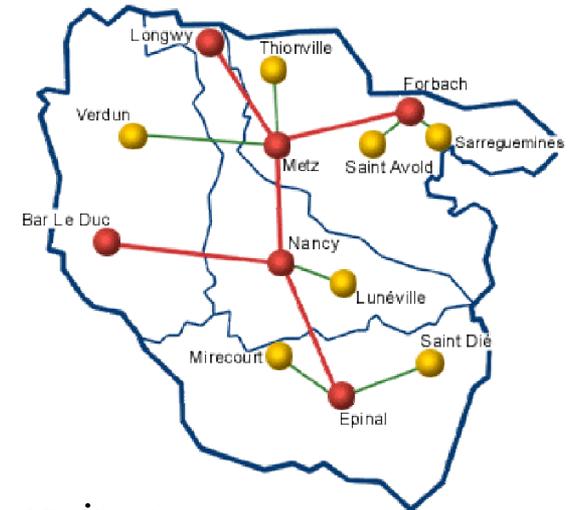


 **iSup** - Développement d'une
plate-forme de supervision complète et homogène
pour les réseaux Lorrains

JRES 2007

21 novembre 2007

- Introduction
- Besoins identifiés
- iSup : Concepts et fonctionnement
- Analyse et alertes
- Présentation de l'information
- Bilan



- L'équipe réseau du CIRIL gère
 - des réseaux métropolitains
 - des réseaux de campus
 - bâtiments universitaires, CROUS ...
 - sur plusieurs villes de Lorraine
 - des réseaux régionaux
 - le réseau Lothaire interconnectant 13 villes lorraines
 - le réseau eLorraine des établissements scolaires du second degré
 - plus de 1000 équipements réseaux de type commutateurs et routeurs
 - des services associés (portail captif, VPN ...)

- Cette session
 - présente les fonctionnalités de la solution de supervision mise en œuvre par le CIRIL pour l'ensemble des réseaux gérés
 - ne présente pas le fonctionnement interne de l'application

- Introduction
- **Besoins identifiés**
- iSup : Concepts et fonctionnement
- Analyse et alertes
- Présentation de l'information
- Bilan

- Unification des outils
 - multiplicité des outils existants
 - netup, Cricket, Nagios, Cacti ...
 - duplicité des informations
 - maintenance fastidieuse
 - besoin d'un point unique et central de configuration
 - disposer d'une base regroupant l'ensemble des informations sur les équipements ou services gérés

- Automatisation
 - de la configuration des outils
 - de l'ajout d'un service ou d'un équipement
 - des procédures de vérification de la cohérence

- Multiplicité des usages : des outils différents pour des usages différents
 - Administrateurs/opérateurs des services
 - données très techniques
 - court terme
 - corrélation des informations
 - gestion d'alertes
 - Décideurs administratifs et financiers
 - données analysées
 - analyse de tendance
 - prévision des évolutions
 - Correspondants locaux et proches des usagers
 - information en temps réel
 - qualification/quantification de la qualité du service
 - outil d'aide au diagnostique
 - possibilité de réception des alertes
-

- Gestion des autorisations
 - les réseaux gérés par le CIRIL sont sous la responsabilité de correspondants locaux
 - la solution doit présenter à chaque correspondant des informations concernant uniquement ses réseaux

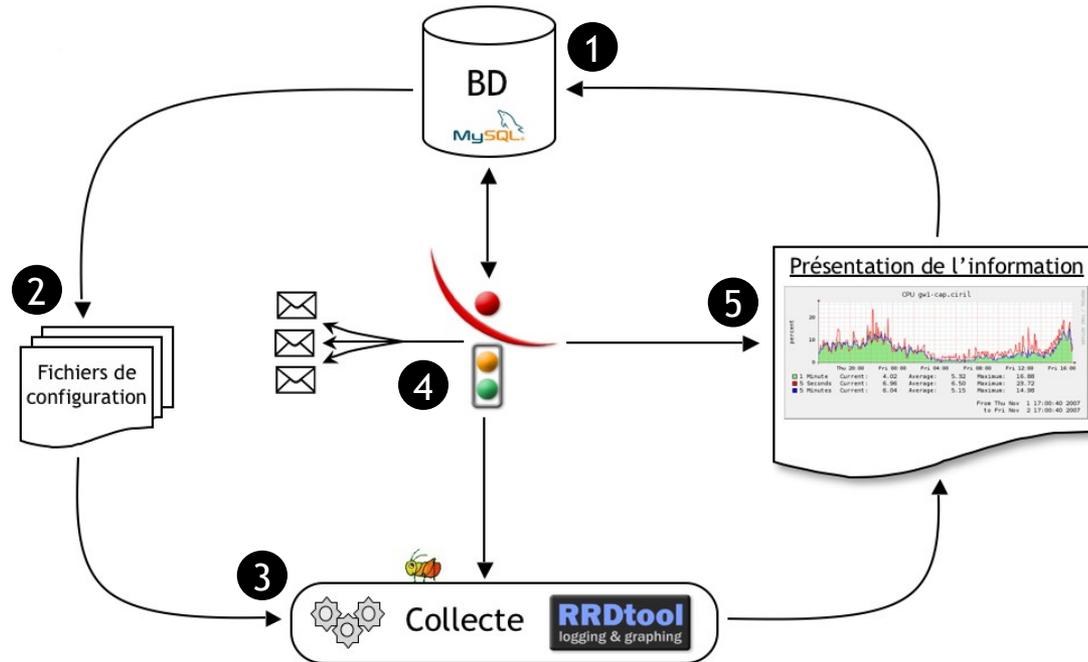
- Pérennité des informations
 - les indicateurs de la disponibilité ou de la qualité d'un services sont indépendants de sa mise en œuvre
 - ex.: le temps de traversé d'une liaison doit pouvoir être conservé dans le temps, indépendamment des technologies ou des équipements utilisés
 - nécessité d'une convention de nommage homogène pour l'ensemble des services

