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

JRES 2007

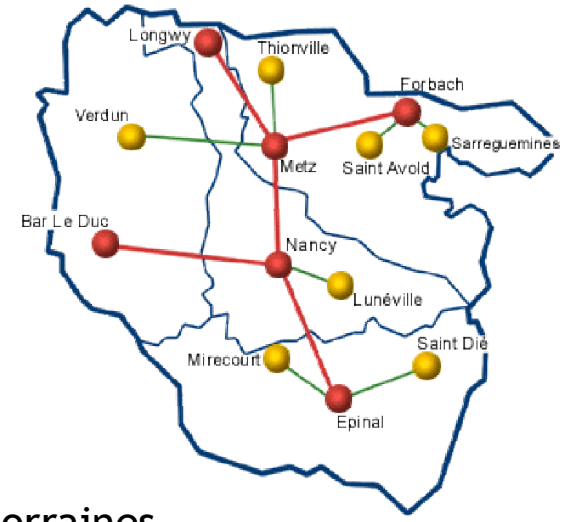
21 novembre 2007

Vincent.Delove@ciril.fr
Sebastien.Morosi@ciril.fr

Au programme

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

Introduction



- 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

Au programme

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

Besoins identifiés

- 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

Besoins identifiés

- 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

Besoins identifiés

- 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

La solution retenue

- 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

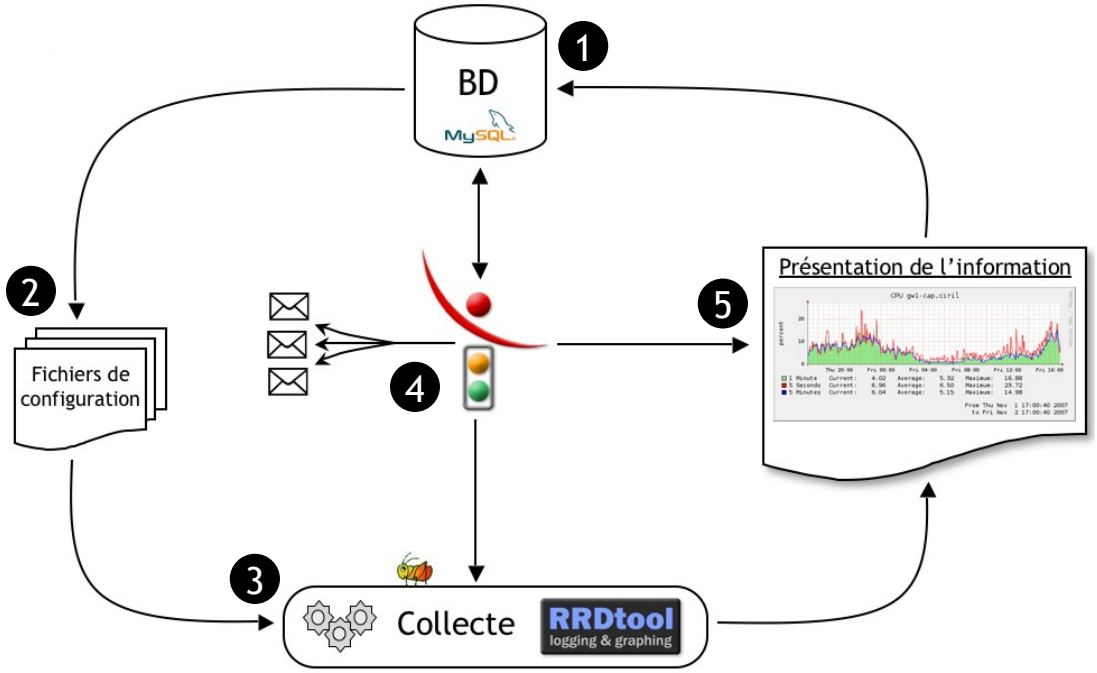
Au programme

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

Notions élémentaires

- *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 pemet d'avoir une représentation globale du service « liaison Nancy-Metz »

Synoptique



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, …)

