Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

CONCOURS INTERNE
DE TECHNICIEN DE CLASSE NORMALE
DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- Session 2016 -

Mardi 6 septembre 2016

Spécialité : Infrastructures et réseaux

Traitement de questions et résolution de cas pratiques dans la spécialité choisie, à partir d'un dossier, permettant d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le dossier ne peut excéder 20 pages.

(Durée : 3 heures – Coefficient 2)

Le dossier documentaire comporte 17 pages.

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.
ECRIRE EN NOIR OU EN BLEU - PAS D'AUTRES COULEURS

QUESTIONS

Les questions sont notées sur 10 points. Pour chacune des questions, hormis la 3 et la 4, vous donnerez une réponse rédigée en quelques lignes.

Question 1 :

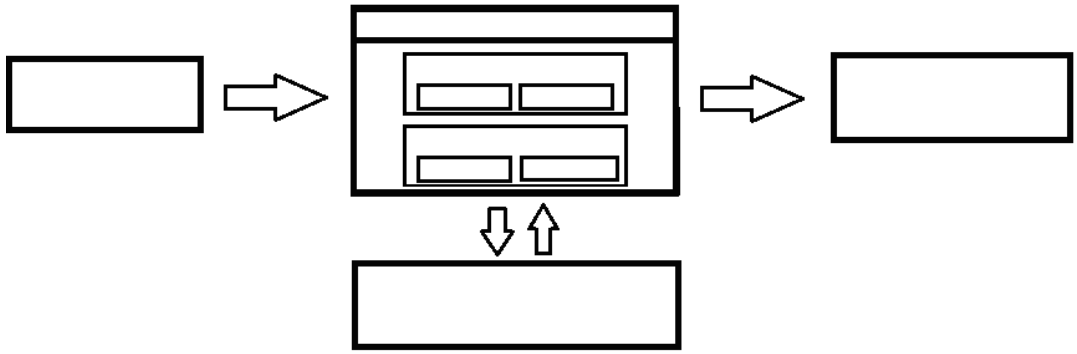
Définissez un NAS et un SAN et expliquez la différence principale.

Question2 :

Quelle est la principale différence du codage UTF8 par rapport à ASCII ?

Question 3 :

Le schéma suivant représente sommairement un ordinateur.



Reproduisez le schéma en y positionnant dans les cadres les éléments suivants :

- Mémoire centrale
- Mémoire de masse
- Microprocesseur
- Périphériques d'entrée
- Périphériques de sortie
- RAM
- ROM
- UAL (unité arithmétique et logique)
- UC (unité de commande)
- Unité centrale

Question 4 :

Donnez le nom des 7 couches du modèle OSI (*Open Systems Interconnection*) en les numérotant dans l'ordre et indiquez dans quelle couche vous positionnez les protocoles ICMP, TCP, SMTP, IP.

Question 5 :

A quoi correspond l'adresse IP 8.8.8.8 ?

Question 6 :

Quel organisme veille à ce que les adresses MAC attribuées aux cartes réseaux puissent être uniques et par quel moyen ?

Question 7 :

Décrire les caractéristiques des câbles à paires torsadées de catégorie 5 et de catégorie 6 et précisez dans quels cas vous utiliserez un câble de catégorie 6 plutôt que de catégorie 5 ?

Question 8 :

Expliquer le principe de fonctionnement d'un système RAID5.

Question 9 :

A cause d'une table de routage erronée, un paquet envoyé par le routeur A est redirigé vers le routeur B qui le redirige vers A et ainsi de suite indéfiniment. Comment l'erreur est elle détectée ?

Question 10 :

4 trains d'informations analogiques sont multiplexés sur une ligne téléphonique de bande passante 300-3400 Hz. La bande passante de chaque train est de 500Hz. Expliciter le processus de multiplexage.

CAS PRATIQUES

Cas 1 : *(4 points)*

L'entreprise POL dispose du réseau 10.203.92.0/23. Ce réseau doit être découpé en un maximum de sous-réseaux de 60 hôtes chacun.

1. Combien de bits sont nécessaires sur la partie hôte de l'adresse du réseau pour accueillir au moins 60 hôtes ?

2. Quel est le nombre maximum d'adresses utilisables dans chaque sous-réseau ?

3. Quel est le nombre maximum de sous-réseaux définis ?

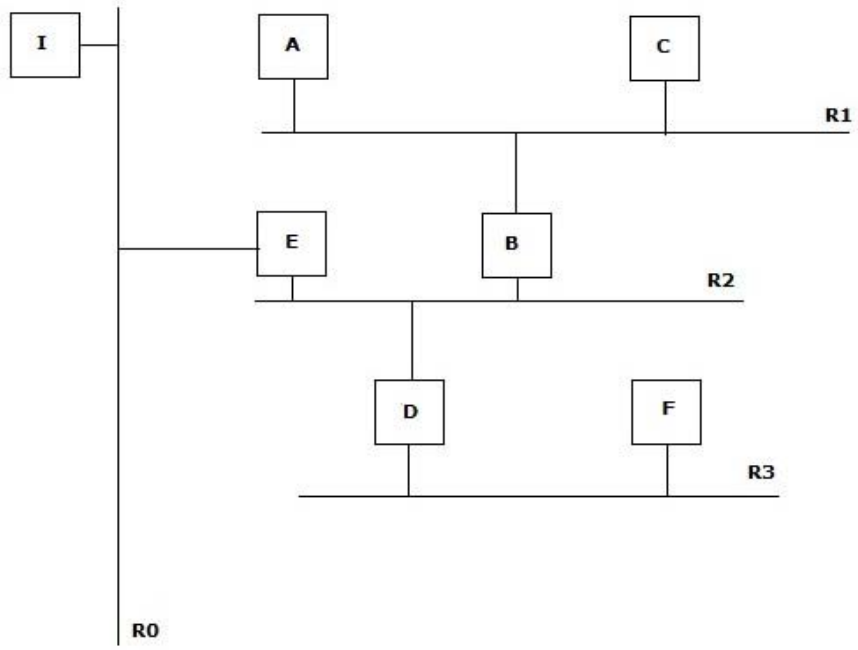
4. Donnez les adresses de tous les sous-réseaux (S1, …, Sx) définis, en décimal et en binaire.

5. En déduire l'écriture au format CIDR du masque des sous-réseaux définis.

6. Quelle est l'adresse de diffusion du sous-réseau S2 ?

7. L'adresse 10.203.93.66 appartient-elle au sous-réseau S5 ?
   Appuyer la réponse en utilisant le masque de sous-réseau S5 bit à bit.

