الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Projet Fin D'études
présenté par

Belkadi Mourad
&
Bouchata Zakaria

pour l'obtention du diplôme Master II en
réseaux et télécommunications

Thème

La mise en place d'un système de supervision réseau (Cas Pratique Univ BLIDA)

Proposé par :Mr. MEHDI Merouane

Année Universitaire 2015-2016

Remerciements

ملخص:

كلمات المفاتيح:

Résumé : Utiliser ces trois champs pour écrire un résume de votre mémoire dans l'ordre suivant : arabe, français et anglais.Ces trois langues sont indispensables pour le mémoire. Le résumé ne doit pas dépasser les huit lignes ni moins de quatre lignes. Eviter de faire des sauts de lignes dans le résumé pour ne pas dépasser le nombre de lignes exigé.

Ce document doit être fourni pour chaque binôme en cours de préparation du mémoire du projet de fin d'études. Le non respect de ce format entrainera le rejet du mémoire. Nous vous prions de respecter le format.

Mots clés : Premier mot; Deuxième mot; Troisième mot clé.

Abstract :

Keywords :

Listes des acronymes et abréviations

Table des matières

Les titres **liste des figures** et **liste des tableaux** ne figurent pas dans la table des matières.

Liste des figures

Utiliser cette liste si vous avez des figures dans votre manuscrit.

Liste des tableaux

Utiliser cette liste si vous avez des tableaux dans votre manuscrit.

Introduction générale

Chapitre 1 Titre du premier chapitre

1.1 Première Section

1.1.1 Deuxième section

a Troisième section

1.2 Texte

1.2.1 Taille de la police

La taille de la police est 12.

1.2.2 Interligne

L'interligne dans tout le document doit être de 1.5.

1.2.3 Alignement

Le texte doit être aligné partout dans le document.

1.2.4 Références

Les références doivent être numérotées en chiffre arabe et dans l'ordre de l'apparition [1].

1.3 Figures

Les figures doivent être centrées dans le corps du texte.

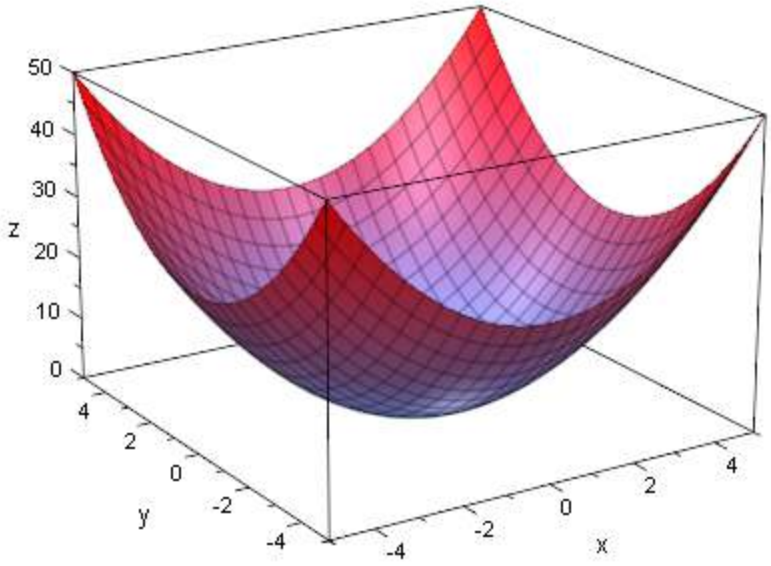


Figure 1.1. Exemple.

1.4 Tableaux

MASTERs	Nombre de projets	Nombre d'étudiants
Traitement de l'information et systèmes	10	5
Réseaux et Télécom.	25	15

Tableau 1.1. Exemple.

1.5 Numérotation des pages

La numérotation doit commencer de l'introduction générale ou du premier chapitre (s'il n'a pas d'introduction générale dans le projet de fin d'études).

Conclusion générale

Annexes

Bibliographie

[1] Auteur1, Auteur2 et Auteur3 : 'Titre du livre', éditeur, année de l'édition.

[2] Auteur1 et Auteur2 : 'Titre de l'article', Thème de la conférence, Pays, numéros de page, année.

[3] Auteur1 et Auteur2 : 'Titre de l'article', 'Titre de la revue, éditeur, numéros de volume et de page, année.

Dédicaces

Avant tout, je remercie le grand Dieu, qui nous a aidés à élaborer ce modeste travail.
J'ai l'immense honneur de dédier ce modeste travail :

A mes très chers parents qui étaient présents pour moi durant toute ma vie.

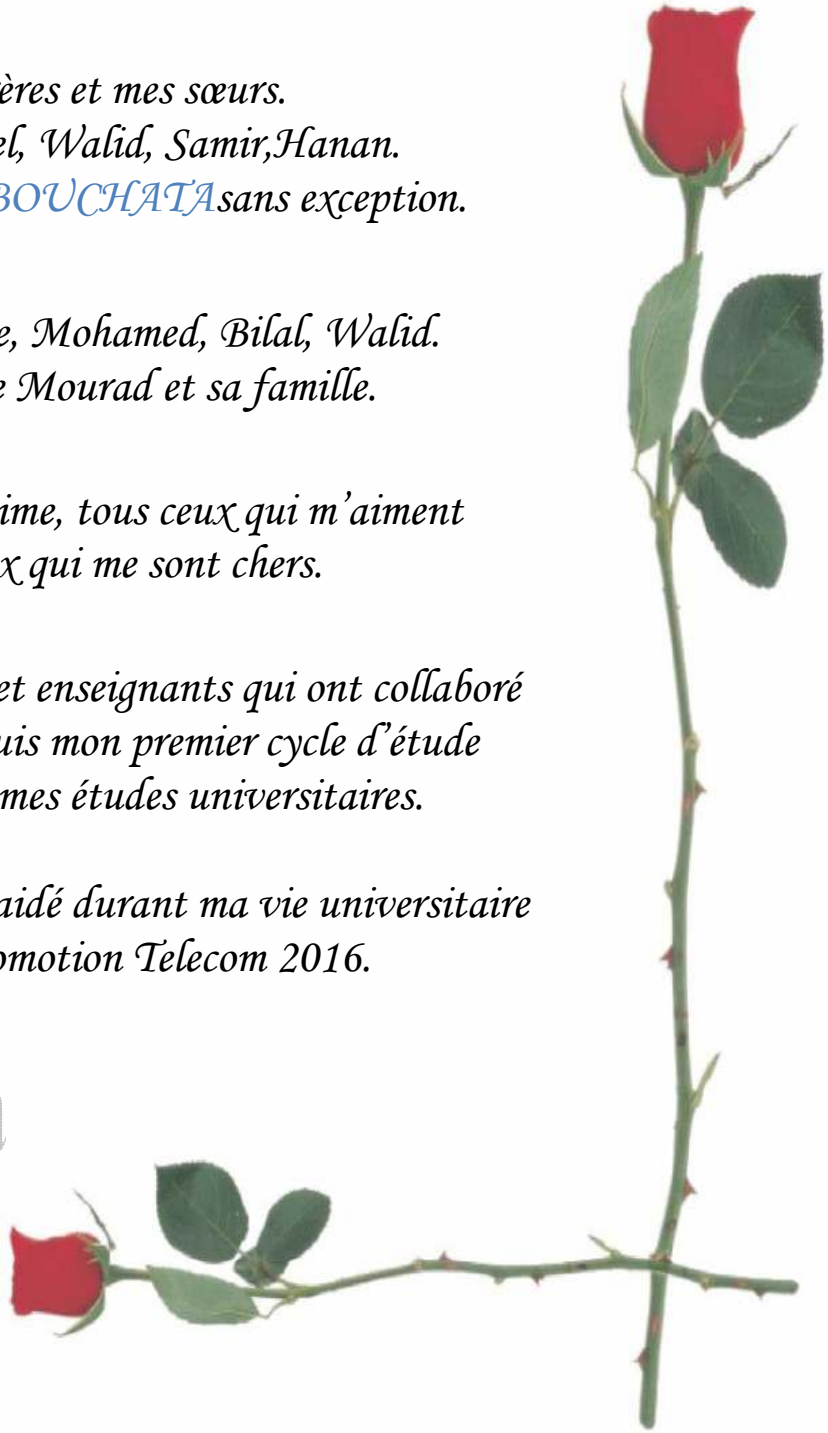
A mes frères et mes sœurs.
Mohamed, Amel, Walid, Samir,Hanan.
A toute la famille BOUCHATA sans exception.

A mes amis Amine, Mohamed, Bilal, Walid.
A mon binôme Mourad et sa famille.

A tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers.

A tous les professeurs et enseignants qui ont collaboré à ma formation depuis mon premier cycle d'étude jusqu'à la fin de mes études universitaires.

A tous ceux qui m'ont aidé durant ma vie universitaire
A toute la promotion Telecom 2016.



BOUCHATA Zakaria

Je remercie avant tout, DIEU le tout puissant de m'avoir crée et de pouvoir réaliser ce modeste travail.

Je tiens à exprimer tout ma reconnaissance à Monsieur MEHDI Merouane pour avoir encadré ce projet ainsi que pour sa disponibilité.

Je remercie également les membres de jury d'accepter d'évaluer ce travail.

J'adresse mes remerciements à tous nos enseignants de département d'électronique et le laboratoire d'informatique qui ont contribué à notre formation.

A tous ceux qui nous ont aidés, nous disons…… MERCI.

BELKADI Mourad & BOUCHATA Zakaria

RESUME :

Avoir une bonne gestion des réseaux informatiques est devenue aujourd'hui une nécessité pour assurer une bonne exploitation des ressources. La gestion concerne le domaine de la configuration, de performances, d'anomalies, de complexité et de sécurité. Le protocole **SNMP** est devenu un standard dans le domaine.

Ce que nous avons présenté rentre dans le cadre d'offrir à l'administration réseau est un outil de gestion de performances et d'anomalies d'un réseau local **TCP/IP** s'appelle **Ipswitch** (**WhatsupGold)** en utilisant le protocole **SNMP**. Cet outil présente la topologie du réseau sous forme d'une cartographie

التلخيص:

تحقيق التسيير الجيدلشبكات الإعلام الألي أصبح اليوم ضرورة من أجل ضمان الاستغلال الجيد للموارد. التسيير يخص ميدان الضبط، الأداء، الأشياء الاستثنائية، التعقيدات و الأمن. خاصة أن البروتوكولSNMPأصبح معيارا في هذا المجال.

ما استعرضناه في هذا العمل يدخل في إطار إدارة الشبكيات حيث أن أداة تسيير الأداء و الأشياء الاستثنائية للشبكة المحلية TCPIP تعرف بـ: **Ipswitch(WhatsupGold)و باستعمال البروتوكول SNMP.** هذه الأداة باستطاعتها تمثيل طوبولوجيا الشبكة على شكل خرائطية.

.

ABSTRACT:

To acquire a good management of networks today became a necessity to assure a good exploitation of resources. The management regards the domain of the profile, of performance, of anomalies, accounting and security, the **SNMP** protocol became a switchboard in this field.

This work includes in the setting to the administrator a management tool of performances and anomalies of local network it's**Ipswitch** (**WhatsupGold)**with the use the SNMP protocol. This tool presents the topology of the network under shape of cartography.

Conclusion générale :

Une bonne gestion des réseaux est devenue une nécessite au sein des réseaux informatiques surtout avec l'augmentation de la taille des réseaux et la diversité des équipements utilisés. Notre choix s'est porté sur l'outil**Ipswich**et leur protocole **SNMP** car ce dernier est standard dans le domaine de la gestion des réseaux, il est introduit dans les équipements réseau par la plupart des constructeurs.

Dans cette optique nous avant développé à travers ce mémoire la conception et la réalisation d'une gestion « superviseur réseau » avec l'outil **Ipswich**et a base de protocole**SNMP**. Cet outil permet à l'administrateur de surveiller l'état de son réseau et d'avoir devant lui une cartographie qui représente la topologie de son réseau et des informations sur chaque équipement en temps réel.

Ce que nous avons réalisés dans ce projet est une gestionde supervision pour l'administrateur du réseau localа base des protocoles **TCP/IP et** l'outil **Ipswich**, elle traite essentiellement la récolte des informations concernant les nœuds (**Switchs**) d'un réseau informatique et facilite la visualisation du réseau à travers une cartographie ce qui permettra une gestion aisée.

Sommaire

LISTE DES TABLEAUX

LISTE DES FIGURE

LISTE DES ABREVIATIONS:

A

AD: Active Directory

ARP: Address Resolution Protocol

ATM: Asynchronous Transfer Mode

B

C

CSMA/CA: Carrier Sense Multiple Access with Collision Detect

CSV : Valeurs séparées par des virgules (Comma-separated values)

D

DNS : Nom Du Domaine (Domain Name System)

E

F

FDDI: Fiber Distributed Data Interface

FIA Fournisseur d'Accès Internet

FTP : File Transfer Protocol

G

H

HTTP: Hyper Text TRANSFER PROTOCOL

I

ISO: International Standards Organization

IP: Internet Protocol

J

K

L

LAN: Local Area Network

LDAP:Lightweight Directory Access Protocol

LED: Diode electrolumineuse (Light Emitting Diode)

LLC: Layer Link Control

M

MAU: Medium Access Unit

MAC:Midiuem Access Control

MAN : Réseaux métropolitains (Metropolitan Area Network)

MIB : Gestion des Information de Base (Management Information Base)

N

O

OSI: Open Systems Interconnection

P

PAN:Réseau personnel (Personal Area Network)

PHY: Physique (Physical)

PMD:Physical Medium Dependant

Q

QoS :Qualité de Service (Qualite of Service)

R

S

SSH:Secure Shell

SNMP: Simple Network Management Protocol

SMTP: Simple Mail Transfer Protocol

STP: Pairetorsadée (Shielded Twisted Pair)

SMF : Fibre Monomode (Single Mode Fiber)

T

TAC : Assistant technique de Cisco

TCP : Transmission Control Protocol

TCP/IP : Transmission Control Protocol/ Internet Protocol.

Telnet : connexion à distance (Telecommunication-Network)

U

UDP : Unit Datagram Protocol

UTP : Paire torsadée non blindée (UnsheildedTwisted Pair)

V

VOIP : Voice Internet Protocol

VLAN : Virtuelle réseau local (Virtuel Local Area Network)

W

WMI : Windows Management Instrumentation

WAN:Réseauxétendus (Wide Area Network)

X

Y

Z

DEDICACES

Avant tout, je remercie ***le grand Dieu****, qui nous a aidés à élaborer ce modeste travail.*

Je dédie ce modeste travail :

A mes très chers parents et surtout ma tendre Mère qui a veillée jour et nuit sur mon éducation et qui est présente à chaque instant pour moi, à qui je dis aujourd'hui merci ***MERE****.*

A mes très chères sœurs ***et*** *à mon frère.*

A mes très chers parents de ma femme ***AMI RACHID*** *et* ***KHALTO*** *et ses sœurs.*

Tous mes remerciements vont également à mes meilleurs amis ***Mourad, Hamza BILALE, Mounir, Sid Ahmed , Sellali et Ouahid*** *qui m'ont toujours aidés et encouragés.*

A mon très cher binôme ***Zakaria***

*A tous ceux que j'****aime****, qui m'****aiment*** *et tous ceux qui me sont chers*

A toute la promotion ***Master Réseaux & Télécommunications 2016****.*

Sans oublier ***ma femme FOUZIA*** *qui a été toujours présente, et celle qui a sacrifié toute sa jeunesse pour mon bonheur, et ma réussite. Celle qui prouve sans cesse sa générosité, sa compréhension et sa tendresse. Pour cela, je tiens à lui exprimer vivement mes chaleureux et vifs remerciements.*

MOURAD.

1. contexte générale :

L'importance croissante des réseaux informatiques ainsi que la diversité des équipements utilisés entrainant une augmentation de la complexité de leur gestion. En effet le nombre important est croissant des machines et d'utilisateurs nécessite une administration de plus en plus difficileà mettre en place.

Sur les réseaux physiques de nombreuses composantes sont donc à surveiller : utilisation de la largeur de bande, l'état de fonctionnement des liens les éventuels goulets d'étranglement les problèmes de câblage le bon cheminement de l'information entre les nœuds, etc. pour ce faire différents points stratégique sont a observer comme les routeurs, les concentrateurs, les liens, les stations et les imprimantes..etc. Ainsi, en cas de panne ou de mouvais fonctionnement sur le réseau, l'administrateur doit pouvoir interpréter l'information reçu pour identifier la source du problème.

La gestion des réseaux est un facteur déterminant du bon fonctionnement sur du parc informatique d'une entreprise. Le nombre d'éléments qui compose le réseau et leurs éloignements potentiels peuvent rendre l'administration très difficile à assurer. En effet, pour gérer un réseau, il faut tenir compte de plusieurs paramètres, comme la gestion des performances, des pannes, etc. pour réaliser ces différentes tâches. Un protocole de gestion est nécessaire pour exercer les fonctions de gestion sur un réseau. Il doit être capable de dialoguer avec tous les éléments de l'état du réseau et la gestion des anomalies, plusieurs protocoles ont été implémentés on peut distinguer les protocoles **SNMP** (Simple Network Management Protocole) .

Dans un but d'avoir une bonne administration réseau, il est nécessaire de mettre en œuvre une stratégie de gestion des réseaux de ressources humaines en affectant des rôles pour chaque personne de l'équipe qui va gérer le réseau.

2- Problématique :

On va essayer à travers ce mémoire de répondre a la question suivante :

- **Comment permettre à un administrateur réseau d'avoir la structure de son réseau local et d'avoir toutes les informations de n'importe quel nœud de ce réseau en temps réel ?**

3- Objectifs et motivations :

Nous allons aborder notre mémoire par une étude d'efficacité d'un système de supervision réseau, on fera un tour d'horizon sur les outils de supervision réseau existant et après cette étude on va proposer une plate-forme d'un superviseur réseau local (LAN) et en finalité implémenter cette plate-forme.

La motivation qui nous a poussés a s'intéresser à la conception et l'implémentation d'un outil de supervision réseau est le fait qu'un superviseur réseau et un outil indispensable aux administrateurs réseau car il permet de contrôler l'état des nœuds d'un réseau, de détecter les défaillances et de localier rapidement leur source.

4- Contenu du mémoire :

Ce mémoire subdivise en quatre chapitres :

En premier chapitre on va voir les fondamentaux des réseaux avec une présentation des matériels et architectures protocolaires nécessaires à leur construction.

