Annexe 1 : Installation d'Iperf2 et Iperf3

Configuration réalisée sur Ubuntu 12.04

Installation Iperf2 sur Linux

Etape 1: Installation
DL le fichier Iperf-2.0.5.tar.gz sur le net

```
sudo apt-get install Iperf
sudo gunzip -c iperf-2.0.5.tar.gz | tar -xvf -
cd "le_dossier_ou_est_installé_Iperf"/iperf-2.0.5
sudo ./configure
sudo make
sudo make install
```

Etape 2: Définir le client et le serveur
Installer Iperf sur les 2 machines (client et serveur)
Exemple: IP client = 192.168.1.12, Ip serveur = 192.168.2.48
Côté serveur faire : Iperf -s (il faut d'abord lancer le côté serveur pour que le client fonctionne)
Côté client faire : Iperf -c 192.168.2.48 (on spécifie son serveur)

Installation Iperf3 sur Linux

Etape 1: Installation
Télécharger la dernière version sur leur site officiel
https://iperf.fr/iperf-download.php

```
cd "le_dossier_ou_est_installé_Iperf3"/iperf3
sudo dpkg -i *.deb
sudo apt-get -f install
```

Supprimer les fichiers .deb qui sont maintenant installé

Etape 2: Définir le client et le serveur
Installer Iperf3 sur les 2 machines (client et serveur)
Exemple pour: IP client = 192.168.1.12, Ip serveur = 192.168.2.48
Côté serveur faire : Iperf3 -s (il faut d'abord lancer le côté serveur pour que le client fonctionne)
Côté client faire : Iperf3 -c 192.168.2.48 (on spécifie son serveur)

Installation Iperf3 sur Windows 7

Etape 1: Telecharger Iperf3

Télécharger la dernière version sur leur site officiel

https://iperf.fr/iperf-download.php

Dézipper le dossier téléchargé

Placer le téléchargement dans le dossier de l'utilisateur (ici cisco)

Démarrer Iperf3 en ligne de commande

```
cd C:\Users\cisco\iperf3.1_32
iperf3.exe
```

Iperf et maintenant installé, le fonctionnement est le même que sur Linux à l'exception que pour l'utiliser, il faudra toujours être dans le dossier d'installation d'Iperf.

Annexe 2 : Configuration du protocole SNMP sur un équipement Cisco

Etape1: Créer l'access-list pour autoriser le serveur à y accéder

```
R1(config)#access-list 10 permit host 192.168.2.48
R1(config)#access-list 10 deny any log
```

Etape2: configuration de SNMP
On va spécifier la community "public", SNMP read only et on y applique l'access-list n°10.

```
R1(config)#snmp-server community public ro 10
R1(config)#snmp-server ifindex persist
R1(config)#snmp-server location LOCATION_R1
R1(config)#snmp-server chassis-id CHASSIS_R1
R1(config)#logging history debug
```

On spécifie le serveur qui va recevoir les trap, on utilise la version2 de SNMP et la community public

```
R1(config)#snmp-server host 192.168.2.48 traps ver 2 public
R1(config)#snmp-server trap-source loopback0 (vlan1 si switch)
R1(config)#snmp-server source-interface trap loopback0
R1(config)#snmp-server enable trap
```

Commandes de vérification:

```
R1#sh run | in snmp
R1#sh snmp community
R1#sh snmp host
```

Pour contrôler que le tout fonctionne:
Lancer Wireshark et filtrer par: port udp 162
Déclenchez une trap (shut / no shut une interface)
On doit alors voir les paquets SNMP arriver

Annexe 3 : Configuration de SNMP sur le serveur Linux

Configuration réalisée sur Ubuntu 12.04

Etape 1: installation

```
sudo apt-get update
sudo apt-get install snmp snmpd
sudo nano /etc/snmp/snmp.conf (verifier que "mibs :" n'est pas en commentaire)
```

Etape 2 : Configuration

```
sudo nano /etc/snmp/snmpd.conf
#commenter la ligne 2, decommenter la ligne 4)
  #Listen for connections from the local system only
  #agentAddress  udp:127.0.0.1:161
  #Listen for connections on all interfaces (both IPv4 *and* IPv6)
  agentAddress udp:161,udp6:[::1]:161

#Sous la partie ACCESS CONTROL remplacer les 3 "systemonly" par "all"
  view all included .1.3.6.1.2.1.1
  view all included.1.3.6.1.2.1.25.1
  rocommunity public default   -V all
#Decommenter “rocommunity secret 10.0.0.0/16”. et y ajouter l’adresse #réseau du serveur Cacti
  rocommunity secret 192.168.2.0/26
#Sous SYSTEM INFORMATION on peut changer le sysLocation et sysContact #si on veut
Enregistrer et quitter le fichier
sudo service snmpd restart
```

Installation de snmp et snmpd terminé, notre serveur est maintenant configuré pour faire du SNMP.

Annexe 4 : Configuration de Cacti

Configuration réalisée sur Ubuntu 12.04

Etape 1: Installation de Cacti

```
sudo apt-get install Cacti-spine
       Répondre OK au fait que le répertoire php change d'endroit
       choisir la bdd par défaut proposée
       définir les mots de passe
```

Etape 2: Configuration générale de l'interface web

Lancer Cacti: 192.168.2.48/Cacti/
Cliquer next pour installer le tout (chaque ligne doit être verte [OK: FILE FOUND])
Se connecter avec: login, admin - password, admin - changer le mot de passe
On arrive sur la page d'accueil de Cacti

Dans le menu de gauche, cliquer sur "settings"
Sous l'onglet Général, changer les champs suivants:
 SNMP Version: Version 2
 SNMP Community: secret (va servir à pouvoir monitorer le serveur)
Cliquer sur "save" en bas à droite

Aller dans l'onglet Poller, changer les champs suivants:
 Poller Type: spine
 Poller Interval: Every Minute
Cliquer sur "save" en bas à droite
Dans le menu de gauche, cliquer sur "System Utilities"
Cliquer sur "Rebuild Poller Cache" pour vider le cache

Etape 3: Créer le serveur et ses graphiques

Avant de commencer cette étape il faut avoir installé et configurer snmp et snmpd afin de pouvoir configurer le monitoring du serveur

Dans les menus de gauche, Cliquer sur "Devices"
On supprime le device présent "localhost", on ne va pas l'utiliser:
Cocher la case à droite, choisir l'action "delete" et cliquer "go"

En haut à droite, cliquer sur "Add" pour créer un nouvel équipement
Modifier les champs suivant:
 Description: Ubuntu Cacti Server
 Hostname: 192.168.2.48
 Host Template: Local Linux Machine
 SNMP Version: Version 2
 SNMP Community: secret
Cliquer sur "create" en bas une fois le tout configuré
Si tout marche, vous verrez des infos sur la config de votre serveur snmp apparaitre en haut sur la gauche
Si l'erreur rouge SNMP error apparait, redémarré le daemon snmp:
sudo service snmpd restart

Descendre en bas sous "Associated Graph Templates"
Ajouter le template "Unix - Ping Latency" et cliquer sur "Add"