8. Une partie du réseau est représentée dans l'illustration suivante :
   (les sous-réseaux R1, R2, R3 ne correspondent pas obligatoirement aux sous-réseaux S1, S2, S3 des questions précédentes)



Le routeur I (10.108.37.1/24) est géré par quelqu'un d'autre, il relie les réseaux de l'entreprise POL à internet. Le routeur par défaut de E est I.

Machine	Adresse IP	Routeur par défaut
A	10.203.92.3	À déterminer
B	10.203.92.62 – 10.203.93.129	À déterminer
C	10.203.92.37	À déterminer
D	10.203.93.1 - 10.203.93.130	À déterminer
E	10.108.37.12 - 10.203.93.190	I 10.108.37.1 (imposé)
F	10.203.93.27	À déterminer

Indiquez les routeurs par défaut des autres hôtes, ainsi que les éventuelles routes statiques permettant à toutes les machines de communiquer entre elles et avec internet.

Cas 2 ***:*** *(6 points)*

1) Attaques et sécurisation
   1. Recensez l'ensemble des attaques dont la voix sur IP pourrait être victime.
   2. Précisez pour chacun des types d'attaque les mesures de sécurisation que vous mettriez en place pour éviter au maximum toutes ces menaces en précisant à quel niveau de l'infrastructure elles se situent.

2) Quelle est la fonctionnalité du protocole RTP ? Le couple RTP/RTCP offre t-il un moyen de garantir des délais d'acheminement respectables pour la voix sur IP ?

3) La voix humaine pour la téléphonie doit être numérisée à 8 kHz et sur 8 bits.
   1. Que représentent ces deux valeurs ?
   2. Montrer que si l'on veut transmettre correctement une voix numérisée, il faut que le canal de transmission ait un débit binaire d'au moins 64 kbit/s.

4) On rappelle que la longueur minimale de la trame est égale à 512 octets. On veut y faire transiter sur un réseau éthernet une parole téléphonique compressée dont le débit est 8 kbit/s.
   On suppose que les deux postes téléphoniques sont éloignés de 100m sur le réseau et que la vitesse de propagation des signaux sur le support est égale à 100 000 km/s. Calculez la latence subie par la parole. Cette latence est-elle acceptable ?

Dossier documentaire :

La VOIP pour tous

La voix sur IP, plus communément appelée « VoIP » (Voice over IP) est une technique permettant de communiquer oralement sur des réseaux compatibles IP (protocoles de communication de réseaux informatiques), qu'il s'agisse de réseaux privés ou d' Internet, filaire (cable/ADSL/optique) ou non (satellite, wifi, GSM) . Cette technologie est le plus souvent utilisée pour prendre en charge le service de téléphonie sur IP (« ToIP » pour Telephony over Internet Protocol).

Comment est transportée la voix ?

Le transport de la voix sur IP est relativement compliqué. La première étape est la numérisation (codage) du signal acoustique. Ensuite, les informations sont découpées en trames (blocs d'informations) pouvant circuler sur un réseau informatique. De nombreux protocoles peuvent alors être utilisés pour acheminer les informations au(x) destinataire(s).

Comment la voix est-elle codée ?

Dans une conversation, la voix produit des sons à des fréquences différentes.

Grâce à ces changements de fréquences constants, nous percevons les émotions et les intonations. Cette multitude de fréquences serait remarquable par un affichage sinusoïdal si on visualisait son signal sur un oscilloscope.

La voix provoque un signal sinusoïdal, qui est analogique. Cependant, pour le passer sur un réseau TCP/IP (Numérique), il va falloir convertir ce signal (analogique vers numérique) en format PCM (Pulse Code Modulation) à 64 kb/s.

Une fois convertie, il est nécessaire de compresser la voix (numérisée) par le biais d'un codec (Compresseur/Décompresseur) pour l'insérer dans un paquet IP. Ce codage doit offrir une qualité de voix la meilleure possible pour un débit et un délai de compression les plus faibles possibles. Il existe plusieurs techniques de codage qui sont mesurées de façon totalement subjectives.

Le mode de diffusion de la Voix sur IP :

Le terme « VoIP » est en général utilisé pour décrire des communications dites « point à point ». Pour la diffusion de son ou de vidéos sur IP en mode multipoints, on parle plutôt de streaming pour une simple diffusion, comme l'utilisent les radios web par exemple. Le terme multipoints est plutôt réservé aux visioconférences.

Cette technique peut se faire en mode unicast (un émetteur et un récepteur), broadcast (un émetteur et tous les récepteurs sans exception) ou multicast (un émetteur et plusieurs récepteurs) sur les réseaux.

Le transport de communication sur IP est très dépendant du délai de latence (délai de transfert) d'un réseau. Ce délai influe beaucoup sur la qualité psycho-acoustique d'une conversation.

Influence et matériel:

La voix sur IP entraine le remplacement des postes téléphoniques traditionnels par des « postes téléphoniques IP » dont les caractéristiques sont:

- Le remplacement des prises téléphoniques (RJ11) par des prises réseau (RJ45).
- Le remplacement des interfaces analogiques ou numériques des postes téléphoniques avec le réseau par une interface de protocoles IP.
- Le remplacement du protocole de signalisation téléphonique traditionnel par un système de voix sur IP.
- Le remplacement du combiné téléphonique par un nouveau combiné ayant les

caractéristiques précitées, ou encore par un logiciel pouvant être installé sur un ordinateur (muni d'un casque et d'un micro).

Accessibilité :

Une infrastructure de voix sur IP peut être disponible pour les mêmes zones de disponibilité que les systèmes téléphoniques traditionnels:

- D'une manière fermée (Intranet): par l'utilisation d'un central IP privé.
- D'une manière semi-publique (Extranet): par le partage d'un central IP avec ses partenaires ou clients (via un VPN par exemple = extension du réseau local).
- D'une manière publique mais limitée (Internet): par une ouverture sur l'Internet du central IP.
- D'une manière publique et ouverte (Internet): par une ouverture sur l'Internet du central IP et l'affiliation de passerelle(s) vers le réseau PSTN.

Les types d'architectures en Téléphonie sur IP

Par Jordan CRAMPONT Publié le 30/10/2015

Introduction

Aujourd'hui on entend beaucoup parler de "téléphonie sur IP" en entreprise, en effet celle-ci represente un atout majeur en terme d'économie et d'évolution technologique pour les entreprises. Cependant, une solution de téléphonie IP peut faire intervenir de nombreux acteurs (Terminaux IP, produits VOIP, coûts de formations, coûts d'exploitations, etc...). Alors avant de mettre en place toute architecture pour résoudre les problèmes liés à l'entreprise, il est important et impératif d'étudier toutes les solutions envisageables qui pourraient être plus bénéfiques à l'entreprise.
Il faut donc analyser, comprendre, gérer, le coût, la performance, la sécurité, de chaque solution, c'est-à-dire tous les critères à prendre en compte dans toute amélioration d'un système d'information.

