Continue

Lorsque vous surfez sur internet, vous utilisez sans le savoir un serveur DNS. Sans lui, impossible d'afficher la moindre page ! Ce service s'apparente en quelque sorte à l'annuaire des sites web et permet aux moteurs de recherche de se connecter aux liens sélectionnés. Chaque site est identifié par une adresse IP - sorte de carte d'identité - composée d'une série de nombres séparés par des points, difficilement mémorisables par les internautes. Le nom de domaine se caractérise lui, par une succession de caractères correspondant au lien d'accès à un site web, bien plus simple à utiliser par l'internaute. Le serveur DNS a donc été conçu pour permettre la connexion aux services disponibles sur le web. Ce protocole absolument indispensable au fonctionnement et à l'utilisation d'Internet fait correspondre le nom de domaine du site web avec son adresse IP. C'est ce que l'on appelle un enregistrement DNS. C'est à partir des noms de domaine que le serveur DNS effectue les recherches d'adresses IP et charge la page du site recherché. Sans ce serveur, les internautes ne pourraient pas utiliser un navigateur pour trouver des sites web sans être obligés de mémoriser l'adresse IP des pages qu'ils souhaitent consulter. Tous les enregistrements DNS n'étant pas publics, il faut savoir qu'il existe des serveurs DNS privés et bien faire la distinction entre les deux. Les serveurs DNS publics sont accessibles à tous les internautes sans aucune restriction. Quant au DNS privé, il permet aux ordinateurs protégés par un pare-feu ou fonctionnant en réseau interne d'utiliser un enregistrement DNS privé afin que les ordinateurs locaux puissent communiquer entre eux en toute confidentialité. L'accès est donc uniquement réservé aux membres de l'organisation et impossible pour les autres internautes. Toutefois, il existe un point commun entre les serveurs DNS publics et les serveurs DNS privés : ils ne nécessitent aucune authentification. Fonctionnement du serveur DNS Un nombre incalculable d'ordinateurs composent le réseau internet. Il serait donc impensable de réunir les adresses de toutes ces machines dans un seul annuaire volumineux. Le DNS fonctionne à l'image des Pages jaunes divisées en petits répertoires appelés « domaines », chacun organisé en « zones ». Ainsi, lorsqu'un utilisateur recherche un site web, il saisit une adresse ou une requête dans la barre de recherche et le navigateur va interroger le serveur DNS afin d'obtenir l'adresse IP associée à ce site pour le localiser et le charger sur l'écran. De la même façon qu'une adresse postale permet de trouver un domicile ou une entreprise, le serveur DNS permet à l'utilisateur de se connecter à la bonne adresse sur le web. Il existe deux types de serveurs DNS : les DNS faisant autorité, c'est-à-dire le serveur qui stocke toutes les données et utilisé directement par l'internaute, et les DNS résolveurs qui interrogent le DNS d'autorité par l'intermédiaire des machines des utilisateurs pour accéder aux informations liées à la requête. Il existe également quatre serveurs DNS impliqués dans le chargement d'une page web : le récurseur DNS qui reçoit les requêtes des ordinateurs par le biais d'applications comme les navigateurs web et effectue les demandes supplémentaires nécessaires pour répondre aux requêtes DNS ; le serveur racine qui représente la première étape de la traduction des noms de domaines en adresses IP et permet de trouver d'autres emplacements plus spécifiques ; le serveur de noms TLD (Top-level domain) qui correspond au serveur de domaine de premier niveau et qui, en tant qu'étape suivante dans la recherche d'une adresse IP spécifique, héberge la dernière partie d'un nom d'hôte ; le serveur de noms de référence qui permet de traduire un nom spécifique en définition et représente la dernière étape d'une requête effectuée au serveur DNS. Les enregistrements DNS sur le serveur sont recherchés pendant le processus de résolution. S'ils sont disponibles, toutes les données du nom de domaine sont récupérées, sinon la requête est transmise à d'autres serveurs jusqu'à la récupération des données liées au nom de domaine. De la requête DNS à l'affichage d'une page web, le processus DNS repose sur une série d'étapes déclenchées lors d'une recherche : L'utilisateur saisit une URL dans un navigateur web. Cette requête est transmise au résolveur DNS qui se charge de trouver l'adresse IP connectée au site web. Le résolveur DNS, qui correspond généralement à celui du fournisseur d'accès à internet, recherche le TLD en envoyant la demande au serveur racine. Le serveur racine, qui répertorie tous les sites web de chaque TLD, répond au résolveur DNS en spécifiant le serveur qui correspond à l'extension de nom de domaine TLD lié à la requête. Après avoir trouvé le TLD, le résolveur DNS récupère l'adresse IP du site web. Puis il l'envoie aux serveurs de noms faisant autorité. Les serveurs de noms faisant autorité, qui disposent de toutes les informations nécessaires concernant le domaine, contrôlent l'adresse du site web souhaité avant de la renvoyer au navigateur. Maintenant que le navigateur connaît l'adresse IP, le site s'affiche. Comment résoudre un problème sur le serveur DNS ? Il arrive parfois que le serveur DNS ne réponde pas ou qu'il soit indisponible. Le message d'erreur « serveur DNS ne répond pas » peut-être lié à une défaillance du réseau. Dans ce cas, les utilisateurs