Programme
Opérations de registre avancées

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 ?

Des idées ?

PCMAG.COM

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

WIKIPEDIA

*L’expression **supervision de réseau** fait référence à un dispositif assurant la supervision constante d’un réseau d’ordinateurs afin d’en détecter les éléments lents ou défectueux et d’alerter l’administrateur par courrier électronique, signal ou tout autre dispositif de notification en cas d’interruption. Il s’agit d’un sous-ensemble des fonctions de gestion du réseau.*

Qu'entend-on par gestion de réseau ?

(Webopēdia)™

La notion de gestion de réseaux englobe au sens large la gestion de réseaux d'ordinateurs. Les administrateurs ont à leur disposition toute une panoplie de produits logiciels et matériels pour les aider dans cette tâche. La gestion de réseau porte en particulier sur :

- la **sécurité :** protéger le réseau contre des accès non autorisés.
- les **performances :** éviter les goulots d'étranglement.
- la **fiabilité :** veiller à ce que l'ensemble du réseau demeure disponible et apporter une réponse aux dysfonctionnements matériels et logiciels.

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 ?

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
- gigue entre les extrémités
- 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.

Détection des attaques

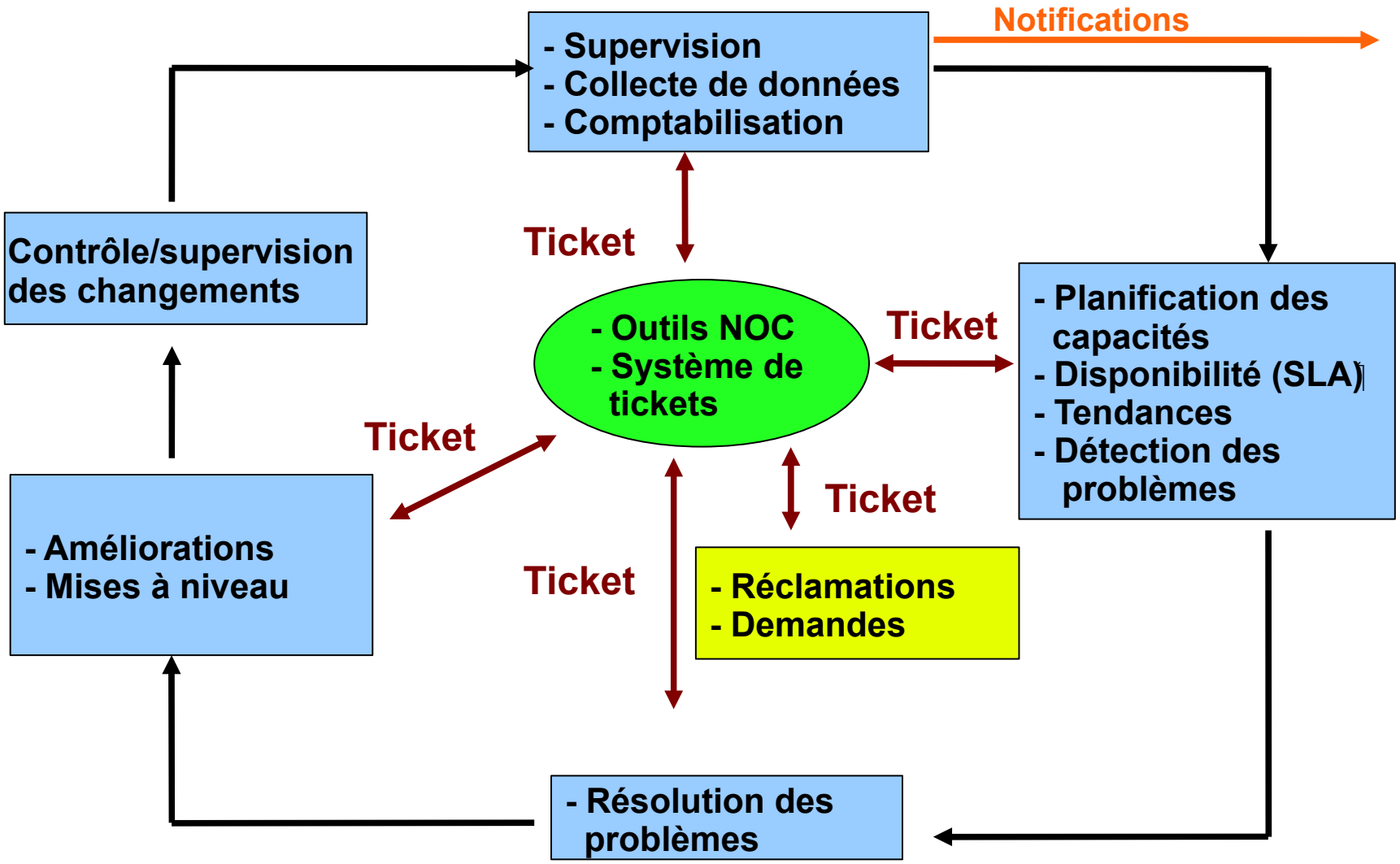
- Les tendances et l'automatisation vous informent des attaques.
- Les outils peuvent vous aider à atténuer l'incidence des attaques :
  - flux à travers les interfaces du réseau
  - charge sur des serveurs ou services spécifiques
  - défaillances répétées.

