Surveillance du réseau et de gestion

Introduction à la supervision et à la gestion de réseaux

Partie I : présentation générale

Principaux concepts présentés :

- Qu'entend-on par supervision de réseau
- Qu'entend-on par gestion de réseau
- Démarrage
- Pourquoi une gestion de réseau
- Détection des attaques
- Consolidation des données
- Vue d'ensemble

Qu’entend-on par supervision de réseau ?

Une définition ?

Supervision d’un réseau de communication actif afin de diagnostiquer les problèmes et de recueillir des statistiques d’administration et d’ajustement.

PC MAGAZINE

Network Management

…the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

Operation: keeping the network (and the services that the network provides) up and running smoothly. It *includes monitoring the network* to spot problems as soon as possible, ideally before users are affected.

Administration: deals with keeping track of resources in the network and how they are assigned.

Maintenance: concerned with performing repairs and upgrades. Maintenance also involves corrective and preventive measures to make the managed network run "better".

Provisioning: is concerned with configuring resources in the network to support a given service.

FCAPS

Fault, **C**onfiguration, **A**ccounting, **P**erformance and **S**ecurity
(The ISO Telecommunications Management Network model and framework for network management)

Source: wikipedia

Network Management Details

We Monitor

- **System & Services**
  - Available, reachable
- **Resources**
  - Expansion planning, maintain availability
- **Performance**
  - Round-trip-time, throughput
- **Changes and configurations**
  - Documentation, revision control, logging

Network Management Details

We Keep Track Of

- **Statistics**
  - For purposes of accounting and metering
- **Faults (Intrusion Detection)**
  - Detection of issues,
  - Troubleshooting issues and tracking their history

- Ticketing systems are good at this
- Help Desks are a useful to critical component

Qu'entend-on par gestion de réseau ?

- **Supervision des systèmes et services**
  - accessibilité, disponibilité
- **Mesure et supervision des ressources**
  - planification et disponibilité des capacités
- **Supervision des performances (temps de RTT, débit)**
- **Statistiques & comptabilisation/métrologie**
- **Gestion des fautes (détection des intrusions)**
  - détection des fautes, dépannage et suivi
  - système de tickets, centre d'assistance
- **Gestion et changements et supervision des configurations**

Démarrage

Nous allons superviser le réseau afin de vérifier qu'il est en service et fonctionne :

- contrat de niveau de service (SLA, Service Level Agreements)
- politique
  - → attentes de la direction ?
  - → attentes des usagers ?
  - → attentes des clients ?
  - → exigences à l'échelle d'internet ?
- une supervision 24x7 suffit-elle ?
  - → aucun réseau ne fonctionne à 100% (nous allons le voir) →

Démarrage : “temps utilisable”

Conditions d’un fonctionnement à 99,9 % ?

30,5 x 24 = 762 heures par mois

(762 – (762 x 0,999)) x 60 = 45 minutes

seulement 45 minutes d’arrêt par mois !

Besoin d’un arrêt d’1 heure/ semaine ?

(762 - 4) / 762 x 100 = 99,4 %

N’oubliez pas d’inclure dans vos calculs vos plannings de maintenance et de préciser à vos utilisateurs/ clients s’ils font partie du SLA

Comment mesure-t-on la disponibilité ?

Au coeur du système ? De bout en bout ? Depuis l’internet ?

Démarrage : 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 devez connaître un certain nombre de paramètres :

- charge sur les liens (➔ Cacti)
- gigue entre les extrémités (➔ Smokeping)
- pourcentage d'utilisation des ressources
- "bruit" :
  - balayages du réseau
  - données abandonnées
  - erreurs ou défaillances signalées

Pourquoi gérer le réseau ?

Mises à niveau

- 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 ?

Piste d'audit des changements

- consignation de tous les changements
- identification facilitée des problèmes liés aux mises à niveau et changements de configuration

Historique du fonctionnement du réseau

- historique des événements reposant sur un système de tickets
- moyen de justifier de votre gestion et de la vérifier.

Pourquoi gérer le réseau ? (suite)

Comptabilisation

- suivi de l'utilisation des ressources
- facturation des clients en fonction de l'utilisation

Etre informé des problèmes

- avoir une longueur d'avance sur les usagers !
- Des logiciels de supervision produisent des tickets qui informent automatiquement le personnel des problèmes

Tendances

- Toutes ces informations permettent de visualiser les tendances du réseau.
- Elles font partie des bases, de la planification des capacités et de la détection des attaques.

Les “Trois Grands”?

