



## Gestion et Supervisions des Réseaux

# Introduction à la gestion et supervision des réseaux



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

# Partie I : Présentation générale

## Principaux concepts présentés :

- Qu'entend-on par supervision de réseau ?
- Qu'entend-on par gestion de réseau ?
- Pourquoi une gestion de réseau ?
- Les trois grands
- Consolidation des données
- Vue d'ensemble

# Gestion de réseau

## Ce que nous surveillons :

- **Systemes et services**
  - Accessibilité, disponibilité
- **Ressources**
  - Planification et disponibilité des capacités
- **Performances**
  - Temps de RTT, débit
- **Changements et configurations**
  - Documentation, suivi des révisions, journalisation

# Gestion de réseau (suite)

## Nous assurons un suivi des

- **Statistiques**
  - À des fins de comptabilisation/mesure
- **Anomalies (détection des intrusions)**
  - Détection des problèmes
  - Dépannage et historique des problèmes
- Les systèmes de tickets sont performants dans ce domaine
- Les centres d'assistance (help desk) sont une composante utile voire indispensable

# Attentes

Un réseau doit faire l'objet d'une surveillance :

- Respect des contrats de niveau de service (Service Level Agreements)
- Les SLA sont tributaires de la politique
  - Attentes de la direction ?
  - Attentes des usagers ?
  - Attentes des clients ?
  - Exigences à l'échelle de l'Internet ?
- Un temps utilisable de 99,999 % est-il suffisant ?
  - Aucun réseau ne fonctionne à 100 % (nous allons le voir) →

# Attentes en matière de "temps utilisable"

## Conditions d'un fonctionnement à 99,9 % ?

$30,5 \times 24 = 732$  heures par mois

$(732 - (732 \times 0,999)) \times 60 = 44$  minutes

seulement 45 minutes d'arrêt par mois !

## Besoin d'un arrêt de 1 heure / semaine ?

$(732 - 4) / 732 \times 100 = 99,4$  %

*N'oubliez pas d'inclure la maintenance planifiée dans vos calculs et de préciser à vos utilisateurs/clients s'ils font ou non partie du SLA*

## Comment mesure-t-on la disponibilité ?

Au cœur du système ? De bout en bout ?

Depuis l'Internet ?

# Éléments de base

**Qu'est-ce qui peut être considéré normal pour votre réseau ?**

Si vous n'avez jamais mesuré ni supervisé votre réseau, vous devrez connaître un certain nombre de paramètres :

- La charge type sur les liens (→ Cacti)
- Le niveau de fluctuation entre des points de terminaison (→ Smokeping)
- Le pourcentage type d'utilisation des ressources
- Niveau de "bruit" type :
  - Balayages du réseau
  - Données perdues
  - Erreurs ou défaillances signalées

# À quelles fins ?

## **Déterminer le moment où une mise à niveau est nécessaire**

- L'utilisation de la bande passante est-elle trop élevée ?
- Où va le trafic ?
- Faut-il une ligne plus rapide ou plus de fournisseurs ?
- L'équipement est-il trop ancien ?

## **Garder trace des changements**

- Consignez tous les changements
- Vous pourrez identifier plus facilement les problèmes liés aux mises à niveau et modifications de configuration

## **Conserver l'historique des opérations réseau**

- Un système de tickets vous permet de garder l'historique des événements
- L'historique vous permet de vous défendre et de vérifier ce qu'il s'est passé.



# Pourquoi une gestion de réseau ?

## Comptabilisation

- Suivi de l'utilisation des ressources
- Facturation des clients en fonction de l'utilisation

## Être informé des problèmes

- Avoir une longueur d'avance sur les utilisateurs est bon pour votre image.
- Des logiciels de surveillance peuvent générer des tickets et informent automatiquement le personnel des problèmes.