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
- pmacct
- rrdtool
- SmokePing
- SNMP/Perl/ping

Tickets

- RT, Trac, Redmine

Gestion des changements

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Sécurité/NIDS

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

Gestion du réseau

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

Des questions ?

?

Partie II : précisions

Quelques précisions sur les notions de base :

- documentation du réseau
- outils de diagnostic
- outils de supervision
- outils de performances
- outils actifs et passifs
- SNMP
- systèmes de tickets
- gestion des configurations et des changements

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/

IPplan : [[IPplan]]

D’après la page web d’IPplan :

IPplan est à la fois un logiciel web multilingue et gratuit de gestion d’adresses TCP IP (IMAP) et un outil de suivi en php 4, qui simplifie l’administration de l’espace d’adressage IP. IPplan surpasse la gestion d’adresses TCP IP en incluant l’administration de DNS, la gestion de fichiers de configuration, la gestion de circuits (personnalisable par des modèles) ainsi que le stockage d’informations sur le matériel (personnalisable par des modèles).

De nombreuses captures d’écran :

http://iptrack.sourceforge.net/doku.php?id=screenshots

Netdisco : 

- Projet lancé en 2003. Version 1.0, octobre 2009
- Quelques applications courantes de Netdisco :
  - **localisation** d'une machine du réseau par MAC ou IP et affichage de son port de commutation
  - **arrêt d'un port** tout en laissant une piste d'audit; documentation indiquant à l'administrateur le motif de l'arrêt
  - **inventaire** du matériel réseau par modèle, vendeur, carte de commutation, micrologiciel et système d'exploitation
  - **rapport** sur l'adresse IP et l'utilisation du port de commutation : historique et actuel
  - **représentations attrayantes** du réseau.

Netdot : {net.} NETwork DOcumentation Tool

Inclut, entre autres, les fonctions de IPplan et Netdisco. Principales fonctions :

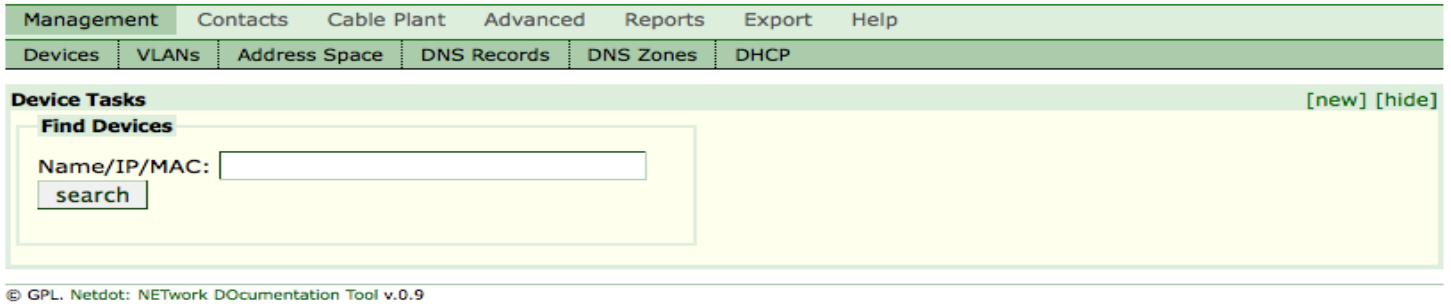
- découverte de périphériques par SNMP
- découverte de topologie de couche 2 et graphiques avec :
  - CDP/LLDP
  - Protocole STP
  - tables d'acheminement de commutation
  - sous-réseaux point à point avec routeurs
- Gestion d'espaces d'adressage IPv4 et IPv6 (IPAM)
  - visualisation des espaces d'adressage
  - gestion des configurations DNS/DHCP
  - suivi d'adresses IP et MAC