- Solutions libres ou commerciales
 - non conformes aux attentes
 - nécessitent tout de même une intégration lourde

- Choix de développer une solution maison
 - réutilisation d'outils libres déjà maîtrisés
 - Cricket, RRD, MySQL
 - développements spécifiques
 - « Psychopinger », moteurs d'analyse, présentation de l'information
 - intégration de l'ensemble via des scripts Perl

- Introduction
- Besoins identifiés
- **iSup : Concepts et fonctionnement**
- Analyse et alertes
- Présentation de l'information
- Bilan

- *Equipement* : un matériel de type routeur/commutateur/ serveur permettant de mettre en œuvre certains services
- *Métrique* : une information mesurable concernant un équipement
 - temps de réponse, utilisation d'une ligne, % CPU, ...
 - interrogation SNMP, résultat de l'exécution de commandes ...
- *Service* « de base »
 - L'association d'une métrique à un équipement
 - ex: compteur SNMP du nombre d'octets de l'interface Gi 0/3 du routeur gw1.nancy = « Trafic sur la liaison entre Nancy et Metz »
- *Service composé*
 - Association de services « de base »
 - Vue globale de la disponibilité et de la qualité d'un service
 - ex : pour la liaison entre Nancy et Metz, l'association de la disponibilité, des temps de réponse, des paquets perdus et du taux d'occupation permet d'avoir une représentation globale du service « liaison Nancy-Metz »



- 1 Base de données centralisée
- 2 Génération automatique des fichiers de configuration
- 3 Collecte des données (Cricket/RRD)
- 4 Analyse des données collectées et alertes
- 5 Présentation de l'information (graphiques, statistiques, ...)

- Les fondements de la supervision
 - collecter les bonnes informations
 - aux bons endroits

- Le plus basique : s'assurer du fonctionnement de chaque service
 - via des interrogations SNMP ou PING
 - via des scripts de test des services

- Evaluer la qualité du service et la santé des équipements : travail important pour déterminer
 - les variables à interroger
 - la fréquence d'interrogation
 - les durées de rétention

- Nécessaire pour faciliter la maintenance et la cohérence de la solution :
 - centralisation des informations dans la base de données
 - rassemble toutes les informations de configuration et de gestion
 - génération automatique des configurations
 - plus de modifications manuelles sources d'erreurs
 - modèles de supervision en fonction du type d'équipement
 - métriques disponibles et définitions associées
 - découverte des équipements et des services associés
 - cohérence avec d'autres systèmes d'informations :
 - DNS, configurations des équipements

- Choix d'une politique de conservation des données
 - Plusieurs niveaux de détails (RRAs)
 - très détaillé à court terme
 - plus global à long terme

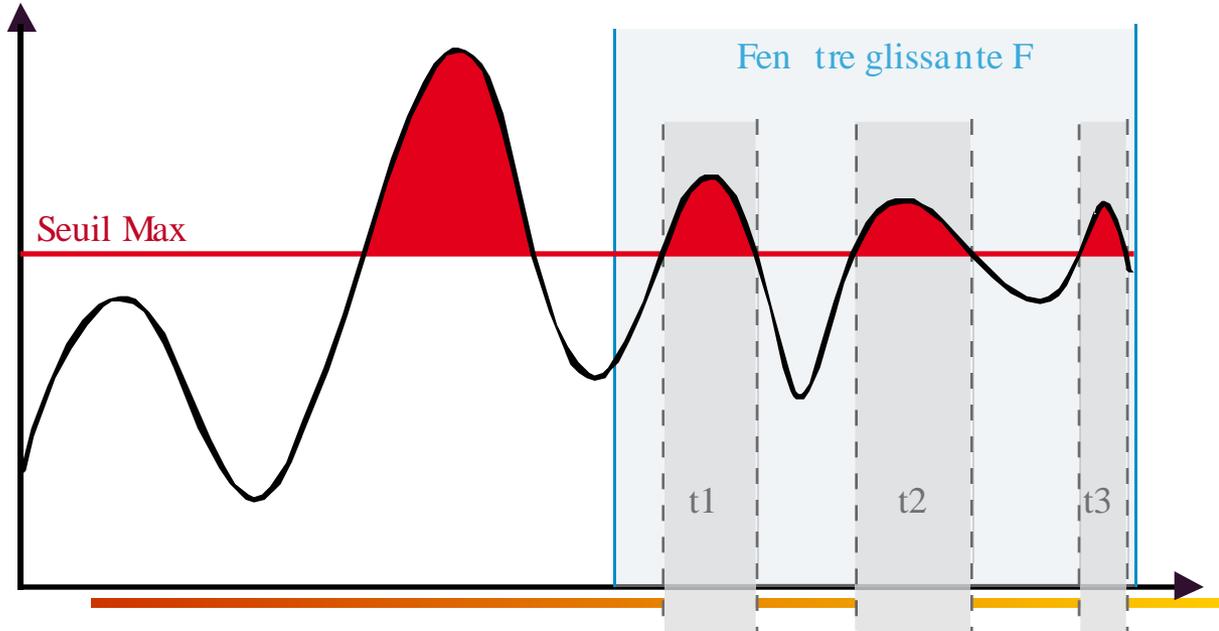
- Continuité de l'information
 - Assurer une continuité malgré les évolutions régulières des infrastructures
 - convention de nommage des services
 - possibilité de modification d'un service
 - renommage, changement d'équipement
 - modification des paramètres

