Ecole Centrale de Lyon – 3A – Supervision et Contôle (IC fo SI 3.6) - BE
Année 2011-2012

Administration de réseau

(Version 3.2 - a – 13/02/2012)

Objectifs :

Ce BE permet d'aborder la supervision de réseau avec HP OpenView.

Compte-rendu

Les BE sont réalisés par binôme. Les comptes-rendus doivent être rédigés sous forme électronique. Le dépôt des comptes-rendus se fait sous forme d'un UNIQUE fichier par binôme et par BE au format Acrobat (PDF). Les formats MS-Word (DOC, DOCX) et Open-Office (SXW, ODT) sont aussi acceptés.

Le compte-rendu est à déposer sur le serveur http://pedagogie.ec-lyon.fr/ dans la rubrique *Travaux* du cours *Supervision et contrôle*. Au moment du dépôt, merci de bien vouloir rédiger le champ Titre sous la forme :

```
CR <nom eleve 1> - <nom eleve 2> - <N° BE>
```

En cas de problèmes techniques avec le dépôt sur le serveur, merci d'envoyer votre compte-rendu par E-mail.

1 Introduction, découverte du réseau étudié

L'ensemble du BE se déroule sur un petit réseau d'étude au bâtiment H9 relié au réseau de l'Ecole Centrale de Lyon.

1.1 Rappels

Un réseau est composé de nœuds et de liens :

- les nœuds terminaux (hôtes) sont des systèmes de traitement de l'information (ordinateurs, imprimantes, etc…)
- les nœuds intermédiaires sont des systèmes permettant l'acheminement des paquets, appelés routeurs
- les liens sont soit des des liaisons point à point, soit des liaisons multipoints généralement des réseaux locaux du type Ethernet ou Token-Ring

Chaque nœud possède une ou plusieurs adresses selon le nombre d'interfaces réseau qu'il possède. Il faut également distinguer les adresses selon le niveau de la couche OSI considérée.

Adressage de niveau 2 (niveau OSI "liaison de données") :

Sur les réseaux locaux, les équipements possèdent un adresse de niveau 2. Dans le cas d'Ethernet, il s'agit d'une adresse sur 6 octets attribuée de manière unique par le constructeur de la carte d'interface. Dans cette adresse, les 3 premiers octets sont le code du constructeur, les 3 derniers octets sont un numéro de série unique attribué par le constructeur. De cette manière on est sûr qu'il n'y a pas 2 cartes dans le monde entier qui possède la même adresse.

Il existe plusieurs adresses Ethernet spécifiques, comme les adresses multicast et broadcast. Toutes ces adresses ont un premier octet impair (ce qui correspond aux adresses de 01:xx:xx:xx:xx:xx, 03:xx:xx:xx:xx:xx, etc.... En particulier l'adresse FF:FF:FF:FF:FF:FF est l'adresse de broadcast.

Pour de plus amples informations on consultera le cours sur Ethernet sur http://pedagogie.ec-lyon.fr/.

Adressage de niveau 3 (niveau OSI "réseau") :

Les hôtes sont caractérisés par leur adresse de niveau 3 (ou réseau), unique en général, sauf en cas d'attachement multiple. Les routeurs possèdent plusieurs adresses réseau, une pour chaque interface rattachée à un réseau.

Si les hôtes et les routeurs supportent plusieurs protocoles réseau, alors ils doivent posséder une adresse par protocole (adresse IP, adresse IPX, adresse X25, etc…)

Par la suite nous considérons uniquement le protocole IP. Les adresses IP sont constituées de 4 octets et subdivisées en 2 parties :

- le numéro de réseau, chaque réseau devant posséder un numéro unique.
- l'adresse dans le réseau : chaque hôte doit posséder une adresse unique dans le réseau

La taille de chaque partie est variable et est définie par un masque de sous-réseau (netmask) de 4 octets dont les bits à 1 spécifient la partie numéro de réseau, le reste étant l'adresse dans le réseau. Par exemple, un netmask de 255.255.255.0 signifie que le numéro de réseau utilise 3 octets et l'adresse dans le réseau 1 octet.