Aller en dessous sous "Associated Data Queries"
Ajouter les 3 Query SNMP:
        SNMP - Get Mounted Partitions

SNMP - Get Processor Information
SNMP - Interface Statistics
Cliquer sur "Add" à chaque fois
Cliquer sur "save" pour sauvegarder le tout

En haut de la page cliquer sur "Create Graphs for this Host"
Cocher les cases des graphiques que vous souhaitez créer
Cliquer sur "Create"
Choisir les couleurs pour les graphiques et cliquer "Create"

Tout en haut à gauche de la page cliquer sur le bouton bleu "Graphs"
Pour afficher vos graphiques, allez tout en haut à droite de la page et cliquer sur le bouton bleu tout à droite (il s'appel Preview view en pointant le curseur dessus)
Vous êtes sur la page où vous pouvez consulter tous vos graphiques
Attention, la première fois, les graphiques mettent beaucoup de temps à se créer et à se générer. (~5-10min)

Etape 4: Ajouter un équipement cisco au serveur Cacti
! Il faut avoir configuré l'équipement cisco avant de commencer cette étape !
Dans les menus de gauche, Cliquer sur "Devices" et cliquer sur "Add"
Description: nom_community_routeur nom_routeur
Hostname: ip_routeur
Host Template: Cisco Router (même si c'est un switch)
SNMP Version: Version 2
SNMP Community: nom_community_routeur
Cliquer sur "save"
Aller en dessous sous "Associated Data Queries"
y ajouter la query SNMP "SNMP - Interface Statistics" (peut-être elle y sera déjà)
Aller à la page de création de graphiques
Lors de la génération des graphiques, prendre ceux dont les interfaces sont up uniquement
Ajouter autant d'équipement Cisco que vous voulez en répétant cette étape.

Annexe 5 : Configuration de Netflow sur un équipement Cisco

Etape 1: Activer le protocole netflow sur une interface

```
R1(Config)#int fax/x
R1(Config-if)#ip route-cache flow
R1(Config-if)#ip flow ingress
R1(Config-if)#ip flow egress
R1(Config-if)#exit
```

Avec la commande ip route-cache flow qui active netflow, les flux affichés par Nfsen sont erronés, on va alors la remplacer par les deux commandes ip flow ingress et egress. Il existe plusieurs articles sur le net qui explique la différence entre ces deux méthodes.

Etape 2: Configurer netflow (version 9)

```
R1(Config)#ip flow-export version 9
```

Configurer le routeur pour envoyer les données vers nfsen et choisir le port (9995):

```
R1(Config)#ip flow-export destination <addresseIP_nfsen>
<port_utilisé>
R1(Config)#ip flow-export source fa0/0
```

Etape 3: Gérer les timers du cache (ETAPE TRES IMPORTANTE)

On autorise ici les flow actif à rester en cache 1 minute et les flow inactif à rester 15 minutes en cache avant de les supprimer

```
R1(Config)#ip flow-cache timeout active 1
R1(Config)#ip flow-cache timeout inactive 15
```

Cette commande est très importante puisque si vous oubliez de la configurer sur le routeur Cisco, par défaut, il va exporter les flow chaque 30 minutes ou lorsque le cache soit remplis. Cela peut donner des résultats très inattendus sur Nfsen.

Etape 4 (Facultative): Configurer l'échantillonnage

Créer un groupe d'échantillonnage Netflow et décider de la valeur d'échantillonnage en spécifiant le taux d'échantillonnage (1/n paquets à échantillonner) ou n {1 : 65'535}. Finalement, assigner le groupe d'échantillonnage à une interface

```
Router(config)# flow-sampler-map mysampler1
Router(config-sampler)#mode random one-out-of n
Router(config-sampler)#exit
Router(config)#interface fa0/1
Router(config-if)#flow-sampler mysampler1
```

Vérification:

```
R1#sh ip cache flow
```

Annexe 6 : Configuration de Nfsen (Netflow)

Configuration réalisée sur Ubuntu 12.04

Etape 1: Installer les dépendances

```
sudo apt-get install gcc flex librrd-dev make
sudo apt-get install apache2 libapache2-mod-php5 php5-common
sudo apt-get install libmailtools-perl rrdtool rrdtool-dbg
```

Etape 2: Définir les proxys

Laisser vide entre "=" et ";" si on n'en a pas

```
mkdir /home/src
cd /home/src
http_proxy=proxyhes.etat-ge.ch:80;export http_proxy
ftp_proxy=proxyhes.etat-ge.ch:80;export ftp_proxy
```

Etape 3: Installation de Nfdump et Nfsen

```
cd /home/src/
sudo wget http://sourceforge.net/projects/nfdump/files/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
sudo tar zxvf nfdump-1.6.13.tar.gz
cd nfdump-1.6.13
sudo ./configure --enable-nfprofile
sudo make
sudo make install

cd /home/src/
sudo wget http://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.6p1/nfsen-1.3.6p1.tar.gz
sudo tar zxvf nfsen-1.3.6p1.tar.gz
```

Etape 3.1 : Installation du module PERL manuellement

```
cd nfsen-1.3.6p1
perl -MCPAN -e 'install Socket6'
      répondre non à l'installation automatique
      déterminer les proxys et l'utilisateur, (laisse vide dans le proxy si on n'en a pas)
      choisir http://mirror.switch.ch/ftp/mirror/CPAN/ comme mirror site
      Laisser tout le reste par défaut en cliquant enter
```

Si on s'est trompé dans la config, allé sous /home/cisco/.cpan/CPAN/MyConfig.pm pour la modifier

Etape 3.2: Installer les modules PERL qui permettront d'envoyer des emails

L'étape du dessus doit s'être correctement déroulée pour installer ces modules.

installation de Mail::Header et Mail::Internet qui permettra de gérer les alertes email de Nfsen:

```
perl -MCPAN -e shell (on rentre dans la console MCPAN)
  install Mail::Header
  install Mail::Internet (Devrait déjà être installe)
  quit
```

Etape 4: Configuration de Nfsen

Creer le fichier nfsen.conf dans le répertoire /home/src/nfsen-1.3.6p1/etc/ à partir du fichier nfsen-dist.conf:

```
cd /home/src/nfsen-1.3.6p1/etc/
sudo cp nfsen-dist.conf  nfsen.conf
sudo gedit /etc/nfsen.conf

  #Changer le BASEDIR en le mettant sous: /home/nfsen et mettre wwwdir
  #dans /home/wwwdir (wwwdir existe pas, on l'ajoute)
  $BASEDIR = "/home/nfsen";
  $WWWDIR = "/home/wwwdir";

  #Configurer les groupes et utilisateurs
  $USER = "www-data";
  $WWWUSER = "www-data";
  $WWWGROUP = "www-data";
  #Configurer les équipements à ajouter à Nfsen
  %sources = (
  # 'upstream1'     => { 'port' => '9995', 'col' => '#0000ff', 'type'
=> 'netflow' },
    'nom_routeur1'  => { 'port' => '9995', 'col' => '#33FF33','IP' =>
'192.168.2.1' },
    'nom_routeur2'  => { 'port' => '9995', 'col' => '#0066FF', 'IP' =>
'192.168.1.1' },
  );
  #Autres config
  $syslog_facility = 'local7'; #configurer le local7 sur les routeurs
aussi
  $MAIL_FROM = 'example@mail.com'; #adresse depuis laquelle on va
pouvoir envoyer des mails
  $SMTP_SERVER = 'localhost';  #laisser localhost
Sauvegarder le fichier et quitter.
```

