MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU.

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

Présenté en vue de l'obtention

du Diplôme d'ingénieur d'état en électronique

Option : Communication.

Thème :

Services d'accélération des applications et optimisation des liens WAN (WAAS : Wide Area Application services) au niveau de la CNAS d'Alger.

Proposé et encadré par :

Mr. AKKA Abdelhakim

Dirigé par :

Mr. LAGHROUCHE Mourad

Présenté par :

Mlle .BELAID Nassima

Mlle. ARKOUB Chabha

Année universitaire 2010/2011

Résumé

Cisco WAAS (Wide area application services) est une nouvelle solution attractive d'accélération des applications et d'optimisations du WAN pour les sites distants, qui améliore les performances de toutes les applications basées sur TCP circulant sur un réseau étendu (WAN). Avec Cisco WAAS, les entreprises peuvent consolider les serveurs couteux et les éléments de stockage distants à l'intérieur des Datacenter centraux, tout en continuant d'offrir un niveau de service similaire au LAN pour les utilisateurs distants. Ce projet a été réalisé en deux étapes. La première étape, consiste à réaliser une étude théorique sur technologie WAAS à savoir compression, accélération …ainsi que l'état d'avancement de cette technologie. Dans la deuxième étape, Nous avons procédé à une implémentation de WAAS entre trois sites : le site central, un site distant et un centre payeur.

Abstract

Cisco WAAS (Wide Area Application Services) is a new attractive solution for application acceleration and WAN optimization for remote sites, which improves performance of all TCP-based applications running over a wide area network (WAN). With Cisco WAAS, enterprises can consolidate costly servers and remote storage elements within the central data center, while continuing to offer a similar level of service to LAN for remote users. This project was conducted in two stages. The first step is to conduct a theoretical study on WAAS namely compression, acceleration .... and the status of this technology. In the second step, we conducted an implementation of WAAS from three sites: the central site, a remote site and a payment center.

Sommaire

Sommaire :

Chapitre III : Optimisation des applications WAAS

Chapitre IV : Administration WAAS

Liste des figures :

Organisme d'accueil

Chapitre I

Chapitre II

Chapitre III :

Chapitre IV :

Liste des tables :

Chapitre I :

Chapitre II :

Chapitre IV :

Introduction générale

La solution Cisco WAAS (Wide Area Application Services) est une nouvelle technologie puissante d'accélération WAN qui permet l'optimisation des applications basées sur TCP transitant vers le WAN elle permet de fournir des performances équivalentes à des réseaux LAN pour les sites distants et de réduire au minimum l'effet de la latence et le temps de réponse ainsi que le transfert inutile d'objet a travers le WAN .Elle fait appelle à des techniques d'accélération et d'optimisation du WAN les plus avancées, incluant la compression, l'élimination des données redondantes. Chacune de ces techniques est conçue pour surmonter les limitations dues à la bande passante, le débit, et à la latence caractérisant les liens WAN.

L'Intégration de la solution WAAS est transparente et assure un déploiement aisé des boitiers a travers l'auto-découverte dynamique sans la nécessité de créer et d'administrer des réseaux supplémentaires , ainsi la visibilité de bout en bout et la comptabilité des données (pas de tunneling) sont fournis dans l'infrastructure existante, comme la QOS, la sécurité est assurée par les Firewalls, le monitoring, et la haute disponibilité , elle ne nécessite pas l'installation d'un logiciel sur le serveur ou sur le client, et de ce fait , ne demande pas à l'utilisateur de se former sur un nouveau produit. Les utilisateurs bénéficient d'un data center sécurisé sans changer le moins du monde leurs habitudes de travail, cette solution offre Une infrastructure unitaire allégée appliquant des couts de gestion nettement réduit .elle peut soutenir jusqu'à quatre millions de connections TCP et offre des largeurs de bande passante pouvant atteindre 16 Mo par seconde.

La société CNAS nous a proposé un travail dans le cadre d'un projet de fin d'étude intitulé : « La mise en place de la technologie WAAS entre deux réseaux WAN» qui sert à déployer la technologie WAAS entre le site central d'Alger situé à Ben Aknoun, le centre de calcule et le Centre payeur situés a Tizi-Ouzou.

Dans ce cadre, nous avons organisé notre projet de fin d'études comme suit :

- Nous allons commencer à présenter l'organisme d'accueil CNAS ainsi que son réseau étendu et l'emplacement de notre application.
- Dans le premier chapitre, nous allons introduire la notion de réseau, expliquer son fonctionnement et donner une brève présentation du modèle TCP/IP.
- Dans le deuxième chapitre, nous allons approfondir nos connaissances sur les réseaux étendu et en présentant l'interface utilisateur d'un routeur, les commandes et les

différentes manières de le configurer.

- Dans le troisième chapitre, nous avons traité les fonctionnalités de WAAS en expliquant les différents protocoles d'optimisation et de compression.
- Dans le quatrième chapitre nous avons introduit le centrale manager ainsi que la mise en œuvre de la solution WAAS.

Présentation de l'organisme d'accueil

La caisse nationale des assurances sociales des travailleurs salariés, par abréviation « CNAS » est un établissement public à caractère administratif, doté de personnalité morale et de l'autonomie financière, régi par les lois et les règles en vigueur.

La CNAS est placée sous la tutelle du ministère de la sécurité sociale, le siège de la caisse est fixe à Alger.

Dans chaque wilaya, la CNAS dispose d'une structure dénommée "agence de wilaya" fonctionnant comme annexe de la caisse nationale concernée.

D'autres annexes peuvent être crées, par arrêté conjoint du ministre tutelle et du ministre charge des finances, sous la dénomination de centre de commue, ou d'antenne d'entreprise ou d'administration.

1. Structure de la CNAS :

La CNAS est définie comme suit :

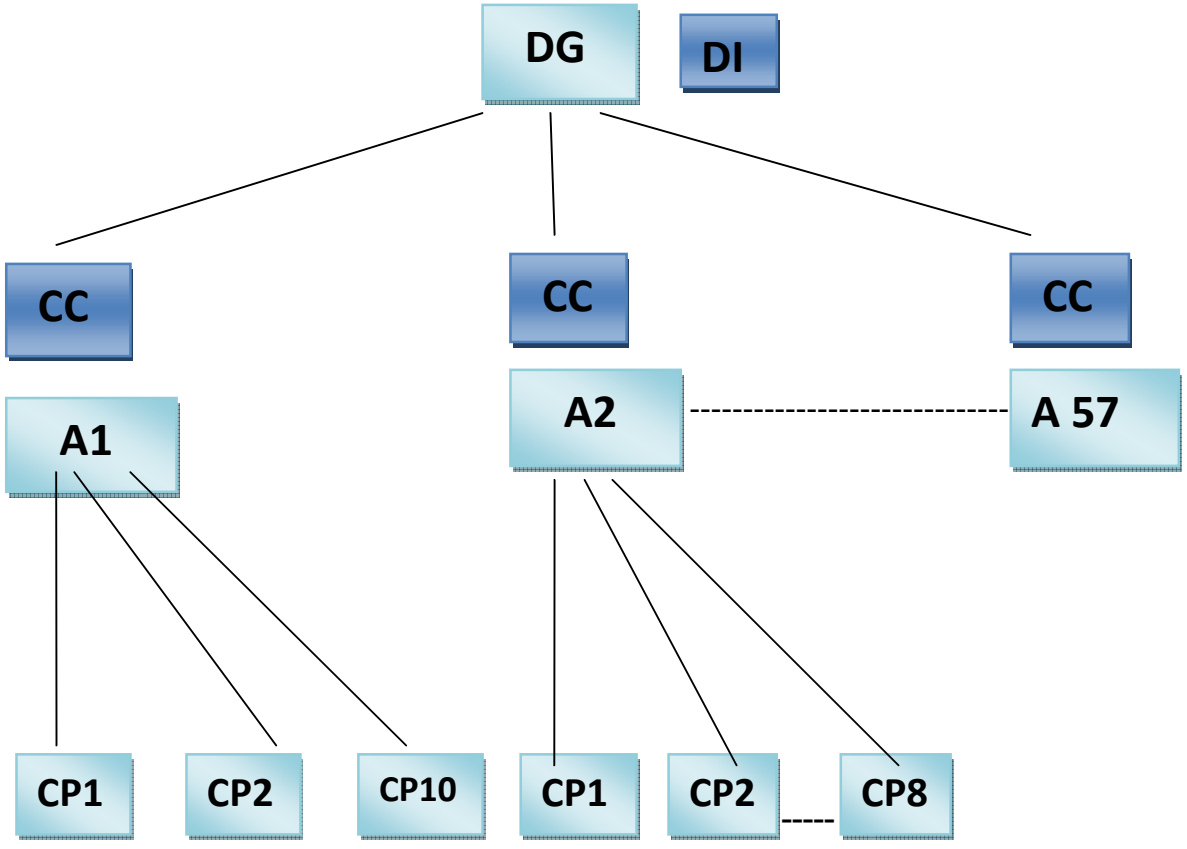


Fig1: structure CNAS

DG : direction générale

DI : direction informatique

CC : centre de calcul

A : agence

CP : centre payeur

1.1 La direction générale :

La direction générale se situe à Ben-Aknoun, son rôle est de gérer toutes les informations provenant des directions centrales à travers les wilayas vers Alger.

La direction générale est représentée par des agences locales auxquelles sont rattachées plusieurs structures (centre payeur et antenne).

1.2 La direction informatique :

Il se trouve une seule direction informatique qui est rattachée à la direction générale. Son rôle est d'établir les différents programmes utilisés dans les structures de la CNAS et d'assurer la maintenance.

1.3 Les agences :

Le rôle de l'agence est de coordonner et contrôler les activités des centres payeurs et des antennes d'entreprise et le cas échéant, des antennes d'administration. On en trouve dans chaque wilaya à l'exception de la wilaya d'Alger. Les agences sont subdivisées en plusieurs sous directions dont les plus importantes sont :

- Sous direction de prestation :

  Elle contient trois services :

  - Service des rentes.
  - Service des allocations.
  - Service des assures.

- Sous direction de recouvrement :

  Elle contient trois services :

  - Service immatriculation employeur.
  - Service immatriculation assurée.
  - Service cotisation.

1.4 Centre de calcul :

Le centre de calcul est chargé de l'exploitation et de la saisie des données ainsi que de l'édition, de l'immatriculation, des allocations familiales, de la comptabilité, des mutations des assurés….etc.

Le centre de calcul fait partie de l'agence, et chaque agence à un centre de calcul sauf dans les wilayas dont le taux de population est très fiable, son travail se fait par d'autres centres de calcul.

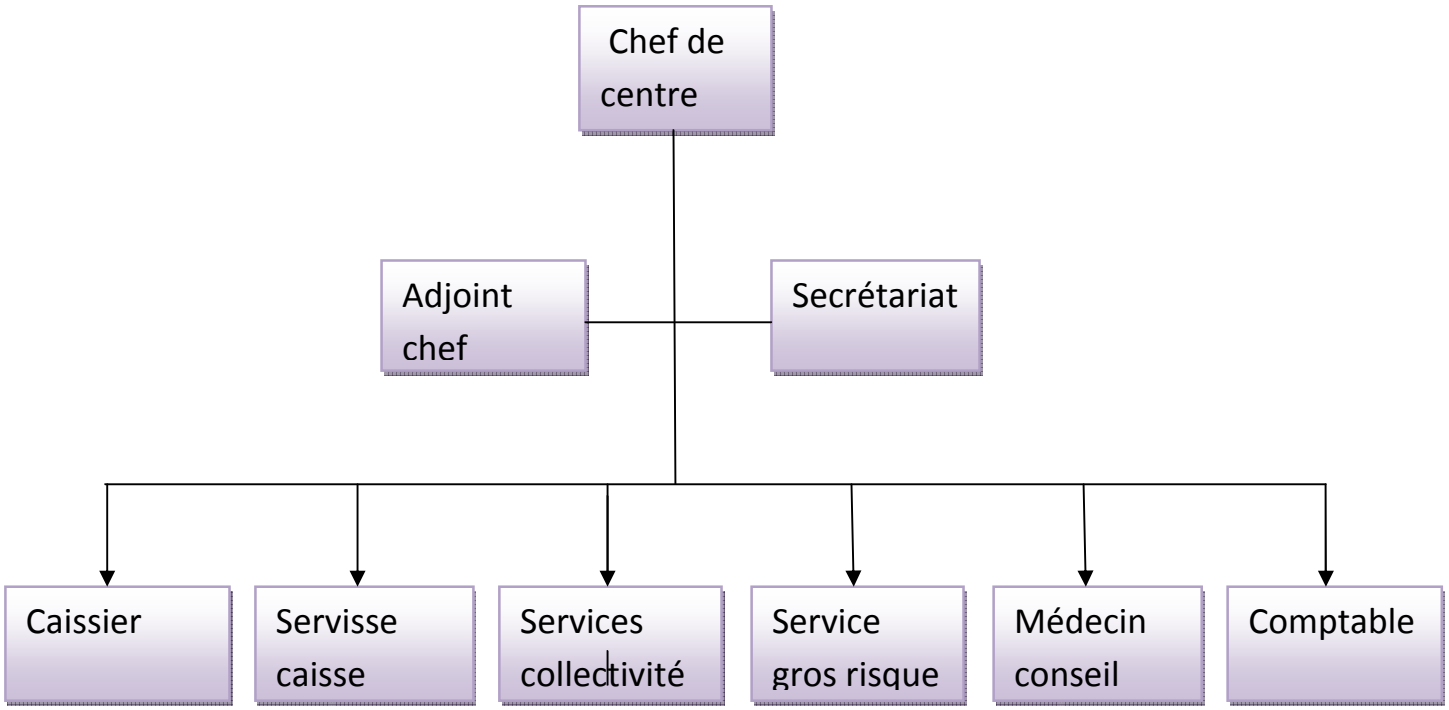


Fig2: Hiérarchie centre payeur

2. Le réseau CNAS :

Le réseau étendu «CNAS» est composé de plusieurs réseaux résidant dans les régions à plus forte densité démographique d'Algérie et de façon à ouvrir tout le territoire national.

Notre application a pour rôle de mettre en place la solution WAAS entre la direction informatique sise à Ben Aknoun et l'agence CNAS de Tizi Ouzou pour améliorer les performances des applications au niveau distant.

Le schéma qui suit montre en détail la structure du réseau étendu CNAS ainsi que la place de notre application dans ce réseau :

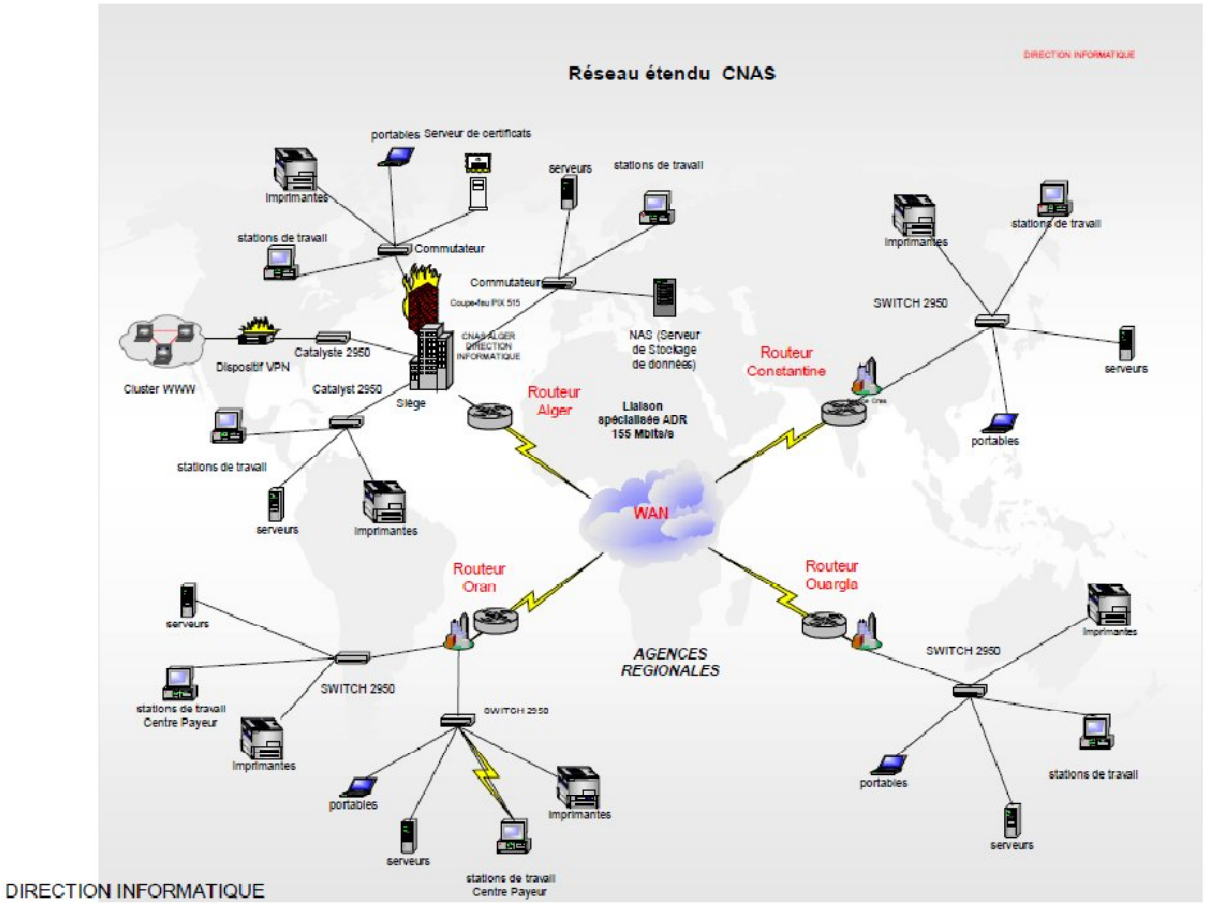


Fig3 : Réseau étendu CNAS

Conclusion

Nous avons présenté de manière très brève l'organisme d'accueil «CNAS» ainsi que représenté schématiquement son réseau étendu (WAN) et le rôle qu'aura notre application dans l'entreprise.

Chapitre 1 :

Généralité sur Les_réseaux informatiques

Le réseau informatique et défini comme étant un ensemble d'ordinateurs appelé aussi entité complexe (nœud), ensemble de moyens matériels et logiciels géographiquement dispersés, relié entre eux grâce à des lignes physiques destinées à véhiculer et transporter sous forme de données numériques.

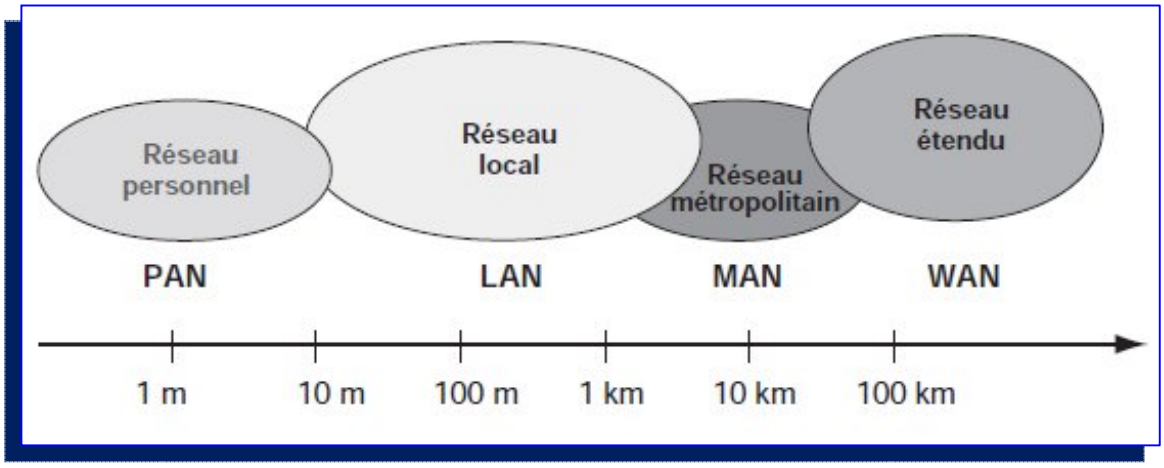
I.1-Définition d'un réseau :

Le réseau, dans son acceptation traditionnelle, est assimilé à une structure de transport qui offre la possibilité de réguler des flux de communications, ou des échanges de biens.

Un réseau est un ensemble d'entités interconnectées les unes les autres, et donc permet de faire circuler des données entre chacune de ces entités, et selon des lois bien définies.

I.2-Classification des réseaux :

Cette classification est fondée sur la notion d'étendue géographique entre systèmes informatique.



I.2.1-LAN: (Local Area Network).

Ce sont des réseaux locaux d'étendue limitée. C'est des réseaux intra-entreprises destinés à l'échange de données et ou partage locale de ressources informatique.

I.2.2-MAN: (Métropolitain Area Network).

C'est des réseaux d'étendus de l'ordre de quelques kilomètres, utilisés pour fédérer plusieurs sites équipés d'un réseau local (réseau de campus).

I.2.3-WAN: (Wide Area Network).

C'est des réseaux très étendus, qui assurent le transport des informations sur de grandes distances entre plusieurs villes et l'interconnexion de réseaux d'une même entreprise.

I.2.4-Sans fil:

Les ordinateurs mobiles ou les assistants personnels (palm pilot) constituent le secteur informatique en plus forte progression, beaucoup de possesseurs de ce type d'ordinateurs ont également un ordinateur relié à des WAN ou des LAN, chez eux ou au bureau auxquels ils souhaitent être reliés à tout moment.

I.3-Topologie physique des réseaux :

Il y a trois types de topologie:

I.3.1-Topologie en bus :

Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En, bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.
L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile à mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles

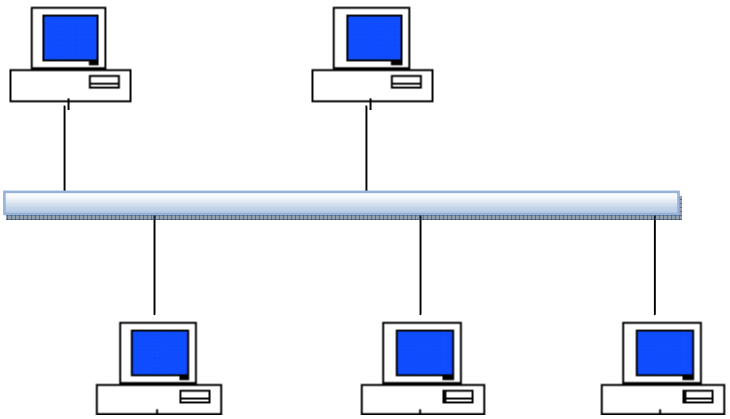


Fig I.1 : Topologie en bus

I.3.2-Topologie en étoile :

C'est la topologie la plus courante, notamment avec les réseaux Ethernet RJ45. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub) ou uniquement au destinataire (Switch).

Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies.

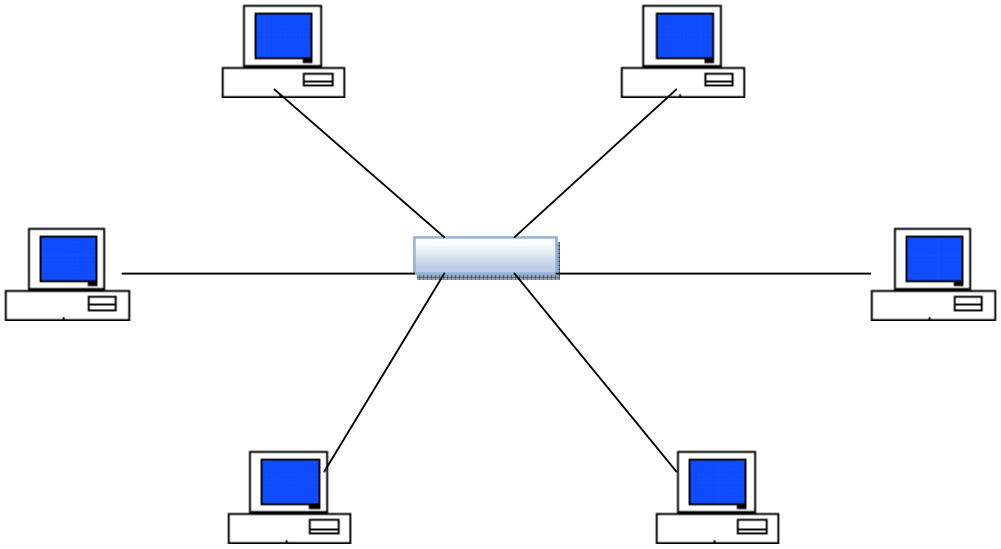


Fig I.2 : topologie en étoile

I.3.3-Topologie en anneau :

Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring.

Token Ring utilise la technique d'accès par « jeton ». Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…

Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable. L'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre.

Enfin, cette architecture étant la propriété d'IBM, les prix sont élevés et la concurrence quasiment inexistante.

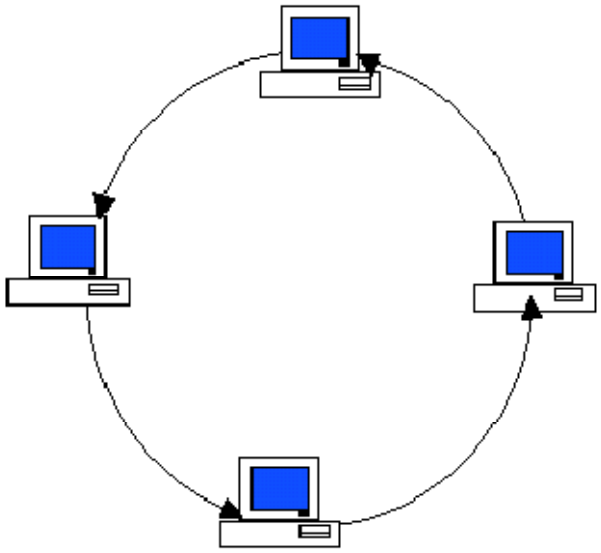


Fig I.3 : topologie en anneau

I.3.4-Topologie Arborescente :

C'est une structure arborescente hiérarchisée. Un réseau arborescent est formé d'un ensemble de réseaux en étoile reliés entre eux par des concentrateurs jusqu'à un nœud unique central. Cette structure est très utilisée dans les réseaux locaux.

I.3.5-Topologie maillée

Pour des raisons de défaillances, le réseau est maillé où chaque nœud est caractérisé par sa connectivité, c'est-à-dire que pour accéder à un même nœud, il existe plusieurs chemins, cette structure optimisé emploi des ressources en répartissant la charge entre les différentes voies.

I.4-Modèle en couche et paquet :

Le principe de modèle en couche est de découper le travail en tâche élémentaires. Ainsi chaque étape d'un processus permet de rajouter, une information, un contrôle, un service, qui n'était pas dans la couche précédente.

