Gestion et Surveillance de Réseau

Introduction à la gestion et surveillance de réseau

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 ?
- Démarrage
- Pourquoi une gestion de réseau ?
- Les trois grands
- Détection des attaques
- Documentation
- Consolidation des données
- Vue d'ensemble

Qu’entend-on par surveillance 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

Qu’entend-on par Gestion de réseau ?

… les activités, méthodes, procédures et outils ayant trait à l'exploitation, l'administration, la maintenance et le dimensionnement des systèmes en réseau.

Exploitation : maintenir le réseau et les services qu'il fournit, actifs et en bon état de fonctionnement. L'exploitation *englobe la surveillance du réseau* aux fins de détecter les problèmes au plus vite et dans l’idéal avant que les utilisateurs ne soient affectés.

Administration : consiste à garder trace des ressources du réseau et leur affectation.

Maintenance : le fait d’effectuer des réparations et des mises à niveau. La maintenance englobe également les mesures correctives et préventives visant à améliorer le fonctionnement du réseau géré.

Dimensionnement : consiste à configurer les ressources du réseau pour assurer un service particulier.

FCAPS

Fault, **C**onfiguration, **A**ccounting, **P**erformance and **S**ecurity
(modèle de réseau ISO de gestion des télécommunications et cadre de gestion de réseau)

Source : wikipedia

Gestion de réseau

Ce que nous surveillons :

- **Systèmes 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 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 de 1 heure / semaine ?

(762 - 4) / 762 x 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.

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

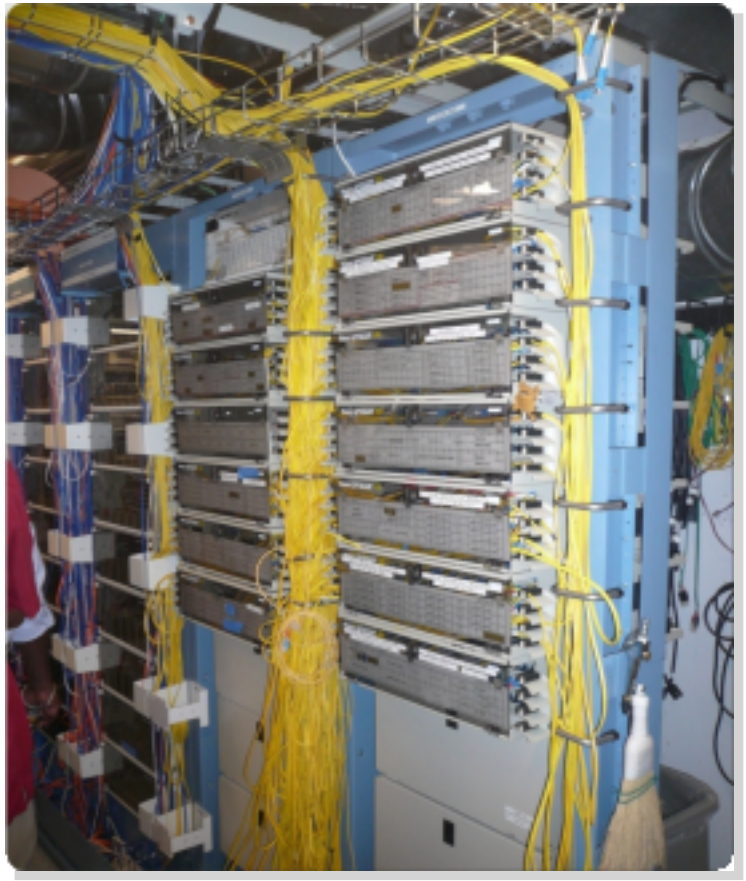
Les fonctions de ces programmes se chevauchent en partie !

Détection des attaques

- Les tendances et l'automatisation vous informent des attaques.
- Les outils utilisés peuvent vous aider à atténuer l'incidence des attaques :
  - Flux passant par les interfaces réseau
  - Charge sur des serveurs et/ou services spécifiques
  - Défaillances répétées de services

Documentation

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



Documentez,
documentez,
documentez…

Documentation

Règle de base : documenter les commutateurs...

- À quoi chaque port est-il connecté ?
- Un simple fichier texte suffit, avec une ligne pour chaque port de commutateur :
  - 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 pourraient être mises à disposition de votre personnel réseau et d'assistance, par le biais d'un wiki, une interface logicielle, etc.
- Pensez à étiqueter vos ports !

