42:af:83</td>
<td>19</td>
<td>4 (FastEthernet0/2)</td>
</tr>
</tbody>
</table>

Informations STP du switch 2

L’antenne Mikrotik SXT 2 est bien le commutateur racine et le lien radio est privilégié par rapport au trunk (lien filaire).
**Nouvelle élection du commutateur racine**

Nous allons maintenant changer le commutateur racine en augmentant la priorité des bridges sur les antennes Mikrotik SXT.

Nous choisissons de mettre la valeur maximale 36864 (9000 en hégadécimal) au lieu de 32768 (8000 en hégadécimal).

---

**Modification de la priorité des bridges des 2 antennes Mikrotik SXT**

**Observations :**

Nous recevons des événements STP au niveau des 2 switches Cisco nous indiquant la nouvelle convergence du réseau. Le nouveau commutateur racine est le switch 2 et que le trunk devient prioritaire.
**Principe de fonctionnement du protocole STP** : Le commutateur avec la priorité la plus basse l’emporte, et en cas d’égalité, c’est l’adresse MAC la plus basse qui l’emporte.

**Explication** :

En modifiant les priorités pour les 2 antennes Mikrotik SXT à 36864, nous les éliminons de l’élection du commutateur racine car la priorité des switchs Cisco est de 32768 et est donc plus petite. La concurrence se fait donc entre les 2 switchs Cisco. Vu qu’ils ont la même priorité, l’élection du nouveau commutateur racine se fait sur l’adresse MAC.

Switch 1: **00:23:34:15:12:80**

Switch 2: **00:26:ca:a4:24:00**

Le switch 1 ayant la plus petite adresse MAC l’emporte.
Modification de la topologie

Actuellement le trafic entre les 2 postes de travail passe par le trunk (lien filaire).

Nous allons forcer le trafic à passer par le lien radio c'est -à-dire le bridge STP établi entre les 2 antennes et voir la réaction des équipements. Pour ce faire, nous allons désactiver l'interface fa0/11 sur le switch 1 et évaluer le temps nécessaire pour le rétablissement de la communication entre les 2 postes de travail.

Avant de désactiver l'interface FastEthernet 0/11, nous avions lancé un ping entre les 2 postes de travail 192.168.1.1/24 et 192.168.1.2/24. Nous avons évalué le temps nécessaire au rétablissement du lien entre les 2 postes de travail suite à la désactivation de l'interface FastEthernet 0/11.

Evaluation du temps de rétablissement

Pour évaluer le temps nécessaire au rétablissement du lien suite à la désactivation du lien entre les 2 Switchs, nous avons utilisé Wireshark pour recueillir les résultats du ping. Un filtrage sur la réponse du ping (réponse echo de type 0) nous permet d’être plus précis sur la durée de rétablissement du lien entre les 2 postes de travail.
Nous constatons que l’interruption du lien s’est effectuée au bout d’un temps t1 = 48 secondes et que le rétablissement s’est effectué au bout d’un temps t2 = 89 secondes.

\[ t1 - t2 = 89 \text{ secondes} - 48 \text{ secondes} = 41 \text{ secondes} \]

Donc, il a fallu 41 secondes pour que le lien soit établi de nouveau entre les postes de travail, ce qui est non négligeable même s’il est plus réduit par rapport à celui obtenu entre les 2 antennes Ubiquity NanoStation (48 secondes).

Cependant, ces 2 temps de rétablissement sont en accord avec les délais établis par la norme STP IEEE 802.1D (entre 30 et 50 secondes).

- **Activation du Rapid Spanning Tree Procol (RSTP)**

L’activation du protocole RSTP a pour but d’accélérer la convergence après un changement de topologie.

Au niveau des Switchs Cisco, l’activation du protocole RSTP s’effectue grâce aux commandes suivantes :

```
sw1>en
sw1#conf t
sw1(config)#spanning-tree mode rapid-pvst
sw1(config)#exit
```

**Modification du mode de protocole en RSTP sur les Switchs Cisco**

Les antennes Mikrotik ont actuellement des bridges configurées avec le mode STP. Nous allons maintenant modifier le mode STP en RSTP pour tenter d’avoir une meilleure vitesse de convergence.
Modification du mode de protocole en RSTP

sur les antennes Mikrotik

- Modification de la topologie

Actuellement le trafic entre les 2 postes de travail passe par le ttrunk (lien filaire).

