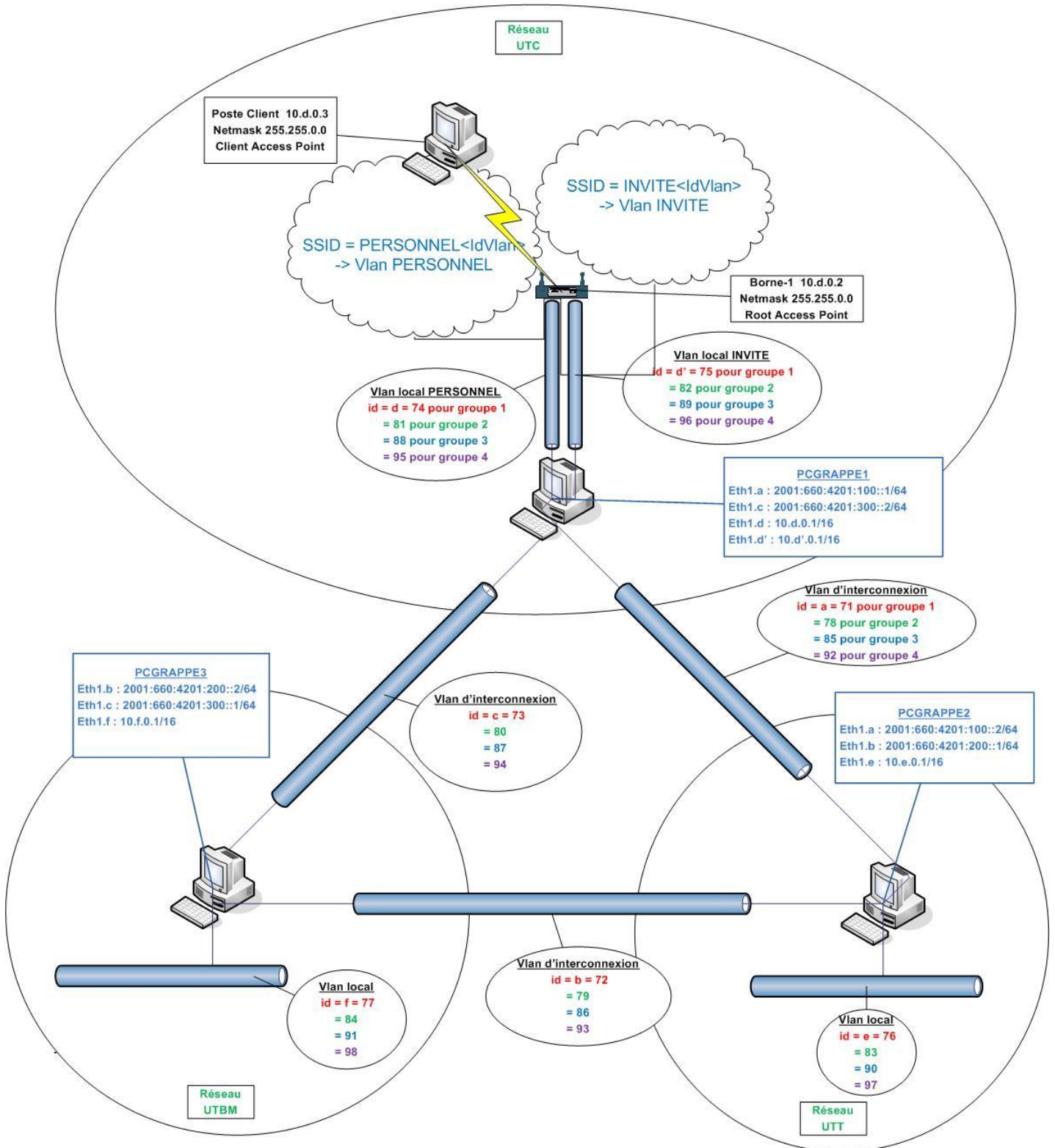


Projet Réseau SR06
Automne 2010

Le projet consiste en la réalisation d'une mini infrastructure réseau, composée de 3 postes de la grappe (salle J210), 1 borne wifi et un portable étudiant pouvant faire office de client wifi. Ce projet s'effectuera par groupe de 3 binômes, de manière à pouvoir utiliser 3 postes. Si un groupe de 4 est constitué, il conviendra d'adapter le schéma de principe avec 1 réseau supplémentaire sur le même principe que celui de l'UTT ou l'UTBM, connecté entre l'UTBM et l'UTC (voir 1. schéma de principe).

1. Schéma de principe et adressage.



2. Routing

Le routing devra être possible entre tous les vlans.