Documentation : Étiquetage

Impeccable !

Documentation du réseau

Une automatisation plus généralisée pourrait s'avérer nécessaire. Un système de documentation réseau automatisé est à envisager.

- Vous pouvez écrire des scripts locaux pour réaliser cette tâche.
- Vous pouvez choisir parmi plusieurs systèmes de documentation automatisés.
- Vous finirez probablement par utiliser et faire 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/
- Rack Tables :
  http://www.racktables.org/

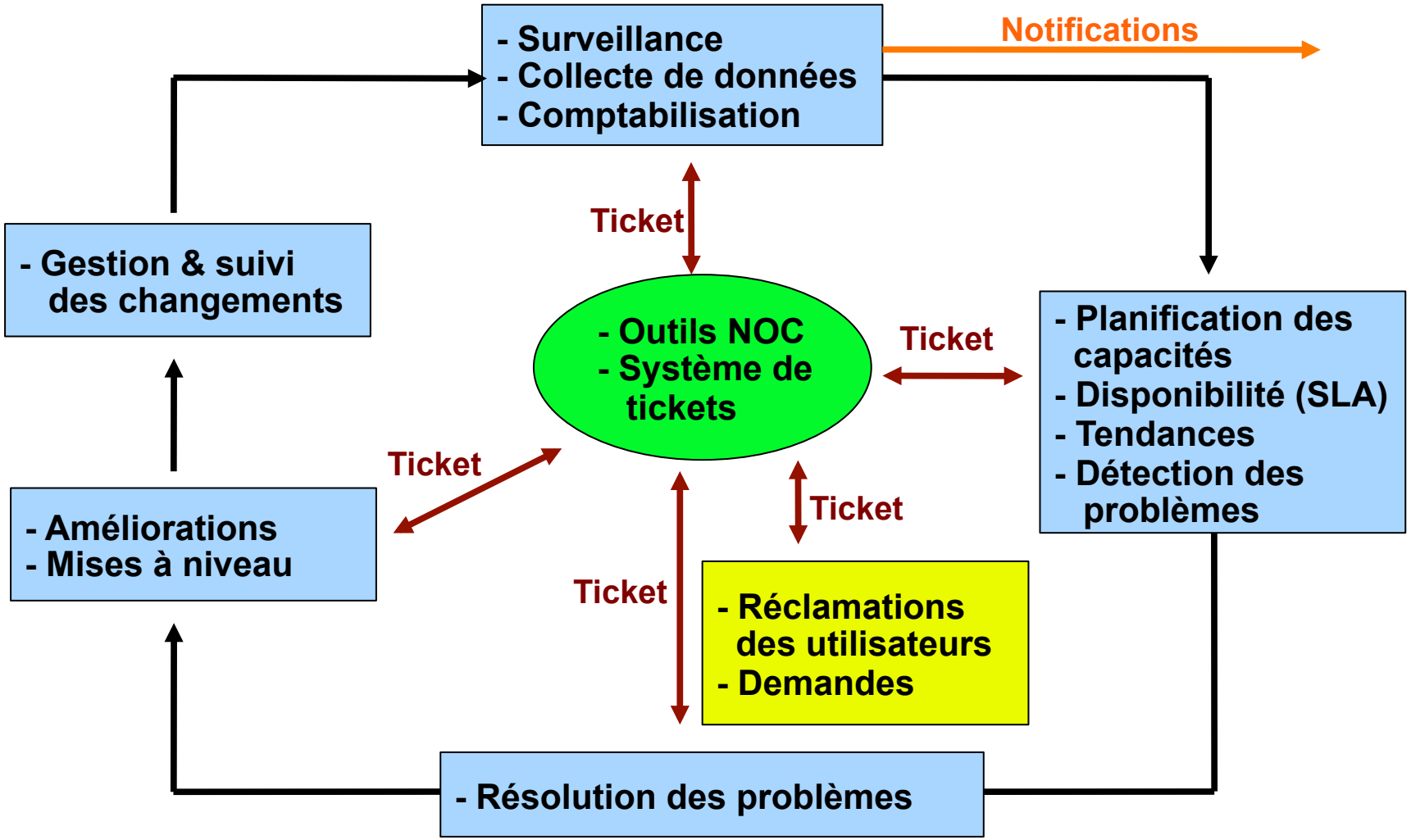
Consolidation des données

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 :

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

Documentation (Suite)

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]]

Extrait de la page web d'IPplan :

“IPplan est à la fois un logiciel web multilingue et gratuit de gestion d’adresses TCP IP (IPAM) et un outil de suivi écrit en php 4, qui simplifie l'administration de l’espace d’adressage IP. IPplan va au-delà de 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).”