Nous allons forcer le trafic à passer par le lien radio c’est-à-dire le bridge STP établi entre les 2 antennes et voir la réaction des équipements. Pour ce faire, nous allons désactiver l’interface fa0/11 sur le switch 1 et évaluer le temps nécessaire pour le rétablissement de la communication entre les 2 postes de travail.

Avant de désactiver l’interface FastEthernet 0/11, nous avions lancé un ping entre les 2 postes de travail 192.168.1.1/24 et 192.168.1.2/24. Nous avons évalué le temps nécessaire au rétablissement du lien entre les 2 postes de travail suite à la désactivation de l’interface FastEthernet 0/11.

Pour évaluer le temps nécessaire au rétablissement du lien suite à la désactivation du lien entre les 2 Switchs, nous avons utilisé Wireshark pour recueillir les résultats du ping. Un filtrage sur la réponse
du ping (réponse echo de type 0) nous permet d’être plus précis sur la durée de rétablissement du lien entre les 2 postes de travail.

Nous constatons que l’interruption du lien s’est effectuée au bout d’un temps \( t_1 = 18 \) secondes et que le rétablissement s’est effectué au bout d’un temps \( t_2 = 50 \) secondes.

\[
32 \text{ secondes}
\]

Donc, il a fallu \( 32 \) secondes pour que le lien soit établi de nouveau entre les postes de travail. Ce temps est donc réduit par rapport à celui obtenu en STP avec les 2 modèles d’antennes.

L’activation du protocole RSTP sur les équipements est donc fortement recommandée pour avoir des temps de convergence réduits.

**Réduction du temps de convergence**

Jusque là, les délais et temps du protocole sont à leurs valeurs par défaut.

Au niveau des Switchs Cisco, nous avons :
Au niveau des antennes Mikrotik, nous avons :

<table>
<thead>
<tr>
<th>Name</th>
<th>bridge1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Bridge</td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
</tr>
<tr>
<td>L2 MTU</td>
<td>1598</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:0C:42:F1:AF:83</td>
</tr>
<tr>
<td>ARP</td>
<td>enabled ✗</td>
</tr>
<tr>
<td>Admin. MAC Address</td>
<td>✗</td>
</tr>
<tr>
<td>Protocol Mode</td>
<td>none ✗ stp ✗ rstp</td>
</tr>
<tr>
<td>Priority</td>
<td>8000 hex</td>
</tr>
<tr>
<td>Max Message Age</td>
<td>00:00:20</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>00:00:15</td>
</tr>
<tr>
<td>Transmit Hold Count</td>
<td>6</td>
</tr>
<tr>
<td>Ageing Time</td>
<td>00:05:00</td>
</tr>
</tbody>
</table>

**Définitions :**

Les ports des commutateurs où STP est actif sont dans l’un des états suivants :

- **Listening** : le commutateur « écoute » les BPDU et détermine la topologie réseau.
- **Learning** : le commutateur construit une table faisant correspondre les adresses MAC aux numéros des ports.
- **Forwarding** : un port reçoit et envoie des données, opération normale.
*Blocking* : un port provoquant une boucle, aucune donnée n’est envoyée ou reçue mais le port peut passer en mode *forwarding* si un autre lien tombe.

*Disabled* : désactivé, un administrateur peut manuellement désactiver un port s’il le souhaite.

**Forward Delay** : Le délai de transition entre les modes Listening vers Learning et Learning vers Forwarding est nommé *forward delay*, il est fixé par le root bridge et vaut 15 secondes par défaut.

**Max-Age** : Le timer max age contrôle le temps maximum pendant lequel un commutateur garde en mémoire une BPDU de configuration. Il est égal à 20 secondes par défaut mais peut être réglé de 6 à 40 secondes.

**Hello Time** : Le Hello time est le temps entre deux trames BPDU transmises sur un port. Il est égal à 2 secondes par défaut mais peut être réglé de 1 à 10 secondes.

Les équipements sont calés sur les mêmes délais c’est-à-dire même Max Age (20 secondes), même Forward Delay (15 secondes) et même Hello Time (5 secondes). Ceci dans le but d’avoir une concurrence équitable.

Nous allons maintenant réduire ces délais pour tenter de réduire le délai de convergence dès l’interruption d’une liaison.

**Nouvelles valeurs** :

Max age : 6 secondes

Forward Delay : 4 secondes

La modification des valeurs se fait facilement sur l’interface web graphique des antennes Mikrotik.

