Le Net du Kermeur
Monitoring réseau

Présentation du réseau

Statut associatif

Comité des Fêtes du Kermeur

Association locale depuis 1961

Le Kermeur est un quartier d'une commune de 3000h.

Installation initiale par Alsatis en 2005

Satellite + Wifi en mode infrastructure sur une zone blanche ADSL

13 abonnés, une seule AP – Financement DATAR, Morlaix Communauté

Débit max abonné : 512 Kbps download, 128 Kbps upload

Evolution en 2006

Liaison spécialisée Oléane

AP principale passe en Mikrotik RB532 sous Openwrt

35 abonnés, cinq relais, étendue géographique 15 x 5 km

Débit max abonné : 2 Mbps download, 512 Kbps upload

Equipements centraux

AP Mikrotik RB532

Openwrt Kamikaze (Mips) sur carte flash (RouterOS conservé en Nand)

Deux passerelles (M0n0wall, pfSense, base FreeBSD)

PC avec des cartes flash au lieu du disque dur

Serveur PC sous Netbsd

Apache, Mysql, Php, Cacti, ...
Scripts de maintenance

Serveur Powermac G4 sous Debian

Mail : Exim, Spamassassin, Clamav, serveur Pop
Collecte des logs de connexion

Liaison wifi dédiée à la sauvegarde

PC avec carte flash, Openwrt Kamikaze (i386). AP de secours

Firmware des routeurs

40 routeurs, 34 WRT54G(L), 6 Buffalo WHRG54S

Firmware base OpenWrt WhiteRussian RC6

- Patch du wificonf, gestion du txpower de la RC4
- Intégration des packages suivants :
  - wl,
  - screen (avec libncurses)
  - snmpd
  - gpio de la RC4 au lieu du module diag.
- Répertoire /usr/local/bin (scripts locaux)
  - en autres, setupow.sh, lancé a la 1ère connexion

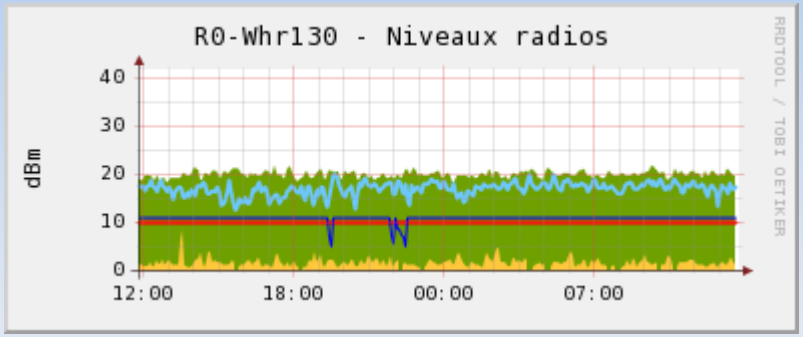
L'interface graphique du routeur est inutilisée

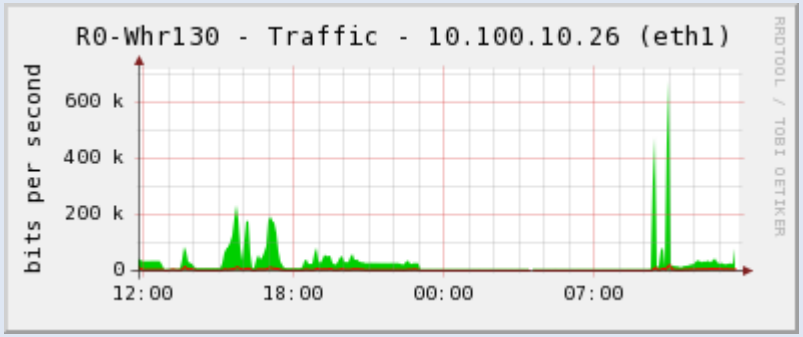
Modifications de configuration par SSH depuis la machine de maintenance