La collecte

- 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

Centralisation et automatisation

- 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

Pérennité des informations

- 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

Au programme

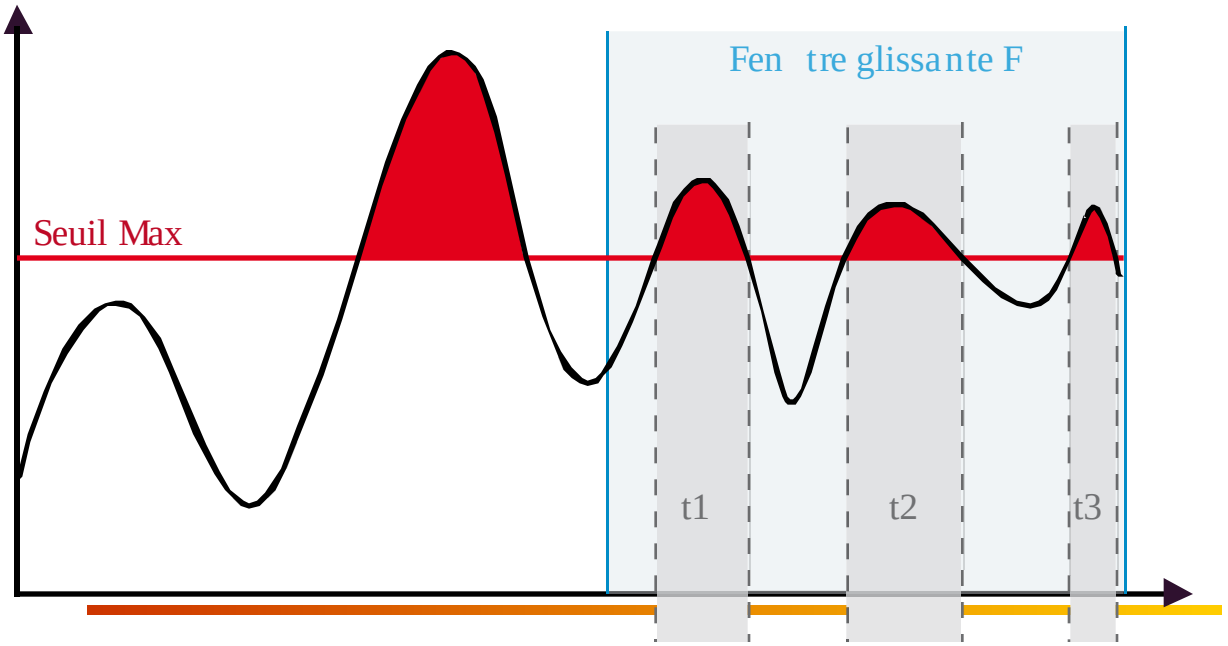
- Introduction
- Besoins identifiés
- iSup : Concepts et fonctionnement
- Analyse et alertes
- Présentation de l'information
- Bilan

Analyser les données

- Pourquoi ?
  - faciliter le travail de l'administrateur
    - détecter les pannes
    - anticiper les disfonctionnements
  - 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

Analyser les données

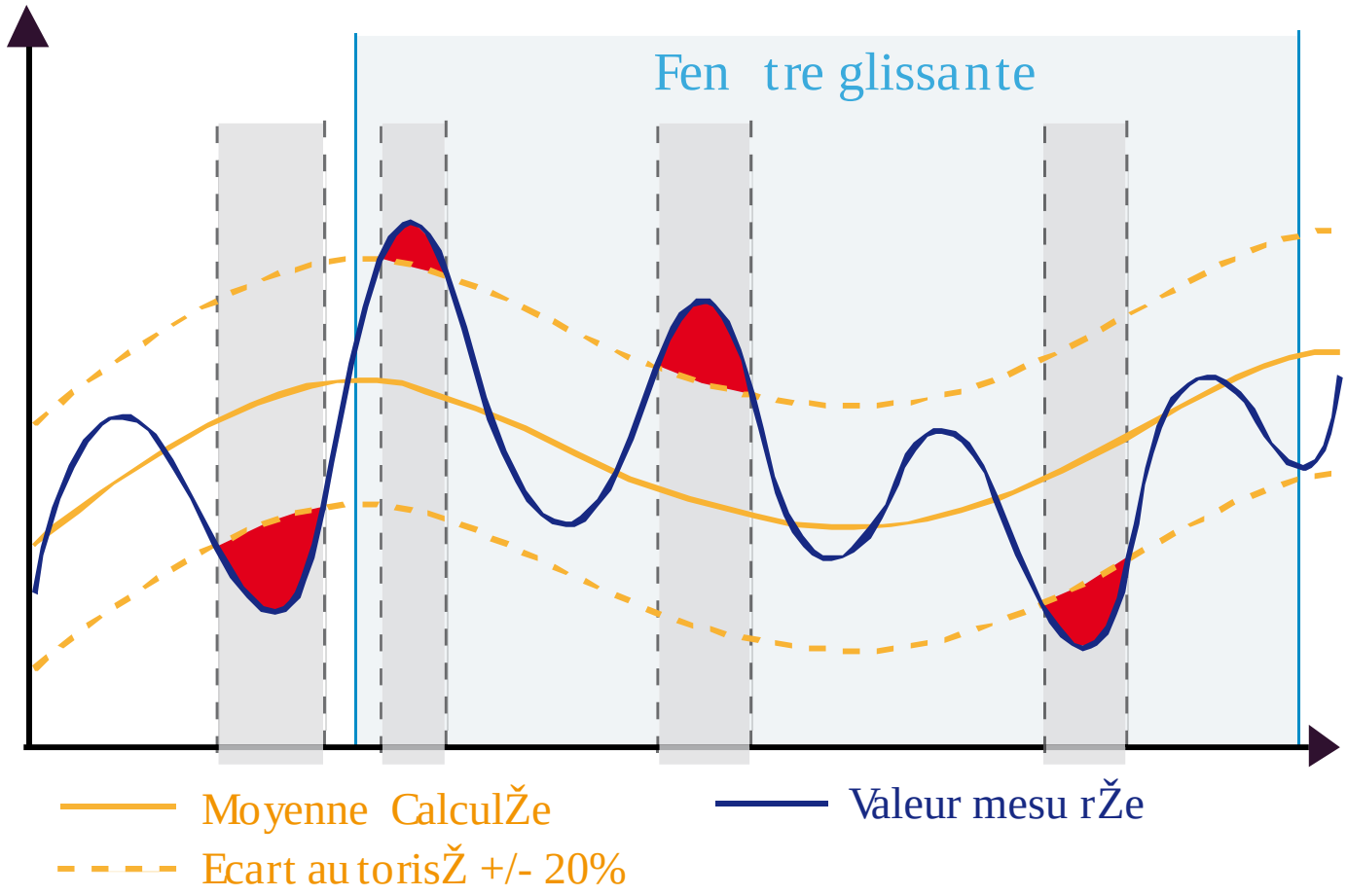
- Anticiper une panne
  - sur le dépassement d'un seuil critique
    - *risque important de fausse alerte*
  - nécessité d'algorithmes plus élaborés
    - fenêtre glissante
    - dépassement cumulé de seuils