## Tendances

- Toutes ces informations permettent de visualiser les tendances au sein du réseau.
- Elles font partie intégrante de la création du référentiel, de la planification des capacités et de la détection des attaques.

# Pourquoi une gestion de réseau ?

## Sécurité

- Difficile de savoir si un problème est une panne ou attaque en cours
  - Différence entre un déni de services (DoS) et une panne de réseau ?
- Tendances et automatisation vous permettrons de savoir si vous êtes en cours d'attaque
- Les outils utilisés peuvent aider à mitiger le succès d'une attaque:
  - Les flux sur un interface
  - Une charge anormale sur des serveurs spécifiques.
  - Des pannes de service

# Les "Trois Grands"

## Disponibilité

- [Nagios](#) Services, serveurs, routeurs, commutateurs

## Fiabilité

- [Smokeping](#) État de la connexion, rtt, temps de réponse des services, latence

## Performances

- [Cacti](#) Trafic total, utilisation des ports, UC, RAM, Disque, processus

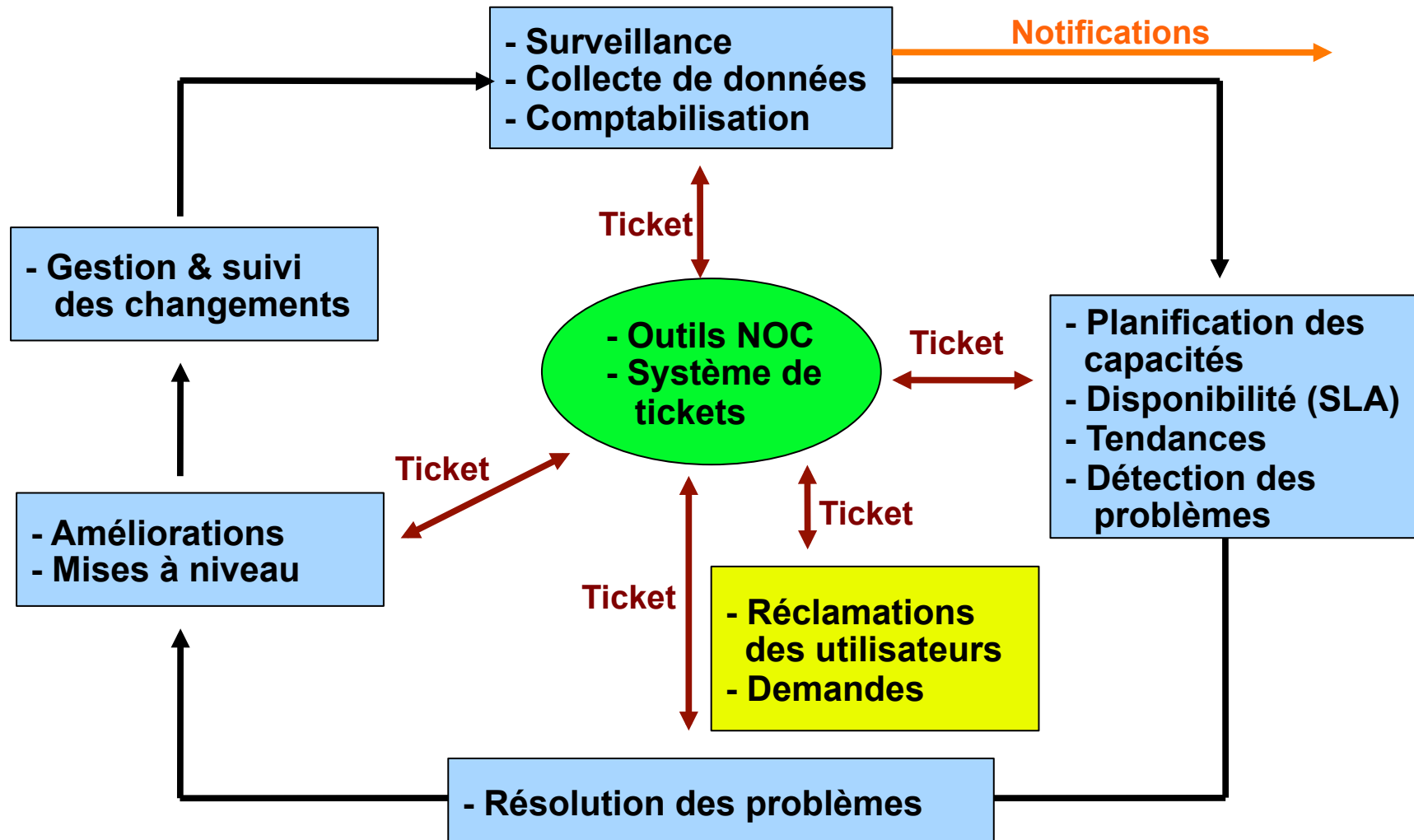
*Les fonctions de ces programmes se chevauchent en partie !*