Chaque couche a la possibilité de communiquer seulement avec deux autres couches, celle qui la précède est celle qui la suit. Cette communication se fait par l'intermédiaire d'interface. Si l'on prend l'exemple d'une chaîne de production, chaque maillon de cette chaîne reçoit une pièce du maillon précédent, va ensuite faire une opération sur la pièce (comme la tester, lui

greffer une autre pièce…) et une fois cette opération terminée, la nouvelle pièce sera transmise au maillon suivant.

Il est à ce moment important de comprendre qu'une couche ne voit que ses voisines, et donc ; l'ensemble du modèle est complètement invisible à cette couche, chacune des couche n'a pas besoin de savoir comment les couches supérieurs ou inférieurs fonctionnent : elle a juste besoin de savoir comment leur transmettre des données.

C'est l'une des raisons qui rend les modèles en couches ainsi populaires, car si le modèle est bien fait, l'impact changement de technologie sur l'ensemble des protocoles ne posera aucun problème.

Dans une communication à travers le réseau, deux machines sont impliquées : l'Emetteur et le Récepteur. Chacune de ces machines implémente un modèle en couche. Le principe est que chaque couche sur une machine communique avec son homologue.

Lorsqu'il s'agit d'une émission sur le réseau, les données sont transmises vers le bas du modèle, et vers le haut lorsqu'il s'agit d'une réception de données. Chaque couche ajoute certaines informations de contrôle appelées en-tête pour la bonne livraison des données. Les informations sont encapsulées, car une couche considère que toutes les informations reçues d'une autre couche voisine comme étant des données et place sa propre en-tête.

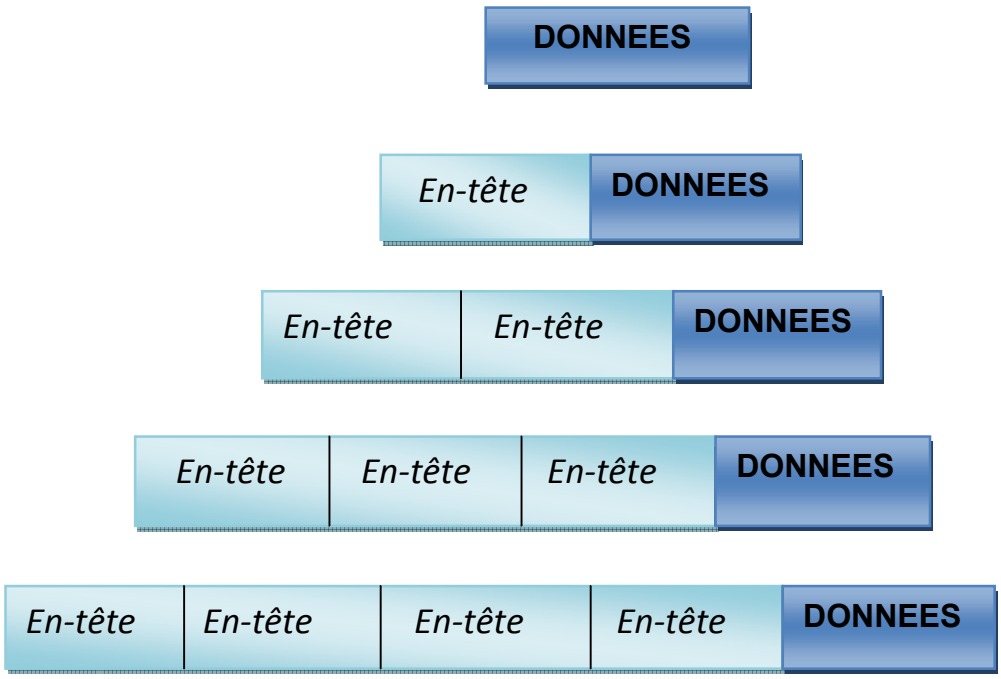
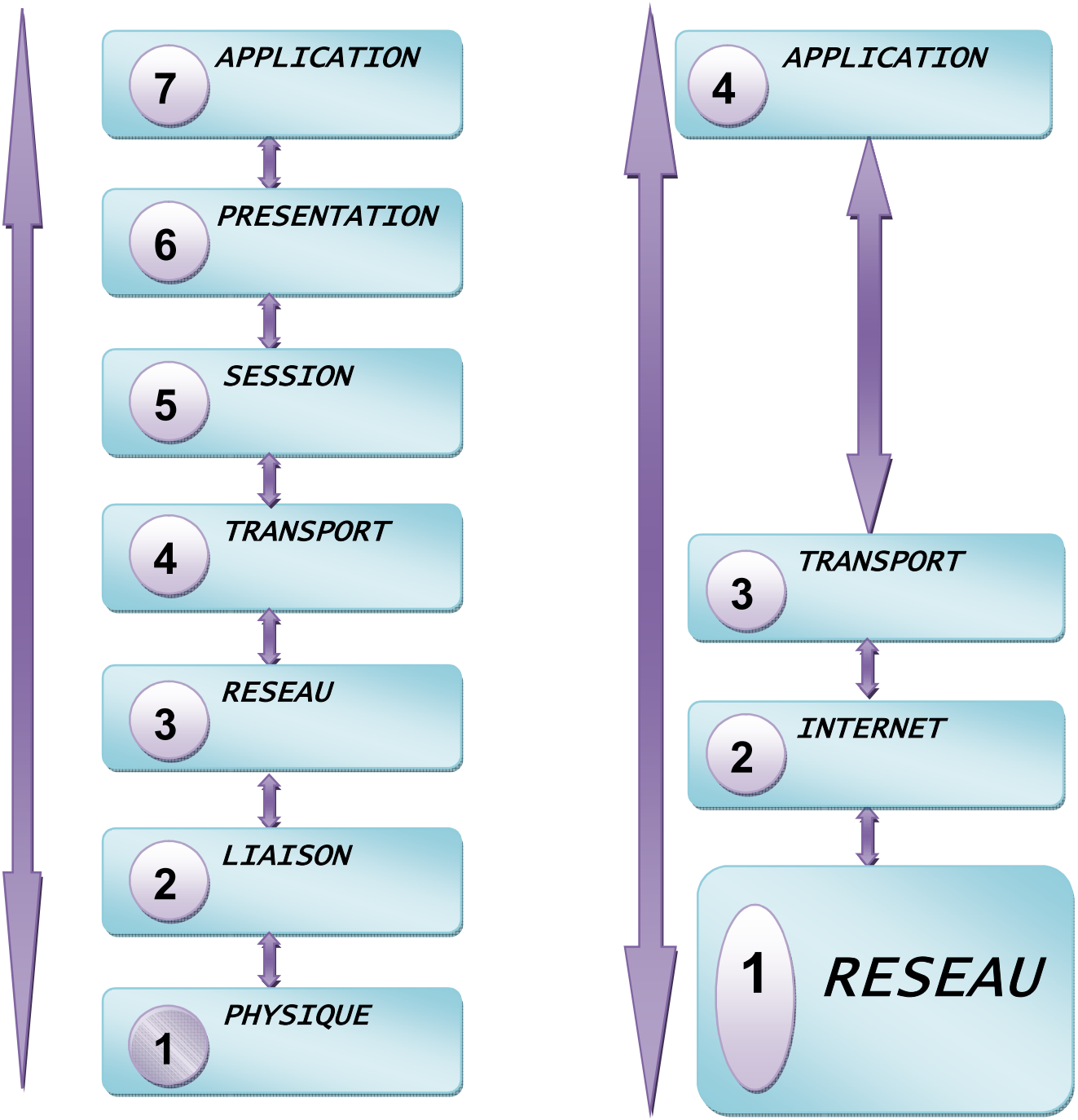


Fig I.4 : Encapsulation de données

Il existe deux modèles en couche majeurs **ISO** et TCP/IP. Le premier est théorique et le seconde pratique. Ils sont représentés par le schéma suivant :



Modèle TCP/IP **Modèle OSI**

Fig I.5 : Architecture des modèles OSI et TCP/IP

Le schéma ci-dessus représente les différentes couches dont est composé chaque modèle nous abordons dans la section suivante le modèle TCP/IP pour mieux assimiler le fonctionnement des routeurs en introduisant les notions d'adressages et de routages.

I.5-Le modèle TCP/IP :

TCP/IP (Transmission Control Protocole / Internet Protocole) est un ensemble de protocoles organisés en couches. Le terme "TCP/IP" fait référence à toute une panoplie de protocoles de communication et tire son nom de deux protocoles, les plus importants faisant partie de cet ensemble.

Il offre une méthode pour transférer des informations d'une machine à une autre.TCP/IP est un protocole de communication qui traite les erreurs survenant lors de la transmission, gère le routage et la livraison des données et contrôle la transmission elle-même. Ce protocole suppose donc l'existence d'un lien fiable entre les deux ordinateurs.

I.5.1-Couche application :

Au sommet et au plus haut niveau de l'architecture des protocoles TCP/IP, se trouve la couche application. Cette couche fournit tous les processus utilisant les protocoles de la couche transport pour véhiculer leurs données. Il existe plusieurs protocoles d'applications qui fournissent des services à l'utilisateur et dont le nombre ne cesse d'augmenter.

Les protocoles d'application les plus connus et fréquents sont :

- **Tel net :** (Network Terminal Protocol).
- **FTP :** (File Transfer Protocol).
- **SMTP :** (Simple Mail Transfert Protocol).
- **http :** (hyper Texte Transfert Protocol).

I.5.2-La couche transport :

La couche transport du modèle TCP/IP est l'étape du processus de communication pendant laquelle les données seront regroupées en segments de données et ordonnés pour livraison par les standards de transport des données. Par exemple : TCP/IP et UDP.

- **UDP :** (User Datagram Protocol)

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la

transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

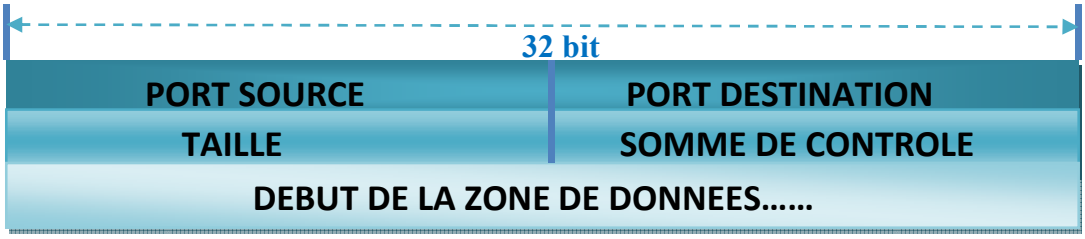


Fig I.6 : Format de message UDP.

- **TCP :** (Transmission Control Protocol)

Le Protocole TCP est crée dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs raccordés à un réseau (protocole orienté connexion).

TCP est fiable grâce à un mécanisme appelé «accusé ou acquittement de bonne réception avec retransmission». Cela signifie qu'un récepteur doit répondre à un émetteur en lui confirmant que les données ont bien été reçues. Si l'émetteur ne reçoit pas d'acquittement, il se charge de réémettre les données jusqu'à ce qu'il reçoit un message de la machine distante signifiant que les données sont bien arrivées.

L'unité de donnée échangée entre deux entités TCP coopérants est appelée ***segment.*** Dans chaque segment il y'a une somme de contrôle «***Checksum***» utilisée par le récepteur qui envoi à l'émetteur un accusé de réception positif pour s'assurer que les données sont bien arrivées. Si les données sont endommagées le récepteur n'en tient pas compte et détruit le segment.

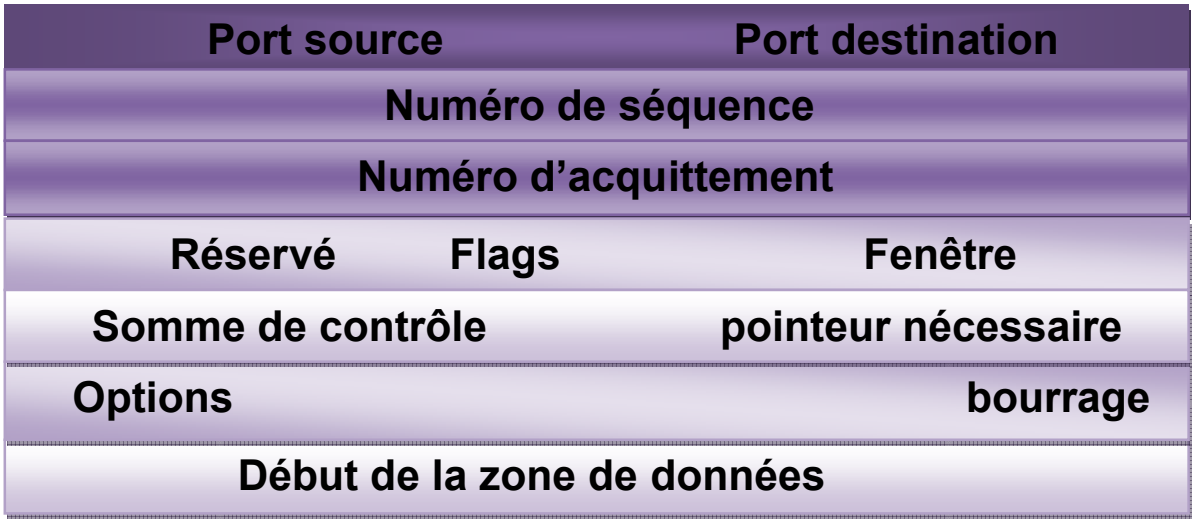


Fig I.7 : Format de segment TCP.

La description des champs est la suivante :

- **Numéro de séquence** : sur 32 bits, il est initialisé lors de la connexion et identifie l'ordre des segments transmis. Si le bit SYN est positionné il représente le numéro de séquence initial (le premier octet a pour numéro ISN+1), sinon il représente le numéro du premier octet par rapport au début de la transmission.

- **Accusé de réception** : sur 32 bits, si le bit ACK est positionné il est égal au numéro de séquence du prochain octet attendu.

- **Longueur d'entête** : sur 4 bits, c'est la taille de l'en-tête TCP exprimée en multiple 32 bits. Elle indique là ou commence les données.

- **Réservé** : 6 bits réservés pour usage futur. Initialisé à 0.

- **Bits de contrôle**: 6 bits (de gauche à droite) dont les significations sont données ci-dessous.
  . URG: Pointeur de données urgentes significatif.
  . ACK: Accusé de réception significatif.
  . PSH: Fonction Push.
  . RST: Réinitialisation de la connexion.
  . SYN: Synchronisation des numéros de séquence.
  . FIN: Fin de transmission.

- **Fenêtre** : sur 16 bits, c'est le nombre d'octets que la machine distante peut recevoir. Elle est relative à la position marquée dans l'accusé de réception.

- **Checksum** : sur 16 bits, il prend en compte les adresses IP émetteur et destinataire.

- **Pointeur de données urgentes** : sur 16 bits, si le bit URG est positionné il fournit la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence.

- **Options** : variable. Ce champ sert en particulier à échanger la taille maximale d'un segment. Cette taille est classiquement calculée pour que la longueur d'un datagramme corresponde au MTU du réseau (bourrage).

La quantité de données à transmettre est souvent trop volumineuse pour être envoyée dans un seul segment de données. Dans ce cas les données doivent êtres divisées en segments plus petits pour permettre une meilleure transmission.

TCP est responsable de la répartition de ces données en segments. De plus l'unité réceptrice peut ne pas être capable de recevoir les données aussi rapidement que la source les envoie, car elle peut être occupée par d'autres activités ou simplement parce que l'émetteur est plus rapide.

TCP établit une connexion entre l'émetteur et le récepteur pour dialoguer certaines informations de contrôle avant la transmission des données. La fonction de contrôle est matérialisée par le positionnement du bit approprié dans le champ flag du quatrième mot de l'en-tête du segment.

Pour l'établissement d'une connexion TCP, émetteur et récepteur déroulent un processus appelé initialisation en trois voyages (Three-Way-Hand-Shake) car trois segment sont échangés. Ce processus certifie, avant toute émission de données, que la machine distante est active, pour initier la communication, l'émetteur envoi un segment SYN dans le quel le bit SYN (Synchronisation des numéros de séquences «Synchronize sequence numbers» est positionné à la machine distante pour l'aviser de son intention de communiquer et établir une connexion, et l'informe du numéro de séquence à partir du quel débutera la numérotation des segments. Ces numérotations servent à garantir l'ordonnancement correct des paquets à l'arrivée. Le récepteur répond en envoyant un segment qui accuse la réception du segment émis par l'émetteur, et avise ce dernier du numéro de séquence initial utilisé, et dont les bits SYN et ACK sont positionnés. Enfin l'émetteur envoie un segment pour acquitter l'information reçue du récepteur et commence à transférer les données réelles.

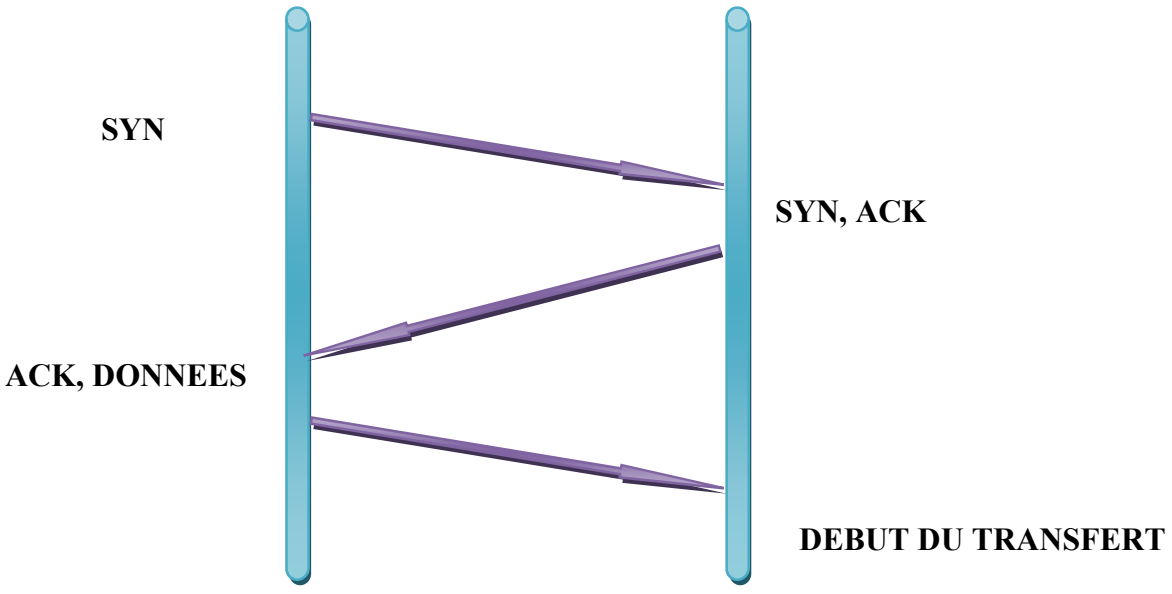


Fig I.8 : Initialisation en trois voyages

A la fin du transfert de données les deux modules du même niveau ont recours au même processus avec des segments dont le bit FIN est positionné pour fermer la connexion.

TCP considère les données qu'il véhicule comme un flux continu d'octets, et non pas comme une suite de paquets indépendants, il doit donc maintenir l'ordre dans lequel les octets lui sont soumis. Les champs numéro de séquence et numéro d'acquittement de l'en-tête d'un segment TCP permettent pour cela de numéroter les octets du flux.

Il est également du ressort de TCP de transmettre les données reçues de la couche IP à la bonne application. Pour cela, les numéros de port source et de port destination sur 16 bits contenus dans le premier mot de l'en-tête, permettent d'identifier l'application destinataire. La transmission correcte des données depuis et vers la couche application est une tache importante de la couche transport.

I.5.3-La couche internet :

La couche internet réalise l'interconnexion des réseaux distants sans connexion. Son rôle est de permettre l'injection des paquets dans n'importe quel réseau et l'acheminement de ces paquets est indépendamment les uns des autres jusqu'à destination. Tout le trafic, qu'il soit entrant ou sortant passe par cette couche (par IP) le rôle principal de la couche est de router les paquets entre différents hôtes.

La couche internet compte quatre protocoles

- **Le Protocole Internet :** Le rôle du protocole Internet est la transmission de blocs de données, appelés datagrammes, d'une source vers une destination, la source et la destination étant des ordinateurs hôtes identifiés par une adresse de longueur fixe. Le protocole Internet dispose des mécanismes permettant la fragmentation de longs datagrammes et leur réassemblage, lors de leur transmission à travers des réseaux.

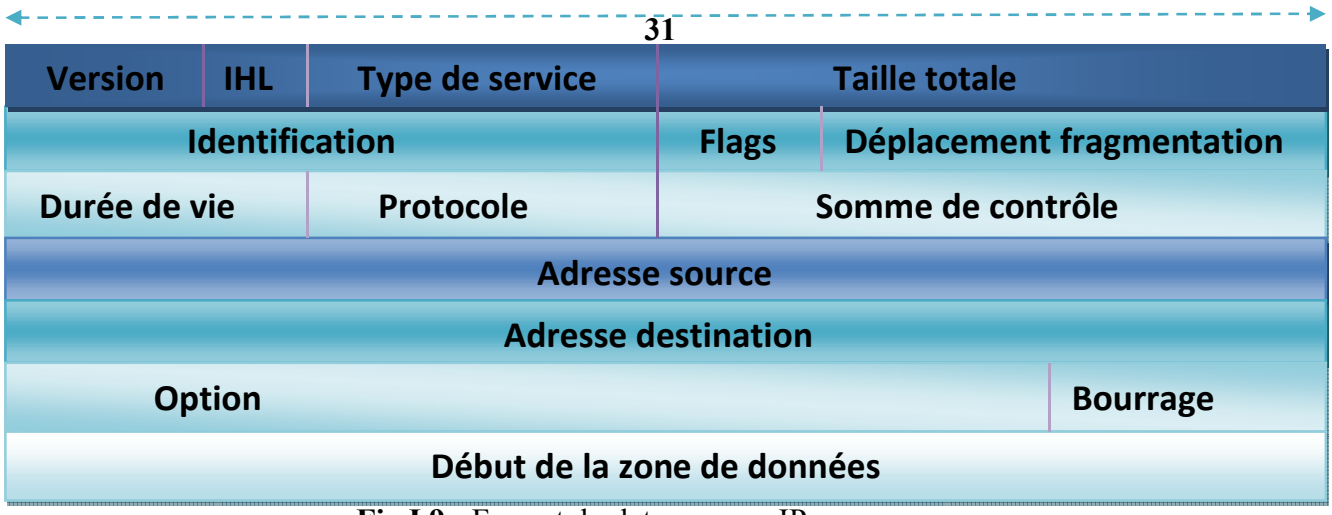


Fig I.9 : Format du datagramme IP

- **Le Protocole ICMP :** (Internet Control message Protocol)

Ce protocole joue un rôle informatif, il comporte plusieurs fonctions de contrôle de flux, l'alerte sur destination inaccessible, la direction des routes et le test des hôtes distants.

- **Les Protocoles ARP et RARP :** il existe deux protocoles qui couvrent les couches internet et accès au réseau :

ARP (protocole de résolution d'adresse) et **RARP** (protocole de résolution d'adresse inverse).

ARP est un protocole internet utilisé pour faire correspondre une adresse IP à une adresse physique du type adresse MAC. Chaque entité IP du réseau gère une table de résolution des adresses qui fait correspondre des adresses MAC à des adresses IP.

Lorsqu'un ordinateur exploitant IP veut remettre un message à une station située sur le même segment de réseau, il se sert de l'agresse MAC pour acheminer le paquet à la bonne station de travail.

RARP (est employé pour fournir une adresse IP à une station de travail. Cette station connait son adresse MAC et va demander son adresse IP à un serveur RARP en envoyant un message de diffusion

I.5.4-La couche réseau :

La couche réseau prend en charge l'optimisation des chemins de transmission entre les ordinateurs distants. Les paquets de données sont transmis grâce à l'établissement d'une connexion logique entre les ordinateurs, qui peut comprendre plusieurs nœuds, L'adressage des ordinateurs est réalisé dans cette couche par des adresses logiques (par exemple des adresses IP) qui doivent être configurées sur chacun des ordinateurs.

I.5.5-L'adressage TCP/IP :

Comme nous l'avons déjà vu, lorsque deux systèmes sont connectés sous TCP/IP, l'implantation de chaque couche de protocoles dans une machine communique directement avec son équivalent de même niveau sur l'autre machine distante. Ainsi chaque couche dispose de son propre système d'adressage qu'elle utilise pour diriger et transmettre les données vers le don destinataire.

Fig I.10 : Adresse intervenant dans un paquet pour convoyer des données application dans un réseau

I.6-Définition de l'adresse IP :

Sur internet, les ordinateurs communiquent entre eux grâce au protocole TCP/IP qui utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8bits),on le note donc sous la forme xxx.xxx.xxx.xxx, ou chaque xxx représente un entier de 0 à 255.Ces numéros servent aux ordinateurs du réseau pour se reconnaitre, aussi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP.

Par exemple, 194.153.205.26 est une adresse TCP/IP donnée sous une forme technique. C'est l'IANA (Internet Assigned Numbers Agency) qui est chargée d'attribuer ces numéros.

I.7-Les classes de réseaux :

Les adresses IP sont donc reparties en classe, c'est à dire selon le nombre d'octets qui représente le réseau.

- **Classe A :**

  Dans une adresse IP de classe A, le premier octet représente le réseau, le bit de poids fort (le premier bit, celui de gauche) est à zéro ce qui signifie qu'il y a 2^7 **(00000000) à (01111111)** possibilités de réseaux, c'est-à-dire 128 toute fois le réseau (0000 0000) n'existe pas et le nombre 127 est réservé pour désigner votre machine. Les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.0 (lorsque les derniers octets sont des zéros cela indique qu'il s'agit d'un réseau et non d'un ordinateur).

  Les trois octets de droite représentent les ordinateurs du réseau peut donc contenir :

  2^{24}–2=16777214 ordinateurs.

  Une adresse IP de classe A en binaire, ressemble à ceci :

  0XXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

  Réseau **Ordinateur**

- **Classe B :**

  Dans une adresse IP de classe B, les deux premiers octets représentent le réseau. Les deux premiers bits sont 1et 0 ce qui signifie qu'il y a 2^{14} (10 000000.00000000 à 10 111111.11111111) possibilités de réseau c'est-à-dire 16384. Les réseaux disponibles en classe B sont donc les réseaux allant ce 128.0.0.0 à 191.255.0.0.

Les deux octets de droite représentent les ordinateurs de réseau, le réseau peut donc contenir :

2^{16}–2=65534 ordinateurs.

Une adresse IP de classe B, en binaire ressemble à ceci :

10 XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Réseau Ordinateur

- **Classe c :**

  Dans une adresse de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1.1.0 ce qui signifie qu'il y a 2^{21} possibilités de réseau c'est-à-dire 2097152.

  Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.255.0

  L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir :

  2^{8}–2=254 ordinateurs

  Une adresse IP de classe C en binaire ressemble à ceci :

110 XXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Réseau ordinateur

I.8-Attribution des adresses IP :

Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. En effet avec cette notation il est possible de chercher dans un premier temps le réseau que l'on désire atteindre puis de chercher un ordinateur sur celui-ci. Ainsi l'attribution des adresses IP se fait selon la taille du réseau.

classe	Nombre de réseaux disponibles	Nombre d'ordinateur maximum
A	**126**	**16777214**
B	**16384**	**65534**
C	**2097153**	**254**

Table I.1 : Les classes de réseau

Les adresses de classe A sont réservées aux très grand réseaux, tandis que l'on attribuera les adresses de classe C à des petits réseaux d'entreprises par exemple.

- **Adresses IP réservées**

Il arrive fréquemment dans une entreprise qu'un seul ordinateur soit relié à internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à internet (on parle généralement de proxy). Dans ce cas, seul l'ordinateur relié à internet a besoin de réserver une adresse IP auprès de l'INTERNIC. Toute fois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble de façon interne.

Ainsi l'INTERNIC a réservé une poignée dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à internet sans risque de créer de conflits d'adresse IP sur le réseau. Il s'agit des adresses suivantes :

- 10.0.0.1 à 10 .255.255.254
- 172.160.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

I.9-Masque de sous-réseau

I.9.1-Notion de masque :

On fabrique un masque contenant des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut rendre égaux à zéro. Une foi ce masque crée, il suffit de faire un ET entre la valeur que l'on désire masquer et le masque afin de garder intacte la partie que l'on désire et annuler le reste.

Ainsi le masque réseau se présente sous la forme de 4 octets séparés par des points comme une adresse IP. Il comprend dans sa notation binaire des zéros au niveau des bits de l'adresse IP que l'on veut annuler et des 1 au niveau de ceux que l'on désire conserver.

I.9.2-Intérêt d'un tel masque :

Il y'en a en fait plusieurs. Un d'entre eux est de pouvoir connaitre le réseau associé à une adresse IP. En effet, comme nous l'avons vu précédemment, le réseau est déterminé par un certain nombre d'octets de l'adresse IP (1octet pour les adresses de classe A, 2 octets pour les adresses de classe B, et 3 octets pour la classe C)

De plus nous avons vu que l'on note un réseau en prenant le nombre d'octets qui le caractérise puis en complétant avec des zéros. Ainsi le réseau associé à l'adresse 34.56.123.12 est 34.0.0.0 (puisqu'il s'agit d'une adresse de classe A). Il suffit donc pour connaitre l'adresse du

réseau associé à l'adresse IP 34.56.123.12 d'appliquer un masque dont le premier octet ne comporte que des 1(ce qui donne 255), puis des 0 sur les octets suivants (ce qui donne 0). Le masque est : 11111111.00000000.00000000.00000000. Le masque associé à l'adresse IP 34.208.123.12 est donc 255.0.0.0. La valeur binaire de 34.208.123.12 est : 00100010.11010000.01111011.00001100. Un ET entre 00100010.11010000.01111011.00001100 ET 11111111.00000000.00000000.00000000 donne : 00100010.00000000.00000000.00000000 c'est-à-dire 34.0.0.0 c'est bien le réseau associé à l'adresse 34.56.123.12.

En généralisant, on obtient les masques suivants pour chaque classe

- Pour une adresse da classe A, seul le premier octet nous intéresse. On a donc un masque de la forme 11111111.00000000.00000000.00000000, c'est-à-dire en notation décimale : 255.0.0.0.
- Pour une adresse de classe B, les deux premiers octets nous intéressent, on a donc un masque de la forme 11111111.11111111.00000000.00000000, c'est-à-dire en notation décimale 255.255.0.0.
- Pour une adresse de classe C, on s'intéresse aux trois premiers octets, on a donc un masque de la forme 11111111.11111111.11111111.00000000 c'est-à-dire en notation décimale : 255.255.255.0

I.10-Création de sous-réseaux :

Reprenons l'exemple du réseau 34.0.0.0, et supposons que l'on désire que les deux premiers bits du deuxième octet permettent de désigner le réseau. Le masque à appliquer sera alors : 11111111.11000000.00000000.00000000, c'est-à-dire 255.192.0.0. Si on applique ce masque à l'adresse 34.208.123.12 on obtient 34.192.0.0.

En réalité il y a 4 cas de figures possibles pour le résultat du masquage d'une adresse IP d'un ordinateur du réseau 34.0.0.0

- Soit les deux premiers bits du deuxième octet sont 00, le résultat du masquage est 255.0.0.0.
- Soit les deux premiers bits du deuxième octet sont 01, le résultat de masquage est 255.64.0.0.
- Soit les deux premiers bits du deuxième octet sont 10, le résultat de masquage est 255 .128 .0.0.

❖ Soit les deux premiers bits du deuxième octet sont 11, le résultat de masquage est 255 .192 .0.0.

Ce masquage divise donc un réseau de classe A en 4 sous-réseaux (d'où le nom de masquage sous-réseau) pouvant admettre 2^{22}ordinateurs, c'est-à-dire 4194304 ordinateurs.

Au passage on remarque que le nombre d'ordinateurs possibles dans les deux cas est au total de 16777214ordinateurs (4*4194304–2=16777214).

Le nombre de sous- réseaux dépend du nombre de bits que l'on attribue en plus au réseau le nombre de sous-réseaux est donc :

Nombre de bits	Nombre de sous-réseaux
1	**2**
2	**4**
3	**8**
4	**16**
5	**32**
6	**64**
7	**128**
8 (impossible pour une classe C)	**256**

Table I.2 : Création de sous-réseaux

Conclusion :

Ce chapitre a présenté les différents composants d'une architecture réseau, ainsi que le découpage en couches effectué pour prendre en charge les fonctionnalités nécessaires à la bonne marche de ces systèmes. À partir de ces composants, il est possible de définir des architectures, et nous avons explicité les deux grandes solutions, OSI et TCP/IP, prépondérantes dans le domaine des réseaux.

Il faut bien insister, dans le cas de l'architecture OSI, sur le fait qu'elle ne représente qu'une solution théorique inspirée par le modèle de référence. La solution TCP/IP est aujourd'hui la plus répandue.

Chapitre 2 :

WAN et Routeurs

Dans notre projet, nous avons opté pour les équipements CISCO, ce choix a été fait car l'entreprise CISCO est la laideur dans ce domaine, la plus avancée technologiquement et équipe la CNAS.

II.1-Définition d'un réseau WAN :

Un réseau WAN se distingue d'un réseau LAN de diverses façons. Par exemple, contrairement à un réseau LAN qui relie des stations de travail, des périphériques, des terminaux et d'autres unités situés dans un même bâtiment ou dans un lieu rapproché, un réseau WAN assure des connexions de données sur une zone géographique étendue. Les entreprises utilisent les réseaux WAN pour interconnecter leurs divers sites de façon à pouvoir échanger des informations entre des bureaux distants.

Un réseau WAN fonctionne au niveau de la couche physique et de la couche liaison de données du modèle de référence OSI. Il interconnecte des réseaux LAN qui sont généralement séparés par de vastes étendues géographiques. Les réseaux WAN permettent l'échange de paquets et de trames de données entre les routeurs et les commutateurs qui constituent le réseau jusqu'au réseau LAN qu'ils prennent en marche.

Les principales caractéristiques d'un réseau WAN :

- Ils fonctionnent au-delà de la portée géographique des réseaux LAN
- Ils utilisent diverses connexions série pour communiquer sur de vastes aires géographiques.
- Ils utilisent les services d'opérateur Télécom.
- Les réseaux WAN relient des dispositifs séparés par de vastes étendus. Ces dispositifs sont notamment les suivants :

II.2-Les technologies WAN :

Les technologies WAN les plus répondues sont regroupées en services à commutation de circuits, services à commutation de cellules, services numériques dédiés et services analogiques.

II.2.1-Services à commutation de circuits :

a. Réseau téléphonique analogique ; il ne s'agit pas d'un service de données informatiques, mais il est présenté ici pour deux raisons :

- Bon nombre de ses technologies font partie de l'infrastructure Telecom en pleine expansion
- Il constitue un modèle de réseau de communication longue distance extrêmement fiable et facile à utiliser. Le média type est le fil de cuivre à paire s torsadées.

b. RNIS (Réseau Numérique à Intégration de services) ; technologie répondue et polyvalente, importante du point de vue historique. Premier services commuté entièrement numérique, son usage varie considérablement d'un pays à un autre. D'un coût modéré, la bonde passante maximale de 128 Kbits/s pour l'interface de base RNIS et d'environ 2Mbits/s pour l'interface à débit primaire. Son usage est assez répandu, bien qu'il diffère sensiblement d'un pays à un autre. Le média type est le fil de cuivre à paires torsadées

II.2.2-Services à commutation de paquets :

Optimisation de la commutation de message qui consiste à découper les messages en plusieurs paquets pouvant être acheminés plus vite et indépendamment les uns des autres. Cette technique nécessite la mise en place de la numérotation des paquets.

II.2.3-Services à commutation de cellules :

a. ATM (Asynchronous Transfer Mode) ; étroitement lié aux réseaux RNIS-à large bande. Il s'agit d'une technologie WAN (et même LAN) dont l'importance ne cesse pas d'augmenter. Elle utilise des petites cellules de longueur fixe (53 octets) pour transporter les données. La bande passante maximale actuelle est de 622 Mbits/s, mais des débits supérieurs sont en cours de développement. Les médias types sont le fil de cuivre à paires torsadées et la fibre optique. D'un usage répandu et en expansion, son coût est élevé.

b. Service de commutation de données débits (SMDS) ; étroitement lié à ATM et généralement utilisé dans les réseaux métropolitains (MAN), la bande passante maximale est de 44.736 Mbits/s. les médias types sont de fil de cuivre à paires torsadées et la fibre optique. D'un usage assez peu répondu, son coût est relativement élevé.

II.2.4-Services numériques dédiés :

a. T1, T3, E1et E3; Les services T offerts aux Etats-Unis et les services E en Europe sont les technologies WAN très importantes. Elles utilisent le multiplexage temporel pour "découper" et assigner des tranches de temps pour la transmission des données. Bande passante :

- T1 - 1.544 Mbits/s
- T3 - 44.736 Mbits/s
- E1 – 2.048 Mbits/s
- E3 – 34.368 Mbits/s

Les médias utilisés sont le fil de cuivre à paire torsadées et la fibre optique. Leur usage est extrêmement répondu et leur coût est modéré.

b. xDSL (DSL pour Digital Subsciber Line et x pour désigne une famille de technologies) ; nouvelle technologie WAN en développement pour un usage domestique. Offre une bande passante qui diminue en fonction de la distance par rapport à l'équipement de l'operateur. Un débit de 51.84 Mbits/s est possible à proximité d'une centrale téléphonique, mais des débits largement inférieurs sont plus courants (de quelques centaines de Kbits/s à plusieurs Mbits/s). d'un usage peu répandu, mais en augmentation rapide, son coût est modéré et en baisse. Le caractère x indique l'ensemble de la famille de technologie DSL, dont :

- HDSL – ligne numérique (DSL) à haut débit binaire
- SDSL – ligne numérique (DSL) à débit symétrique
- ADSL – ligne numérique à paire asymétrique (DSL asymétrique)
- VDSL – ligne numérique asymétrique (DSL) à très haut débit
- RADSL – ligne numérique (DSL) débit adaptable

c. SONET (Synchronnous Optical Network) ; famille de technologie propre à la couche physique, offrant de très haut débit et conçue pour la fibre optique. Elle peut aussi être utilisée avec deux fils de cuivre. Elle offre une série de débits de données disponibles avec désignation spéciales. Elle est mise en œuvre à différents niveaux d'opérateur optique, de 51.84 Mbits/s (OC – 1) à 9.952 Mbits/s (OC – 192) ? Ces débits exceptionnels peuvent être atteints grâce au multiplexage en longueur d'onde, permettant aux lasers d'être réglés sur des couleurs (longueur d'onde) légèrement différentes, afin d'envoyer d'énormes quantités de données par voie optique. D'un usage répandu sur le backbone internet, cette technologie reste d'un coût élevé. [SNET est la technologie équivalente utilisée en Amérique du Nord].

II.3-Optimisation Wan via WAAS:

Cisco Wide Area Application Services (WAAS) est une nouvelle application puissante d'accélération WAN et une solution d'optimisation qui permet

- La consolidation des serveurs de succursale
- L'amélioration des performances pour les applications centralisées.

Cette solution sera déployé entre le site centrale et direction régionales, et entre les directions régionales et centres payeurs afin d'améliorer les performances des applications de la CNAS. Comme l'illustre la figure II.1

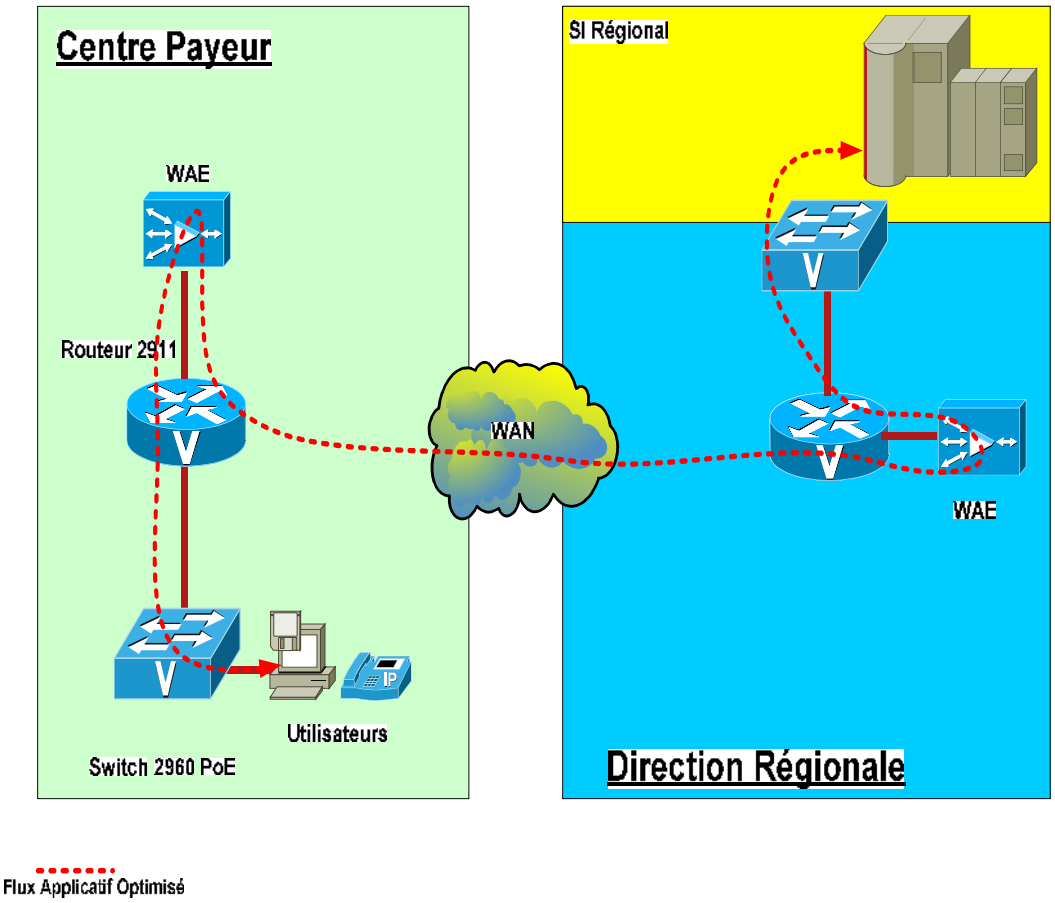


Fig II.1 : Réseau WAN optimisé

Plan de nommage:

Le tableau qui suit représente la liste nominative des équipements :

Type	Nom	Commentaires
WAE-512	CentralMGR	Central manager des WAAS
WAE-627	WAAS-Alger	WAAS du site central d'Alger
NME-WAE-502	WAAS-Agence	WAAS de sitedistant

Table II.1 : Les équipements WAAS

II.3.1-Protocole d'interception:

Le protocole responsable de l'interception est le WCCP (Web Cache Communication Protocole). Il permet aux équipements WAAS d'être déployé en off-Path.

Si l'équipement est installé en In-Path, le WCCP doit être désactivé.

II. 3.2-WCCP Groups :

Avec Cisco WAAS, deux numéros de group de services sont utilisés pour mettre en place l'interception de tout le trafic TCP, ces deux groups sont 61 et 62. Les deux groups (61 et 62) notifient le routeur que tout le trafic TCP doit être intercepté et rediriger vers le WAAS.

Le group 61 prend en charge le trafic en se basons sur l'adresse IP source.

Le group 62 prend en charge le trafic en ce basons sur l'adresse IP destination.

II.3.3-Configuration WCCP:

Avec des simples commandes, on peut activer les deux groups WCCP 61 et 62. En mode config, les commandes sont:

Router (config)#ipwccp 61

Router (config)#ipwccp 62

II.3.4-Application de la redirection sur les interfaces :

Router (config)#interface Fastethernet 0/0

Router (config-if)#ipwccp 61 redirect in

Router(config)#interface Serial 0/0

Router(config-if)#ipwccp 62 redirect in

II.3.5-Disponibilité matérielle des appliance WAE :

Les matériels proposés disposent des niveaux de redondance interne suivants :

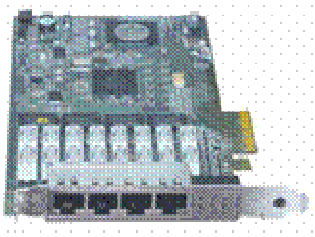
- WAE-512 : supporte deux disques SATA2 configurables en RAID mais qui ne sont pas échangeables à chaud. Pas d'alimentations redondantes.
- WAE-612 : supporte deux disques SCSI SAS configurables en RAID et échangeables à chaud. Pas d'alimentations redondantes.

- WAE-7326 : cette appliance dispose d'une double alimentation et de disques SCSI et ventilateurs échangeables à chaud.

Dans le cas où un matériel serait défectueux, son remplacement par un nouveau matériel est très rapide puisque le logiciel WAAS est pré-chargé sur les disques. Il suffit de restaurer la configuration pour que le boîtier soit opérationnel.

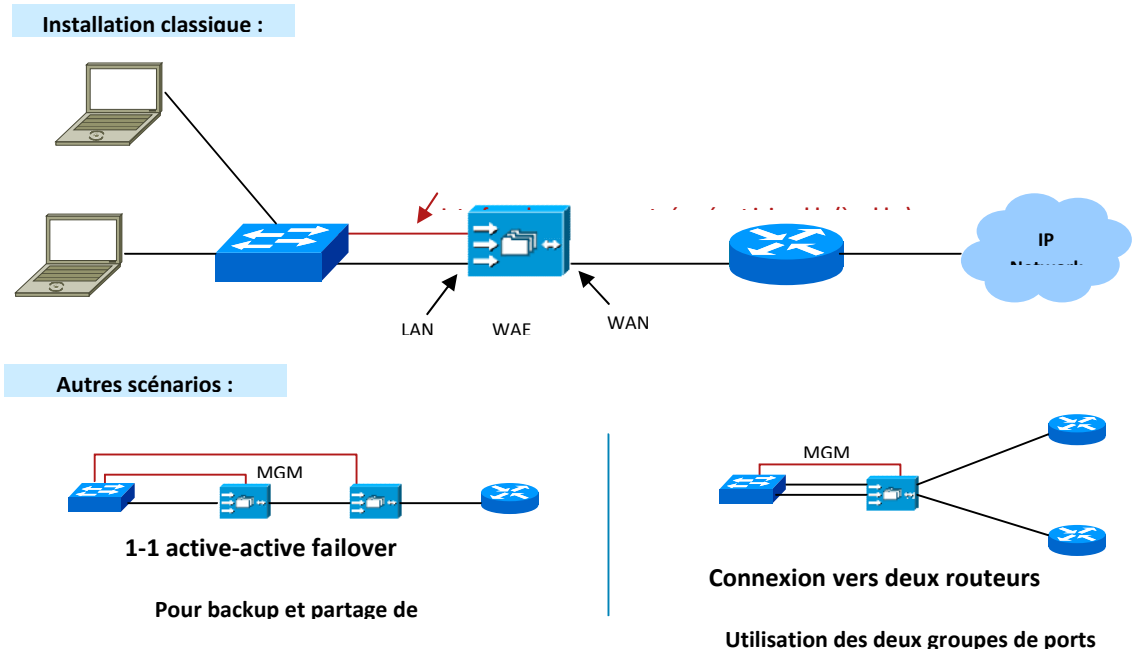
II.3.6-Positionnement du WAE en coupure (Mode INLINE) :

La méthode la plus simple pour déployer le WAE est de le positionner en coupure entre le LAN et le routeur. Ainsi tous les flux vont passer à travers le WAE. Seuls les flux qui auront été définis pour être optimisés, seront traités par les algorithmes d'optimisation du WAE. Les autres traverseront tout simplement sans traitement du WAE, avec une latence extrêmement faible, permettant ainsi par exemple de ne pas augmenter le délai de communications VoIP (sur UDP). Un mécanisme de bypass physique permet de gérer un disfonctionnement du WAE, que ce soit au niveau électrique ou au niveau logiciel.



FigII.2 : Carte INLINE pour WAE

Dans la figure II.2 nous avons une carte INLINE qui dispose de 4 ports RJ45 10/100/1000. Les ports sont regroupés en 2 groupes de deux interfaces : une LAN et une WAN. Les déploiements possibles sont représentés dans la figure II.3 :



FigII.3 : Utilisation de la carte INLINE

En plus des ports LAN et WAN de la carte Inline, il est nécessaire de câbler l'une des interfaces Ethernet primaire du WAE. Ce sera à travers cette interface, qui supportera l'adresse IP, qu'on accèdera au management du WAE. Les interfaces de la carte Inline fonctionnant en mode bridge (elles n'ont pas d'adresse IP).

Il est possible de chainer deux WAE en mode Inline, afin d'offrir un cluster permettant un fonctionnement résilient, mais aussi permettant d'augmenter la capacité de traitement du nombre de sessions TCP. En effet, dès que le premier WAE atteindra les limites de traitement (qui sont hard codés sur le WAE), il laissera passer les demandes de connexion (mode passthrough), qui seront alors traités par le second WAE.

En mode Inline, ce mode cluster n'est possible que pour deux WAE, à la différence du mode WCCP, qui peut aller jusque 32 WAE.

La carte Inline supporte le 802.1Q. Aussi, dans le cadre d'un lien trunk supportant plusieurs Vlan entre le switch et le routeur, il est possible de configurer sur la carte Inline du WAE uniquement les VLAN qui pourront être optimisés. Les autres Vlans seront bypassés par la carte sans même remonter au niveau de la CPU du WAE.

II.4-Les routeurs :

Le routeur est un ordinateur qui sélectionne les meilleurs chemins et qui gère la communication des paquets entre deux réseaux différents. Les composants de configuration internes d'un routeur sont les suivants :

a. Microprocesseur (CPU): l'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation du routeur.

b. Mémoire Flash : la flash représente une sorte de ROM effaçable et programmable. Sur beaucoup de routeurs, la mémoire flash est utilisée pour maintenir une image d'un ou plusieurs systèmes d'exploitation.

c. ROM : la ROM contient le code pour réaliser les diagnostics de démarrage (POST : Power On Self Test). En plus, la ROM permet le démarrage et le changement du système d'exploitation contenu sur flash.

d. RAM : la RAM est utilisée par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir la configuration qui s'exécute (running), les tables de routage, la table ARP, etc. et comme c'est de la RAM, lors de la coupure de l'alimentation elle est effacée.

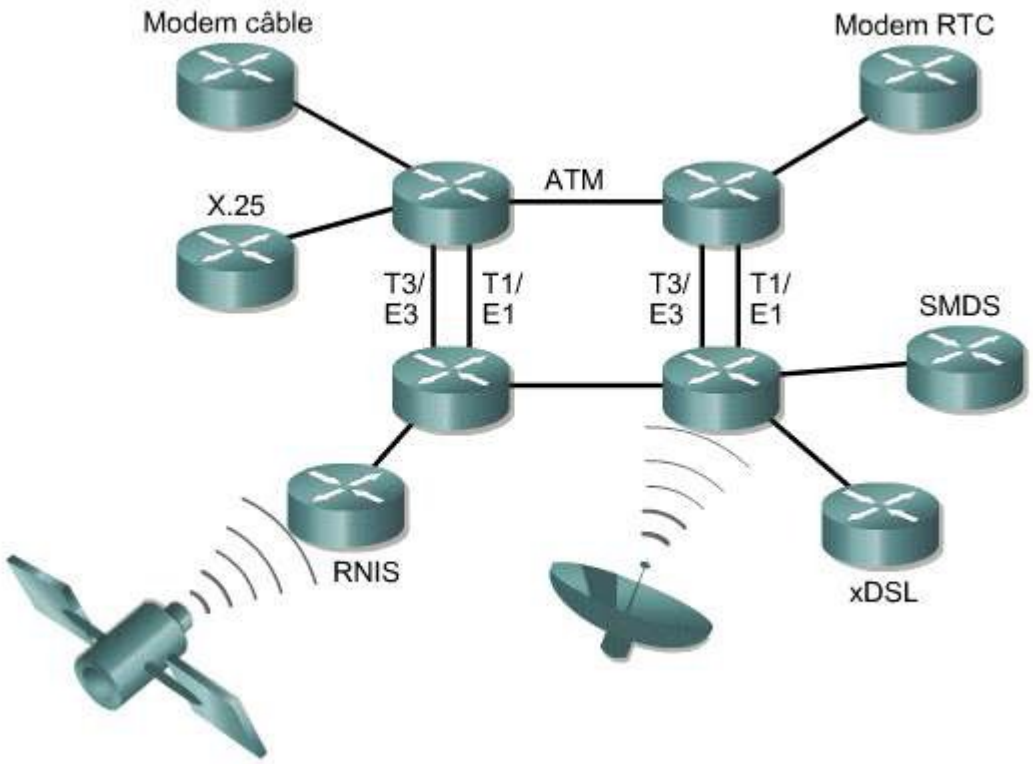
e. NVRAM (RAM non valide) : le problème de la RAM est le non conservation des données après la coupure de l'alimentation. La NVRAM solutionne le problème, puisque les données sont conservées même après la coupure de l'alimentation. La configuration set maintenue dans la NVRAM.

f. Les interfaces : connexion réseau par laquelle les paquets entrent et sortent d'un routeur. Elle peut se trouver sur la carte mère ou sur un module d'interface distinct.

A l'image des ordinateurs qui ont besoin de système d'exploitation pour exécuter les applications, les routeurs doivent être équipés d'une plate-forme logicielle IOS (Internetworking Operating Software) pour exécuter les fichiers de configuration. Ces fichiers contrôlent le flux de données en direction du routeur. Plus précisément, en utilisant des protocoles de routage et des tables de routage pour rediriger les protocoles routés, ils choisissent les meilleurs chemins pour les paquets. Pour contrôler ces protocoles et décisions il convient de configurer le routeur.