ne peuvent pas charger les pages web qu'ils souhaitent consulter ni effectuer de requêtes sur un navigateur web. Pour résoudre ce problème, il existe plusieurs méthodes : choisir un autre navigateur web ; désactiver temporairement le pare-feu ; redémarrer le routeur ; changer de serveur DNS. La première chose à faire pour résoudre un problème de connexion au serveur DNS est de vérifier si ce problème provient du navigateur Internet. Pour cela, il suffit d'essayer soit de désinstaller et réinstaller votre navigateur habituel, soit d'accéder au site web souhaité en recourant à d'autres navigateurs sans oublier d'avoir au préalable vérifié leur configuration et leur version. Si le changement de navigateur ne permet pas de résoudre le problème, le pare-feu peut être en cause. Rien de plus simple, il suffit de le désactiver temporairement en passant par le panneau de configuration. L'autre moyen pour résoudre les problèmes de connexion à internet consiste au redémarrage du routeur en appuyant sur le bouton marche/arrêt ou en faisant un redémarrage forcé en débranchant le câble réseau. Dans ce cas, il faut attendre 30 secondes le temps que les composants électroniques se déchargent avant de rallumer le routeur. Si le problème persiste, changez de serveur DNS. En principe, ce dernier est automatiquement prédéfini par le fournisseur d'accès Internet. Toutefois, il peut être remplacé par n'importe quel autre serveur. Les services DNS publics que l'on trouve dans des listes de serveurs DNS spécifiques représentent de bonnes alternatives. Par exemple, Google fournit des serveurs DNS publics rapides, gratuits et fiables. Pour aller plus loin, découvrez l'hébergeur de site web gratuit de HubSpot et hébergez votre site web dans une infrastructure entièrement gérée et optimisée qui évolue avec votre entreprise. Les serveurs des DNS sont des serveurs qui cataloguent les adresses IP et permettent de les faire correspondre aux noms de domaines qu’ils référencent. Une requête sur un nom de domaine permet ainsi d’obtenir l’adresse IP associée et de se connecter sur le site recherché. Il existe plusieurs distinctions sur les serveurs DNS : Les serveurs DNS des FAI sont les connexions standards. Des DNS privés assurent des connexions plus rapides ou plus sécurisées. Les requêtes DNS sont traitées par quatre groupes de serveurs DNS et non par un seul serveur. Les DNS sont souvent la base d’attaques informatiques. « DNS » redirige ici. Pour les autres significations, voir DNS (homonymie). Domain Name System Informations Fonction Résolution de nom de domaine en adresse IP Sigle DNS Port 53 RFC 1983 : RFC 882[1] - RFC 883[2]1987 : RFC 1034[3] - RFC 1035[4]1994: RFC 1591[5]2011 : RFC 6195[6]2013 : RFC 6895[7]2018 : RFC 8375[8] - RFC 8467[9] - RFC 8483[10] - RFC 8484[11]2019 : RFC 8499[12] modifier Le Domain Name System[13] (Système de nom de domaine) ou DNS est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de résolution de noms, le DNS est un composant essentiel du développement du réseau informatique. À la demande de l'agence américaine pour les projets de recherche avancée de défense (DARPA), Jon Postel et Paul Mockapetris conçoivent le DNS et en rédigent la première implémentation en 1983. La structure du Domain Name System. Les équipements (ou hôtes) connectés à un réseau IP, comme Internet, possèdent une adresse IP qui les identifie sur le réseau. Ces adresses sont numériques afin de faciliter leur traitement par les machines. En IPv4, elles sont représentées sous la forme « - - - . - - - . - - - . - - - », où chaque groupe de trois tirets est substituable par un nombre entre 0 et 255 (en représentation décimale). En IPv6, les adresses sont représentées sous la forme « .... : .... : .... : .... : .... : .... : .... : .... », où chaque groupe de quatre points est substituable par une valeur hexadécimale de 0000 à FFFF. Pour faciliter l'accès aux hôtes sur un réseau IP, un mécanisme a été mis en place pour associer un nom à une adresse IP. Ce nom, plus simple à retenir qu'une suite de chiffres, est appelé « nom de domaine ». Résoudre un nom de domaine consiste à trouver l'adresse IP qui lui est associée. En plus des adresses IP, des informations complémentaires peuvent être associées aux noms de domaine comme des enregistrements dans le contexte de la lutte contre le spam (SPF), RRSIG pour la sécurité des informations du DNS (DNSSEC) ou NAPTR pour associer des numéros de téléphone à des adresses e-mail (ENUM). Article détaillé : hosts. Avant le DNS, la résolution d'un nom sur Internet devait se faire grâce à un fichier texte appelé HOSTS.TXT (RFC 608[14]) maintenu par le NIC du Stanford Research Institute et copié sur chaque ordinateur du réseau par transfert de fichier. En 1982, ce système centralisé montre ses limites et plusieurs propositions de remplacement voient le jour, parmi lesquelles le système distribué Grapevine de Xerox et IEN 116[15]. Le premier (Grapevine) est jugé trop compliqué tandis que le second (IEN 116) est insuffisant[16]. C’est finalement l’équipe dirigée par Elizabeth Feinler au NIC qui définira le Domain Name System afin de gérer la croissance de l'internet en déléguant la gestion des noms de domaine à des serveurs de noms distribués. Paul Mockapetris publie la conception du système dans les RFC 882[1] et RFC 883[2] en 1983. La norme correspondante est publiée dans les RFC 1034[3] et RFC 1035[4] en 1987. En 1987, le fichier HOSTS.TXT contenait 5 500 entrées, tandis que 20 000 hôtes étaient définis dans le DNS. Hiérarchie du DNS. Résolution itérative d'un nom dans le DNS par un serveur DNS (étapes 2 à 7) et réponse (étape 8) à la suite de l'interrogation récursive (étape 1) effectuée par un client (resolver) DNS. (remarque: Le serveur DNS récursif est dit récursif car il accepte ce type de requêtes mais il effectue des requêtes itératives) Le système des noms de domaine consiste en une hiérarchie dont le sommet est appelé la racine. On représente cette dernière par un point. Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une délégation pour ceux-ci, c'est-à-dire une indication que les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur. Ces sous-domaines peuvent à leur tour déléguer des sous-domaines vers d'autres serveurs. Tous les sous-domaines ne sont pas nécessairement délégués. Les délégations créent des zones, c'est-à-dire des ensembles de domaines et leurs sous-domaines non délégués qui sont configurés sur un serveur déterminé. Les zones sont souvent confondues avec les domaines. Les domaines se trouvant immédiatement sous la racine sont appelés domaine de premier niveau (Top Level Domain, TLD). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des domaines génériques (gTLD), par exemple .org ou .com. S'ils correspondent à des codes de pays (fr, be, ch, etc.), ce sont des domaines de premier niveau national, aussi appelés ccTLD de l'anglais country code TLD. On représente un nom de domaine en indiquant les domaines successifs séparés par un point, les noms de domaines supérieurs se trouvant à droite. Par exemple, le domaine org. est un TLD, sous-domaine de la racine. Le domaine wikipedia.org. est un sous-domaine de .org. Cette délégation est accomplie en indiquant la liste des serveurs DNS associée au sous-domaine dans le domaine de niveau supérieur. Les noms de domaines sont donc résolus en parcourant la hiérarchie depuis le sommet et en suivant les délégations successives, c'est-à-dire en parcourant le nom de domaine de droite à gauche. Pour qu'il fonctionne normalement, un nom de domaine doit avoir fait l'objet d'une délégation correcte dans le domaine de niveau supérieur. Les hôtes (ordinateurs des utilisateurs finaux) n'ont qu'une connaissance limitée du système des noms de domaine. Quand ils doivent résoudre un nom, ils s'adressent à un ou plusieurs serveurs de noms dits récursifs (ou résolveur) ou bien ils recherchent l'information dans les caches, comme ceux des navigateurs ou bien ceux des résolveurs eux-mêmes. Il y a deux types de serveurs DNS: les résolveurs (aussi appelés récursifs, bien qu'ils travaillent de manière itérative) et les serveurs faisant autorité[17]. Les serveurs DNS récursifs ne font qu'interroger les serveurs faisant autorité. Les serveurs faisant autorité détiennent les informations DNS sur les domaines sur lesquels ils ont autorité.serveurs faisant autorité Les serveurs récursifs vont parcourir la hiérarchie DNS et faire suivre la requête à un ou plusieurs autres serveurs de noms ayant autorité pour fournir une réponse. Les adresses IP de ces serveurs récursifs sont souvent obtenues par l'utilisateur final via DHCP ou encore configurés en dur sur la machine hôte de l'utilisateur. Les fournisseurs d'accès à Internet mettent à disposition de leurs clients ces serveurs récursifs. Il existe également des serveurs récursifs publics comme ceux de Cloudflare, Yandex.DNS, Google Public DNS, OpenNIC ou FDN. Quand l'ordinateur d'un utilisateur a besoin de charger une page internet de fr.wikipedia.org, il s'adresse d'abord à un serveur récursif pour trouver l'adresse IP (ie l'adresse numérique) de fr.wikipedia.org. Pour trouver l'adresse IP de fr.wikipedia.org, le serveur DNS récursif démarre un processus itératif pour consulter la hiérarchie DNS: Ce serveur demande à des serveurs DNS ayant autorité appelés serveurs racine quels serveurs ont autorité pour la zone org. Parmi ceux fournis dans la réponse, le serveur récursif va en choisir un pour lui demander quels serveurs ont autorité pour la zone wikipedia.org. C'est un de ces derniers qui pourra lui donner l'adresse IP de fr.wikipedia.org. S'il se trouve qu'un serveur ne répond pas, un autre serveur de la liste sera consulté. Pour optimiser les requêtes ultérieures, les serveurs DNS récursifs font aussi office de DNS cache : ils gardent en mémoire (cache) la réponse d'une résolution de nom afin de ne pas effectuer ce processus à nouveau ultérieurement. Cette information est conservée pendant une période nommée Time to live et associée à chaque nom de domaine. Il existe aussi un cache au niveau du navigateur de l'utilisateur et eventuellement de son système d'exploitation. Un nom de domaine peut être défini, à l'identique, dans plusieurs serveurs DNS ayant autorité. Généralement, les noms de domaines en utilisent au moins deux : un primaire et un secondaire. Il peut y avoir plusieurs serveurs secondaires. L'ensemble des serveurs primaires et secondaires font autorité pour un domaine, c'est-à-dire que la réponse ne fait pas appel à un autre serveur ou à un cache. Les serveurs récursifs fournissent des réponses qui ne sont pas nécessairement à jour, à cause du cache mis en place. On parle alors de réponse ne faisant pas autorité (non-authoritative answer). Cette architecture garantit au réseau Internet une certaine continuité dans la