Les adresses IP comprises entre 0.1.0.0 et 223.255.255.255 sont des adresses classiques unicast. Chaque hôte doit posséder une adresse unique pour pouvoir communiquer dans l'Internet.

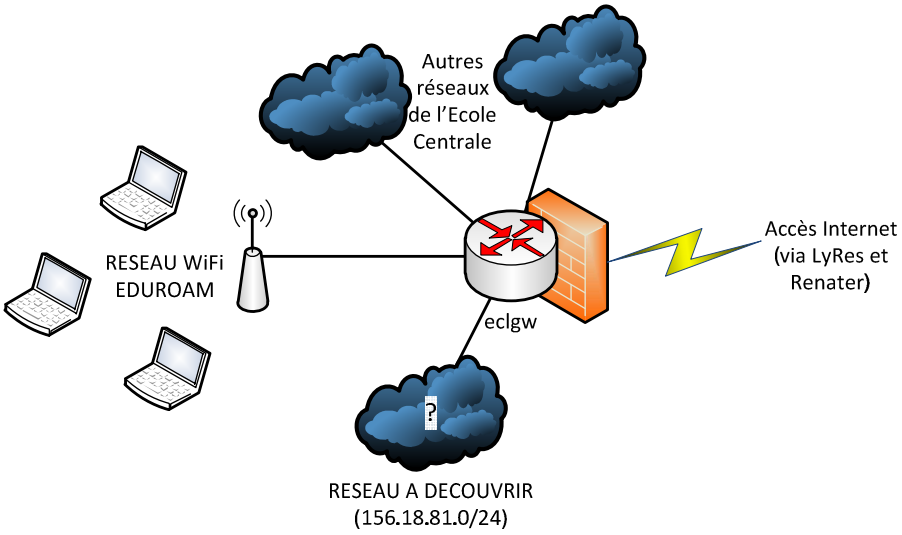
Les adresses comprises entre 224.0.0.0 et 239.255.255.255 sont des adresses multicast. Un hôte peut utiliser un ou plusieurs de ces adresses pour recevoir le trafic multicast correspondant (on peut comparer ces adresses à des chaînes de télévision).

Enfin, l'adresse 255.255.255.255 est réservée pour le broadcast à l'intérieur d'un réseau (le broadcast n'est jamais routé).

Pour en savoir plus, vous pouvez consulter le cours sur TCP/IP sur http://pedagogie.ec-lyon.fr/.Vous pouvez aussi consulter les RFC 1700 et RFC 1117. Pour l'adressage des sous-réseaux voir la RFC 950, mise à jour par la RFC 1122. La RFC 1519 présente l'adressage sans classe et le sur-adressage. Les RFC peuvent être consultées sur : http://www.rfc-editor.org/

1.2 Découverte du réseau étudié

Le réseau de travail de la salle est composé de 4 sous-réseaux et d'un routeur. Un des sous-réseaux est lui-même connecté au réseau de l'Ecole Centrale de Lyon par le routeur principal de l'Ecole, « eclgw ». Le schéma ci-dessous montre l'architecture globale du réseau de l'Ecole.



Les 4 sous-réseaux, qu'on vous demande de découvrir, utilisent des adresses qui sont toutes comprises dans le bloc 156.18.81.0/24

On utilisera les commandes élémentaires d'administration (dans une fenêtre « Invite de commandes ») :

- ping
- netstat
- tracert (Note: sous Unix=traceroute)
- nslookup

On peut aussi utiliser les commandes suivantes permettant d'avoir la configuration de sa machine :

- ipconfig, pour connaître l'état des interfaces réseau (Note: sous Unix=ifconfig)
- arp, pour la correspondance entres adresses IP et adresses Ethernet
- route, pour connaître le routage (ou netstat -r)