II.4.1-Le rôle d'un routeur dans un réseau WAN:

Bien que les routeurs puissent servir à segmenter des réseaux LAN, ils sont essentiellement utilisés en tant qu'équipement WAN. Les routeurs sont dotés à la fois d'interfaces LAN et WAN. En fait, les technologies WAN sont souvent utilisées pour interconnecter des routeurs. Dans ce cas de figure, les routeurs s'échangent des informations via les liaisons WAN constituant ainsi des systèmes autonomes ou le backbone d'internet.



FigII.4 : Routeurs reliés par des technologies WAN.

Lorsqu'un routeur utilise les protocoles et normes de la couche physique et de la couche liaison de données qui sont associés aux réseaux WAN, il fonctionne comme une unité WAN. Le rôle principal d'un routeur dans un WAN n'est pas le routage, mais la compatibilité des connexions vers et entre les diverses normes physiques et de liaison de données d'un réseau WAN. La sélection des meilleurs chemins pour les paquets de données entrants et la communication des paquets vers l'interface de sortie appropriée. Pour ce faire les routeurs créent des tables de routages et échangent des informations sur le réseau avec d'autres routeurs.

II.4.2-L'interface utilisateur CISCO:

En supposant qu'un terminal connecté port console d'un routeur préalablement configuré et que l'on ait saisi, si nécessaire un mot de passe, on voit s'afficher le prompt suivant :

```
Hostname>
```

Il faut alors taper des commandes. Dans l'interface Cisco il y a deux niveaux d'accès utilisateur et privilégié. Le premier niveau, qui permet de connaitre l'état d'un routeur, s'appelle également mode **Exec**utilisateur.

Le mode privilégié, par ailleurs appelé “mode Exec“, sert à connaitre la configuration, la modifier et à exécuter les commandes de mise au point. On évoque parfois, à ce propos, le mode “Enable“, parce que pour instaurer ce “mode Exec“ privilégié, il faut taper la commande “Enable“, suivi d’un mot de passe. Voici un exemple de commandes :

Hostname>enable appuyez sur entrée

Password : donnez le mot de passe Enable et appuyez sur Entrée

Hostname#

Le caractère d’invite et maintenant # et non plus > : c’est la manifestation visible du fait que le mode privilégié est bien active.

Avant de poursuivre, il faut noter que le routeur dispos de deux modes. Le premier se nomme mode “vue“ (view mode). On peut alors saisir les commandes “show“ et “debug“. Cela permet de connaitre l’état des interfaces, des protocoles et autres composants. C’est le mode par défaut du routeur, lorsqu’on s’y connecte. Le second est mode configuration. Il permet de modifier la configuration du routeur en temps réel.

Il est impératif de savoir qu’au sitôt la commande de configuration validée par la touche Entrée, elle prend effet avant même que l’on quitte le mode correspondant. Pour activer ce mode, il faut absolument avoir obtenu le privilège Enable, comme ci-dessous :

Hostname#config terminal appuyer sur Entrée

Enter configuration commands, one per line. End with Ctrl/z.

Hostname (config)#

La ligne qui indique qu’il faut terminer par un “Ctrl-z“ est envoyée par l’ordinateur. La commande d’entrée en mode configuration, dans ce cas précis, indique au routeur qu’il est configuré à partir du terminal. Il est possible de lui signifier qu’il doit récupérer sa configuration sur un serveur de réseau.

Là encore, remarquons que l’invite change pour signaler que l’on passe en mode configuration.

Voici un exemple illustrant la façon de saisir les commandes de configuration de l’interface Ethernet0 :

Hostname (config)# interface ethernet0 Appuyez sur Entrée

Hostname (config-int)#

Pour revenir d'un niveau, il suffit de taper :

Hostname (config-int)#exit appuyez sur Entrée

Hostname (config)#

Pour sortir du mode de configuration à un niveau quelconque que l'on soit, il suffit de maintenir appuyée la touche Ctrl et de taper Z :

Hostname (config) # <Ctrl-z>

Hostname#

Pour sortir du mode enable, taper :

Hostname#exitappuyez sur Entrée

Hostname>

Vous disposez maintenant des bases de la navigation dans l'interface utilisateur. Voici ci-dessous quelques commandes au clavier bien utiles :

<Ctrl-A>	Ramène le curseur au début de la ligne.
<Ctrl-B>	Déplace le curseur d'un caractère ver l'arrière.
<Ctrl-D>	Supprime le caractère situé sous le curseur.
<Ctrl-H>	Même effet que retour arrière ; supprimer le caractère qui préside le curseur.
< Ctrl-K>	Supprimer tous les caractères jusqu'à la fin de la ligne. Les caractères sont mis dans une mémoire tampon et peuvent être ainsi réinséré dans une ligne de commande.
< Ctrl-U>	Supprimer jusqu'à la fin de la ligne ; là encore, les caractères sont stockés dans une mémoire tampon.
< Ctrl-V>	Permet d'insérer des caractères de contrôle dans une ligne de commande. Indique à l'interface utilisateur que le caractère suivant va être inséré tel que et non interprété comme une commande de l'éditeur.
< Ctrl-W>	Supprime le mot précédent
<Ctrl-Y>	Colle les caractères pris dans le tampon (indique à la commande yank sous Unix).

Esc<	Affiche la première ligne de l'historique des commandes.
Esc>	Affiche la dernière ligne de l'historique des commandes.
Esc b	Recule le curseur d'un mot.
Esc d	Supprime le mot qui suit le curseur.
Esc f	Avance le curseur d'un mot.
Esc Del	Supprime le mot qui précède le curseur.

Table II.2 : commande de clavier d'un routeur

Conclusion :

Nous avons vu dans ce chapitre le concept de réseau, son mode de fonctionnement et la notion de protocoles ainsi que l'optimisation du réseau WAN avec les appliances WAE (WAAS) que nous allons étudier dans le chapitre suivant.

Chapitre3 :

Optimisation des Applications WAS

Afin de réduire l'influence de la bonde passante sur les liaisons spécialisées. La CNAS à choisit un compromis entre la bonde passante et le cout de réalisation. A cet effet la technologie WAAS dans des routeurs d'interconnexion répond aux exigences

Cette technologie se manifeste dans l'intégration dans les routeurs des directions de wilaya (3845) un module NME-WAE qui permet d'optimiser le trafic TCP/IP circulant sur un réseau étendu(WAN).

Sur un réseau WAN on est toujours confronté à des contraintes techniques, à savoir le débit et la latence, ajouter à ça les contraintes budgétaires : le coût élevé des débits des lignes spécialisé. Pour cela la technologie WAAS offre un mécanisme d'optimisation des flux et augmentation des performances applicatives sans avoir recours à l'augmentation de la bonde passante du lien spécialisé.

La technologie WAAS a pour objectif d'améliorer à la fois les performances applicatives, d'optimisation de l'utilisation des liens WAN, mais aussi les accès aux serveurs de fichier, au travers du WAN permettant ainsi une consolidation sur un site central des serveurs auparavant éparpillés dans les filiales des entreprises.

III.1-Principe de fonctionnement:

La technologie WAAS propose des mécanismes d'optimisation générique sur les flux applicatifs tels que :

- **DRE** (Data redundancy Elimination) qui consiste à ne pas réémettre des données redondantes.
- **Compression LZ** (Lempel Zip), qui permet de compresser toutes les données qui doivent transiter sur le WAN.
- **TFO** (TCP Flow Optimisation), qui permet une meilleure utilisation de la bonde passante en optimisant les mécanismes de TCP.

Associés à ces mécanismes génériques, la solution WAAS propose un ensemble de proxy applicatif spécifique, permettant d'optimiser dans le détail ces différents protocoles :

- CIFS pour l'accès aux serveurs de fichiers en environnement Windows avec mécanisme de pré positionnement.
- NFS pour l'accès aux serveurs de fichiers en environnement Unix.
- http pour tous les accès aux applications aux formats WEB.
- MAPI pour l'optimisation des échanges de messagerie Exchange.
- VIDEO Streaming : optimise la diffusion vidéo sur les sites distants.

III.2-Fonctionnalités et protocoles supportés par Cisco WAAS :

Le logiciel Cisco WAAS est basé sur un certain nombre de composants, chacun étant conçu dans l'objectif d'offrir un accès hautement performent aux données distantes, sans pour autant compromettre l'intégrité des données.

Toutes les fonctionnalités décrites ci-dessous sont activables ou non sous forme de politiques d'accélération. Ces politiques doivent être appliquées de manière homogène sur les appliances ; si la cohérence de configuration entre les sites de périphérie et le data center n'est pas respectée, certains types d'accélération ne seront pas effectifs (comme la compression DRE et l'optimisation TFO). Par contre, cela n'induit pas d'interruption de service pour l'utilisateur : les applications continuent de transiter même si elles ne sont pas optimisées.

III.2.1-Optimisation TCP avec TFO :

L'implémentation standard des stacks TCP au niveau des clients et des serveurs peut entraîner une perte de performance au niveau des applications. Plusieurs raisons peuvent exister :

- Impossibilité de remplir la ligne (mauvaise utilisation de la bonde passante disponible).
- Mauvaise récupération lors de la perte de paquets, retransmission,
- Consommation de toute la bande passante par de très nombreuses connexions courtes.

La fonction WAAS TFO (Transport Flow Optimization) implémente des mécanismes standards du marché pour résoudre ces problèmes de performance liés à certaines implémentations de TCP.

- **Fenêtrage TCP :**

La première fonction permettant d'améliorer les performances de TCP consiste à ajuster la valeur du fenêtrage de TCP. Après un certain nombre de paquets, TCP va attendre un acquittement de la part du destinataire. Sur une liaison WAN, apportant une latence importante, le temps perdu lors de ces phases d'acquittement entraîne un impacte important sur les performances. Le fenêtrage classique de TCP (identifié sur un champ de 16 bits) limite celui-ci à 64 Ko. L'utilisation du RFC1323 permet d'augmenter la limite jusqu' à une valeur de 1Go (correspondant à un champ de 30 bits). Ainsi le lien est utilisé de façon plus massive pour la transmission des données et les phases d'acquittements (impactés par la latence) sont proportionnellement moins importantes.

- **Acquittement sélectif (Sack) :**

Les implémentations TCP standard acquittent l'ensemble de la fenêtre de transmission. Ce qui veut dire que si sur 3 paquets seule 3eme n'a pas été reçu, l'ensemble des 3 paquets est retransmis (figure III.1). Cela pose d'autant plus de problème que l'on a augmenté la fenêtre pour optimiser la performance de transmission.

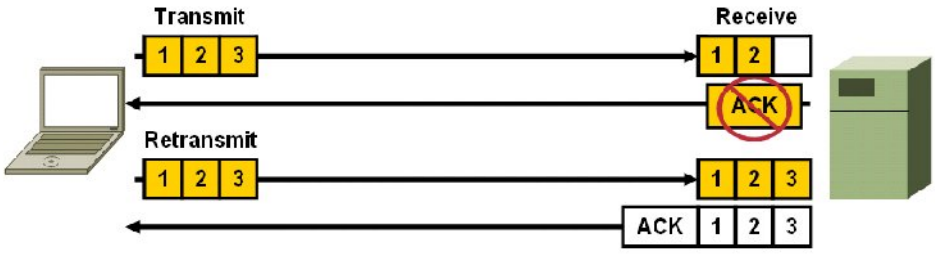


Fig III.1 : Acquittement standard

L'acquittement sélectif permet de ne demander la réémission que du paquet manquant.

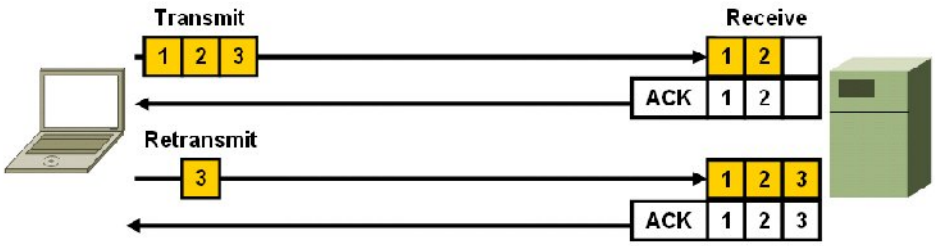


Fig III.2 : Acquittement des paquets

- **Adaptive Increase Windows size**

La fonction TFO va aussi réduire le temps de remontée de la fenêtre TCP, une fois le maximum atteint. L'objectif de cette fonction est de limiter l'effet « dent-de-scie » que l'on peut constater avec les flux TCP.

La figure III.1illustrent ainsi le meilleur usage de la liaison :

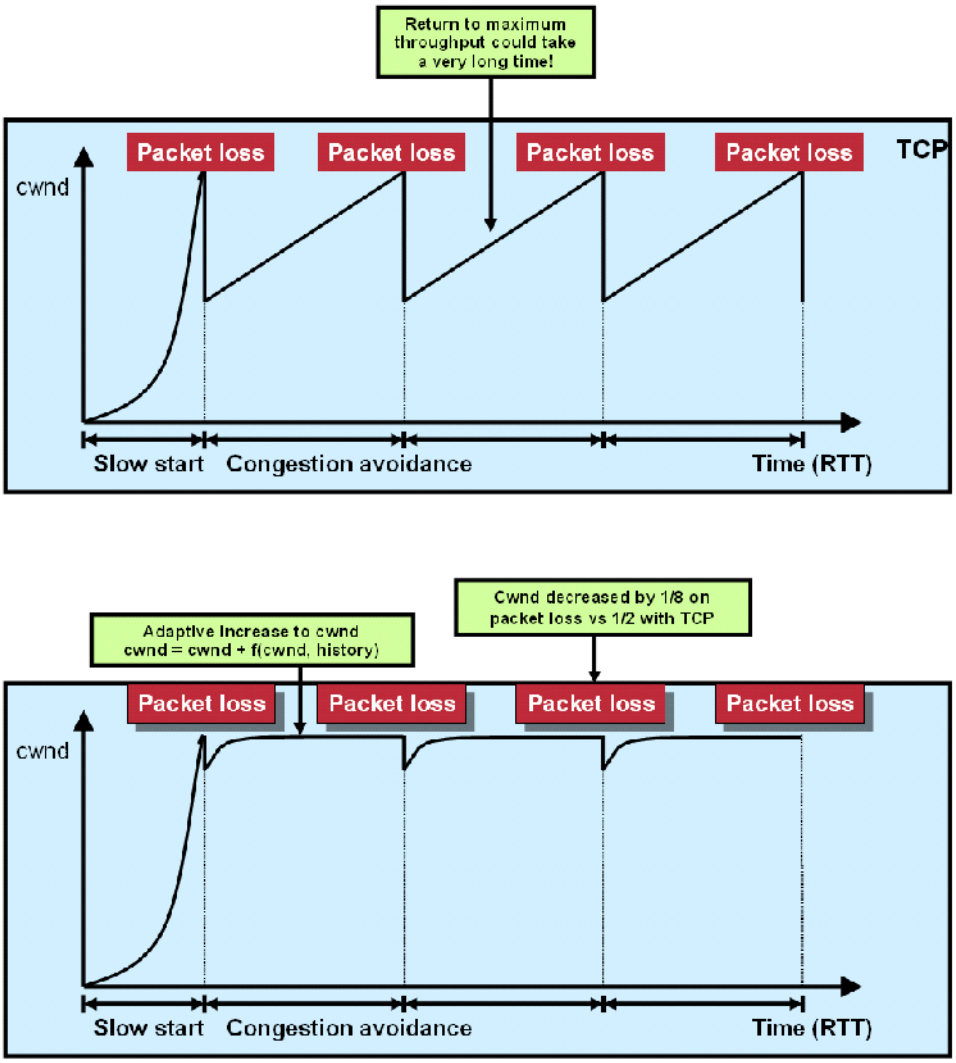


Fig III.3: Action de « l'adaptive increase windows size »

III.2.2-Compression DRE

Cisco WAAS utilise deux mécanismes de compression avancés au niveau de la couche de transport :

- **La compression LZ (Lempel Zip) :** Compression standard réalisée en temps réel sur le flux
- **DRE (Data Redundancy Elimination) :** Mécanisme évolué permettant la suppression des données redondantes lors de la transmission.

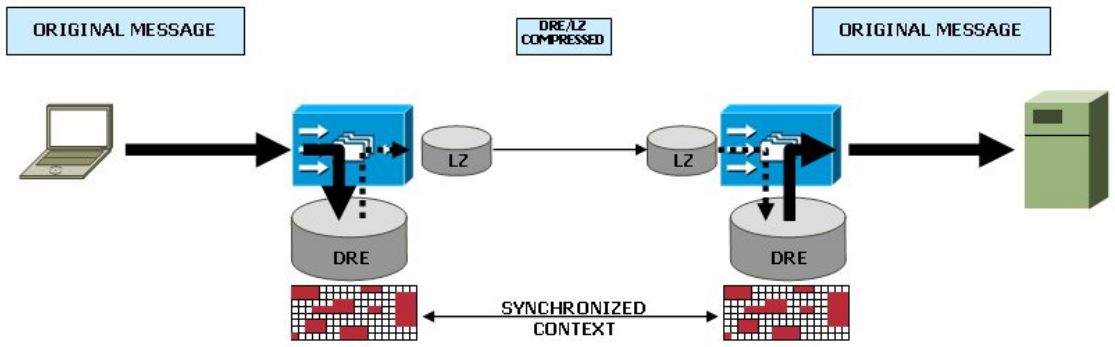


Fig III.4 : Représentation globale des mécanismes de compression

DRE utilise les ressemblances entre les données qui sont transmises sur le lien. Une fonction sophistiquée de reconnaissance par masques sur le contenu, identifie les blocs de données qui sont répétées (appelés « chunks »).

Ces blocs sont stockés et indexés dans un cache particulier de chaque côté de la liaison. Une fois qu'un bloc est stocké dans le cache, les émissions futures de ce même bloc ne demandent plus que la réémission d'un petit identifiant (« signature » ou « label ») au travers du lien WAN.

La compression LZ est appliquée lors de la première émission du bloc, ou lorsqu'un bloc de données ne correspond à aucun bloc mémorisé dans la zone de stockage.

Afin de maintenir une cohérence entre les caches de blocs des deux côtés de la liaison, la fonction DRE utilise un mécanisme de synchronisation entre les caches.

Le fonctionnement détaillé de la fonction DRE est détaillé ci-dessous :

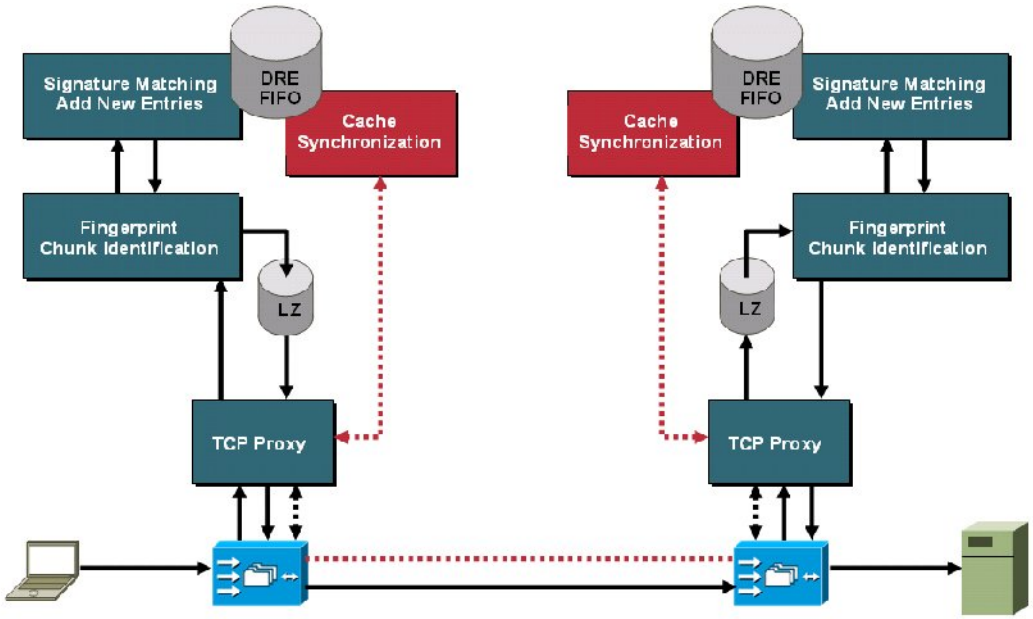


Fig III.5 : Mécanisme de compression DRE

- La trame TCP est redirigée vers le WAE (par exemple par WCCP).
- La trame est traitée par la fonction de TCP proxy de WAAS.
- WAAS identifie les blocs dont une copie a déjà été mémorisée dans le cache.
- Si le bloc n'a pas été trouvé, il le mémorise dans le cache, créé un identifiant. (signature) et envoie le bloc avec sa signature pour synchroniser le cache se trouvant de l'autre côté.
- Si le bloc existe, remplace le bloc par la signature correspondante.
- Compresse les données par LZ.
- Envoi la trame TCP résultante sur le lien WAN (à noter que les propriétés IP/TCP restent les mêmes, seul le payload a été compressé).

A la réception, la trame est traitée par la fonction TCP proxy de WAAS

- Le payload est décompressé par LZ
- Les blocs non transmis sont identifiés par les signatures
- Les données sont recomposées
- La trame est envoyée au destinataire.

DRE va rechercher les blocs en utilisant un algorithme basé sur le parcours d'une fenêtre glissante le long des données. Il va chercher dans un premier temps à identifier les blocs redondants les plus grands, puis devenir plus granulaire. Il indexe alors les blocs dans son cache (figure III.6) du plus grand au plus petit.

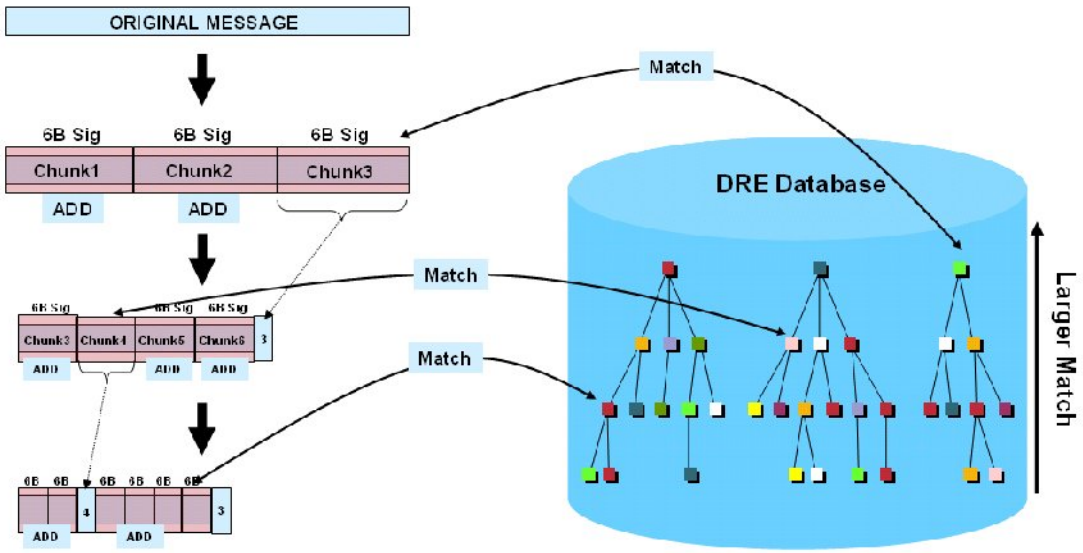


Fig III.6 : Base de données DRE

Un payload passé au travers de DRE sera remplacé par un ensemble de signatures pour les blocs qui ont été remplacés (figure III.7), et un ensemble de blocs précédés par leur signature pour les nouveaux blocs indexés dans le cache. Le payload est terminé par une signature (hashing MD5) du paquet original, permettant de vérifier l'intégrité de la trame une fois recomposée à la réception.

Il est important de noter que DRE est bidirectionnel et donc que les blocs supprimés dans un sens peuvent être utilisé de façon similaire pour le flux retour sans avoir besoin de faire un nouvel apprentissage pour ces mêmes blocs.

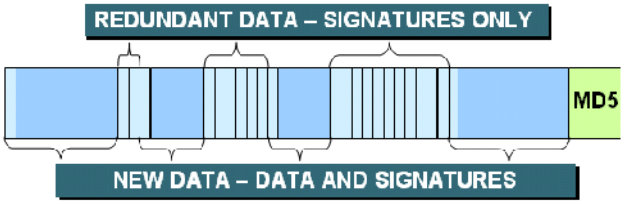


Fig III.7: Message compressé par DRE

Afin de conserver une cohérence entre les caches se trouvant des deux côté de la liaison WAN, un mécanisme de synchronisation existe entre les deux caches. Les caches s'échangent une information de contexte différente pour chaque liaison deux-à-deux. L'information de contexte est bidirectionnelle et va permettre de supprimer les blocs qui ne sont pas synchronisés avec le cache correspondant.

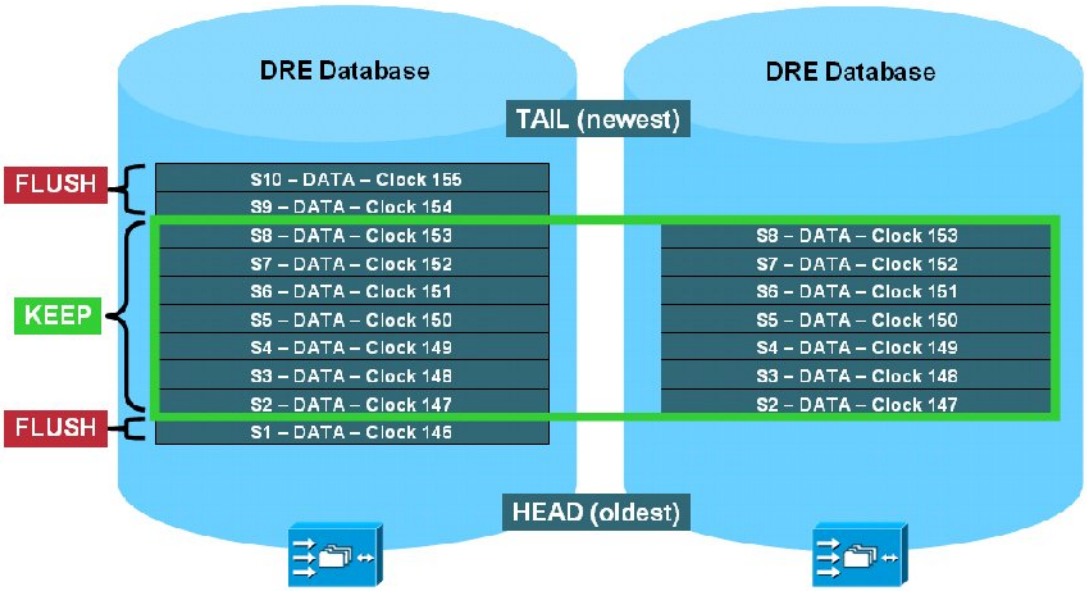


Fig III.8 : Synchronisation des contextes DRE

III.2.3-Wide Area Files Systems (WAFS): CIFS

III.2.3.1- Analyse de flux (flow parsing)

Le logiciel Cisco WAAS fournit une interface protocolaire serveur CIFS aux utilisateurs du site (sur les WAE Edge) et présente une interface protocolaire cliente CIFS vers les serveurs de fichiers et les NAS du data center (sur les WAE core). Etant en lui-même une interface protocolaire avec des fonctions d'analyse de paquets avancées, le logiciel WAAS est capable de regarder dans chaque message de chaque flux. La fonction d'analyse de flux est responsable de l'identification les opérations au sein de chaque paquet pour déterminer la meilleure façon de les traiter.