- Introduction
- Besoins identifiés
- iSup : Concepts et fonctionnement
- **Analyse et alertes**
- Présentation de l'information
- Bilan

- Pourquoi ?
 - faciliter le travail de l'administrateur
 - détecter les pannes
 - anticiper les dysfonctionnements
 - donner des indicateurs aux correspondants
 - analyse de la qualité des services

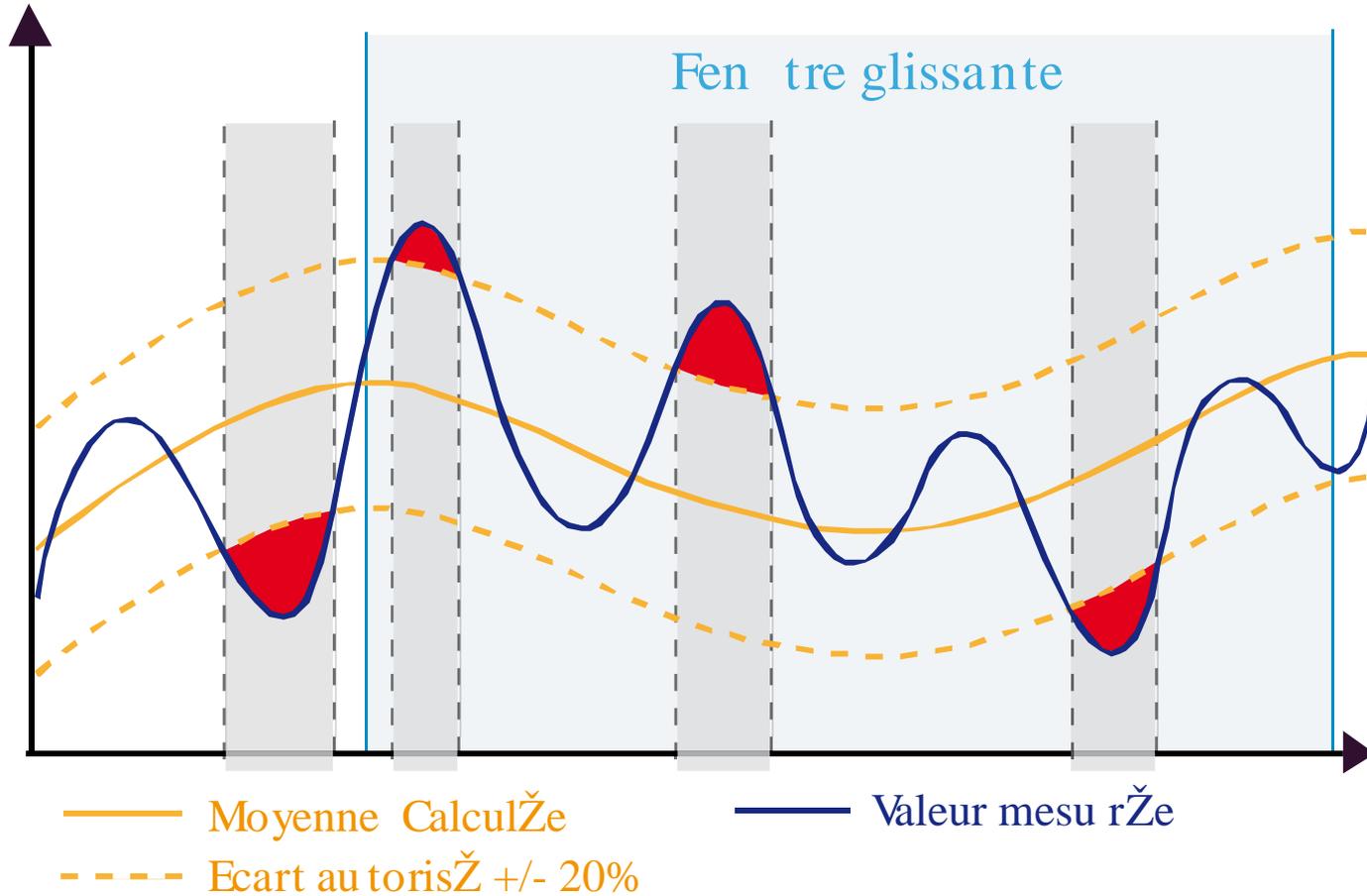
 - Comment ?
 - moteurs d'analyse
 - réactifs
 - proactifs
 - modèles d'analyse
 - paramétrage d'un moteur d'analyse
 - par défaut associés aux métriques
 - possibilité de surcharge pour chaque service
-