Etape 5: création de l'utilisateur netflow

Créer l'utilisateur netflow et ajouter les user netflow et www-data au groupe www-data

```
sudo useradd -m netflow
sudo passwd netflow
sudo adduser www-data www-data
sudo adduser netflow www-data
```

Vérifier le tout en consultant le fichier /etc/group

Etape 6: création du répertoire de nfsen (BASEDIR)

On ajoute d'avance les droits au dossier dans lequel nfsen va s'installer

```
mkdir -p /home/nfsen
chown www-data /home/nfsen
chgrp www-data /home/nfsen
mkdir -p /home/wwwdir
chown www-data /home/wwwdir
chgrp www-data /home/wwwdir
```

Etape 7: Installation et lancement de Nfsen

Installation de Nfsen après l'avoir configuré

```
cd /home/src/nfsen-1.3.6p1
sudo ./install.pl etc/nfsen.conf
```

Démarrer le Daemon Nfsen

```
cd /home/nfsen/bin
./nfsen start
```

Pour verifier qu'il est bien lancé:

sudo /home/nfsen/bin/nfsen status OU ps -ef | grep nfsen)

[sudo ./nfsen reconfig si le système nous le demande

si la commande ./nfsen reconfig bug, supprimmer les dossiers dans /home/nfsen/profiles-data/live avant de lancer la reconfig]

Il faut maintenant approximativement 5 minutes à Nfsen pour générer le tout, on va dans l'attente, configurer le serveur apache2

Etape 8 (facultative): Configurer le serveur avec Apache2

Créer le fichier de config basique pour le site Nfsen

```
cd /etc/apache2/site-available
sudo gedit nfsen (rajouter le VirtualHost)

<VirtualHost *:80>
    ServerName   www.nfsen.ch
    DocumentRoot   /var/www/nfsen
    DirectoryIndex   nfsen.php
```

```
    ErrorLog   /var/log/apache2/nfsen.error.log
    CustomLog   /var/log/apache2/nfsen.log   combined
    <Directory />
        Options   FollowSymLinks
        AllowOverride   none
    </Directory>
    <Directory   /var/www/nfsen>
        Options   FollowSymLinks
        AllowOverride   none
        Order   allow,deny
        allow   from   all
    </Directory>
</VirtualHost>
Sauvegarder et quitter.

cd /etc/apache2/sites-enabled
sudo mv  000-default 999-default (on renomme le lien symbolique)
sudo ln -s ../sites-available/nfsen 001-nfsen (on cree un lien
symbolique pr nfsen)
```

Etape 8.1: Configuration des hosts et du hostname

Vérifier la configuration des fichiers etc/hosts et etc/hostname.

```
Sudo gedit /etc/hosts
  127.0.0.1 localhost
  192.168.2.48 ubuntu www.nfsen.ch
Sauvegarder et quitter
Sudo gedit /etc/hostname
#il faut avoir au moins un nom dans ce fichier
  Ubuntu
Sauvegarder et quitter
```

Redémarrer le tout pour prendre en compte les modifications apache

```
sudo service apache2 reload
```

Etape 9: Démarrer Nfsen

Il faut au préalable avoir configuré les équipements Cisco pour qu'ils envoient du trafic Netflow (Voir **Annexe 5**)

Ouvrir un browser => www.nfsen.ch OU 192.168.2.48/nfsen/nfsen.php

Aller sous l'onglet détail, sélectionner un routeur et cliquer sur le bouton « process »

Si des données s'affichent, tout est bon sinon observer l'erreur qui s'affiche et:

Vérifier que les 5 minutes de l'étape 5 sont passées,

Aller dans le répertoire des profiles-data et sous la date du jour il va falloir ajouter le nfcapd.xxxxx qui s'affiche sur l'interface web

```
cd /home/nfsen/profiles-data/live/Rt-client/2015/mois_en_chiffre/jour_en_chiffre
```

On copie le premier nfcapd du dossier et lui donne le nom attendu:

```
sudo cp nfcapd.201510071535 nfcapd.201510080130
```

Le premier nfcapd.xx est celui du dossier dans lequel on se trouve (il peut y en avoir plusieurs, prendre le premier), le deuxième nfcapd.xx(celui qu'on veut copier) est celui demandé dans l'interface web, il n'existe pas alors on le créé

Cette étape doit uniquement être faite la première fois, si vous redémarrez Nfsen, attendre les 5 minutes de génération et tout sera OK.

Etape 10: Faire démarrer Nfsen automatiquement au démarrage

```
sudo ln -s /home/nfsen/bin/nfsen /etc/init.d/nfsen
sudo update-rc.d nfsen defaults 20
```

Redémarrer l'ordinateur et vérifier que Nfsen s'est bien lancé avec une des 2 commandes suivantes:

sudo /home/nfsen/bin/nfsen status OU ps -ef | grep nfsen

Annexe 7 : Configuration du Syslog sur un équipement Cisco

Etape 1: Configurer les heures des équipements

```
R1(config)#clock timezone MET 1
R1(config)#clock summer-time eet recurring last sun mar 2:00 last sun oct 3:00
R1(config)#ntp server 2.ch.pool.ntp.org / 77.245.18.26 (serveur ntp suisse)
R1(config)# service timestamps debug datetime localtime
R1(config)# service timestamps log datetime localtime
```

Etape 2: Activer et configurer le Syslog

On va indiquer le serveur syslog auquel envoyer les logs et spécifier le niveau de sévérité désiré

```
R1(config)#logging on
R1(config)#logging host ip_serveur_syslog
R1(config)#logging trap debugging / 7 (spécifie le niveau de sévérité qu'on veut voir apparaitre dans les logs)
R1(config)#logging facility local7 (on configure l'étiquette associée à chaque message, ici local7)
R1(config)#end
```

Commandes supplémentaires : Allouer un espace pour stocker les logs sur le routeur OU supprimer les logs du routeur et ne les envoyer qu'au serveur

```
R1(config)#logging buffered 4096 7
R1(config)#no logging console
```

Vérification:

```
Router#show logging
```

N'affichera rien si on a lancé la commande "no logging console"

Les différents niveaux de sévérité:

Emergency: 0
Alert: 1
Critical: 2
Error: 3
Warning: 4
Notice: 5
Informational: 6
Debugging: 7

☞ Si on sélectionner le niveau 5, on ne verra que les niveaux <= 5 dans les logs et ainsi de suite.