Généralités

Un système de téléphonie permet de transmettre et de reproduire de la voix et de gérer d'autres services lié à la gestion de la voix comme la messagerie vocale, la conférence téléphonique,...
Un système de téléphonie est caractérisé par trois éléments principaux :

- Le terminal: postes téléphonique, ou encore fax...,
- Le commutateur téléphonique: PABX, IPBX...,
- Les liaisons entre ces équipements.

Le commutateur téléphonique met en relation deux correspondants, selon des notions basées sur le numéro appelé par le correspondant.
Il existe deux types de commutateurs :

- Les commutateurs publics : Utilisés par les fournisseurs de téléphonie et permettent les jonctions avec le réseau public.
- Les commutateurs privés: Utilisés par les entreprises, et gèrent les communications internes entre les postes de l'entreprise, mais aussi la connexion au réseau téléphonie public.

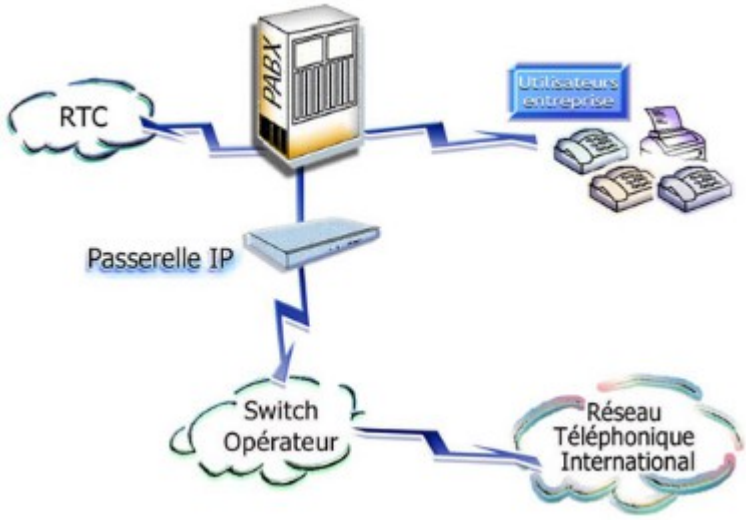
Mise en place d'un PABX avec carte IP

Le PABX « Private Automatic Branch eXchange », est un autocommutateur téléphonique privé, un appareil assurant automatiquement les connexions téléphoniques entre appelé et appelant, aussi bien au sein de l'entreprise que vers l'extérieur. D'où son autre nom : « autocom » pour « autocommutateur ». Il s'appuie sur le protocole H.323. Les principales fonctions du « standard téléphonique » PABX sont :

- Gérer les appels en interne et vers l'extérieur et distribuer les appels entrants.
- Gérer une boîte vocale (si correspondant absent).
- Gérer les terminaux téléphoniques (postes analogiques ou numériques).

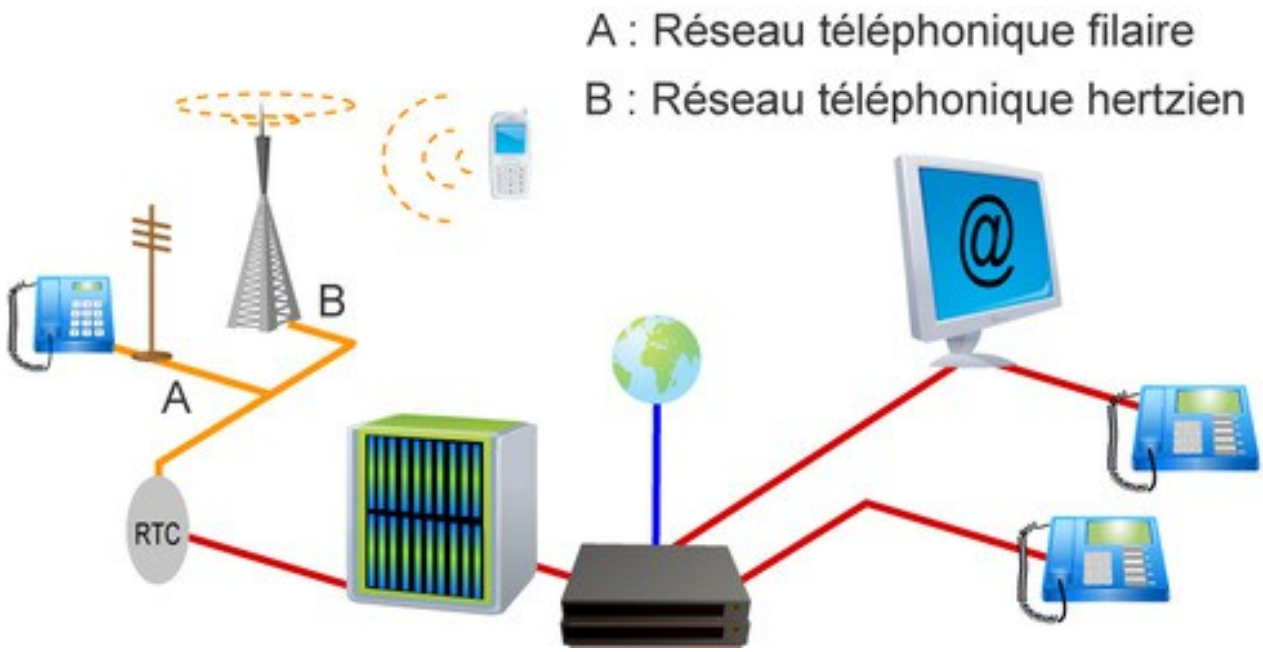
Généralement une entreprise dispose d'un PABX, il serait donc possible d'adapter ce PABX par l'ajout de carte IP, bien évidemment suivant son modèle (Certains PABX ne permettent pas l'ajout de carte IP) et ainsi mettre en place une passerelle VOIP, c'est-à-dire un appareil qui convertirait le

trafic de la téléphonie en IP pour créer une transmission sur le réseau de données.
La passerelle VoIP permet de recevoir et de passer des appels sur un réseau de téléphonie normal. Pour beaucoup d'entreprises, il est préférable de continuer à utiliser des lignes téléphoniques traditionnelles car on peut garantir une meilleure qualité d'appel et une plus grande disponibilité ceci permet à l'entreprise de bénéficier des avantages du fournisseur Internet, en effet les coûts des appels entre bureaux peuvent être réduits en les acheminant via Internet. Le coût téléphonique ne dépendra plus que du forfait pris chez l'opérateur.