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 en laissant une piste d'audit 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'utilisation des adresses IP et des ports de commutation : historique et actuel.
  - **Représentations attrayantes** du réseau.

Netdot : {net.} NETwork DOcumentation Tool

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

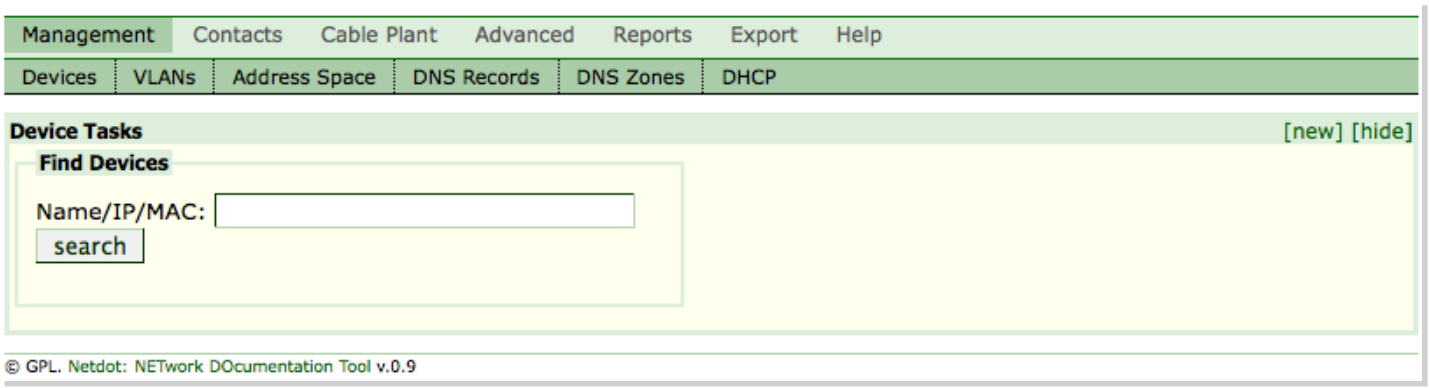
- Découverte de périphériques par SNMP
- Découverte de topologie de couche 2 et graphiques avec :
  - CDP/LLDP
  - Protocole STP
  - Tables d'acheminement de commutation
  - Sous-réseaux point à point avec routeurs
- Gestion d'espaces d'adressage IPv4 et IPv6 (IPAM)
  - Visualisation des espaces d'adressage
  - Gestion des configurations DNS/DHCP
  - Suivi d'adresses IP et MAC

Suite ➔

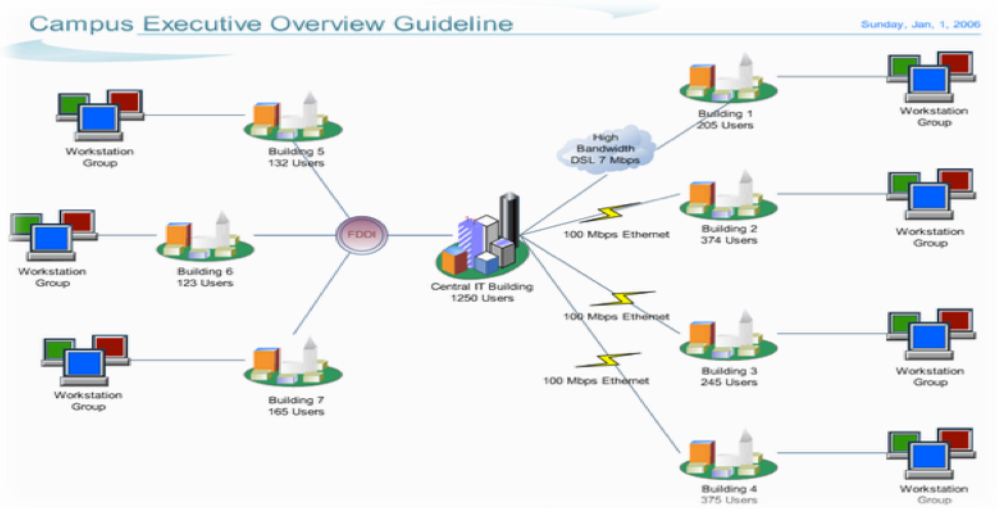
Netdot : {net.} NETwork DOcumentation Tool