Note : Pour obtenir de l'aide pour ces commandes : faire suivre la commande par "/?" ou Menu " Aide… "

Des informations minimales sur ces outils peuvent être obtenues dans les **pages Wikipedia** suivantes :

- ping : http://fr.wikipedia.org/wiki/Ping_%28logiciel%29
- netstat : http://fr.wikipedia.org/wiki/Netstat
- traceroute : http://fr.wikipedia.org/wiki/Traceroute
- nslookup : http://fr.wikipedia.org/wiki/Nslookup
- ipconfig : http://fr.wikipedia.org/wiki/Ipconfig
- ifconfig : http://fr.wikipedia.org/wiki/Ifconfig
- arp : http://fr.wikipedia.org/wiki/Address_Resolution_Protocol

Travail à réaliser :

⇨ On vous demande de découvrir et de tracer le schéma de ce réseau, en faisant figurer les routeurs et les stations situées sur ce réseau avec leur(s) adresse(s) IP, leur(s) adresse(s) Ethernet et leur nom Internet s'il existe. Dans le compte-rendu vous détaillerez l'ensemble des commandes que vous avez utilisées et qui vous ont permis la découverte de toutes ces informations.

⇨ Pensez-vous de ces outils sont adaptés à la découverte des éléments d'un réseau ? Quelles idées auriez-vous pour automatiser cette tâche ?

2 Administration avec un superviseur

Les superviseurs de réseaux ont été créés pour faciliter l'administration des grands réseaux, plus ou moins hétérogènes. A terme, ils devraient supporter l'ensemble des fonctionnalités de l'administration de réseaux. Actuellement, ils ne supportent généralement que les fonctionnalités de :

- Gestion de la configuration et des noms
- Gestion des anomalies (partiellement)

- Gestion des performances (partiellement)
- Gestion de la sécurité (par collecte des alarmes de sécurité)

Le superviseur que nous utilisons dans ce BE est une version réduite de HP Openview qui est limitée à la supervision de 100 nœuds.

Principales fonctions

Un superviseur comporte deux grands groupes de fonctions :

- Les fonctions de surveillance et d'acquisition des informations
- Les fonctions d'observation et de commande

Le premier groupe est supporté par des démons qui tournent de manière permanente sur le système d'administration (qui doit être multitâches : Unix ou Windows)

Le second groupe est lancé à la demande des opérateurs.

Pour des réseaux importants la tâche de description manuelle de l'architecture du réseau serait longue et complexe. C'est pourquoi une des premières fonctionnalités d'un superviseur est la découverte automatique du réseau supervisé.

Lorsque les systèmes constituant le réseau ont été identifiés, ainsi que les moyens de les atteindre, ils sont surveillés soit par des scrutations périodiques (fonction " get " de SNMP), soit par l'acquisition de notifications d'événements émises par des systèmes en anomalie ou sujet à des attaques (fonction " trap " de SNMP). Les informations recueillies servent à mettre à jour la configuration courante du réseau et sont enregistrées dans des journaux (log) pour être consultés à la demande.

2.1 Découverte automatique du réseau

Pour initialiser cette découverte, le superviseur commence par rechercher des informations utiles sur le système qui le supporte: nom, adresse, type de protocole de réseau (IP, IPX, …), valeur du masque de sous-réseau, adresses des serveurs de noms (primaire, secondaire), adresse du routeur d'accès principal au réseau en particulier.

Par des commandes de base, par exemple ping ou traceroute, il peut tester les systèmes identifiés et commencer de configurer son réseau et d'en dessiner la carte.

Si des agents SNMP sont installés sur ces systèmes et qu'il dispose des MIB correspondantes (ce qui est normal si on veut pouvoir administrer correctement le réseau…) il peut alors aller chercher des renseignements sur ces systèmes pour continuer sa découverte. En particulier on peut favoriser cette recherche en envoyant des commandes d'administration à ces systèmes.