# Consolidation des données

## Le Centre d'exploitation du réseau (NOC) "Cœur du réseau"

- Coordination des tâches
- État du réseau et des services
- Remontée des incidents réseau et des réclamations
- Centralisation des outils ("serveur NOC")
- Documentation comprenant :
  - Les schémas du réseau
  - La base de données/le fichier plat de chaque port de chaque commutateur
  - La description du réseau
  - Et bien d'autres ressources, comme vous allez le voir.

# Vue d'ensemble



# Quelques solutions open source...

## Performances

- Cricket
- IFPFM
- flowc
- mrtg\*
- NetFlow\*
- NfSen\*
- ntop
- perfSONAR
- pmacct
- rrdtool\*
- SmokePing\*

## Tickets

- RT\*
- Trac\*
- Redmine

## Gestion des changements

- Mercurial
- Rancid\* (routeurs)
- CVS\*
- Subversion\*
- Git\*

## Sécurité/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

## Journalisation

- swatch\*
- syslog/rsyslog\*
- tenshi\*

- ## Gestion du réseau
- Big Brother
  - Big Sister
  - Cacti\*
  - Hyperic
  - Munin
  - Nagios\*
  - OpenNMS\*
  - Sysmon
  - Zabbix

## Documentation

- IPplan
- Netdisco
- Netdot\*
- Rack Table

## Protocoles/Utilitaires

- SNMP\*, Perl, ping

# Questions ?

?

# Partie II : Précisions

## Quelques précisions sur les concepts de base :

- Outils de diagnostic
- Outils de surveillance
- Outils de performances
- Outils actifs et passifs
- SNMP
- Système de tickets
- Gestion des configurations et des changements



# Systemes et outils de surveillance réseau

## Trois types d'outils

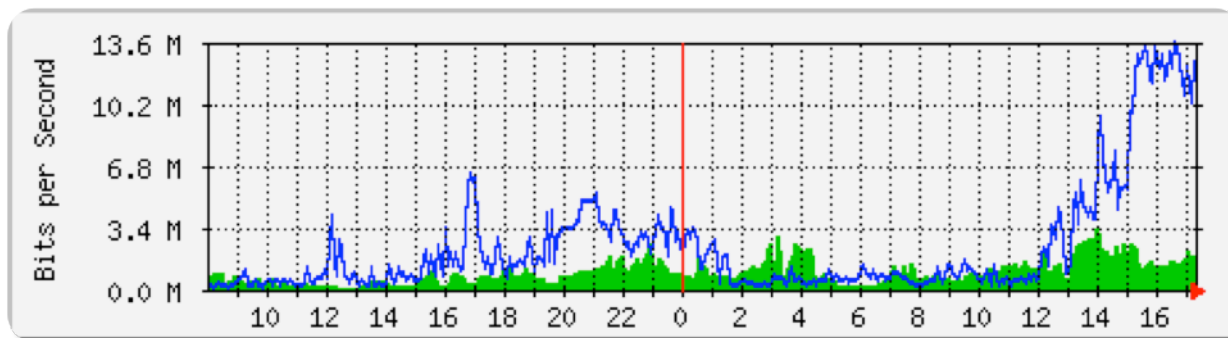
1. **Outils de diagnostic** – permettent de tester la connectivité, de vérifier l'accessibilité d'un site ou le fonctionnement d'un dispositif – il s'agit généralement d'outils actifs.
2. **Outils de surveillance** – outils fonctionnant en arrière-plan ("démons" ou services), chargés de collecter des événements mais également de procéder à leurs propres sondages (au moyen d'outils de diagnostic), et d'enregistrer les résultats de manière planifiée.
3. **Outils de performances** – indiquent comment le réseau gère les flux de trafic.