Analyser les données

- 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

Analyser les données



Les états

- 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 disfonctionnement 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

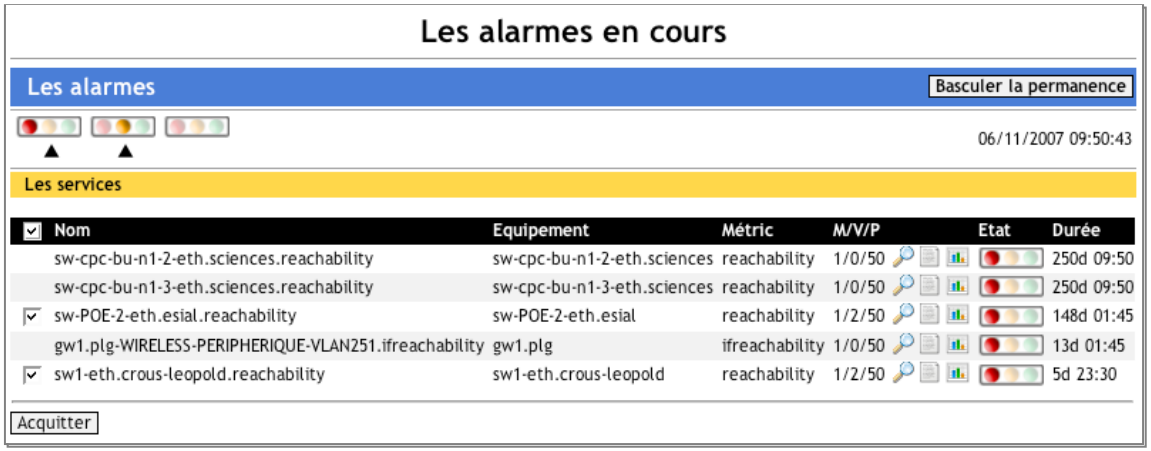
Alerter

- 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

Conserver l'historique

- 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



Au programme

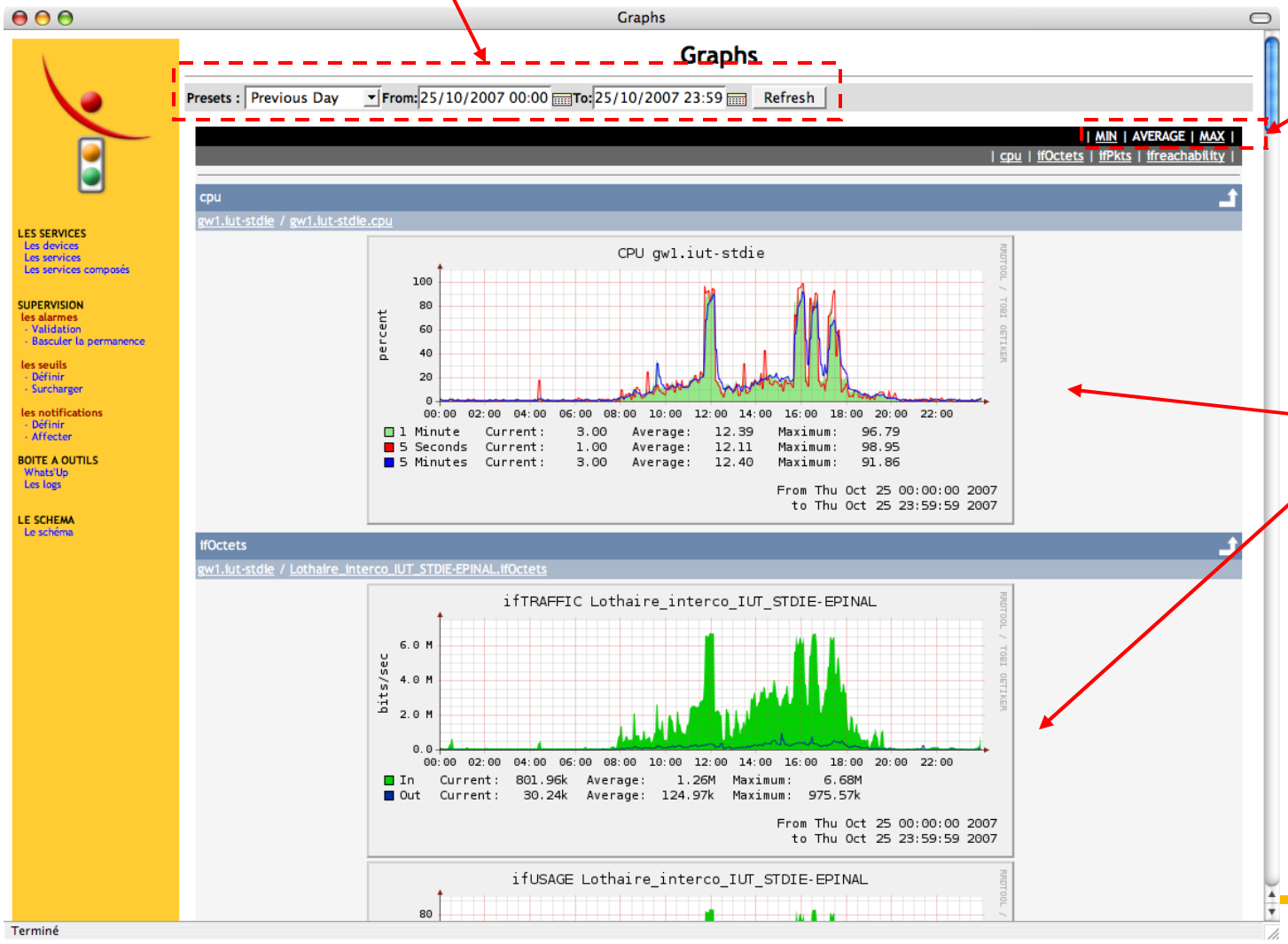
- Introduction
- Besoins identifiés
- iSup : Concepts et fonctionnement
- Analyse et alertes
- Présentation de l'information
- Bilan