- Anticiper une panne
 - sur le dépassement d'un seuil critique
 - *risque important de fausse alerte*
 - nécessité d'algorithmes plus élaborés
 - fenêtre glissante
 - dépassement cumulé de seuils



- Anticiper une panne
 - déterminer le comportement « normal »
 - notion de *base line*
 - détecter un changement de comportement
 - déviation d'une donnée par rapport à la courbe « normale »
 - permet de prendre en compte les comportements atypiques mais licites
 - ex: utilisation intensive la nuit à l'heure des sauvegardes
 - comparer ce qui est comparable
 - un dimanche avec un dimanche

- Cet algorithme n'est pas encore implémenté



- L'analyse des données génère pour chaque service un état
- Chaque service peut avoir un des états suivants
 - ROUGE : le service est indisponible
 - ORANGE : le service fonctionne
 - soit de façon dégradée
 - soit un risque de dysfonctionnement a été détecté
 - VERT : le service fonctionne correctement
 - GRIS : l'état du service n'a pu être déterminé
- Un changement d'état peut donner lieu à des alertes ou à l'exécution de commandes

- Alerter à bon escient
 - prendre en compte
 - la criticité du service ou de l'équipement
 - les plages horaires de supervision
 - les personnes à alerter
 - l'agrégation des alertes
 - disposer de différents modes d'alerte
 - graphique
 - par courrier électronique
 - par SMS

- iSup propose
 - la configuration avancée de modes d'alerte
 - Qui ? Quand ? Comment ?
 - pour chaque service la possibilité d'y associer un ou plusieurs modes d'alerte

- Tout événement doit être conservé
 - ne pas perdre certaines alertes
 - déterminer la fréquence de certains problèmes
 - Déterminer la disponibilité de certains services

- iSup conserve un historique
 - de tout changement d'état
 - pour chaque service

- Console avec acquittement des évènements

Les alarmes en cours

Les alarmes Basculer la permanence

06/11/2007 09:50:43

Les services

<input checked="" type="checkbox"/>	Nom	Equipement	Métric	M/V/P	Etat	Durée
	sw-cpc-bu-n1-2-eth.sciences.reachability	sw-cpc-bu-n1-2-eth.sciences	reachability	1/0/50		250d 09:50
	sw-cpc-bu-n1-3-eth.sciences.reachability	sw-cpc-bu-n1-3-eth.sciences	reachability	1/0/50		250d 09:50
<input checked="" type="checkbox"/>	sw-POE-2-eth.esial.reachability	sw-POE-2-eth.esial	reachability	1/2/50		148d 01:45
<input checked="" type="checkbox"/>	gw1.plg-WIRELESS-PERIPHERIQUE-VLAN251.ifreachability	gw1.plg	ifreachability	1/0/50		13d 01:45
<input checked="" type="checkbox"/>	sw1-eth.crous-leopold.reachability	sw1-eth.crous-leopold	reachability	1/2/50		5d 23:30

- Introduction
- Besoins identifiés
- iSup : Concepts et fonctionnement
- Analyse et alertes
- **Présentation de l'information**
- Bilan

- Adapter la présentation de l'information à l'utilisateur
 - Paramétrage des représentations
 - modèles de graphes

 - Trois catégories chez nos utilisateurs
 - Décideurs
 - rapports d'utilisation (taux d'utilisation, disponibilité, ...)
 - Administrateurs
 - administration de la base, représentations avancées
 - Correspondants
 - accès restreint (gestion des droits)
 - interface personnalisable
-

Choisir la période d'affichage

Choisir la valeur représentée :