résolution des noms. Quand un serveur DNS tombe en panne, le bon fonctionnement de la résolution de nom n'est pas remis en cause dans la mesure où des serveurs secondaires sont disponibles. Pour trouver le nom de domaine associé à une adresse IP, on utilise un principe semblable. Dans un nom de domaine, la partie la plus générale est à droite : org dans fr.wikipedia.org, le mécanisme de résolution parcourt donc le nom de domaine de droite à gauche. Dans une adresse IP V4, c'est le contraire : 213 est la partie la plus générale de 213.228.0.42. Pour conserver une logique cohérente, on inverse l'ordre des quatre termes de l'adresse et on la concatène au pseudo domaine in-addr.arpa. Ainsi, pour trouver le nom de domaine de l'adresse IP 91.198.174.2, on résout 2.174.198.91.in-addr.arpa. La déclaration inverse est importante sur les adresses IP publiques Internet puisque l'absence d'une résolution inverse est considérée comme une erreur opérationnelle (RFC 1912[18]) qui peut entraîner le refus d'accès à un service. Par exemple, un serveur de messagerie électronique se présentant en envoi avec une adresse IP n'ayant pas de résolution inverse (PTR) a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier (message de refus de type : IP lookup failed). De plus, cette résolution inverse est importante dans le cadre de la réalisation de diagnostics réseaux car c'est elle qui permet de rendre les résultats de la commande traceroute humainement exploitables. Les dénominations des noms d'hôtes inverses sont souvent des composites de sous-domaines de localisation (ville, région, pays) et de domaines explicites indiquant le fournisseur d'accès Internet traversé comme francetelecom.net (- - - -.nctou202.Toulouse.francetelecom.net) et opentransit.net (- - - -.Aubervilliers.opentransit.net) pour France Télécom, ou encore proxad.net (- - - -.intf.routers.proxad.net) pour Free. Une adresse IP peut être associée à différents noms de domaine via l'enregistrement de plusieurs entrées PTR dans le sous-domaine .arpa consacré à cette adresse (in-addr.arpa. pour IPv4 et ip6.arpa. pour IPv6). L'utilisation d'enregistrements PTR multiples pour une même adresse IP est éventuellement présente dans le cadre de l'hébergement virtuel de multiples domaines web derrière la même adresse IP mais n'est pas recommandée dans la mesure où le nombre des champs PTR à renvoyer peut faire dépasser à la réponse la taille des paquets UDP de réponse et entraîner l'utilisation du protocole TCP (plus coûteux en ressources) pour envoyer la réponse à la requête DNS[19]. Les délégations des zones inverses se font sur une frontière d'octet, ce qui fonctionne quand les blocs d'adresses sont distribués de façon classful mais pose des problèmes quand les blocs assignés sont de taille quelconque. Par exemple, si deux clients A et B disposent chacun des blocs 192.168.0.0/25 et 192.168.0.128/25, il n'est pas possible de déléguer 0.168.192.in-addr.arpa. au premier pour qu'il puisse définir les PTR correspondant à ses hôtes, car cela empêcherait le second de faire de même. La RFC 2317[20] a défini une approche pour traiter ce problème, elle consiste à faire usage de domaines intermédiaires et de CNAME. $ORIGIN 0.168.192.in-addr.arpa. 0/25 NS ns.clientA.fr. 128/25 NS ns.clientB.fr. 0 CNAME 0.0/25.0.168.192.in-addr.arpa. 1 CNAME 1.0/25.0.168.192.in-addr.arpa. ... 127 CNAME 127.0/25.0.168.192.in-addr.arpa. 128 CNAME 128.128/25.0.168.192.in-addr.arpa. ... 255 CNAME 255.128/25.0.168.192.in-addr.arpa. Le client A définit la zone 0/25.0.168.192.in-addr.arpa. : $ORIGIN 0/25.0.168.192.in-addr.arpa. 1 PTR hote1.clientA.fr. ... 127 PTR hote127.clientA.fr. Le client B fait de même pour 128/25.0.168.192.in-addr.arpa. et les adresses 128 à 255. La résolution inverse de 192.168.0.1 aboutira aux requêtes suivantes : 1.0.168.192.in-addr.arpa. CNAME 1.0/25.0.168.192.in-addr.arpa. 1.0/25.0.168.192.in-addr.arpa. PTR hote1.clientA.fr. Ce qui assure le fonctionnement de la résolution inverse, moyennant un niveau d'indirection supplémentaire. Article détaillé : Serveur racine du DNS. Les serveurs racine sont gérés par douze organisations différentes : deux sont européennes, une japonaise et les neuf autres sont américaines. Sept de ces serveurs sont en réalité distribués dans le monde grâce à la technique anycast et neuf disposent d'une adresse IPv6[21]. Grâce à anycast, plus de 200 serveurs répartis dans 50 pays du monde assurent ce service[22]. Il existe 13 autorités de nom appelées de a à m.root-servers.net. Le serveur k reçoit par exemple de l'ordre de 70 000 à 100 000 requêtes par seconde en avril 2019[23]. Le DNS ne fournit pas de mécanisme pour découvrir la liste des serveurs racine, chacun des serveurs doit donc connaître cette liste au démarrage grâce à un encodage explicite. Cette liste est ensuite mise à jour en consultant l'un des serveurs indiqués. La mise à jour de cette liste est peu fréquente de façon que les serveurs anciens continuent à fonctionner. Article détaillé : Fully qualified domain name. On entend par Fully Qualified Domain Name (FQDN, Nom de domaine pleinement qualifié) un nom de domaine écrit de façon absolue, y compris tous les domaines jusqu'au domaine de premier niveau (TLD), il est ponctué par un point final, par exemple fr.wikipedia.org. La norme prévoit qu'un élément d'un nom de domaine (appelé label) ne peut dépasser 63 caractères, un FQDN ne pouvant dépasser 253 