Pour les Switchs Cisco, les commandes sont les suivantes :

```
sw1>en
sw1#conf t
sw1(config)#spanning-tree vlan 1 max-age 6
sw1(config)#spanning-tree vlan 1 forward-delay 4
```

Nous avons refait les mêmes tests c’est à l’interruption du lien filaire entre les 2 Switchs Cisco et évalué le temps nécessaire au rétablissement :
Ici, nous avons un délai réduit à 19 secondes (36 secondes – 17 secondes).

Nous sommes allés plus loin en diminuant encore le hello-time des Switchs et des antennes Mikrotik.

**Nouvelles valeurs :**

- Max age : 6 secondes
- Forward Delay : 4 secondes
- Hello Time : 2 secondes

Ce nouveau paramétrage nous permet d’avoir un temps de convergence de 11 secondes (21 secondes - 10 secondes) comme constaté sur la capture d’écran suivante:
6. Mise en place de réseaux virtuels : VLAN

Le but de ce travail pratique est de parvenir à faire transiter les différentes données de plusieurs VLANs via un lien radio établi entre 2 antennes.

a. Entre 2 antennes Mikrotik

Ce premier travail s’appuie sur les antennes Mikrokit avec antennes non intégrées 433UAHL et 433L.

Partie 1 :

1. Architecture

Nous partons de l’architecture réseau suivante:
Architecture Réseau

Notre architecture est composée de 4 postes de travail réparties sur 2 VLANs :

- 192.168.1.1/24 et 192.168.1.2/24 sur le VLAN 10
- 192.168.2.1/24 et 192.168.2.2/24 sur le VLAN 20

2 switchs Cisco 3950 assurent l’interconnexion des postes de travail et des antennes. Les 2 antennes Mikrotik assurent le lien radio.

2. Configuration des 2 antennes

Au niveau radio, les 2 antennes radio sont configurées de manière classique c'est-à-dire l’une en station (*station bridge*) qui se connecte sur l’autre antenne point d’accès (*ap bridge*).

Les communications entre les 2 antennes est fonctionnelle.

Au niveau IP, les 2 antennes 433UAHL et 433L ont respectivement comme adresse *192.168.1.24/24* et *192.168.1.25/24*.

3. Mise en œuvre des VLANs sur les 2 antennes Mikrokit

Pour configurer les VLANs, nous accédons d’abord par ssh à l’interface ligne de commandes des antennes à travers la commande suivante :

```
ssh admin@192.168.1.24

ssh admin@192.168.1.25
```
Puis, nous nous authentifions avec le mode de l’utilisateur admin qui est « admin ».

**Configuration des VLANs dans le port trunk**

Nous créons ici 2 VLANs (**vlan-10 et vlan-20**) ayant respectivement comme id 10 et 20 sur l’interface trunk wlan1.

```
[admin@MikroTik] > /interface vlan add name=vlan-10 vlan-id=10 interface=wlan1 disabled=no
[admin@MikroTik] > /interface vlan add name=vlan-20 vlan-id=20 interface=wlan1 disabled=no
```

**Configuration des bridges**

Pour être en mesure de transmettre les paquets depuis les ports d’accès reliés au switch 3950 aux VLANs, nous avons besoin de ponts (bridges). Ici, nous créons 2 bridges (**br-vlan10 et br-vlan20**) pour chacun des 2 vlans précédemment créés.

```
[admin@MikroTik] > /interface bridge add name=br-vlan10 disabled=no
[admin@MikroTik] > /interface bridge add name=br-vlan20 disabled=no
```

**Association des ports d’accès aux bridges**

Maintenant, nous pouvons ajouter les ports d’accès **ether1** aux bridges créés ci-haut.

```
[admin@MikroTik] > /interface bridge port add interface="vlan-10" bridge="br-vlan10" disabled=no
[admin@MikroTik] > /interface bridge port add interface="ether1" bridge="br-vlan10" disabled=no
[admin@MikroTik] > /interface bridge port add interface="vlan-20" bridge="br-vlan20" disabled=no
[admin@MikroTik] > /interface bridge port add interface="ether1" bridge="br-vlan20" disabled=no
```

Au niveau graphique, nous obtenons:
NB : Les configurations ci-dessus ont été faites sur une des antennes Mikrokit et doivent être dupliquées sur l'autre antenne. Les configurations sont similaires.