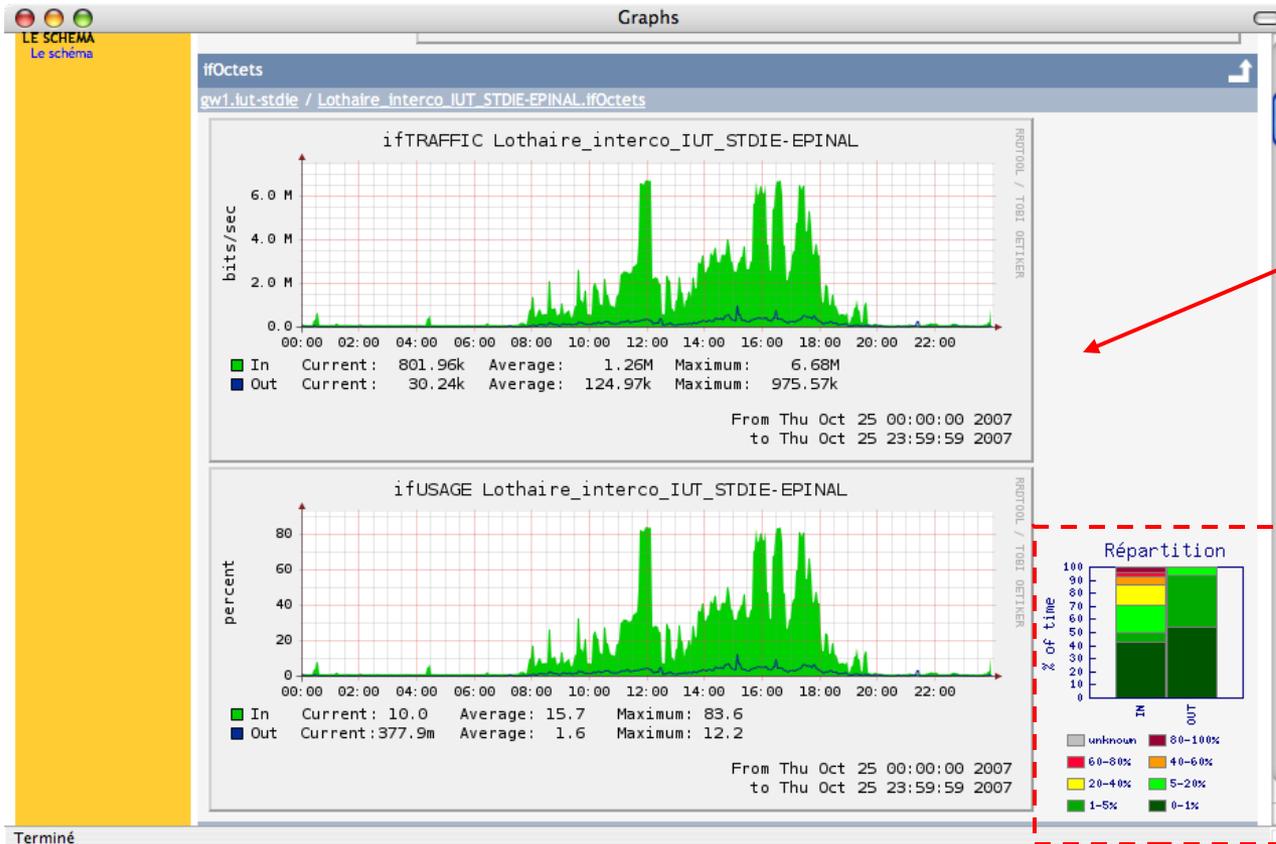
- Minimum
- Moyenne
- Maximum

Disposer sur une même page des données différentes afin de permettre les corrélations

The screenshot shows the 'Graphs' window in the iSup monitoring tool. At the top, there is a navigation bar with 'Presets: Previous Day', a date range 'From: 25/10/2007 00:00 To: 25/10/2007 23:59', and a 'Refresh' button. Below this, a menu allows selecting the metric to display: 'MIN', 'AVERAGE', 'MAX', 'cpu', 'ifOctets', 'ifPkts', and 'ifreachability'. The main area contains three vertically stacked graphs:

- cpu gw1.iut-stdie**: A line graph showing CPU usage in percent over a 24-hour period. It includes a legend for 1 Minute, 5 Seconds, and 5 Minutes intervals. Statistics shown: 1 Minute (Current: 3.00, Average: 12.39, Maximum: 96.79), 5 Seconds (Current: 1.00, Average: 12.11, Maximum: 98.95), 5 Minutes (Current: 3.00, Average: 12.40, Maximum: 91.86).
- ifOctets Lothaire_interco_IUT_STDIE-EPINAL**: A bar graph showing network traffic in bits/sec. Legend: In (Current: 801.96k, Average: 1.26M, Maximum: 6.68M), Out (Current: 30.24k, Average: 124.97k, Maximum: 975.57k).
- ifUSAGE Lothaire_interco_IUT_STDIE-EPINAL**: A bar graph showing disk usage, with a visible value of 80.