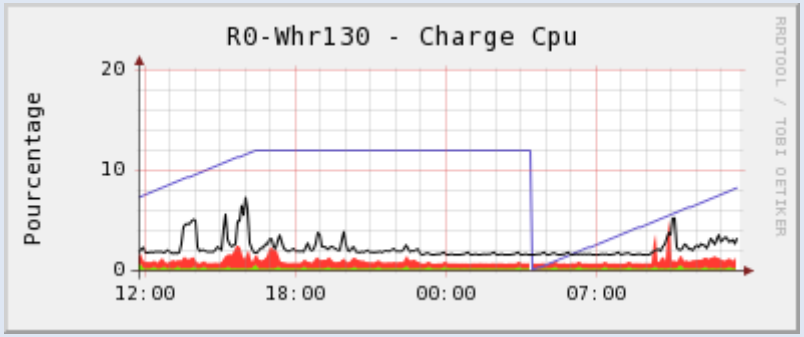
Le Net du Kermeur
Monitoring réseau

Les graphes

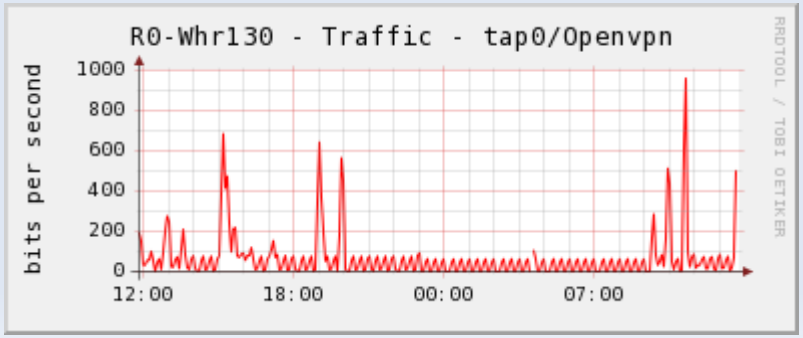
Pour chaque abonné







Optionnel :



Les outils

Cacti

Apache, Mysql, Php, Rrdtools

Relevé de mesures toutes les 5 minutes . Historique sur 1 an

Mysql

Table des routeurs

rt_name, rt_fonction (client, client/relais, relais),

rt_adresse_mac, rt_adresse_ip, rt_online

Snmp

En standard le trafic des interfaces

Extensions pour les niveaux radio, la charge CPU

Scripts shell

Alimentation pour cacti

Mise à jour de config, ...

Extensions SNMP sur le routeur

Exemple pour le rssi

Extrait du /etc/snmp/snmpd.conf :

```
...
exec    .1.3.6.1.2.1.2.2.1.53.  radio_rssi   /usr/local/bin/snmpradio.sh 53
..
```

Extraits du script snmpradio.sh :

```
if [ $1 -eq 53 ]; then
    RETVAL=$((96 - $(wl rssi | sed -e 's/^.* -\([0-9]\+\)$/\1/')))
    [ $RETVAL -lt 1 ] && RETVAL=0
fi
exit  $RETVAL
```

Test depuis la machine d'exploitation

```
snmpwalk -c public -v 1 routeur
```

Le Net du Kermeur
Monitoring réseau

Modèles de données dans Cacti

Data Templates Add

Search: Openwrt go clear

<< Previous Showing Rows 1 to 11 of 11 [1] Next >>

Template Name	Data Input Method	Status
OpenWrt 2.6 CPU Irq	Get SNMP Data	Active
Openwrt 2.6 CPU Soft_Irq	Get SNMP Data	Active
Openwrt 2.6 CPU Uptime	Get SNMP Data	Active
Openwrt Conntrack	Get SNMP Data	Active
Openwrt CPU System	Get SNMP Data	Active
Openwrt CPU User	Get SNMP Data	Active
Openwrt Noise	Get SNMP Data	Active
Openwrt Rssi	Get SNMP Data	Active
Openwrt Speed	Get SNMP Data	Active
Openwrt Txpower	Get SNMP Data	Active
Openwrt Uptime	Get SNMP Data	Active

<< Previous Showing Rows 1 to 11 of 11 [1] Next >>

Le Net du Kermeur
Monitoring réseau

Cacti : Définition du modèle RSSI

Data Source Item [radio_level] — **New**

Internal Data Source Name Use Per-Data Source Value (Ignore this Value)	radio_level
Minimum Value Use Per-Data Source Value (Ignore this Value)	0
Maximum Value Use Per-Data Source Value (Ignore this Value)	50
Data Source Type Use Per-Data Source Value (Ignore this Value)	GAUGE
Heartbeat Use Per-Data Source Value (Ignore this Value)	600

Custom Data [data input: Get SNMP Data]

SNMP IP Address Use Per-Data Source Value (Ignore this Value)	*Value will be derived from the host if this field is left empty.*
SNMP Community Use Per-Data Source Value (Ignore this Value)	*Value will be derived from the host if this field is left empty.*
SNMP Username Use Per-Data Source Value (Ignore this Value)	*Value will be derived from the host if this field is left empty.*
SNMP Password Use Per-Data Source Value (Ignore this Value)	*Value will be derived from the host if this field is left empty.*
SNMP Version (1, 2, or 3) Use Per-Data Source Value (Ignore this Value)	*Value will be derived from the host if this field is left empty.*
OID Use Per-Data Source Value (Ignore this Value)	.1.3.6.1.2.1.2.2.1.53.100.1