4. **Configuration des postes de travail**

Les postes de travail sont associés au VLANs.

Les postes de travail sur le VLAN 10 sont configurés de la manière suivante :

```bash
if config eth0.10 192.168.10.1/24
if config eth0.10 192.168.10.2/24
```

Les postes de travail sur le VLAN 20 sont configurés de la manière suivante :

```bash
if config eth0.20 192.168.20.1/24
if config eth0.20 192.168.20.2/24
```

5. **Test de la communication**

Nous venons de configurer les VLANs sur les antennes et associés les postes de travail au VLANs correspondant.
Un ping vers le poste de travail 192.168.1.1 depuis le poste 192.168.1.2 donne :

```
felucia:/home/etu# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.842 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.834 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.780 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.780/0.818/0.842/0.043 ms
```

Ping OK

Un ping vers le poste de travail 192.168.1.1 depuis le poste 192.168.2.1 donne :

```
felucia:/home/etu# ping 192.168.2.1
connect: Network is unreachable
felucia:/home/etu#
```

Ping non OK

Nous remarquons que le ping ne marche que sur les machines d’un même VLAN. Ce qui est normal. Pour que cette communication puisse être établie, il faut mettre en place du routage inter-vlan.

6. **Capture Wireshark**
Cette capture Wireshark précédente résulte d’un ping effectué depuis la machine 192.168.1.1 et 192.168.1.2 situés dans le VLAN 10. Nous remarquons que les trames sont taggués avec l’ID du VLAN (10).

**Partie 2:**

Cette partie 2 résulte du constat que les données des différents VLANs (vlan-10 et vlan-20) ne transitent pas par les bridges créés (br-vlan10 et br-vlan20) mais passaient plutôt par le bridge1 créé par défaut comme en témoigne la capture suivante :

![Capture Wireshark](image)

Nous avons pensé à rajouter un port (association interface/brigde) entre le wlan1 et les bridges créés pour les VLANs. L’interface wlan1 étant déjà associé au bridge1 par défaut, ceci est impossible car une interface ne peut être associé à une et une seule bridge (voir capture ci dessous) :
Tentative de création d'un nouveau port avec l'interface wlan 1

Message d'erreur lors de la tentative de création d'un nouveau port avec l'interface wlan 1

Nous avons dû revoir les configurations des antennes et mettre en place une nouvelle architecture pour arriver à bout de cette anormalité.

1. **Nouvelle architecture** :
Architecture Réseau

Notre architecture est composée de 4 postes de travail réparties sur 2 VLANs :

- 192.168.10.1/24(sur ether2 de l’antenne) et 192.168.10.2/24(sur ether3 de l’antenne) sur le VLAN 10
- 192.168.20.1/24(sur ether2 de l’antenne) et 192.168.20.2/24(sur ether3 de l’antenne) sur le VLAN 20

Les interfaces ether1 servent à l’administration des antennes.

Les interfaces wlan 1 assurent la liaison radio entre les 2 antennes.

Nous avons enlevé les switchs cisco 3950 car nous les avions mis pour pouvoir connecter les 2 machines alors que nous avions les 2 interfaces ether1 et ether2 disponibles. Au-delà de 2 machines, l’utilisation d’un switch est indispensable.

1. Configuration des 2 antennes :

Au niveau radio, les 2 antennes radio sont configurées de manière classique c'est-à-dire l’une en station (station bridge) qui se connecte sur l’autre antenne point d'accès (ap bridge).

Les communications entre les 2 antennes est fonctionnelle.


2. Mise en œuvre des VLANs sur les 2 antennes Mikrokit

Pour configurer les VLANs, nous accédons d’abord par telnet ou ssh à l’interface ligne de commandes des antennes à travers la commande suivante :

telnet ou ssh admin@192.168.1.24

telnet ou ssh admin@192.168.1.25

Puis, nous nous authentifions avec le mode de passe de l’utilisateur admin qui est « admin ».
### Configuration des VLANs dans le port trunk

Nous créons ici 2 VLANs (*vlan-10 et vlan-20*) ayant respectivement comme id 10 et 20 sur l'interface trunk wlan1.

```plaintext
[admin@MikroTik] > /interface vlan add name=vlan-10 vlan-id=10 interface=wlan1 disabled=no
[admin@MikroTik] > /interface vlan add name=vlan-20 vlan-id=20 interface=wlan1 disabled=no
```

**NB:** Configuration à dupliquer sur les 2 antennes

### Configuration des bridges

Ici, nous n’allons pas créer des bridges pour chaque VLAN créé précédemment comme nous avions fait à la première partie. Nous allons utiliser le bridge1 par défaut pour canaliser toutes les données des VLANs.