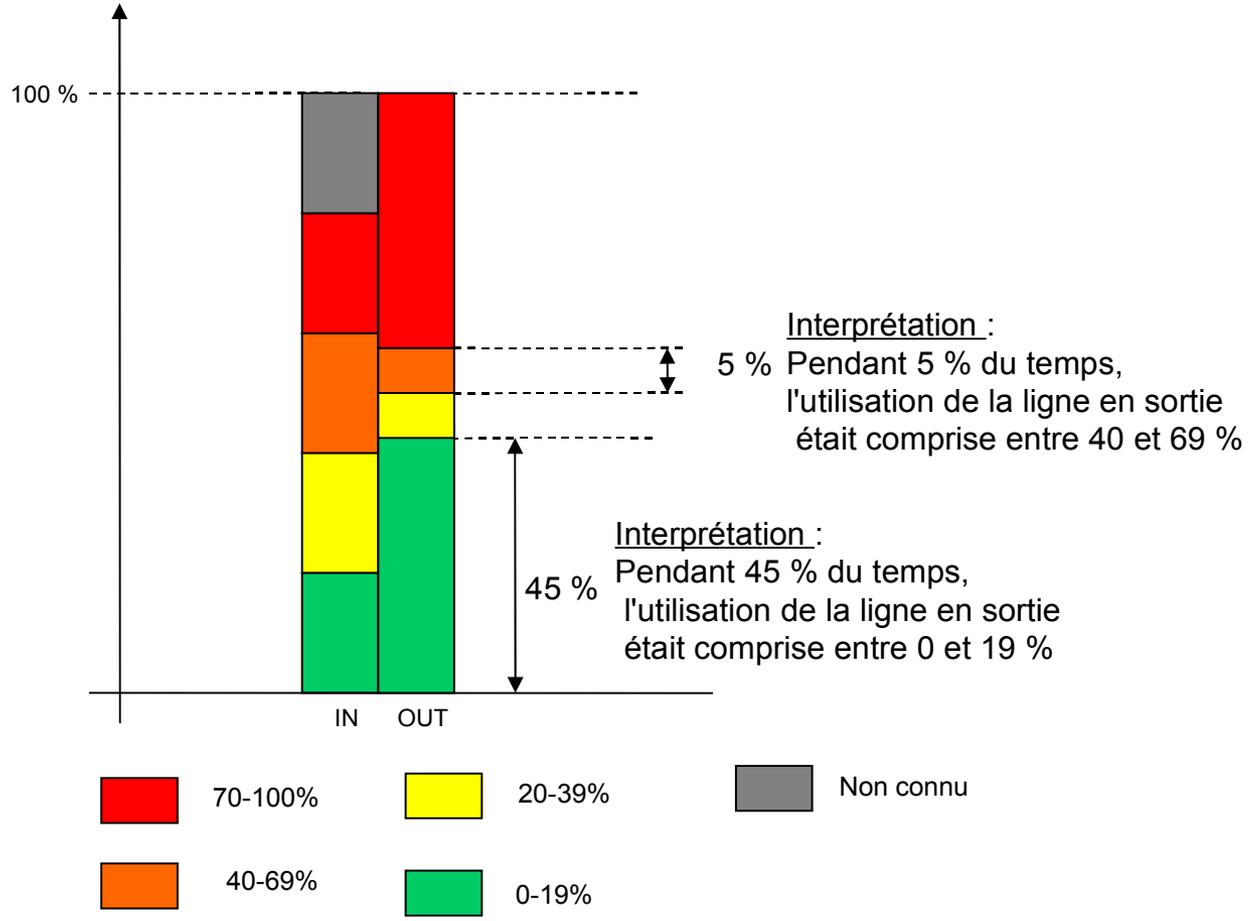
- Proposer un même indicateur avec des vues complémentaires
 - trafic sur une liaison et taux d'utilisation de ligne



Il est parfois plus intéressant de savoir qu'une liaison est chargée à 85% plutôt qu'à 6Mb/s

Graphique de répartition de charge

Répartition de charge



- Graphique de pilotage
 - utilisation des liaisons (plus de 200)
 - pendant les heures ouvrables
 - classement par ordre décroissant