Pour la réalisation du routing, il conviendra d'utiliser quagga.

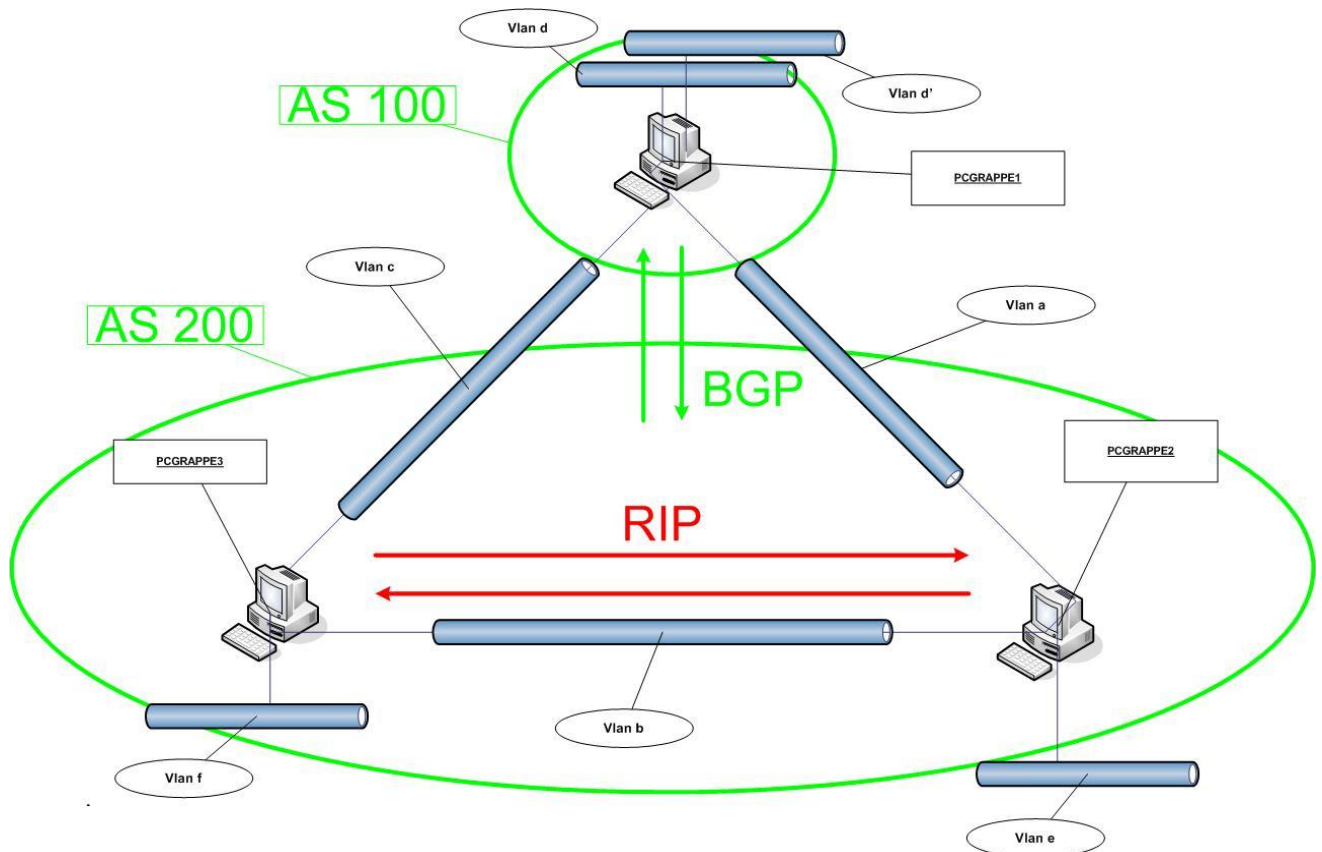
Les algorithmes de routing à mettre en place seront BGP et RIP.

Il conviendra de placer pcgrappe1 dans un autonomous-system 100 (AS 100), alors que

pcgrappe2 et pcgrappe3 feront partie de l'autonomous-system 200 (AS 200).

Le routing à l'intérieur de l'autonomous system 200 se fera en RIP.

Si un 4^{ème} routeur participe au routing, il conviendra de le faire figurer dans l'AS100, et de configurer le protocole RIP entre celui-ci et le routeur PCGRAPPE1.



Afin que les protocoles de routing échangent plus d'informations, 3 routes statiques devront être créées et dirigées vers un routeur fictif sur le vlan correspondant au réseau local (vlan d, e ou f).

Chaque routeur devra filtrer au moins une des routes statiques des routeurs adjacents.