# Systemes et outils de surveillance reseau

Il s'agit de superviser chaque interface de routeur (sans avoir necessairement besoin de verifier les ports commutateurs).

Deux outils classiques :

- Netflow/NfSen : <http://nfsen.sourceforge.net/>
- MRTG : <http://oss.oetiker.ch/mrtg/>



MRTG = "Multi Router Traffic Grapher", grapheur de trafic multirouteur

# Systemes et outils de surveillance réseau

## Outils actifs

- Ping – test de connectivité vers un hôte
- Traceroute – vérification du chemin vers un hôte
- MTR – combinaison de ping + traceroute
- Collecteurs SNMP (scrutation)

## Outils passifs

- Surveillance des journaux, récepteurs de trap SNMP, NetFlow

## Outils automatisés

- SmokePing – enregistrement et représentation graphique de la latence pour un ensemble d'hôtes avec ICMP (Ping) ou d'autres protocoles
- MRTG/RRD – enregistrement et représentation graphique de l'utilisation de la largeur de bande sur un port de commutation ou une liaison réseau à intervalles réguliers

# Systemes et outils de surveillance réseau

## Outils de surveillance du réseau et des services

- Nagios – supervision de serveur et de services
  - Peut quasiment tout superviser
  - HTTP, SMTP, DNS, espace disque, utilisation de l'UC...
  - Nouveaux plugins faciles à écrire (extensions)
- Compétences de base nécessaires pour développer des scripts de supervision simples – Perl, scripts Shell, php, etc.
- Beaucoup de bons outils open source
  - Zabbix, ZenOSS, Hyperic, OpenNMS...

## Pour superviser l'accessibilité et la latence du réseau

- Les mécanismes de dépendance parent-enfant sont très utiles !

# Systemes et outils de surveillance réseau

## Surveillez vos services réseau critiques

- DNS/Web/courrier électronique
- Radius/LDAP/SQL
- SSH vers les routeurs

## Quid des notifications ?

## N'oubliez pas de collecter les journaux !

- Chaque périphérique du réseau (et serveur UNIX et Windows) peut signaler des événements système au moyen de syslog
- Vous **DEVEZ** récupérer et surveiller vos journaux !
- Négliger de le faire constitue l'une des erreurs les plus courantes en matière de surveillance réseau

# Protocoles de gestion réseau

## SNMP – Simple Network Management Protocol

- Un standard de l'industrie avec des centaines d'outils pour l'exploiter
- Présent sur tout équipement de réseau digne de ce nom
  - Débit du réseau, erreurs, charge de l'UC, température...
- Environnements UNIX et Windows également
  - Espace disque, processus en cours d'exécution...

## SSH et telnet

- Il est également possible d'automatiser par des scripts la supervision des hôtes et des services

# Outils SNMP

## Ensemble d'outils Net SNMP

- <http://net-snmp.sourceforge.net/>

## Pour construire facilement des outils simples

- Un outil pour obtenir des instantanés des IP utilisés par les différentes adresses Ethernet
- Un autre pour des instantanés des adresses Ethernet et des ports et commutateurs correspondants
- ou pour interroger une série de contrôleurs RAID distants afin d'en connaître l'état
- ou encore des serveurs, commutateurs et routeurs afin d'en connaître la température.
- Etc.