Présenter l'information

- 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

Présentation de l'information

Choisir la période d'affichage



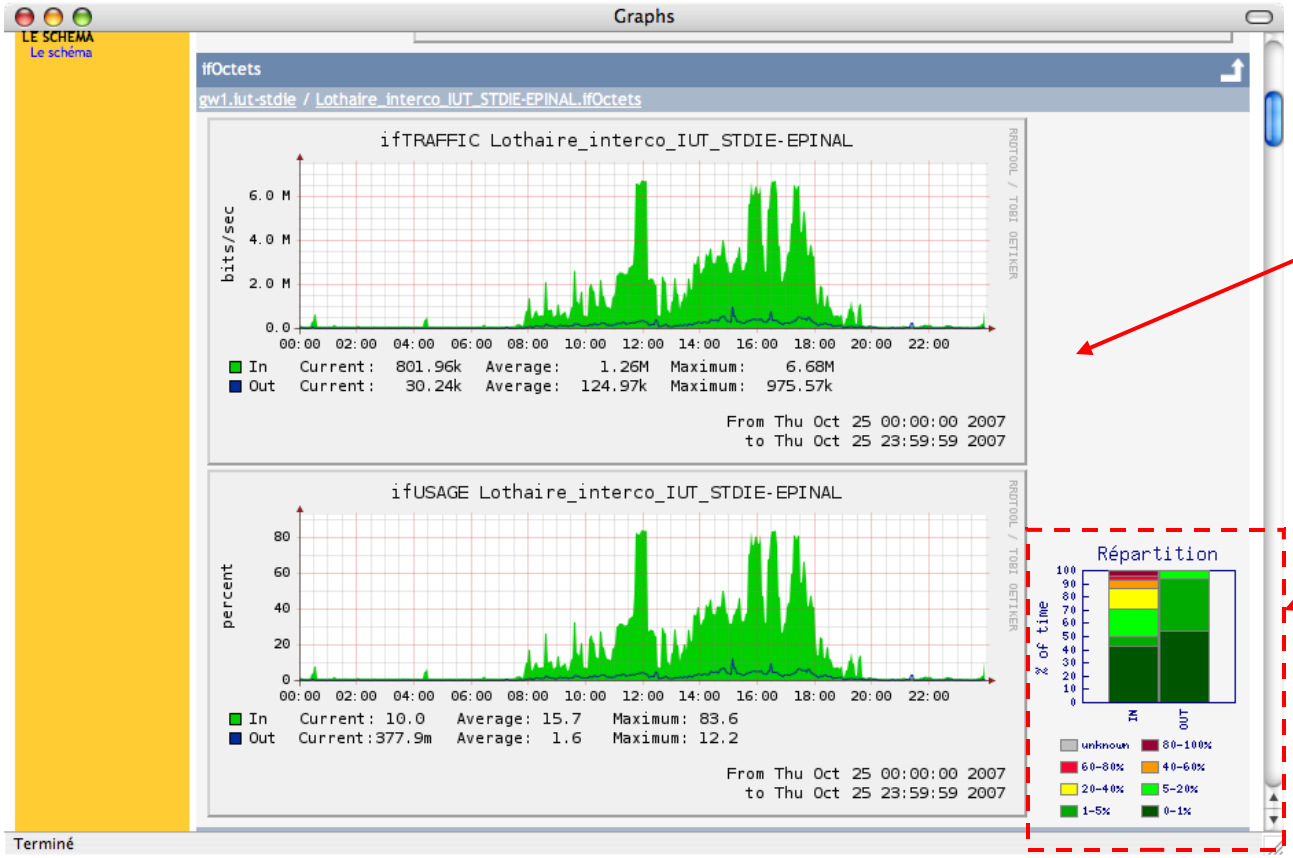
Choisir la valeur représentée :