3. Filtrage

La gestion du filtrage sera réalisé grâce à « **iptables** ».
Il sera impératif d'utiliser un fichier de configuration d'access-list.

Remarque : Les protocoles de routage précédemment mis en place devront être défiltrés de manière à être opérationnels après la mise en place du filtrage.

a) Le poste local

Les postes locaux devront être protégés de TOUS les accès du réseau **SAUF** pour le protocoles suivants :

Icmp
Telnet
MySQL
http
snmp

Il sera impératif de logger des infos sur les trames « dropées »

b) Routeur

Un des routeurs choisi au hasard devra laisser passer **UNIQUEMENT** les protocoles suivants :

Icmp : pour tout le monde
Telnet : depuis poste-1 vers postes+1 et vice versa
MySQL : depuis poste-1 vers postes+1 et vice versa
http : depuis poste-1 vers postes+1 et vice versa
snmp : depuis poste-1 vers postes+1 et vice versa
snmp : depuis poste-1 vers borne 1
snmp : depuis poste+1 vers borne 1

Poste-1 et Poste+1 étant les postes adjacents au routeur.

Il sera impératif de logger des infos sur les trames « dropées »

4. Wifi

Pour vous aider dans la réalisation de cette partie, et surtout dans la configuration des points d'accès, vous pouvez vous référer au lien :

http://www.utc.fr/~quetwilf/sr06/TD4_WIFI.pdf (user = **sr06**, password = **sr06**)

La borne wifi sera administrée par le vlan Personnel.

Elle devra diffuser un SSID « **Personnel<NoVlan>** » sur le Vlan «Personnel » et un SSID « **Invite<NoVlan>** » sur le vlan « Invite ».

Configurer un poste client comme cliente de la borne wifi sur le SSID « Personnel ».

Le but est de réaliser un pont entre le réseau X et le réseau Y sans passer par le firewall.

La réalisation de ce pont ne sera pas réellement possible car les bornes ne sont pas des réellement des ponts : c'est-à-dire qu'une communication entre le poste 1 et le poste 3 ne pourra pas aboutir.

L'essentiel sera de pouvoir voir dans les logs de la borne wifi que le client a pu s'associer et s'authentifier.

Il faudra choisir un nom de réseau (SSID) différent des autres groupes de TD et si possible un canal de communication différent.

Mettre en place un cryptage WPA non basé sur clé pré-partagée.

Filtrer les adresses ethernet des bornes non connues.

Authentification Radius :

Mettre en place un mécanisme d'authentification pour les clients sur la borne wifi basé sur LEAP Pour ce, il faudra installer et configurer un serveur radius de type freeradius.

L'attribution du Vlan Personnel devra être effectuée par le serveur Radius (attribution de vlan dynamique 802.1x).

Pour ce faire, il faudra utiliser les attributs suivants en fonction du login utilisateur :

Tunnel-Type = 13,

Tunnel-Medium-Type = 6,

Tunnel-Private-Group-Id = <n° vlan à affecter>

indications : configurer les fichiers radiusd.conf,eap.conf, clients.conf et users. Le serveur radius peut être lancé en mode debug grâce à la commande « **radiusd -X** »

5. Administration

a) Intérogation SNMP

But : réaliser des intérogations SNMP vers la borne wifi à intervalles réguliers via un script shell ou tout autre méthode et stocker les résultat dans des fichiers distincts pour 2 mibs suivantes :

- IfInOctets.x = Nombre d'octets entrants sur l'interface d'index x de la borne (interface de nom Dot11Radio0)

- IfOutOctets.x) = Nombre d'octets sortants sur l'interface d'index x de la borne (interface de nom Dot11Radio0)

Grâce à la branche IfDesc de la mib standard mib-2 (.1.3.6.1.2.1.2.2.1.2), identifier l'index de l'interface Dot11Radio0.

Les interrogations s'effectueront après avoir changé la communauté SNMP des bornes (choisir une même communauté pour les 2 bornes)

L'installation du package ucd-snmp sera nécessaire.

b) Trap SNMP

Un service de trap SNMP sera mis en place de manière à exécuter automatiquement un script à la réception d'un événement d'association sur la borne 1.

L'installation du package snmpd sera nécessaire.
Le fichier snmptrapd devra être configuré de manière à recevoir les traps concernant les événements radio (dot11) de la borne 1 :

```
traphandle SNMPv2-SMI::enterprises.9.9.41.2.0.1 /usr/local/bin/script.sh
```

c) Syslog

But : Renvoi des messages informationnels de la borne sur un serveur syslog sur le poste administrateur

Choisir une facility non utilisée par le système