# Outils statistiques et de comptabilisation

## Mesure et analyse du trafic

- Usage et intensité d'utilisation de votre réseau
- Mesure de la qualité du service, détection des abus et facturation
- Protocole dédié : NetFlow
- Identification des "flux" de trafic : protocole, source, destination, octets
- Il existe différents outils pour traiter l'information

→ Flowtools, flowc

→ NFSen

→ Et bien d'autres encore :

<http://www.networkuptime.com/tools/netflow/>



# Gestion des erreurs et des problèmes

## Problème transitoire ?

- Surcharge, ressources momentanément insuffisantes

## Problème permanent ?

- Panne matérielle, interruption d'une liaison

## Comment détecter les erreurs ?

- Surveillance !
- Réclamations clients

## Un système de tickets s'impose

- Ouvrez un ticket pour suivre un événement (planifié ou accidentel)
- Définissez les règles d'affectation/escalade
  - Qui est chargé de gérer le problème ?
  - Qui est le responsable suivant en cas d'indisponibilité ?

# Systemes de tickets

## En quoi sont-ils importants ?

- Suivi de tous les événements, pannes et problèmes

**Élément central pour la communication avec le service d'assistance**

**Suivi de toutes les communications**

- Internes et externes

**Événements d'origine externe :**

- Réclamations clients

**Événements internes :**

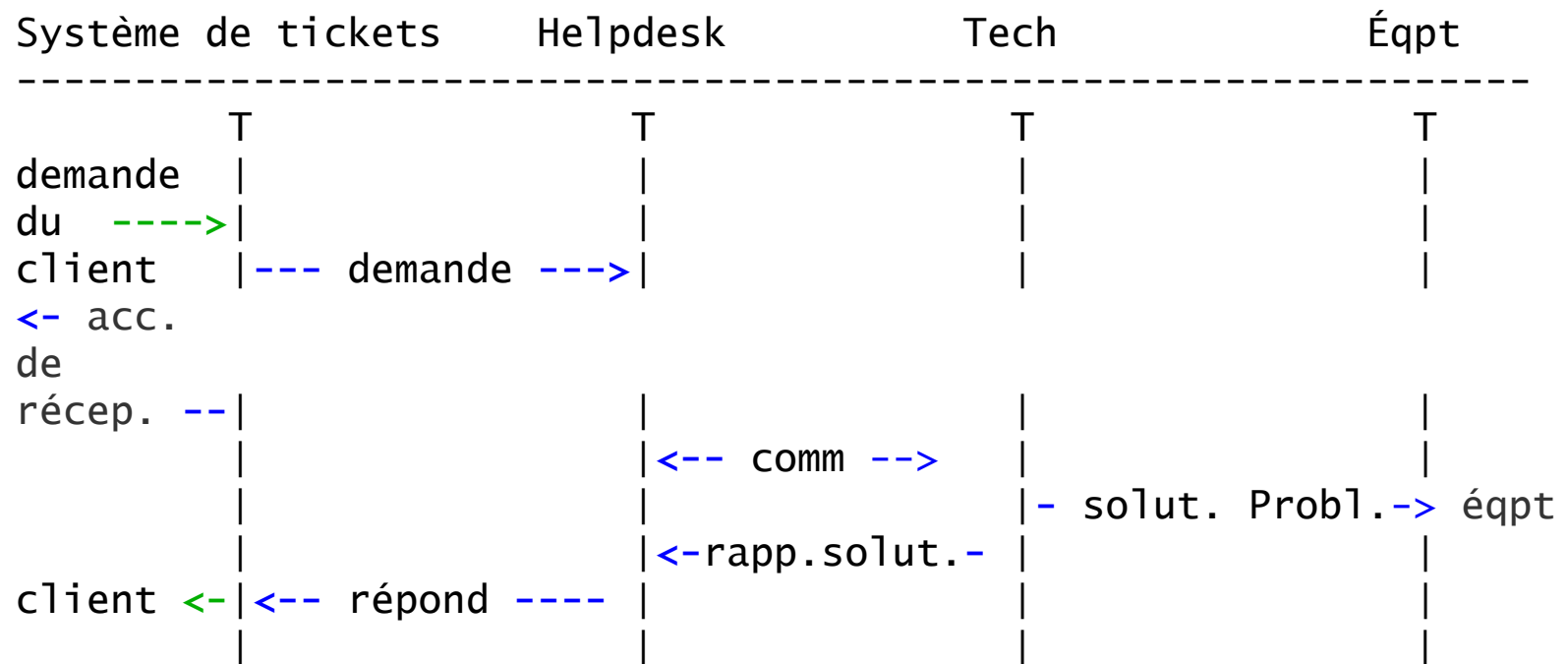
- Pannes du système (directes ou indirectes)
- Maintenances ou mises à niveau planifiées – n'oubliez pas d'en informer vos clients !