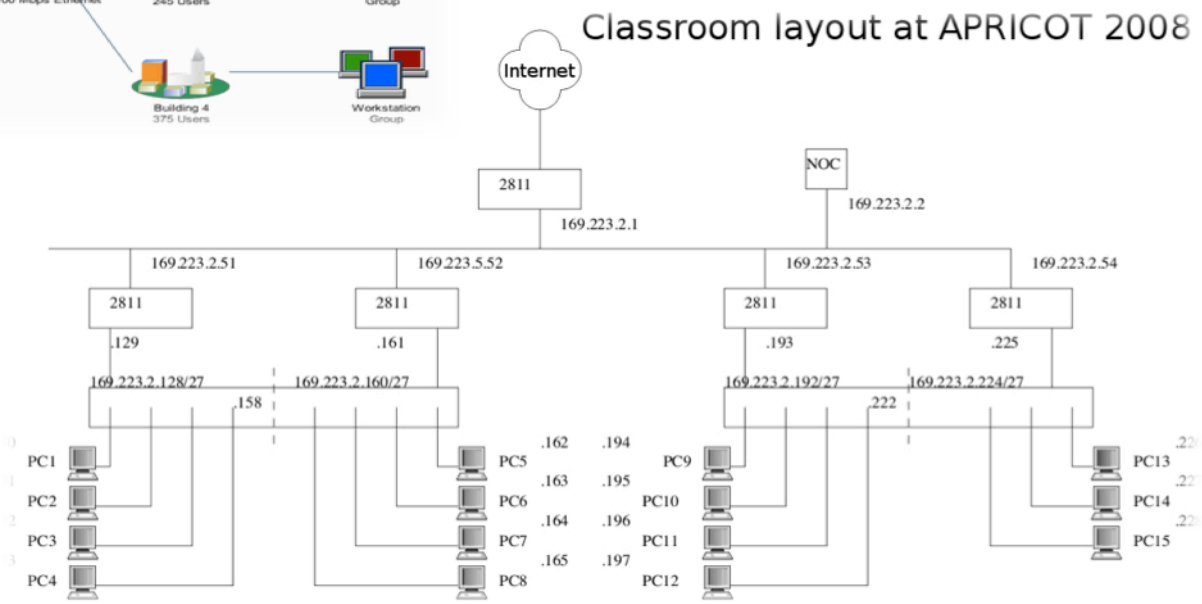
Fonctions (suite)

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



Documentation : Schémas





Logiciels de création de diagrammes

Logiciels Windows

- Visio :
  http://office.microsoft.com/en-us/visio/FX100487861033.aspx
- Ezdraw :
  http://www.edrawsoft.com/

Logiciels open source

- 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/

Questions ?

Partie III : 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

Systèmes et outils de surveillance réseau

Trois types d'outils

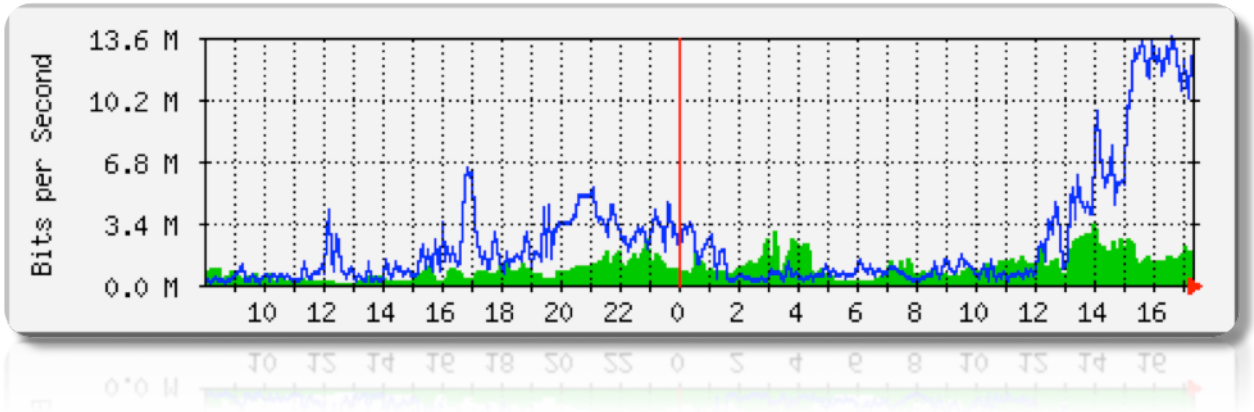
1. **Outils de diagnostic** – permettent de tester la connectivité, de vérifier l'accessibilité d'un site ou le fonctionnement d'un dispositif – il s'agit généralement d'outils actifs.
2. **Outils de surveillance** – outils fonctionnant en arrière-plan ("démons" ou services), chargés de collecter des 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.