Cacti : les modèles de graphes pour Openwrt

Le Net du Kermeur
Monitoring réseau

Cacti : définition du modèle de graphe radio

Graph Template Items [edit: Openwrt radio] **Add**

Graph Item	Data Source	Graph Item Type	CF Type	Item Color
Item # 1	**(radio_level): Niveau du signal**	**AREA**	**AVERAGE**	**6EA100**
Item # 2	(radio_level): Actuel:	GPRINT	LAST	
Item # 3	(radio_level): Mini:	GPRINT	MIN	
Item # 4	(radio_level): Maxi:<HR>	GPRINT	MAX	
Item # 5	**(noise_level): Niveau de bruit**	**AREA**	**AVERAGE**	**FFC73B**
Item # 6	(noise_level): Actuel:	GPRINT	LAST	
Item # 7	(noise_level): Mini:	GPRINT	MIN	
Item # 8	(noise_level): Maxi:<HR>	GPRINT	MAX	
Item # 9	**(openwrt_txpower): Puissance émise**	**LINE2**	**AVERAGE**	**FF0000**
Item # 10	(openwrt_txpower): Actuel:<HR>	GPRINT	LAST	
Item # 11	**(data_niveau_borne): Reçue par l'AP**	**LINE2**	**AVERAGE**	**6DC8FE**
Item # 12	(data_niveau_borne): Actuel:	GPRINT	LAST	
Item # 13	(data_niveau_borne): Mini:	GPRINT	MIN	
Item # 14	(data_niveau_borne): Maxi:<HR>	GPRINT	MAX	
Item # 15	**(data_rate): Vitesse radio (Mbps)**	**LINE1**	**AVERAGE**	**0000FF**
Item # 16	(data_rate): Actuel:	GPRINT	LAST	
Item # 17	(data_rate): Mini:	GPRINT	MIN	
Item # 18	(data_rate): Maxi:<HR>	GPRINT	MAX	

Cacti : Modèle de host Openwrt

Host Templates [edit: Openwrt]

Name
A useful name for this host template. Openwrt

Associated Graph Templates

1) Interface - Traffic (bits/sec)
2) Openwrt charge CPU
3) Openwrt radio

Add Graph Template: Cisco - CPU Usage **add**

Associated Data Queries

1) SNMP - Interface Statistics

Add Data Query: Karlnet - Wireless Bridge Statistics **add**

Remarque : La charge CPU est également sur un modèle spécifique

Récupération de la donnée niveau vu de l'AP

Sur les AP en Openwrt Kamikaze (Madwifi)

```
for AP in $(Requete_Mysql_AP_Kamikaze); do
        ssh  $AP "cat /proc/.../associated_sta" | sed -e :a -e '$!N;s/\n / /;ta' -e 'P;D'
done
```

Sur les AP en Openwrt RC6

```
for AP in $(Requete_Mysql_AP_RC6) ; do
        # Retrouve les adresse Macs des clients associés
        for CLIENT in $(ssh $AP  "wl assoclist" | cut -d ' ' -f 2); do
                RES=$(ssh $AP "wl rssi $CLIENT")
                echo   "$ADRM;$RES"
        done
done
```

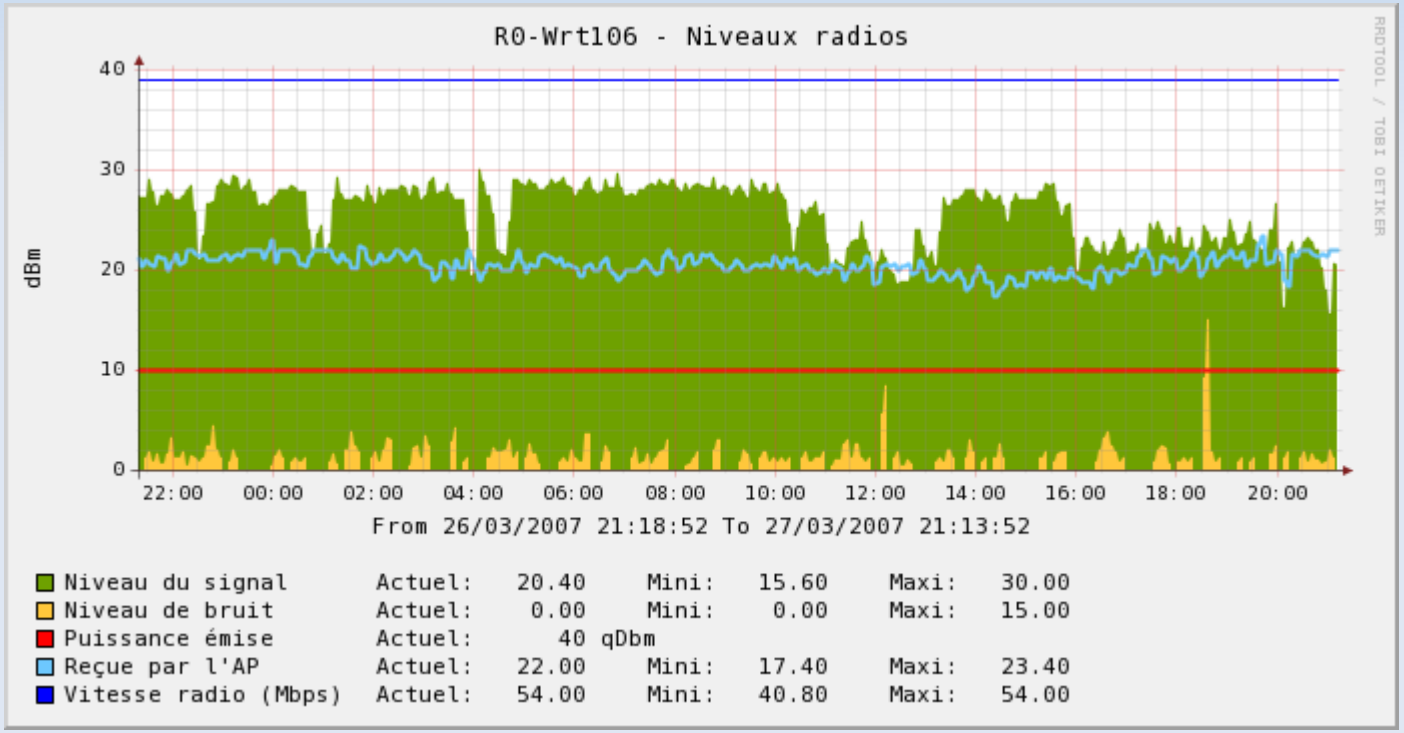
Filtre perl rajoutant le nom d'hote retrouvé dans la base Mysql, on obtient :

```
whr130   |00:16:01:4d:ae:57 |18   |99   |0    |0    |0    |0
wrt144   |00:12:17:d7:ba:85 |18   |99   |0    |0    |0    |0
## *** Relais whr132 ***
wrt123   |00:18:39:c0:64:30 |14   |99   |0    |0    |0    |0
```

