Réseaux informati

Nouvelle édition en français

Cisco CCNA

Guide de préparation à l'examen de certification CCNA 200-301

Volume 1

Fondamentaux TCP/IP

Cisco CCNA 200-301 Volume 1

Guide de préparation au Cisco CCNA 200-301 en français, Volume 1 Fondamentaux TCP/IP

François-Emmanuel Goffinet

Ce livre est en vente à http://leanpub.com/cisco-ccna-1

Version publiée le 2021-09-19

Aussi par François-Emmanuel Goffinet

Cisco CCNA 200-301 Volume 2

Cisco CCNA 200-301 Volume 3

Cisco CCNA 200-301 Volume 4

Linux Administration Volume 1

Linux Administration Volume 2

Linux Administration Volume 3

Linux Administration Volume 4

Protocole SIP

Table des matières

Avertissement

Le projet lié à cet ouvrage est conçu principalement pour des candidats francophones à l'examen de certification Cisco CCNA 200-301.

Le document sera probablement utile comme *support de formation* dans d'autres contextes tels que celui de l'autoapprentissage, de l'enseignement ou de la formation professionnelle.

Si le document peut sans doute contribuer à mieux connaître les réseaux d'entreprise dans la perspective du CCNA, il ne peut aucunement garantir la réussite de l'examen. Aussi, ce projet n'a jamais poursuivi l'ambition de remplacer d'autres sources d'information/formation issues des canaux officiels tels que *Cisco Press*, *Cisco Learning Network*, les *Cisco Systems Learning Partners*, *Cisco Academy* ou encore la documentation officielle du fabricant. D'ailleurs l'auteur est totalement indépendant de tout fabricant cité. Celles-ci, toutes mieux présentées les unes que les autres, ne manquent pas au contraire, mais il est rare de trouver des sources de qualité et fiables en français.

Copyrights

Dédicace

À mes parents qui m'ont toujours apporté un soutien sans faille dans tous mes projets.

Remerciements

Merci aux milliers de visiteurs quotidiens du site cisco.goffinet.org.

Merci aux centres de formation et aux écoles qui m'accordent leur confiance et qui me permettent de rencontrer mon public en personne.

Merci à Wendell Odom, mon mentor sur le sujet Cisco CCNA. N'hésitez pas à vous procurer ses livres en anglais chez Cisco Press.

Merci à Stéphane Bortzmeyer dont la prose prolifique m'inspire et m'aide à vulgariser les technologies de l'Internet.

Merci enfin à Cisco Systems d'être aussi ouvert depuis tant d'années dans sa documentation et pour son effort à rendre les technologies des réseaux plus accessibles, mieux comprises et plus populaires.

Avant-Propos

François-Emmanuel Goffinet est formateur IT et enseignant depuis 2002 en Belgique et en France. Outre Cisco CCNA, il couvre de nombreux domaines des infrastructures informatiques, du réseau à la virtualisation des systèmes, du nuage à la programmation d'infrastructures hétérogènes en ce y compris DevOps, Docker, K8s, chez AWS, GCP ou Azure, etc. avec une forte préférence et un profond respect pour l'Open Source, notamment pour Linux.

On trouvera ici un des résultats d'un projet d'autopublication en mode *agile* plus large lié au site web cisco.goffinet.org. La documentation devrait évoluer dans un format vidéo. Les sujets développés devraient trouver des questionnaires de validation de connaissances. Enfin, une solution accessible et abordable de simulation d'exercices pratiques mériterait réflexion.

Cisco CCNA 200-301

L'examen Cisco CCNA 200-301[1] est disponible en anglais uniquement. Il se déroule sous surveillance dans un centre de test VUE après une inscription sur leur site vue.com et un paiement (de maximum 300 EUR) avec un bon de réduction (*voucher*) ou par carte de crédit.

Cet examen de niveau fondamental sur la théorie des réseaux évalue votre niveau avec un examen sur ordinateur en anglais constitué d'une centaine de questions théoriques et pratiques. Cet examen a une durée de 120 minutes. Il est interdit de revenir sur une question à laquelle on a déjà répondu. Le seuil de réussite est fixé entre 82,5% et 85%. Tout diplômé d'un premier cycle de l'enseignement supérieur en informatique devrait être en mesure de réussir cet examen dans un délai de trois mois. Tout qui voudrait entrer dans une carrière dans les réseaux ne perd pas son temps en passant cet examen. Certains prétendent même que c'est fortement recommandé.

Sujets et objectifs de l'examen Cisco CCNA 200-301

On trouve 53 objectifs dans six sujets[2] : Fondamentaux des Réseaux (20%), Accès au Réseau (20%), Connectivité IP (25%), Services IP (10%), Sécurité de base (15%), Automation et Programmabilité (10%).

On trouve aussi dix verbes dans les objectifs de la certification CCNA 200-301 qui correspondent à certaines compétences à valider :

1. "Expliquer" (6)
2. "Décrire" (15)
3. "Comparer" (6)
4. "Identifier" (1)
5. "Reconnaître" (1)
6. "Interpréter" (2)
7. "Déterminer" (1)
8. "Définir" (1)
9. "Configurer" (17)
10. "Vérifier" (1)

On peut considérer que seuls les objectifs qui demandent à "Configurer" et à "Vérifier" seraient purement pratiques. Toutefois, "Identifier", "Interpréter" et "Déterminer" pourraient aussi trouver leur application opérationnelle. Les autres objectifs comme "Expliquer", "Décrire", "Définir", "Reconnaître" seraient validés par des questions d'examen plus théoriques.