caractères. Article détaillé : Nom de domaine internationalisé. Dans leur définition initiale, les noms de domaines sont constitués des caractères de A à Z (sans différence de casse : les lettres capitales ne sont pas différenciées), de chiffres et du trait d'union. La RFC 3490[24] définit un format appelé Punycode qui permet l'encodage d'un jeu de caractère plus étendu. Article détaillé : DNS round-robin. Lorsqu'un service génère un trafic important, celui-ci peut faire appel à la technique du DNS Round-Robin (tourniquet DNS), une des techniques de répartition de charge qui consiste à associer plusieurs adresses IP à un FQDN. Les différentes versions de Wikipedia, comme fr.wikipedia.org par exemple, sont associées à plusieurs adresses IP : 207.142.131.235, 207.142.131.236, 207.142.131.245, 207.142.131.246, 207.142.131.247 et 207.142.131.248. L'ordre dans lequel ces adresses sont renvoyées sera modifié d'une requête à la suivante. Une rotation circulaire entre ces différentes adresses permet ainsi de répartir la charge générée par ce trafic important entre les différentes machines ayant ces adresses IP. Il faut cependant nuancer cette répartition car elle n'a lieu qu'à la résolution du nom d'hôte et reste par la suite en cache sur les différents resolvers (client DNS). Article détaillé : Liste des enregistrements DNS. Le type d'enregistrement de ressource (RR, Resource Record) est codé sur 16 bits[25], l'IANA conserve le registre des codes assignés[26]. Les principaux types d'enregistrements définis sont les suivants : A record ou address record (également appelé enregistrement d’hôte) qui fait correspondre un nom d'hôte ou un nom de domaine ou un sous-domaine à une adresse IPv4 de 32 bits distribués sur quatre octets ex: 123.234.1.2 ; AAAA record ou IPv6 address record qui fait correspondre un nom d'hôte à une adresse IPv6 de 128 bits distribués sur seize octets ; CNAME record ou canonical name record qui permet de faire un alias d'un domaine vers un autre. MX record ou mail exchange record qui définit les serveurs de courriel pour ce domaine ; PTR record ou pointer record qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit « reverse » puisqu'il fait exactement le contraire du A record ; NS record ou name server record qui définit les serveurs DNS de ce domaine ; SOA record ou Start Of Authority record qui donne les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone ; SRV record qui généralise la notion de MX record, mais qui propose aussi des fonctionnalités avancées comme le taux de répartition de charge pour un service donné, standardisé dans la RFC 2782[27] ; NAPTR record ou Name Authority Pointer record qui donne accès à des règles de réécriture de l'information, permettant des correspondances assez lâches entre un nom de domaine et une ressource. Il est spécifié dans la RFC 3403[28] ; TXT record permet à un administrateur d'insérer un texte quelconque dans un enregistrement DNS (par exemple, cet enregistrement est utilisé pour implémenter la spécification Sender Policy Framework) ; d'autres types d'enregistrements sont utilisés occasionnellement, ils servent simplement à donner des informations (par exemple, un enregistrement de type LOC indique l'emplacement physique d'un hôte, c'est-à-dire sa latitude et sa longitude). Certaines personnes[Qui ?] disent que cela aurait un intérêt majeur mais n'est que très rarement utilisé sur le monde Internet. L'enregistrement NS crée une délégation d'un sous-domaine vers une liste de serveurs. Dans la zone org, les enregistrements NS suivants créent le sous-domaine wikipedia et délèguent celui-ci vers les serveurs indiqués. L'ordre des serveurs est quelconque. Tous les serveurs indiqués doivent faire autorité pour le domaine. wikipedia NS ns1.wikimedia.org. wikipedia NS ns2.wikimedia.org. wikipedia NS ns0.wikimedia.org. À l'inverse d'une entrée de type A ou AAAA, une entrée PTR indique à quel nom d'hôte correspond une adresse IPv4 ou IPv6. Si elle est spécifiée, elle doit contenir l'enregistrement inverse d'une entrée DNS A ou AAAA. Par exemple (pour une adresse IPv4) cet enregistrement PTR : 232.174.198.91.in-addr.arpa. IN PTR text.esams.wikimedia.org. correspond à cette entrée A : text.esams.wikimedia.org. IN A 91.198.174.232 Dans le cas d'une adresse IPv6, les entrées de type PTR sont enregistrées dans la zone ip6.arpa. (pendant de la zone in-addr.arpa. des adresses IPv4). La règle permettant de retrouver l'entrée correspondant à une adresse IPv6 est similaire à celle pour les adresses IPv4 (renversement de l'adresse et recherche dans un sous-domaine dédié de la zone arpa.), mais diffère au niveau du nombre de bits de l'adresse utilisés pour rédiger le nom du domaine où rechercher le champ PTR : là où pour IPv4 le découpage de l'adresse se fait par octet, pour IPv6 c'est un découpage par quartet qui est utilisé. Par exemple à l'adresse IPv6 : 2001:610:240:22::c100:68b correspond le nom de domaine : b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa. PTR www.ipv6.ripe.net. Une entrée DNS MX indique les serveurs SMTP à contacter pour envoyer un courriel à un utilisateur d'un domaine donné. Par exemple : wikimedia.org. IN MX 10 mchenry.wikimedia.org. wikimedia.org. IN MX 50 lists.wikimedia.org. On voit que les courriels envoyés à une adresse en @wikimedia.org sont envoyés au serveur mchenry.wikimedia.org. ou lists.wikimedia.org. Le nombre précédant le serveur