# Systemes de tickets

- Utilisez le système de tickets pour suivre chaque dossier, y compris les communications internes entre techniciens
- Un numéro est attribué à chaque dossier
- Chaque dossier passe par un cycle de vie similaire :
  - Nouveau
  - Ouvert
  - ...
  - Résolu
  - Fermé

# Systemes de tickets

## Déroulement des opérations



# Systemes de tickets : exemples

## **rt (request tracker)**

- Largement utilisé à travers le monde.
- Système de tickets classique, personnalisable en fonction du lieu.
- Relativement complexe à installer et à configurer.
- Gère les opérations à grande échelle.

## **trac**

- Système hybride intégrant un wiki et des fonctionnalités de gestion de projet.
- Moins robuste que RT mais fonctionne bien.
- Souvent utilisé pour suivre des projets de groupe.

## **Redmine**

- Semblable à trac, mais plus robuste. Plus difficile à installer.

# Systemes de détection d'intrusions dans le réseau (NIDS)

Ces systèmes observent tout le trafic du réseau et signalent les problèmes spécifiques tels que :

- des hôtes infectés ou source de spams.

## Quelques outils :

- **SNORT** - SNORT – outil open source couramment utilisé :  
<http://www.snort.org/>
- **Prelude** – système de gestion des informations de sécurité  
<https://dev.prelude-technologies.com/>
- **Samhain** – HIDS centralisé  
<http://la-samhna.de/samhain/>
- **Nessus** - recherche de failles :  
<http://www.nessus.org/download/>

# Gestion et surveillance des configurations

- Enregistrement des changements de configuration des équipements par *gestion des versions* (s'applique également aux fichiers de configuration)
- Gestion des stocks (équipements, IP, interfaces)
- Utilisation de la gestion des versions
  - Aussi simple que :  