Le deuxième chapitre jeux le rôle de présentation du concept générale d'architecture de notre université ainsi que les différents logiciels et matériels utilisés pour le bon fonctionnement du réseau. Ensuite le troisième chapitre est consacré comme une présentation d'outil utilisé à l'administration de notre réseau, en passant type par type avec des explications montrent la puissance, la performance, l'efficacité, la sécurisation et la fiabilité.

Enfin le dernier quatrième chapitre fais partie le plus important de notre étude et réalisation du supervision de notre réseau avec le logiciel **Ipswich(WhatsUp Gold)**, cet expérience est basées sur les essais réel et suivant chaque résultat prés doit être interprété et commenter pour prouver l'indispensabilité de cet outil dans notre réseau.

Chapitre I : Généralités sur les réseaux informatiques

I.1.1. Introduction :

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. Au début de l'utilisation de l'informatique, toutes les informations nécessaires aux traitements étaient centralisées sur la même machine. Pour des raisons de coût ou de performance, on a multiplié le nombre de machines. Les informations devaient alors être dupliquées sur les différentes machines du même site. Cette duplication était facile mais elle ne permettait pas toujours d'avoir des informations cohérentes sur les machines. On a donc commencé à relier ces machines entre elles; on a vécu l'apparition des réseaux locaux.

Les réseaux étaient souvent des réseaux "maisons" ou propriétaires. Plus tard on a éprouvé le besoin d'échanger des informations entre des sites distants. Les réseaux moyennes et longue distance ont commencé à voir le jour. Aujourd'hui, les réseaux se retrouvent à l'échelle planétaire.

Dans ce chapitre on va faire une généralité sur les réseaux informatiques et les déférents protocoles célèbre d'administration réseau.

I.2. Définition du réseau informatique

Un réseau informatique est un ensemble d'équipements informatiques reliés entre eux, grâce à des supports de communication (câbles ou ondes) dans le but d'échanger des données numériques. Si le lien est assuré par le biais d'un câble on parle de réseau câblé. Si le lien est sous forme d'ondes, on parle de réseau sans fil.

Les intérêts majeurs d'un réseau sont :

-Communiquer entre personnes (messagerie, discussion en direct,...),

- Diminuer les coûts par le partage des ressources matérielles (imprimantes, espaces disque, graveurs, etc.),
- Partager des données et des applications,
- Standardiser les applications,
- Travailler sur une même base de données,
- Permettre une communication efficace, rapide et peu coûteuse.

Un réseau peut être de n'importe quelle taille :

- A la maison on peut relier deux ordinateurs pour partager une connexion Internet.
- Une entreprise peut créer un réseau en reliant une dizaine d'ordinateurs pour partager des dossiers et des imprimantes.
- Un réseau peut également connecter des millions d'ordinateurs afin d'échanger des informations partout dans le monde.

I.3. Les déférents types des réseaux informatiques

On distingue généralement quatre catégories de réseauxinformatiques, déférences par la distance maximaleséparant les points les plus éloignés du réseau :

I.3.1. Lesréseauxpersonnels, ou PAN (personnels Area Network) :

Interconnectent sur quelque mètre des équipements personnels tels que terminaux.

I.3.2. Lesréseaux locaux ou LAN (Local Area Network):

Unréseau qui relais des ordinateurs et des périphériques situé les uns des autres sr une mêmepièce au dans un bâtiment. Il ne comporter pas plus de cent ordinateur. Ceréseau est limite a une zone géographiqueréduite de quelques centaines de mètres a quelques kilomètres et sont débits est importants, jusqu'aplusieurscentaines de Mégabits

I.3.3. Les réseaux métropolitains ou MAN (Métropolitain Area Network) :

Constitue d'une séries desréseaux locaux permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé a haut débit qu est géré a l'échèle d'une métropole pour leur donnée la possibilité de dialogué avec l'extérieur. Ceréseau est étendu sur une dizainede kilomètres.

I.3.4.Lesréseauxétendus ou WAN (Wide Area Network) :

Destiné a transporté des donnéesnumériques sur des distances a l'échèle nationale, voire d'un continent ou plusieurs continents (Internet). Ils sont soient terrestres, soientsatellitaires et ils relient des réseaux MAN et LAN.

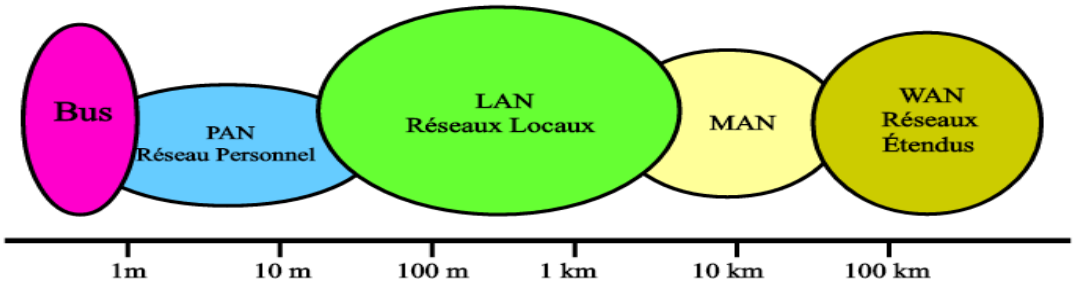


Figure I.1 : Type des réseaux.

I.4. Architectures des réseaux

I.4.1. Architecture Client/serveur

Le principe d'un environnement client/serveur est basé sur le fait que des machines clientes communiquent avec un serveur qui leur fournit des services qui sont des programmes fournissant des données telles que l'heure, pages web, fichiers, etc.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines dites clientes.

Cette architecture présente une hiérarchie à deux niveaux :

- **Le serveur** : C'est un ordinateur qui centralise les ressources partagées entre les postes. Ainsi, les ressources sont disponibles en permanence. Afin de satisfaire les requêtes (demandes) de l'ensemble des postes du réseau, le serveur possède une configuration évoluée : un (ou plusieurs) processeur(s) rapide(s), une mémoire centrale de grande taille, un ou plusieurs disques durs de grande capacité, etc.

- **Les clients** : Les postes connectés sur le réseau sont de simples stations de travail, qui exploitent les ressources mises à leur disposition par le serveur. Leurs configurations sontadaptées aux besoins des utilisateurs.

Figure I.2 : Schéma client/serveur.

I.4.1.1. avantages de l'architecture client/serveur

- une administration au niveau du serveur des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction

- sécurité : l'application d'une stratégie de sécurité est plus facile à mettre en œuvre vu que le nombre de point d'accès est limité.

- un réseau évolutif : grâce à cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure

I.4.1.2. Inconvénients de l'architecture client/serveur

Etant donné que tout le réseau est articulé autour du serveur, sa mise hors service engendre la paralysie de tout le réseau. En plus, l'implémentation d'un réseauclient/serveur entraîne un coût élevé et demande un personnel qualifié pour l'administrer.

I.4.2.Architecture Poste à Poste (égal à égal)

Dans une architecture d'égal à égal (Peer to Peer, notée P2P), contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié : tous les ordinateurs sont égaux, chacun reste indépendant, tout en mettant certaines ressources à la disposition des autres.

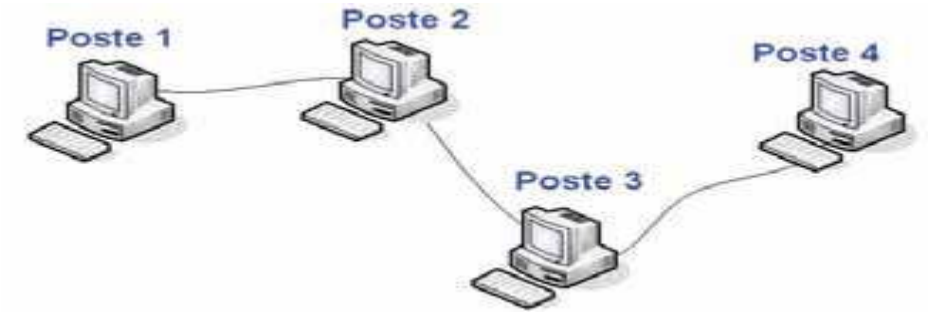


Figure I.3: Architecture poste à poste

I.4.2.1. Avantages de l'architecture poste à poste

- L'architecture d'égal à égal est simple à mettre en œuvre et son coût est réduit par rapport au coût engendré par la mise en œuvre d'une architecture client/ serveur.

-La mise hors service d'un poste n'atteint pas gravement le fonctionnement du reste du réseau.

I.4.2.2 Inconvénients des réseaux poste à poste

Les réseaux d'égal à égal présentent un certain nombre d'inconvénients :

- Ce système n'est pas centralisé, ce qui le rend très difficile à administrer,
- La sécurité est plus difficile à assurer, compte tenu des échanges transversaux,
-Aucun poste du réseau ne peut être considéré comme fiable.

Ainsi, les réseaux d'égal à égal sont utilisés pour des applications ne nécessitant ni un haut niveau de sécurité ni une disponibilité maximale.

I.5. Topologie des réseaux

I.5.1.Topologie physique

Une fois un équipement connecté physiquement sur le réseau, il faut qu'il puisse recevoir et envoyer des informations aux autres nœuds du réseau.

Le tableau suivant décrire les déférentes topologies physique en détails :

Topologie	Description
Topologie en bus	Tous les postes sont directement connectes a un seul segment
Topologie en anneau	Chaque poste est connecte a son voisin. Le dernier poste se connecte au premier. Cette topologie crée un anneau physique de câble. Inconvénient :si une machine tombe en panne, le réseau est coupe
Topologie en étoile	Tous les câbles sont raccordes a un point central. La fiabilité du réseau est conditionnée par le nœud central
Topologie étoile étendue	Repose sur la topologie en étoile. Elle relie les étoiles individuelles entre elles en relient les nœuds centraux. Cette topologie étend la portée et l importance du réseau.
Topologie hiérarchique	Est créée de la même façon qu' une topologie en étoile étendue. Toutefois, au lieu de relier les nœuds centraux ensemble, le système est relie a un ordinateur qui contrôle le trafic dans la topologie
Topologie maillée	Chaque poste possède ses propres connexions a tous les autres postes. Inconvénient majeur : necessaire beaucoup de câbles (pour n machine il faux n(n-1)/2 câbles)

Tableau. I.1 : Les Topologies physique et leurs descriptions des réseaux informatiques.

Dans La figure suivante on présente les déférentes topologies de réseau informatique

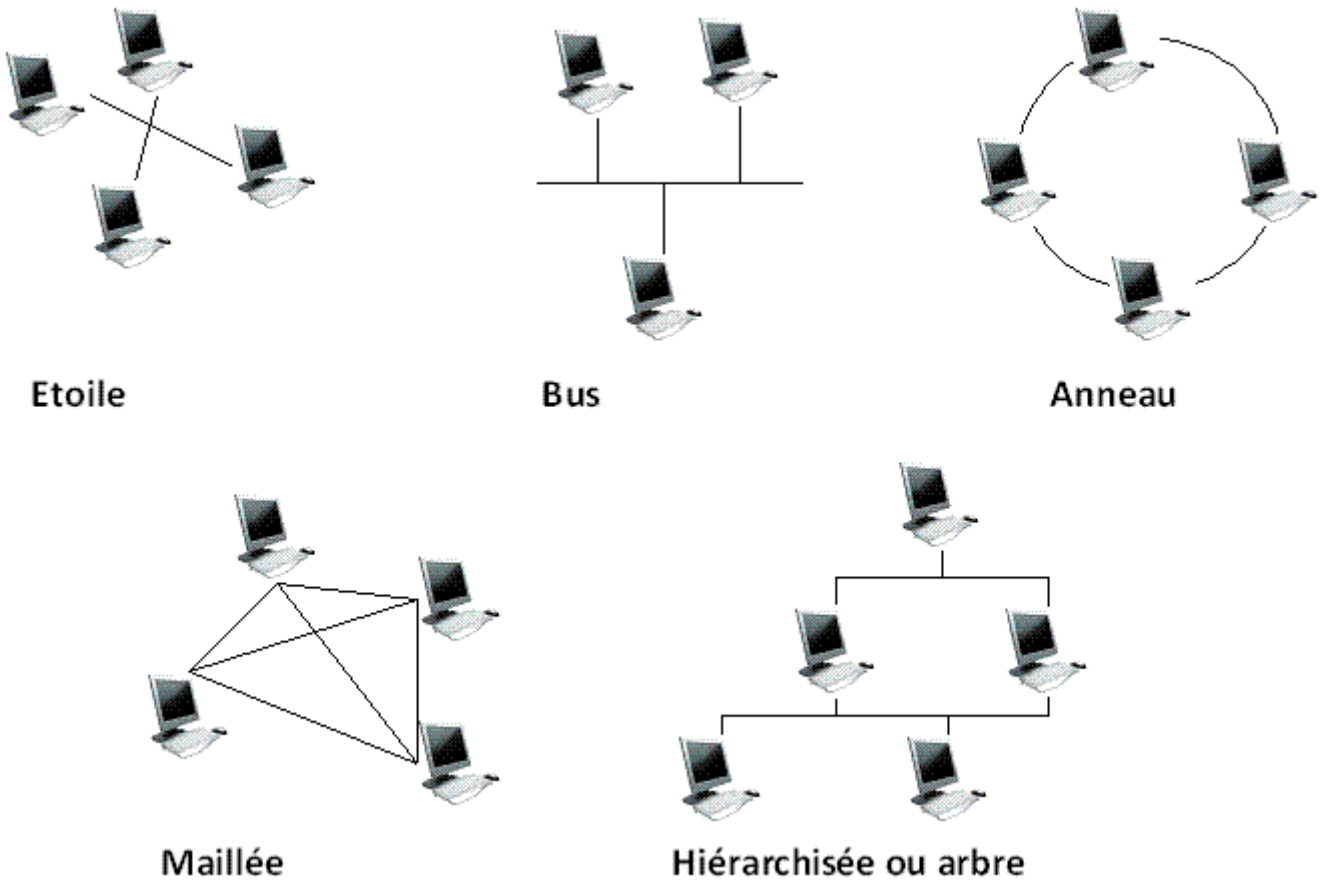


Figure I.4 : les Topologies physique des réseaux informatiques.

I.5.2.Les topologies logiques

Désignela manière dont un réseau transfère les trames d'un nœud a l'autre .Cette configuration est composée de connexions virtuelles entre les nœuds d'un réseau .Ces chemins de signaux logiques sont définis par les protocoles de couches liaison de données. (4)

- **Topologie Ethernet :**tous les ordinateurs sont reliés a un seulsupport de transmission .la communication se fait a l'aide d'un protocole appelé **CSMA/CD**(Carrier Sense Multiple Access WithColisionDetecr),ce qui fait qu'il aura une très grande surveillance des données a transmettre pour éviter toute sorte de collision .Par conséquent un poste qui veut émettre doit vérifier que le canal est libre avant d'émettre .(4)
- **Le FDDI** (FiberDistributed Data Interface) : une technologie d'accès réseau utilisant des

câbles en fibre optiques ,**le FDDI** est constitué de deux anneaux :un anneau primaire et anneau secondaire ,l'anneau secondaire sert a rattraper les erreurs de l'anneau primaire ,le **FDDI** utilise un anneau a jeton qui sert a détecter et a corriger les erreurs, ce qui fait que si une station tombe en pane ,le réseau continuera de fonctionner .

- **L'ATM (**Asynchrones Transfer Mode):c'est mode de transfert asynchrone ,il s'agit d'un protocole de niveau 2.Les cellules **ATM** sont envoyés de manière asynchrone ,en fonctions des données a transmettre ,mais sont insérés dans le flux de donnés synchrone d'un protocole de niveau inferieur pour leur transport .
- **Le Token Ring :** Token Ring repose sur une topologie en anneau(Ring) .Il utilise la méthode d'accès par jeton (token),seul le poste ayant le jeton a le droit de transmettre .Si un poste veut émettre ,il doit attendre jusqu'a ce qu'il ait le jeton. Dans un réseau Token Ring chaque nœud du réseau comprend un **MAU** (Multi station Access Unit)qui peut recevoir les connexions des postes et qui régénère le signal.(4)

I.6. Les équipements d'un réseau informatique :

- **Le répéteur:**

Un des désavantages du câble à paire torsadé est la limite due à sa longueur maximale dans un réseau. Au-delà de 100m, les signaux s'affaiblissent et deviennent inexploitables. Pour prolonger un réseau, il faut ajouter une unité matérielle appelée répéteur. Celui-ci régénère les signaux au niveau du bit et augmente de ce fait la distance de parcours. Le répéteur est un équipement qui intervient au niveau 1 du modèle **OSI**. C'est donc un connecteur car il peut permettre de relier deux réseaux d'ordinateur.

- **Concentrateur :**

Le concentrateur est un équipement qui intervient au niveau de la couche 1 du modèle **OSI**. Son avantage est qu'il autorise plusieurs entrées et sorties des signaux (4, 8, 16 ou 24 ports), cet équipement est aussi appelé "hub". Il est surtout utilisé dans les réseaux locaux ayant une topologie en étoile. Il peut avoir une alimentation autonome permettant son fonctionnement même en cas de coupure de courant. Le concentrateur joue le rôle de répéteur en plus plusieurs entrées et sorties.

- **Le pontouBridge:**

Le pont est un équipement qui intervient au niveau deux du modèle **OSI**. Il connecte deux segments de réseau locaux, pour cela il filtre les informations en circulation dans un réseau en empêchant celles destinées aux **LAN** de se retrouver au dehors.

- **Les commutateursouSwitch:**

Le commutateur est une variante du pont. On appelle parfois pont multi port. Il possède des acheminements sélectifs des informations vers certaines machines du réseau en utilisant les adressages correspondants. Par contre le hub réalise un acheminement non sélectif des informations sur le réseau. Toutes les machines reçoivent les mêmes informations, seules celles qui reconnaissent leur adresse effectuent la tâche qui leur incombe. Cette technique s'appelle aussi diffusion des données dabs un réseau. C'est une technique facile à mettre en œuvre mais elle devient inadaptée, lorsque le nombre de machine devient important et supérieur à 10.