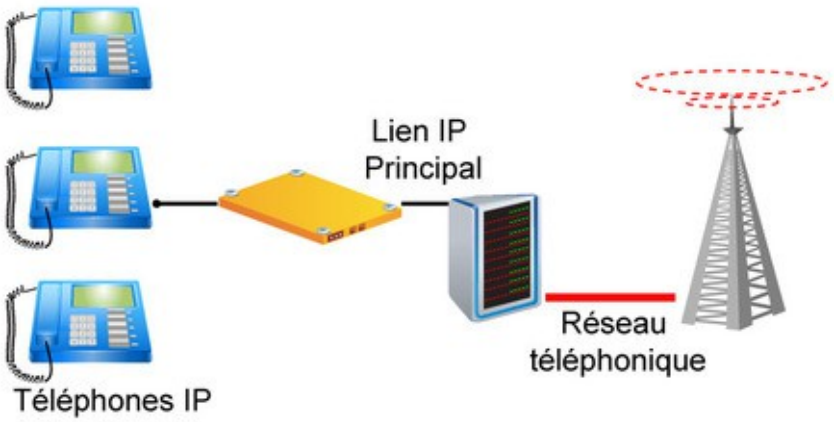
Mise en place d'une solution "Full IP"

Il est également possible de remplacer le PABX classique par un IP PBX impliquant le remplacement des terminaux téléphoniques analogiques classiques par des téléphones IP. C'est le choix de la rupture, impliquant un renouvellement complet des infrastructures. L'IPBX est un des noms d'une Appliance qui permet à une entreprise d'acheminer tout ou une partie de ses communications (voix et data) en utilisant le protocole Internet (IP), en interne sur le réseau local ou le réseau étendu de l'entreprise.
En plus des services classiques du PBX, l'IPBX permet d'adjoindre au réseau téléphonique de l'entreprise des téléphones IP, fixes et portables (en Wi-Fi), ou encore des PC équipés de logiciels VoIP de type Skype, appelés « soft phone ». Par ailleurs, les services de messagerie collaborative, d'agendas partagés, c'est-à-dire l'ensemble des services que l'on regroupe sous le terme de communication unifiée, peuvent être gérés par des IPBX. Il s'appuie sur le protocole SIP.
Les téléphones IP sont interconnecté via l'IP-PBX qui celui-ci est connecté au réseau de l'entreprise via le protocole IP (passerelle IP) permettant ainsi la communication interne entre les différents sites de l'entreprise. En ce qui concerne les appels entrants (Externe), ces appels sont redirigés via l'opérateur de téléphonie IP qui permet la communication des appels venant d'une ligne RTC (Reseau Téléphonique Commuté : Réseau Téléphonique International) à l'IP-PBX. Le coût téléphonique ne dépendra plus que du forfait pris chez l'opérateur. On établit alors, un canal de communication entre l'IPBX et un opérateur VOIP. Les flux de signalisation sont échangés en utilisant le protocole SIP. Pour connecter les trunk SIP les opérateurs installent alors des softswitchs (Contrôle d'appel).



Mise en place d'un "Centrex IP"

Enfin, il est possible d'externaliser les fonctions de téléphonie vers un IP Centrex, service fourni par un opérateur ou autre fournisseur de solution de VoIP, qui gère le service de bout en bout.
Un Centrex IP est un IPBX hébergé et géré par une tierce partie, généralement un opérateur de téléphonie fixe. Les téléphones des utilisateurs s'authentifient au Centrex au travers d'Internet. Les appels entrants et sortants transitent en IP. Cette solution permet de supprimer le standard téléphonique et de réduire considérablement le coût des appels téléphoniques. L'ensemble du service est alors géré par un prestataire et facturé sous forme d'abonnement périodique tout compris ne nécessitant pas d'investissement pour l'entreprise (en dehors des postes téléphonique IP). Le cout téléphonique se perçoit vis-à-vis du forfait délégué chez le prestataire.



Conclusion

Il est donc possible de voir l'existence de plusieurs types d'architectures en téléphonie IP pouvant s'adapter aux besoins de l'entreprise. Chacune de ces architectures à bien évidemment ses avantages et inconvenients suivant l'architecture dont dispose de base l'entreprise, de ce fait le choix de telle ou telle architecture se basera sur les critères que l'entreprise aura mis en évidence, soit au niveau coût, soit au niveau performance, soit au niveau sécurité. Sachant qu'aujourd'hui, certaines entreprises se dirigent vers l'association de plusieurs architectures, par exemple, l'architecture appelée "progressive": l'entreprise preserve son PABX et ajoute un IPBX, et se laisse un temps d'adaptation par peur de perdre "pied" dans cette nouvelle technologie qui ne cesse d'évoluer.

Classe d'adresse IP

Extrait de https://fr.wikipedia.org/wiki/Classe_d'adresse_IP

La notion de **classe d'adresse IP** a été utilisée sur Internet pour distribuer des plages d'adresses IPv4 à des utilisateurs finaux. Avec cette méthode, le masque de réseau pouvait être déduit de l'adresse IP et les protocoles de routage comme Border Gateway Protocol (jusqu'à la version 3), RIPv1 et IGRP sont dits *classful* car ils font usage d'un masque réseau implicite lié à l'adresse.

La notion de classe est obsolète depuis le milieu des années 1990. Les assignations d'adresses du protocole IPv4 (et de son successeur IPv6) ne tiennent plus compte de la *classe d'adresse* et les protocoles de routage modernes indiquent explicitement le masque réseau de chaque préfixe routé.

Adressage en classe

Dans les premières années d'Internet, l'assignation des adresses aux réseaux finaux consistait à octroyer le premier octet de l'adresse au réseau, c'est-à-dire que 256 réseaux de 16 millions d'adresses étaient possibles. Devant la limitation qu'impose ce modèle, le document IEN 46 propose de modifier la façon dont les adresses sont assignées.

En 1981, la RFC 790 (*Assigned numbers*) prévoit qu'une adresse IP est divisée en deux parties : une partie servant à identifier le réseau (*net id*) et une partie servant à identifier un poste sur ce réseau (*host id*).

Il existe cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités en termes de répartition du nombre d'octet servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

- Une adresse IP de classe A dispose d'une partie *net id* comportant uniquement un seul octet.
- Une adresse IP de classe B dispose d'une partie *net id* comportant deux octets.
- Une adresse IP de classe C dispose d'une partie *net id* comportant trois octets.
- Les adresses IP de classes D et E correspondent à des adresses IP particulières.