Pour limiter la taille de la carte et contrôler son développement, la découverte d'un routeur et des sous-réseaux qui y sont attachés entraîne la création de cartes de niveau 2 (submap) qui ne sont établies qu'à la demande de l'opérateur. On peut aussi masquer explicitement certains systèmes ou même les supprimer du champ d'observation. (Attention: sur le système que nous utilisons cette fonction n'est pas réversible pour certains type de nœuds en particulier les routeurs : les machines supprimées ne peuvent être redécouvertes et le superviseur peut devenir inutilisable et doit être désinstallé puis réinstallé complètement)

On peut aussi limiter les domaines observés en plaçant des filtres (masques de sous-réseaux) dans les fonctions de découvertes. La gestion des noms de communauté SNMP limite aussi l'accès aux agents SNMP, donc aux informations récupérables.

Travail à réaliser :

- ⇨ Connectez-vous avec « Bureau à distance » ou « VNC » sur une machine de travail → ***Voir les détails de votre connexion dans l'annexe personnalisée « connexion aux machines de travail » distribuée sous forme papier***.
- ⇨ Lancer le logiciel OpenView dans « Menu Démarrer | HP OpenView | OpenView »
- ⇨ Faites la découverte automatique du réseau de travail. Pour cela, ouvrez le menu « Autodiscovery | Configure | Discovery Networks »; dans la boite de dialogue affichée, entrez les paramètres suivants:
  - IP subnet mask : 255.255.255.192
  - IP router/gateway : 156.18.81.253
  - IP router/gateway community : public
  - dans "Networks" entrer successivement les 4 réseaux, en faisant "Add" à chaque fois:
  - 156.18.81.0,
  - 156.18.81.64,
  - 156.18.81.128,
  - 156.18.81.192.
- ⇨ Fermer la boite de dialogue. Ouvrez le menu « Autodiscovery | Discover | Discovery Manager » et cliquez sur « Start discovery » et regardez la découverte s'effectuer.
- ⇨ Lorsque les nœuds sont découverts, vous pouvez lancer la commande « Autodiscovery | Layout | Do basic layout ». Les cartes vont se tracer automatiquement. Vous pouvez, par la suite, relancer cette commande, les nouveaux nœuds découverts étant rajoutés aux cartes.
- ⇨ Observer les nœuds découverts.
- ⇨ Est-ce que vous retrouvez bien les mêmes informations que dans la première partie?
- ⇨ D'après vous, pourquoi certaines machines ne sont-elles pas découvertes ?
- ⇨ Comment peut-on "forcer" OpenView à les découvrir ?
- ⇨ Comparer avec vos voisins pour voir si vous obtenez la même carte. Il peut être utile de consulter la documentation en ligne pour comprendre le processus de découverte d'OpenView.

⇨ Toutes les machines sont-elles administrables par SNMP ? (regarder dans la documentation-menu Help, les différentes icones possibles et leur signification).

En cliquant avec le bouton droit (menu "Describe") sur un élément vous pouvez regarder les informations associées : adresse IP, adresse Ethernet, son nom, son label. Vous pouvez également modifier certains de ces éléments. Il est également possible d'ajouter des éléments à la main avec le menu "Edit|Add".

Il est demandé de faire un "snapshot" (avec Alt-ImprEcran ou Alt-PrtScr) de vos cartes et de les joindre au compte-rendu.

2.2 Surveillance du réseau par "polling"

On peut surveiller l'état du réseau et de ses éléments par scrutation périodique (polling en anglais). Les éléments surveillés sont déterminés par l'utilisateur.

L'ajout d'un élément à surveiller se fait dans le menu « Monitor | Polling | Add device(s) » en sélectionnant au préalable les éléments sur la carte.

La liste des éléments surveillés peut être vérifiée par « Monitor | Polling | View polling list ».

Enfin, pour que la surveillance fonctionne, il faut l'activer avec le menu « Monitor | Polling | Start polling ».