- **Le routeur**:

Le routeur est un équipement qui intervient au niveau 3 du modèle **OSI**, il intervient surtout dans la régulation du trafic dans les grands réseaux. Il analyse et peut prendre des décisions (c'est un équipement intelligent). Son rôle principal consiste à examiner les paquets entrants, à choisir le meilleur chemin pour le transporter vers la machine destinataire. On peut relier un routeur à un ordinateur afin de permettre sa configuration (mot de passe, type de réseau). Le routeurest intelligent parcequ'ilestdoté:

- D'unememoir
- D'un programme (algorithme)
- Logicield'exploitation.

- **Le modem modulateurdémodulateur :**

Le modem est un équipement électrique qui effectue une double conversion des signaux (analogique-numérique) dans le sens ligne téléphonique vers ordinateur et numérique-analogique dans le sens ordinateur vers ligne téléphonique.

Il est surtout caractérisé par son débit binaire qui peut être de 512Kbits/s, 256Kbits/s, 56Kbits/s. Il permet à un ordinateur d'accéder au réseau Internet à partir d'une ligne téléphonique classique.

- **La passerelle (Gateway)**

Considérée au sens matériel du terme, la passerelle est un équipement recouvrant les 7 couches du modèle OSI. Elle assure l'interconnexion des réseaux n'utilisant pas les mêmes protocoles, exemple: **TCP/IP→IBM.SNA** .La passerelle permet de résoudre les problèmes d'hétérogénéité des réseaux (matériel et logiciel). La passerelle peut aussi être un ordinateur disposant de 2 cartes réseaux et d'un logiciel spécifique qui se charge de convertir les données en provenance d'un réseau d'expéditeur vers le réseau destinataire.

La passerelle est donc utilisée pour différents types d'application:

- Transfert de fichiers
- Accès à des serveurs distants etc.

I.6.1. La structuration physique :

I.6.2. Le support de communication :

Les communications d'information à travers un réseau s'effectuent sur un support qui fournit le canal via lequel le message se déplace de la source à la destination. chaque nature de support correspond une forme particulières du signal qui s' y propage, et donc des caractéristiques différents pour choisir le bon câblage , les supports de transmission sont nombreux. Parmiceux-ci , toitsfamilles à sontdistinguer : [1]

a. **Les support métalliques :** Les paires torsadées et les câbles coaxiaux, sont les plus anciens et les plus utilisées et servent à transmettre des courants électriques.

   Paires torsadées : On trouve deux types une paire torsadée non blindée (UTP : Unshieledtwinted Pair) et une paire torsadée blindée (STP : Single Mode Fibre) se composent de deux conducteurs en cuivre, isolés l'un de autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal . l'enroulement réduit les conséquences des inductions électromagnétiques parasites provenant de l'environnement réduit les conséquences des inductions électromagnétiques parasites prouvant de l'environnement. de plus la STP est enrobées d'un conducteur cylindrique, elles sont mieux protégées des rayonnements électromagnétiques parasites, et donc les plus utiliser dans notre réseau.

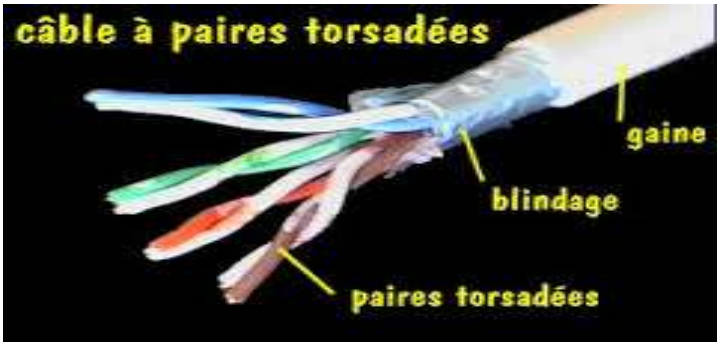


Figure I.5: Câble à paires torsadées non blindées et blindées

Son principale inconvénient est affaiblissement des courants transmis, d'autant plus important réguliers, des éléments appelés est faible. les paires torsadées contiennent, à intervalles réguliers, des éléments appelés est faible. Les paires torsadées contiennent, à intervalles réguliers, des éléments appelés répéteurs qui régénèrent les signaux transmis. utiliser pour les réseaux locaux qui se limitent à quelques kilomètres.

Des avantages sont nombreux : technique maitrisée, facilité de connexion et d'ajout de nouveaux équipements, faible cout. [1]

Câbles coaxiaux : Appelé ainsi le câble BNC. Il est constitué de deux conducteurs pour concentriques maintenus à distance constante par un diélectrique. Le conducteur externe a pour rôle de protéger le conducteur interne des interférences. ce câble présent de meilleures performances que la paire torsadée : autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures. Son débit peut atteindre 10 Mb/s sur une distance de 1 km et diminue en plus grande distance.

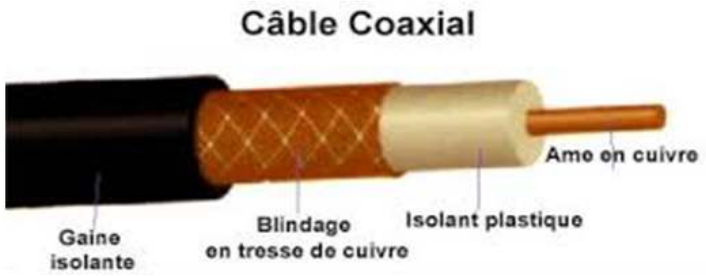


Figure.I.6 : Câbles coaxial

b. Le support en verre :

La fibre optique permet la transmission de données sur les longues distances et à des débits plus élevés qu'avec l'autre support réseau. composé un fil en verre transparent, à la fois flexible et très fin. Les bits àtransmettre sont codé sous forme d'impulsions lumineuses.
Elle sert de guide d'ondes ou « toyou lumineux » qui transmet la lumière entre les deux extrémités avec un minimum de perte du signal. [6]

- La fibre optique monomode : son cœur présente un très fiable diamètre, elle fait appel à la technologie couteuse telle que le laser pour envoyer un seul rayon lumineux. Elle est répandue dans les réseaux longue distance (plusieurs centaine de kilomètres .
- La fibre monomode : la taille de son cœur est supérieure à celle de la monomode et utilise des émetteurs **LED** pour envoyer des impulsions lumineuses selon différents angles.
  Elle est généralement utilisée dans les réseaux locaux pour son faible cout et pour sa bande passante allant jusqu'à 10 Gbit/s sur des liaisons pouvant atteindre 550 mètres de long.
- Connecteur **ST** (Straight-Tip) : concentrateur à baïonnette d'ancienne version couramment utilise avec la fibre monomode.
- Connecteur **SC**(subscriberconnector) : parfois appelé connecteur carre ou connecteur standard , il s'agit d'un connecteur largement utilisé dans les réseaux locaux et étendus qui fiat appel à un mécanisme de clissage permettent de vérifier l'insertion , ce type de connecteur est utilisé avec la fibre optique multi mode et monomode .
- Connecteur **LC**(Lucentconnecter) : parfois appelé petit connecteur ou connecteur local, il est de plus en plus répandu en raison de sa petite taille, il est utilisé avec la fibre monomode et prend &également en charge la fibre multi mode.
- Les câbles de brassage en fibre optique sont nécessaires pour interconnecter des périphériques d'infrastructures.
- Câbles de brassage multi mode SC-SC et ST-LC
- Câbles de brassage monomode LC-LC et SC-ST

Les câbles à fibre optique doivent être protégés par un petit embout en plastique lorsqu'ils ne sont

pas utilisés, notez &également l'utilisation de couleurs permettant de différencier les câbles de brassage monomode et multi mode, c'est la norme TIA 598 qui recommande l'utilisation d'une gaine jaune pour les câblés à fibre optique monomode et d'une gaine orange (ou bleue) pour les câbles à fibre multi mode.

c. Les supports immatériels des communications sans fil :

Les signaux sans fil sont des ondes électromagnétiques qui peuvent circuler dans le vide ou dans des médias tels que l'air (aucun média physique), pour communiquer, un réseau **LAN** sans fil on utilise des ondes radios, des micro-ondes ou des ondes infrarouges.

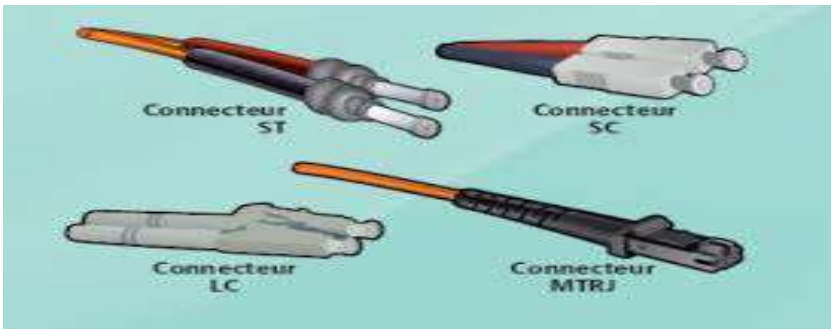


Figure I.7:Fibreoptique.

I.7.1 Le modèle OSI

I.7.1.1. Les couches du modèle OSI de L'ISO :

- **La couche 1 : Matériel**

Dans cette couche, on va s'occuper des problèmes strictement matériels. (Support physique pour le réseau). Pour le support, on doit également préciser toutes ces caractéristiques. Pour le câble :

• Type câble (coaxial, paires torsadées, ...)

• Type du signal électrique envoyé (tension, intensité, ...)

• Limitations (longueur, nombre de stations,...) Pour des communications hertziennes

• Fréquences

• Type de modulation (Phase, Amplitude, ...) Fibre optique

• Couleur du laser
• Section du câble
• Nombre de brins

- **La couche 2 : Liaison**

  La couche liaison des données assure un transit fiable de ces données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (adresses MAC : Medium Access Control), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames (séquences de bits) et du contrôle de flux. Exemple : Ethernet, Token ring.

- **La couche 3 : Réseau**

  Le rôle principal de cette couche est de trouver un chemin pour acheminer un paquet entre 2 machines qui ne sont pas sur le même support physique. Exemple :protocolesIP, ARP, RARP,…

- **La couche 4 : Transport**

  La couche transport doit normalement permettre à la machine source de communiquer directement avec la machine destinatrice. On parle de communication de bout en bout (end to end). La couche transport segmente les données envoyées par la machine source en paquets et les rassemble en flux de données sur la machine destinatrice. Exemple :protocolesTCP, UDP.

- **La couche 5 : Session**

  Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux machines en communication. Cettecouchefournit des services à la coucheprésentation.

- **La couche 6 : Présentation**

  A ce niveau on doit se préoccuper de la manière dont les données sont échangées entre les applications. La couche présentation s'assure que les informations envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système.

- **La couche 7 : Application**

Dans la couche 7 on trouve normalement les applications qui communiquent ensemble. (Courrier électronique, transfert de fichiers,...). La couche application est la couche OSI la plus proche de l'utilisateur. Elle fournit des services réseau aux applications de
l'utilisateur tel que navigateur, tableurs, logiciels de terminaux bancaires, etc.

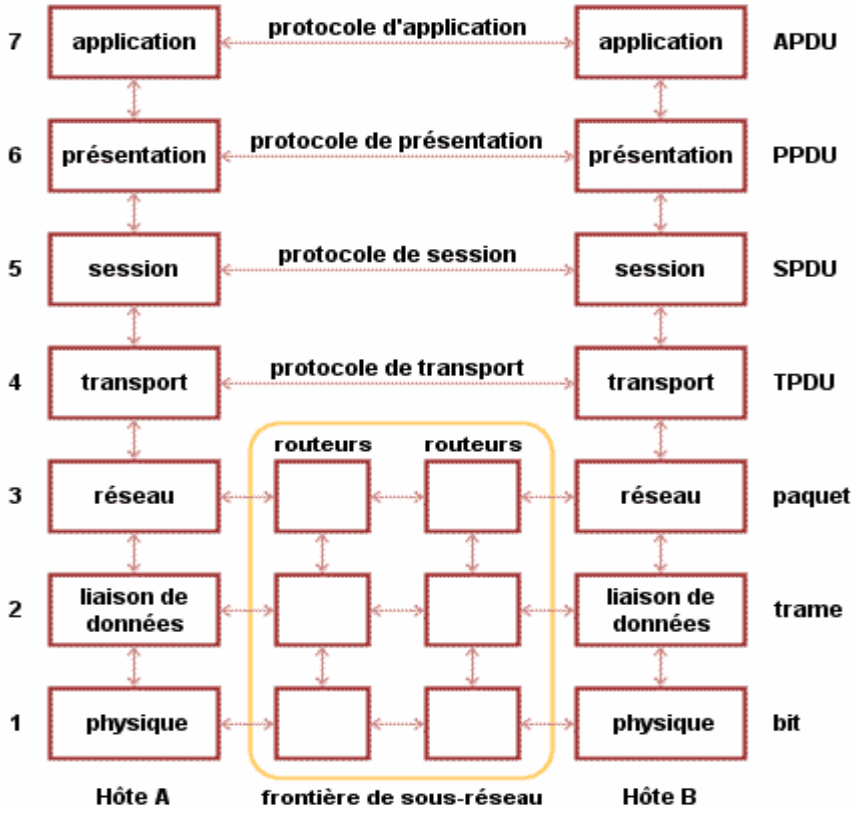


Figure I.8 : Le modèle OSI.

I.7.2 Présentation du modèle TCP/IP

I.7.2.1 Introduction

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP/IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.

L'origine de TCP/IP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l'ARPA (Advanced ResearchProjects Agency), l'agence de recherche du ministère américain de la défense (le DOD : Department of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergeante promettant. C'est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974. L'ARPA signa alors plusieurs contrats avec les constructeurs (BBN principalement) et l'université de Berkeley qui développait un Unix pour imposer ce standard, ce qui fut fait.

I.7.2.2. Description du modèle

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches, et le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

- **La couche hôte réseau :**

Cette couche est assez "étrange". En effet, elle semble "regrouper" les couches physiques et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

- **La couche internet :**

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

- **La couche transport :**

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

- **La couche application :**

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

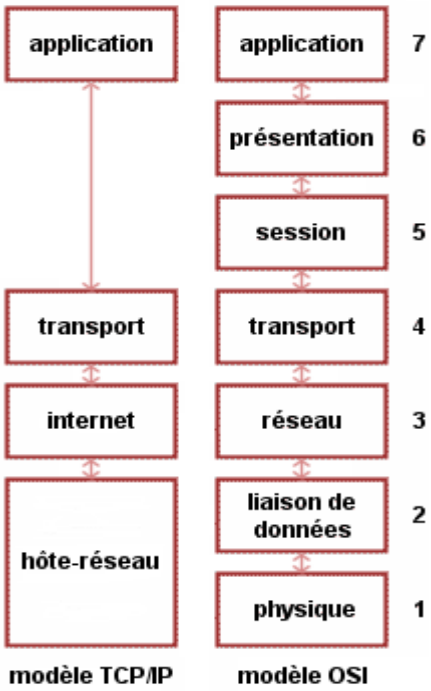


Figure I.9 : Le modèle TCP/IP en parallèle ISO

I.8. Les protocoles

I.8.1.Catégories de protocoles :

Généralement on distingue deux catégories de protocoles selon le niveau de contrôle des données que l'on désire :

- les protocoles orientées connexion : il s' agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machine. Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données quelle envoie les données sont ainsi envoyé en utilisant le protocole TCP.
- les protocoles non orientées connexion : il s'agit d'un mode de communication lequel la machine émettrice envoie des données sans prévenir la machine réceptrice, et cette dernière reçoit les données sans envoyés d'avis de réception à la première ,les données sont ainsi envoyés en utilisant le protocole UDP.

I.8.2. Les protocoles utilisés dans le cadre de notre travail :

Dans notre travaille on a utilisé certains protocoles parmi eu le SNMP quand on a l''utilisé beaucoup plus, le tableau suivant montre les protocoles et leur numéro de port ainsi que leur couche de fonctionnement.

N° Couche ISO	Protocole	N° Port
3	IP	4
4	UDP	17
4	TCP	6
3	ICMP	1
3	IGMP	2
3	ESP	50
3	GRE	47
3	EGP	8
3	IGP	9
3	IGRP	88
3	OSPF	89
3	BGP	179
5	LDAP	389
5	DNS	53
7	SNMP	161/162
7	TFTP	69
7	NTP	123
7	HTTPs	443
7	SSH	22
7	FTP	20/21
7	Telnet	23
7	SMTP	25
7	HTTPs	80

Tableau I.2 : les protocoles les plus utilisés.

les protocoles les plus utilisés :

- Protocole ARP : le protocole ARP (adresse Résolution Protocol) fait la correspondance entre les adresse IP et les adresse MAC. Les adresses MAC sont les trames Ethernet. Lors d'une demande ARP, l'adresse de destination est l'adresse de diffusion (braodcast) font de sorte à ce que tout le réseau reçoit la demande. En revanche , seule la machine possédant l'adresse IP précise dans la demande, répond en fournissant son adresse MAC.
- Fonction PING : la fonction PING (Packet Internet Groper) vérifie la connectivité IP d'un ordinateur en envoyant à travers le protocole ICMP des messages (requète écho) dans le but d'avoir des réponses d'une machine. Les réponses à la requête écho, s'affichent avec les temps des parcours circulaires. PING est la principale commande TCP/IP utilisé pour résoudre les problèmes de connectivité, d'accessibilité.
- TCP : (Transport Control Protocol) fonctionne mode connecté. Avec un contrôle de flux et récupération d'erreur.
- UDP : (User Data Protocol) fonctionne en mode non connecté. Pas de contrôle de flux ni récupération d'erreur.
- TELNET : (Télécommunication NETwork) fournit des services de type présentation, permet de connecter des terminaux virtuels à distance.
- SNMP : (Simple Network Management Protocol) : C'est un protocole de l'information entre les défient agents (des agents écoutant les requêtes sur les ports UDP 161 et les alarmes sur le port 162). Chaque agent situé sur un nœud de réseau renseigne périodiquement les variables de **MIB** (délai paramétrable dans le fichier de configuration par default fixé à 30 seconde avec agent net-**SNMP**).[8]

Le format de trame **SNMP** est décrit ci-dessous :

Version	Communauté	PDU

Tableau. I.3 : Format de la trame SNMP.