### Association des ports d’accès aux bridges

Maintenant, nous ajoutons les ports d’accès *ether2 et ether3* au bridge1 par défaut :

```plaintext
[admin@MikroTik] > /interface bridge port add interface="vlan-10" bridge="bridge1" disabled=no
[admin@MikroTik] > /interface bridge port add interface="ether2" bridge="bridge1" disabled=no
[admin@MikroTik] > /interface bridge port add interface="vlan-20" bridge="bridge1" disabled=no
[admin@MikroTik] > /interface bridge port add interface="ether3" bridge="bridge1" disabled=no
```

**NB:** Configuration à dupliquer sur les 2 antennes

Au niveau graphique, nous obtenons:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Type</th>
<th>L2 MTU</th>
<th>Tx</th>
<th>Rx</th>
<th>Tx Packet [pps]</th>
<th>Rx Packet [pps]</th>
<th>Tx Drops</th>
<th>Rx Drops</th>
<th>Tx Errors</th>
<th>Rx Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ether1</td>
<td>Ethernet</td>
<td>1524</td>
<td>922 kbps</td>
<td>922 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>ether2</td>
<td>Ethernet</td>
<td>1524</td>
<td>9 kbps</td>
<td>9 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>ether3</td>
<td>Ethernet</td>
<td>1524</td>
<td>9 kbps</td>
<td>9 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>vlan-10</td>
<td>VLAN</td>
<td>2290</td>
<td>9 kbps</td>
<td>9 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>vlan-20</td>
<td>VLAN</td>
<td>2290</td>
<td>9 kbps</td>
<td>9 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>wlan1</td>
<td>Wi-Fi</td>
<td>496 kbps</td>
<td>496 kbps</td>
<td>496 kbps</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Au niveau des ports, le bridge1 assure maintenant le lien ether2/wlan1 et aussi le lien ether3/wlan1 comme indiqué ici :

<table>
<thead>
<tr>
<th>6 Items</th>
<th>Interface</th>
<th>Bridge</th>
<th>Priority (hex)</th>
<th>Path Cost</th>
<th>Horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>- D</td>
<td>ether1</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>- D</td>
<td>ether2</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>- D</td>
<td>ether3</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>- D</td>
<td>vlan-10</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>- D</td>
<td>vlan-20</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>- D</td>
<td>wlan1</td>
<td>bridge1</td>
<td>80</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

3. **Affectation des adresses IP de VLAN**

Nous allons maintenant configurer les adresses IP sur chaque VLAN.

- **Antenne 1 : Mikrokit 433UAHL**

[admin@MikroTik] /ip address> add address=192.168.10.24/24 interface=vlan-10

[admin@MikroTik] /ip address> add address=192.168.20.24/24 interface=vlan-20

Nous avons affecté l’adresse IP 192.168.10.24 à l’interface de VLAN 10 et l’adresse IP 192.168.20.24 à l’interface de VLAN 10

- **Antenne 2 : Mikrokit 433L**

[admin@MikroTik] /ip address> add address=192.168.10.25/24 interface=vlan-10

[admin@MikroTik] /ip address> add address=192.168.20.25/24 interface=vlan-20

Au niveau graphique, nous obtenons :

4. **Test de la communication**

Une fois les configurations terminées, nous pouvons maintenant faire le test d’abord entre les antennes sur un même VLAN donné.

Ping effectué depuis l’antenne Mikrokit 433UAHL ayant comme adresse 192.168.10.24 sur le VLAN 10 vers l’antenne Mikrokit 433L ayant comme adresse 192.168.10.25 sur le VLAN 10

```
[admin@MikroTik] /ip address> /ping 192.168.10.25
HOST         SIZE TTL TIME STATUS
192.168.10.25 56  64 1ms
192.168.10.25 56  64 2ms
```

**sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms PINK OK**

Ping effectué depuis l’antenne Mikrokit 433UAHL ayant comme adresse 192.168.20.24 sur le VLAN 10 vers l’antenne Mikrokit 433L ayant comme adresse 192.168.20.25 sur le VLAN 20
Le trunk entre les 2 antennes est **fonctionnel**.