Sur notre superviseur :

- les systèmes ou sous-réseaux non gérés apparaissent en beige,
- les systèmes ou sous-réseaux sans défaut en vert,
- les systèmes ou sous-réseaux en défaut en rouge,
- les sous-réseaux ayant des systèmes en défaut en jaune.
- La couleur bleu indique un système ou sous-réseau trouvé mais sans renseignements utilisables.

D'autres couleurs sont utilisées pour affiner ces notions et sont décrites dans la documentation en ligne d'OpenView.

Travail à réaliser :

⇨ Ajouter les machines du réseau de travail (y compris le routeur « cisco ») à la liste de polling et activer la fonction. Au bout d'un certain temps (10 minutes environ) toutes ces machines doivent devenir vertes.
⇨ On simule une panne (en débranchant la machine TIC139 du réseau)
⇨ Quels signaux vous permettent sous OpenView d'être mis au courant de cette panne ? Avec quel délai ?
⇨ On reconnecte la machine. Avec quel délai est-elle détectée comme sans défaut par le superviseur ?

La périodicité de polling est fixée par défaut à 5 minutes mais est ajustable élément par élément.

⇨ Que pensez-vous de cette valeur par défaut ?
⇨ Donner des arguments en faveur de son allongement et/ou de sa réduction.

2.3 Remontée des alarmes

La fenêtre des alarmes est consultable par le menu « Monitor | Alarm log ». Elle affiche tous les messages d'alertes :

- soit générés par le polling d'OpenView (node up, node down, etc...)
- soit générés par des messages SNMP "trap" envoyés par les machines

Ces messages doivent être acquittés :

- soit manuellement par l'utilisateur en utilisant le bouton "Acknowledge" ou "Acknowledge all"
- soit automatiquement par la réception d'autres messages (par exemple "link up" acquitte "link down" et vice-versa)

Les alarmes et leurs acquittements peuvent être configurés par le menu « Monitor | Customize traps ».

Dans notre salle, chaque machine XP est configurée pour renvoyer ses messages "trap" à elle-même. Par ailleurs, la machine TIC139 et le routeur Cisco renvoient leurs messages "trap" à toutes les machines XP.

Travail à réaliser :

⇨ Ouvrir la fenêtre des alarmes et regarder celles que vous avez reçues (Pour afficher toutes les alarmes, cliquer sur "History"). D'où proviennent-elles?
⇨ Utiliser le bouton "Filters" pour n'afficher que les alarmes provenant soit d'un type de machine, soit d'une catégorie spécifique.

2.4 Interrogation de périphériques par SNMP

HP OpenView permet de superviser plus finement les éléments du réseau par SNMP. Pour cela, après avoir sélectionné un élément sur la carte, on peut utiliser le menu « Control | SNMP manager ». Il existe trois interrogations prédéfinies :

- system: permet de visualiser les variables systèmes de l'élément administé,
- ip: affiche un graphique du nombre de paquets ip reçus et transmis par l'élément,
- udp: idem mais au niveau udp

Travail à réaliser :

⇨ Utiliser le menu « Control | SNMP manager | ip » sur :
  - le routeur cisco 156.18.81.253
  - un switch 156.18.81.61 ou 156.18.81.189

Laisser les fenêtres ouvertes pour regarder se tracer le trafic sur une dizaine de minutes pendant que vous répondez aux questions suivantes.

Il est possible de faire ses propres interrogations avec le menu « Control | SNMP manager | Define query ». On peut se promener dans l'arborescence des variables et sélectionner celles que l'on veut interroger (bouton "add").

Le bouton "Perform" permet de lancer la requête et d'obtenir le résultat dans une fenêtre. Il est aussi possible de visualiser le résultat sous forme de graphique en définissant une fréquence d'interrogation et un nombre d'échantillons (sélectionner le bouton radio « Display | Graph » puis le bouton « Options »).