Annexe 8 : Installation du serveur Syslog

Configuration réalisée sur Ubuntu 12.04

Etape 1: Installer Syslog (sysklogd)

```
sudo apt-get install sysklogd
```

Etape 2: Accepter les connexions distantes au serveur

Changer la ligne du fichier syslogd 'SYSLOGD=""' par 'SYSLOGD="-r"' pour permettre à syslog de recevoir les logs des hôtes distant)

```
sudo gedit /etc/default/syslogd
      SYSLOGD="-r"
Enregistrer et quitter
sudo service sysklogd restart
```

Etape 3 (facultative): Afficher le nom de l'équipement plutôt que l'IP

Il faut ajouter dans la table les IP des équipements avec leur nom :

```
sudo gedit /etc/hosts
#Exemple
  192.168.1.1     Rt-client
  192.168.1.3     Rt-blabla
```

Etape 4: Consulter les logs du fichier syslog

Permet de voir les mouvements du fichier syslog en live sur la console

```
sudo tail -f /var/log/syslog
```

On peut aussi simplement consulter le fichier log :

```
 sudo gedit /var/log/syslog
```

Pour vérifier que les logs sont bien envoyé, effectuer du trafic sur un équipement cisco pour y voir du mouvement, ex: shut/no shut une interface (le routeur doit avoir la config syslog, voir **annexe 7**) et constater que les messages arrivent bien dans les logs.

Etape 5 : configurer le logrotate pour créer un file de log par jour

```
Sudo gedit /etc/logrotate.d/syslog
  /var/log/syslog {
        daily
         rotate 7
        compress
        delaycompress
        missingok
        notifempty
         create 644 root root
        }
sauvegarder et quitter.
sudo chmod 644 /etc/logrotate.d/syslog
sudo chown root.root /etc/logrotate.d/syslog
```

Annexe 9 : Configuration de storm control sur un équipement Cisco

Etape 1: Configurer les seuils du storm control

```
S2(config)# interface0/1
S2(config-if)# storm-control broadcast level 75 70
S2(config-if)# storm-control multicast pps 755 700
S2(config-if)# storm-control unicast bps 7.5m 7m
```

Ci-dessus sont représentées les trois variantes possibles à savoir : le pourcentage de bande passante, les paquets par secondes, les bits par seconde

Etape 2A : Configurer l'action trap

Configures traffic storm control to generate an SNMP trap when a storm is detected on the port.

```
S2(config)# interface0/1
S2(config-if)# storm-control action trap
S2(config-if)# exit
S2(config)# snmp-server enable traps storm-control trap-rate 0
```

On autorise SNMP à envoyer des trap storm-control chaque fois qu'il en détecte une avec la dernière commande

Etape 2B : Configurer l'action shutdown et l'errdisable

```
S2(config-if)# storm-control action shutdown
Configurer errdisable recovery pour que le port se réactive tout seul s'il tombe
S2(config)#errdisable recovery cause all
S2(config)#errdisable recovery interval 300
```

Ici, errdisable va permettre de réactiver les interfaces shutdown chaque intervalle de 300 secondes

Idéalement, il faudrait configurer qu'une seul des étapes 2A et 2B.

Commandes de vérification :

```
Router#show run int fa0/1
Router#show storm-control fa0/1
Router#show storm-control history
```

Annexe 10 : Configuration de Postfix

Configuration réalisée sur Ubuntu 12.04

Etape 1: Installation de Postfix et des dépendances

```
sudo apt-get update
sudo apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules
Lors de l'installation:
      choisir "Internet site"
      mail.exemple.com (ça n'a pas d'importance)
```

Etape 2: Configuration

!! Cette configuration est pour une adresse Gmail !!

```
cd /etc/postfix
sudo gedit main.cf
  #On indique le serveur SMTP de Gmail et son port
  #On peut également utiliser le port 25 ou 465
  relayhost = [smtp.gmail.com]:587
  #On active l'authentification et on indique ou se trouve le fichier sasl_passwd
  smtp_sasl_auth_enable = yes
  smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
  smtp_sasl_security_options = noanonymous
  smtp_tls_CAfile = /etc/postfix/cacert.pem
  smtp_use_tls = yes
  smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
  broken_sasl_auth_clients = yes
Sauvegarder et quitter
```

Il faut maintenant préciser l'adresse Gmail d'où on veut que les mails partent

```
sudo gedit /etc/postfix/sasl_passwd
  [smtp.gmail.com]:587  mon_adresse@gmail.com:mon_password_gmail
Sauvegarder et quitter
```

On va changer les droits du fichier puisqu'on a écrit notre mot de passe en clair

```
sudo chmod 400 /etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd
```

Etape 3: Configuration du certificat SSL

On redirige le certificat dans le fichier /etc/postfix/cacert.pem et on reload postfix pour prendre en compte les modifications

```
cat /etc/ssl/certs/Thawte_Premium_Server_CA.pem | sudo tee -a /etc/postfix/cacert.pem


sudo /etc/init.d/postfix reload
```

Etape 4: Autoriser Gmail pour accepter les applications moins sécurisées

Se connecter à son compte Gmail et aller dans les paramètres

Cliquer sur l'onglet "Comptes et importation"

Sous "Modifier les paramètres du compte" cliquer sur "Autres paramètres de votre compte Google"

Une nouvelle page s'ouvre, sous Connexion et sécurité cliquer sur "Applications et sites connectés"

Une nouvelle page s'ouvre, tout en bas, activer "Autoriser les applications moins sécurisées"

Etape 5: Tester le tout

Lancer cette commande pour vous envoyer un mail

```
echo "Test mail from postfix" | mail -s "Test Postfix" adresse@mail.com
```

"adresse@mail.com" est la personne qui recevra le mail

Connectez-vous à l'adresse émail et vérifier que le mail a bien été reçu

Annexe 11 : Filtrer le Syslog sous Linux

Configuration réalisée sur Ubuntu 12.04

Etape 1: Créer les fichiers qui vont contenir l'information filtrée

```
cd /var/log (Idéalement, on les créé au même endroit que les logs)
sudo vi syslog.rt-pat
sudo vi syslog.storm-control
```

Ici on a créé 2 fichiers, un qui va par exemple récolter tous les messages du routeur « Rt-PAT » et l'autre qui va récolter les informations relatives au Storm control

Etape 2: Création du script:

On doit d'abord se rendre sous init.d pour créer le script. Ensuite il faudra lui donner les droits d'exécution, enfin il faudra lui dire de démarrer au démarrage et redémarrer l'ordinateur

```
cd /etc/init.d/
sudo vi logs-syslog.sh
  #!/bin/bash
  # capture de texte du fichier /var/log/syslog
  for (( ; ; ))
  do
    cat /var/log/syslog | grep Rt-PAT > /var/log/syslog.rt-pat
    cat /var/log/syslog | grep storm-control > /var/log/syslog.storm-
control
  done
enregistrer le fichier et le quitter

sudo chmod +x logs-distant.sh
sudo update-rc.d logs-syslog.sh defaults
sudo init 6 (réinitialise l'ordinateur)
```