Afin d'identifier à quelle classe appartient une adresse IP, il faut examiner les premiers bits de l'adresse

Classe A
: Une adresse IP de classe A dispose d'un seul octet pour identifier le réseau et de trois octets pour identifier les machines sur ce réseau. Un réseau de classe A peut comporter jusqu'à $2^{3\times 8}-2$ postes, soit $2^{24}-2$, soit 16 777 214 terminaux. Le premier octet d'une adresse IP de classe A commence toujours par le bit *0*, il est donc compris entre 0 et 127, certaines valeurs étant réservées à des usages particuliers. Un exemple d'adresse IP de classe A est : 10.50.49.13.

Classe B
: Une adresse IP de classe B dispose de deux octets pour identifier le réseau et de deux octets pour identifier les machines sur ce réseau. Un réseau de classe B peut comporter jusqu'à $2^{2\times 8}-2$ postes, soit $2^{16}-2$, soit 65 534 terminaux. Le premier octet d'une adresse IP de classe B commence toujours par la séquence de bit *10*, il est donc compris entre 128 et 191. Un

exemple d'adresse IP de classe B est : 172.16.1.23.

Classe C
: Une adresse IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau. Un réseau de classe C peut comporter jusqu'à 2^8-2 postes, soit 254 terminaux. Le premier octet d'une adresse IP de classe C commence toujours par la séquence de bits *110*, il est donc compris entre 192 et 223. Un exemple d'adresse IP de classe C est : 192.168.1.34.

Classe D
: Les adresses de classe D sont utilisées pour les communications multicast. Le premier octet d'une adresse IP de classe D commence toujours par la séquence de bits *1110*, il est donc compris entre 224 et 239. Un exemple d'adresse IP de classe D est : 224.0.0.1.

Classe E
: Les adresses de classe E sont réservées par IANA à un usage non déterminé. Les adresses de classe E commencent toujours par la séquence de bits *1111*, ils débutent donc en 240.0.0.0 et se terminent en 255.255.255.255.

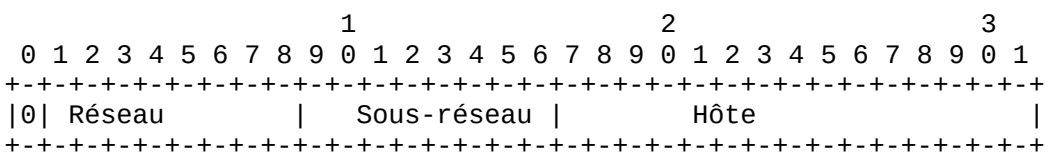
Résumé

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		non défini
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

Sous-réseau

En 1984, devant la limitation du modèle de classes, la RFC 917 (*Internet subnets*) crée le concept de *sous-réseau* qui introduit un niveau hiérarchique supplémentaire entre le numéro de réseau et le numéro d'hôte. Ceci permet par exemple d'utiliser une adresse de Classe B comme 256 sous-réseaux de 254 ordinateurs au lieu d'un seul réseau de 65 534 ordinateurs, sans toutefois remettre en question la notion de classe d'adresse. Ceci permet plus de flexibilité et d'efficacité dans l'attribution des adresses.

Exemple de sous-réseau dans un réseau de classe A :



Le *masque de sous-réseau* permet de déterminer les deux parties d'une adresse IP correspondant respectivement au numéro du réseau et au numéro de l'hôte. Il est obtenu en mettant à 1 les bits du

réseau et à 0 les bits de l'hôte. Le masque 255.255.255.0 correspond par exemple à un sous-réseau de 24 bits. Bien que les sous-réseaux soient encore fréquemment définis aux frontières d'octet, les réseaux 24 bits étant les plus courants, d'autres masques sont désormais possibles.

Deux adresses IP appartiennent au même sous-réseau si elles ont en commun les bits du sous-réseau. Pour déterminer si la machine de destination appartient au même sous-réseau, un hôte utilise l'opération ET binaire entre l'adresses IP et le masque de sous-réseau, et fait de même avec l'adresse destination. Si le résultat est identique, alors la destination est dans le même sous-réseau.

Agrégation des adresses

En 1992, la RFC 1338 (*Supernetting: an Address Assignment and Aggregation Strategy*) propose d'abolir la notion de classe qui n'était plus adaptée à la taille d'Internet.

Le *Classless Inter-Domain Routing* (CIDR), est mis au point en 1993 afin de diminuer la taille de la table de routage contenue dans les routeurs. Ce but est atteint en agrégeant plusieurs entrées de cette table en une seule.

La distinction entre les adresses de classe A, B ou C a été ainsi rendue obsolète, de sorte que la totalité de l'espace d'adressage unicast puisse être gérée comme une collection unique de sous-réseaux indépendamment de la notion de classe. Le masque de sous-réseau ne peut plus être déduit de l'adresse IP elle-même, les protocoles de routage compatibles avec CIDR, dits *classless*, doivent donc accompagner les adresses du masque correspondant. C'est le cas de Border Gateway Protocol dans sa version 4, utilisé sur Internet (RFC 1654 *A Border Gateway Protocol 4*, 1994), OSPF, EIGRP ou RIPv2. Les registres Internet régionaux (RIR) adaptent leur politique d'attribution des adresses en conséquence de ce changement.

L'utilisation de *masque de longueur variable* (*Variable-Length Subnet Mask*, VLSM) permet le découpage de l'espace d'adressage en blocs de taille variable, permettant une utilisation plus efficace de l'espace d'adressage.

Un fournisseur d'accès internet peut ainsi se voir allouer un bloc /19 (soit 8192 adresses) et créer des sous-réseaux de taille variable en fonction des besoins à l'intérieur de celui-ci : de /30 pour des liens points-à-point à /24 pour un réseau local de 200 ordinateurs. Seul le bloc /19 sera visible pour les réseaux extérieurs, ce qui réalise l'agrégation et l'efficacité dans l'utilisation des adresses.

Les plus grandes attaques informatiques en France en 2015

Par tous les moyens et dans tous les domaines : c'est la phrase qui peut qualifier l'attaque des pirates informatiques en France. Le retard informatique des services français ouvre un marché potentiel pour les hackers. Sur 1 475 personnes interviewées, seules 96 personnes se daignent de créer des mots de passe différents pour des services internet différents (Webmail, forums,…) 27 individus ont recours à un checking fréquent de leur solde bancaire, et 339 font un backup mensuel de leurs données, même si on devrait le faire chaque jour.