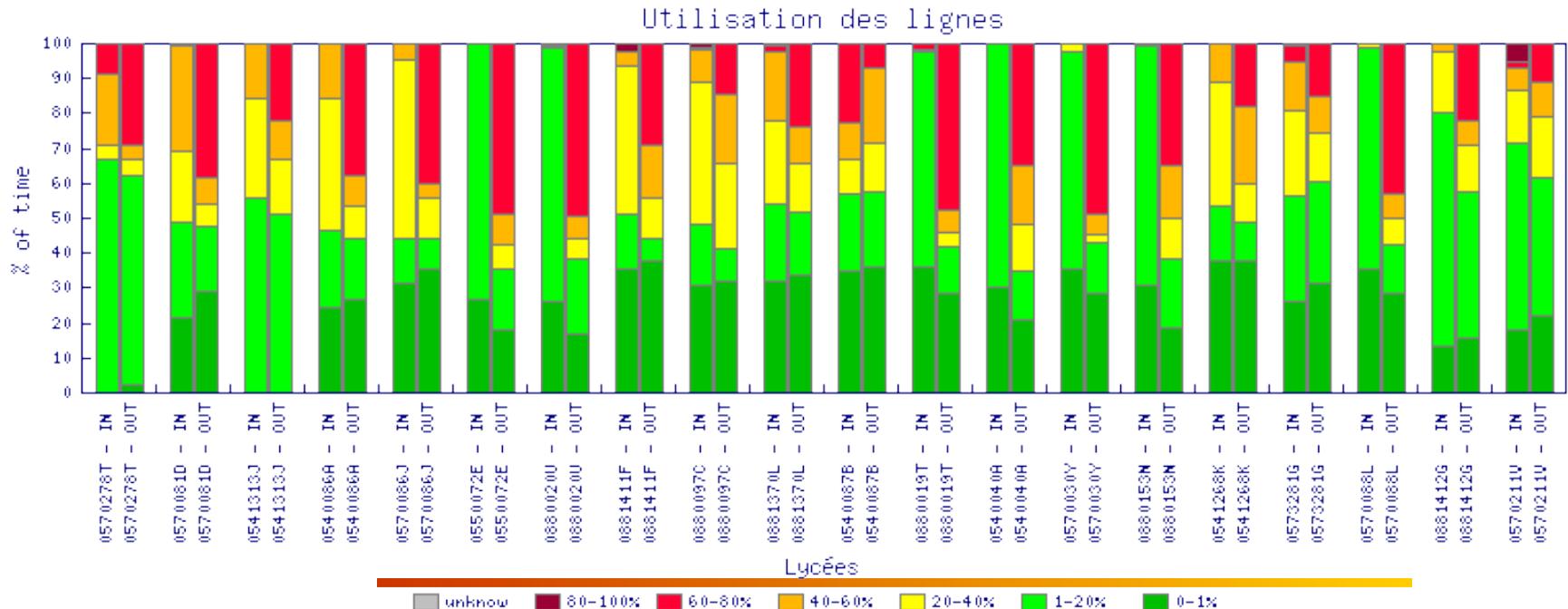


Tableau de bord pour *correspondants*

Les Alarmes ...
Configurer

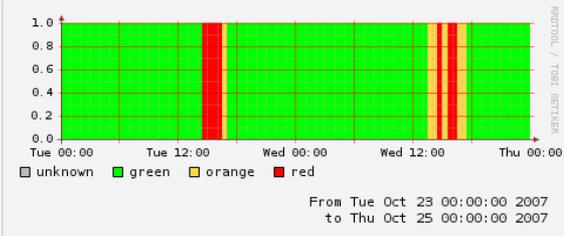
Voulez vous continuer à recevoir les notifications d'alarmes : OUI NON

02/11/2007 14:55:49

Nom	Equipement	Métric	Etat	Durée
sw-cpc-bu-n1-2-eth.sciences.reachability	sw-cpc-bu-n1-2-eth.sciences	reachability	●	246d 14:55
sw-cpc-bu-n1-3-eth.sciences.reachability	sw-cpc-bu-n1-3-eth.sciences	reachability	●	246d 14:55
sw-POE-2-eth.esial.reachability	sw-POE-2-eth.esial	reachability	●	144d 06:50
sw1-eth.crous-leopold.reachability	sw1-eth.crous-leopold	reachability	●	2d 04:35

Les évènements
Refresh

Presets : Last Day From: 23/10/2007 00:00 To: 25/10/2007 00:00



From Tue Oct 23 00:00:00 2007
to Thu Oct 25 00:00:00 2007

2007-10-24 17:15:00 gw3-cap.ciril.cpu from GREEN to ORANGE (2007-10-24 17:25:00)

2007-10-24 16:30:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-24 17:10:00)

2007-10-24 16:25:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-24 16:30:00)

2007-10-24 16:10:00 gw3-cap.ciril.cpu from GREEN to ORANGE (2007-10-24 16:25:00)

2007-10-24 15:55:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-24 16:00:00)

2007-10-24 15:50:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-24 15:55:00)

2007-10-24 15:20:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-24 15:50:00)

2007-10-24 14:55:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-24 15:20:00)

2007-10-24 14:40:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-24 14:55:00)

2007-10-24 14:35:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-24 14:40:00)

2007-10-24 13:50:00 gw3-cap.ciril.cpu from GREEN to ORANGE (2007-10-24 14:35:00)

2007-10-23 16:35:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-23 16:40:00)

2007-10-23 16:10:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-23 16:35:00)

2007-10-23 16:00:00 gw3-cap.ciril.cpu from RED to ORANGE (2007-10-23 16:10:00)

2007-10-23 14:45:00 gw3-cap.ciril.cpu from ORANGE to RED (2007-10-23 16:00:00)

2007-10-23 14:40:00 gw3-cap.ciril.cpu from GREEN to ORANGE (2007-10-23 14:45:00)

Configuration de la notification des alarmes

Alarmes en cours

Graphique de disponibilité du service

Journal des évènements

Tableau de bord pour *correspondants*

Mon tableau de bord



Mes graphes

Choix des graphes favoris

Zoom

Choix des services favoris

ifTRAFFIC StanNet_bBone_CIRIL-UHP.ifOctets

In	Current: 1.29M	Average: 1.29M	Maximum: 9.53M
Out	Current: 2.35M	Average: 1.04M	Maximum: 4.73M

CPU gw1.ciril.cpu

1 Minute	Current: 38.02	Average: 17.68	Maximum: 32.77
5 Seconds	Current: 20.10	Average: 20.94	Maximum: 43.55
5 Minutes	Current: 19.02	Average: 17.33	Maximum: 25.88

ifTRAFFIC Lothaire_interco_NANCY-RENAIER.ifOctets

In	Current: 333.74M	Average: 209.69M	Maximum: 441.75M
Out	Current: 130.33M	Average: 93M	Maximum: 193M

CPU gw1-cap.ciril.cpu

1 Minute	Current: 35.14	Average: 16.77	Maximum: 51.97
5 Seconds	Current: 36.09	Average: 18.37	Maximum: 58.80
5 Minutes	Current: 38.05	Average: 16.70	Maximum: 48.98

ifTRAFFIC StanNet_Site_CIRIL

In	Current: 10.56M	Average: 6M	Maximum: 16.13M
Out	Current: 16.13M	Average: 5M	Maximum: 21.7M

CPU gw1-cap.ciril.cpu

1 Minute	Current: 35.14	Average: 16.77	Maximum: 51.97
5 Seconds	Current: 36.09	Average: 18.37	Maximum: 58.80
5 Minutes	Current: 38.05	Average: 16.70	Maximum: 48.98