- Minimum
- Moyenne
- Maximum

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

Présentation de l'information

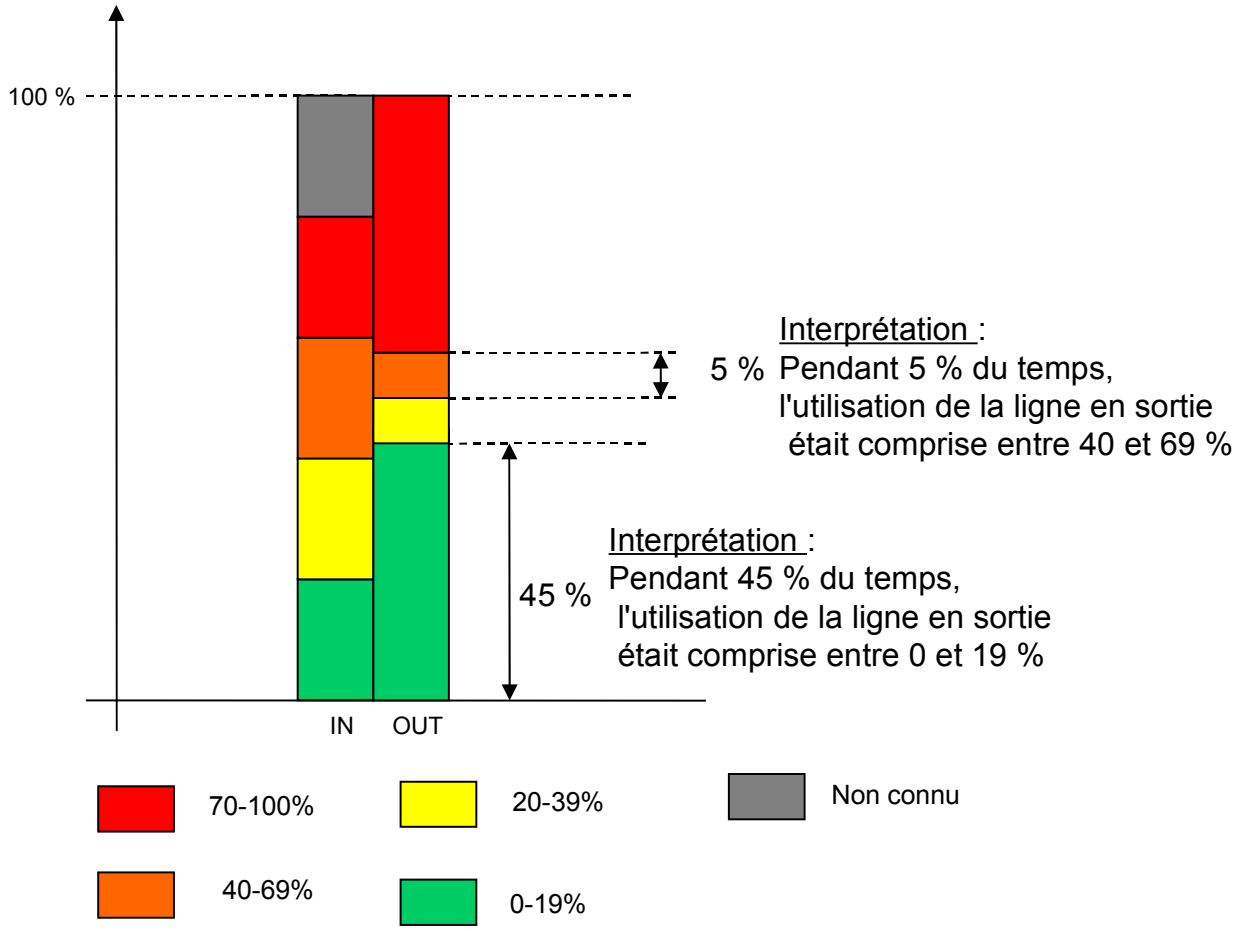
- Proposer un même indicateur avec des vues complémentaires
  - trafic sur une liaison et taux d'utilisation de ligne