Suite ➔

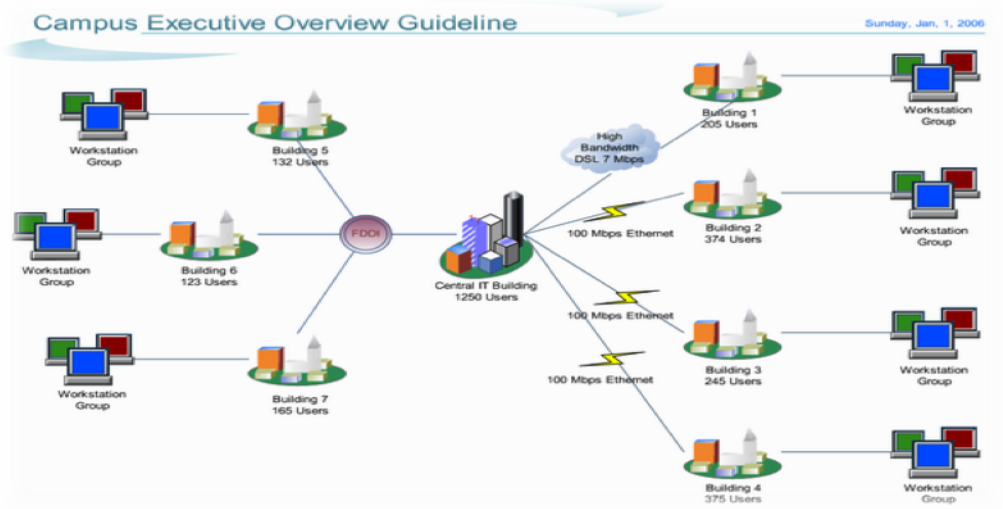
Netdot : {net.} NETwork DOcumentation Tool

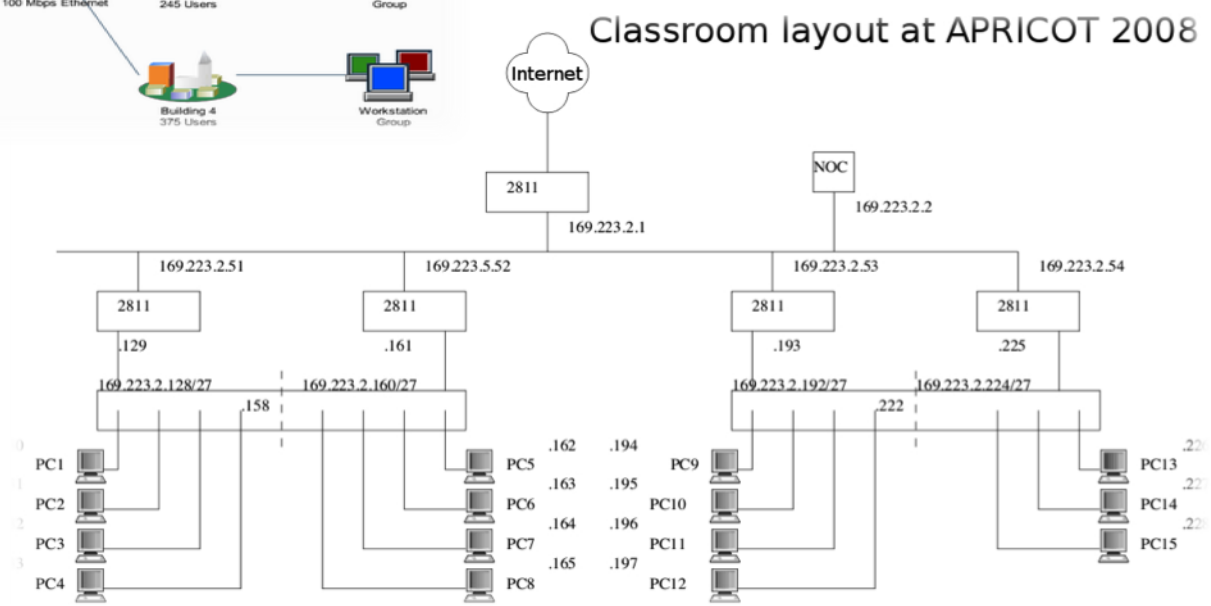
Fonctions (suite) :