Etape 3: Envoyer les logs par email

Envoyer les logs par email sous forme de fichier txt

```
sudo apt-get install mutt
echo "Ci-joint les logs du routeur rt-pat" | mutt -s "Les logs rt-pat"
-a /var/log/syslog.rt-pat – mon_adresse@mail.com
```

« -s » défini l'objet du message, mutt permet d'encoder le fichier syslog.rt-pat afin de l'envoyer sous forme de fichier .txt

Envoyer les logs par email en texte brut:

```
cat mon_fichier | mail -s "ceci est le sujet" mon_adresse@mail.com
```

Annexe 12 : Configuration des équipements du schéma n°1

Configuration du routeur Rt-Client :

```
sh run
Building configuration...

Current configuration : 3260 bytes
!
! No configuration change since last restart
!
version 12.2
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname Rt-Client
!
logging queue-limit 100
logging buffered 4096 debugging
enable secret 5 $1$8JTA$5xZO23b4/HcMHpVOL7dRl.
!
memory-size iomem 10
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
ip subnet-zero
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
location LOCATION_RT-CLIENT
!
interface Loopback0
 ip address 192.168.4.2 255.255.255.255
!
interface FastEthernet0/0
 description liaison vers PC HEG918 sur carte mere
 ip address 192.168.1.1 255.255.255.192
 ip helper-address 192.168.0.1
 duplex auto
 speed auto
!
interface Serial0/0
 description liaison vers Rt-PAT sur s0/0
 ip address 192.168.0.2 255.255.255.192
 ip route-cache flow
 clockrate 1000000
 no fair-queue
!
interface FastEthernet0/1
 description liaison vers PC cisco-td-08 sur carte mere
 ip address 192.168.1.65 255.255.255.192
 ip helper-address 192.168.0.1
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
```

```
 shutdown
!
ip http server
ip flow-export source Serial0/0
ip flow-export version 5
ip flow-export destination 192.168.2.48 9995
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
ip route 192.168.2.0 255.255.255.192 192.168.0.1
!
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
!
snmp-server community lab1 RO 10
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server chassis-id CHASSIS_RT-CLIENT
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps cnpd
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-
message
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps atm subif
snmp-server enable traps pppoe
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps voice poor-qov
snmp-server enable traps dnis
snmp-server enable traps xgcp
snmp-server host 192.168.2.48 version 2c lab1
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 password 7 05080F1C2243
 login
!
ntp clock-period 17208535
ntp server 82.220.2.2
ntp server 5.148.175.134
```

```
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
ntp server 212.147.10.180
!
end

Rt-Client#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.2 is directly connected, Loopback0
     192.168.0.0/26 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Serial0/0
     192.168.1.0/26 is subnetted, 1 subnets
C       192.168.1.64 is directly connected, FastEthernet0/1
     192.168.2.0/26 is subnetted, 1 subnets
S       192.168.2.0 [1/0] via 192.168.0.1
S*   0.0.0.0/0 [1/0] via 192.168.0.1
Rt-Client#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            192.168.1.1     YES NVRAM  up
down
Serial0/0                  192.168.0.2     YES NVRAM  up                    up
FastEthernet0/1            192.168.1.65    YES NVRAM  up                    up
Serial0/1                  unassigned      YES NVRAM  administratively down
down
Serial0/2                  unassigned      YES NVRAM  administratively down
down
Virtual-Access1            unassigned      YES unset  up                    up
Loopback0                  192.168.4.2     YES NVRAM  up                    up
Rt-Client#sh access-lists
Standard IP access list 10
    10 permit 192.168.2.48 (16092 matches)
    20 deny   any log
Rt-Client#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab1      security model: v2c

Rt-Client#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active

Community name: lab1
Community Index: cisco1
Community SecurityName: lab1
storage-type: nonvolatile        active access-list: 10
```

onfiguration du routeur Rt-PAT :

```
sh run
Building configuration...

Current configuration : 5693 bytes
!
! Last configuration change at 09:43:28 MET Wed Nov 18 2015
! NVRAM config last updated at 10:00:45 MET Thu Nov 19 2015
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname Rt-PAT
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 informational
enable secret 5 $1$YR5H$tZl8GhNY2dd0mMCagW64J0
!
no aaa new-model
memory-size iomem 10
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool CLIENTS
   network 192.168.1.0 255.255.255.192
   default-router 192.168.1.1
   dns-server 8.8.8.8
   domain-name client.ch
!
ip flow-cache timeout active 1
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
flow-sampler-map mysampler1
 mode random one-out-of 100
!
interface Loopback0
 ip address 192.168.4.1 255.255.255.255
!
interface FastEthernet0/0
 description liaison vers le reseau externe
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/0
 description liaison vers Rt-Client sur s0/0
 ip address 192.168.0.1 255.255.255.192
 ip nat inside
 ip virtual-reassembly
 no fair-queue
!
interface FastEthernet0/1
 description liaison vers server HEG883 sur carte mere
```

```
 ip address 192.168.2.1 255.255.255.192
 ip flow ingress
 ip flow egress
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 flow-sampler mysampler1
!
interface Serial0/1
 no ip address
 shutdown
!
ip forward-protocol nd
ip route 192.168.1.0 255.255.255.0 192.168.0.2
!
ip flow-export source FastEthernet0/1
ip flow-export version 9
ip flow-export destination 192.168.2.48 9995
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/0 overload
!
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 1 permit 192.168.2.0 0.0.0.63
access-list 1 permit 192.168.1.0 0.0.0.63
access-list 1 permit 192.168.0.0 0.0.0.63
access-list 1 permit 192.168.1.64 0.0.0.63
access-list 50 permit 192.168.2.48
access-list 50 deny   any log
snmp-server community lab1 RO 10
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server location location_Rt-PAT
snmp-server ip dscp 26
snmp-server contact lab1.com
snmp-server chassis-id CHASSIS_Rt-PAT
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps xgcp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps atm subif
snmp-server enable traps bgp
snmp-server enable traps bstun
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps dial
snmp-server enable traps dlsw
snmp-server enable traps dsp card-status
snmp-server enable traps entity
```

```
snmp-server enable traps event-manager
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-
old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-
message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server enable traps stun
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps vtp
snmp-server enable traps director server-up server-down
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps voice poor-qov
snmp-server enable traps voice fallback
snmp-server enable traps dnis
snmp-server host 192.168.2.48 version 2c lab1
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password 7 104D000A0618
 login
!
ntp clock-period 17207817
ntp server 82.220.2.2
ntp server 5.148.175.134
ntp server 82.197.164.46
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
!
end

Rt-PAT#sh dhcp lease
Temp IP addr: 172.18.67.155  for peer on Interface: FastEthernet0/0
Temp  sub net mask: 255.255.255.192
```

```
   DHCP Lease server: 172.18.67.129, state: 3 Bound
   DHCP transaction id: 73A
   Lease: 259200 secs,  Renewal: 129600 secs,  Rebind: 226800 secs
Temp default-gateway addr: 172.18.67.129
   Next timer fires after: 03:31:21
   Retry count: 0   Client-ID: cisco-000d.ed19.20a0-Fa0/0
   Client-ID hex dump: 636973636F2D303030642E656431392E
                       323061302D4661302F30
   Hostname: Rt-PAT
Rt-PAT#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.1 is directly connected, Loopback0
     192.168.0.0/26 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Serial0/0
S    192.168.1.0/24 [1/0] via 192.168.0.2
Rt-PAT#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            172.18.67.155   YES DHCP   up
down
Serial0/0                  192.168.0.1     YES NVRAM  up                    up
FastEthernet0/1            192.168.2.1     YES NVRAM  up
down
Serial0/1                  unassigned      YES NVRAM  administratively down
down
NVI0                       unassigned      NO  unset  up                    up
Loopback0                  192.168.4.1     YES NVRAM  up                    up
Rt-PAT#sh access-lists
Standard IP access list 1
    10 permit 192.168.2.0, wildcard bits 0.0.0.63 (12659 matches)
    20 permit 192.168.1.0, wildcard bits 0.0.0.63 (5196 matches)
    30 permit 192.168.0.0, wildcard bits 0.0.0.63 (817 matches)
    40 permit 192.168.1.64, wildcard bits 0.0.0.63 (1290 matches)
Standard IP access list 50
    10 permit 192.168.2.48
    20 deny   any log
Rt-PAT#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab1      security model: v2c

Rt-PAT#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active

Community name: lab1
Community Index: cisco1
Community SecurityName: lab1
storage-type: nonvolatile        active access-list: 10
```