- **Version** : numéro de version SNMP. L'administrateur et agent (de l'équipement) doivent utiliser le même numéro.
- **Communauté** : ce champ sert à identité l'agent auprès de l'administrateur avant de lui accorder un accès.
- **PDU** : il y'a cinq type de PDU GetRequest, GetNextRequest, GetResponse, SetRequest et TRAP.

a- La mise en place d'une structure utilisant SNMP fait intervenir plusieurs concepts :

- **La station d'Administration** : c'est la machine qui centralisé les données, c'est le cœur du système .c'est notamment cette station qui va dialoguer avec les différents équipements administrer
- **Les agents SNMP** : ils sont installés sur tous les éléments du réseau supervisé (machines serveurs ou élément active).Ils envoient les TRAPs SNMP et répondent aux requêtes de la station d'administration.
- **Les MIBs** : (Management Information Base) sont des sorties de base de donnée avec une topologie en arbre qui décrivent et sauvegardent des variables SNMP. Elles sont présentées sur tous les équipements, y compris la station d'administration.
- **Les variables SNMP** : ce sont les feuilles de la MIB. Ces variables sont identifies numériquement ou normalement par des OID (Objet IDentifier). Comme nous le disions plus haut, le protocole est utilisé pour connaitre a un instant donné l'état d'un matériel. Ainsi ce sont ces variables qui nous permettrons par exemple le nombre des paquets entrants et sortants sur une interface donne ou encor la température CPU d'un serveur.

b- Son fonctionnement :

comme nous allons voir dans le troisième et le quatrième chapitre, SNMP est le protocole de référence au matériels de supervision il permet à un serveur central de communiquer avec tous les équipements et les serveurs pour connaitre l'état de très nombreux paramètres tels que la température dans le châssis de la machine l'état des interfaces, des ports , le taux d'utilisation CPU… ce protocole permet également au serveur centrale (appelé station d'administration SNMP), récupérer toutes les alertes

SNMP (les TRAPs) émisses par les éléments actifs au serveur supervisé une interface permet généralement d'administrer l'ensembles des machines et de visualiser leur état en temps réel .

Ce protocole est basé sur un échange d'information (par message) entre le matériel et la station de supervision .SNMP est un protocole de type client serveur, donc basé sur l'utilisation des agents SNMP.

L'accès aux variables d'un matériel réseau se fait grâce a un mot de passe particulier que l'on appelle la communauté :

- La communauté en lecture (RO :ReadOnly) pour le public.
- La communauté en écriture (RW :ReadWrite) pour le public.

le schéma ci-dessous nous montre les différentes étapes d'une connexion par le protocole SNMP entre une NMS (pour Network Management Station) et des nœuds de réseau.

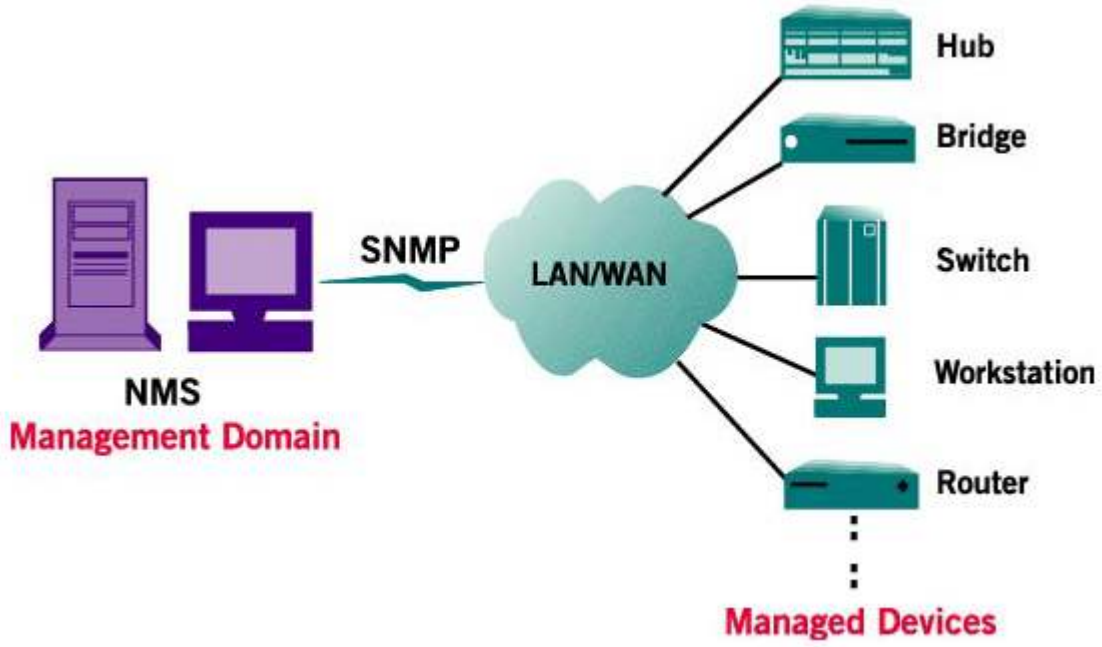


Figure I.10 : Schéma de communication entre une NMS et les équipements

On peut voir apparaitre notamment trois des cinq types de requête de basiques proposées par le protocole.

- Les requêtes « get » servent à obtenir des informations.
- Les requêtes « set » servent à modifier la valeur des variables des MIB.
- Les requêtes « getresponse » servent à obtenir la réponse de l'agent distant.

Ainsi on pourra également trouver des requêtes « TRAP » qui représente des messages d'alerte envoyés spontanément par la machine administrée à la station administratrice (c'est un cas particulier car en principe le nœud ne fait que répondre à des requêtes du serveur). Enfin il faut citer les requêtes du types « getnext » qui permettent de connaitre la valeur de la variable se trouvant après celle qu'un on lui passe en paramètre (permet notamment de parcourir toute une branche de MIB…)

D'une manière générale nous distinguons deux modes de fonctionnement complémentaires mais aux principes bien distincts :

- Le mode « poll SNMP » : la station d'administration demande à un agent SNMP de lui retrouver la valeur de telle ou variable. Cela se passe donc en deux étapes, la requête du serveur pour interroge le client, et la réponse du client. Le serveur (ou station d'administration SNMP) peut ainsi connaitre à des intervalles réguliers les informations qu'il souhaite. Nous venons de citer à titre d'exemple la température interne d'un élément actif, mais on peut aussi connaitre le taux d'utilisation du processeur en temps réel, l'espace disque libre d'une machine.. le serveur est donc charger d'interroger une liste d'informations bien précise pour connaitre l'état de la machine. Le problème qui se pose est que l'on ne pas connaitre à l'avance la nature des incidents. Ainsi,si l'un des deux processeur d'un élément active est en panne , le second prend le relais automatiquement et personne ne s'aperçoit de rien, jusqu'au jour où le deuxième tombe en panne à son tour…
- Le mode <<Trap SNMP>> : un trap SNMP est un message informatif qui est envoyé par l'agent SNMP en cas d'incident à destination du serveur qui est toujours en écoute des ces messages. Pour reprendre notre exemple du processeur, si le premier venait à griller, un message indiquant la nature de l'incident est envoyé automatiquement à la station d'administration pour prévenir l'administrateur que le processeur n°1 de tel élément est hors service. La station d'administration se contente donc d'être à l'écoute de ces traps SNMP

  Ces deux modes permettent donc de superviser l'état des différents équipements du réseau. c'est ici que ce trouve la limite de ce protocole SNMP. Le protocole de SNMP ne supervise que les premières couches du modèle OSI. On peut ainsi connaitre l'état

d'une machine, si elle est active et en << bonne état >> ou non, mais on ne sait pas si les services eux sont bien actifs et accessibles.

- Protocole ICMP : le protocole ICMP (internet contrôle message protocole) est un protocole d'information entre nœuds utilisateurs de service internet (Ping, algorithmes de traçage de route). Il permet aussi de gérer les informations relatives aux erreurs des machines connectées et d'en informer les différents émetteurs des datagrammes en erreurs. ICMP ne sait pas corrigé ses erreurs et il n'a aucun moyen de s'assurer que les paquets arrivent bien à destination. Les messages d'erreurs ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi ,les messages d'erreur peuvent eux-mêmes être sujet d'erreurs.

I.9. La supervision des réseaux

I.9.1. Définition :

La supervision réseau (ou monitoring) comprend un ensemble de protocoles matériels et logiciels informatiques permettant de suivre à distance l'activité d'un réseau informatique. Ces solutions permettent également de cartographier le réseau.

La supervision est particulièrement adaptée pour des réseaux de plus de 50 machines et pour les prestataires de services.

Le principe général est le suivant :

- Des agents (ou sondes) sont placés sur les équipements à surveiller
- Un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs.

Il convient de distinguer la supervision qui utilise des technologies quasi temps réel de la gestion de parc informatique qui utilise des technologies moins dynamiques (inventaires de machines, gestion des stocks, …).

I.9.2. Types de surveillance et actions liées :

Globalement, les outils de supervision sont utilisés pour la surveillance :

- Matérielle (activité d'un équipement, charge, ...)
- Réseau (débit, latence, taux d'erreur, QoS, protocoles, sécurité ...)
- Système (logs, performances, intégrité)
- Applicative (performances, modifications de configuration, analyse)

Les actions liées aux événements peuvent être :

- Un enregistrementdans un journal
- Un tracégraphique
- Unealerte (mail, SMS, …)
- Une exécution de script pour automatiser les tâches à faire.

I.9.3. Protocoles :

- SNMP : est le protocole incontournable de la supervision. C'est un protocole de niveau applicatif. Il sait analyser les informations de tous les niveaux (physiques, réseaux, services, systèmes). Toutes les plateformes peuvent installer le service SNMP (Windows, Linux, Cisco, HP, …) mais aucune ne l'active par défaut, pour raison de sécurité.

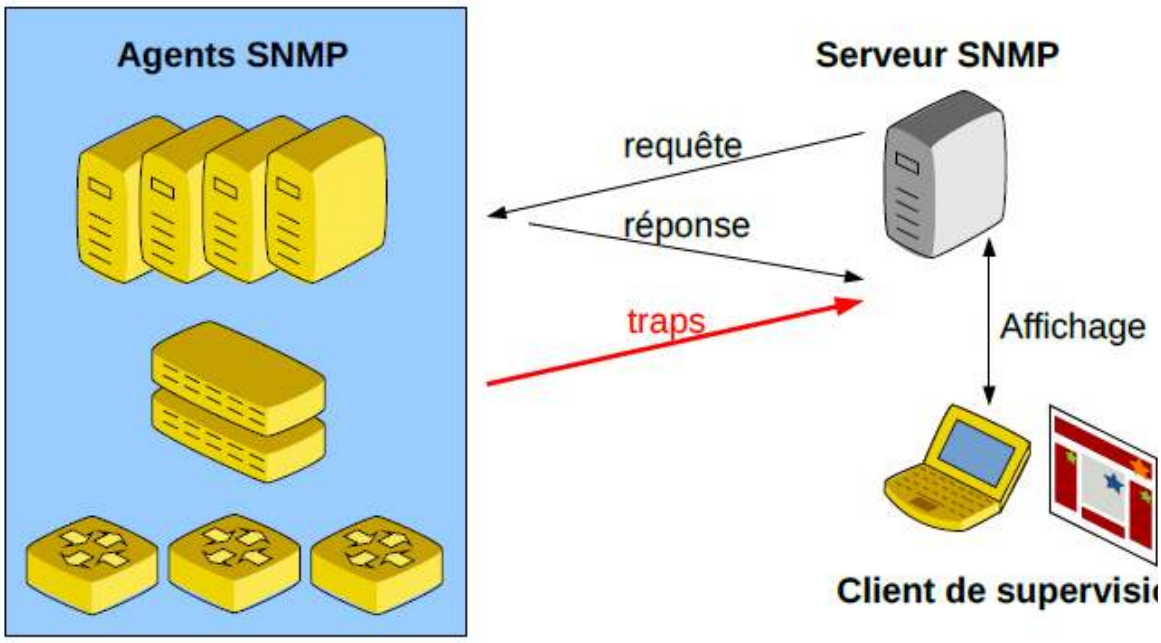


Figure I.11 : Communication Client/serveur avec Les agents SNMP.

Protocole : Les agents de supervision communiquent avec le serveur de trois manières :

• Requête **SNMP** (du serveur vers l'agent)
• Réponse **SNMP** (de l'agent vers le serveur)
• Alarme (ou trap) envoyée de l'agent vers le serveur quand un problème arrive.

Communautés : Une communauté est un groupe d'agents. **SNMP** fonctionne par communauté.
Côté agents :
• On créé une communauté publique (souvent nommée public) accessible à tous en lecture seule
• On créé une communauté privée (avec un nom quelconque) accessible en lecture/écriture mais protégée par un mot de passe. Côté serveur, on ajoute les hôtes et on indique les éléments de **la MIB** à surveiller.

Versions :

SNMPv1 n'est plus utilisé aujourd'hui car il est très peu performant dans les échanges de trames. Le standard est la version **SNMPv2.**

La version SNMPv3 apporte la notion de sécurité et de chiffrement mais n'était pas supportée par tous les équipements jusqu'à maintenant.

Solutions applicatives :

Pour simplifier le travail de supervision et ne pas être dépendant du protocole **SNMP**, les logiciels de supervisions développent souvent un protocole ou un agent particulier pour leur solution (agent zabbix, NRPE pour Nagios, etc.).

- **MIB (Management Information Base) :** Le protocole spécifie une base de données qui stocke des attributs classées dans un arbre. La **MIB** utilisée peut-être normalisée (ex : Mib II) ou spécifique.

Exemple partiel de **MIB**(Requête pour connaître le nom de la zone d'un serveur **DNS**) :

iso.internet.internet.internet.mgmt.mib-2.dns.dnsServ**MIB**.dnsServMIBObjects.
dnsServZone.dnsServZoneTable.dnsServZoneEntry.dnsServZoneName
1.3.6.1.2.1.32.1.1.4.1.1.1

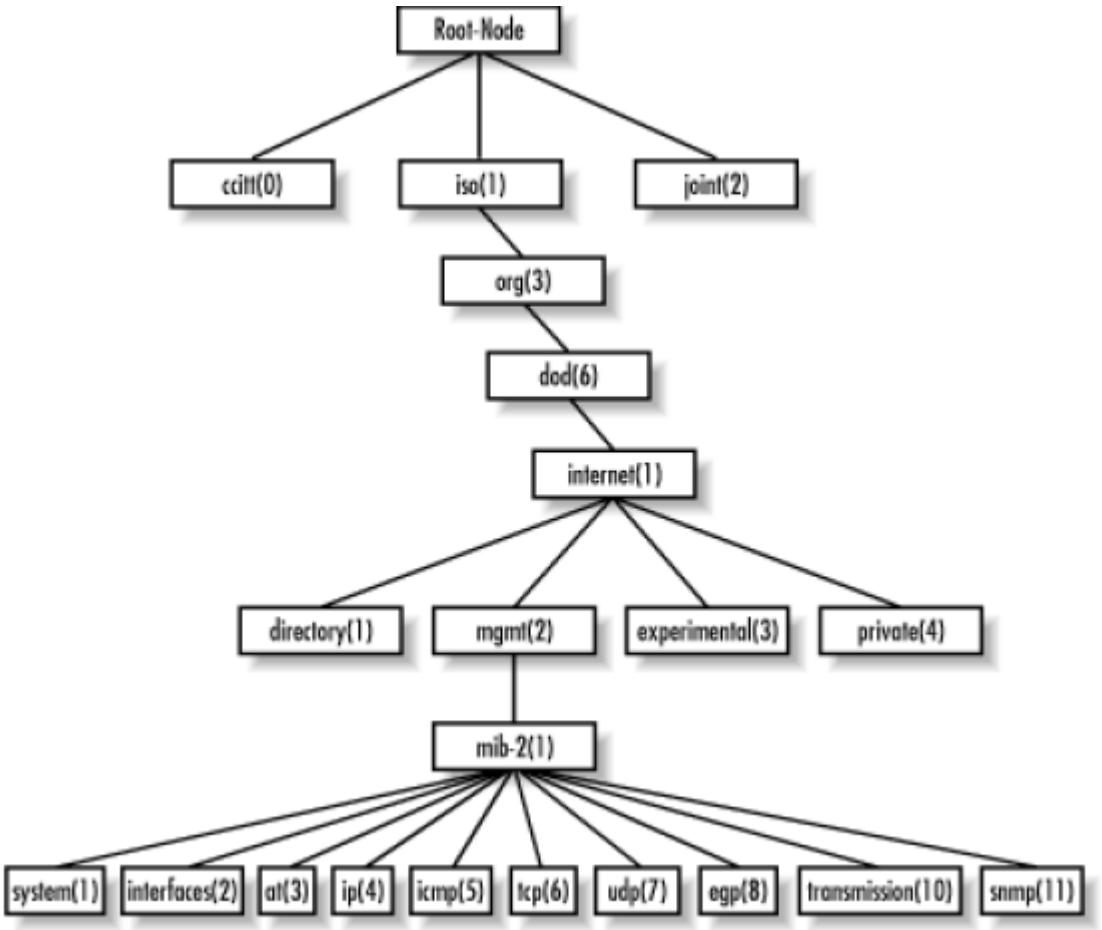


Figure I.12 : Représentation hiérarchique Requête de cet exemple **MIB**.

- **ICMP** : est le protocole associé à **IP** (niveau 3) qui permet le dépannage et la surveillance et la détection de problèmes du niveau 3.

  Il est utilisé par certains systèmes de supervision d'équipements réseau

  C'est un protocole très simple qui envoie un code d'erreur en cas de problème.

Pour les supervisions systèmes et applicatives, **ICMP** ne peut être efficace car il est limité au niveau3.

I.9. 4. Solution de supervision :

Il existe de très nombreuses solutions de supervision existantes. Le monde du logiciel libre est particulièrement actif dans ce domaine. On distingue parmi eux des solutions libres les plus connues, des solutions propriétaire privés pour les grandes entreprises et le tableau I.4 ci dessous représente un comparatif :

Noms	Nature	Mode d'acquisition	Prise en main	Exigences matériels
Nagios	Libre	Téléchargement	Difficile	Tourne sur linux
Centreon	Libre	Téléchargement	Assez facile	Tourne sur linux
Shinken	Libre	Téléchargement	Facile	Tourne sur linux
Zabbix	Libre	Téléchargement	Difficile	Tourne sur linux
Eyes of network	Libre	Téléchargement	Facile	Tourne sur linux
HP Open view	Propriétaire	Achat	Facile	Lourd
IBM Tivoli monitoring	Propriétaire	Achat	Facile	Lourd
Microsoft système center	Propriétaire	Achat	Facile	Lourd
PRTG	Propriétaire/libre	Téléchargement/achat	Assez Facile	Assez lourd
Netcrunch	Propriétaire/libre	Téléchargement/achat	Assez Facile	Assez lourd

Tableau I.4 : Comparatif des solutions de la supervision d'un réseau informatique.