Chaque flux qui impacte directement l'intégrité des données, l'authentification de l'utilisateur ou les niveaux d'accréditation sont transmis de manière synchrone au serveur de fichier d'origine via un mécanisme de transport optimisé (décrit plus loin dans ce document).

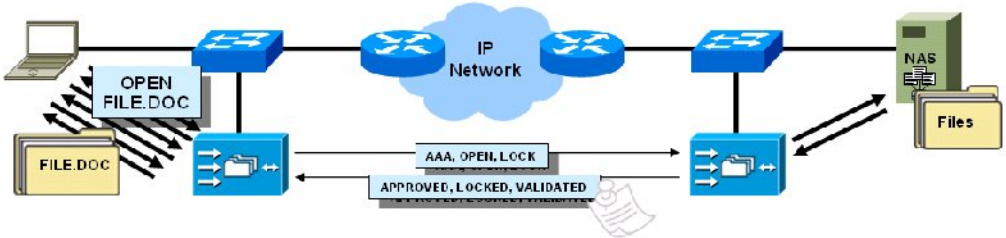


Fig III.9 : Gestion des opérations synchrones

Les opérations toujours traitées par le serveur d'origine sont notamment les suivantes :

❖ **Authentification des utilisateurs :** les opérations d'établissement et fermeture de session, authentification utilisateur incluse, sont toujours gérées par le serveur de fichier ou le NAS central. De ce fait, il n'est pas nécessaire de redéfinir les utilisateurs d'un site distant et la sécurité d'accès aux fichiers qui est toujours gérée par les mécanismes d'authentification en central (comme par exemple l'Active Directory).

❖ **Autorisation des utilisateurs :** les opérations de connexion et déconnexion à une ressource requièrent que l'utilisateur soit autorisé à y accéder. Toutes les demandes d'autorisation d'accès aux ressources sont aussi contrôlées par le serveur ou le NAS d'origine. De ce fait, de même que pour l'authentification, tous les mécanismes d'autorisation centralisés s'appliquent : permissions partagées, politique de groupe, permissions sur le système de fichiers, gestion des quotas,….

❖ **Vérouillage des fichiers (Locking) :** pour garantir que les fichiers puissent être partagés par des utilisateurs situés sur de multiples sites, les demandes de verrouillage de fichier sont transmises au serveur ou NAS central dans le data center**.** En délégant la gestion du verrouillage au serveur central, tous les utilisateurs peuvent sans aucun problème travailler sur les même fichiers, en disposant toujours de la dernière version, et ce sans se soucier de l'intégrité des données. Le serveur de fichiers gère donc toutes les demandes de verrouillage mais aussi toutes les notifications de verrouillage, par exemple lorsqu'un fichier est déjà ouvert par un utilisateur d'un autre site. Contrairement aux architectures qui distribuent la gestion du verrouillage, il ne peut pas y avoir d'incohérence dans les données suite à une panne quelconque de l'infrastructure.

❖ **Ouverture et fermeture avec vidange des buffers :** les demandes d'ouverture et de fermeture de fichiers sont propagées de manière synchrone vers le serveur de fichiers ou NAS central pour garantir l'application des modes partagés et pour préserver les sémantiques protocolaires. De plus, la visibilité sur ces requêtes permet au logiciel WAAS de toujours connaître l'état d'un fichier sur les serveurs. L'opération de fermeture implique un transfert immédiat de toutes les données stockées dans les buffers avant de confirmer l'opération à l'utilisateur. Ce dernier est donc certain que son fichier est sauvegardé et présent intégralement à jour sur le NAS central lorsqu'il reçoit le message de confirmation.

III.2.3.2-Mécanismes de cache :

Le logiciel WAAS utilise un cache de segments de fichiers (data cache) ainsi qu'un cache de métadonnées (metadata cache) qui sont utilisés pour maintenir des copies de fichiers et dossiers

récemment consultés. De plus, un cache « write-back » permet de masquer les contraintes de performance lorsque l'on sauvegarde un fichier via le WAN.

❖ **Le Data Cache** : le data cache est un point de stockage des segments de fichiers qui ont été précédemment consultés ou volontairement pré-positionnés. Du fait que les protocoles d'accès aux fichiers fonctionnent en mode segment (les clients demandent en fait un certain nombre d'octets d'un fichier pour fournir les données nécessaires à l'environnement applicatif), l'usage d'un cache adapté permet de servir uniquement les segments disponibles et nécessaires, même si le fichier n'est pas intégralement présent. Lorsque l'utilisateur ouvre un fichier, un processus de validation (« validate-on-open ») est immédiatement déclenché pour comparer le contenu du cache avec celui du serveur central, afin que le logiciel WAAS ne délivre pas une version obsolète du fichier. Différents mécanismes sont utilisés pour cela comme une comparaison des métadonnées des fichiers demandés. Si la comparaison « validate-on-open » du fichier échoue, les segments concernés du fichier sont effacés du cache et remplacés par une nouvelle copie à jour des données du serveur central.

➢ **Le Metadata Cache :** le cache des métadonnées offre un stockage des informations relatives aux structures des répertoires et fichiers du serveur central, ainsi que des fichiers présents dans le data cache. De nombreuses requêtes de métadonnées d'un utilisateur peuvent être servies directement depuis le metadata cache, cela comprend la navigation dans les répertoires ou encore les opérations de recherche. Contrairement aux données des fichiers qui sont validées à chaque accès, le metadata cache est contrôllé à intervalle de temps régulier et configurable.

❖ **Cache « write-back » asynchrone :** le logiciel WAAS dispose d'un buffer « write-back » asynchrone qui masque les difficultés à écrire des données via le WAN. Il permet notamment de concaténer plusieurs opérations d'écriture pour maximiser l'usage de la bande passante et donc limiter l'impact de la latence (mécanisme connu sous le nom de « pipelining »). Les opérations d'écriture initiées par les utilisateurs sont examinées et classifiées comme supportant un traitement asynchrone ou non. Une opération supportant ce mode est par exemple une écriture pour laquelle le client n'attend pas de réponse immédiate. Cela ne remet en rien en cause l'intégrité des données. A contrario, l'opération de fermeture de fichier où l'utilisateur sauve son document et ferme l'application par exemple doit être traité de manière synchrone et ne bénéficie donc pas du cache « write-back ». De la même manière, certaines opérations peuvent avoir été marquées comme synchrone par l'application et ne peuvent donc pas être cachées.

❖ **Lecture intelligente en avance de phase (« Read-ahead ») :** le logiciel WAAS suit également l'activité des utilisateurs et de leurs accès aux fichiers, ce qui lui permet de pronostiquer

un certain nombre de lectures en avance de phase à réaliser. Il va ainsi charger de lui-même des segments de fichiers qui n'ont pas encore été consultés ni cachés, dans le souci d'améliorer les temps de réponse pendant que l'utilisateur continue à travailler sur le même fichier.

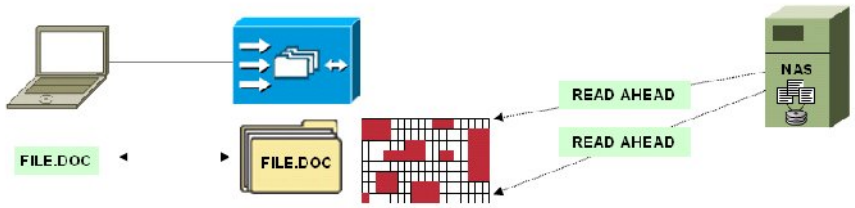


Fig III.10: Illustration du cache de segments et de la fonction "read-ahead" de WAAS

III.2.3.3-Proxies protocolaires :

Le logiciel WAAS joue un rôle de proxy intelligent pour le protocole CIFS. De ce fait, il est capable de traiter un grand nombre de messages localement, libérant le WAN des multiples échanges qu'ils occasionnent et réduisant ainsi grandement les temps d'accès aux fichiers.

Le logiciel WAAS dispose donc du proxy protocolaire suivant :

❖ **CIFS :** ce proxy interprète l'intégralité des opérations CIFS. Il permet également d'insérer WAAS dans une architecture DFS en tant que point de réplication local des ressources. Dans un environnement Microsoft, WAAS peut donc être utilisé de 3 manières différentes :

- En adressage directe CIFS : les utilisateurs indiquent l'UNC du WAAS pour accéder à leurs ressources
- En l'intégrant dans un environnement DFS : les utilisateurs pointent sur le partage « root » et sont redirigés sur l'appliance du site.
- En utilisant la redirection WCCP : le WAAS constate qu'un utilisateur tente d'accéder à une ressource centrale et insère ses fonctions d'optimisation de manière transparente.

Si nécessaire, par exemple pour gérer des « home directories » locaux, il est possible de configurer WAAS pour gérer de la cohérence locale pour les accès aux fichiers et donc d'utiliser les mécanismes d'opportunistic Locking (OpLock) de CIFS.

Dans les deux cas, le système d'optimisation repose en grande partie sur un mécanisme nommé IMS (Intelligent Message Suppression). Un tunnel TCP permanent est établie entre un WAE Edge

et un WAE coré du data center. Toutes les communications CIFS entre le site distant et le site central sont reformatées afin de les optimiser et de ne transmettre via le tunnel que les messages réellement nécessaires. Le WAE réceptionnant des instructions ou des données par le tunnel les retransforment en CIFS natif pour les transmettre au destinataire (utilisateur ou NAS). IMS permet notamment de :

- traiter un maximum d'opérations en local et ainsi minimiser les échanges.
- grouper les commandes (notion de commandes composite)
- pronostiquer les futurs messages et pré-charger le data cache par anticipation

III.2.3.4-Pré-positionnement de fichiers :

Le logiciel WAAS permet de pré-positionner ou « pousser » des fichiers sur les WAE Edge de manière contrôlée à partir du Central Manager, et ceci de manière immédiate ou programmée. Le choix des fichiers à distribuer peut se faire selon une sélection automatique par motif (ex : tous les fichiers commençant par x y z). Les recherches récursives de fichiers au sein d'une arborescence de répertoires sont également supportées.

La fonction de pré-positionnement prend également certaines contraintes en compte avant de réaliser l'opération. Celles-ci sont configurables par l'administrateur qui programme la tâche. Elles peuvent être de natures suivantes :

- ❖ Plage horaire autorisée pour l'opération
- ❖ Espace de cache disponible sur les WAE cibles
- ❖ Taille maximale des fichiers distribuables
- ❖ Fréquence d'utilisation des fichiers (en fonction de la date de dernière modification)

Enfin, l'opération de pré-positionnement est optimisée, et ce de trois manières :

- ❖ Si le fichier existe déjà (en entier ou partiellement), seuls les segments manquants ou modifiés sont transférés.
- ❖ Les fichiers complets sont distribués s'ils ne sont pas du tout présent dans le cache de l'appliance de destination.
- ❖ La distribution tient compte de l'expiration potentielle des données du cache si celui-ci est déjà plein.

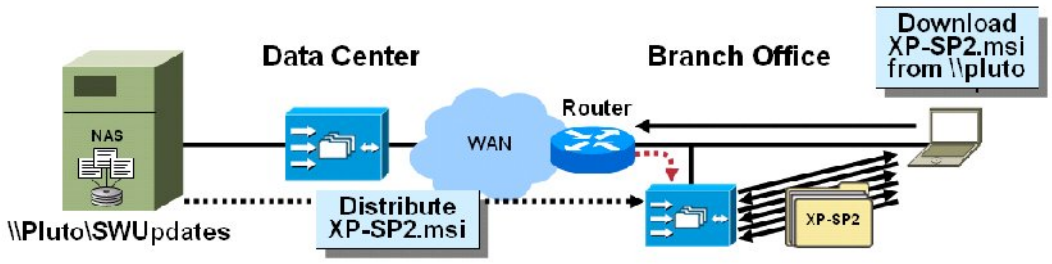


Fig III.11 : Illustration du pré-positionnement de fichiers

III.3-Intégration et disponibilité du service WAAS :

III.3.1-Utilisation de la redirection avec WCCPv2 :

WCCP, ou Web Cache Communication Protocol**,** est un mécanisme disponible sur les routeurs Cisco depuis 1997, ainsi que sur certaines gammes de commutateurs. Il assure la redirection du trafic en temps réel vers un groupe de caches. Cela n'interfère pas avec le fonctionnement normal des routeurs et des commutateurs. WCCP permet de configurer des groupes de service, correspondant à des interceptions applicatives, auxquels viennent s'abonner tout équipement souhaitant recevoir ces flux. L'application à intercepter est caractérisée par son protocole de transport, UDP ou TCP, ainsi que par le numéro de port. Les bénéfices apportés par WCCPv2 concernant le service WAAS sont les suivants :

- Equilibrage de charge sur l'ensemble des WAE Edge du site distant
- Tolérance aux pannes d'un WAE

Les versions logicielles minimum par plateforme pour supporter WCCPv2 sont les suivantes :

- Routeur : IOS 12.0(3)T (version 12.2 ou supérieure recommandée)
- Catalyst 6500 (redirection L2) : IOS 12.1(2)E
- Catalyst 6500 / Sup720 (toute redirection) : IOS 12.2(18)SXD4
- Catalyst 4500 : supporté depuis la version 12.2(31)SG
- Catalyst 3750/3560 : à venir en Q1 2007

III.3.2 Gestion des flux intercepté :

WCCP offre un mécanisme d'équilibrage de charge simple et performant en fonction de l'adresse IP source et / ou destination des flux interceptés. Ce partage de charge peut évoluer dynamiquement pour prendre en compte aussi bien l'introduction de nouvelles appliances pour ajouter de la capacité de traitement, que la perte de toutes les appliances.

Le routeur cherche en permanence à répartir un lot de 256 jetons de charge entre tous les WAE qui se sont abonnés à un service de redirection donné. S'ils sont au nombre de 3 et qu'aucune pondération particulière n'est paramétrée, le routeur attribuera 85 jetons à chacun d'entre eux (figure III.12) : de 1 à 85 pour le premier, de 86 à 170 pour le second et de 171 à 255 pour le dernier. L'appliance qui traitera un flux donné est simplement déterminé en passant l'adresse IP source et/ou destination dans une fonction de hachage qui retourne une valeur entre 1 et 256, correspondant à un numéro de jeton. Le WAE choisi par le routeur est celui à qui le jeton a été attribué. La fonction de hachage garanti qu'un même flux passera toujours par le même WAE (à moins d'un changement dans le nombre d'appliances disponibles). Si l'un des 3 WAE de l'exemple précédent vient à être retirer de l'architecture, le routeur constate automatiquement sa disparition et répartit à nouveau les jetons entre les 2 appliances restantes.

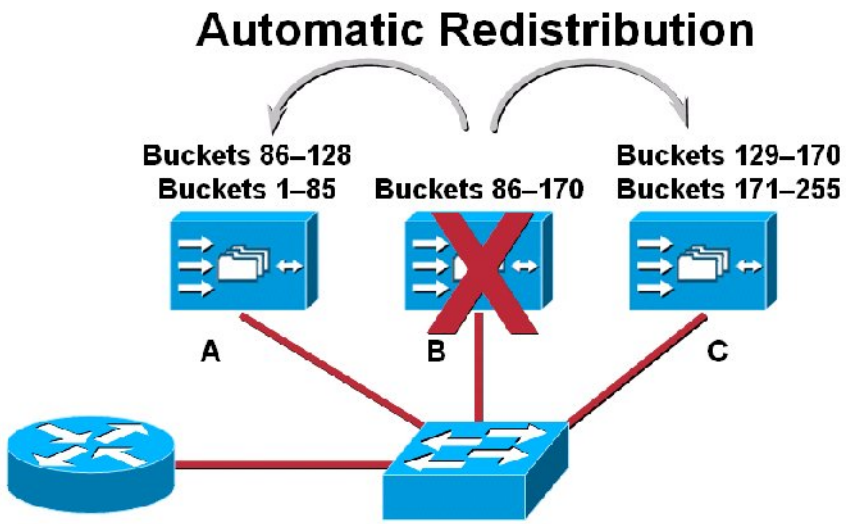


Fig III.12: Algorithme de partage de charge WCCP

Lorsqu'aucun WAE n'est enregistré à un service donné, ou lorsque tous les WAE ont été retirés, le routeur arrête automatiquement l'interception et transmet le trafic directement au travers du WAN**.** De cette manière, en cas de panne des appliances, le trafic n'est plus optimisé mais le service continue de fonctionner.

III.3.3-Fonctionnement de l'interception WCCP :

Lors de l'accès aux fichiers, les étapes sont les suivantes**:**

Le client initie la communication vers le serveur de fichiers.

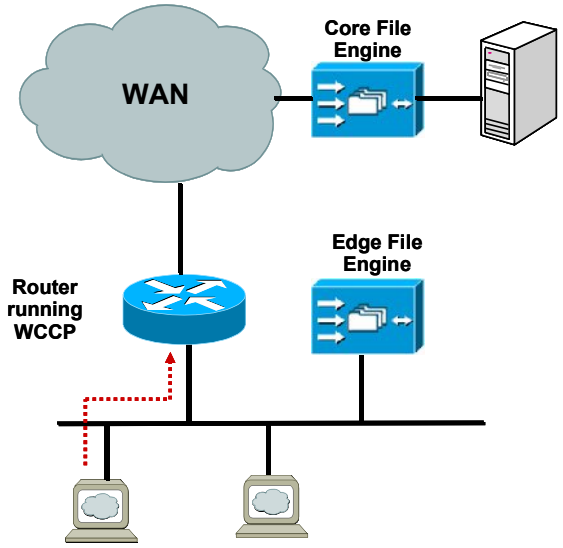


Fig III.13 : Requête initiale

Le routeur intercepte le flux et le redirige vers le WAE Edge. Le paquet original est encapsulé dans une trame GRE à destination du WAE Core pour ne pas modifier l'adresse IP source. Les commutateurs tels que les Catalyst 6500 et Catalyst 4500 peuvent également faire de la redirection de niveau 2 sans altérer les adresses IP de la trame. Par contre, cette seconde solution nécessite une connexion directe des WAE sur le commutateur.

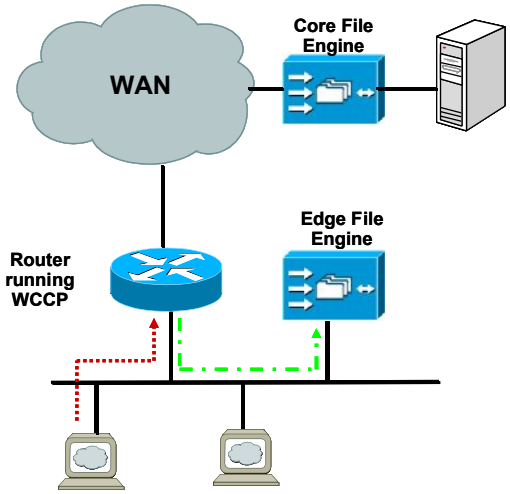


Fig III.14 : Interception WCCP

Dans le cas où la donnée est présente dans le cache de l'Edge (cache hit), celle-ci est fournie directement par celui-ci. Sinon, la donnée est récupérée du serveur de fichier (cache miss).

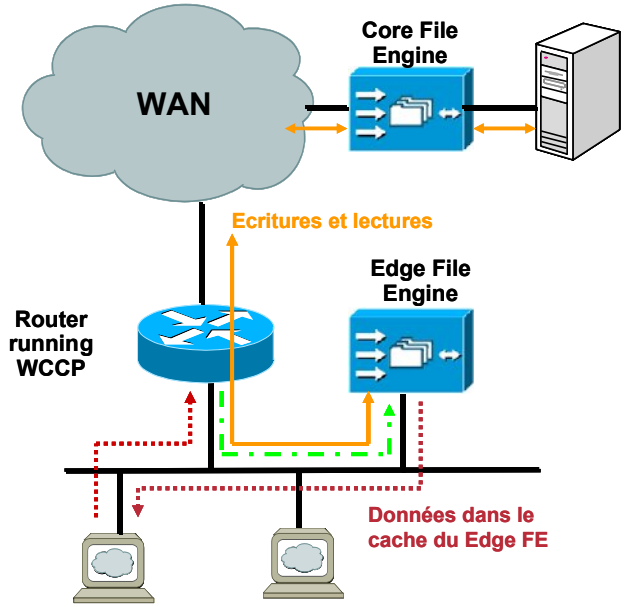


Fig III.15: Propagation de la requêtes en central en cas de "cache miss"

III.4-Mécanisme d'Auto-Discovery des WAE :

L'une des grandes forces de la solution d'optimisation WAAS de CISCO repose sur une intégration et une gestion transparente des données sur le réseau, à la différence d'un mode tunnel qui masque les informations nécessaires pour le traitement de politiques de sécurité, de QOS…

En plus des mécanismes d'intégration transparente décrits dans les chapitres précédents, la solution WAAS possède aussi un mécanisme d'auto-découverte des WAE qui sont entre un client et un serveur lors de l'ouverture d'une session TCP. Cette auto-découverte permet ainsi de s'affranchir de toute une phase de configuration qui nécessiterai de définir les possibles relations entre des couples de WAE. Il est à noter que pour la partie CIFS, il est nécessaire de configurer les notions de connectivité entre les WAE qui servent de Edge et ceux qui servent de Core.

Cette auto-découverte est réalisée à l'ouverture de la session TCP entre un client et un serveur, dans la phase de négociation TCP (three-wayhandshake : Syn – SynAck – Ack), ou les WAE utilisent une option TCP pour se découvrir et négocier les capacités de traitement de l'application qui sont possible (TFO, DRE, LZ) entre les WAE les plus proches du client et du serveur.

Les deux figures ci-dessous représentent les différentes phases de cette auto-découverte :

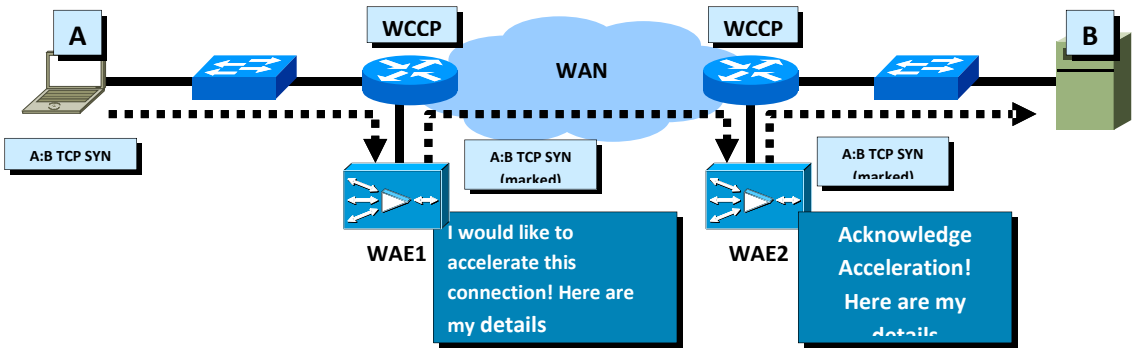


Fig III.16 : Auto-découverte, sens A vers B

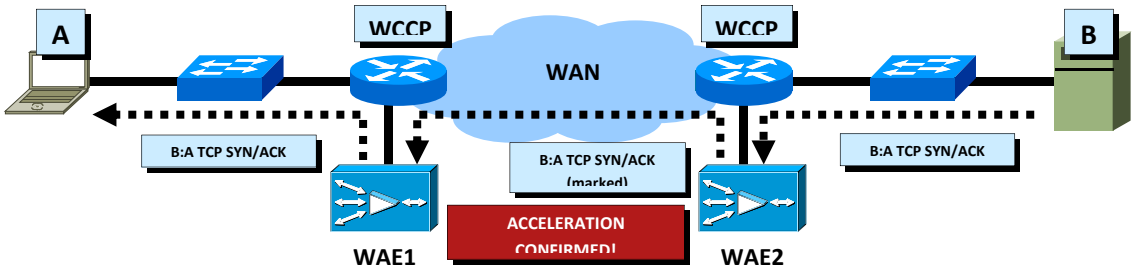


Fig III.17 : Auto-découverte, sens B vers A

Ce mécanisme d'auto-découverte permet aussi de faire en sorte que tout éventuel WAE intermédiaire entre les deux WAE les plus proches du client et du serveur, bypasse le trafic pour cette session sans traitement, qui serait inutile car déjà optimisé par le premier WAE. Le dernier avantage majeur de cette auto-découverte est qu'en cas de perte d'un WAE, ce mécanisme permet pour toutes les nouvelles sessions TCP de faire en sorte que le seul WAE qui reste sur le chemin des flux ne fasse aucun traitement d'optimisation sur la session car il n'y a plus de WAE distant pour faire l'optimisation inverse, et cela de façon dynamique et en temps réel.

Conclusion :

Associées avec WCCPv2, les appliances WAAS offrent une garantie de transparence lors de l'implémentation, mais aussi assurent la disponibilité de service d'optimisation des accès fichiers. le déploiement de plusieurs appliance sur chaque site agence assure la tolérance aux pannes d'un boîtier ; dans le cas où tous les éléments WAAS seraient inopérants, la transparence de l'implémentation, grâce entre autre à WCCP mais aussi au mécanisme d'AutoDiscovery, assure la continuité des sessions TCP mais sans les bénéfices apportés par le service WAAS.

Chapitre 4 :

Administration WAAS

L'ensemble des appliances WAAS déployées sur le réseau d'Entreprise est administré par le WAAS Central Manager.

IV.1-WAAS Central Manager :

WAAS Central Manager est installé sur une appliance de type WAE-512 dédiée. Lors de l'initialisation des boîtiers Core (site central) et Edge (site agence), l'adresse IP correspondant à l'appliance WAAS Central Manager est indiquée de manière à mettre en relation l'ensemble des boîtiers avec l'outil d'administration central.

L'interface d'administration est de type HTML et peut être accédée depuis n'importe quel point d'accès au réseau en HTTPS. Le Central Manager propose également une CLI évoluée de type IOS permettant de configurer la majorité des fonctions du système.

IV.1.1-Authentification:

Le Central Manager ainsi que les WAE arrivent par défaut avec un login administrateur. Il est aussi possible d'ajouter deux types de comptes supplémentaires :

- Device-Based CLI account : ce type de compte fournit uniquement un accès CLI à un Device (WAE) ou à un groupe de WAE.
- Roles-Basedaccount : ce type de compte permet d'administrer et de configurer certaines fonctionnalités de WAAS (complètement paramétrables par l'administrateur principal) à travers l'interface graphique du Central Manager. En plus de la restriction au niveau fonctionnalité, on associe à ce compte un domaine qui peut être la totalité ou un sous-ensemble des WAE de l'architecture.

Pour les comptes Roles-Based, on peut aussi autoriser ou non ces comptes à accéder au CLI des WAE de son domaine.