- Réseau de câblage (sites, fibre, cuivre, armoires, circuits...)
- Contacts (départements, fournisseurs, vendeurs, etc.)
- Exportation de scripts pour différents outils (Nagios, Sysmon, RANCID, Cacti, etc.)
  - Ex. : comment automatiser la création de noeuds dans Cacti !
- Accès utilisateur multi-niveau : administrateur, opérateur, utilisateur
- Représentations attrayantes de votre réseau.



Documentation : schémas





Logiciel de schémas

Logiciels Windows

- Visio :

  http://office.microsoft.com/en-us/visio/FX100487861033.aspx

- Ezdraw :

  http://www.edrawsoft.com/

Logiciels libres

- Dia :

  http://live.gnome.org/Dia

- Icônes de référence Cisco :

  http://www.cisco.com/web/about/ac50/ac47/2.html

- Nagios Exchange :

  http://www.nagiosexchange.org/

Systèmes et outils de supervision réseau

Trois types d'outils

1. **Outils de diagnostic** – tests de connectivité, d'accessibilité, de fonctionnement des périphériques – il s'agit généralement d'outils actifs.

2. **Outils de supervision** – outils fonctionnant en arrière-plan ("démons" ou services), chargés de collecter des événements mais également de procéder à leurs propres sondages (par des outils de diagnostic), et d'enregistrer les résultats de manière planifiée.

3. **Outils de performances** – pour savoir comment le réseau gère les flux de trafic.

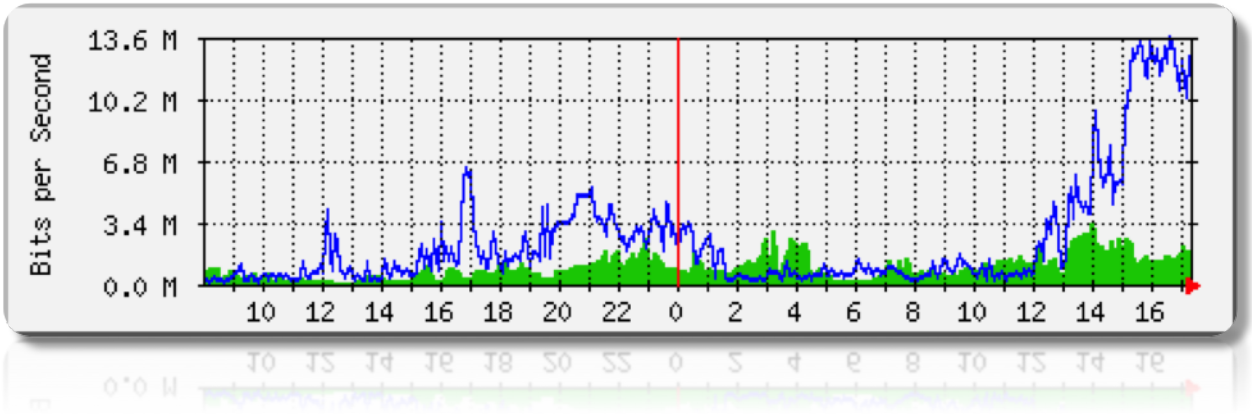
Systèmes et outils de supervision réseau

3. Outils de performances

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

Deux outils classiques :

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



MRTG = "Multi Router Traffic Grapher", logiciel de graphiques de trafic réseau multirouteur

Systèmes et outils de supervision réseau

Outils actifs

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

Outils passifs

- Surveillance des journaux, récepteurs de piège SNMP, NetFlow

Outils automatisés

- SmokePing – enregistrement et représentation graphique de la latence pour un ensemble d'hôtes avec ICMP (Ping) ou 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.