1.10. Conclusion

Les techniques utilisées dans les réseaux informatiques nécessitent du matériel, des supports de communication dans leur différente constitution, et des couches et leurs différents protocoles, ce qui permettra de mieux appréhendé le chapitre suivant qui consiste une vue globale sur l'architecture du réseau universitaire de sa gestion et son contrôle.

Chapitre II :

Architecture du réseau universitaire

II.1. Introduction :

Ce chapitre présente le concept général de l'architecture de notre compus universitaire ainsi que les différents logiciels et matériels utilisés quiassure le bon fonctionnement du réseau informatique.

II.2. Intranet :

Un intranet est un réseau privé utilisant la technologie de l'internet, généralement dans une société ou une organisation,inaccessible de l'extérieur il utilise le standard client – serveur de l'internet via les protocoles TCP/IP. Les intranets sont habituellementutilisés pour le contenu d'entreprise interne. La sécurité étant étroitement contrôlée par l'administrateur. Ils peuvent être moins restrictifs que ceux utilisés pour le contenu en provenance d'internet. L'accès au service intranet se fait grâce à l'utilisation de navigateur – internet et des serveurs web, basé sur le protocole http.[12]

Son architecture repose généralement sur trois niveauxcomposée de :

- Clients (navigateur web internet)
- Serveurs d'application
- Serveurs de base de données

II.3. Intranet à Université SAAD DAHLEB BlLIDA :

L'intranet de l'université Blida 1 est né dans le besoin de doter les facultés et les établissements d'enseignement et de recherche (laboratoire, salles, bureaux…) d'une infrastructure à la fois solide, dynamique et sécurisée.

L'établissement est lié à internet par une liaison délivrée par le fournisseur d'accès à internet CERIST avec un débit théorique de 100Mbt/s partagé. La connexion internet passe par deux CA (Centre d'Amplification) Alger et Blida avant de parvenir à l'université (figure II.1.)

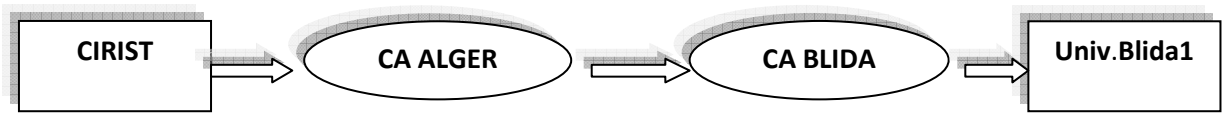


Figure II.1 : parcours de la livraison internet

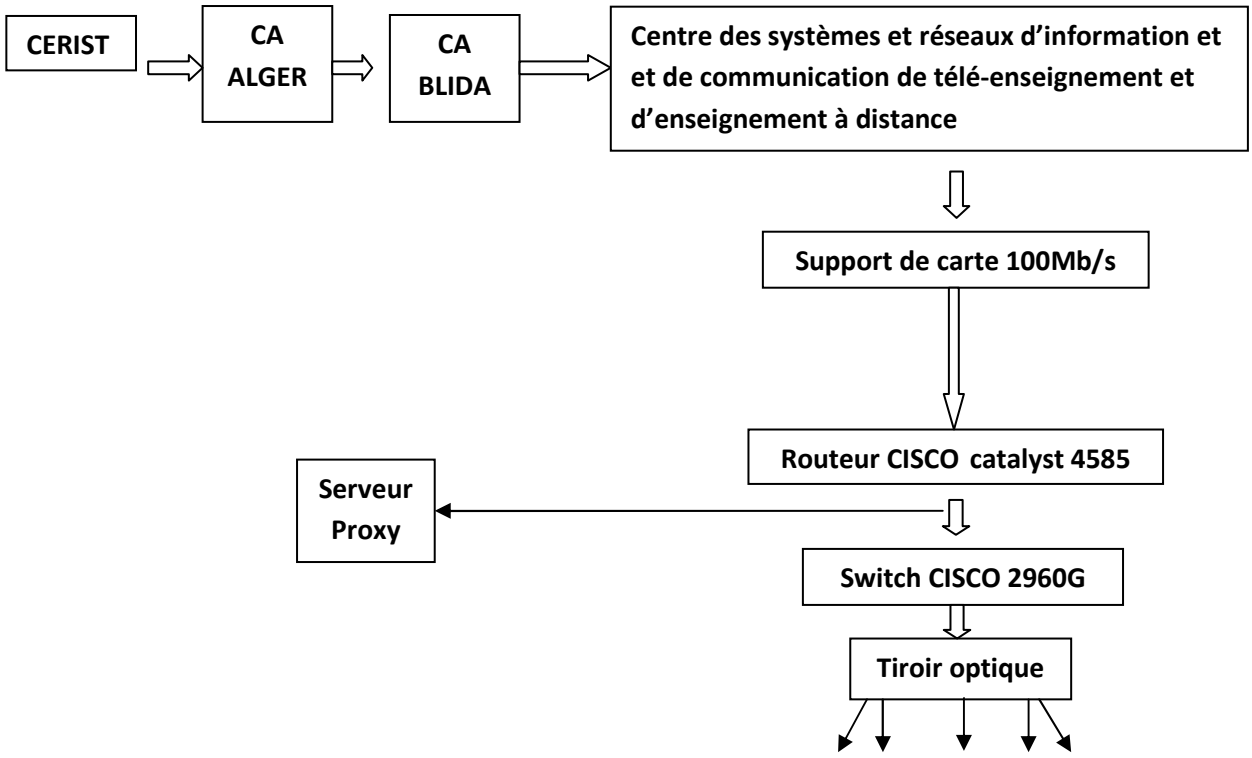


Figure II.2 : Schéma passage de liaison spécialisé

Le tableau II.1 récapitulatif ci-dessous montre en détaille le dispatching des prises à travers les différents pavillons avec un totale de 1705 prises, 78 Switch et 2 routeur.

Branches	**Pavillons**	**Nombres de prises**
01	15	72 pièces installées
	18	48 pièces installées
Groupe principal	20	123 pièces installées
	Bibliothèque	289 pièces installées
02	13	36 pièces installées
	14	65 pièces installées
ZONE 48	16	123 pièces installées
	19	49 pièces installées
03	01	57pièces installées
	02	10 pièces installées

ZONE 03	04	21 pièces installées
	05	34 pièces installées
	27	73 pièces installées
	Rectorat	132 pièces installées
04	Admnistration	13 pièces installées
Groupe de science médicales	LABOS	30 pièces installées
	Bibliothèque	23 pièces installées
05 ZONE 4C	22	64 pièces installées
	23	37 pièces installées
	24	13 pièces installées
	26	46 pièces installées
06 ZONE 4A	06	104 pièces installées
	07	124pièces installées
	08	92 pièces installées
07	Faculté des sciences Économiques	80 pièces installées
	Auditorium	02 pièces installées

Tableau II.1 : Nombre de prise à l'université

Le total de prises installées est 1700

II.4. Présentation de réseau LAN du campus :

Le réseau LAN du campus universitaire de Blida 1 se présente comme étant un système modulaire, articulé autour d'un groupement central ayant le rôle de Data centre, à travers duquel lui sont raccordés l'ensemble des pavillons par un Switch fédérateur catalyst 4006. Les liaisons vers le Switch fédérateur du groupement centrale se fait selon deux modes :

- Une connexion directe (principale), du pavillon concerné vers le groupement central de la fibre optique.
- Des connexion secondaires en fibre optique, pour relier plusieurs pavillon vers un seul, celui-ci est considéré comme étant un « pavillon sous fédérateur », pour aller par la suite se raccorder au Switch fédérateur du groupement central.

Comme le montre la figure suivante (Figure II.4).

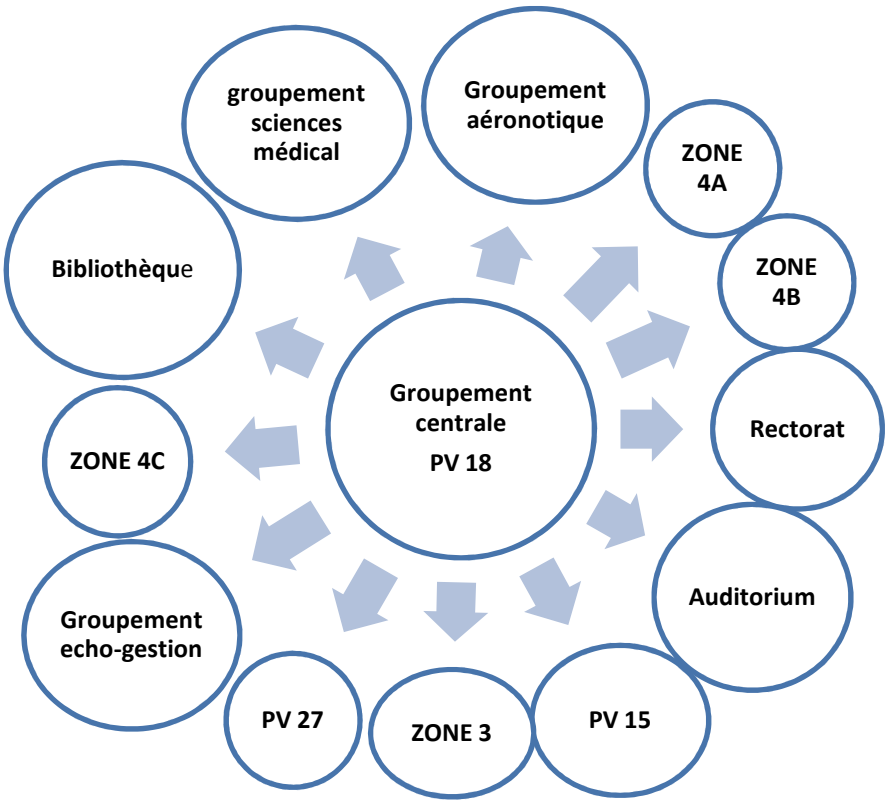


Figure II.3 : Le schéma du réseau LAN du campus universitaire de Blida 1.

II.5. Architecture du réseau :

Le Data Centre du campus universitaire héberge les plateformes de serveurs informatiques.

L'ensemble des équipements, logiciels et de sécurité du réseau vont assurer l'hébergement des applications informatiques, ainsi que la gestion et l'administration du réseau interne de l'université et de l'accès vers le réseau INTERNET via le serveur proxy qui se trouve au pavillon 18. Les réseaux locaux informatiques permettent d'assurer la connexion des postes de travail au niveau de chacun des pavillons du campus universitaire.

II.6. Le plan d'adressage IP :

` Un système de communication doit permettre à n'importe quel hôte de communiquer avec un autre, il est indispensable d'admettre un principe générale d'identification et pour cella trois informations sont nécessaire :

- Le nom de la distante,
- Son adresse,
- La route à suivre pour y parvenir,

Généralement les utilisateurs choisissent des noms symboliques pour identifier les machines tandis que les processeurs de ces mêmes machines ne comprennent que les nombres exprimés au format binaire.

Les adresses IPv4 (version 4) sont standardisées sous forme d'un nombre de 32 bits qui permet à la fois l'identification de chaque hôte et du réseau auquel il appartient. Le choix des nombres composants une adresse IP n'est pas laissée au hasard, au contraire il fait l'objet d'une attention particulière pour faciliter les opérations de routage.[6].

Pour identifier les différents équipements connectés au réseau, le campus universitaire utilise IPv4 la classe « B ». Chaque machine est clairement identifiée par son adresse IP, sans risque de conflits avec d'autres adresses grâce au serveur DHCP qui distribue des adresses IP de manière dynamique.

L'adresse IP des Switchs est attribué manuellement (elle est statique), est donné comme suit 172.20.2X.Y avec :

- X : signifie le numéro du pavillon.
- Y : signifie le numéro du Switch.

Par exemple : 172.20.216.1 est l'adresse IP du premier switch du pavillon 16.

II.7. Les serveurs de l'université :

II.7.1.. Les serveurs actifs Directory :

Active Directory (AD) fournit un service d'annuaire de Microsoft intégré aux versions serveur de Windows. Ce service d'annuaire est basé sur le protocole le plus connu du domaine : LDAP (LIGHTWEIGHT Directory Access Protocol), qui fonctionne en TCP/IP et donc :

a. Les switchs dans chaque pavillon :

Branches	**Pavillons**	**Adressip**	**Non de switch**	**Non du produit**
01 Groupe Principal	15	172.20.215.1 172.20.215.2 172.20.215.3	Non fonctionel SWC2960-PV27-A1-SW2 Non fonctionnel	Catalyst 2950Family
	18	172.20.218.2 172.20.218.10 172.20.218.19	Blida 18_2950 Blida 18_4506 Quidway	Catalyst 2950Family Catalyst 4006 Quidway S3900
	20	172.20.220.1 172.20.220.2 172.20.220.3 172.20.220.4	SW-Aero-1-A1 SW-Aero2-1-A1 SW-Aero2-1-A2 SW-Aero2-1-A3	Catalyst 2900 24TTsw Catalyst 2900 24TTsw Catalyst 2900 24TTsw Catalyst 2900 24TTsw
	bibliothèque	170.20.230.1 172.20.230.2 172.20.230.3 172.20.230.4 172.20.230.5 172.20.230.6 172.20.230.7 172.20.230.8	SW-Bibl_S.etud-0-A1 SW-Bibl_S.etud-0-A2 SW-Bibl_S.ens-0-A1 SW-Bibl_S.ens-0-A2 SW-Bibl_AdminB-1-A1 SW-Bibl_AdminA-1-A1 SW-Bibl_Mag-0-A1 SW-Bibl_Mag-0-A2	Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950 switch Catalyst 2950

				switch
02	13	172.20.213.1 172.20.213.2	SW-Science-1-A1 SW-Science-1-A1	Catalyst 2900 24TTsw Catalyst 2900 24TTsw
Zone 4B	14	172.20.214.1 172.20.214.2	SW-Math-1-A1 SW-Gcivil-1-A1	Catalyst 2900 24TTsw Catalyst 2900 24TTsw
	16	172.20.216.1 172.20.216.2 172.20.216.3 172.20.216.4	SW-Electro-1-A1 SW-Electro-1-A2 SW-Electro-2-A1 SW-Electro-2-A2	Catalyst 2960G séries Catalyst 2960G séries Catalyst 2960G séries Catalyst 2960G séries
	19	172.20.219.1 172.20.219.2 172.20.219.3	SW-Mecanic-1-A1 SW-Mecanic-2-A1 SW-Mecanic-2-A2	Catalyst 2960G séries Catalyst 2960G séries Catalyst 2960G séries
03	01	172.20.201.1	SW2960-Pav1-A12-S11	Catalyst 2950Family
	04	172.20.204.1 172.20.204.2	SW-Techno-1-AA1 SW-Techno-1-A2	Catalyst 2950Family Catalyst 2950Family
	05	172.20.205.1 172.20.205.2	 SW-Tranc-1-A2	 Catalyst 2950Family
	27	172.20227.1 172.20.227.2 172.20.227.3 172.20.227.4	SwC2960-PV27-A12-SW22 SwC2960-PV27-A22-SW12 SwC2960-PV27-A22-SW22 Quidway	Catalyst 2950CSW Catalyst 2950cSW Catalyst 2950cSW Quidway S3900

	rectorat	172.20.231.1	SW-Rect_DFC-0-A1	Catalyst 2950CSW
04		172.20.231.2	SW-Rect_DFC-0-A2	Catalyst 2950CSW
		172.20.231.3	SW-Rect_Planif-0-A1	Catalyst 2950CSW
Groupe		172.20.231.4	SW-Rect_Planif-0-A2	Catalyst 2950CSW
		172.20.231.5	SW-Rect_Planif-0-A3	Catalyst 2950CSW
Science		172.20.231.6	SW-Rect_PED1-0-A1	Catalyst 2950CSW
Médicales	28	172.20.228.1	SW-Medecine_admin-1-A1	Catalyst 2950Family
		172.20.228.2	SW-Medecine_PED-1-A2	Catalyst 2950Family
		172.20.228.3	SW-Medecine_PED-1-A2	Catalyst 2950Family
		172.20.228.4	SW-Medecine_Bibl-0-A1	Catalyst 2950Family
05	22	172.20.222.1	SW-Chimie_Indus-1-A1	Catalyst 2950Family
		172.20.222.2	SW-Chimie_Indus-1-A2	Catalyst 2950Family
Zone		172.20.222.3	SW-Chimie_Indus-1-A3	Catalyst 2960 C
		172.20.222.4	SW-Chimie_Indus2-1-A1	Catalyst 2950Family
4C	23	172.20.223.1	SW-Medecine_23-0-A1	Catalyst 2950Family
		172.20.223.2	SW-Medecine_23-0-A2	Catalyst 2950Family
	06	172.20.206.1	SW-Droit-0-A1	Catalyst 2950Family
		172.20.206.2	SW-Droit-0-A2	Catalyst 2950Family
06		172.20.206.3	SW-Droit-0-A3	Catalyst 2950Family
		172.20.206.4	SW-Droit-0-A4	Catalyst 2950Family
	07	172.20.207.1	SW-Socio-1-A1	Catalyst 2950Family
Zone		172.20.207.2	SW-Socio-1-A2	Catalyst 2950Family
		172.20.207.3	SW-Socio-1-A3	Catalyst 2950Family
4A	08	172.20.208.1	SW-Lang-1-A1	Catalyst 2950Family
		172.20.208.2	SW-Lang2-1-A1	Catalyst 2950Family
		172.20.208.3		
	29	172.20.229.1	SWC2960-PV29-A22SW22	Catalyst 2950Family
		172.20.229.2	SWC2960-PV29-A22SW12	Catalyst 2950Family
		172.20.229.3	SWC2960-PV29-A12SW22	Catalyst 2950Family
		172.20.229.4	Quidway	Quidway S3900

Tableau II.2 : Les Switchs dans chaque pavillon.

Avecle serveur DNS. L'objectif principal est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs, pour pallier des sites web illicites et le téléchargement illégal, Le tableau suivant indique le nombre des personnes authentifiés au sein de notre université.