Il existe aussi pour chaque type de compte 2 types de privilèges :

- Accès complet et modification des configurations
- Accès en visualisation uniquement

IV.1.2-Directives de connectivité :

Les directives de connectivité correspondent à la mise en relation d'un WAE Edge avec un WAE Core. Elles sont nécessaire à la publication des partages / points de montage du serveur de fichiers sur le WAE Edge.

Les paramètres à définir sont les suivants :

- Core WAE (ou cluster)
- Edge WAE (ou groupe)
- Utilisation du WAN
    - Bande passante allouée maximum
    - Latence moyenne

IV.1.3-Paramétrages pour les serveurs de fichiers :

Les différents paramètres de communication entre les Core et les Edge sont effectués dans WAAS Central Manager :

- File Blocking : blocage de l'optimisation pour certains types de fichiers
- File prepositionning : mise à disposition des données dans le cache de l'Edge de manière planifiée pour optimiser les temps d'accès
- Policy distribution : tous les paramètres peuvent être transmis sur l'ensemble des WAE lors du déploiement de l'infrastructure

IV.2-Exemples d'applications optimisées :

IV.2.1-Optimisation de WAAS sur Lotus Notes :

Lotus Notes est une suite d'application qui offre des solutions performantes aux entreprises pour communiquer, collaborer et augmenter leur productivité. Cependant, les organisations IT s'attaquent aujourd'hui à la question de fournir des niveaux acceptables de performances et de service pour les utilisateurs de succursale qui accèdent aux serveurs Lotus Notes à travers un raccordement de type WAN.

Ces applications sont très largement impactées par la faible bande-passante, le délai important, ainsi que la perte de paquets rencontrés sur ce type de lien.

Cisco WAAS 4.0 fournit une solution qui peut atténuer plusieurs de ces problèmes d'exécution en utilisant un ensemble robuste de techniques d'accélération et d'optimisation sur les liens WAN.

Tous les tests exécutés ci-dessous sur Lotus Notes ont été réalisés sur un lien T1 (1.544-Mbps) avec 80mS de latence aller-retour. En outre, la compression a été désactivée sur les serveurs et

clients Lotus Notes afin de profiter pleinement des mécanismes d'optimisation de Cisco WAAS. On notera également que les serveurs sont ainsi libérés des tâches de compressions.

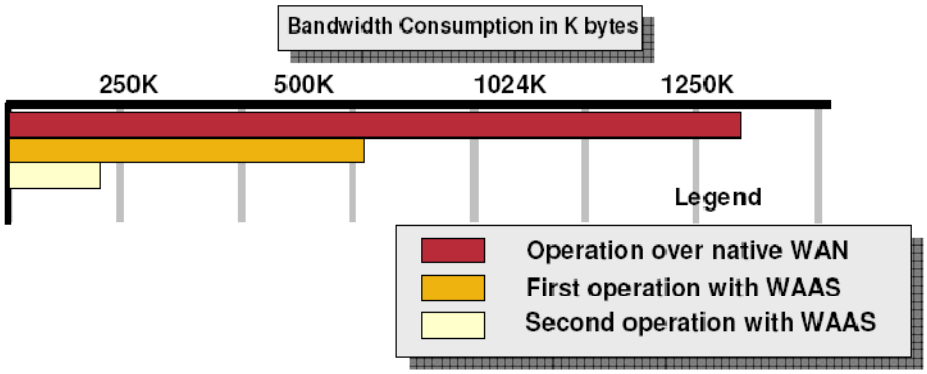


Fig IV.1: La bande passante consommée lors de l'envoi d'email avec un attachement de 600 KB

La figure ci-dessus montre l'économie immédiate de bande passante grâce à la mise en œuvre des technologies de compression sur la session Lotus Notes

La retransmission de cet email avec le même attachement, ou, avec ce même attachement après modification, consomme peu de bande passante grâce cette fois à l'utilisation des technologies de cache DRE «Data Redundancy Elimination »

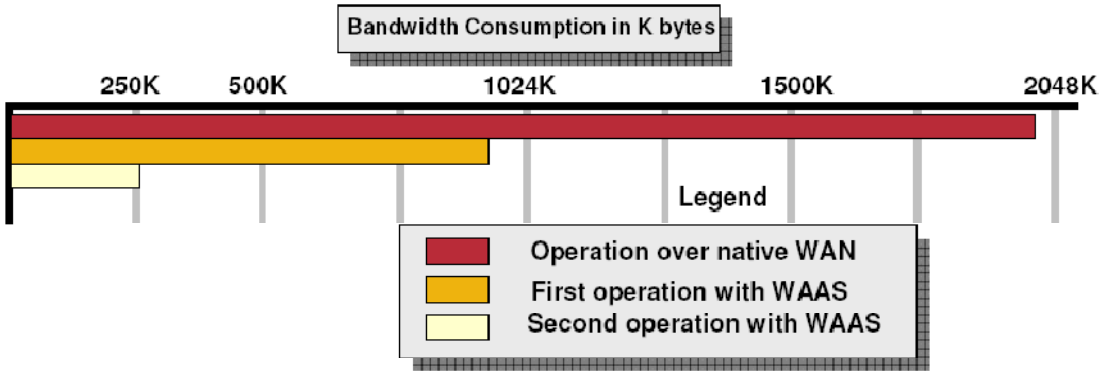


Fig IV.2 : Envoi d'email avec un attachement de 1MB Email.

Nous constatons ici encore que la combinaison des fonctions d'optimisation fournies par Cisco WAAS (persistent session-based LZ compression and DRE) permettent une économie significative de la bande passante.

On montre ci-dessous l'amélioration du temps de réponse apporté par Cisco WAAS lors de l'envoie d'un attachement de 5MB

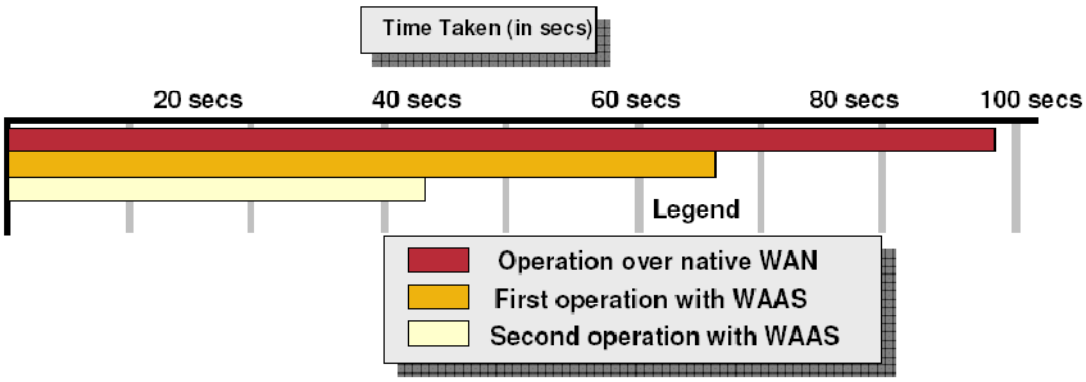


Fig IV.3: Temps de réponse Lotus Notes Send of a 5MB Email and Attachment

Cisco WAAS démontre une amélioration importante des performances dans l'environnement Lotus Notes pour l'envoi de pièces attachées de différentes tailles. Le gain concerne à la fois sur la bande passante consommée sur le lien WAN que le temps de réponse pour les utilisateurs distants.

Nous avons constaté que ces améliorations pouvaient aller jusqu'à 85% de réduction de la bande passante consommée, et un temps de réponse pouvant être divisé par 4. Il est aussi important de noter que ces améliorations sont réalisés sans aucun changement coté client et serveur et n'apportent aucun risque sur l'intégrité des données.

IV.2.2-Optimisation de WAAS sur Citrix :

IV.2.2.1-Performance de l'optimisation Citrix :

Lorsqu'un client Citrix accède à une application à travers le serveur Citrix, Cisco WAAS améliore les performances et réduit l'utilisation de la bande passante, fournissant ainsi de meilleurs temps de réponse tout en diminuant l'utilisation des liens WAN.

Optimisé pour les environnements WAN, le protocole ICA comporte lui-même des mécanismes de gestion de file d'attente pour les mouvements de souris, de cache bitmaps, et de compression

du trafic. Cependant, Cisco WAAS apporte des améliorations supplémentaires sur l'optimisation du lien WAN, grâce aux mécanismes DRE, LZ compression, et TFO, comme décrit précédemment.

En utilisant Cisco WAAS pour optimiser les flux Citrix, les entreprises peuvent réduire jusqu'à 85% la bande passante consommée sur les liens WAN en compressant les flux Citrix n'étant pas déjà compressé, et jusqu'à 50% de réduction de bande passante comparé au flux Citrix compressé nativement. Dans le test décrit ci-dessous, un client et un serveur Citrix ont été déployé sur des sites différents séparés par un lien T1 avec 80 ms de RTT.

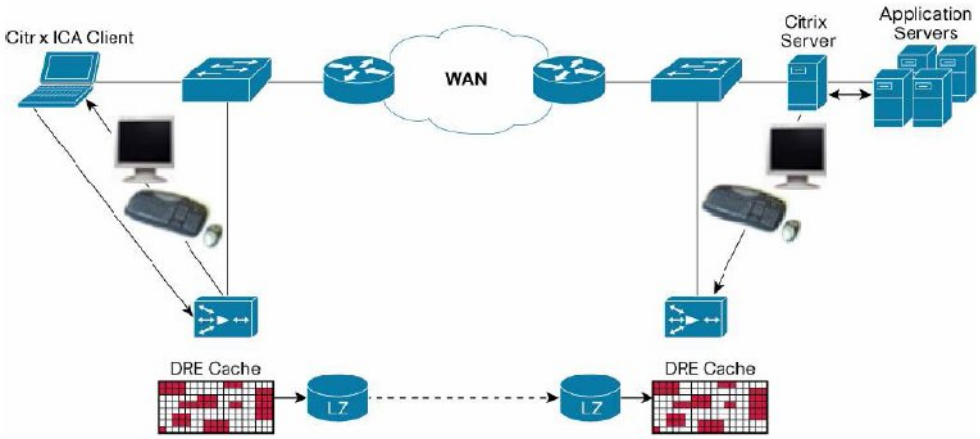


Fig IV.4 : Test de compression des flux Citrix

L'environnement de test comprenait un serveur Citrix version 4 tournant sur un Windows Serveur 2003. Les applications accédées étaient également installées sur un serveur Windows 2003 avec IIS version 6. Les applications testées étaient relativement standards, Microsoft Word, Excel, Web content, et Macromedia Flash Player.

Le poste client était un Windows XP Pro SP2 équipé du client Citrix ICA version 9.

La figure ci-dessous montre l'amélioration apportée par Cisco WAAS comparativement aux flux natif Citrix compressé et non compressé.

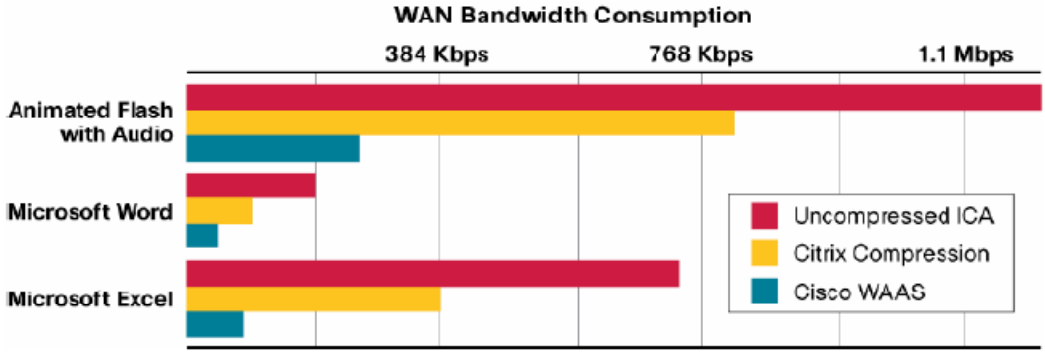


Fig IV.5: Optimisation Citrix réalisé avec Cisco WAAS

Comme le montre la figure ci-dessus, Cisco WAAS délivre une réduction significative du flux Citrix, et une compression plus efficace que ce que peut réaliser Citrix nativement.

IV.3-La mise en œuvre de la solution WAAS :

IV.3.1-Les équipements utilisés dans chaque site :

- Le Site Centrale (SC) est constitué de :
  - un routeur de Cisco 7200
  - un switch 2960 (24 ports Fastethernet et 2 ports Gigabitethernet)
  - serveurs (FTP.CIFS.HTTP.HTTPS. Messagerie).
  - WAE- 7326
  - WAE -512MGT (centrale manager)
  - serveur de base de données
- Le Centre de Calcule(CC) de Tizi-Ouzou est constituée de :
  - pc
  - serveur de base de données
  - un switch 2960 (24 ports fastethernet et 2 ports Gigabitethernet)
  - WAE 500
  - un routeur Cisco 3845
- Le Centre Payeur de Tizi-Ouzou est constitué de :
  - Un routeur Cisco 2900
  - une carte NME-NCE 512 K 9
  - switch un switch 2960 (24 ports Fastethernet et 2 ports Gigabitethernet)
  - PC

IV.3.2-Objectifs :

1. Faire un test d'application dans un réseau sans l'intégration du WAAS et observation de l'état de la latence du réseau.
2. Intégration de la solution Cisco WAAS dans le réseau non optimisé avec la configuration des équipements suivant :

IV.3.3-Adressage :

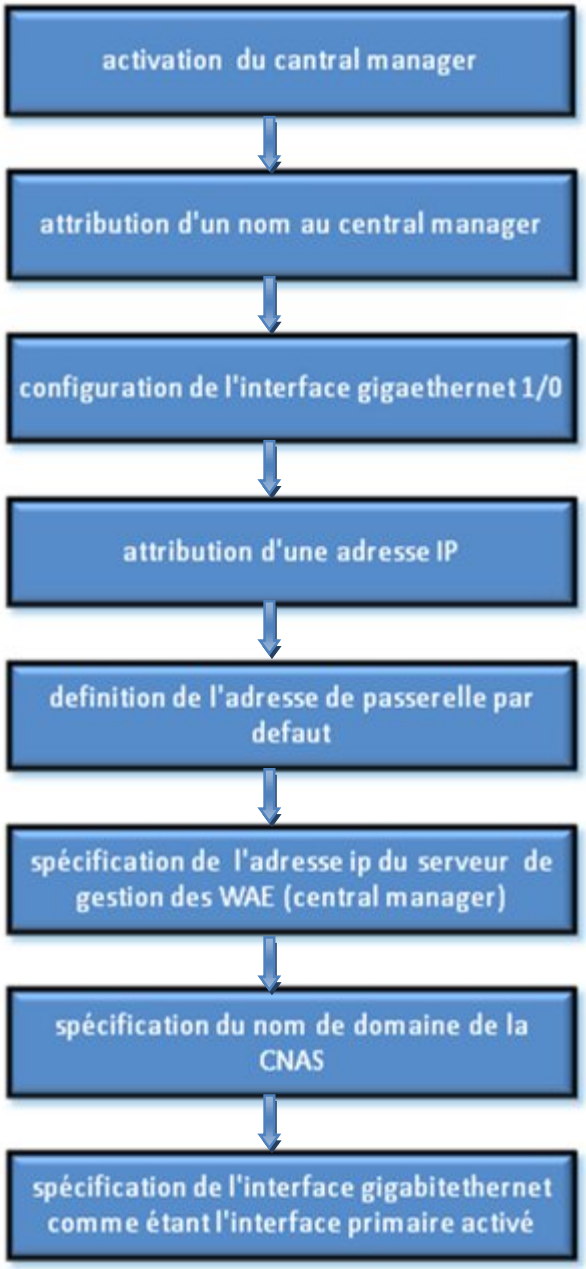
site	équipements	Interface	Adresse IP	Masque de sous réseau	Passerelle par défaut
ALGER	Routeur	Gigabitethernet 0/0	10.116.1.2	255.255.255.0	N/A
		Gigabitethernet 0/2	10.77.16.1	255.255.255.252	N/A
		Serial 0/0/0	10.40.1.1	255.255.255.252	N/A
	WAAS	Gigabitethernet 2/0	10.77.16.2	255.255.255.252	10.77.16.1
Centre de calcul Tizi-	Routeur	Gigabitethernet 0/0	10.115.1.2	255.255.255.0	N/A
		Gigabitethernet 0/2	10.77.15.1	255.255.255.252	N/A
		Serial 0/0/0	10.40.1.2	255.255.255.252	N/A
		Serial 0/0/1	10.40.2.1	255.255.255.252	N/A

Ouzou	WAAS	Gigabitethernet 2/0	10.77.15.2	255.255.255.252	10.77.15.1
Centre payeur de Tizi-Ouzou	Routeur	Gigabitethernet 0/0	10.115.2.2	255.255.255.0	N/A
		Gigabitethernet 0/2	10.77.15.5	255.255.255.252	N/A
		Serial 0/0/1	10.40.2.2	255.255.255.252	N/A
	WAAS	Gigabitethernet 1/0	10.77.15.6	255.255.255.252	10.77.15.5
Pc ALGER		Gigabitethernet	10.116.1.3	255.255.255.0	10.116.1.2
Pc Tizi-Ouzou		Gigabitethernet	10.115.1.3	255.255.255.0	10.115.1.2
Pc centre payeur		Gigabitethernet	10.115.2.3	255.255.255.0	10.115.2.2

Table IV.1 : Tableau récapitulatif d'adressage

IV.3.4-Configuration :

CONFIGURATION DE CENTRALE MANAGER :


activation du cantral manager
attribution d'un nom au central manager
configuration de l'interface gigaethernet 1/0
attribution d'une adresse IP
definition de l'adresse de passerelle par defaut
spécification de l'adresse ip du serveur de gestion des WAE (central manager)
spécification du nom de domaine de la CNAS
spécification de l'interface gigabitethernet comme étant l'interface primaire activé

configuration de routeur:

configuration pour SC et CC:

1-configuration des mots de passes (accès en mode console,mode privilégié,accès à distance)

2-attribution des noms aux routeurs

3-configuration des interfaces serials :

SC : serial 0/0/0 :

attribution d'une adresse IP

ajout d'une description a l'interface

spécification du signal horloge

activation de l'interface

CC : serial0/0/0 :

attribution d'une adresse IP

ajout d'une description a l'interface

spécification du signal horloge

activation de l'interface

serial0/0/1:

attribution d'une adresse IP

ajout d'une description a l'interface

spécification du signal horloge

activation de l'interface

4-configuration des interfaces gigaethernet 0/0 (LAN) et gigabitethernet 0/2(WAAS) :

attribution d'une adresse IP

ajout d'une description a l'interface

activation de l'interface

5-configuration des routes statique entre les trois sites (SC,CC,CP)

activation du routage sans class

6-configuration du protocole de routage dynamique RIP v 2

choix de la version 2 de RIP

spésification du l'adresse reseau géré par RIP v2

désactivation du résumé automatique d'adresse IP

configuration du protocole de redirection WCCP sur les deux interface (Gigabitethernet0/0,Gigabitethernet 0/2)

7-sauvgarde

configuration pour CP:

1-configuration des mots de passes (accès en mode console,mode privilégié,accès à distance)

2-attribution des noms aux routeurs

3-configuration de l'interface serial 0/0/1 :

attribution d'une adresse IP

ajout d'une description a l'interface

spécification du signal horloge

activation de l'interface

4-configuration des interfaces gigaethernet 0/0 (LAN) :

attribution d'une adresse IP

ajout d'une description a l'interface

activation de l'interface

5-Configuration des routes statique entre les trois sites (SC,CC,CP)

activation du routage sans class

6-configuration du protocole de routage dynamique RIP v 2

choix de la version 2 de RIP

spésification du l'adresse reseau géré par RIP v2

désactivation du résumé automatique d'adresse IP

configuration du protocole de redirection WCCP sur les deux interface (Gigabitethernet0/0,interface integrated service engin 1/0)

7-configuration de l'interface integrated service engin 1/0 (WAAS) :

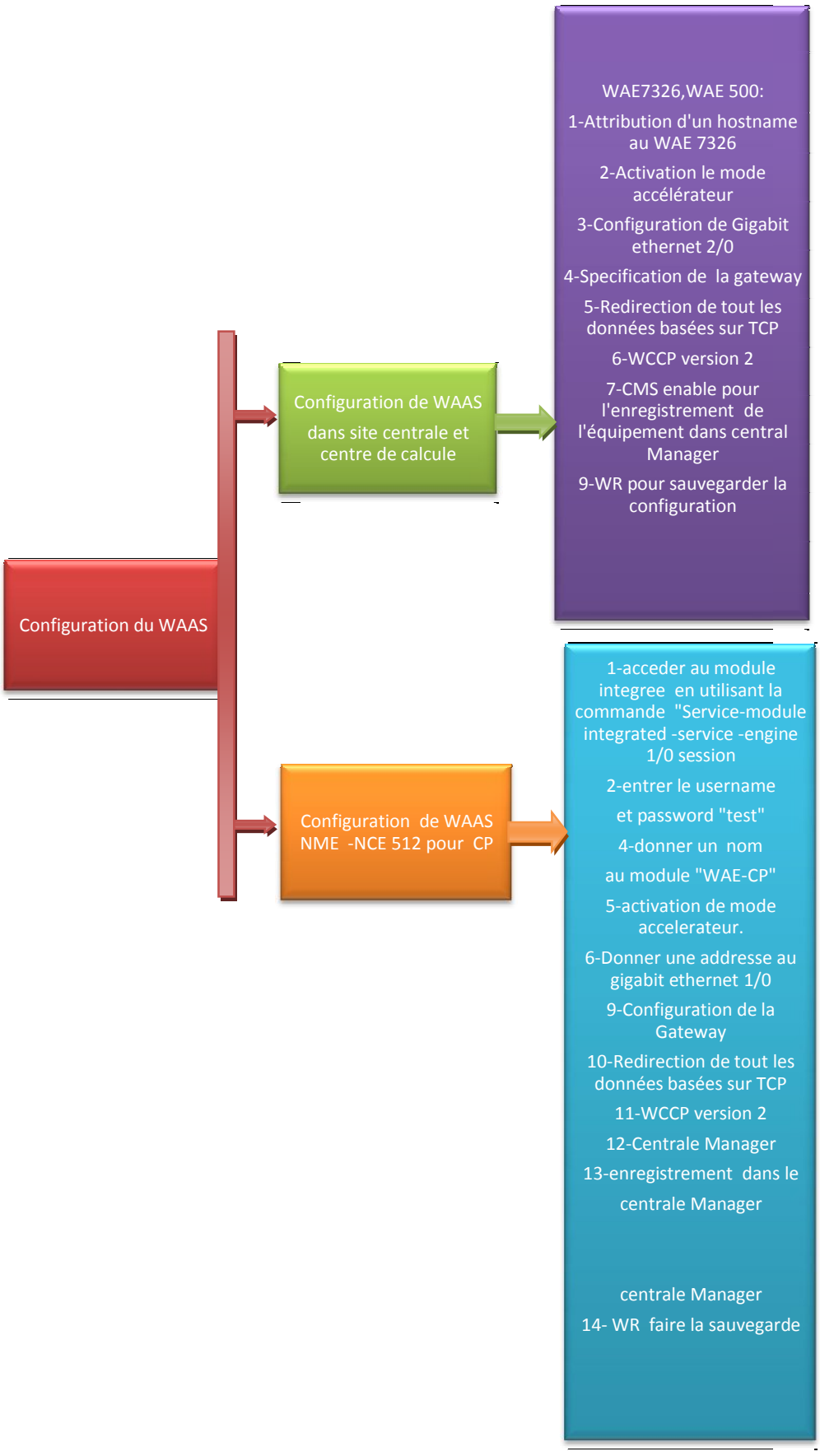
attribution d'une adresse IP coté routeur

activation de l'interface

attribution d'une adresse IP coté WAAS

spécification de la passerelle par defaut du module intégré WAAS

8-sauvgarde



IV.3.5-Le contrôle d'opération de Cisco WAAS en utilisant le Central Manager :

- On se connecte au poste de travail relié au Centrale Manager .
- On ouvre le navigateur Web internet explorer à l'adresse HTTPS:\\10.77.16.5 :8443 celle du centrale Manager.
- On se connecte au Centrale Manager et la page d'ouverture de ce dernier nous donne l'accès aux différentes fonctions :

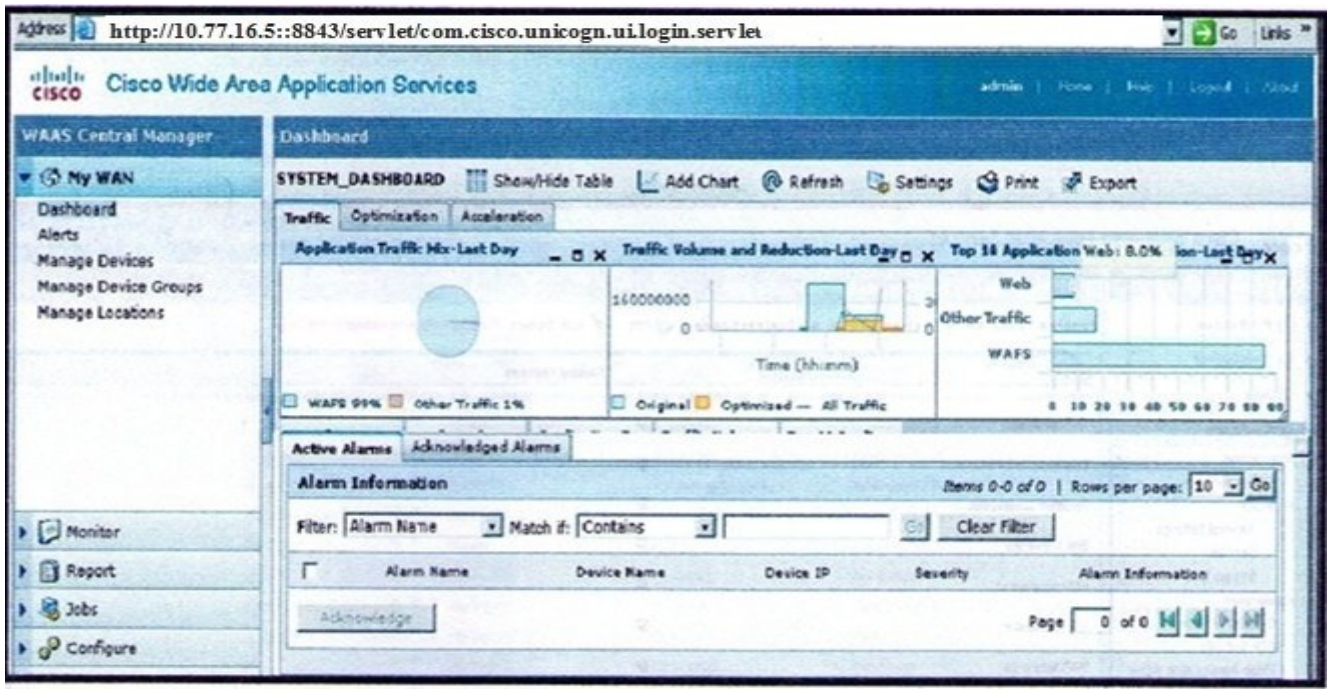


Fig IV.6 : La page d'ouverture du centrale manager

Fig IV.7 : Vérification de l'état des appliances

- Les fonctions d'accélération :