représente la priorité. Le serveur avec la priorité numérique la plus petite est employé en priorité. Ici, c'est donc mchenry.wikimedia.org. qui doit être utilisé en premier, avec une valeur de 10. Les serveurs indiqués doivent avoir été configurés pour accepter de relayer les courriers pour le nom de domaine indiqué. Une erreur courante consiste à indiquer des serveurs quelconques comme serveurs secondaires, ce qui aboutit au rejet des courriers quand le serveur primaire devient inaccessible. Il n'est pas indispensable de disposer de serveurs secondaires, les serveurs émetteurs conservant les messages pendant un temps déterminé (typiquement, plusieurs jours) jusqu'à ce que le serveur primaire soit à nouveau disponible. Les entrées MX sont généralisées par les entrées SRV qui permettent de faire la même chose mais pour tous les services, pas seulement SMTP (le courriel). L'avantage des entrées SRV par rapport aux entrées MX est aussi qu'elles permettent de choisir un port arbitraire pour chaque service ainsi que de faire de la répartition de charge plus efficacement. L'inconvénient c'est qu'il existe encore peu de programmes clients qui gèrent les entrées SRV. Cependant, depuis 2009, avec l'augmentation de l'utilisation du protocole SIP sur les services de VoIP, les enregistrements SRV deviennent plus fréquents dans les zones DNS. L'enregistrement CNAME permet de créer un alias. Par exemple : fr.wikipedia.org. IN CNAME text.wikimedia.org. text.wikimedia.org. IN CNAME text.esams.wikimedia.org. text.esams.wikimedia.org. IN A 91.198.174.232 Celui-ci exclut tout autre enregistrement (RFC 1034[3] section 3.6.2, RFC 1912[18] section 2.4), c'est-à-dire qu'on ne peut avoir à la fois un CNAME et un A record pour le même nom de domaine. Par exemple, ceci est interdit : fr.wikipedia.org. IN CNAME text.wikimedia.org. fr.wikipedia.org. IN A 91.198.174.232 Par ailleurs, pour des raisons de performance, et pour éviter les boucles infinies du type fr.wikipedia.org. IN CNAME text.wikimedia.org. text.wikipedia.org. IN CNAME fr.wikimedia.org. les spécifications (RFC 1034[3] section 3.6.2, RFC 1912[18] section 2.4) recommandent de ne pas faire pointer un CNAME sur un autre CNAME ni sur un DNAME (alias pour un nom et tous ses sous-noms). Ainsi, le premier exemple serait préférablement enregistré de la façon suivante : fr.wikipedia.org. IN CNAME text.esams.wikimedia.org. text.wikimedia.org. IN CNAME text.esams.wikimedia.org. text.esams.wikimedia.org. IN A 91.198.174.232 Peu répandus à l'heure actuelle (ils sont surtout utilisés par ENUM), ils décrivent une réécriture d'une clé (un nom de domaine) en URI. Par exemple, dans ENUM, des enregistrements NAPTR peuvent être utilisés pour trouver l'adresse de courrier électronique d'une personne, connaissant son numéro de téléphone (qui sert de clé à ENUM). Ses paramètres sont dans l'ordre : Order : indique dans quel ordre évaluer les enregistrements NAPTR ; tant qu'il reste des enregistrements d'une certaine valeur de order à examiner, les enregistrements des valeurs suivantes de order n'entrent pas en considération ; Preference : donne une indication de priorité relative entre plusieurs enregistrements NAPTR qui ont la même valeur de order ; Flags : indique par exemple si l'enregistrement décrit une réécriture transitoire (dont le résultat est un nom de domaine pointant sur un autre enregistrement NAPTR) ou une réécriture finale ; la sémantique précise du paramètre flags dépend de l'application DDDS ('Dynamic Delegation Discovery System', RFC 3401[29]) employée (ENUM en est une parmi d'autres) ; Services : décrit le service de réécriture ; par exemple dans ENUM, la valeur de services spécifie le type de l'URI résultante ; la sémantique précise de ce paramètre dépend également de l'application DDDS employée ; Regexp : l'opération de réécriture elle-même, formalisée en une expression rationnelle ; cette expression rationnelle est à appliquer à la clé ; ne peut être fourni en même temps que replacement ; Replacement : nom de domaine pointant sur un autre enregistrement NAPTR, permettant par exemple une réécriture transitoire par délégation ; ne peut être fourni en même temps que regexp. L'enregistrement NAPTR est défini par la RFC 3403[28]. Article détaillé : SOA Resource Record. Cet enregistrement permet d'indiquer le serveur de nom maître (primaire), l'adresse e-mail d'un contact technique (avec @ remplacé par un point) et des paramètres d'expiration. Il désigne l'autorité (start of authority) ou le responsable de la zone dans la hiérarchie DNS. C'est l'acte de naissance de la zone DNS. Ces paramètres sont dans l'ordre : wikipedia.org. IN SOA ns0.wikimedia.org. hostmaster.wikimedia.org. 2010060311 43200 7200 1209600 3600 Serial : indique un numéro de version pour la zone (32 bits non signé). Ce nombre doit être incrémenté à chaque modification du fichier zone ; on utilise par convention une date au format « yyyymmddnn » (« yyyy » pour l'année sur 4 chiffres, « mm » pour le mois sur 2 chiffres, « dd » pour le jour sur 2 chiffres, « nn » pour un compteur de révision si le numéro de série est modifié plusieurs fois dans un même jour. Cette convention évite tout débordement du 32 bits non signé jusqu'en l'an 4294) ; Refresh : l'écart en secondes entre les demandes successives de mise à jour réalisées depuis le serveur secondaire ou les serveurs esclaves ; Retry : le délai en secondes que doivent attendre