Annexe 13 : Configuration des équipements du schéma n°2

Configuration du routeur R1 :

```
sh run
Building configuration...

Current configuration : 3469 bytes
!
! Last configuration change at 09:43:42 MET Thu Nov 19 2015
! NVRAM config last updated at 09:57:08 MET Thu Nov 19 2015
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096
enable secret 5 $1$x8UL$pxGGeeLZHHTm.qGbDc8Lg1
!
no aaa new-model
memory-size iomem 10
clock timezone MET 1
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool client-switch
   network 192.168.1.0 255.255.255.192
   dns-server 8.8.8.8
   domain-name clientswitch.ch
   default-router 192.168.1.1
!
multilink bundle-name authenticated
!
!
flow-sampler-map mysampler1
 mode random one-out-of 100
!
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 192.168.4.1 255.255.255.255
!
interface FastEthernet0/0
 description liaison vers serveur HEG883 sur carte mere
 ip address 192.168.2.2 255.255.255.192
 ip flow ingress
 ip flow egress
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
```

```
 flow-sampler mysampler1
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0/0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet0/1
 description liaison vers S3 sur fa0/7
 ip address 192.168.1.1 255.255.255.192
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Ethernet1/0
 description liaison vers le reseau externe
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 half-duplex
!
ip forward-protocol nd
!
ip flow-cache timeout active 1
ip flow-export source FastEthernet0/0
ip flow-export version 9
ip flow-export destination 192.168.2.48 9995
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet1/0 overload
!
ip sla responder udp-echo port 5000
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 1 permit 192.168.1.0 0.0.0.63
access-list 1 permit 192.168.2.0 0.0.0.63
access-list 10 permit 192.168.2.48
snmp-server community lab2 RO 10
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server location LOCATION_R1
snmp-server chassis-id CHASSIS_R1
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps envmon
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
```

```
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server host 192.168.2.48 version 2c lab2
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password 7 030752180500
 login
!
ntp clock-period 17180082
ntp server 82.220.2.2
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
!
end

R1#sh dhcp lease
Temp IP addr: 172.18.67.154  for peer on Interface: Ethernet1/0
Temp  sub net mask: 255.255.255.192
   DHCP Lease server: 172.18.67.129, state: 5 Bound
   DHCP transaction id: 8AB
   Lease: 259200 secs,  Renewal: 129600 secs,  Rebind: 226800 secs
Temp default-gateway addr: 172.18.67.129
   Next timer fires after: 1d05h
   Retry count: 0   Client-ID: cisco-000b.fdd8.3e90-Et1/0
   Client-ID hex dump: 636973636F2D303030622E666464382E
                       336539302D4574312F30
   Hostname: R1
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.18.67.129 to network 0.0.0.0

     172.18.0.0/26 is subnetted, 1 subnets
C       172.18.67.128 is directly connected, Ethernet1/0
     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.1 is directly connected, Loopback0
     192.168.1.0/26 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/1
     192.168.2.0/26 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 172.18.67.129
R1#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            192.168.2.2     YES NVRAM  up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down
down
BRI0/0                     unassigned      YES NVRAM  administratively down
down
BRI0/0:1                   unassigned      YES unset  administratively down
```

```
down
BRI0/0:2                   unassigned      YES unset  administratively down
down
FastEthernet0/1            192.168.1.1     YES NVRAM  up                    up
Serial0/1                  unassigned      YES NVRAM  administratively down
down
Ethernet1/0                172.18.67.154   YES DHCP   up                    up
NVI0                       192.168.4.1     YES unset  up                    up
Loopback0                  192.168.4.1     YES NVRAM  up                    up
R1#sh access-lists
Standard IP access list 1
    10 permit 192.168.1.0, wildcard bits 0.0.0.63 (30062 matches)
    20 permit 192.168.2.0, wildcard bits 0.0.0.63 (46709 matches)
Standard IP access list 10
    10 permit 192.168.2.48 (6302 matches)
R1#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab2      security model: v2c

R1#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active


Community name: lab2
Community Index: cisco1
Community SecurityName: lab2
storage-type: nonvolatile        active access-list: 10
```

Configuration du switch S1 :

```
sh run
Building configuration...

Current configuration : 3212 bytes
!
! Last configuration change at 16:42:50 MET Tue Nov 17 2015
! NVRAM config last updated at 16:43:18 MET Tue Nov 17 2015
!
version 12.1
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname S1
!
enable secret 5 $1$WjD7$G0attaYJBs8WdmE/BRHFI1
!
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
interface FastEthernet0/1
```

```
 description liaison vers S2 sur fa0/1
 speed 100
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 description liaison vers client HEG918 sur carte mere
 speed 100
!
interface Vlan1
 ip address 192.168.1.10 255.255.255.192
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
snmp-server community lab2 RO 10
snmp-server ifindex persist
snmp-server trap-source Vlan1
snmp-server location LOCATION_S1
snmp-server ip dscp 26
snmp-server chassis-id CHASSIS_S1
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps config
snmp-server enable traps copy-config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps bridge
snmp-server enable traps stpx
snmp-server enable traps rtr
snmp-server enable traps c2900
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps MAC-Notification
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps hsrp
snmp-server enable traps cluster
snmp-server enable traps vlan-membership
snmp-server host 192.168.2.48 version 2c lab2
!
line con 0
line vty 0 4
 password 7 070C285F4D06
 login
line vty 5 15
 login
!
ntp clock-period 17179979
ntp server 82.220.2.2
ntp server 77.245.18.26
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 217.147.208.1
```

```
ntp server 91.234.160.19
ntp server 192.33.214.47
!
end

S1#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
Vlan1                      192.168.1.10    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES unset  up                    up
FastEthernet0/2            unassigned      YES unset  administratively down
down
FastEthernet0/3            unassigned      YES unset  administratively down
down
FastEthernet0/4            unassigned      YES unset  administratively down
down
FastEthernet0/5            unassigned      YES unset  up                    up
S1#sh access-lists
Standard IP access list 10
    permit 192.168.2.48 (460 matches)
    deny   any log
S1#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab2      security model: v2c

S1#sh snmp community

Community name: lab2
Community Index: lab2
Community SecurityName: lab2
storage-type: nonvolatile        active access-list: 10
```