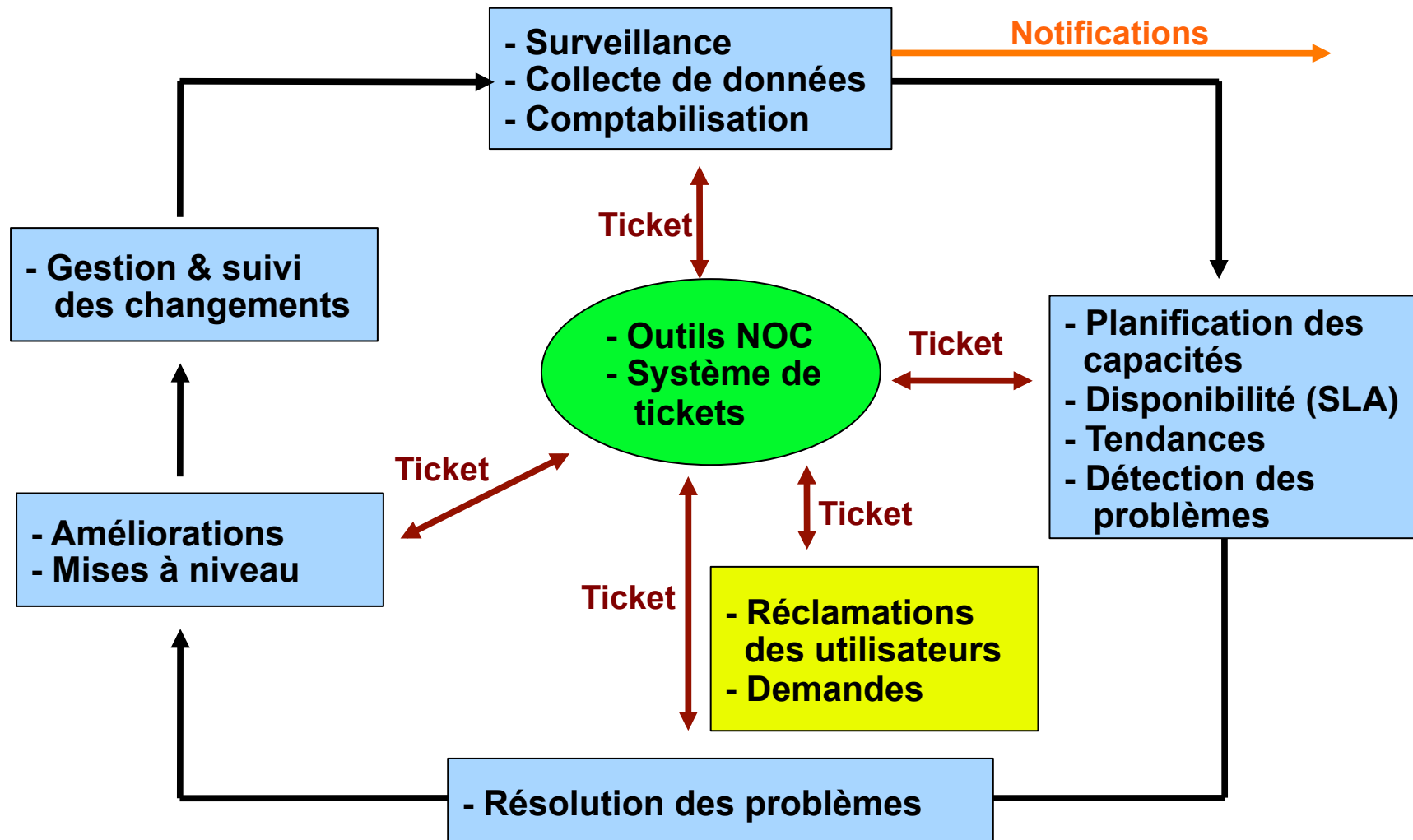
```
"cp named.conf named.conf.20070827-01"
```
- Pour les fichiers de configuration simples :
  - **CVS, Subversion (SVN)**
  - **Mercurial**
- Pour les routeurs :
  - **RANCID**

# Gestion et surveillance des configurations

- Traditionnellement utilisé pour le code source (programmes)
- Fonctionne parfaitement avec tout fichier texte de configuration
  - Ainsi qu'avec les fichiers binaires, mais les différences sont moins facilement identifiables
- Pour les équipements réseau :
  - **RANCID** (récupération et archivage automatiques de la configuration Cisco et d'autres types d'équipements)
- Intégré dans certains logiciels de gestion de projets tels que
  - **Trac**
  - **Redmine**
  - Et dans un grand nombre d'autres produits wiki. Grande efficacité pour documenter un réseau.



# Vue d'ensemble... de nouveau



# Questions

?