Disponibilité

- Nagios — Services, serveurs, routeurs, commutateurs

Fiabilité

- Smokeping — La santé de connexion, rtt, temps de réponse du services, temps de latence

Performance

- Cacti — L’ensemble du trafic, l’utilisation des ports, CPU, RAM, disque les processus

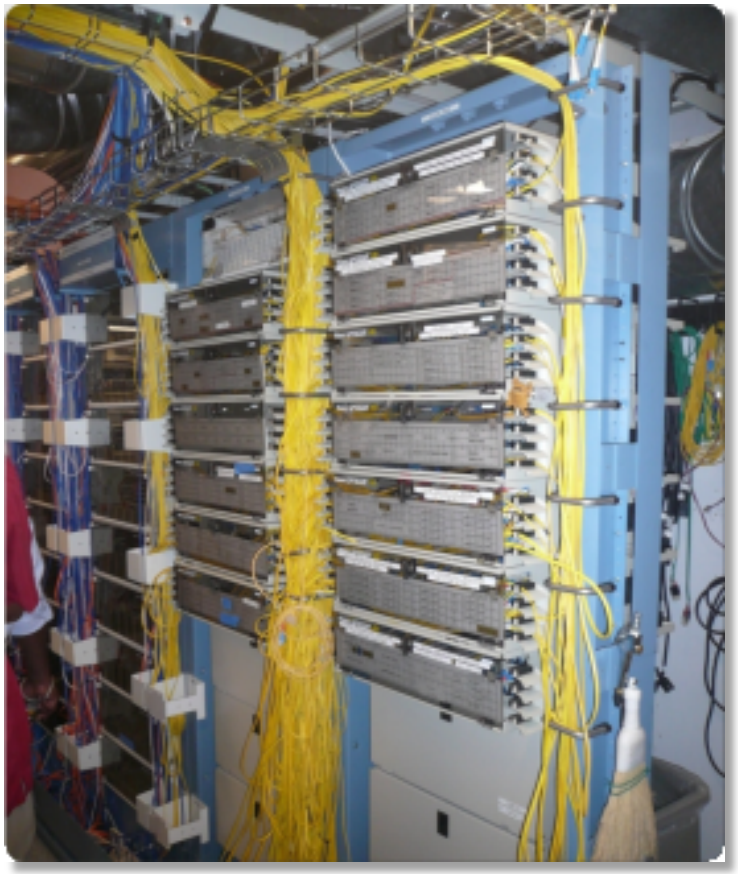
Fonctionnelle existe un chevauchement entre ces programmes!

Détection des attaques

- Les tendances et l'automatisation vous informent des attaques.
- Les outils peuvent vous aider à atténuer l'incidence des attaques :
  - flux à travers les interfaces du réseau
  - charge sur des serveurs ou services spécifiques
  - défaillances répétées.

Documentation

Vous vous demandez peut-être *comment conserver une trace de tout cela ?...*



… documentez, documentez, documentez…

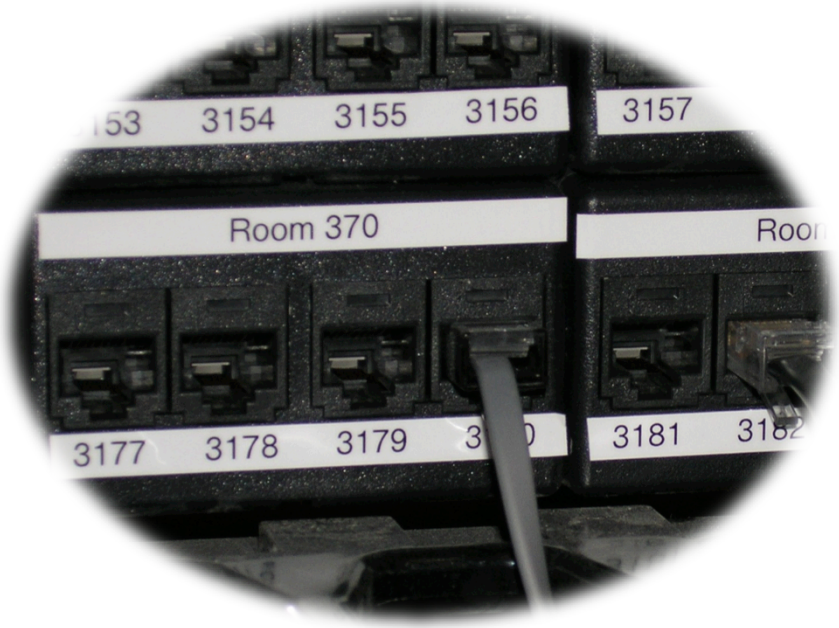
Documentation

Documentation de base, par exemple pour les commutateurs...

- A quoi chaque port est-il connecté ?
- Il peut s'agir d'un simple fichier texte avec une ligne pour chaque port de commutation :
  - health-switch1, port 1, salle 29 – bureau de la Direction
  - health-switch1, port 2, salle 43 – Réception
  - health-switch1, port 3, salle 100 – Salle de cours
  - health-switch1, port 4, salle 105 – Salle des formateurs
  - …..
  - health-switch1, port 25, liaison montante vers dorsale
- Ces informations peuvent être mise à la disposition de l'équipe réseau et du service d'assistance par un wiki, une interface logicielle, etc.
- N'oubliez pas d'étiqueter vos ports !

Documentation : étiquetage

Pratique…



Documentation du réseau

Besoin d'automatiser ? Un dispositif de documentation réseau automatisé peut être envisagé. Vous pouvez pour cela :

- écrire des scripts locaux
- envisager des systèmes de documentation automatisés
- voire finalement les deux.