Ces données sont également utilisées pour la régulation du txpower des routeurs

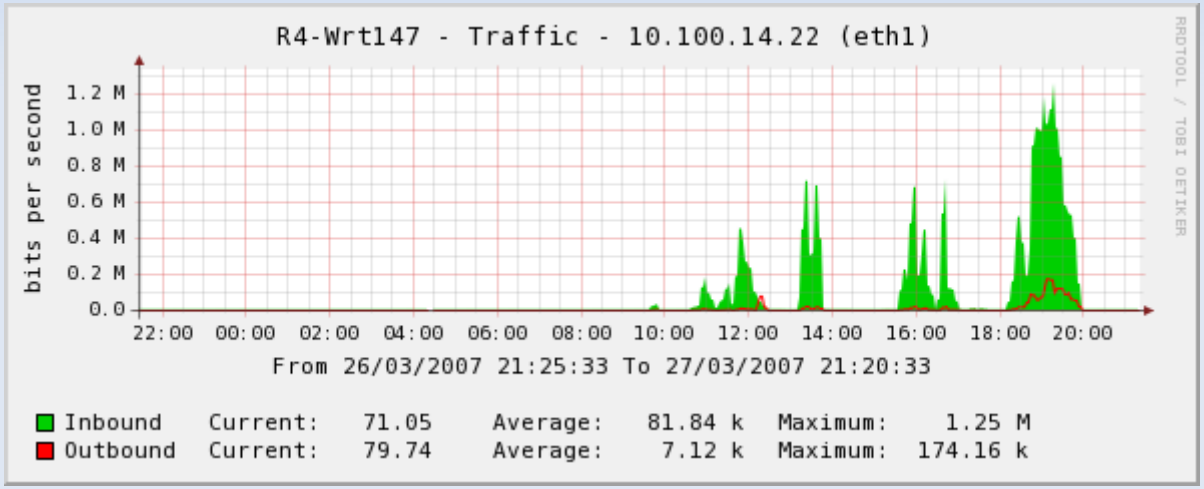
Le Net du Kermeur
Monitoring réseau

Le graphe radio



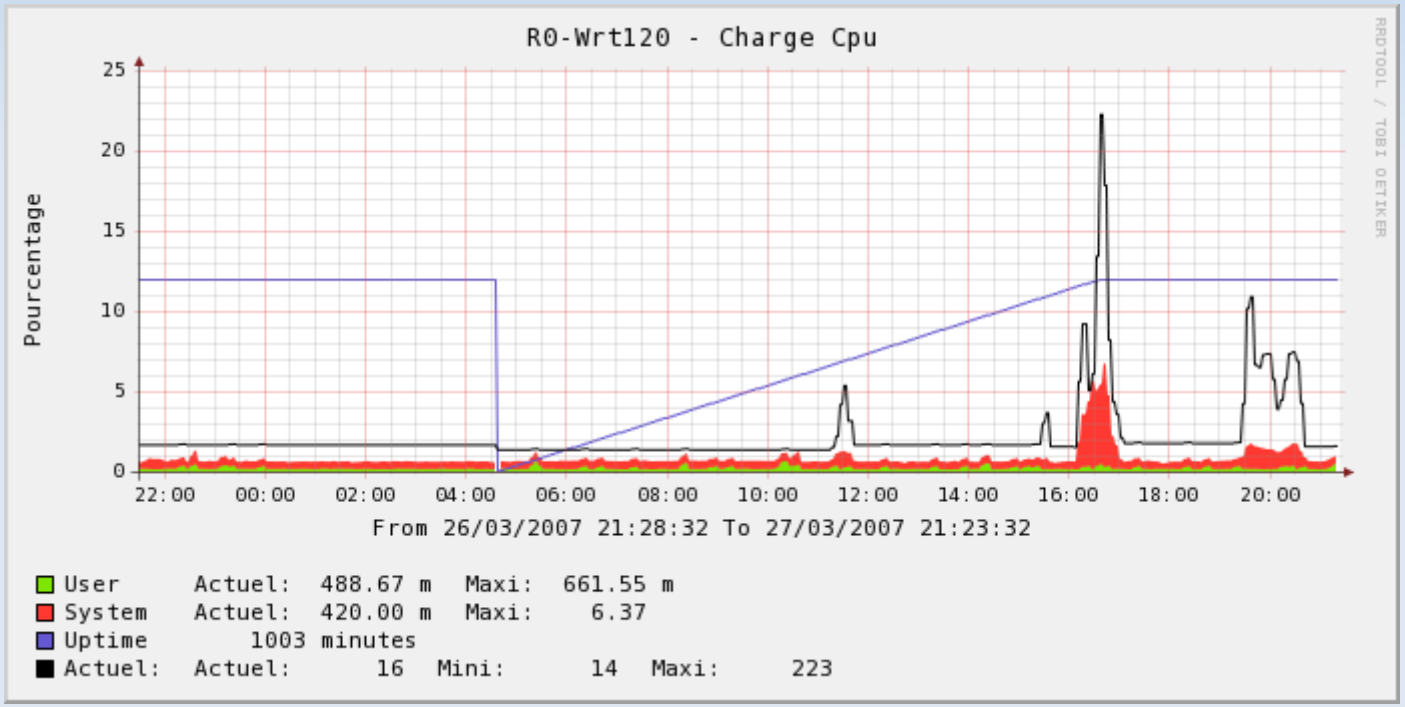
Le Net du Kermeur
Monitoring réseau

Le graphe trafic



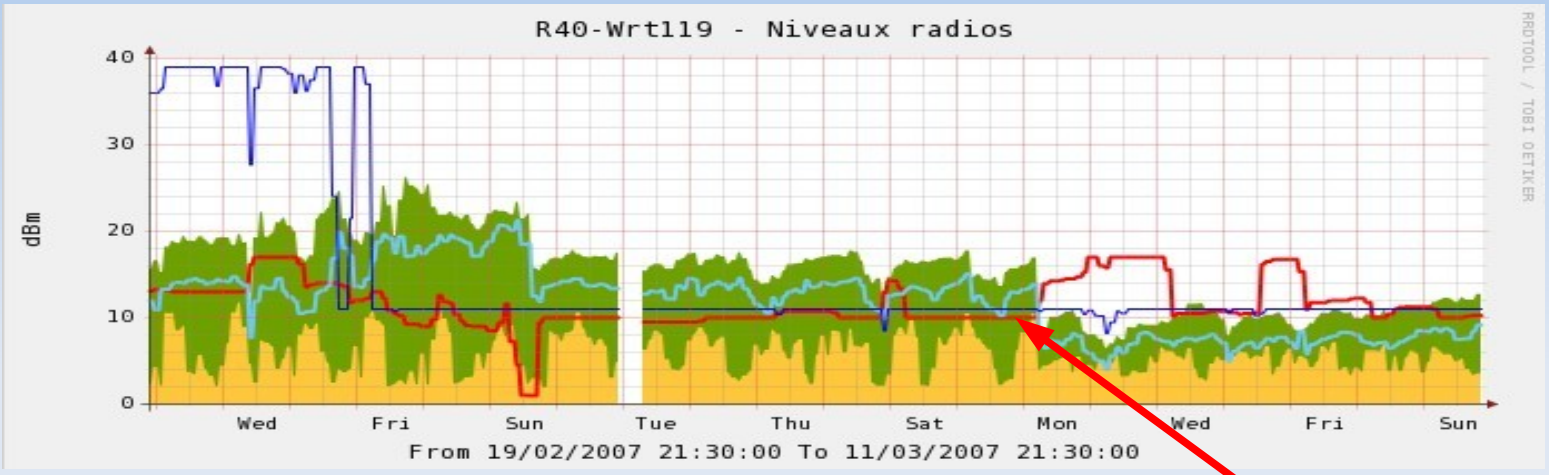
Le Net du Kermeur
Monitoring réseau

Le graphe charge CPU

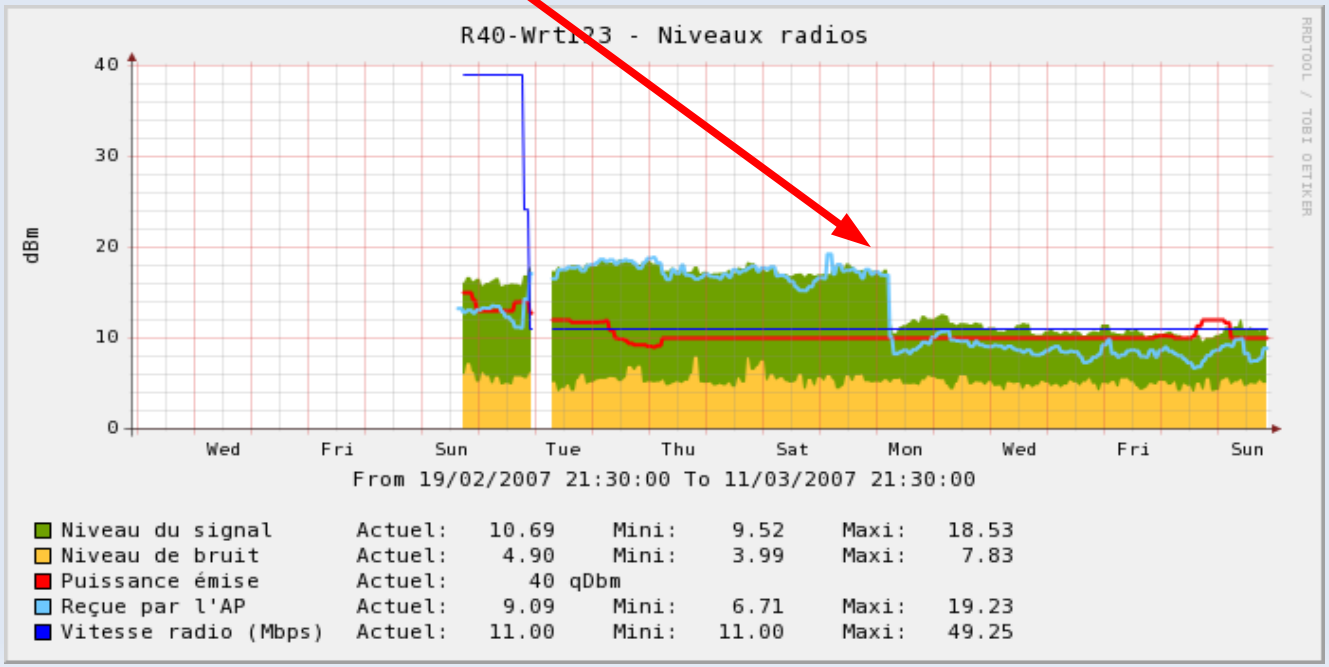


Le Net du Kermeur
Monitoring réseau

Exemple en maintenance



Deux clients d'un même relais + bruit de tonnerre : Sélecteur d'antenne du relais



Mise en place SSH