Systèmes et outils de supervision réseau

Outils de supervision 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, Shell scripts, php, etc...
- Beaucoup de bons outils libres
  - Zabbix, ZenOSS, Hyperic, OpenNMS ...

Pour superviser l'accessibilité et les latences du réseau

- Des mécanismes de dépendance parent-enfant sont

Systèmes et outils de supervision réseau

Surveillez vos services réseau critiques

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

Quid des notifications ?

N'oubliez 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 superviser vos journaux !
- négliger de le faire constitue l'une des erreurs les plus courantes en matière de supervision de réseau.

Protocoles de gestion réseau

SNMP – protocole de gestion réseau simple

- Standard de l'industrie, avec des centaines d'outils pour l'exploiter
- Présent sur n'importe quel équipement 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 de recourir 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.
- etc…

Outils statistiques et comptabilisation

Mesure et analyse du trafic

- À quoi sert votre réseau et à quelle intensité
- 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 plus : http://www.networkuptime.com/tools/netflow/

Gestion des erreurs et des problèmes

Problème transitoire ?

- surcharge, pénurie temporaire de ressources

Problème permanent ?

- défaillance d'équipement, interruption d'une liaison

Comment détecter les erreurs ?

- supervision !
- réclamations des clients

Un système de tickets s'impose

- ouvrez un ticket pour suivre un événement (planifié/erreur)
- définissez les règles de distribution/progression

→ qui est chargé de gérer le problème ?

Systèmes de tickets

En quoi sont-ils importants ?

- suivi de tous les événements, erreurs et problèmes

Au coeur de la communication avec le service d'assistance

Suivi de toutes les communications

- internes et externes

Evénements d'origine externe :

- réclamations des clients

Événements internes :