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



Exemple de rapport

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

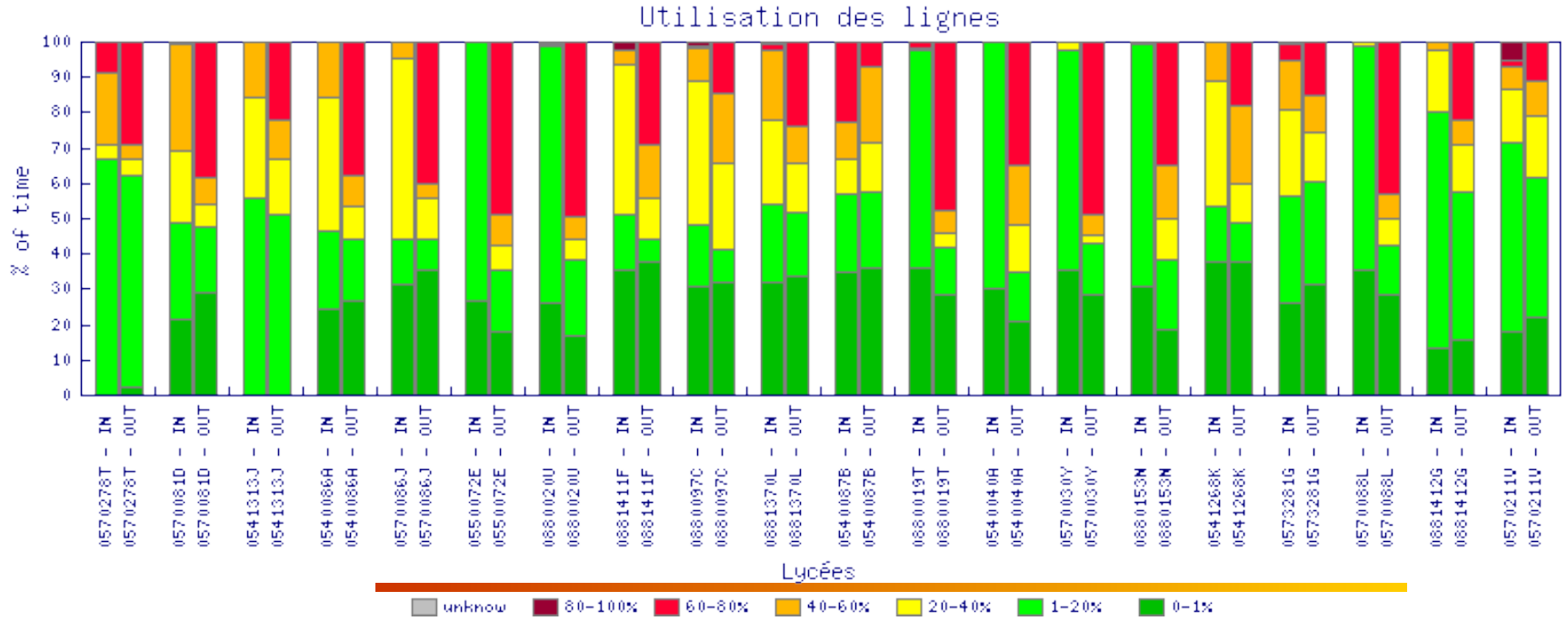
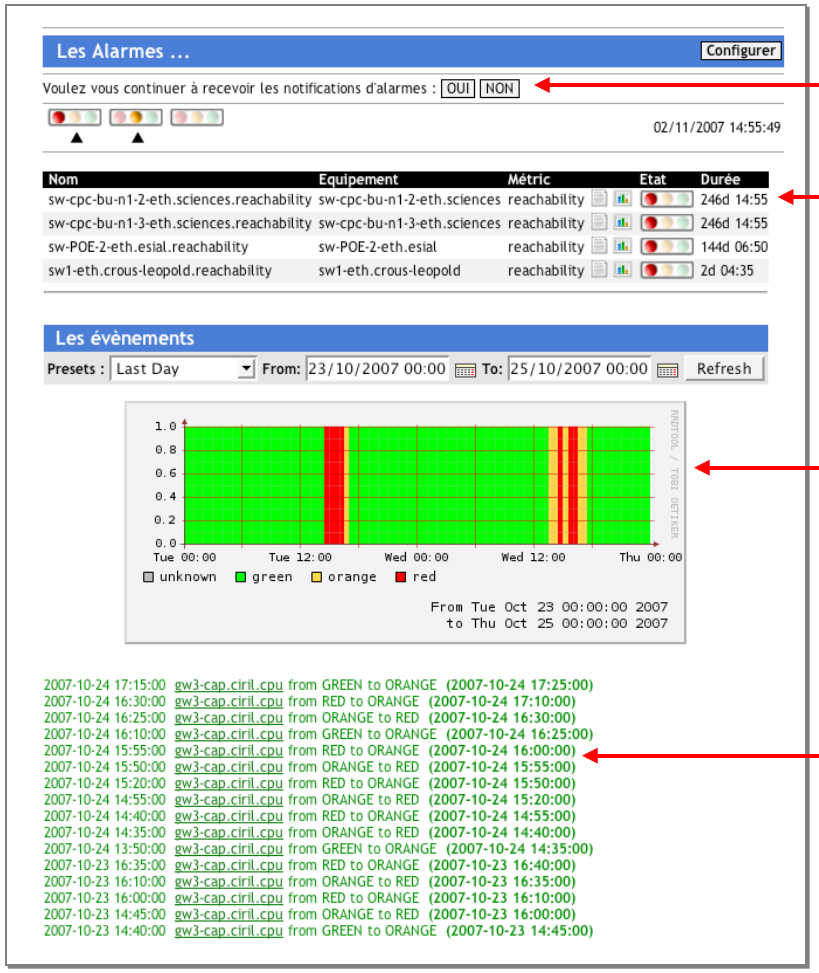