ssh_keygen

Clé publique dans /etc/dropbear/authorized_keys du routeur

Clé privée sur le serveur de maintenance

```
ssh -l root -i fichier_clé nom_routeur commandes_sur_le_routeur
```

Script wrtxxx.sh :

```
WRT=$(basename $0)
if [ $# -eq 0 ]; then
    echo "Connexion a $WRT"
fi
ssh -l root -i $HOME/.ssh/keykivabien $WRT $*
```

Faire les liens, permettant de faire nom_routeur commande

```
ln -s wrtxxx.sh wrt102
```

Commandes en rafale

```
for WRT in liste_de_wrt ; do $WRT commande; done
```

Mise à jour au redémarrage

Les routeurs sont à l'heure UTC, avec TZ défini, alignés par NTP
Dans leur crontab, redémarrage journalier

/etc/init.d/S42localnet, génération d'un startup personnalisé

```
SRV=$(nvram get cfk_serveur)
wget http://$SRV/startup.php?ADRMAC=xxx -o /tmp/startup.sh
/tmp/startup.sh
```

Dans ce startup.sh, en genéral mises à jour de fichiers de conf, de script, ...
Minimiser les écritures en flash mais commande diff inexistante

```
wget http//serveur/fichier -o /tmp/fichier
CONT1=cat fichier_original
CONT2=cat /tmp/fichier
if [  "x$CONT1 " !=  "x$CONT2 " ]; then
      mv /tmp/fichier fichier_original
fi
```