Systèmes automatisés

Il existe plusieurs systèmes de documentation réseau automatisés, avec chacun ses spécificités :

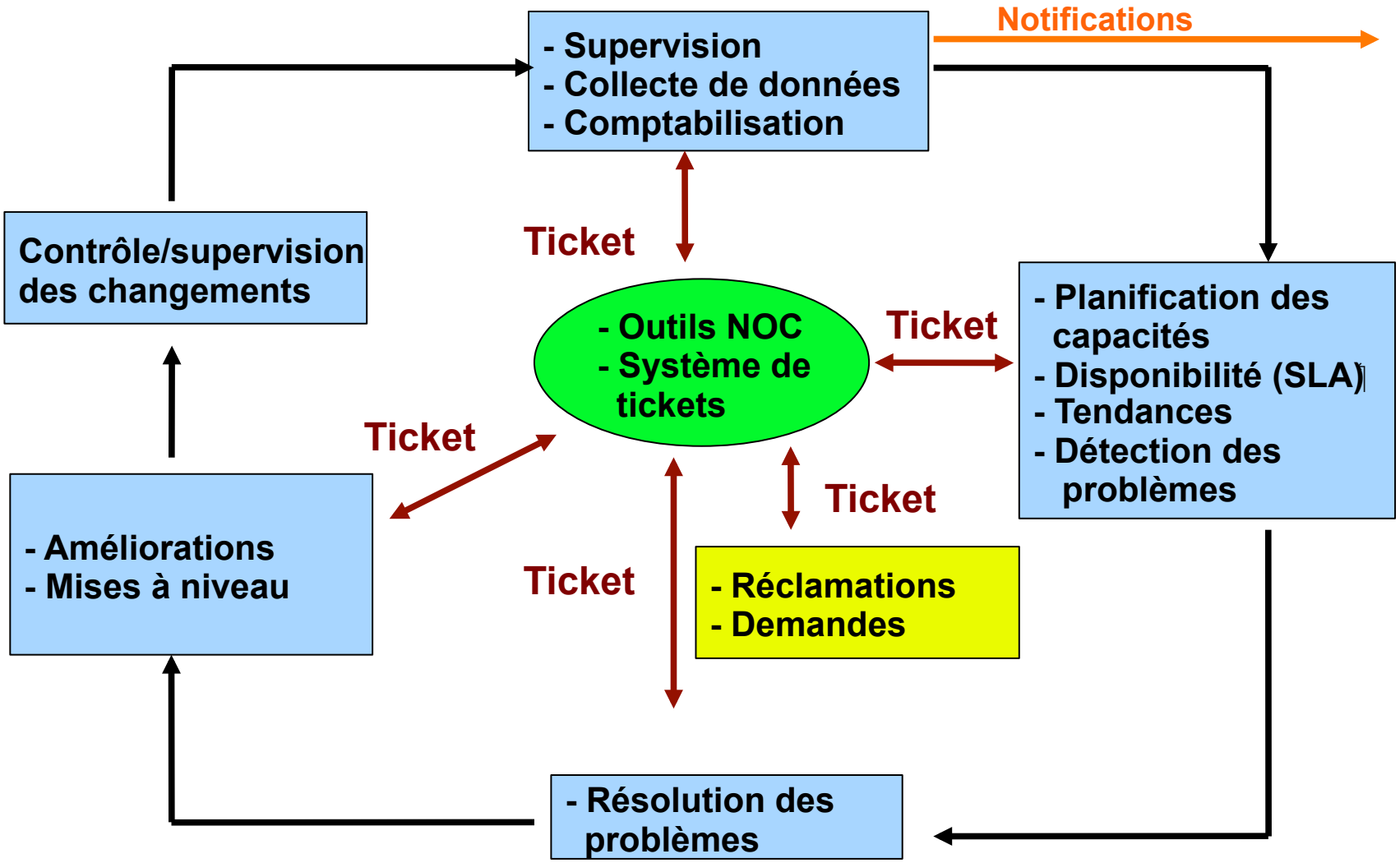
- IPplan:
  http://iptrack.sourceforge.net/
- Netdisco :
  http://netdisco.org/
- Netdot :
  https://netdot.uoregon.edu/

Consolidation des données

Le NOC (Network Operations Center), “coeur du réseau”

- coordination des tâches
- état du réseau et des services
- remontée des incidents et des réclamations
- centralisation des outils (“serveur NOC”)
- documentation incluant :
  - ➔ les schémas du réseau
  - ➔ la base de données/le fichier plat de chaque port de chaque commutateur
  - ➔ le descriptif du réseau
  - ➔ et bien d’autres ressources, vous le verrez un peu plus tard.

Vue d'ensemble



Quelques solutions libres …

Performances

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

Tickets

- RT*
- *Trac*,*
- *Redmine*

Gestion des changements

- Mercurial
- Rancid* (routers)
- CVS*
- Subversion
- git*

Securité/NIDS

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

Logging

- 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/Utilitie

- SNMP*, Perl, ping

Des questions ?

?