le serveur secondaire ou les serveurs esclaves lorsque leur précédente requête a échoué ; Expire : le délai en secondes au terme duquel la zone est considérée comme invalide si le secondaire ou les esclaves ne peuvent joindre le serveur primaire ; Minimum ou negative TTL : utilisé pour spécifier, en secondes, la durée de vie pendant laquelle sont conservées en cache les réponses qui correspondent à des demandes d'enregistrements inexistants. Les versions récentes de BIND (named) acceptent les suffixes M, H, D ou W pour indiquer un intervalle de temps en minutes, heures, jours ou semaines respectivement. Chaque enregistrement est associé à un Time To Live (TTL) qui détermine combien de temps il peut être conservé dans un serveur cache. Ce temps est typiquement d'un jour (86400 s) mais peut être plus élevé pour des informations qui changent rarement, comme des records NS. Il est également possible d'indiquer que des informations ne doivent pas être mises en cache en spécifiant un TTL de zéro. Certaines applications, comme des navigateurs web disposent également d'un cache DNS, mais qui ne respecte pas nécessairement le TTL du DNS. Ce cache applicatif est généralement de l'ordre de la minute, mais Internet Explorer par exemple conserve les informations jusqu'à 30 minutes[30], indépendamment du TTL configuré. Quand un domaine est délégué à un serveur de noms qui appartient à ce sous-domaine, il est nécessaire de fournir également l'adresse IP de ce serveur pour éviter les références circulaires. Ceci déroge au principe général selon lequel l'information d'un domaine n'est pas dupliquée ailleurs dans le DNS. Par exemple, dans la réponse suivante au sujet des NS pour le domaine wikimedia.org : wikimedia.org. IN NS ns2.wikimedia.org. wikimedia.org. IN NS ns1.wikimedia.org. wikimedia.org. IN NS ns0.wikimedia.org. Il est nécessaire de fournir également les adresses IP des serveurs indiqués dans la réponse (glue records[31]), car ils font partie du domaine en question : ns0.wikimedia.org. IN A 208.80.152.130 ns1.wikimedia.org. IN A 208.80.152.142 ns2.wikimedia.org. IN A 91.198.174.4 Une extension du DNS nommée DNS dynamique (DDNS) permet à un client de mettre à jour une zone avec des informations qui le concernent (RFC 2136[32]). Ceci est utile quand des clients obtiennent une adresse IP par DHCP et qu'ils souhaitent que le DNS reflète le nom réel de la machine. Les mises à jour se font sur le serveur primaire du domaine, les serveurs secondaires recopiant les informations du serveur primaire dans un mécanisme appelé transfert de zone. Pour déterminer si un transfert de zone doit avoir lieu, le serveur secondaire consulte le numéro de version de la zone et le compare à la version qu'il possède. Le serveur primaire détermine à quelle fréquence le numéro de version est consulté. Quand un changement est effectué, les serveurs envoient des messages de notification aux serveurs secondaires pour accélérer le processus. Il se peut que des informations qui ne sont plus à jour soient cependant conservées dans des serveurs cache. Il faut alors attendre l'expiration de leur TTL pour que ces informations cachées disparaissent et donc que la mise à jour soit pleinement effective. On peut minimiser le temps nécessaire en diminuant le TTL associé aux noms de domaines qui vont être modifiées préalablement à une opération de changement. Quand la liste des serveurs de noms change, ou quand une adresse IP qui fait l'objet d'un Glue Record est modifiée, le gestionnaire du domaine de niveau supérieur doit effectuer la mise à jour correspondante. Pour éviter les points individuels de défaillance, on évite de partager l'infrastructure entre les serveurs qui font autorité. Un serveur secondaire sera de préférence délocalisé et routé différemment du serveur primaire. Bien que cela soit techniquement possible, on évite de mêler sur un même serveur le rôle de DNS récursif et celui de serveur qui fait autorité. De même, un hôte sera configuré avec plusieurs serveurs récursifs, de sorte que si le premier ne répond pas à la requête, le suivant sera employé. En général, les serveurs récursifs fournis par les FAI refusent les requêtes émanant d'adresses IP appartenant à d'autres FAI. Il existe des services de DNS récursifs ouverts, c'est-à-dire qu'ils acceptent les requêtes de tous les clients. Il est donc possible à un utilisateur de configurer ceux-ci en lieu et place de ceux fournis par le FAI. Ceci pose cependant les problèmes suivants : il n'y a pas de garantie que les réponses fournies seront les mêmes qu'avec des serveurs récursifs habituels. Un tel service pourrait en effet faire référence à une autre hiérarchie depuis la racine, disposer de TLD additionnels non standard, restreindre l'accès à certains domaines, voire altérer certains records avant leur transmission au client ; il n'y a pas de garantie de confidentialité, c'est-à-dire que ce service pourrait déterminer à quels domaines un utilisateur a accès en conservant des traces des requêtes DNS. Le protocole DNS a été conçu avec un souci minimum de la sécurité. Plusieurs failles de sécurité du protocole DNS ont été identifiées depuis. Les principales failles du DNS ont été décrites dans le RFC 3833[33] publié en août 2004. Une des failles mises en avant est la possibilité d'intercepter les paquets transmis. Les serveurs DNS communiquent au moyen de paquets uniques et non signés. Ces deux