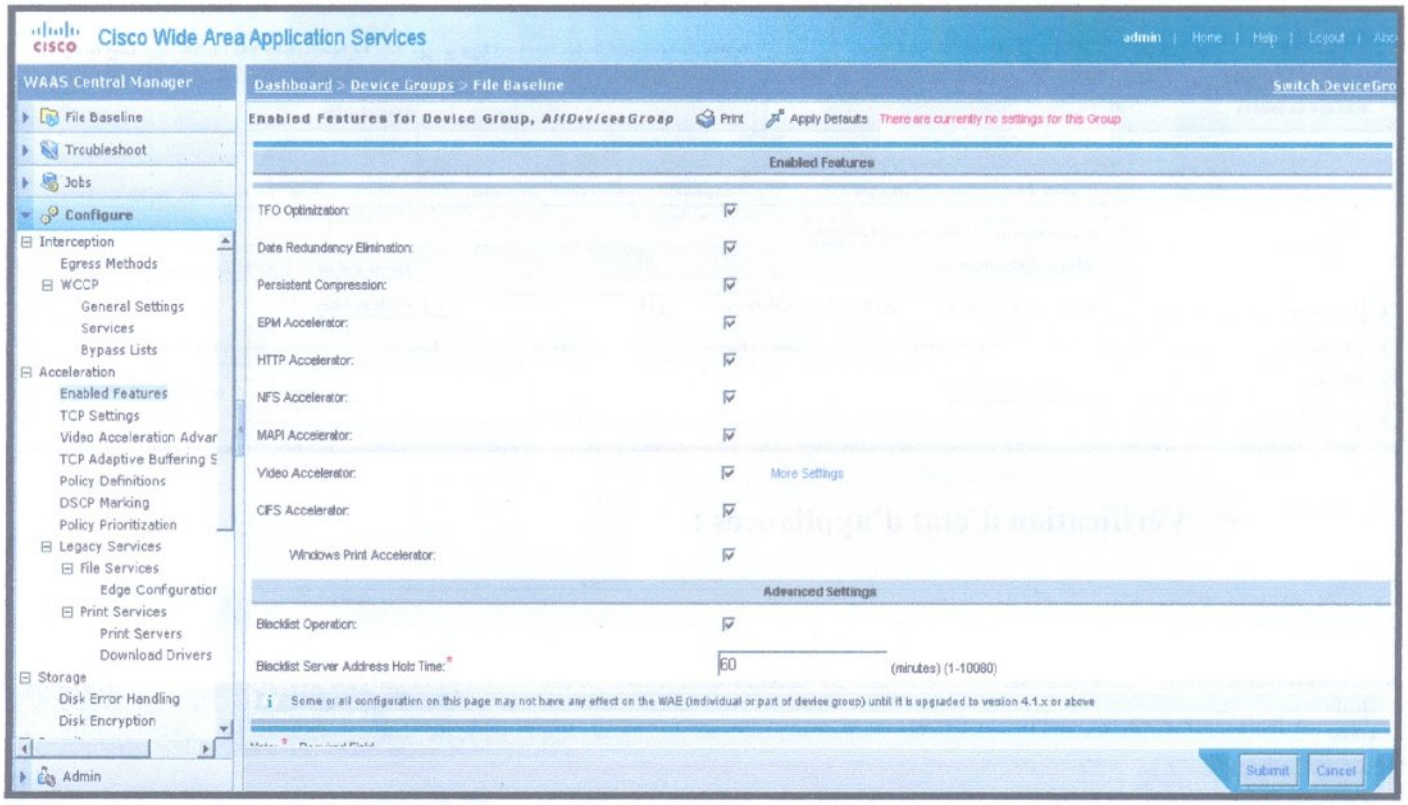


Fig IV.8: Les fonctions d'accélérations

- Application traficpolicy :

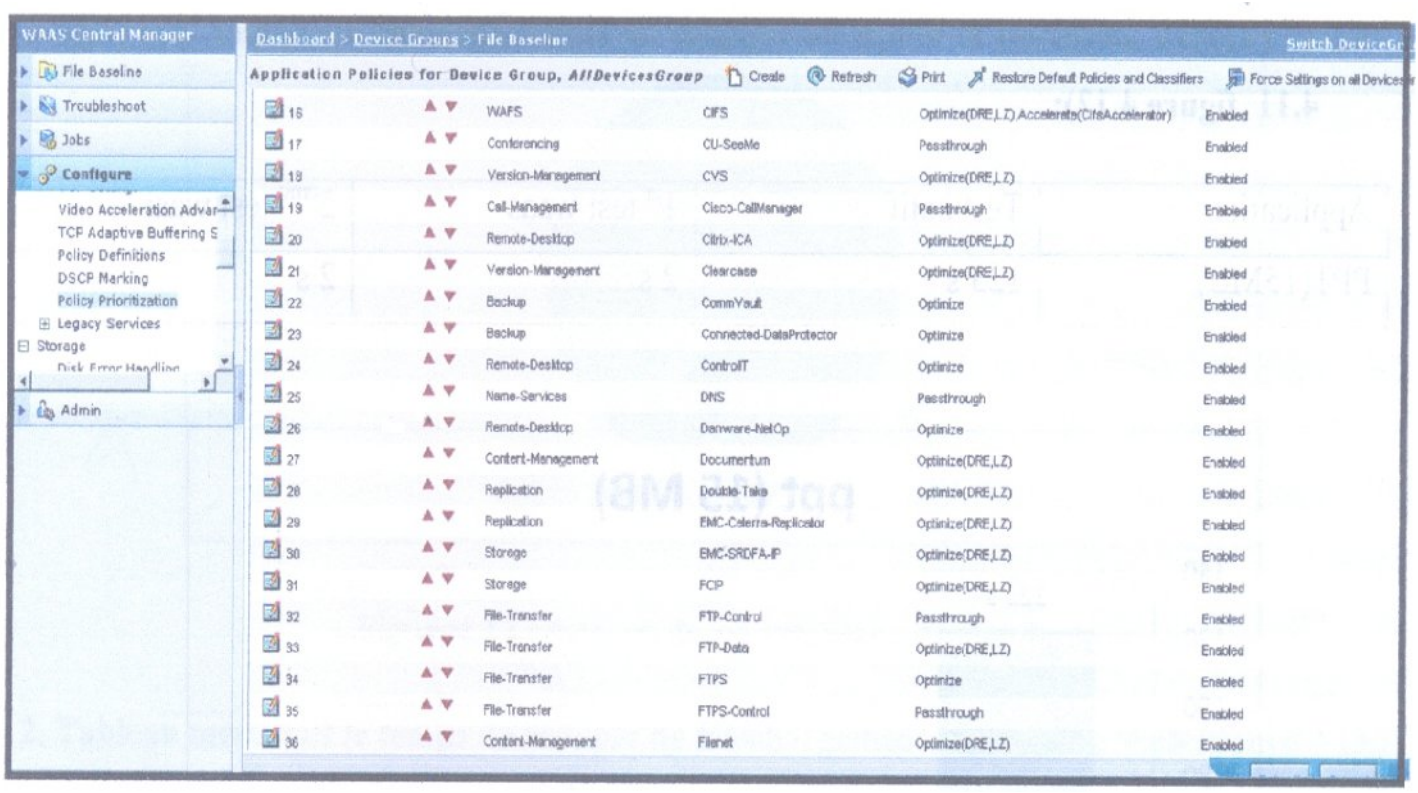


Fig IV.9: Application trafic policy

- Les applications configuré et traité par le WAAS :

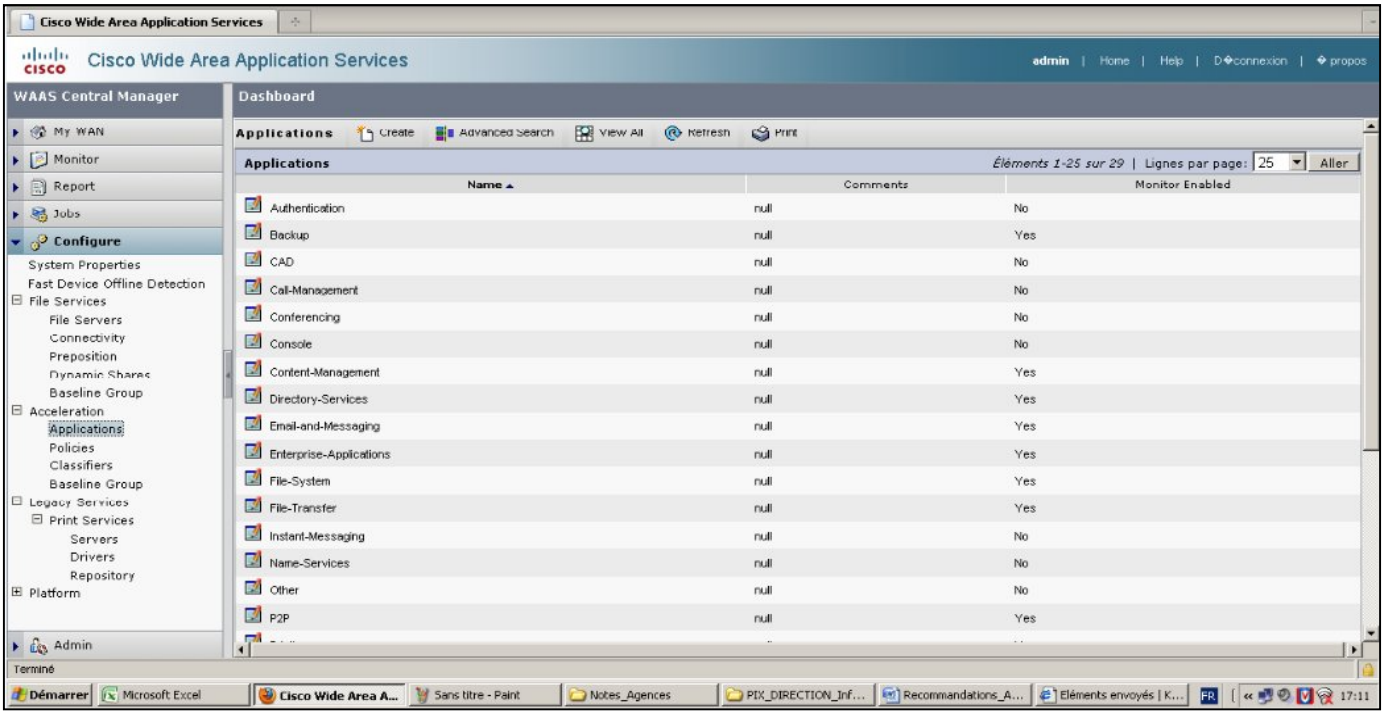


Fig IV.10: Les applications configuré et traité par le WAAS.

IV.3.6-Test de téléchargement d'une page Web :

IV.3.6.1-Téléchargement de la page Web sans le WAAS :

- On accède à Mozilla Firefox.
- On efface l'historique avec la commande: TOOL\clearprivate Data ou ctrl +shift+Del .
- On se connecte à l'adresse http ://10.10.100.100/index1.html ,on télécharge la page Web puis on estime le temps de téléchargement.

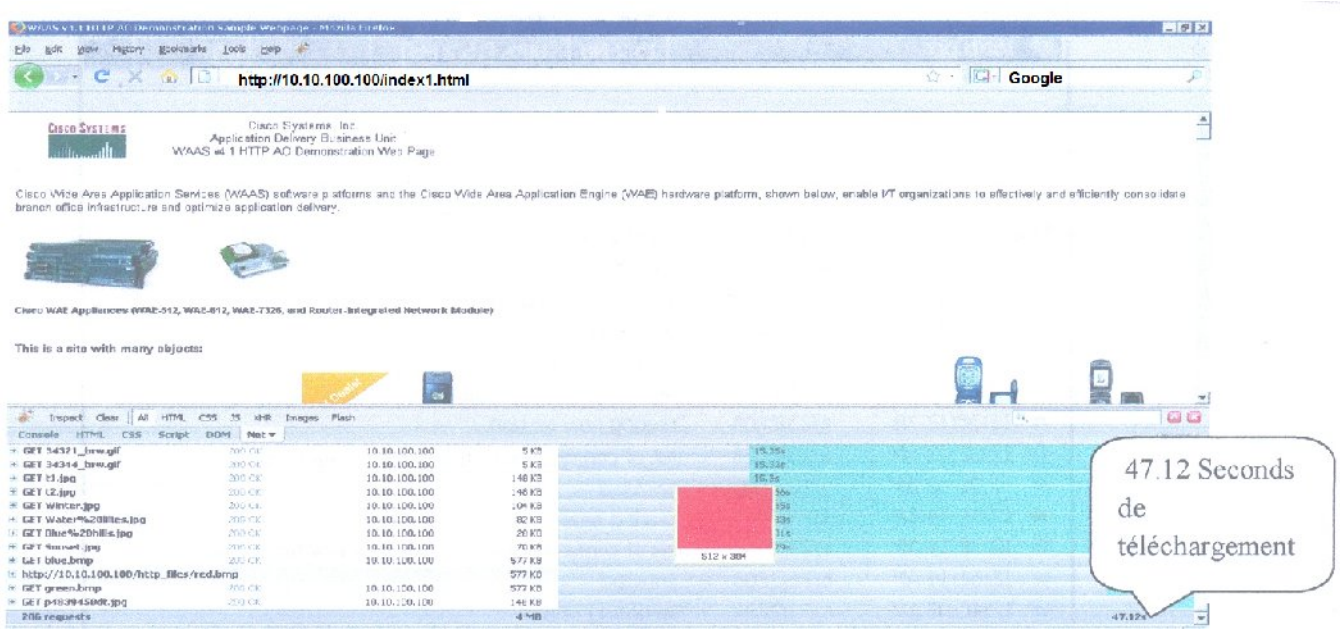


Fig IV.11: Le temps de téléchargement d'une page Web

- On efface l'historique avec la commande : TOOL\clearprivate Data ou ctrl +shift+Del

IV.3.6.2-Téléchargement de la page Web avec le WAAS la première fois :

- On accede a Mozilla Firefox .
- On efface l'historique avec la commande: TOOL\clearprivate Data ou ctrl +shift+Del comme le montre la figure ci-dessous
- On se connecte à l'adresse http://10.10.100.100/index.html on télécharge la page pour une première fois (cold test) et enfin on estime le temps de téléchargement comme le montre la figure ci-dessous.

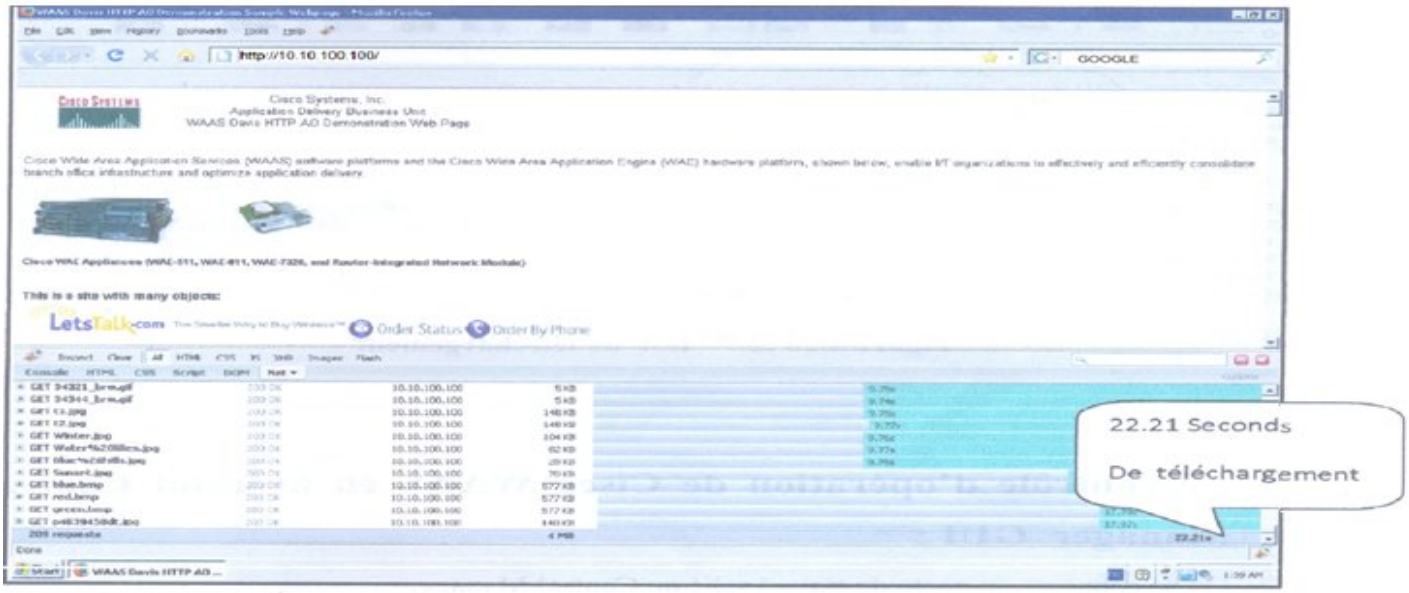


Fig IV.12: 1er test de téléchargement.

IV.3.6.3-Téléchargement de la page Web avec le WAAS la deuxième fois :

Fig IV.13: 2éme test de téléchargement

IV.3.6.4-Comparaison des temps de téléchargement des pages Web :

application	Test natif	1 er test WAAS	2éme test WAAS

Page Web (4MB)	47,12s	12,12s	15,12s

Table IV.2: Tableau récapitulative des temps de téléchargement des pages Web

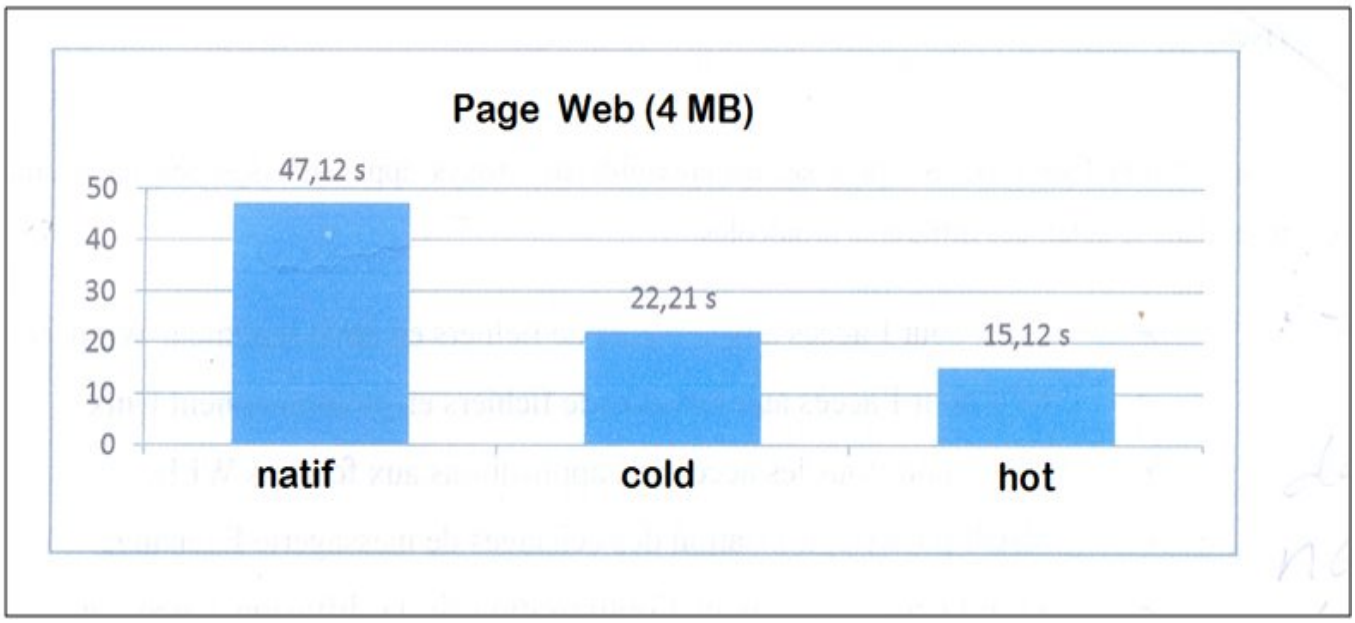


Fig IV.14 ::Mesure des temps de téléchargement

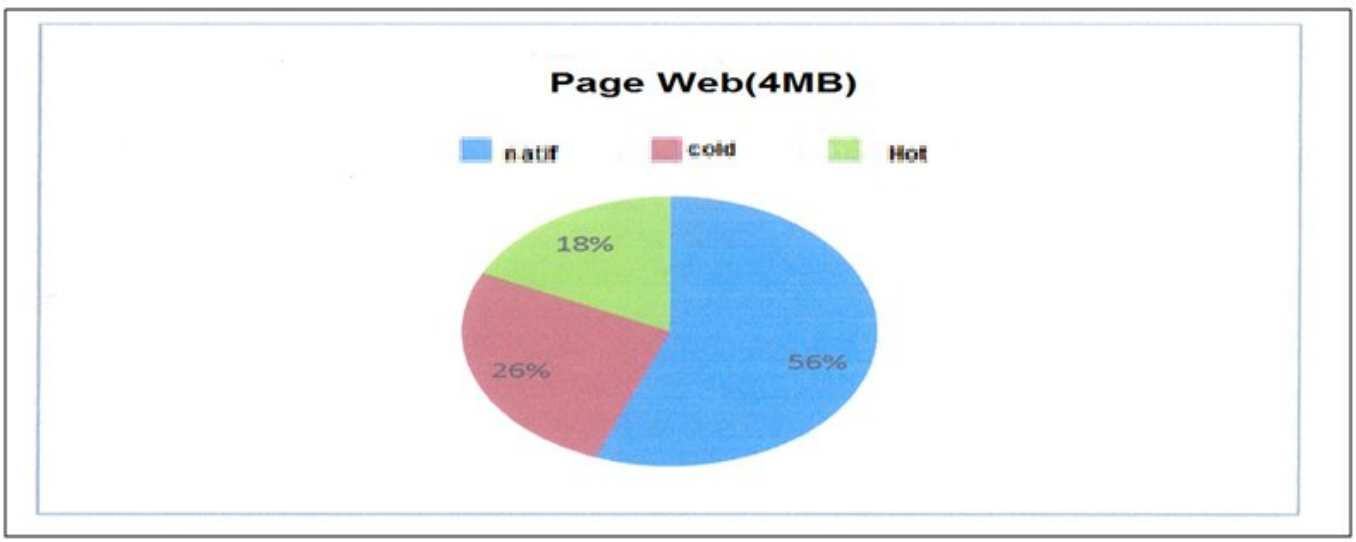
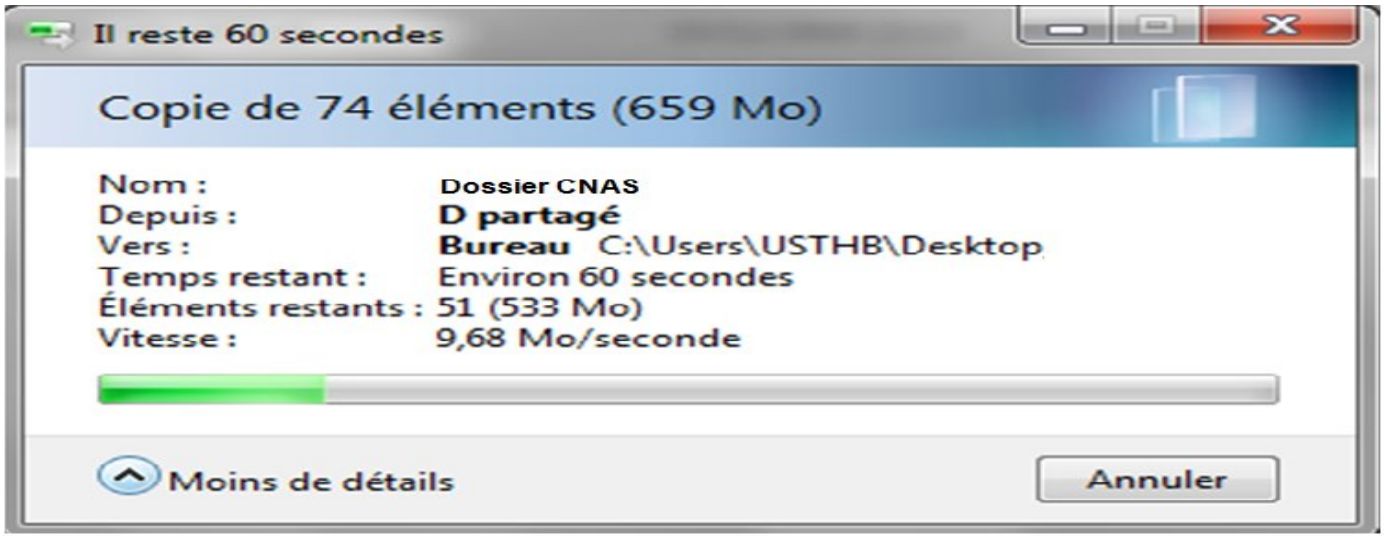


Fig IV.15: Mesure du pourcentage de téléchargement

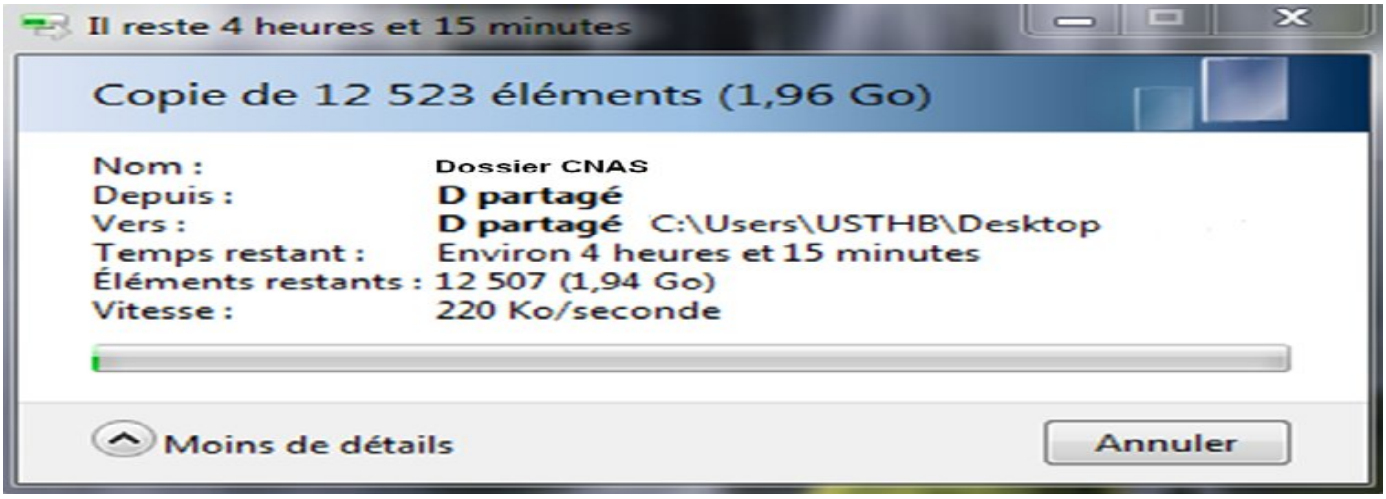
On constate une amélioration des temps de téléchargement grâce à l'exploitation efficace de la bande passante ainsi la latence est nettement diminué.