Les médias français attaqués

Le mois d'avril 2015, tout le monde était abasourdi ! Les différents comptes de réseaux sociaux TV5 étaient en pleine diffusion de la propagande de la secte Daesh. Une situation qui entrainait la coupure obligatoire à l'antenne pendant quelque temps. Quant au responsable, Trend Micro suspecte l'implication d'un groupe APT d'origine russe ainsi que Pawn storm. Cinq mois après l'attaque, une autre faille informatique sur les serveurs de la chaine a été décelée par un service expert. Une faille qui mérite une correction même si le présumé hacker a été arrêté en Bulgarie le mois d'avant. Cela démontre le retard des médias français sur les pirates informatiques. Parmi les attaques dans le domaine du média, figure le cas de TF1 : les pirates ont mis la main sur les données de 1,9 million de Français abonnés à des journaux papier. Ces informations sont directement accessibles via des tiers commerciaux.

Les entités publiques

GDF Suez a été victime d'une attaque informatique du genre Ransomware. Pour ce cas, les pirates bloquent le disque dur ou chiffrent les données importantes des cibles pour les rendre totalement inutilisables ; et ce, jusqu'à ce qu'il y ait paiement de rançon. Mais l'université de Lyon 3 a aussi connu un drame informatique. Février 2015, des pirates ont eu accès à la base de données de l'école, cinq mois après, l'histoire se répète. Le cas s'est aggravé pour le groupe éducatif ESG. La fuite de donnée causée par les pirates a conduit à la fermeture de l'établissement.

Les cosmétiques et santés

Les pirates ne filtrent pas leur cible. Le site Internet de la boutique Officielle « Urban » est informatiquement attaqué. Les données clients sont volées et l'espace numérique de la boutique a dû être fermé pendant plusieurs jours. Ainsi, le laboratoire Santé Beauté représentant les marques « Barbara Gould, poulina, nair, batiste, femfresh, linéance ; était aussi victime d'un vol de données. Par le système de Black SEO, les pirates utilisent des sites légitimes pour créer le référencement de leur lien et leur page. C'est le cas de la chambre des huissiers de Justice de Paris, qui a été piraté par des vendeurs de viagra en juin 2015. Autres cas similaires en 2015 : le cas de la haute autorité de la santé, la fédération nationale des associations d'accueil et de réinsertion sociale ou encore, l'Établissement de la préparation et de Réponse aux urgences sanitaires.

La qualité de service en VOIP

Jadis séparés, les réseaux voix/vidéo et données convergent aujourd'hui vers une architecture commune, exploitant le protocole Internet. Ce dernier, conçu pour le transport asynchrone de données informatiques, n'a cependant pas été prévu pour des applications présentant des contraintes de temps réel.
La maîtrise de la Qualité de Service sur les réseaux IP des opérateurs, mais également sur l'Internet, reste un vaste chantier, d'une importance stratégique extrême.

I - Paramètres agissant sur la qualité de la voix/IP:

I -1) Généralités:

La qualité de service de la voix sur IP dépend de l'ensemble de la chaîne des éléments mis en œuvre dans une communication téléphonique. A ce titre, on peut identifier les deux domaines suivants comme influant sur la qualité de service de la voie sur IP:
· les équipements eux mêmes (terminaux, passerelles) par le biais de leurs éléments constitutifs (codeurs audio, mécanismes d'annulation d'écho…)plus ou moins performants;
· le réseau IP par les perturbations éventuelles qu'il peut introduire (délai de transmission, perte de paquets, gigues…)
La qualité de service peut alors s'exprimer et être mesurée selon deux méthodes différentes et complémentaires:
· la qualité perçue de bout en bout, le plus souvent mesurée par des tests subjectifs avec de vrais auditeurs;
· la mesure de paramètres ayant une influence sur la qualité de service et leur comparaison avec des valeurs recommandées dans les normes.

I-2) Paramètres réseau:

Les paramètres qui agissent directement sur la qualité de la voix sur IP sont les suivants:
· le délai de transmission
· le taux de perte de paquet
· la gigue
De nombreux facteurs concourent à la qualité de service parmi lesquels:
· la bande passante disponible sur chaque lien (selon la BP initiale);
· la longueur du réseau traversé et le débit de transmission;
· le nombre de routeurs traversés, et leur temps de traitement;
· la charge des routeurs traversés (traitement des files d'attente, taille des buffers, mécanismes de priorisation de flux);
· la taille des paquets de voix sur IP;
· la nature (UDP ou TCP) des autres paquets traités (hors voix sur IP);
· la taille des paquets issus d'autres services que la voix sur IP;
· la présence ou non de pics de trafic;
· etc …

I-2-1) Délai de transmission:

La maîtrise du délai de transmission est un élément essentiel pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho (similaire aux désagréments causés par les conversations par satellites, désormais largement remplacés par les câbles pour ce type d'usage).

Or la durée de traversée d'un réseau IP dépend de nombreux facteurs:
· le débit de transmission sur chaque lien;
· le nombre de routeurs traversés;
· le temps de traversée de chaque routeur, qui est lui même fonction de la puissance et la charge de ce dernier, du temps de mise en file d'attente des paquets, et du temps d'accés en sortie du routeur;
· et enfin, de délai de propagation de l'information, qui est non négligeable si on communique à l'opposé de la terre. Une transmission par fibre optique, à l'opposé de la terre, dure environ 70 ms.
Noter que le temps de transport de l'information n'est pas le seul facteur responsable de la durée totale de traitement de la parole. Le temps de codage et la mise en paquet de la voix concoure lui aussi de manière importante à ce délai.

Il est important de rappeler que sur les réseaux IP actuels (sans mécanismes de garantie de qualité de service), chaque paquet IP " fait sont chemin" indépendamment des paquets qui le précèdent ou le suivent: c'est ce qu'on appelle pudiquement le "Best effort" pour signifier que le réseau ne contrôle rien. Ce fonctionnement est fondamentalement différent de celui du réseau téléphonique où un circuit est établi pendant toute la durée de la communication.
Les chiffres suivants (tirés de la recommandation UIT-T G114) sont donnés à titre indicatif pour préciser les classes de qualité et d'interactivité en fonction du retard de transmission dans une conversation téléphonique. Ces chiffres concernent le délai total de traitement, et pas uniquement le temps de transmission de l'information sur le réseau.

Classe	Retard par sens	Commentaires
1	0 à 150 ms	Acceptable pour la plupart des conversations; seules quelques tâches hautement interactives peuvent souffrir.
2	150 à 300 ms	Acceptable pour des communications faiblement interactives (voir satellite 250 ms par bond)
3	300 à 700 ms	Devient pratiquement une communication half duplex
4	> à 700 ms	Inutilisable sans une bonne pratique de la conversation half duplex

En conclusion, on considère généralement que la limite supérieure " acceptable ", pour une communication téléphonique, se situe entre 150 et 200 ms par sens de transmission (en considérant à la fois le traitement de la voix et le délai d'acheminement).