From Mon Nov 5 10:16:25 2007 to Tue Nov 6 10:16:25 2007

Stannet_bbone_likil-nancy.ifstatus

- ain.cpu
- 6log.cpu
- gw1.nancy.cpu
- gw1.ciril.cpu
- gw1.plg.cpu

Tableau de bord pour *hotline*

eBoard :: Tableau de bord e-LorraineHD - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

e-Lorraine :: netVIS :: CIRIL

e-lorraine.net

Home

eAlarm

Valider alerte SMS

Basculer la permanence

Tableau de bord

eBoard

What's Up

Echantillon type

Translations NAT

Utilisation des lignes

Indicateurs

Boîte à outils

Looking Glass

Chercher un site

CVS des confs e-Lorraine

Métriologie

netMET e-LorraineHD

Certificat SSL

Installez-moi la CA du CIRIL

eBoard :: Tableau de bord e-LorraineHD

Informations gw-116-AGR-0570086J (incident)

RNE	0570086J	Download	2048 kb/s
Type liaison	TDSL 2CA		250 kb/s
Tronc : PVC	1 : 1/135		320 kb/s
Interco. CCR	172.25.1.206		250 kb/s
Interco. site	172.25.1.205	Upload	250 kb/s
Localisation	Lycee agricole	easy-graph-it	
eStatus	COURCELLES-CHAUSSY	Site at a glance	
	RTT = 228 ms		

Recherches 3 Sites injoignables

click-me

RNE	num	
↑	gw-131-PUB-0573491K	0d 00:15
	gw-062-CFA-0542389D	85d 08:05
	DNS2-TRANSPAC	101d 07:40

Choix du graphique

Graph netMET e-Lorraine <-> Lot4

Graph What's UP

Graph QoS sur échantillons type

Statistiques pour Services

Tempo: Du Fri-26/10/2007 00:00 au Sat-27/10/2007 00:00

Last update : vendredi 26 octobre 2007 16:40:29

Document created by [Alexandre SIMON]. Last modifications on : Friday, 07-Jan-2005 16:40:56 CET
Generated by XML to HTML Library for easy Web :: libX4easyWeb:: byas(c) - CIRIL. [v.20040921]

Info contextuelle au service sélectionné :

- Débit
- Localisation
- Statut

Liste des services indisponibles

Graph configurable : Utilisation globale du réseau

Tableau de bord pour *hotline*

https://eboard.e-lorraine.net - eBoard :: Tableau de bord e-LorraineHD - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

e-Lorraine :: netVIS :: CIRIL

Home

eAlarm

Valider alerte SMS

Basculer la permanence

Tableau de bord

eBoard

What's Up

Echantillon type

Translations NAT

Utilisation des lignes

Indicateurs

Boîte à outils

Looking Glass

Chercher un site

CVS des configs e-Lorraine

Métrieologie

netMET e-LorraineHD

Certificat SSL

Installez-moi la CA du CIRIL

eBoard :: Tableau de bord e-LorraineHD

Liaisons spécialisées

Informations gw-116-AGR-0570086J incident

RNE 0570086J Download 2048 kb/s
 Type liaison TDSL 2CA 250 kb/s
 Tronc : PVC 1 : 1/135 320 kb/s
 Interco. CCR 172.25.1.206 250 kb/s
 Interco. site 172.25.1.205 Upload
 Localisation Lycee agricole
 eStatus COURCELLES-CHAUSSY easy-graph-it
 RTT = 187 ms Site at a glance

Recherches 3 Sites injoignables

gw-131-PUB-0573491K 0d 00:20
 gw-062-CFA-0542389D 85d 08:10
 DNS2-TRANSPAC 101d 07:45

Trafic du CCR vers et depuis 0570086J

	Max	M1n	AVG	Last
site->CCR(in)	131.9 kb/s	682.0 b/s	30.9 kb/s	1.1 kb/s
CCR->site(out)	1.7 Mb/s	566.6 b/s	284.1 kb/s	1.5 kb/s

From Thu Oct 25 16:42:41 2007 to Fri Oct 26 16:42:41 2007

Temps de reponse (RTT en ms) vers 0570086J

■ min of 20 pings
 ■ average of 20 pings
 ■ max of 20 pings

From Thu Oct 25 16:42:41 2007 to Fri Oct 26 16:42:41 2007

du graphique

netMET e-Lorraine <-> Lot4

What's UP

QoS sur échantillons type

Temp. Du Fri-25/10/2007 00:00 au Sam-27/10/2007 00:00

Tronc TDSL 2 Last update : vendredi 26 octobre 2007 16:43:12

Document created by [Alexandre SIMON]. Last modifications on : Friday, 07-Jan-2005 16:40:56 CET
 Generated by XML to HTML library for easy Web :: www.easyweb.fr byas(C) - CIRIL. [v.20040921]

- En cours
 - des développements de fonctionnalités
 - du paramétrage pour superviser tous les services

- En quelques chiffres
 - 20 métriques : cpu, trafic, SAA, température, ...
 - Plus de 3000 services
 - 265 routeurs
 - 650 commutateurs
 - 40 serveurs
 - 8 onduleurs
 - En production
 - Depuis mars 2007 pour l'équipe réseau du CIRIL
 - Bientôt pour les correspondants

Questions