Régulation de la puissance émission

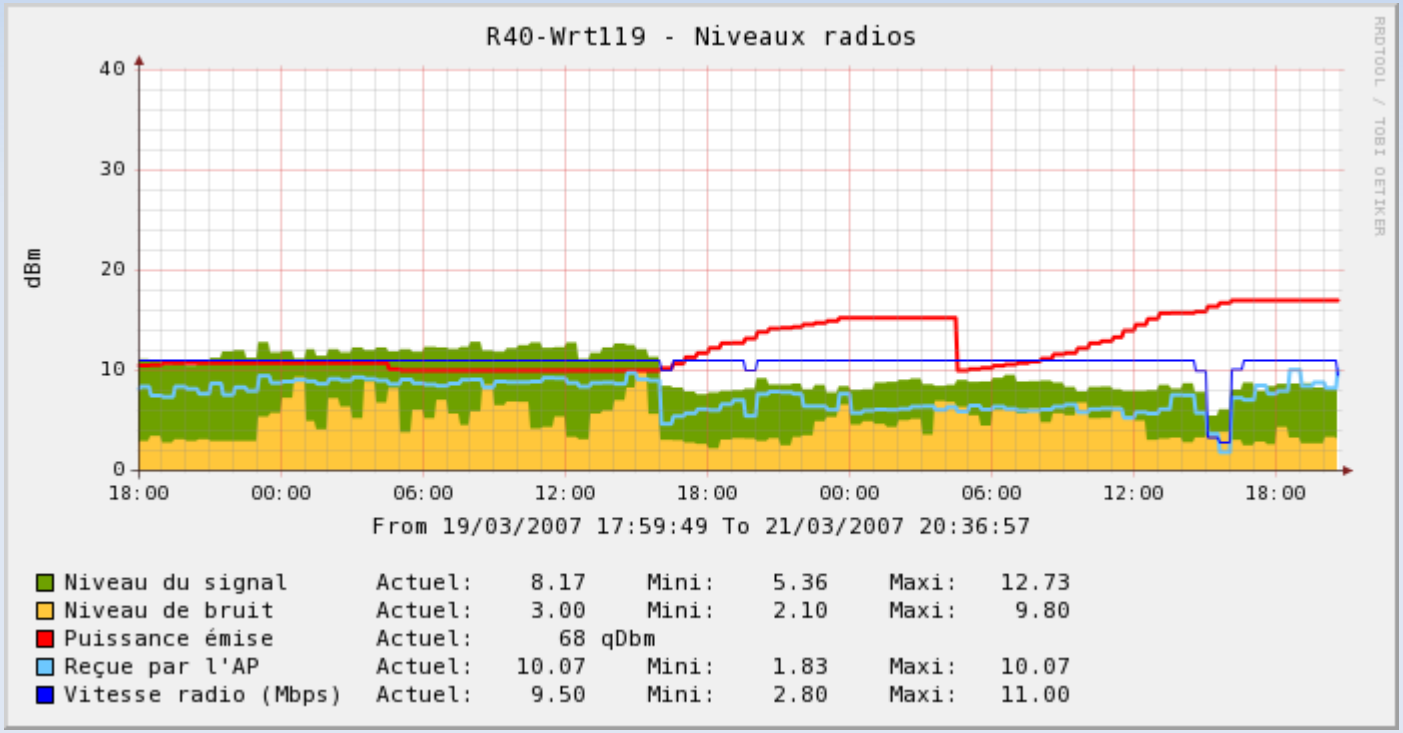
En crontab sur la machine d'exploitation, toutes les 5 minutes
A partir du fichier des mesures relevés sur les AP, le principe :

```
LSTWRT=$(grep ^w[hr][rt] Fichier | cut -d '|' -f 1 | sort | uniq )
for WRT in $LSTWRT ; do
    NIVEAU=$(grep ^$WRT Fichier | cut -d '|' -f 3)
    if [ $NIVEAU -gt $MAXI ]; then
        TXPWR=$(snmpget $WRT  Mib_Txpower_Qdbm)
        ssh $WRT  "wl txpwr1 -q $(( $TXPWR  - 1))"
    fi
    if [ $NIVEAU -lt $MINI ]; then
        TXPWR=$(snmpget $WRT  Mib_Txpower_Qdbm)
        ssh $WRT  "wl txpwr1 -q $(( $TXPWR  + 1))"
    fi
done
```

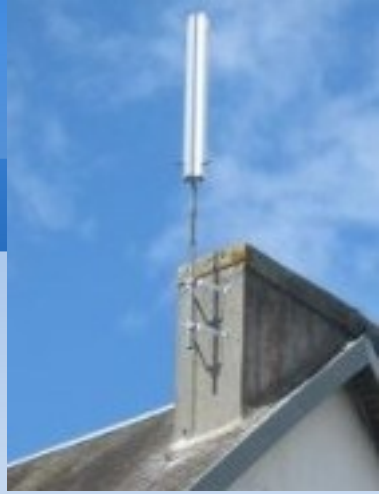
Le wl txpwr1 -q Valeur serait à remplacer par snmpset Mib_Txpower_Qdbm

Le Net du Kermeur
Monitoring réseau

Régulation de la puissance émission
Exemple



Le seul fonctionnant avec les antennes d'origine du WRT
Apparement posé sur une fenêtre



Analyse des dmesg

Lancée toute les heures en crontab sur la machine d'exploitation
Initialement détection des routeurs ayant des problèmes de nvram vérolée, principale cause de panne depuis le lancement du réseau.