I-2-2) Perte de paquets:

Lorsque les routeurs IP sont congestionnés, ils "libèrent" automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrant, en fonction de seuils prédéfinis. Cela permet également d'envoyer un signal implicite aux terminaux TCP qui diminuent d'autant leur débit au vu des acquittements négatifs émis par le destinataire qui ne reçoit plus les paquets. Malheureusement, pour les paquets de voix, qui sont véhiculés au dessus d'UDP, aucun mécanisme de contrôle de flux ou de retransmission des paquets perdus n'est offert au niveau du transport. D'ou

l'importance des protocoles RTP et RTCP qui permettent de déterminer le taux de perte de paquet, et d'agir en conséquence au niveau applicatif.
Si aucun mécanisme performant de récupération des paquets perdus n'est mis en place (cas le plus fréquent dans les équipements actuels), alors la perte de paquet IP se traduit par des ruptures au niveau de la conversation et une impression de hachure de la parole. Cette dégradation est bien sûr accentuée si chaque paquet contient un long temps de parole (plusieurs trames de voix de paquet). Par ailleurs, les codeurs à très faible débit sont généralement plus sensibles à la perte d'information, et mettent plus de temps à "reconstruire" un codage fidèle.
Enfin connaître le pourcentage de perte de paquets sur une liaison n'est pas assez suffisant pour déterminer la qualité de la voix que l'on peut espérer. En effet, un autre facteur essentiel intervient; il s'agit du modèle de répartition de cette perte de paquets, qui peut être soit " régulièrement" répartie, soit répartie de manière corrélée, c'est à dire avec des pics de perte lors des phases de congestion, suivies de phases des phases moins dégradées en terme de QoS.

I-2-3) Gigue:
La gigue est la variance statistique du délai de transmission . En d'autres termes, elle mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective. Cette irrégularité d'arrivée des paquets est due à de multiples raisons dont: l'encapsulation des paquets IP dans les protocoles supports (Frame Relay, ATM, …), la charge du réseau à un instant donné , la variation des chemins empruntés dans le réseau, etc…
Pour compenser la gigue, on utilise généralement des mémoires tampon (" buffer de gigue") qui permettent de lisser l'irrégularité des paquets. Malheureusement ces paquets présentent l'inconvénient de rallonger d'autant le temps de traversée global du système. Leur taille doit donc être soigneusement définie, et si possible adaptée de manière dynamique aux conditions du réseau.
La dégradation de la qualité de service due à la présence de gigue, se traduit, en fait par, par une combinaison des deux facteurs cités précédemment: le délai et la perte de paquets; puisque d'une part on introduit un délai supplémentaire de traitement (buffer de gigue) lorsque l'on décide d'attendre les paquets qui arrivent en retard, et que d'autre part on finit tout de même par perte certains paquets lorsque ceux-ci ont un retard qui dépasse le délai maximum autorisé par le buffer.

II - Outils de mesure de la Qualité de Service sur VoIP

La qualité de la voix sur IP résulte de deux composantes majeures:
· la qualité des équipements VoIP (type de codeur, annuleur d'écho, etc…)
· les caractéristiques du réseau support (perte de paquet, délai de transmission, gigue)
Pour évaluer cette qualité de service deux types d'outil (complémentaire l'un de l'autre) peuvent être employés:
· les outils de mesure de la qualité de la voix, qui permettent d'évaluer la dégradation de la voix, en fonction de la configuration des équipements et de la qualité du réseau de support;
· les outils de mesure de la qualité du réseau, qui permettent de " prédire" la qualité de la voix que pourrait fournir tel ou tel réseau.
Nous allons présenter, dans ce chapitre, quelques outils disponibles sur le marché, permettant de réaliser ces mesures.

II-1) Outils de mesure de la qualité de la voix:

Pour juger de la qualité de la voix, deux méthodes peuvent être employées: soit effectuer des tests réels auprès d'un panel d'auditeurs remplissant des grilles d'appréciation (tests dits subjectifs), soit s'appuyer sur un outil capable de mesurer les caractéristiques de la voix et de quantifier les éventuelles dégradations (mesures objectives).
Qu'il s'agisse de tests subjectifs ou de mesures objectives, les résultats doivent faire apparaître:
· les problèmes de distorsion de voix
· les problèmes de perte d'information
· les phénomènes d'écho
· les bruits parasites
· les fluctuations de niveau sonore
· les problèmes de transition voix/silence
· etc…

II-2) Outils de la mesure de la qualité du réseau:

Le second type d'outil de mesure a pour objectif d'analyser la QoS d'un réseau IP opérationnel, pour un trafic de type de voix.
Deux produits différents peuvent être mis en œuvre, selon que l'on souhaite tester la QoS du réseau avant d'ouvrir un service VoIP, ou que l'on souhaite tester cette qualité alors que le service est déjà en place, ou au moins que l'on dispose des équipements VoIP pour générer ce type de trafic.
Dans le premier cas l'outil de test permettra de répondre à la question suivante: " Mon réseau IP dispose t-il d'une bande passante et d'une QoS suffisante, pour supporter un service VoIP?"
Cette étude sera alors menée, sans devoir acquérir et installer, au préalable, des équipements.
Dans le second cas, l'outil permettra d'analyser la QoS d'un réseau supportant un service VoIP de manière opérationnelle, ce qui permettra de corréler la qualité perçue par les clients, à la QoS du réseau à un instant donné.

II-2-1) Outil d'analyse de QoS réseau, en prévision de l'ouverture d'un service VoIP

II-2-1-1) Simulateur de trafic VoIP (flux média)

Un tel outil doit simuler un trafic sur VoIP, en générant des paquets UDP de manière irrégulière, pour représenter les différentes phases de parole et de silence. La taille et la fréquence d'émission des paquets doit par ailleurs être paramétrable, afin de tester les diverses configurations de codeur possibles. L'outil doit enfin pouvoir simuler plusieurs appels simultanés, en augmentant le débit d'émission des paquets UDP.
Les opérations de pilotage de l'émission des paquets, de leur réception et de leur analyse doivent être effectuées à distance.
Concrètement, ce type d'outil se substitue à l'emploi de deux passerelles de téléphonie sur IP. Il permet donc de tester la QoS d'un réseau pour un service de type " Phone to Phone ", pour la partie transmission de la voix. Il ne mesure donc pas la QoS de bout en bout intègrant le temps de traitement du terminal et le temps de traversée des NAS. Il ne mesure pas non plus le temps d'établissement de l'appel.