Configuration du switch S2 :

```
sh run
Building configuration...

Current configuration : 6944 bytes
!
! Last configuration change at 08:59:33 MET Thu Nov 19 2015
! NVRAM config last updated at 08:59:47 MET Thu Nov 19 2015
!
version 12.2
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname S2
!
enable secret 5 $1$fAFN$eIcx5ySb3yXldyn6QHNIp.
!
no aaa new-model
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
```

```
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause unicast-flood
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause link-monitor-failure
errdisable recovery cause oam-remote-failure
errdisable recovery cause loopback
ip subnet-zero
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 description liaison vers S1 sur fa0/1
 switchport mode dynamic desirable
 speed 100
 storm-control broadcast level 80.00 75.00
 storm-control multicast level 80.00 75.00
 storm-control unicast level 80.00 75.00
 storm-control action trap
!
interface FastEthernet0/2
 switchport mode dynamic desirable
 shutdown
!
interface FastEthernet0/3
 description liaison vers S3 sur fa0/3
 switchport mode dynamic desirable
 speed 10
 storm-control broadcast level 80.00 75.00
 storm-control multicast level 80.00 75.00
 storm-control unicast level 80.00 75.00
 storm-control action trap
!
interface FastEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface Vlan1
 ip address 192.168.1.9 255.255.255.192
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip classless
ip http server
ip http secure-server
!
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
snmp-server community lab2 RO 10
snmp-server trap-source Vlan1
snmp-server location LOCATION_S2
snmp-server ip dscp 26
snmp-server chassis-id CHASSIS_S2
snmp-server enable traps snmp authentication linkdown linkup coldstart
```

```
warmstart
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps vtp
snmp-server enable traps flash insertion removal
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mac-notification
snmp-server enable traps vlan-membership
snmp-server host 192.168.2.48 version 2c lab2
snmp ifmib ifindex persist
!
control-plane
!
line con 0
line vty 0 4
 password 7 030752180500
 login
line vty 5 15
 login
!
ntp clock-period 17180243
ntp server 82.220.2.2
ntp server 77.245.18.26
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
ntp server 212.147.10.180
end

S2#sh ip int brief
Interface              IP-Address      OK? Method Status
Protocol
Vlan1                  192.168.1.9     YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  up                    up
S2#sh access-lists
Standard IP access list 10
    10 permit 192.168.2.48 (5920 matches)
    20 deny   any log
S2#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab2      security model: v2c

S2#sh snmp community

Community name: lab2
Community Index: lab2
Community SecurityName: lab2
storage-type: nonvolatile        active access-list: 10
```

Configuration du switch S3 :

```
sh run
Building configuration...

Current configuration : 5910 bytes
!
! Last configuration change at 17:37:09 MET Tue Nov 17 2015
! NVRAM config last updated at 17:49:05 MET Tue Nov 17 2015
!
version 15.0
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$X5dS$EzdtIdtZkVTN1f.AUV.N2.
!
no aaa new-model
clock timezone MET 1 0
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
system mtu routing 1500
!
no setup express
!
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig (STP)
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery cause small-frame
errdisable recovery cause psp
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 description liaison vers S2 sur fa0/3
 speed 10
 storm-control broadcast level bps 8.0m 7.5m
```

```
 storm-control multicast level bps 8.0m 7.5m
 storm-control unicast level bps 8.0m 7.5m
 storm-control action trap
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 description liaison vers R1 sur fa0/1
 speed 100
 storm-control broadcast level 80.00 75.00
 storm-control multicast level 80.00 75.00
 storm-control unicast level 80.00 75.00
 storm-control action trap
!
interface FastEthernet0/8
 shutdown
!

interface Vlan1
 ip address 192.168.1.8 255.255.255.192
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
logging history debugging
logging trap debugging
logging host 192.168.2.48
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
snmp-server community lab2 RO 10
snmp-server trap-source Vlan1
snmp-server location LOCATION_S3
snmp-server ip dscp 26
snmp-server chassis-id CHASSIS_S3
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-
inconsistency
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.2.48 version 2c lab2
snmp ifmib ifindex persist
!
line con 0
line vty 0 4
 password 7 030752180500
 login
line vty 5 15
 login
!
ntp server 217.147.208.1
```

```
ntp server 82.220.2.2
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 91.234.160.19
ntp server 77.245.18.26
ntp server 192.33.214.47
ntp server 212.147.10.180
end

S3#sh ip int brief
Interface              IP-Address      OK? Method Status
Protocol
Vlan1                  192.168.1.8     YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  administratively down down
FastEthernet0/6        unassigned      YES unset  administratively down down
FastEthernet0/7        unassigned      YES unset  up                    up
S3#sh access-lists
Standard IP access list 10
    10 permit 192.168.2.48 (166 matches)
    20 deny   any log
S3#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab2      security model: v2c

S3#sh snmp community

Community name: lab2
Community Index: lab2
Community SecurityName: lab2
storage-type: nonvolatile        active access-list: 10
```