Tableau de bord pour *correspondants*



Configuration de la notification des alarmes

Alarmes en cours

Graphique de disponibilité du service

Journal des évènements

Tableau de bord pour *correspondants*

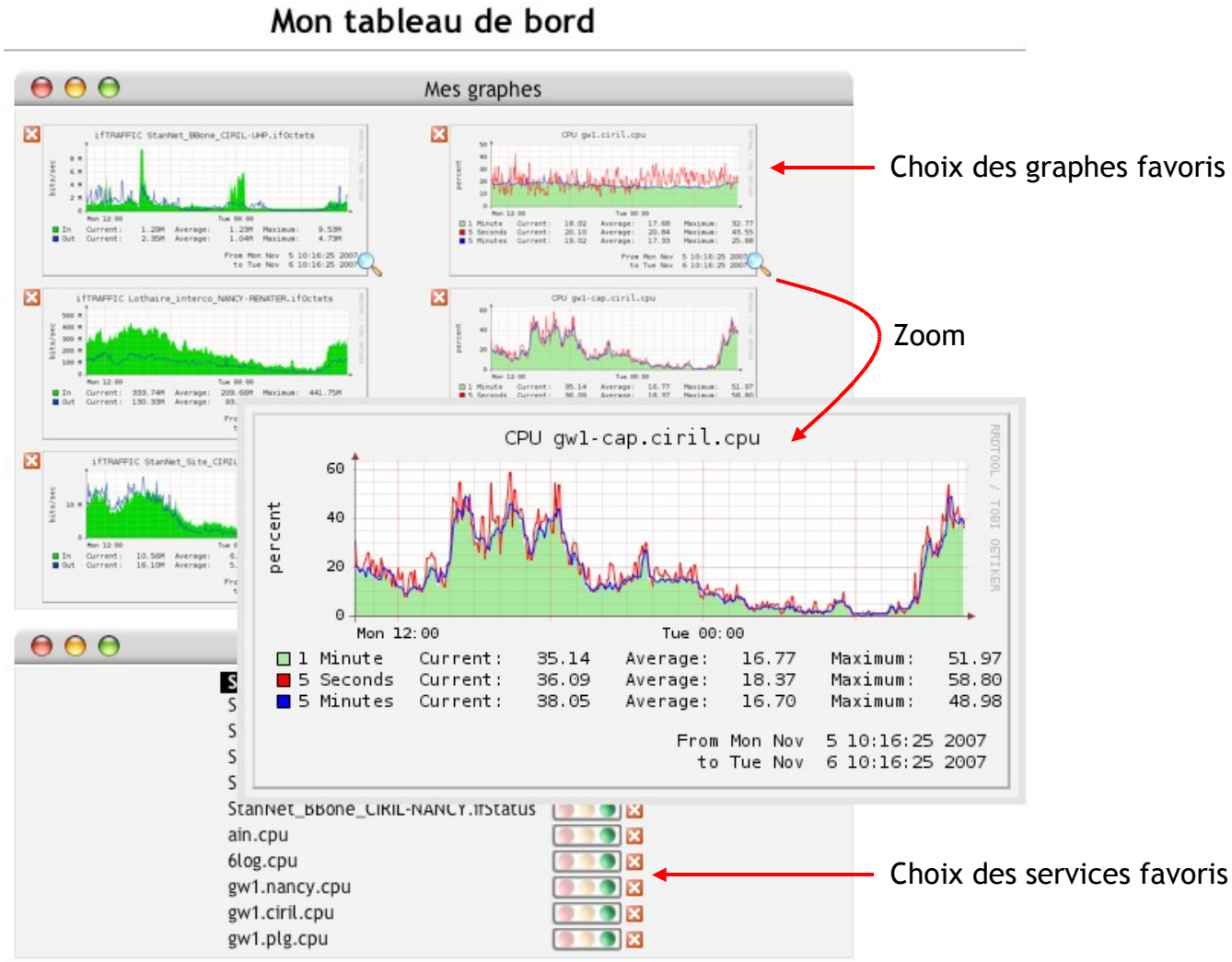
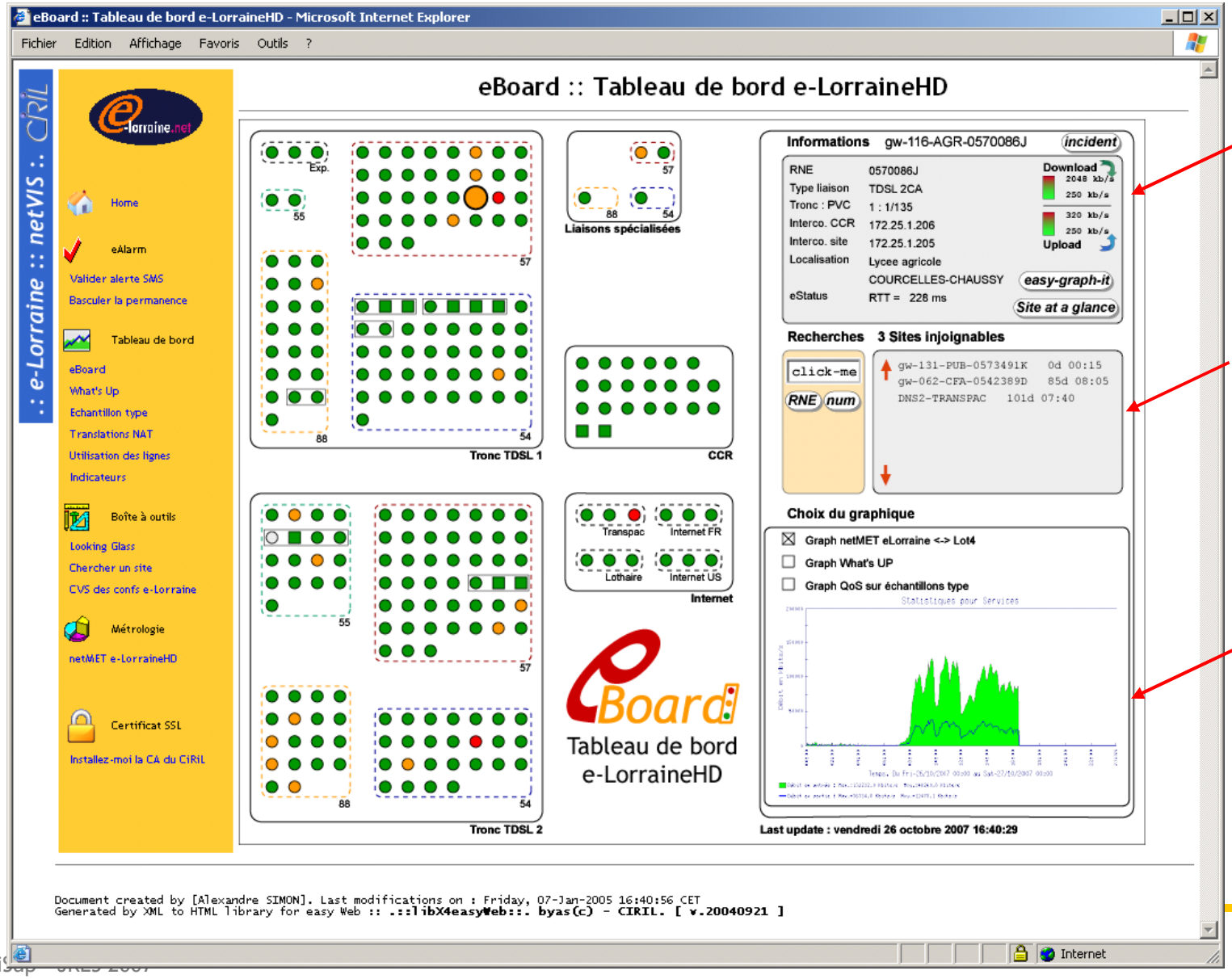