Total des utilisateurs authentifiés à l'université 2364 utilisateurs

	Désignation	Nombre
01	Administrations	580
02	Enseignements	830
03	Etudiants	1022

Tableau II.3. : Le nombre des personnes authentifiés

II.7.2. les serveurs de messagerie :

Un serveur de messagerie électronique est un logiciel qui est connecté a l'interne. Il peut bénéficier des services de active directory pour : l'ajoute, la suppression, la modification automatique des comptes et extraction d'adresse pour les listes de diffusion. Logiciel client peut être émulé en http, ce qui permit l'accès au courriel depuis un simple navigateur internet. Un serveur LDAP est également disponible et gratuitement pour la gestion des comptes. Il détecte la SPAM il est tentative d'accès non autorisé. Un module additionnel sécurité de plus pour MDaemon, assure une protection efficace du serveur contre les virus.

Au sein de l'université de Blida nous disposons d'une boite de messagerie sous URL htt://mail.univ/Blida réservé pour les enseignants.

II.7.3. Serveur Web :

Un serveur web (également appelé serveur HTTP) est une ordinateur connecté à internet et sur lequel sont hébergés des sites, composés de pages HTML. Le logiciel fédérateur, sur un serveur WEB (Apache, le plus fréquemment), auquel viennent s'adjoindre un interpréteur de langage dynamique (PHP dans la plupart des cas), un gestionnaire de base de données (tel que My SQL) et d'autres programmes, comme un serveur SMTP. La fonction d'unserveur web est de répondre aux requêtes des navigateurs internet (internet Explorer, Firefox, Chrome,…). La page web du site universitaire est **www.univ-blida.dz.**les URL des pages HTML (c'est-à-dire les adresses saisies dans la barre d'adresse du navigateur) commencent par http : //.

II.8. Conclusion :

Dans ce chapitre nous avons vue l'architecture global de université ainsi que les différents nœuds et pavillons qui sont relies entre eux par différents support de transmission, ensuite on a vu les Switchs et leur descriptions ainsi que leur configuration qui est très importante ce qui nous permettra de les détectées dans le réseau grâce à communauté SNMP.

Pour savoir gérer et accéder, superviser et maintenir notre réseau à distance c'étais grâce au logiciel **Ipswich,** Ce que nous allons voir dans le prochain chapitre.

Chapitre III :

Présentation de l’outil de la supervision

III.1 I introduction:

Au sein des environnements d'entreprise actuels, le réseau constitue l'entreprise. En effet, en cas de panne de réseau, c'est toute l'entreprise qui se retrouve bloquée. La gamme de solutions de gestion réseau**Ipswich(WhatsUpGold)**représente le choix idéal pour toutes les entreprises, quels que soient leur profil et leur taille, qui exigent une disponibilité optimale de leurs applications. Grace à une visibilité complète de vos réseaux et applications on peut prendre des décisions pertinentes à partir de données métier exploitables et garder un contrôle total sur l'infrastructure réseau.

Dans Ce chapitreon va présenter cet outil de gestion de réseau avec ces déférents versions et caractéristiques de ce dernier.

III.2 Ipswich(WhatsUpGold):

III.2.1 DéfinitionIpswich(WhatsUpGold) :

Un logiciel de puissantes capacités de détection automatique, de cartographie, de surveillance **SNMP**, d'alerte et de génération de rapport, il offre une visibilité à **360°,** des données métiers exploitables et un contrôle total du réseau.

Il donne aussi une bonne visibilité de la topologie actuelle et de fonctionnement de réseau et nous permet aussi de faire d'éventuelle mise œuvre dessus. **Ipswich**propose une solution de haute performance pour gérer et surveiller de façon efficace l'infrastructure réseau de l'intranet pour assure une croissance stable et bien réorganiser.

Les vues de l'espace de travail et les tableaux de bord intuitifs sur Windows et sur le Web offrent un accès approfondi aux alertes et aux problèmes, ce qui nous donne une vision précise de l'intégralité de notre réseau en temps réel.[13]

La figure III.1 suivante montre la plateforme d'**IpswichWhatsUpGold**:

Figure III.1:plate-formede**Ipswich(WhatsUpGold).**

III.2.2 Caractéristiques d'Ipswich :

III.2.2.1 Détection :

- Détection complète des couches **2** et **3.**
- Ressources de l'infrastructure périphériques réseau, contrôleurs de **LAN** (Local Area Network) , serveurs, logiciels déployés, machines virtuels, connectivité **VLAN** (Virtuel LAN) et port à port.
- Analyse partielle et compète du réseau.
- Mise à jour automatique des cartes et de l'inventaire.

III.2.2.2. Cartographie :

- Cartes détaillées de topologie de couche **2/3** avec infrastructure filaire, sans fils, physiques et virtuelles.
- Connectivité physique et **IP**, relation hôte-invité **VMware**, vus du **VLAN** et des sous réseau, localisation des systèmes physique
- Personnalisation complète des cartes.
- Visualisation des dépendances entre périphérique et la topologie multi-niveau.
- Utilitaire trace-route de couche **2.**
- Enregistrement, impression ou partage de carte avec notre équipe.

III.22..3. Surveillance :

- Prise en charge de **SNMP, SSH (Secure Shell), WMI (Windows Management Instrumentation)**
- Infrastructure sans fils : consommation de la bande passante, décompte des clients, identification des utilisateurs illégitime, donné **RSSI**, utilisation de processeur, rapport signale-bruit et utilisation de la mémoire.
- Jusqu'**20 000** périphériques et **100 000**moniteurs avec un seul serveur **IP Switch.**
- Surveillance en temps réel optimisé avec information et graphe instantané.
- Surveillance des applications**WMI.**
- Surveillance des matériels (onduleur, imprimante, ventilateur et température).
- Surveillance des applications synthétiques.
- Surveillance personnalisé : **JavaScript, VBscript** et **PowerSHELL**.
- Analyseur de requête**SQL** pour **SQL,My SQL** et **ORACLE.**
- **MIB (Management Information Base)** Walker, **MIB**exploré et **MIB** Manager
- Analyseur de performance (utilisation de processeur, espace disque, mémoire).
- Moniteur actifs/passifs préconfigurés.
- Prés en charge de compteurs **32** et **64** bits.

III.2.3 Principales fonctionnalités :

IP Switchnous permet d'établir une correspondance rapide et permanente avec les équipements de notre réseau, ce qu'il nous initie à la surveillance ainsi on reçoit une notification de l'état du dispositif. Les alertes qui sont programmé pour des fonctions précise se déclencherons au moment propice, par exemple lorsqu'un service ou équipement est éteint.

- **Découverte des équipements du réseau :**

La découverte du réseau est une étape irréfutable dans notre travaille, qui consiste a importé les équipements sur une carte réseau pour cela on spécifie l'intervalle qui comporte nos **Switchs**. Elle nous offre une vue unifiée de tous le campus universitaire qui nous permettra de surveiller en permanence notre réseau.

Un sondage du réseau peut être qui consiste à vérifier chaque dispositif dans la carte, il peut ainsi diagnostiquer rapidement les problèmes de performances complexes etlocaliser leur origine puis le surveiller une fois qu'on a crée ou chargé une carte réseau. Chaque contrôle consiste à envoyer une demande de scrutin (poll) à un dispositif et de suivre la réponse. Des informations de la carte du réseau sont disponibles en permanence sur l'état des**Switchs,** qui est actualisé chaque minute.

- **Statistiques des équipements :**

Information sur l'état des appareils qui fonctionnent ou pas ou bien viennent de s'arrêté en indiqué, le pourcentage de réponse et de perte s'il y on a ainsi que le type du protocole.

- **configuration d'un Switch :**

Pour qu'un puisse superviser nos switch Cisco, il faut activer le protocole SNMP sur ceux-ci En effet, le protocole SNMP permet notamment de récupérer des informations statistiques sur les équipements réseaux.

a. Accéder au routeur par la console SSH ou Telnet et activer le mode d'exécution privilégié :

Pour passer au mode privilégié de commande« enable »

Switch>enable

Switch#

b. Passer en mode de configuration :

On tape la commande configue terminal (en abrégé : conf t)

Switch #conf t

Entrerconfiguration commandes, une per line. End with CNTL/A

switch (config)#

c. Attribuer un nom de périphérique au routeur :

Switch (config) # hostname SWC2960-PV1-A12-S11

SWC2960-PV1-A12-S11 (config) #

d. Mettre des mots de passe :

SWC2960-PV1-A12-S11 (config) #enable secret <password>

SWC2960-PV1-A12-S11 (config) #line vty 0 15

SWC2960-PV1-A12-S11 (config) #password <password>

SWC2960-PV1-A12-S11 (config) #login

SWC2960-PV1-A12-S11 (config) #interface vlan1 ip address 172.20.1.1 255.255.0.0

SWC2960-PV1-A12-S11 (config) #no shutdown

SWC2960-PV1-A12-S11 (config) #exit

SWC2960-PV1-A12-S11 (config) #

e. Pour intéger le switchà la communauté SNMP :

SWC2960-PV1-A12-S11 (config) #access-list 99 permit 172.20.218.18

SWC2960-PV1-A12-S11 (config) #snmp-server connunity<nom de la communauté> RO 99 (RO : Read Only)

SWC2960-PV1-A12-S11 (config) #snmp-server connunity<nom de la communité> RW 99 (RW : Read Write)

f. Enregistrer la configuration en cours dans le fichier de configuration initiale.

SWC2960-PV1-A12-S11 (config)#copy running-configstartop-config

SWC2960-PV1-A12-S11 (config)#exit

SWC2960-PV1-A12-S11 #exit

SWC2960-PV1-A12-S11>

\Fin de la configuration, puis fermé la session.

On peut par SNMP suite ajouter des configurations au besoin, par exemple la configuration des traps SNMP qui varie d'un switch a un autre et qu'on peut lister à partir d'une commande

SWC2960-PV1-A12-S11 (config)#snmp-server enable traps ?

Enfin vous active chaque traps SNMP grace à la commande :

SWC2960-PV1-A12-S11 (config)#snmp-server enable traps <type>

\Fin de la configuration, puis fermé la session.

III.3 Conclusion :

Dans ce chapitre nous avons fait une présentation d'usage de cet outil de supervision et explique les différentes fonctionnalités et sa mise en place dans un réseau. Installation d'exécutable de**Ipswich**est simple et flexible il suffit d'activé le policier l'agent SNMP, Après installation et l'activation des outils de **Ipswich**, nous avons pu obtenir les informations sur notre équipements relié au réseau.

Cet outil permet ainsi d'anticiper une panne sur le matériel grâce à un flux d'informations et une clarté des alertes grâce à un code couleur assez explicite que nous allons voir dans chapitre qui suit. On fait les tests de fonctionnalité de cet outil de monitoring

Chapitre IV :
Conceptions,
Réalisation et Test

IV .1. Introduction

Nous avons abordées dans ce chapitre la partie de dispositif de la gestion de notre réseau du campus qu'est constitué d'environs de quarante (40) Switchs avec l'outil de supervision **Ipswich**. Ou dans Chaque étape d'essai on a procédé des tests de fonctionnement au sein du campus.

IV.2. Conception de notre réseau:

Comme nous avons déjà vue dans le chapitre II .notre campus universitaire de Blida contient plus de 40 **Switchs** répartis sur l'ensemble des pavillons. La figure IV.1 .représente cette conception.

Ce Schéma représente la répartition des différentes équipements pour chaque pavillons, notre objectif est d'administré et rétablir les pannes à distance de ce réseau se que nous devoir faire une implémentation sur notre carte interactive **Ipswich** identique avec l'architecture de campus.

IV.3. Tests et Réalisation :

La réalisation de notre projet suit les étapes suivantes :

- Préparation des équipements de gestion.
- Détection des équipements
- La Cartographie
- La Surveillance
- Les Rapports des Alertes

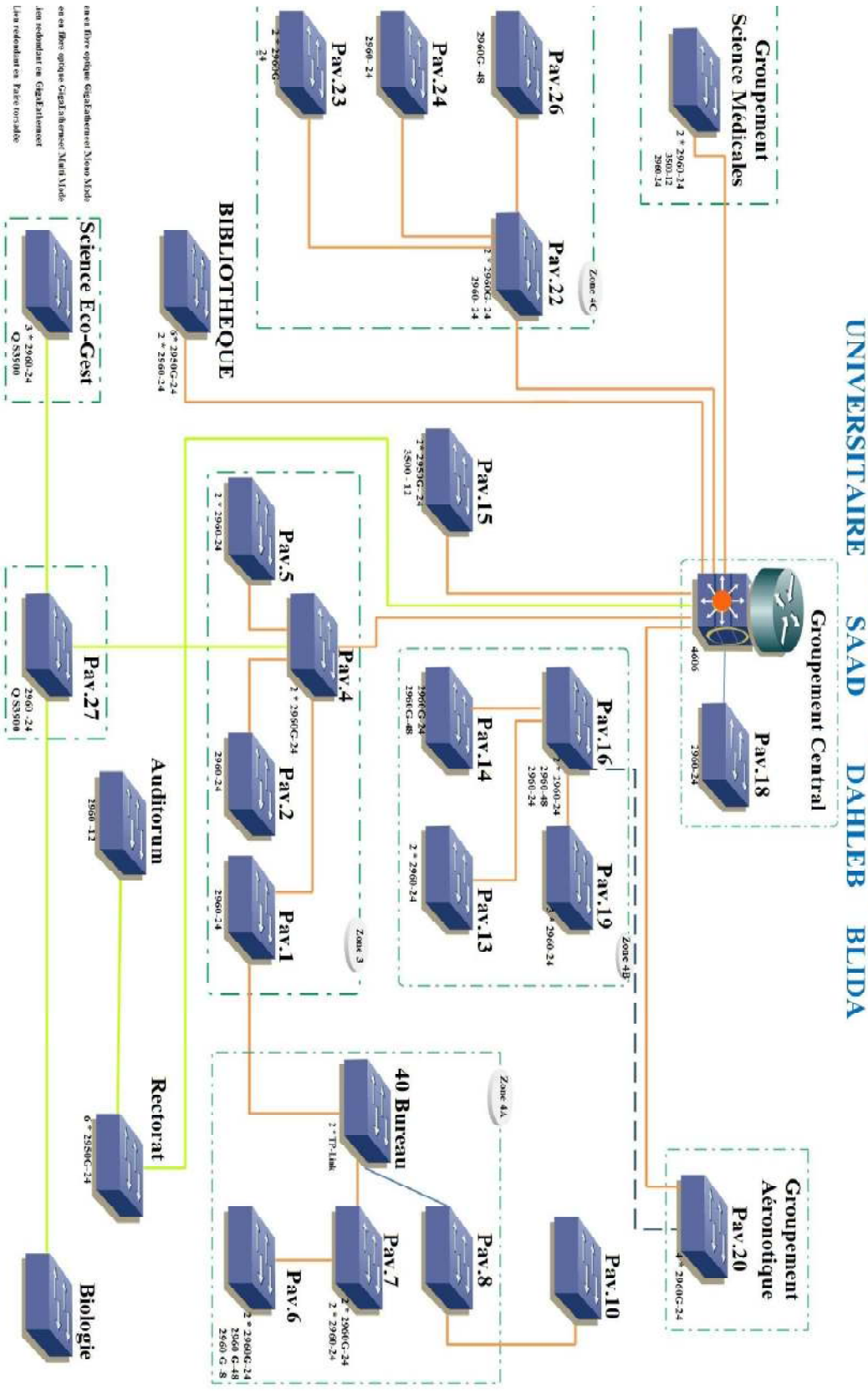


Figure IV.1: Schéma globale du campus universitaire

A partir du schéma de l'architecture du campus on a fait une carte identique sur la plateforme **Ipswich (WhatsUpGold)** pour administrer nos équipements réseau suivant les étapes :

Etape 0:Préparation des équipements de gestion :

Cette étape initiative contient la configuration sur les différents périphériques et le poste administrateur ce que nous permettre d'établir une communication entre l'administrateur et les équipements administrer sur la même communauté du protocole **SNMP**, ces configurations ce déroulent comme suit :

a. Configuration du poste administrateur:

- Installation d'un Windows server 2008 puisque il est compatible et assure un bon fonctionnement du **Ipswich (WhatsUpGold)**.
- Installation **SQL** Server c'était la base des donnés compatible et plus pratique avec l'**Ipswich (WhatsUpGold).**
- Attribuer une adresse **IP** statique au poste administrative ((172.20.100.11).

b. La configuration des Switchs :

- Nous accédons au Switch via **Telnet** (accès à distance) pour apporter les configurations nécessaires.
- On affecte des règles de filtrage (liste d'accès: Access List) aux consultations **SNMP**. Ce filtrage nous offre un complément de sécurité car il permet d'autoriser une adresse IP ou un rang d'adresse **IP** à communiquer avec l'agent, comme suit:

  SWC2960-A12-S11 (config)

Etape 1: détection des équipements :

Cette étape est basée sur la recherche de nos équipements comme suit :

a. **Authentification** :

Afin d'accéder aux différentes fonctionnalités offerte par **Ipswich** (**WhatsUpGold)** une authentification est requise le schéma suivante :

Figure IV.2 :l'Authentification.

Le compte est mots de passe sont modifiables est seront attribué par site. Chaque compte n'aura les droits de lecture que sur les équipements informatiques de son site.

b. La Découverte des équipements de réseau (scanning) :

✓ Recherche d'équipement :

On a lancé une recherche sur nos équipements Switchs à base de plusieurs critères, à savoir : le nom **DNS**, le nom d'affichage ou l'adresse **IP**.

Depuis l'interface **WEB**, on suit les clique suivantes GO > DEVICES>FindDevicecomme elles sont montrées dans la figure suivante :

Figure IV.3 : Recherche des équipements (Switchs).

✓ **Types de recherche des équipements:**

Notre choix de recherche est basé sur les adresses **IP** et l'étape suivante nous permettrons d'entrer le paramètre de recherche souhaité comme suit :

Figure IV.4 : Types de recherche des équipements

Leséléments affichés sur cet onglet dépondront du compte de connexion, comme évoqué auparavant : chaque compte ne sera permissionnaire que sur les éléments de son site.La figure suivante montre les Switchs existants trouvés.