Systèmes et outils de surveillance réseau

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", grapheur de trafic multirouteur

Systèmes 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

Systèmes et outils de surveillance réseau

Outils de surveillance du réseau et des servic

- 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 !

Systèmes 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 ?

- Suveillance !
- 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 ?

Systèmes 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 :

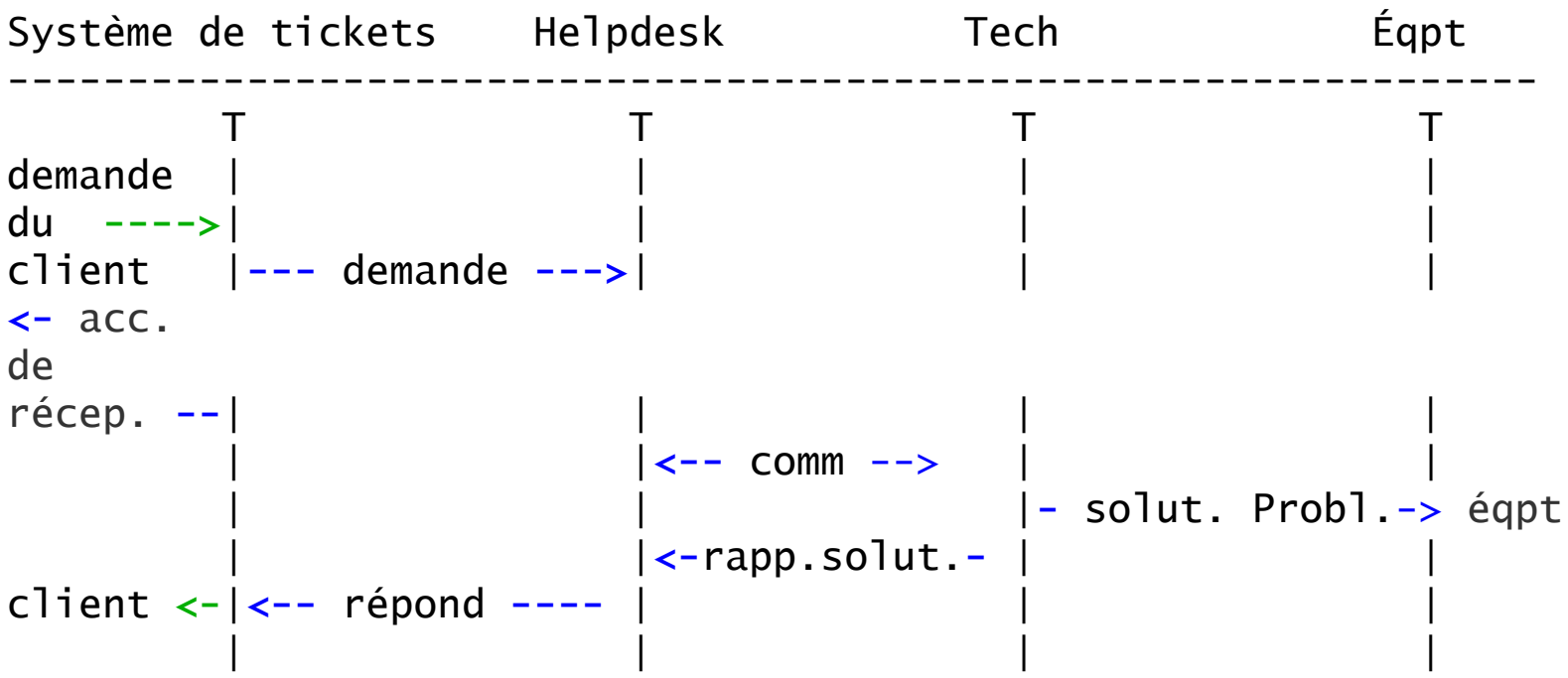
- Pannes du système (directes ou indirectes)
- Maintenances ou mises à niveau planifiées – n’oubliez pas d’en informer vos clients !