Tableau de bord pour *hotline*

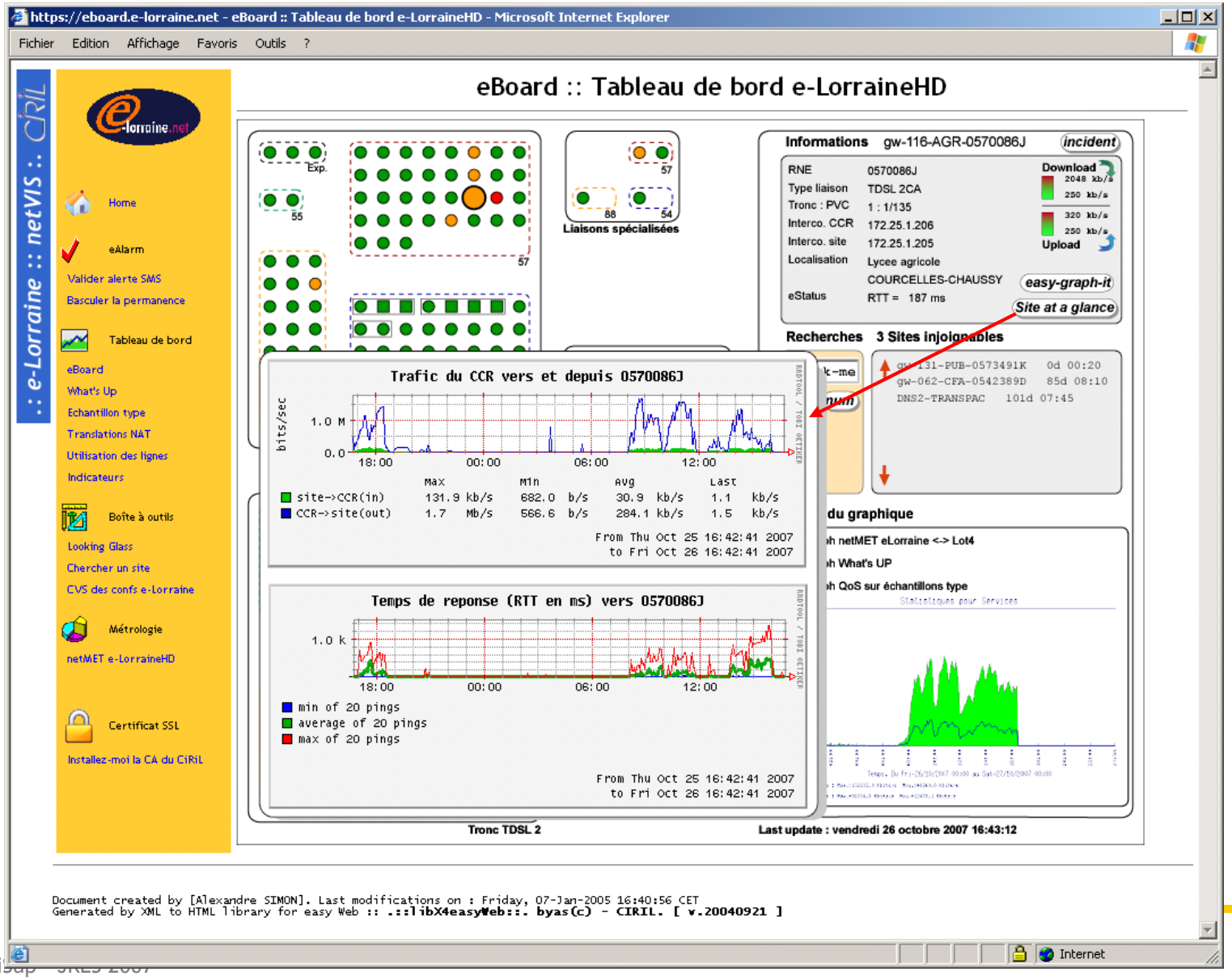


Info contextuelle au service sélectionné :
- Débit
- Localisation
- Statut

Liste des services indisponibles

Graph configurable : Utilisation globale du réseau

Tableau de bord pour *hotline*



Bilan

- 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