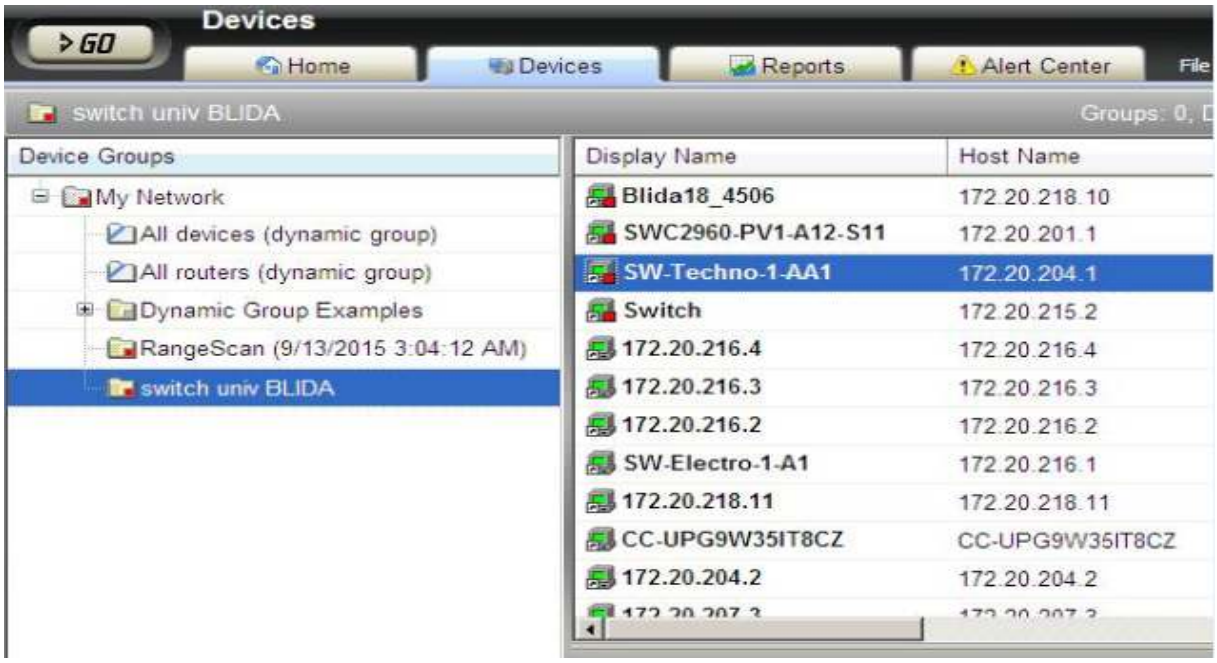


Figure IV.5 : Les Switchs existants

Etape 02: La Cartographie :

Après notre recherche des équipements quand a fait déjà on passe à la deuxième étape avec l'affichage aléatoire des Switchs trouvés on doit les organisés selon l'architecture du campus.

a. Affichage obtenue après la recherche :

1. Le menu principal de l'interface Web : le bouton GO.

2. Arbre du groupe de dispositif : ceci est une liste de tous les groupes associe au site. Ces groupes servent a organisés et classés tous les équipements par type : réseaux, systèmes ou services.

3. Volets de vue : ce volet affiche le groupe sélectionné sur la base de l'onglet ci-dessous (DeviceView/MapView) .

4. Modes d'affichage : on va choisir une façon dont nous souhaitons afficher notre groupe de périphériques (Switchs) parmi les modes suivants :

- ✓ **Affichage des équipements (DeviceView)** : cette vue donne un aperçu de chaque Switch dans un groupe de périphérique sélectionné avec appellation de notre groupe Switvhs « **switch univ BLIDA** » comme il est représente dans la **figure IV.6.**

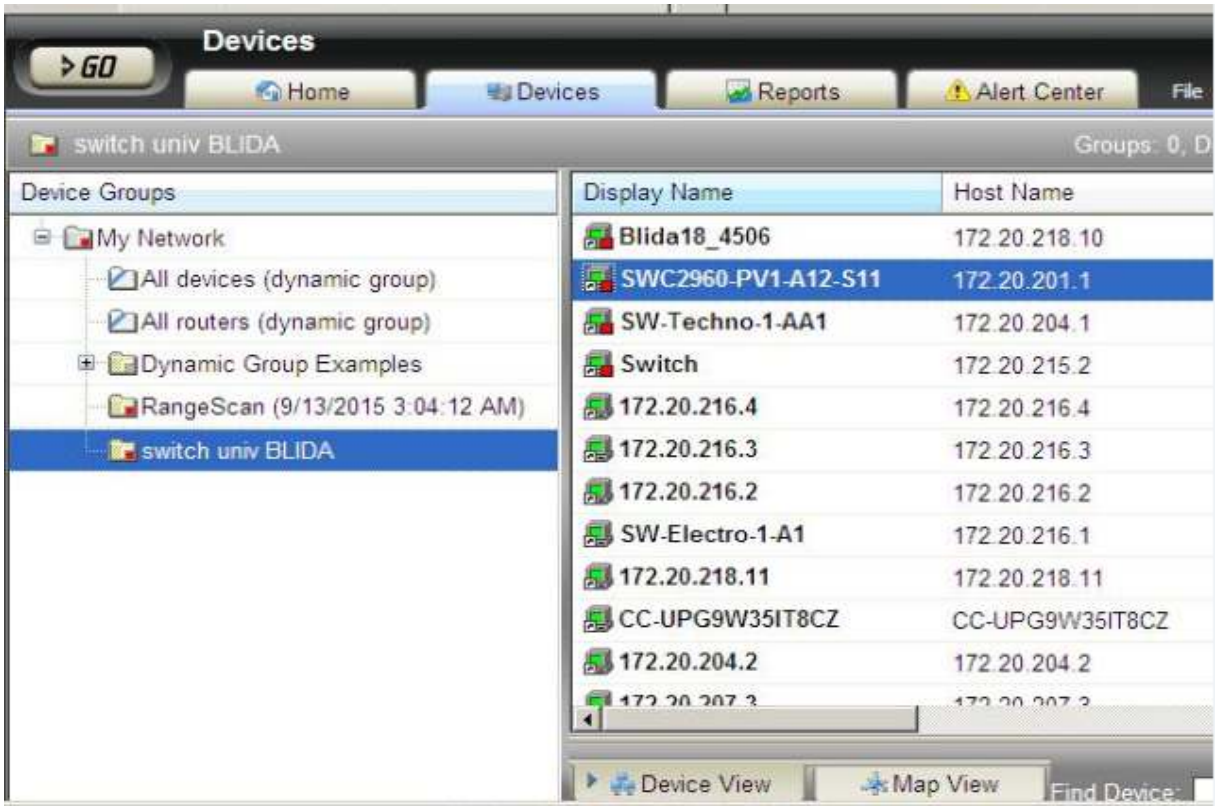


Figure IV.6 : Affichage des Swhitchs

- ✓ **Affichage en Map (MapView)** : cette vue illustre en schéma interconnexion entre nos Switchs de notre site voir la figure IV.7.

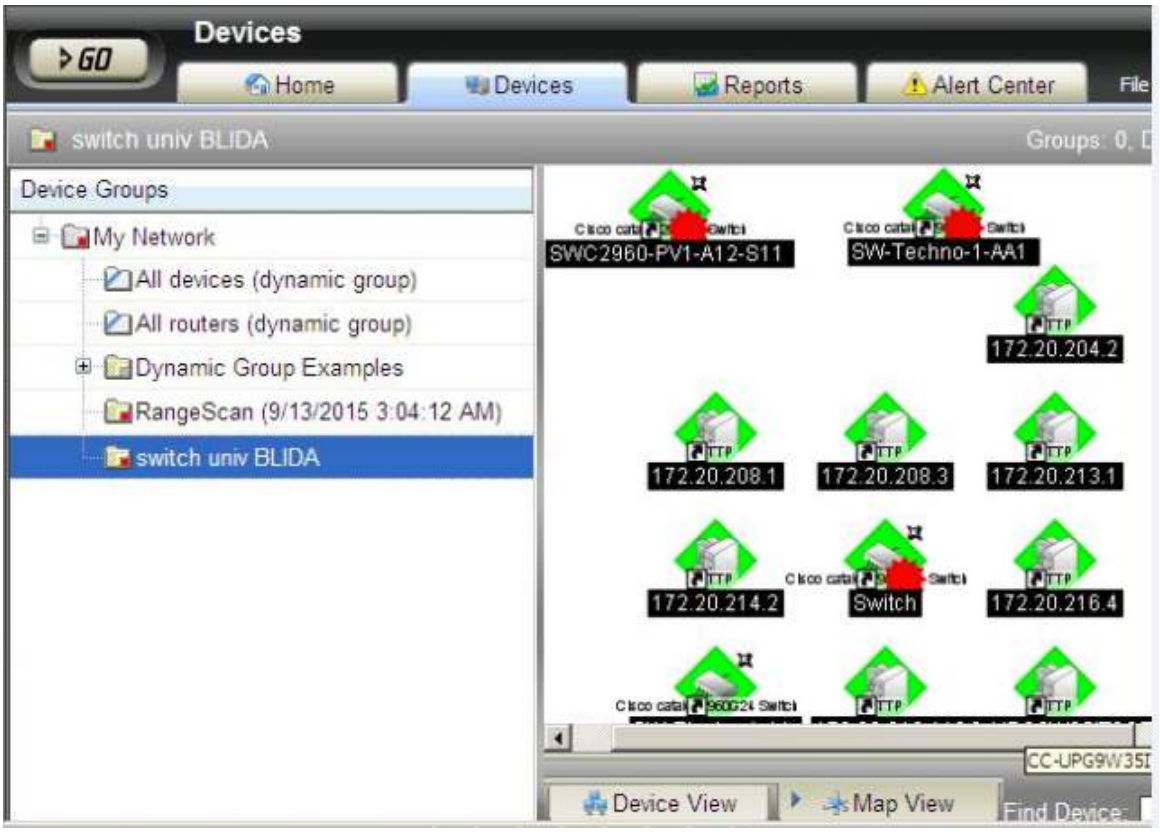


Figure IV.7 : Affichage en Map des Swirchs..

- **Barre d'outils d'équipement (Device) :**

  - ✓ Nouveau équipement (New Device) on utilise ce bouton pour ajouter un nouveau périphérique a notre liste d'équipement (Switch) surveillé.
  - ✓ Nouveau Groupe (New Group) : on utilise ce bouton pour ajouter un nouveau Group à notre liste surveillé.
  - ✓ Nouveau Groupe dynamique (New Dynamic Group) : on utilise ce bouton pour ajouter un nouveau groupe dynamique à notre liste.

b.Organisation des périphériques :

Cette fois on va repartie les Switchs existants chacun dans son propres bloc et selon des types des groupes.

- ✓ **Types des groupes despériphériques (Switchs)** :

En **Ipswich (WhatsUpGold)** les équipements sont organisés en groupe pour nous permettre de trouver et diagnostiquer rapidement les problèmes.

Nous pouvons créer autant de groupe de périphérique que nous souhaitons, cela mène à organiser la console **Ipswich (WhatsUpGold)** d'une manière significative répondant à nous besoin de surveillance.

Les deux types de groupes d'équipements dans **Ipswich (WhatsUpGold)** quand a utilisé sont:

- ✓ Les groupes non dynamiques : sont simplement appelés Groupe
- ✓ Les groupes dynamiques : peuvent être créer pour des types spécifiques d'équipement, des attributs de périphérique Moniteur actifs,… les Groupes Dynamiques agissent comme des requêtes SQL qui s'exécutent sur la base de données **IPSwitch (WhatsUp Gold)**, et affichent en temps réel les données.

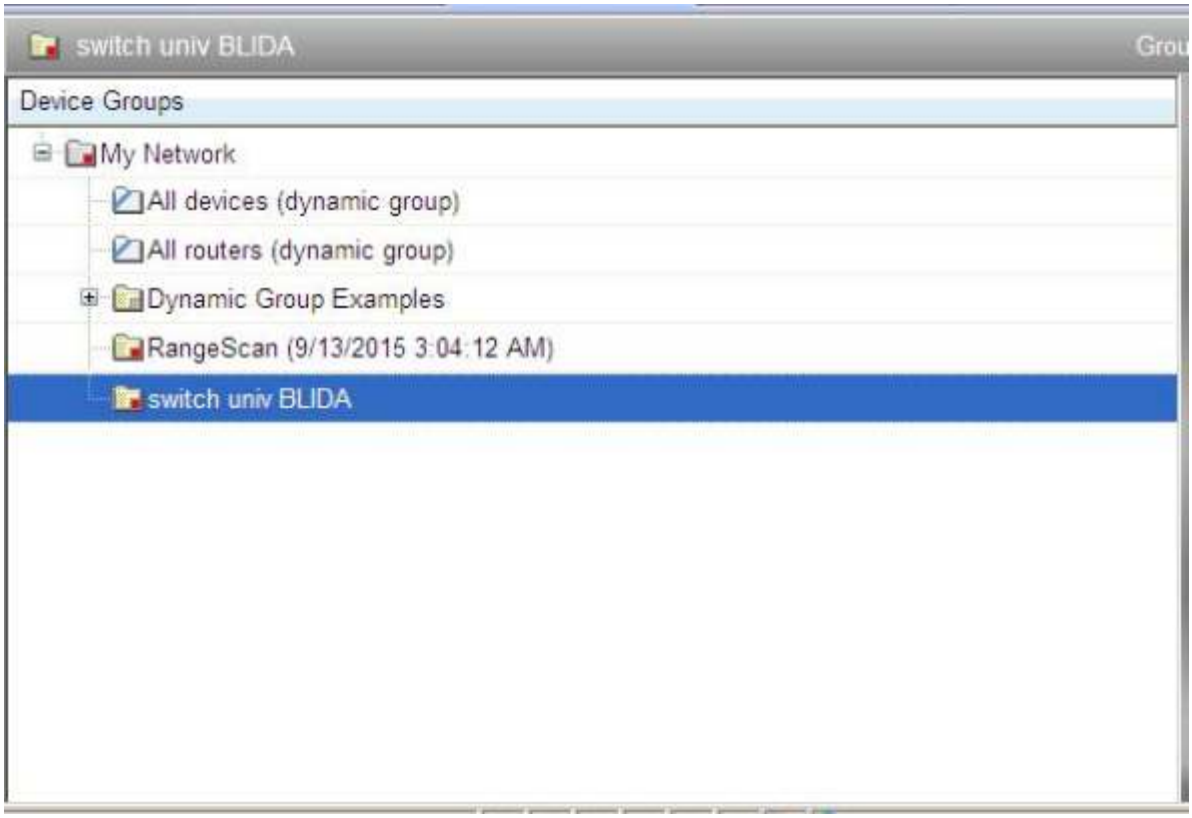


Figure IV.8 : Les Groupes des Switchs.

Etape 3 : la surveillance :

Cette étape est la plus sensible puisque elle montre les performances de chaque Switchs avec des datagrammes qui montre l'état de fonctionnement des composants Switchs à chaque Test quand a fait.

a. Tests de fonctionnalités d'équipement :

A chaque fois quand a fait les tests d'outil on a près pour chaque fonctionnalités une image d'épreuve qui sont apparaitre par la suite :

- **Graphe CPU** : Cette partie elle nous affiche la charge du CPU, c'est très utile lors d'un diagnostic de pertes ou lenteurs. Voir Figure **IV.9.**

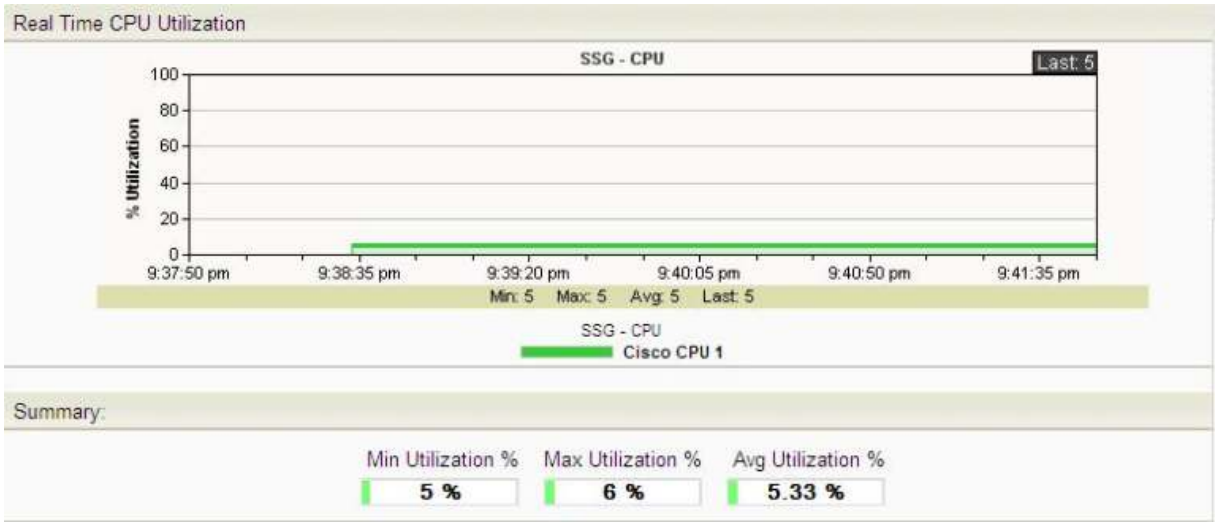


Figure IV.9 : Utilisation CPU en temps réel.