Remarque : les objets SNMP de type table sont représentés entre accolades { }. Il n'est possible d'interroger qu'une seule table à la fois avec OpenView.

Travail à réaliser :

⇨ Faites des requêtes SNMP sur les éléments suivants:
- le routeur cisco 156.18.81.253
- la machine 156.18.81.99
- un switch 156.18.81.61 ou 156.18.81.189

⇨ Pour chacune de ces éléments répondez aux questions suivantes :
- Quel est le nom de l'administrateur système, la localisation de l'élément, depuis combien de temps est-il allumé ?
- Quel est le contenu de la table ARP ?
- Quel(s) sont les adresse(s) IP de cet élément ?
- Quel est le contenu de la table de routage ?
- Parcourez les différents groupes de variables. Quels sont les variables ou les groupes non définis ?

>>> FIN <<<

---

3 Complément - Ajout de MIB

Il est possible de rajouter des MIB à OpenView pour visualiser d'autres variables. Ces variables ne sont plus génériques mais spécifiques:
- soit à un type de matériel : Token Ring, Token Bus, Ethernet, FDDI, pont de niveau 2, etc...
- soit à des protocoles : OSPF, AppleTalk, etc...
- soit à des constructeurs : variables propriétaires à chaque constructeur.

Pour visualiser ces variables il faut d'abord les compiler dans la base de OpenView avec le menu « Control | SNMP manager | Manage database ». Il faut toujours sélectionner la MIB rfc1213.mib (définition des types de base) et un ou plusieurs autres fichiers. Plusieurs sont fournis par OpenView, la liste est consultable ci-dessous. Ces fichiers sont situés dans le sous-répertoire MIBS. Il est aussi possible de récupérer les fichiers de définition pour les variables propriétaires de Cisco.

Travail à réaliser :

⇨ Ajouter d'autres MIB à la base de données. Essayer d'interroger les différentes machines du réseau pour voir si elles y répondent.

⇨ Quelles machines répondent à quels groupes de variables ?

Supplied MIBs with HP OpenView

HP OpenView 7.2 for Windows ships with the following standard mibs in the \OV\MIBS directory. All are standard or draft standard and are under mib-2 (which means that rfc1213 must be compiled first). No private mibs are supplied.

Mib-2 will be ready compiled into the database. You need to use the Manage Database command to access the compiler to add other mibs manually. This is to keep the compiled database size reasonable.

(Note: rfc1286 has been modified to so that enumerated types are less than 32768.)

File	Top Object	Description
rfc1213.mib	mib-2	MIB-II Standard
rfc1229.mib	mib-2.ifExtensions	Extensions to MIB-II Interface Table
rfc1230.mib	mib-2.transmission.dot4	IEEE 802.4 Token Bus devices
rfc1231.mib	mib-2.transmission.dot5	IEEE 802.5 Token Ring devices
rfc1232.mib	mib-2.transmission.ds1	
rfc1233.mib	mib-2.transmission.ds3	
rfc1243.mib	mib-2.appletalk	AppleTalk
rfc1253.mib	mib-2.ospf	OSPF
rfc1269.mib	mib-2.bgp	
rfc1271.mib	mib-2.rmon	Remote Monitoring
rfc1284.mib	mib-2.transmission.dot3	IEEE 802.3 Ethernet-like devices
rfc1285.mib	mib-2.transmission.fddi	FDDI
rfc1286.mib	mib-2.dot1dBridge	IEEE 802.1d Bridge mib
rfc1289.mib	mib-2.phiv	DECnet PhaseIV

rfc1304.mib	mib-2.transmission.sip	SIP objects
rfc1315.mib	mib-2.transmission.frame-relay	DLC Frame Relay Service
rfc1316.mib	mib-2.char	Character stream devices
rfc1317.mib	mib-2.transmission.rs232	RS-232-like devices
rfc1318.mib	mib-2.transmission.para	Parallel printer-like devices