IV.3.7-Test de copie d'un fichier :

IV.3.7.1-avec l'implémentation du WAAS :



IV.3.7.2-sans l'implémentation du WAAS :



On constate une augmentation de débit grâce à l'exploitation efficace de la bande passante ainsi la latence est aussi nettement diminué.

Conclusion :

Durant notre étude nous avons découvert la technologie WAAS avec ses avantages en accélération d'application ,d'optimisation et de sécurité offrant des performances d'accès aux applications a travers le WAN similaire au LAN ,permettant l'exploitation efficace du réseau avec une intégration facile et transparente dans le réseau IP existant assurant une grande fiabilité et évolutivité ,le WAAS réduit les couts d'investissements en assurant une haute disponibilité des serveurs consolidés dans les Datacenters auparavant éparpiller dans les sites distants ,permettant ainsi une protection et une sauvegarde central des données .

Conclusion générale

Conclusion générale

Dans la partie Application de notre projet on a testé un transfert de fichiers sans le WAAS ensuite avec l'implémentation du WAAS, les résultats obtenus reflètent l'optimisation, l'accélération des applications, l'amélioration des performances Applicatives et l'utilisation de l'infrastructure WAN et la réduction des couts d'investissement de l'entreprise.

L'élaboration de notre projet nous a permis de découvrir la technologie WAAS et d'en savoir plus sur le déploiement d'un réseau informatique en termes d'installation, de configuration de routeurs , de Switch et d'administration de ces derniers ainsi que la configuration des équipements WAAS , d'adressage IP et de la mise en œuvre d'un réseau implémentant le WAAS. Notre projet nous a aussi permis de découvrir le Central Manager.

En perspectives, nous suggérons l'implémentation de la technologie WAAS sur tout le territoire national afin d'avoir une exploitation efficace en terme de bandes passante dans le but d'offrir à ses clients et ses prestataires « pharmacien, médecin.. »Une meilleure qualité de service.

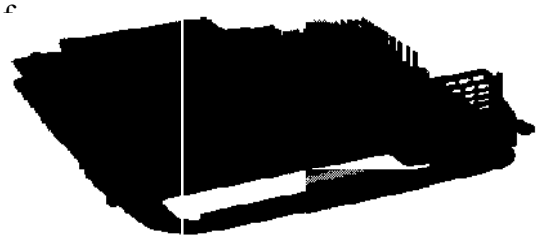
En plus, cette technologie nous offre la possibilité de vidéoconférence pour les réunions et la formation du personnel en utilisant le E-learning.

ANNEXE

APPLIANCE WAAS :

- **Carte NME-WAE :router integrated network module for the cisco integrated services router:**

  providescription the lowest Cap-ex and OPEX
  Integrates within the ISR ;addresses 80 percent of remote
  brunch offices.single processor system can be clustere with WCCPV2,PBR,and is supported in ISR mod 2811, 2821 ,2851, 3825 and 3845
  Model NME –WAE-302et 502 :Jusque 4M, 200/5 TCP connections, 80/120GB un Network Module (NM) pour les routeurs de la gamme ISR (28xx et 38xx)pour offrir les fonctions WAAS de manière complètement intégrée



- **WAE -7326:**

  dual- core processor, 4gb of Ram up to 155 mbps WAN connections and 7500 optimized TCP connecti 900 gb RAID1 protected and hot Swapable SCSI disk with optional disk encryption

- **WAE-512 appliance:**

  quad-core processor 8gb of Ram up to 310 mbps WAN connections and 1200 optimized TCP connections .Disk capacity with up to 900 gb RAID 5 protected and hot swapable SAS optional disk encryption

- **WAE -7341:**

  Dual quad –core processors 24 gb of RAM u To 1 gbps WAN connections and optimized TCP connections up to 1.5 TB"tera byte" RAID -5 protected and hot swapable SAS disk capacity with optional disk encryption

- **WAE -7371:**

Single processor system
with 250 gb of RAID-1protected SATA2di
capacity And optionnel disk encryption.1gb
memory configuration supports 8mbps WA
connections and 750 optimized TCP conne
2gb memory Configuration supports 20 mbps WAN
connections and 1500 optimized TCP connections.

Annexe B:

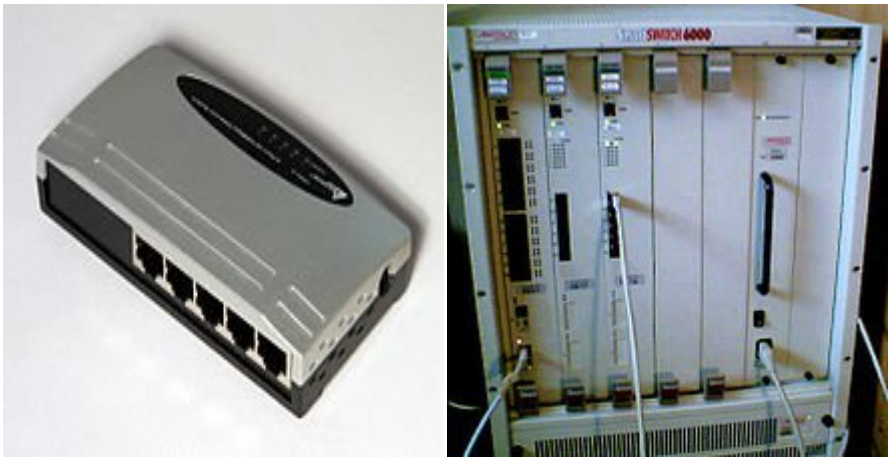
Routeur :

Routeur Wi-Fi

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. C'est un équipement de couche 3 du modèle OSI.

Il ne doit pas être confondu avec un commutateur (couche 2) ou une passerelle (couche 3 et supérieures).

Commutateur réseau :



Commutateur modulaire professionnel

Un commutateur réseau (ou switch, de l'anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines) . Il a donc la même apparence qu'un concentrateur (hub).

Contrairement à un concentrateur, un commutateur ne reproduit pas sur tous les ports chaque trame qu'il reçoit : il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs.

Contrairement à un routeur, un commutateur de niveau 2 ne s'occupe pas du protocole IP. Il utilise les adresses MAC et non les adresses IP pour diriger les données. Les commutateurs de niveau 2 forment des réseaux de niveau 2 (Ethernet). Ces réseaux sont reliés entre eux par des routeurs (ou des commutateurs de niveau 3) pour former des réseaux de niveau 3 (IP).

User Datagram Protocol(UDP) :

Le User Datagram Protocol (UDP, en français protocole de datagramme utilisateur) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport de la pile de protocole TCP/IP : dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP. Il est détaillé dans la RFC 768.

Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Contrairement au protocole TCP, il fonctionne en mode non-connecté : il n'existe pas de procédure de connexion préalable à l'envoi des données, et il n'y a pas de garantie de bonne livraison d'un datagramme à sa destination, l'ordre d'arrivée des datagrammes peut différer de l'ordre d'envoi. Il est également possible que des datagrammes soient dupliqués. Les fonctions assurant la retransmission et le réordonnancement doivent être assurées par les protocoles de la couche supérieure si elles sont souhaitées.

L'intégrité des données est assurée par une somme de contrôle, l'utilisation de celle-ci est cependant facultative en IPv4 mais obligatoire avec IPv6. Si un hôte n'a pas calculé la somme de contrôle d'un paquet émis, la valeur de celle-ci est fixée à zéro. La somme de contrôle inclut un pseudo en-tête qui inclut les adresses IP source et destination.

Exemples d'utilisation :

- les protocoles DNS, TFTP,
- le streaming
- les jeux en réseau (exemple : jeux de tir subjectifs)
- le programme traceroute,

Transmission Control Protocol(TCP) :

Transmission Control Protocol (littéralement, « protocole de contrôle de transmissions ») abrégé TCP, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793 de l' IETF.

Dans le modèle TCP/IP, TCP est situé au niveau de la couche de transport (entre la couche de réseau et la couche application). Les applications transmettent des flux de données sur une connexion réseau, et TCP découpe le flux d'octets en segments, dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).

Ports TCP ou UDP :

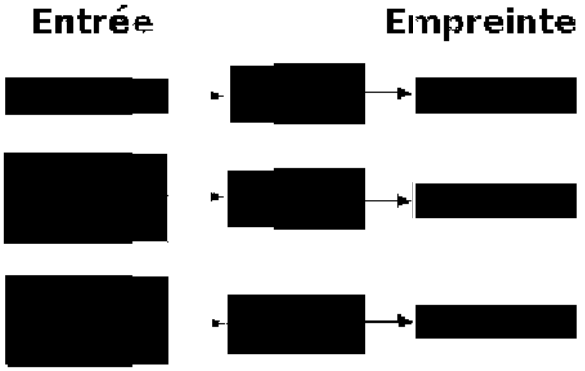
TCP (tout comme UDP) utilise la notion de numéro de port pour identifier les applications. À chaque extrémité (client / serveur) de la connexion TCP est associé un numéro de port sur 16 bits (de 1 à 65535) assigné à l'application émettrice ou réceptrice. Ces ports sont classés en trois catégories :

Internet Protocol(IP)

Internet Protocol (abrégé en IP) est une famille de protocoles de communication de réseau informatique conçus pour et utilisés par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique pour l'ensemble des terminaux connectés.

Fonction de hachage :

On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.



Exemple de fonction de hachage appliquée sur 3 entrées distinctes.

Les fonctions de hachage servent à rendre plus rapide l'identification des données : calculer l'empreinte d'une donnée ne doit coûter qu'un temps négligeable. Une fonction de hachage doit par ailleurs éviter autant que possible les collisions (états dans lesquels des données différentes ont une empreinte identique) : dans le cas des tables de hachage, ou de traitements automatisés, les collisions empêchent la différenciation des données ou, au mieux, ralentissent le processus.

En cryptographie les contraintes sont plus exigeantes et la taille des empreintes est généralement bien plus longue que celle des données initiales ; un mot de passe dépasse rarement une longueur de 8 caractères, mais son empreinte peut atteindre une longueur de plus de 100 caractères. La priorité principale est de protéger l'empreinte contre une attaque par force brute, le temps de calcul de l'empreinte passant au second plan.

Hors cryptographie, les fonctions de hachage ne sont en général pas injectives, car on souhaite conserver des empreintes plus petites que les données traitées – pour des considérations de stockage en mémoire : il faut donc concevoir une fonction de hachage homogène, donnant une empreinte de taille raisonnable tout en minimisant le nombre de collisions. Par exemple on peut associer une clé de 16, 32 ou 64 bits à chaque document d'une bibliothèque de plusieurs millions de fichiers. Si deux fichiers ont des empreintes différentes, ils sont à coup sûr différents. Si leurs empreintes sont identiques en revanche, l'identité n'est pas encore prouvée ; mais la comparaison octet par octet n'aura plus à se faire que sur le sous-ensemble bien plus restreint de fichiers qui ont la même empreinte.

Réseau étendu(WAN) :

Un réseau étendu (terme recommandé au Québec par l'OQLF[]), souvent désigné par l'anglais Wide Area Network (WAN), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Le plus grand WAN est le réseau Internet.

Maintenant qu'Internet fournit un réseau WAN rapide, le besoin de disposer de son propre réseau étendu est moins crucial. Il est possible d'utiliser à la place un réseau privé virtuel (VPN), utilisant le chiffrement et d'autres techniques pour donner l'impression que l'organisation dispose de son propre réseau privé alors qu'elle utilise l'infrastructure partagée d'Internet. Cette solution confère cependant une qualité de service moindre, ou du moins identique à celle de la connexion Internet qui en règle générale dispose d'un taux de disponibilité inférieur.

Serveur de fichiers :

Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichier.

On utilise généralement l'un des quatre protocoles suivant:

- FTP (File Transfer Protocol)
- CIFS (Common Internet File System) anciennement nommé SMB (Server Message Block)
- NFS (Network File System)
- NCP (Netware Core Protocol)

Le choix du protocole dépend principalement de la méthode d'accès des utilisateurs. CIFS est utilisé par les systèmes d'exploitation Microsoft Windows, NFS est répandu dans le milieu UNIX. Toutefois des implémentations de ces protocoles sont disponibles pour tout type de système. Ces deux protocoles permettent d'établir des liaisons permanentes entre le client et le serveur.

FTP est utilisé pour des connexions ponctuelles lorsque le client n'a pas besoin d'être connecté en permanence au serveur de fichier.

Generic Routing Encapsulation :

Generic Routing Encapsulation (GRE ou Encapsulation Générique de Routage) est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau dans n'importe quel paquet de la couche réseau. Le paquet d'origine est le payload (information utile) du paquet final. Par exemple, les serveurs de tunnel qui chiffrent les données peuvent utiliser GRE à travers Internet pour sécuriser les Réseaux privés virtuels.

GRE a été développé par Cisco et peut encapsuler une large gamme de types de paquets de différents protocoles dans des paquets IP. Les tunnels GRE sont conçus pour ne pas avoir besoin de maintenir un état, ce qui signifie que chaque terminaison de tunnel ne conserve aucune information d'état ou de disponibilité de la terminaison distante. Cette fonctionnalité aide les fournisseurs d'accès à proposer des tunnels IP à leurs clients, qui ne sont pas concernés par l'architecture du fournisseur d'accès. Ceci donne aux utilisateurs (les clients du fournisseur d'accès) la flexibilité de configurer ou reconfigurer leur architecture IP sans être concernés par les problèmes de connectivité, en créant un lien point à point virtuel vers des routeurs distants à travers des réseaux ip.

- **Exemples de piles de protocoles utilisant GRE**
  - RADIUS
  - UDP
  - GRE
  - IPv4 (1) et IPv6 (2)
  - Ethernet

- PAPI
- PPTP

Hypertext Markup Language (HTML) :

L'Hypertext Markup Language, généralement abrégé HTML, est le format de données conçu pour représenter les pages web. C'est un langage de balisage qui permet d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des éléments programmables. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation (JavaScript) et des formats de présentation (feuilles de style en cascade).

HTML est un langage de description de document qui se présente sous la forme d'un langage de balisage dont la syntaxe vient du Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol(HTTP) :

L'HyperText Transfer Protocol, plus connu sous l'abréviation HTTP, littéralement le « protocole de transfert hypertexte », est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (avec S pour secured, soit « sécurisé ») est la variante du HTTP sécurisée par l'usage des protocoles SSL.

HTTP est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).

Les clients HTTP les plus connus sont les navigateurs Web permettant à un utilisateur d'accéder à un serveur contenant les données. Il existe aussi des systèmes pour récupérer automatiquement le contenu d'un site tel que les aspirateurs de site Web ou les robots d'indexation.

Ces clients se connectent à des serveurs HTTP tels qu'Apache HTTP Server ou Internet Information Services.

HTTPS :

HTTPS (avec S pour secured, soit « sécurisé ») est la simple combinaison de HTTP avec une couche de chiffrement comme SSL ou TLS.

Il permet au visiteur de vérifier l'identité du site auquel il accède grâce à un certificat d'authentification. Il garantit la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur.

Il est généralement utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc. Il est aussi utilisé pour la consultation de données privées, comme les courriers électroniques par exemple.

Interpréteur de commandes (CLI) :

Un interpréteur de commandes, parfois désigné par l'anglicisme shell, est un programme faisant partie des composants de base d'un système d'exploitation, le Command-line interface (CLI) (ou invite de commandes).

C'est le mode de contrôle fondamental d'un ordinateur ou autre équipement informatique. Ce dernier prend ses données d'entrées en ligne de commande, qui sont transmises à l'interpréteur en mode interactif.

Son rôle est de traiter les commandes tapées au clavier par l'utilisateur. Ces commandes, une fois interprétées, auront pour effet de réaliser telle ou telle tâche d'administration, ou bien de lancer l'exécution d'un logiciel.

Par exemple : sous Windows ,il existe le MS-DOS .

Sous UNIX, la ligne de commande a toujours été le moyen privilégié de communication avec l'ordinateur. Le Bourne shell (sh) est l'interpréteur originel de l'environnement UNIX.

Dans les équipements réseau ,On citera le cas des équipements Cisco, et du CLI intégré dans le système d'exploitation IOS qui reste une référence de CLI ("Cisco Like Interface" pour ceux qui s'en inspirent).

IOS (Cisco) :

IOS (abréviation de « Internetwork Operating System », Système d'exploitation pour la connexion des réseaux), est le système d'exploitation produit par Cisco Systems et qui équipe la plupart de ses équipements.

IOS est muni d'une interface en ligne de commande (ou CLI) accessible via telnet, port série et SSH. IOS peut disposer d'une interface web.

Différentes versions de l'IOS sont utilisées sur la gamme de routeurs, de points d'accès Wi-Fi et des commutateurs de la marque.

L'IOS c'est un système de description a comme particularité de prendre immédiatement chaque changement de configuration en compte. Il utilise deux espaces distincts pour stocker sa configuration :

- la running-config : typiquement stockée en mémoire vive (RAM) et qui contient la configuration actuellement utilisée,
- la startup-config : typiquement stockée en mémoire non volatile (NVRAM) et qui contient la configuration au démarrage du matériel.

C'est pourquoi lors de la fin de la configuration de l'IOS il ne faut pas oublier de copier la running-config à l'intérieur de la startup-config

Centre de traitement de données(DATACENTER) :

Un **centre de traitement des données** (Data center en anglais) est un service généralement utilisé pour remplir une mission critique relative à l'informatique et à la télématique. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Tablettes d'équipement de télécommunications

Un centre de traitement des données se présente comme un lieu où se trouvent différents équipements électroniques, surtout des ordinateurs et des équipements de télécommunications. Comme son nom l'indique, il sert surtout à traiter les informations nécessaires aux activités d'une entreprise. Par exemple, une banque peut recourir à un tel centre, lui confiant les informations relatives à ses clients, tout en traitant les transactions de ceux-ci. En pratique, presque toutes les entreprises de taille moyenne utilisent un tel centre. Quant aux grandes entreprises, elles en utilisent souvent des douzaines.

Les bases de données étant souvent cruciales au fonctionnement des entreprises, celles-ci sont très sensibles à leur protection. Pour cette raison, ces centres maintiennent de hauts niveaux de sécurité et de service dans le but d'assurer l'intégrité et le fonctionnement des appareils sur place.

Les missions principales du centre sont d'offrir une bonne connexion réseau (internet, intranet, ...) et une haute disponibilité du système d'information. En conséquence, il est possible de déployer différentes applications logicielles pour les tâches essentielles à l'activité métier des clients. Parmi ces applications, on retrouve des gestionnaires de bases de données, des serveurs de fichiers et des serveurs d'applications

Lag (latence) :

Lag (ou latence) est un anglicisme désignant un délai dans les communications informatiques.

Il désigne le temps nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau.

À n'importe quel paquet transmis par réseau correspond donc une valeur de lag. Le terme est néanmoins utilisé pour désigner les délais plus longs, perceptibles par les utilisateurs.

Le lag peut être occasionné par plusieurs causes :

- Capacité réseau insuffisante
- Capacité de calcul inefficace ou insuffisante
  Il peut être provoqué par une requête inhabituelle qui ne figure pas encore en mémoire cache, ou si la requête demande une importante quantité de capacité de calcul. Le délai n'est ainsi donc pas nécessairement lié à une distance géographique.
- Contrainte technologique
  En fonction de la technologie employée, le traitement et la transmission des signaux peut demander un délai variable. Les réseaux de transmission par satellite géostationnaire, par exemple, causent un délai minimal de l'ordre de 270 ms.
- Réordonnancement des paquets

A cause du lag, les temps de réponse de certaines applications se trouvent augmentés, ce qui peut s'avérer gênant pour les communications interactives (en téléphonie, on estime qu'un délai de 250 ms est nettement perceptible et que 500 ms et plus rendent la communication très difficile)

La variation du lag dans le temps est appelée jitter ou gigue. Un jitter élevé signifie que les délais sont fortement variables, ce qui perturbe les protocoles en temps réel.

Navigateur Web :

Un navigateur Web est un logiciel conçu pour consulter le World Wide Web. Techniquement, c'est au minimum un client HTTP.

La fonction principale d'un navigateur web est de permettre la consultation d'informations disponibles (« ressource » dans la terminologie du Web) sur le World Wide Web. Les principales étapes de la consultation d'une ressource sont les suivantes :

1. L'utilisateur donne au navigateur Web l'adresse Web de la ressource à consulter. Il existe trois manières de donner une adresse Web :
   - taper soi-même l'adresse web dans la barre d'adresse du navigateur ;

- choisir une ressource dans la liste des favoris (ou marque-page ou bookmark), sachant qu'à chaque favori est associée une adresse Web ;
- suivre un hyperlien, sachant qu'à chaque hyperlien est associée une adresse Web.

2. Le navigateur se connecte au serveur Web hébergeant la ressource visée et la télécharge. Le protocole de communication généralement utilisé est HTTP.
3. le moteur de rendu du navigateur traite cette ressource, télécharge les éventuelles ressources associées et affiche le résultat sur l'écran de l'utilisateur

Server Message Block(ou CIFS)

Server Message Block	
Fonction	Partage de fichiers et d'imprimantes
Sigle	SMB
Port	445[1]

Le protocole SMB (Server Message Blockhttp://fr.wikipedia.org/wiki/Server_Message_Block - cite_note-1) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows. Dans Windows NT 4, il est appelé CIFS (Common Internet File System). Dans Vista et 7, il est appelé SMB 2http://fr.wikipedia.org/wiki/Server_Message_Block - cite_note-2.

SMB fonctionne via une structure de client/serveur, le client va envoyer des requêtes spécifiques et le serveur de fichiers va y répondre. Le protocole est optimisé pour une utilisation dans un réseau local, mais il peut aussi être utilisé sur Internet (la plupart des

attaques simples sous Windows ont pour source cette raison, profitant notamment de la présence du service "Serveur" lancé par défaut).http://fr.wikipedia.org/wiki/Aide:R%C3%A9f%C3%A9rence_n%C3%A9cessaire

Le serveur SMB permet de donner l'accès aux clients du réseau à des systèmes de fichiers, mais aussi à d'autres ressources comme des imprimantes. Le client peut avoir ses propres disques qui ne seront pas partagés et peut accéder en même temps aux disques et imprimantes partagés par le serveur.

Stockage en réseau NAS :

Un stockage en réseau NAS, ou un NAS (de l'anglais Network Attached Storage), est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

Comme un serveur de fichiers, le stockage en réseau NAS fournit des services à travers un réseau IP avec un ou plusieurs des protocoles suivants :

- Common Internet File System (CIFS) anciennement nommé Server Message Block (SMB)
- Network File System (NFS)
- Apple Filing Protocol (AFP)

Parfois les fichiers sont disponibles via File Transfer Protocol (FTP). En général, le NAS est configuré via une interface web.

Le NAS est distingué :

- du Storage Area Network (SAN) qui utilise les protocoles comme SCSI, Fibre Channel, iSCSI, ATA over Ethernet (AoE) ou HyperSCSI à travers un réseau dédié.

- du Direct Attached Storage (DAS), c'est-à-dire d'un disque dur directement connecté à l'ordinateur qui utilise les protocoles ATA, SATA, eSATA, SCSI, SAS et Fibre Channel via des câbles dédiés.

Le NAS peut s'intégrer à un SAN ou en être le point d'entrée.

Le serveur NAS a pour vocation d'être accessible depuis des postes client à travers le réseau pour y stocker des données. La gestion centralisée sous forme de fichiers a plusieurs avantages :

- faciliter la gestion des sauvegardes des données d'un réseau ;
- prix intéressant des disques grands capacités par rapport à l'achat de disques en grand nombre sur chaque serveur du réseau ;
- accès par plusieurs postes clients aux mêmes données stockées sur le NAS ;
- réduction du temps d'administration des postes clients en gestion d'espace disques.

Qualité de service :

La qualité de service (QdS) ou Quality of service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…

La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau (en management du système d'information) ou d'un processus (en logistique) et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure.

File Transfer Protocol :

File Transfer Protocol	
Fonction	Transfert de fichier
Sigle	FTP
Port	21-écoute 20-données par défaut
RFC	RFC 3659

Le File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS.

FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend public une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).

En tète :

Partie d'un message contenant les informations nécessaire à sa gestion telles que telles que l'expéditeur ou le destinataire .le premier octet d'un en tète de paquet s'appelle (signature du paquet).il détermine le format de l'en tète et informe sur le contenu du paquet .Le reste de l'en tète détermine la taille du paquet.

PROXY :

Un serveur mandataire ou proxy est un serveur informatique qui a pour fonction de relayer des requête entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- Mémoire cache
- La journalisation des requêtes (logging)
- La sécurité du réseau local
- Le filtrage et l'anonymat

Pipelining :

Désigne le fait de servir du procédé de pipeline qui est procédé par qui permet de rendre indépendants les différentes étapes de traitement d'une instruction par le processeur .Ces étapes sont par exemple chez Intel :

-1 lecture en mémoire
-2 et 3 décodage
-4exécussion
-5 écritures du résultat en mémoire

Chaque étape utilise en entrée la sortie de la précédence.

Access Control List (CLI) :c'est une liste mentionnant les utilisateurs à atteindre une information.

Cluster :

Ensemble de plusieurs machines vues comme une seule permettant d'obtenir de grandes puissances de traitements.

LOGIN :

Procédure pour se connecter sur un système, un hôte, souvent protégé par un mot de passe. Un login est le nom qui permet d'identifier un utilisateur qui se connecte sur un ordinateur

Bibliographie :

- **Livres:**

  - **Titre : Deploying Cisco wide area application services[1]**

    - Rédiger par :Joel Christner - CCIE (HEPM ID: 9174610) et Zach Seils - CCIE., (HEPM ID: 12811772). Nancy Jin
    - Année: 2010
    - Nombre de pages :625 pages

  - **Titre : Deploying Cisco Wide Area Application Services[2]**

    - Rédiger par :Zach Seils et Joel Christner
    - Année 2008
    - Nombre de pages :377 pages

- **Adresse électronique :**

  - http://www.cisco.com/en/US/products/ps5680/Products_Sub_Category_Home.html [3]
  - http://www.networkworld.com/supp/2007/ndc4/061807-cisco-app-optimization.html?nlhtc=0618ciscoalert1&[4]
  - http://www.networkperformancedaily.com/2006/12/waas_up_with_ciscos_wan_optimi_1.html[5]
  - http://www.pcdistrict.com/netqos-partners-cisco-waas-to-develop-application-response-time-reporting-for-wan-optimization-review299-8.html[6].