Systèmes 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

Systèmes de tickets

Déroulement des opérations



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 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.

Systèmes 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/

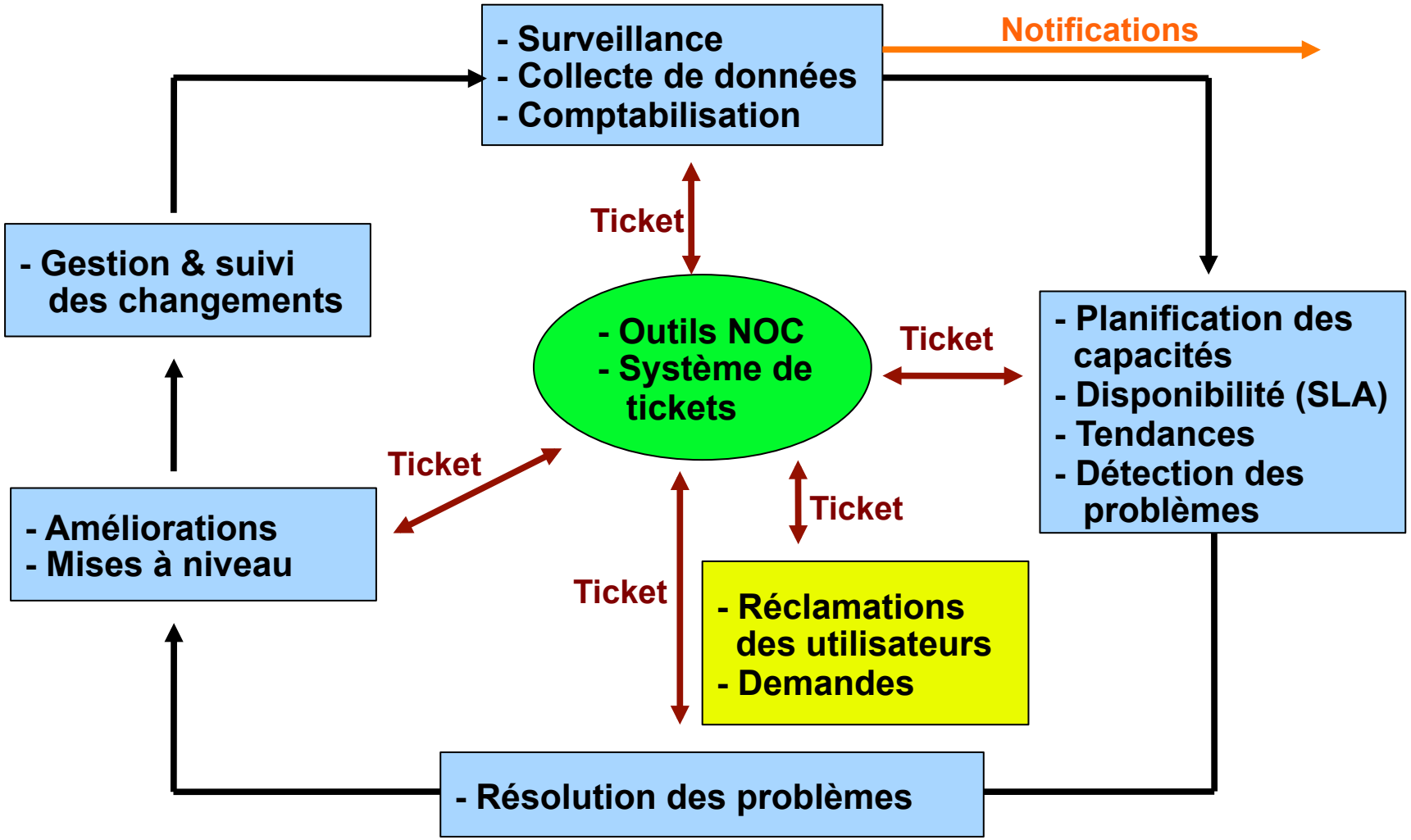
Gestion et surveillance des configurations

- 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

?