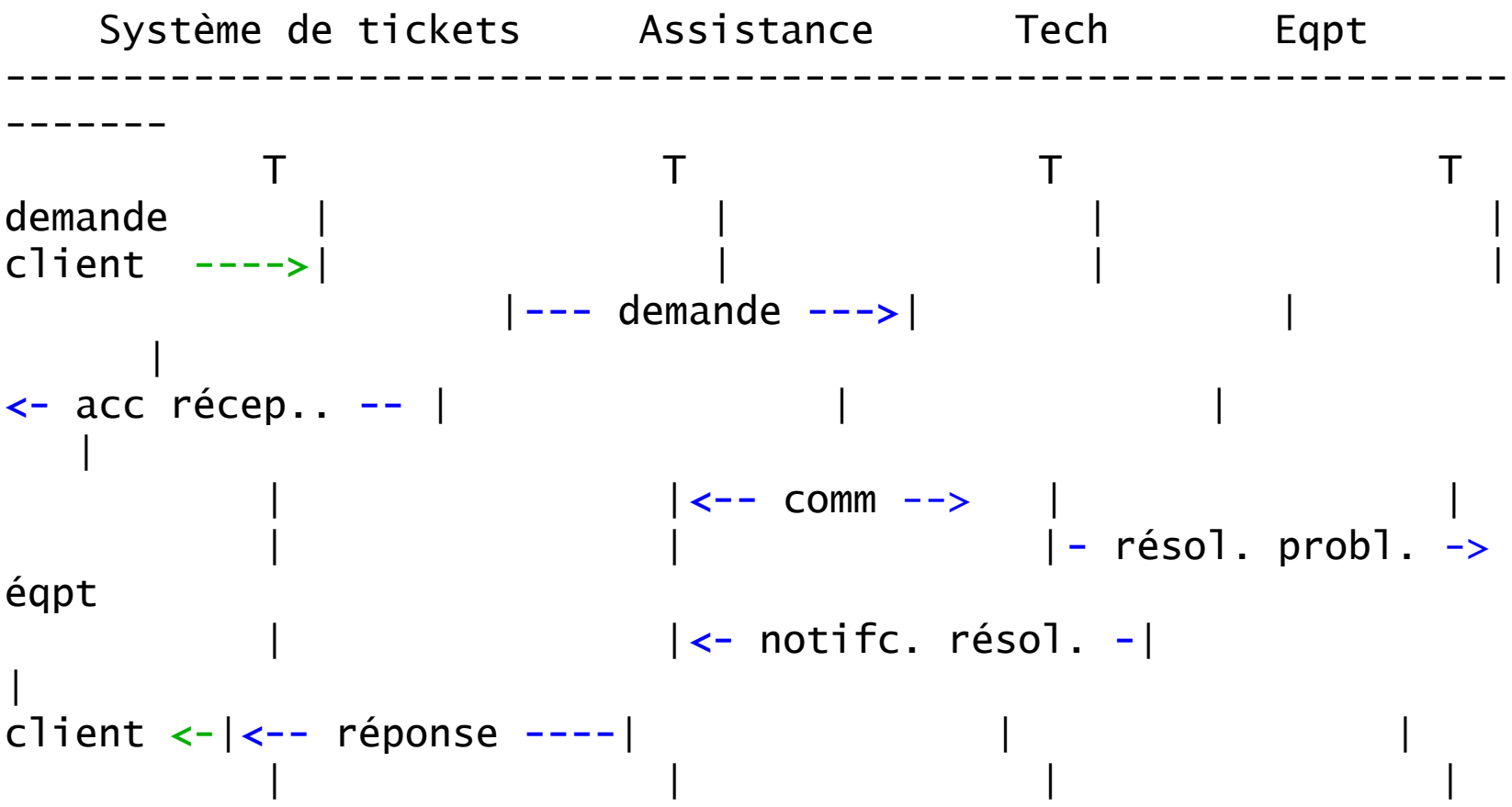
- interruptions du système (directes ou indirectes)
- maintenances ou mises à niveau planifiées – n'oubliez pas d'en informer vos clients !

Systèmes de tickets (suite)

- Les systèmes de tickets permettent de suivre chaque activité, y compris la communication interne entre les techniciens
- A chaque activité est associé un numéro
- Chaque activité passe par un cycle de vie similaire :
  - nouveau
  - ouvert
  - ...
  - résolu
  - fermé

Systèmes de tickets (suite)

Flux de travail :



Systèmes 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 des opérations à grande échelle.

Trac

- système hybride incluant un wiki et des fonctions de gestion de projets
- Moins robuste que RT mais fonctionne bien
- souvent utilisé pour “suivre” des projets de groupe.

Redmine

Systèmes de détection d'intrusions dans le réseau (NIDS)

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

- des hôtes infectés ou source de spams.

Quelques outils :

- **SNORT –** outil libre communément utilisé
  http://www.snort.org/
- **Prelude** – système de gestion des informations de sécurité
  https://dev.prelude-technologies.com/
- **Samhain –** HIDS centralisés
  http://la-samhna.de/samhain/
- **Nessus –** dépistage des faiblesses
  http://www.nessus.org/download/