Annexe 14 : Configuration des équipements du schéma n°3

Configuration du routeur Rt-Client :

```
sh run
Building configuration...

Current configuration : 4654 bytes
!
! Last configuration change at 12:34:38 MET Fri Nov 20 2015
! NVRAM config last updated at 12:34:39 MET Fri Nov 20 2015
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname Rt-client
!
boot-start-marker
boot-end-marker
!
logging buffered 40996 debugging
enable secret 5 $1$jNbK$/85yaqGA.D3HsPMVfSseL/
!
no aaa new-model
memory-size iomem 10
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
no network-clock-participate slot 1
no network-clock-participate wic 0
ip cef
!
ip flow-cache timeout active 1
!
flow-sampler-map mysampler1
 mode random one-out-of 100
!
interface Loopback0
 ip address 192.168.4.2 255.255.255.255
!
interface FastEthernet0/0
 description liaison vers PC HEG918 sur carte mere
 ip address 192.168.1.1 255.255.255.192
 ip helper-address 192.168.0.3
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
```

```
 no ip address
 shutdown
!
interface Serial0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 description liaison vers Rt-PAT sur Ethernet1/0
 ip address 192.168.0.4 255.255.255.192
 ip route-cache flow
 half-duplex
 flow-sampler mysampler1
!
ip route 0.0.0.0 0.0.0.0 192.168.0.3
ip route 192.168.2.0 255.255.255.192 192.168.0.3
ip flow-export source Ethernet1/0
ip flow-export version 9
ip flow-export destination 192.168.2.48 9995
!
ip http server
no ip http secure-server
!
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
snmp-server community lab3 RO 10
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server location LOCATION_RT-CLIENT
snmp-server chassis-id CHASSIS_RT-CLIENT
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-
old
```

```
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-
message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps vtp
snmp-server enable traps atm subif
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps rtr
snmp-server host 192.168.2.48 version 2c lab3
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password 7 110A1016141D
 login
!
ntp clock-period 17208341
ntp server 82.220.2.2
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
!
end

Rt-client#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.0.3 to network 0.0.0.0

     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.2 is directly connected, Loopback0
     192.168.0.0/26 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Ethernet1/0
     192.168.1.0/26 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
     192.168.2.0/26 is subnetted, 1 subnets
S       192.168.2.0 [1/0] via 192.168.0.3
S*   0.0.0.0/0 [1/0] via 192.168.0.3
Rt-client#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
```

```
FastEthernet0/0            192.168.1.1     YES NVRAM  up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down
down
FastEthernet0/1            unassigned      YES NVRAM  administratively down
down
Serial0/1                  unassigned      YES NVRAM  administratively down
down
Serial0/2                  unassigned      YES NVRAM  administratively down
down
Serial0/3                  unassigned      YES NVRAM  administratively down
down
Ethernet1/0                192.168.0.4     YES NVRAM  up                    up
Loopback0                  192.168.4.2     YES NVRAM  up                    up
Rt-client#sh access-lists
Standard IP access list 10
    10 permit 192.168.2.48 (242 matches)
    20 deny   any log
Rt-client#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab3      security model: v2c

Rt-client#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active

Community name: lab3
Community Index: cisco1
Community SecurityName: lab3
storage-type: nonvolatile        active access-list: 10
```

Configuration du routeur Rt-PAT :

```
sh run
Building configuration...

Current configuration : 3981 bytes
!
! Last configuration change at 12:28:35 MET Fri Nov 20 2015
! NVRAM config last updated at 12:28:49 MET Fri Nov 20 2015
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Rt-PAT
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 $1$YR5H$tZl8GhNY2dd0mMCagW64J0
!
memory-size iomem 10
clock timezone MET 1
clock summer-time eet recurring last Sun Mar 2:00 last Sun Oct 3:00
no aaa new-model
ip subnet-zero
```

```
ip cef
!
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool CLIENTS
   network 192.168.1.0 255.255.255.192
   default-router 192.168.1.1
   dns-server 8.8.8.8
   domain-name cClient.ch
!
ip flow-cache timeout active 1
ip audit po max-events 100
!
interface Loopback0
 ip address 192.168.4.1 255.255.255.255
!
interface FastEthernet0/0
 description liaison vers le reseau externe
 ip address dhcp
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0/0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet0/1
 description liaison vers server HEG883 sur carte mere
 ip address 192.168.2.3 255.255.255.192
 ip nat inside
 ip flow ingress
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Ethernet1/0
 description liaison vers Rt-Client sur e1/0
 ip address 192.168.0.3 255.255.255.192
 ip nat inside
 half-duplex
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip classless
ip route 192.168.1.0 255.255.255.192 192.168.0.4
ip flow-export source FastEthernet0/1
ip flow-export version 9
ip flow-export destination 192.168.2.48 9995
ip http server
no ip http secure-server
!
logging history debugging
logging trap debugging
logging 192.168.2.48
access-list 1 permit 192.168.2.0 0.0.0.63
access-list 1 permit 192.168.1.0 0.0.0.63
access-list 1 permit 192.168.0.0 0.0.0.63
access-list 10 permit 192.168.2.48
access-list 10 deny   any log
```

```
!
snmp-server community lab3 RO 10
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server location LOCATION_RT-PAT
snmp-server chassis-id CHASSIS_RT-PAT
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps envmon
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-
message
snmp-server enable traps pppoe
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps atm subif
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps rtr
snmp-server host 192.168.2.48 version 2c lab3
!
line con 0
line aux 0
line vty 0 4
 password 7 104D000A0618
 login
!
ntp clock-period 17180239
ntp server 82.220.2.2
ntp server 5.148.175.134
ntp server 81.94.123.16
ntp server 217.147.208.1
ntp server 91.234.160.19
ntp server 192.33.214.47
!
end

Rt-PAT#sh dhcp lease
Temp IP addr: 172.18.67.158  for peer on Interface: FastEthernet0/0
Temp  sub net mask: 255.255.255.192
   DHCP Lease server: 172.18.67.129, state: 3 Bound
   DHCP transaction id: B2AA
   Lease: 259200 secs,  Renewal: 129600 secs,  Rebind: 226800 secs
Temp default-gateway addr: 172.18.67.129
```

```
   Next timer fires after: 1d11h
   Retry count: 0   Client-ID: cisco-0005.5edd.f500-Fa0/0
   Hostname: Rt-PAT
Rt-PAT#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.18.67.129 to network 0.0.0.0

     172.18.0.0/26 is subnetted, 1 subnets
C       172.18.67.128 is directly connected, FastEthernet0/0
     192.168.4.0/32 is subnetted, 1 subnets
C       192.168.4.1 is directly connected, Loopback0
     192.168.0.0/26 is subnetted, 1 subnets
C       192.168.0.0 is directly connected, Ethernet1/0
     192.168.1.0/26 is subnetted, 1 subnets
S       192.168.1.0 [1/0] via 192.168.0.4
     192.168.2.0/26 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [254/0] via 172.18.67.129
Rt-PAT#
.Nov 20 11:31:24.424: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/0 TDR=2, TRC=0
Rt-PAT#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            172.18.67.158   YES DHCP   up                    up
Serial0/0                  unassigned      YES NVRAM  administratively down
down
BRI0/0                     unassigned      YES NVRAM  administratively down
down
BRI0/0:1                   unassigned      YES unset  administratively down
down
BRI0/0:2                   unassigned      YES unset  administratively down
down
FastEthernet0/1            192.168.2.3     YES NVRAM  up                    up
Serial0/1                  unassigned      YES NVRAM  administratively down
down
Ethernet1/0                192.168.0.3     YES NVRAM  up                    up
Loopback0                  192.168.4.1     YES NVRAM  up                    up
Rt-PAT#sh access-lists
Standard IP access list 1
    10 permit 192.168.2.0, wildcard bits 0.0.0.63 (628 matches)
    20 permit 192.168.1.0, wildcard bits 0.0.0.63 (589 matches)
    30 permit 192.168.0.0, wildcard bits 0.0.0.63 (80 matches)
Standard IP access list 10
    10 permit 192.168.2.48 (244 matches)
    20 deny   any log
Rt-PAT#sh snmp host
Notification host: 192.168.2.48 udp-port: 162   type: trap
user: lab3      security model: v2c

Rt-PAT#sh snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only  active

Community name: lab3
Community Index: cisco1
Community SecurityName: lab3
storage-type: nonvolatile        active access-list: 10
```