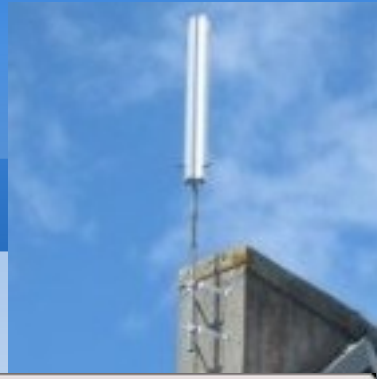
```
for WRT in $(Requete_Mysql_Liste_Routeurs); do
    for ITEM in $(ssh $WRT "dmesg | tail -$NBL | sed -e 's/ /_/g'"); do
        Comparaison avec une liste d'élément connus et normaux ...
        [ "x${ALL[$IJ]}" == "x${ITEM:0:${LN}}" ] && KN=$(($KN + 1))
    done
    [ $KN -ne $NBL ] && echo "Problème sur routeur $WRT"
done
```

A l'usage

Détection des dépassements ip_conntrack (Usage Peer To Peer)
Détection DCC forged (pb pièce-jointe dans Msn ?)

Le Net du Kermeur
Monitoring réseau

http://192.168.1.1/



OpenWrt User Console - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

Le net du Kermeur : Routeur whr130

Hostname: whr130
Uptime: 17:14
Load: 0.00, 0.00, 0.00
Version: WHITE RUSSIAN (rc6)

```
 _______                     ________        __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
WHITE RUSSIAN (rc6) -------------------------------
 * Reseau Wlan du Kermeur (29640 Plougonven Fr)
 * Borne whr130 (00:16:01:4d:ae:57), mode client
-----------------------------------------------------
```

Date/Heure	Wed Mar 28 21:40:29 CET 2007
Version de firmware	WHITE RUSSIAN (rc6)
Version du kernel	Linux version 2.4.30 (marc@vectra) (gcc version 3.4.4 (OpenWrt-1.0)) #1 mer jan 24 14:37:45 CET 2007
Adresse MAC	00:16:01:4D:AE:56
Niveau radio	Signal **-77**, bruit **-95**, marge **18**

Echelle de 0 à 50 (en jaune le bruit, en vert le signal)

Page d'acceuil

Terminé

Le Net du Kermeur
Monitoring réseau

Page http d'un relais

OpenWrt User Console - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils Aide

Le net du Kermeur : Routeur whr132

Hostname: whr132
Uptime: 17:53
Load: 0.16, 0.10, 0.03
Version: WHITE RUSSIAN (rc6)

```
 _______                     ________        __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
WHITE RUSSIAN (rc6) -------------------------------
 * Reseau Wlan du Kermeur (29640 Plougonven Fr)
 * Borne whr132 (00:16:01:4d:ab:bf), mode relais
-----------------------------------------------------
```

Date/Heure	Wed Mar 28 21:54:51 CET 2007
Version de firmware	WHITE RUSSIAN (rc6)
Version du kernel	Linux version 2.4.30 (marc@vectra) (gcc version 3.4.4 (OpenWrt-1.0)) #1 mer jan 24 14:37:45 CET 2007
Adresse MAC	00:16:01:4D:AB:BE

Niveaux radio

wrt146 (00:16:B6:D9:8D:78)	14	
wrt123 (00:18:39:C0:64:30)	14	
whr131 (00:16:01:4D:AE:51)	18	
wrt119 (00:16:B6:D9:60:B7)	13	
wrt124 (00:18:39:C0:64:2D)	14	

Echelle de 0 à 50 (en jaune le bruit, en vert le signal)

Le Net du Kermeur
Monitoring réseau

Objectif : en faire le moins possible ...

- Stabilité du firmware
  - 3 versions : base Sveasoft : moins de 6 mois,
    - Openwrt RC4 : 1 an, RC6 : deux ans ?

- Monitorer
  - Pour voir les coups venir, corriger si possible
    - Moins d'un appel/semaine, dont moins d'un/mois réseau
  - Eléments pour les dimensionnements et les configurations

La suite ?

- Gestion des abonnements : factures, non paiement, etc ...
  - Rapprochement avec les données de réseau et données bancaires

Liens

OpenWrt : http://openwrt.org/
Cacti : http://cacti.net/
RRDtool: http://oss.oetiker.ch/rrdtool/
NetSnmp : http://net-snmp.sourceforge.net/
http://www.net-snmp.org/docs/man/snmpd.conf.html
Mysql : http://www.mysql.com/

M0n0wall : http://m0n0.ch/wall/
pfSense : http://www.pfsense.org/

Site du Kermeur : http://www.lekermeur.net/
Les notes : http://www.lekermeur.net/blog_du_net/