Gestion et supervision des configurations

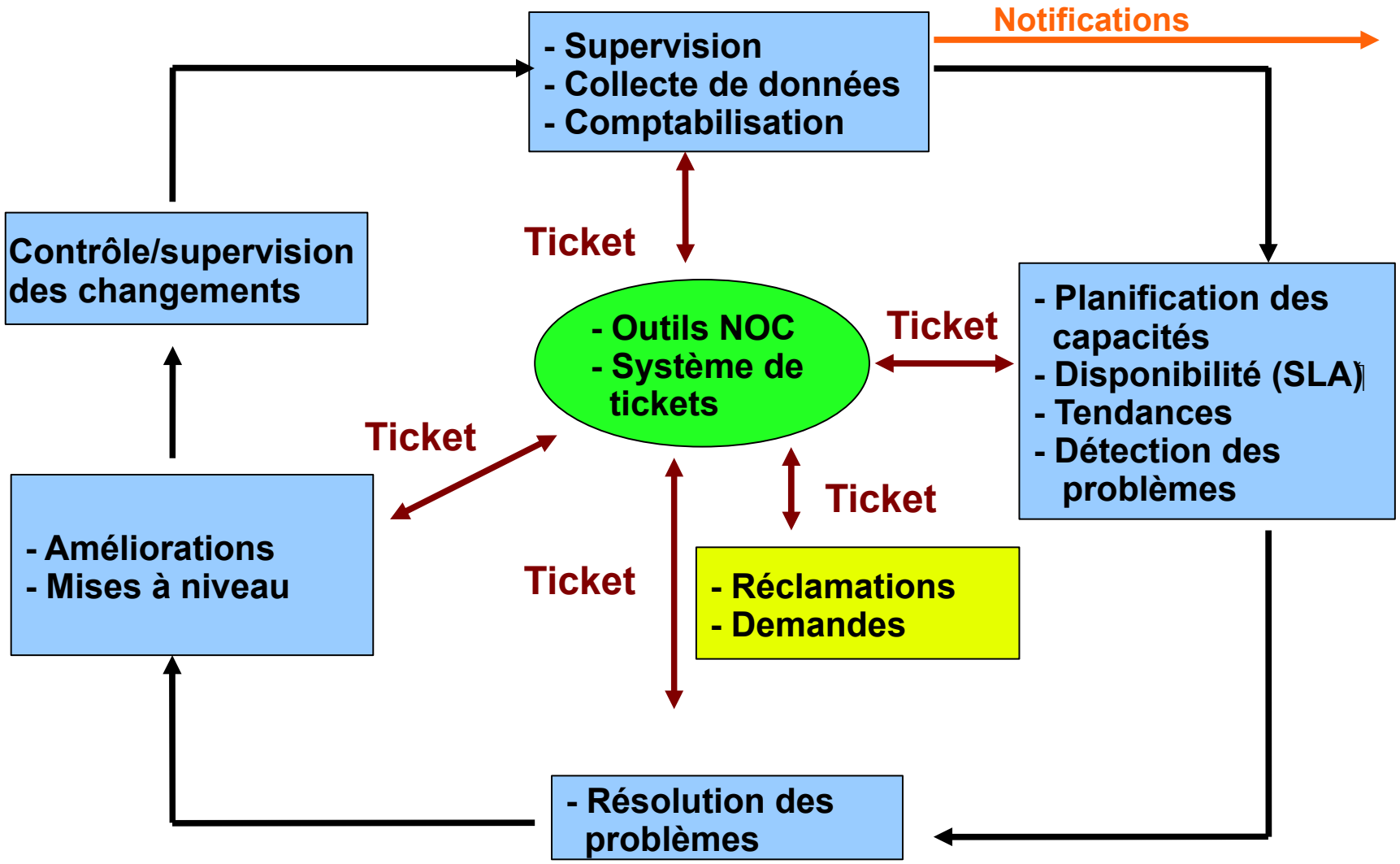
- Enregistrement des changements de configuration
  des équipements par *contrôle des versions* (ainsi que pour les fichiers de configuration)
- Gestion des inventaires (équipements, IP, interfaces)
- Utilisation du contrôle de versions
  - aussi simple que :
    ”`cp named.conf named.conf.20070827-01`”
- Pour des fichiers de configuration simples :
  - **CVS, Subversion (SVN)**
  - **Mercurial**

Gestion et supervision des configurations

- Traditionnellement utilisé pour le code source (programmes)
- Fonctionne bien pour n'importe quel fichier de configuration à base de texte
  - ainsi que pour les fichiers binaires, mais il est plus difficile de voir les différences
- Equipements de réseau :
  - **RANCID** (récupération et archivage automatiques de configuration

    Cisco, ainsi que pour d'autres types d'équipements)
- Logiciels intégrés de gestion de projets tels que :
  - **Trac**
  - **Redmine**
  - ainsi que nombre d'autres produits wiki, excellents pour documenter

Vue d'ensemble… de nouveau



Des questions ?

?