Testons maintenant le lien entre les postes de travail. En faisant un ping depuis le poste de travail 192.168.10.2/24 sur le VLAN 10, nous obtenons :

```
[admin@MikroTik] /ip address> /ping 192.168.20.25

<table>
<thead>
<tr>
<th>HOST</th>
<th>SIZE</th>
<th>TTL</th>
<th>TIME</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.25</td>
<td>56</td>
<td>64</td>
<td>1ms</td>
<td></td>
</tr>
<tr>
<td>192.168.20.25</td>
<td>56</td>
<td>64</td>
<td>2ms</td>
<td></td>
</tr>
<tr>
<td>192.168.20.25</td>
<td>56</td>
<td>64</td>
<td>2ms</td>
<td></td>
</tr>
</tbody>
</table>
```

sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms

**PINK OK**

Ces mêmes tests ont été effectués sur le VLAN20 et ont été aussi réussis.

A noter que seules les machines d’un même VLAN peuvent communiquer.
Nous observons la même situation entre les postes de travail sur le VLAN 20.

Nous constatons aussi que tout le trafic des VLANs transite par le bridge1 par défaut. La création des autres bridges pour chaque VLAN était donc inutile.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Type</th>
<th>L2 MTU</th>
<th>Tx</th>
<th>Rx</th>
<th>Tx Packet (pps)</th>
<th>Rx Packet (pps)</th>
<th>Tx Drops</th>
<th>Rx Drops</th>
<th>TxErrors</th>
<th>RxErrors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>Bridge</td>
<td>1526</td>
<td>82.1 kbps</td>
<td>8.5 kbps</td>
<td>8</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Entre 2 antennes Nanostation**

1. **Architecture**

![Architecture Diagram]

2. **Configuration des 2 antennes** :

Au niveau radio, les 2 antennes radio sont configurées de manière classique c'est-à-dire l'une en station (station) qui se connecte sur l'autre antenne point d'accès (Access Point).
Les communications entre les 2 antennes est fonctionnelle. Au niveau IP, les 2 antennes NansoStation ont respectivement comme adresse 192.168.1.20/24 et 192.168.1.21/24.

3. **Mise en œuvre des VLANs sur les 2 antennes Nanostation**

   **Création des VLANs**

Ici, la configuration se fait par interface graphique contrairement aux antennes Mikrokit où il est possible par l’interface graphique :

Pour créer, il faut accéder à l’onglet *Network* après s’être authentifié avec un compte administrateur à l’interface web de l’antenne.

Puis, il faut changer le mode de configuration de *Simple* à *Avancé*
### Création des bridges

Toujours dans l’onglet *Network*, nous allons créer 2 bridges affectés à chaque VLAN pour le transit des données :

<table>
<thead>
<tr>
<th>Bridge 1</th>
<th>LAN0</th>
<th>WLAN0</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LAN0</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WLAN0</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge 2</th>
<th>LAN1</th>
<th>WLAN0</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LAN1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WLAN0</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

Comme pour les antennes Mikrotik, nous avons créé 2 bridges :
- Un pour faire le lien entre l’interface ethernet principal LAN0 et l’interface WLAN0 sur le VLAN 10
- Un pour faire le lien entre l’interface ethernet secondaire LAN1 et l’interface WLAN0 sur le VLAN 20

**NB** : Ces configurations sont à refaire sur l’antenne NanoStation.

### 4. Affectation des adresses IP de VLAN
Contrairement aux antennes Mikrotik, il n’est pas possible d’affecter des adresses IP aux VLANs créés précédemment. Il est juste possible de mettre une seule adresse IP pour la gestion de l’équipement en choisissant un des bridges créés.

Pour notre cas, nous avons affecté l’adresse IP 192.168.10.20/24 et 192.168.10.21/24 sur les bridge1 des 2 antennes. Ce bridge nous permettra d’administrer les antennes.