- **Graphe Ping** : un graphe qui nous illustre le temps de Ping des différentes interfaces de switch, nous peuvent le configurer afin de modifier l'affichage en cliquant sur menu voir Figure IV.10**.**

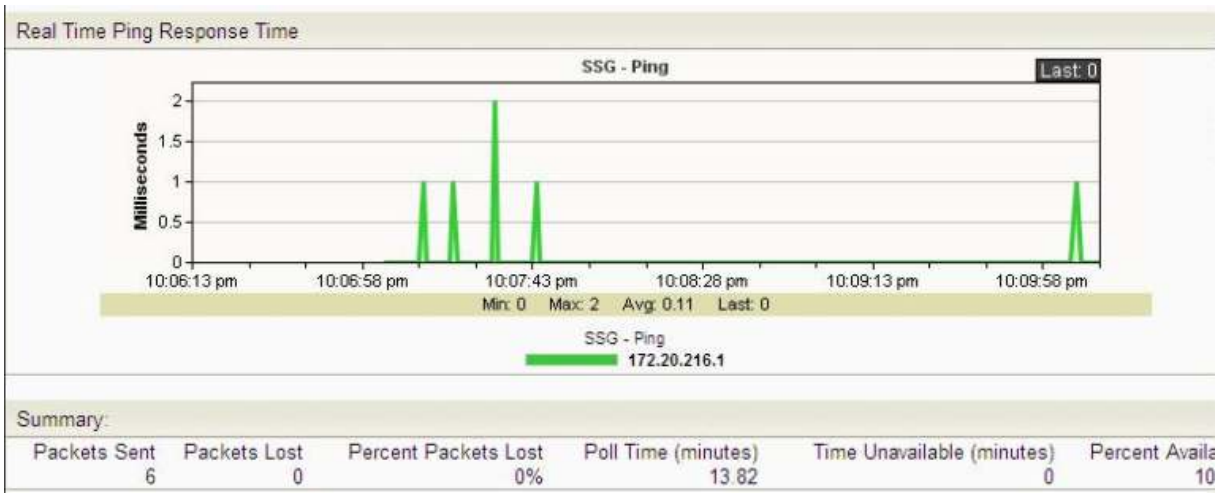


Figure IV.10 : Temps de Réponse Ping en temps réel.

- **Graphe Mémoire (Graphe Memory)** : ce graphe nous illustre en pourcentage le taux de mémoire consommée par switch en question. voir la Figure IV.11.

Figure IV.11 : Utilisation Mémoire en temps réel.

- **Etats active ou passive des interfaces (Device Active Monitor States)** :

Cette partie nous montre tous les moniteurs actifs configurés sur le Switch, ainsi que leurs états.

Nous peuvent visualiser l'un de ces éléments comme suit :

Un « moniteur actif» est un témoin booléen qui remonte le statut, soit "**UP**"montant soit "**DOWN**" descendant, de l'élément supervisé. Actif signifie que c'est le serveur qui initie la demande d'informations auprès de l'agent **SNMP**. Voir la figure suivante

Figure IV.12 : Etats des interfaces.

- **le statut du moniteur (State)** : «Up »montant ou « Down » descendant d'au moins d'x minutes. voir figure suivante :

Figure : IV.13. : Statut du moniteur.

b. Propriétés d'équipement :

On a accédé à la fenêtre des propriétés de notre équipement on entre sur'Device /Equipement/DevicePropretés'.voir figure

Cette option permet de configurer toutes les propriétés de l'équipement (Alias,Interfacesasuperviser, moniteura activer ,config SNMP ….).

La boite de dialogue suivante s'affiche contenant l'ensemble des propriétés de l'équipement, ces derniers seront montrés dans la figure suivante.

Figure : IV.14 : Propriétés d'équipement.

Etape 04 : Rapports Des Alertes :

a. Les catégories des rapports :

On distingue 03 trois catégories de rapports complets sur la base de la portée des informations affichées dans un rapport :

- **Système (system)** : ces rapports affichent des informations systèmes, ne se concentrent pas sur un dispositif particulier, ni un groupe de périphérique spécifiques.
- **Groupe (group)** : ces rapports affichent des informations relatives a un groupe de Switchs spécifiques.
- **Equipement (device)** : ces rapports affichent des informations relatives a Switch spécifique.

- **Performance** : ces rapports affichent des informations recueillies a partir des moniteurs de performances concernant nos Switch (CPU, disque, interface, utilisation de la mémoire, la latence du Ping de la disponibilité).
- **Problèmes zones (Problem Areas)** : ce sont des rapports de dépannage qui nous permettent d'enquêter sur le réseau.
- **Générale (General)** : ces rapports affichent des informations sur nos paramètres et diagnostics d'**Ipswich (WhatsUpGold)**, ainsi que les détails spécifiques au Switch configuré par l'utilisateur.

On peut utiliser la page de présentation des rapports et la catégorie dans le menu déroulant pour accéder à des rapports en fonction de leur catégorie. (Figure : IV.15 et Figure : IV.16).

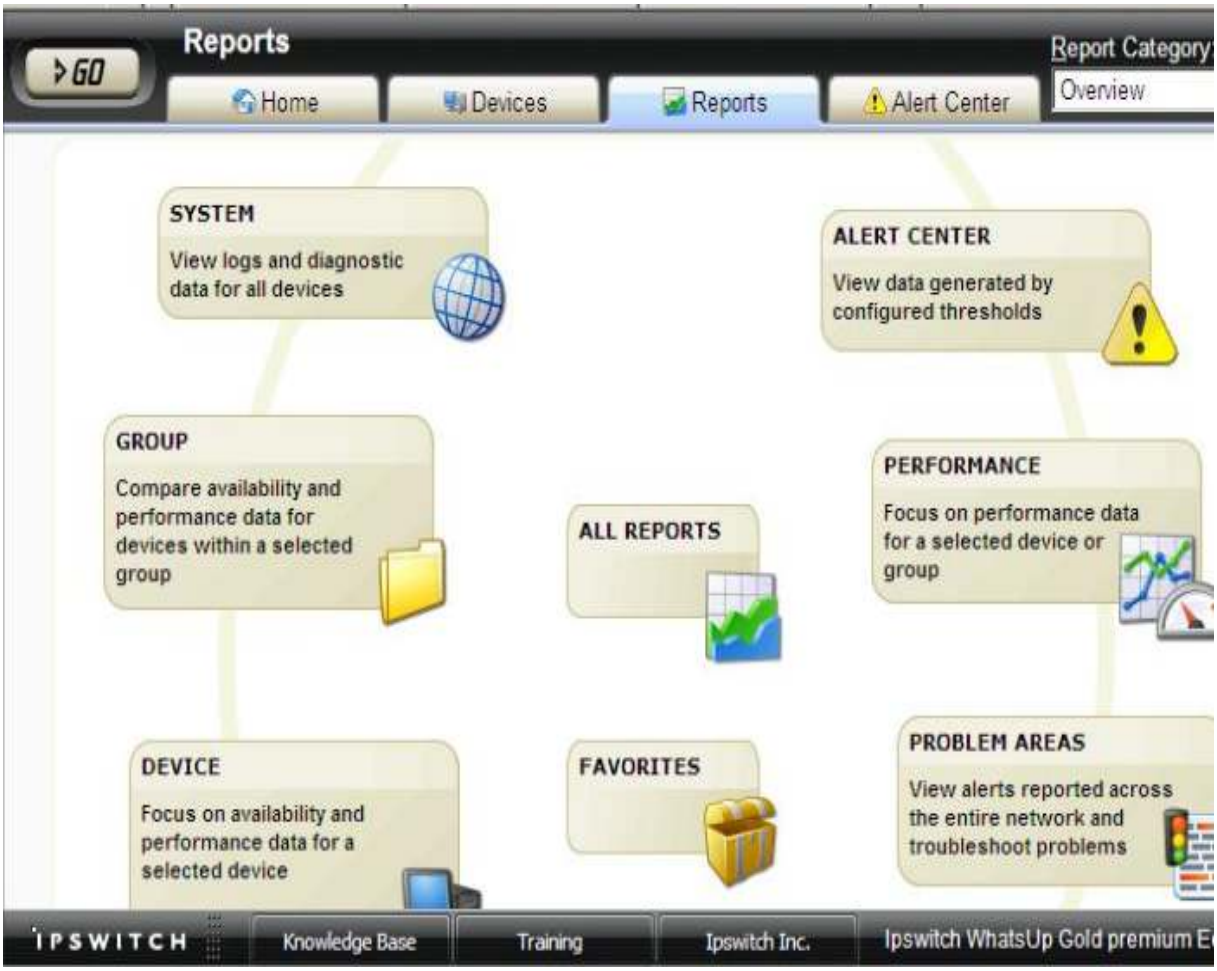


Figure : IV.15 : Catégories des Rapports.

b. Détails des rapports de Switch :

Sur la page regroupant les informations primaires d'un équipement donné, on trouve une barre déroulante intitulée « More Device Reports ».

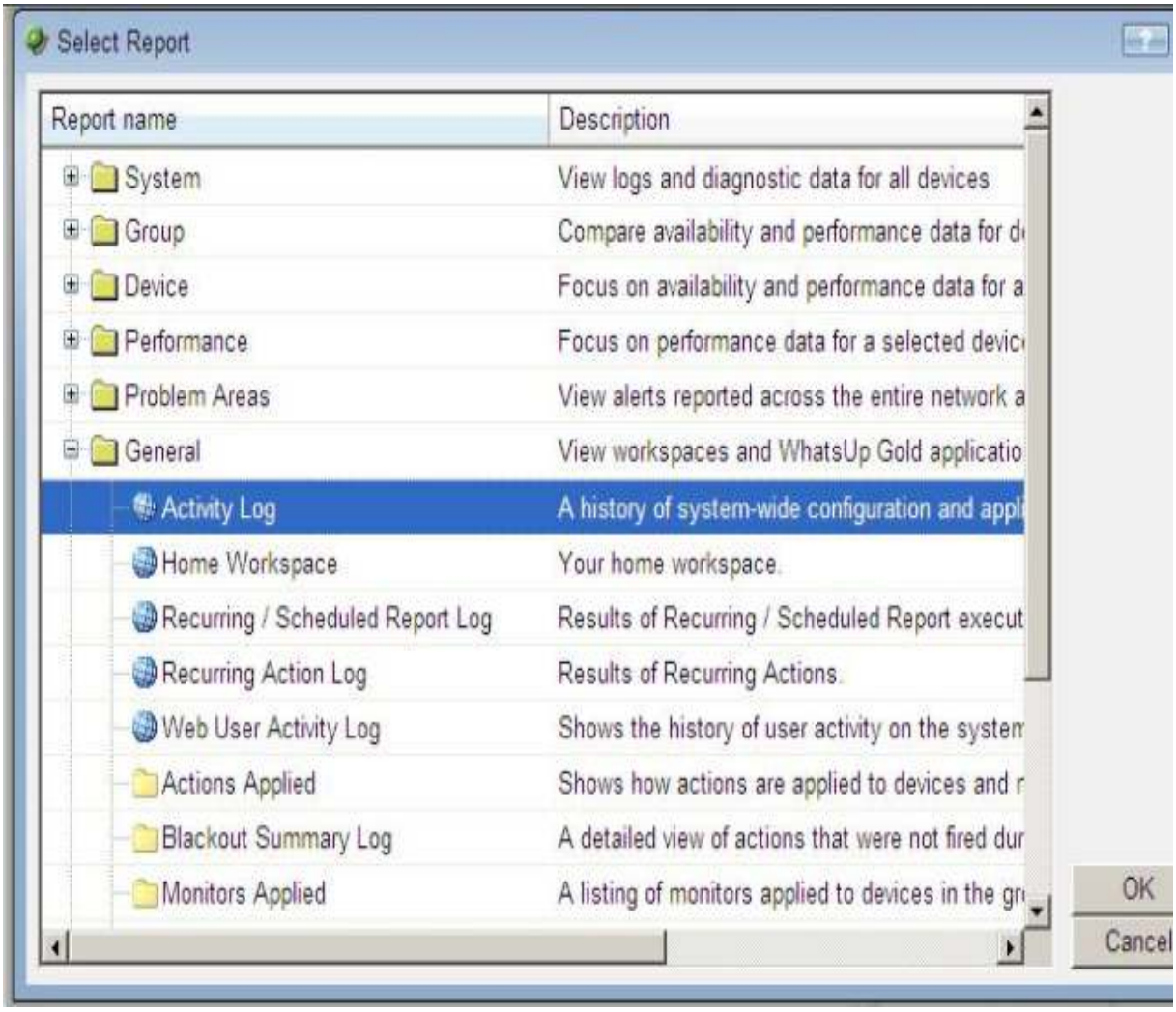


Figure IV.16 : Les Rapports en fonction de leur catégorie.

Ce menu déroulant nous permet de basculer entre les déférents moniteurs actifs sur l'équipement, que ça soit moniteur actif, passif ou moniteur de performance.

Un « moniteur passif » permet de collecter et récupérer les Traps et Logs générés par l'équipement. C'est ce dernier qui initie ce type communication.

c. Détails des Alertes des Switchs :

Pendant une période du temps bien précis on a près les états des différents changements des moniteurs, leurs statuts, et les messages générés. La figure suivante montre les différentes variations

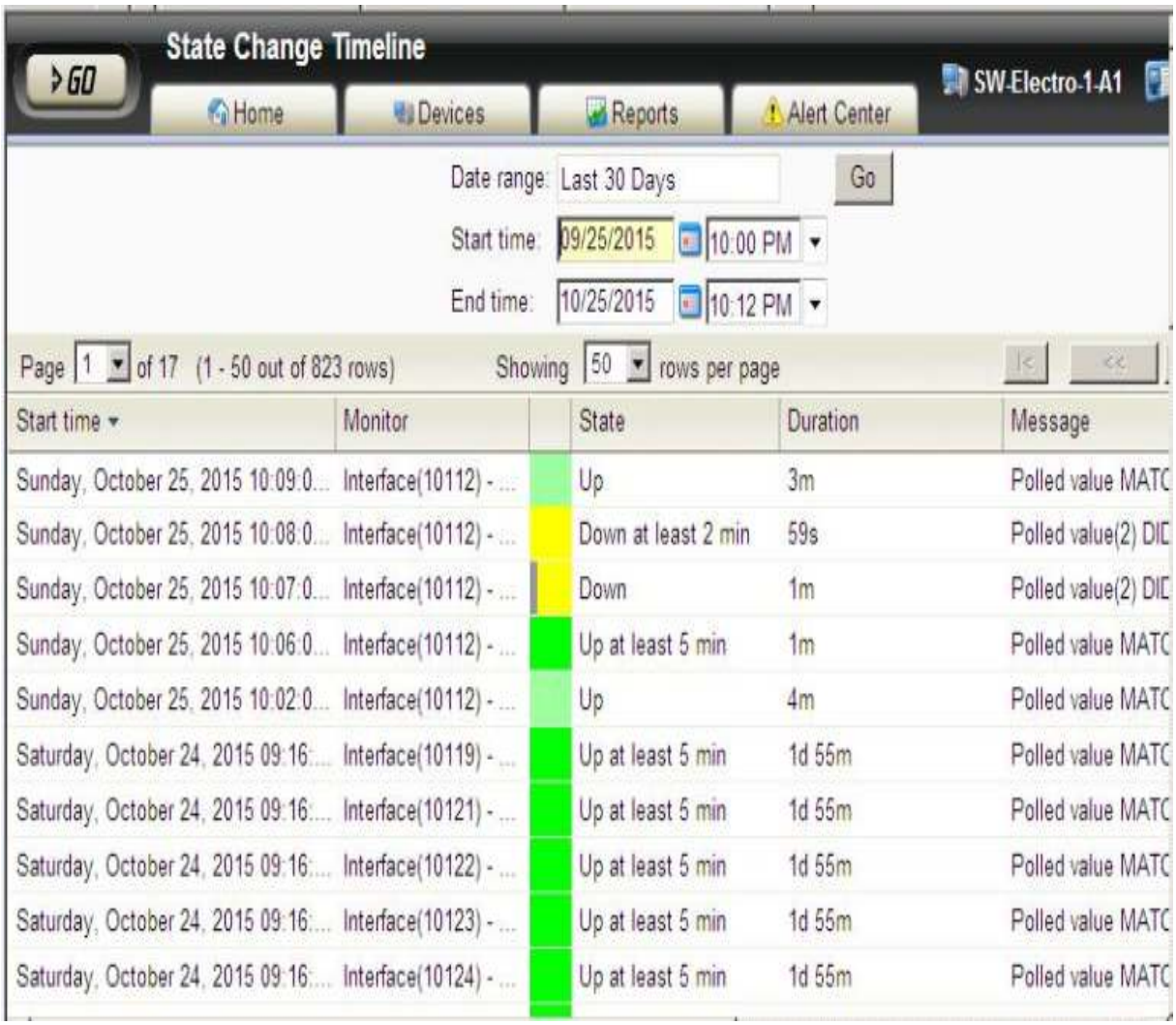


Figure : IV.17 : Changement d'états des Switchs dans une période.

Enfin notre objectif des essais et les tests quand a fait déjà sur les déférentes fonctionnalités de cet outil est une évaluation de leur performance et puissance de la gestion de notre réseau elle était fait avec succès.

IV.4. Conclusion :

Ipswich (WhatsUpGold) fournit une gestion informatique complète pour les réseaux filaires et sans fils les systèmes et les applications avec pour but de renforcer la puissance de notre réseau. Avec **Ipswich (WhatsUpGold)** nos tâches de gestion fréquentes, telles que la détection et la cartographie de couches **2** et **3**, sont complètement automatisé. La gestion intégrée de rapport sur l'inventaire et les ressources informatiques gère des données détails sur la configuration des périphériques, ainsi que des informations actualisé de mise en conformité/d'audit. De plus, nos rapports de surveillances et de performances en temps réel nous permettent en tout simplicité de maintenir une santé et une efficacité optimales sur l'ensemble de notre infrastructure. Tout ceci est prêt à l'emploi au sein d'une seule application.

Dans ce chapitre nous avons constater que le **Ipswich (WhatsUpGold)** est un outil très performant d'administrer un réseau. Avec leurs fonctionnalités, la supervision d'état des équipements réseaux sera représentée dans des rapports qui sont bien détaillés.

Bibliographie :

[1]Danièl DROMARD et Nominique SERET « Architecture_des_réseaux », Editions PEARSON

[2] Philipe Atelin « Réseaux informatiques notions fondamentales » , troisième édition édition ENI

[3] http//watonur blogspot.com/2012/08/les-types-de-réseaux.html

[4] http//www.pasteur.fr/formation/infobio/arch/archi-réseaux.pdf

[5]http://COURS-ARCHITECTURE-DES-RESEAU-INFORMATIQUE.htm

[6]cours Cisco CCNA1 version 5

[7] http://www.intedoc.net/articles/modelisation/modelisation.tcpip.html

[8] RFC 0791.S.J.Postel, “Internet Protocol”, 09/01/1981

[9] http://ip.gaulier.info/gulliver/reseau.pdf

[10] http://www.laissus.fr/pub/cours/cours.pdf

[11] David Imanache – Niolas Joubert – Olivier Mayoud livre informatique & Réseaux-3

[12] André VAUCAMPS, « CISCO notion de bases sur les réseaux », Edition ENI, Mai 2009

[13] site WEB **www.ipswitch.com/www.cisco.com**

[14] site WEB **www.WhatsUpGold.com**