spécificités rendent l'interception très aisée. L'interception peut se concrétiser de différentes manières, notamment via une attaque de type « man in the middle », de l'écoute des données transférées et de l'envoi de réponse falsifiée (voir paragraphe ci-dessous). Les paquets des serveurs DNS étant faiblement sécurisés, authentifiés par un numéro de requête, il est possible de fabriquer de faux paquets. Par exemple, un utilisateur qui souhaite accéder au site fait une demande au site DNS. Il suffit, à ce moment, qu'un pirate informatique réponde à la requête de l'utilisateur avant le serveur DNS pour que l'utilisateur se retrouve sur un site d'hameçonnage. La trahison par un serveur, ou corruption de données, est, techniquement, identique à une interception des paquets. La seule différence venant du fait que l'utilisateur envoie volontairement sa requête au serveur. Cette situation peut arriver lorsque, par exemple, l'opérateur du serveur DNS souhaite mettre en avant un partenaire commercial. Article détaillé : empoisonnement du cache DNS. L'empoisonnement du cache DNS ou pollution de cache DNS (en anglais, DNS Cache Poisoning) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une requête valide tandis qu'elle est frauduleuse[34]. Article détaillé : Déni de service. Une attaque par déni de service, ou attaque par saturation, (en anglais, Denial of Service attack ou DoS attack) est une attaque sur un serveur informatique qui résulte en l'incapacité pour le serveur de répondre aux requêtes de ses clients. Article détaillé : DNSSEC. Pour contrer les vulnérabilités dues à la corruption des données, l'empoisonnement de cache DNS, etc., le protocole DNSSEC (RFC 4033[35], RFC 4034[36], RFC 4035[37]) a été développé. Il utilise les principes de cryptographie asymétrique et de signature numérique pour garantir l'intégrité des données, ainsi qu'une preuve de non-existence si l'enregistrement demandé n'existe pas. La zone racine du DNS a été signée le 15 juillet 2010[38], et le déploiement de DNSSEC sur les TLD continue, une liste des domaines couverts étant disponible. Depuis 2015[39], l'Internet Engineering Task Force (IETF) travaille à la sécurité du canal de communication du DNS (là où DNSSEC protège les données). Cela a débouché sur la publication de plusieurs RFC permettant l'utilisation de TLS afin de chiffrer la communication entre les clients DNS et les résolveurs. Il s'agit principalement de : DNS sur TLS (RFC 7858[40], utilisant le port 853) et DNS sur HTTPS (RFC 8484[11], requête DNS encapsulée dans une requête HTTP, et traitée par un serveur web). Il n'y a pas, en 2018, de possibilités de chiffrer – via TLS – les communications entre un résolveur et un serveur faisant autorité. En juillet 2008, quelques jours après la publication du rapport de la United States Computer Emergency Readiness Team concernant la faille de sécurité des serveurs DNS permettant d'empoisonner leur cache, plusieurs serveurs DNS majeurs ont subi des attaques. Une des plus importantes fut celle menée contre les serveurs de AT&T. L'attaque empoisonnant le cache des serveurs DNS de AT&T a permis au pirate informatique de rediriger toutes les requêtes de Google vers un site d'hameçonnage[41]. DNS utilise en général UDP et le port 53. La taille maximale des paquets utilisée est de 512 octets. Si une réponse dépasse cette taille, la norme prévoit que la requête doit être renvoyée sur le port TCP 53. Ce cas est cependant rare et évité, et les firewalls bloquent souvent le port TCP 53. L'extension EDNS0 (RFC 2671[42]) permet d'utiliser une taille de paquets plus élevée, sa prise en charge est recommandée pour IPv6 comme pour DNSSEC. La norme prévoit qu'il existe une classe associée aux requêtes. Les classes IN (Internet), CH (Chaos) et HS (Hesiod (en)) sont définies, seule la classe IN étant réellement utilisée en pratique. La classe chaos est utilisée par BIND pour révéler le numéro de version[43]. Pour vérifier l'association entre un nom et une adresse IP, plusieurs commandes sont disponibles suivant les systèmes d'exploitation utilisés. Par exemple sur Windows la commande nslookup est disponible via l'invite de commande : > nslookup www.google.fr Serveur : Livebox-6370 Address: 192.168.1.1 Réponse ne faisant pas autorité : Nom : www.l.google.com Addresses: 209.85.229.104 209.85.229.106 209.85.229.103 209.85.229.147 209.85.229.105 209.85.229.99 Aliases: www.google.fr www.google.com ou encore dig sur les systèmes compatibles avec UNIX : > dig www.google.com aaaa ; DiG 9.7.0-P1 www.google.com aaaa ;; global options: +cmd ;; Got answer: ;; ->>HEADER

- huwenoza
- varufu
- instruction manual meaning in telugu
- http://dovolena-jiznicechy.cz/uploads/xekiwolezunu_pawivibefefin_favogokisigubov.pdf
- pomejarupo
- https://infomohelnice.cz/www/ckeditor/kcfinder/upload/files/4340700101.pdf
- http://mariopresto.pl/userfiles/file/8c1a2f7b-0364-41bf-8f96-4f57d4bb8e83.pdf
- linimi
- https://house-well.com/home/housewel/images/ckfinder/files/20250711044026.pdf
- vorufulo
- http://tchid.net/userfiles/file/15861711860.pdf
- covuromu
- how many lakes are there in virginia
- what is the best exercise equipment for beginners
- http://bebsulmare.com/userfiles/files/xasepir_watujevesa_xepuzaja_fovekuvubozowi.pdf
- https://ahiosh.org/userfiles/file/pimotupigimake.pdf
- vocabulary for delf b2
- http://albachiara.info/userfiles/files/427b0cb3_9db7_46f0_acb8_38650b00277a.pdf