L’affectation des adresses de VLAN s’effectue sur les bridges créés précédemment :

- Antenne d’adresse IP 192.168.1.20/24

- Antenne d’adresse IP 192.168.1.21/24

5. **Test de la communication**

Après les configurations terminées, nous pouvons maintenant débuter les tests. Nous avons repris les mêmes tests mais cette fois uniquement entre les postes de travail 192.168.10.1/24 et

```bash
felucis:/home/etu# ping 192.168.10.1
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.711 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.795 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.352 ms
```

Ping du poste de travail 192.168.10.1 réussi

```
PINK OK depuis le poste de travail 192.168.10.2
```

```bash
dagobah:/home/etu# ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=0.765 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=0.742 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=64 time=0.762 ms
```

Ping du poste de travail 192.168.20.1 réussi

```
PINK OK depuis le poste de travail 192.168.20.2
```

Les machines sur le même VLAN communiquent.
CONCLUSION

Ce stage a été pour nous une expérience professionnelle très enrichissante sur plusieurs plans : aussi bien du point de vue de l’approfondissement de nos connaissances en réseau que du point de vue organisationnel.

Nous avons pu approfondir de manière conséquente nos connaissances théoriques en réseau radio et l'utilisation de protocoles de niveau 2 comme le STP ainsi que nos savoirs dans la virtualisation des réseaux.

Par ailleurs, ce stage nous a permis de voir la réalité des petites entités émergentes. Il en ressort qu’avec des moyens limités et beaucoup de volonté, on peut réaliser des projets ambitieux à l’envergure des grandes entreprises.

Ce stage nous a sensibilité sur l’importance d’une bonne documentation avant d’entamer des travaux pratiques ce qui nous a porté préjudice au début du projet mais nous avons su rebondir très vite en suivant les conseils de nos responsables de stage.

Nous pensons avoir rempli notre objectif lors de ce stage et avoir été à l’écoute des demandes tout en n’hésitant pas à demander des conseils en cas de besoin.
REFERENCES BIBLIOGRAPHIQUES

- Documentation
  - http://chiliproject.tetaneutral.net/projects/tetaneutral/wiki/Mikrotik
  - http://chiliproject.tetaneutral.net/projects/tetaneutral/wiki/Relais_Autonome
  - http://chiliproject.tetaneutral.net/projects/tetaneutral/wiki/Wiki

- Vlan

- Familiarisation avec les équipements
  - http://wiki.ubnt.com/AirOS_5.3

- Travaux pratiques Spannig Tree Protocol
  - https://www.dropbox.com/s/lus0jgl0pm1wnxv/Cisco_Networking_Academy.pdf

- Prix des équipements
  - http://www.mhzshop.com/shop/index~cl~details~cnid~85b48899330250ba2.3175552~anid~8b64a
    ae461a7b4c89.68834691.htm
  - http://www.mhzshop.com/shop/index~sid~x~shp~oxbaseshop~cl~details~cnid~26a4510492172792
    2.28473137~anid~fb14a64939cc2f435.07472825.htm
GLOSSAIRE

STP : Spanning Tree Protocol

RSTP : Rapid Spanning Tree Protocol

AP : Point d’ accès

VLAN: Virtual Local Area Network

Switch : il désigne un commutateur réseau, un équipement qui permet l’interconnexion d’entités réseau appartenant à un même réseau physique.

POE : Power over Ethernet, qui permet d'alimenter électriquement un appareil via le câble réseau

LAN : Local Area Network

802.11 : IEEE 802.11 est un ensemble de normes concernant les réseaux sans fil qui ont été mises au point par le groupe de travail 11 du Comité de normalisation LAN/MAN de l'IEEE (IEEE 802).

802.3 af : IEEE 802.3af est une norme appartenant au standard IEEE 802.3 (Ethernet) ratifiée le 11 juin 2003 et publiée le 11 juillet 2003. Plus connue sous le nom de Power over Ethernet, IEEE 802.3af est aussi un groupe de travail du sous-comité IEEE 802.3.

802.1 d : norme mis en œuvre par les ponts et les commutateurs pour gérer les liaisons plus reconnu sous le nom de STP

Bandwith Test : outil intégré aux équipements Mikrotik et permettant d’effectuer des mesures de bande passante

Speed Test : outil intégré aux équipements ubiquity et permettant d’effectuer des mesures de bande passante

RX : Débit en Réception

TX : Débit en Transmission

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

Trunk : Un lien qui permet de faire transiter plusieurs VLAN sur un seul lien physique

SSH : Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé.
Telnet : Telnet (TErminal NETwork ou TELecommunication NETwork, ou encore TELe type NETwork) est un protocole réseau utilisé sur tout réseau prenant en charge le protocole TCP/IP.
ANNEXES

Planning prévisionnel

Planning réel