II-2-2) Outil d'analyse de Qos réseau, pour un trafic réel de voix sur IP

Ce type d'outil s'appuie sur une infrastructure VoIP déjà en place, pour mesurer la qualité de service du réseau support pour le trafic de voix sur IP. Il ne s'agit pas d'un simulateur comme dans le cas

précédent, mais d’un analyseur des données transitant sur le réseau. Pour cela, l’outil vient piéger les éléments RTP et RTCP échangées, qui contiennent toutes les informations permettant de calculer le délai de transfert, la gigue et le taux de perte de paquets. Si l’équipement VoIP ne supporte pas le protocole RTCP, alors l’analyseur se rabat généralement sur les données RTP pour en déduire lui-même le nombre de paquets perdus et le délai de transfert.

L'outil devra fournir au minimum les informations suivantes : taux de perte de paquet, gigue, et délai de transmission. Mais il pourra aussi fournir divers indicateurs permettant d’améliorer le service et d’optimiser l’utilisation du réseau, ou encore d’établir des statistiques, voire la taxation du service. Parmi ces indicateurs, on peut citer (liste non exhaustive) :

· la répartition de la perte de paquets, de la gigue et du délai (facteurs de corrélation) ;
· le " desséquencement " des paquets ;
· l’activation du VAD et le pourcentage de parole / silence ;
· le type de codeur négocié et la longueur des trames ;
· le temps d’établissement d’appel
· le type de trafic (voix / fax / image / données)
· l’origine et la destination des appels
· l’heure et la durée d’appel
· informations de contrôle

III - Conclusion

Alors qu'il existe déja de nombreux logiciels ou appareils de mesure de la qualité de service sur les réseaux privés locaux, la mesure de la qualité de service sur les réseaux des opérateurs de télécommunication n'est pas encore une technique éprouvée. Faute de pouvoir mesurer réellement la qualité sur IP, pour le moment les opérateurs s'appuient très largement sur la couche ATM pour garantir des services de qualité. Mais de nombreux groupes de travail de la communauté Education et Recherche,aidés par les industriels, travaillent sur ce sujet. Les premiers instruments de mesure devraient sortir sur le marché pour début 2002.

Le Déni de Service Distribué (DDoS)

Background

Le "Distributed denial-of-service" ou déni de service distribué est un type d'attaque très évolué visant à faire planter ou à rendre muette une machine en la submergeant de trafic inutile (voir fiche DoS). Plusieurs machines à la fois sont à l'origine de cette attaque (c'est une attaque distribuée) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter. C'est pour cela que cette attaque représente une menace que beaucoup craignent.

Les outils

Pour mieux comprendre le phénomène, il parait impossible de ne pas étudier les outils les plus importants dans ce domaine, qui doivent leur notoriété à des célèbres attaques ayant visé des grands sites sur le net.

Un réseau typique se compose donc d'un maître (point central) et de nombreux hôtes distants, encore appelés démons. Pendant le déroulement de l'attaque, le hacker se connecte au maître qui envoie alors un ordre à tout les hôtes distants (via UDP, TCP ou ICMP). Ces communications peuvent également dans certains cas être chiffrées. Ensuite, les hôtes distants vont attaquer la cible finale suivant la technique choisie par le hacker. Ils vont par exemple se mettre à envoyer un maximum de paquets UDP sur des ports spécifiés de la machine cible. Cette masse de paquets va submerger la cible qui ne pourra plus répondre à aucune autre requête (d'où le terme de déni de service). D'autres attaques existent, tel que l'ICMP flood, le SYN flood (TCP), les attaques de type smurf, les attaques dites furtives, les attaques de déni de service dites agressives (dont le but est bel et bien de faire crasher complètement la cible), ou encore des attaques de type "stream attack" (TCP ACK sur des ports au hasard)...

Certains outils se sont même inspiré des chevaux de Troie (voir fiche sur les chevaux de Troie) qui installent de petits serveurs irc permettant au hacker de les commander via cette interface.

Contre-mesures

Il n'est pas évident de se prémunir contre ces attaques par déni de service, car la mise en place du réseau offensif par l'attaquant repose sur le fait que beaucoup de machines sont peu ou pas sécurisée et présentent des failles. Ces failles sont tellement nombreuses et d'autre part il existe tellement de machines vulnérables sur Internet qu'il devient impossible d'empêcher de telles attaques.
Ainsi, si un outil de DDoS est détecté sur un système, cela signifie sûrement que il a été installé sur de nombreux autres systèmes sans être décelé. D'autre part, la présence de cet outil signifie également que le système a été intégralement compromis, qu'il présente sûrement des backdoors et qu'on y a peut-être installé un rootkit (type Adore). Il est donc urgent et nécessaire de retirer complètement cette machine du réseau et de l'inspecter pour éventuellement la réinstaller.

Le Pushback : une contre-mesure en développement

Face aux menaces grandissantes provoquées par ce type d'attaques, les scientifiques se penchent de plus en plus sur des techniques capables de les contrer; une des plus récentes est la technique du Pushback.

Très brièvement, cette technique a pour but d'identifier les attaques de DoS et surtout de DDoS grâce à des heuristiques, de les contrer en remontant à leur source, enfin de maintenir et de protéger le bon trafic qui souffre également la plupart du temps des congestions engendrées par de telles attaques.

Cette méthode utilise un contrôle de congestion basé sur des agrégats, un agrégat étant défini comme un sous-ensemble du trafic présentant une propriété identifiable. Exemples de propriétés :

- Paquets TCP SYN
- Paquets à destination de X
- Paquets IP dont les checksums sont incorrects

Le but est d'identifier les agrégats responsables de la congestion et de les éliminer pour rétablir un trafic normal. Une fois la signature (c'est-à-dire la propriété identifiante, le trait caractéristique de l'attaque) établie, le flux est comparé en temps réel dans le routeur le plus proche de la cible du DDoS. Ce routeur commence à rejeter (drop) les paquets correspondants à la signature et envoie également un message d'alerte aux routeurs en amont sur les brins d'où lui parvient le trafic incriminé. Ce message d'alerte contient entre autres choses la signature qui va permettre à ces routeurs d'éliminer à leur tour les paquets correspondants à l'attaque. Et ces routeurs vont également envoyer des messages d'alerte aux routeurs situés en amont.
Cette technique récursive a pour avantage de pouvoir remonter jusqu'aux sources de l'attaque; elle permet également de décongestionner le coeur même du réseau, ce qui était impossible avec les techniques centrées sur la protection pure de la cible. Enfin, même si une partie du trafic légitime est tout de même perdue, les résultats finaux sont plutôt positifs.