Les objectifs développés dans ce volume sont indiqués en gras.

1. La page officielle de la certification se trouve à cette adresse.
2. La page officielle des sujets et des objectifs du Cisco CCNA 200-301 se trouve à cette adresse.

1.0 Fondamentaux des Réseaux - 20%

- 1.1 Expliquer le rôle et la fonction des composants réseau
  - 1.1.a Routeurs
  - 1.1.b Commutateurs (switches) L2 et L3
  - 1.1.c Pare-feu NG (Next-generation firewalls) et IPS
  - 1.1.d Point d'accès (Access points)
  - 1.1.e Controlleurs (Cisco DNA Center et WLC)
  - 1.1.f Points terminaux (Endpoints)
  - 1.1.g Serveurs
- 1.2 Décrire les caractéristiques des architectures et topologies réseau
  - 1.2.a 2 tier
  - 1.2.b 3 tier
  - 1.2.c Spine-leaf
  - 1.2.d WAN
  - 1.2.e Small office/home office (SOHO)
  - 1.2.f On-premises et cloud
- 1.3 Comparer les interfaces physiques et les types de câble
  - 1.3.a Fibre monmode (Single-mode) et fibre multimode, cuivre
  - 1.3.b Connexions (Ethernet shared media et point-to-point)
  - 1.3.c Concepts sur PoE
- 1.4 Identifier les problèmes d'interface et de câbles (collisions, errors, mismatch duplex, et/ou speed)
- 1.5 Comparer TCP à UDP
- 1.6 Configurer et vérifier l'adressage et le sous-réseautage (subnetting) IPv4
- 1.7 Décrire la nécessité d'un adressage IPv4 privé
- 1.8 Configurer et vérifier l'adressage et les préfixes IPv6
- 1.9 Comparer les types d'adresses IPv6
  - 1.9.a Global unicast
  - 1.9.b Unique local
  - 1.9.c Link local
  - 1.9.d Anycast
  - 1.9.e Multicast
  - 1.9.f Modified EUI 64
- 1.10 Vérifier les paramètres IP des OS clients (Windows, Mac OS, Linux)
- 1.11 Décrire les principes des réseaux sans-fil
  - 1.11.a Nonoverlapping Wi-Fi channels
  - 1.11.b SSID
  - 1.11.c RF
  - 1.11.d Encryption
- 1.12 Expliquer les fondamentaux de la virtualisation (virtual machines)
- 1.13 Décrire les concepts de la commutation (switching)
  - 1.13.a MAC learning et aging
  - 1.13.b Frame switching
  - 1.13.c Frame flooding
  - 1.13.d MAC address table

2.0 Accès au Réseau - 20%

- 2.1 Configurer et vérifier les VLANs (normal range) couvrant plusieurs switches
  - 2.1.a Access ports (data et voice)
  - 2.1.b Default VLAN
  - 2.1.c Connectivity
- 2.2 Configurer et vérifier la connectivité interswitch
  - 2.2.a Trunk ports
  - 2.2.b 802.1Q
  - 2.2.c Native VLAN
- 2.3 Configurer et vérifier les protocoles de découverte Layer 2 (Cisco Discovery Protocol et LLDP)
- 2.4 Configurer et vérifier (Layer 2/Layer 3) EtherChannel (LACP)
- 2.5 Décrire la nécessité et les operations de base de Rapid PVST+ Spanning Tree Protocol
  - 2.5.a Root port, root bridge (primary/secondary), et les autres noms de port
  - 2.5.b Port states (forwarding/blocking)
  - 2.5.c Avantages PortFast
- 2.6 Comparer les architectures Cisco Wireless Architectures et les modes des APs
- 2.7 Décrire les connexions physiques d'infrastructure des composants WLAN (AP,WLC, access/trunk ports, et LAG)
- 2.8 Décrire les connexions des accès de gestion des APs et du WLC (Telnet, SSH, HTTP,HTTPS, console, et TACACS+/RADIUS)
- 2.9 Configurer les composants d'un accès au LAN sans-fil pour la connectivité d'un client en utilisant un GUI seulement pour la création du WLAN, les paramètres de sécurité, les profiles QoS et des paramètres WLAN avancés

3.0 Connectivité IP - 25%

- 3.1 Interpréter les composants d'une table de routage
  - 3.1.a Routing protocol code
  - 3.1.b Prefix
  - 3.1.c Network mask
  - 3.1.d Next hop
  - 3.1.e Administrative distance
  - 3.1.f Metric
  - 3.1.g Gateway of last resort
- 3.2 Déterminer comment un routeur prend une décision de transfert par défaut
  - 3.2.a Longest match
  - 3.2.b Administrative distance
  - 3.2.c Routing protocol metric
- 3.3 Configurer et vérifier le routage statique IPv4 et IPv6
  - 3.3.a Default route
  - 3.3.b Network route

  - 3.3.c Host route
  - 3.3.d Floating static

- 3.4 Configurer et vérifier single area OSPFv2
  - 3.4.a Neighbor adjacencies
  - 3.4.b Point-to-point
  - 3.4.c Broadcast (DR/BDR selection)
  - 3.4.d Router ID

- 3.5 Décrire le but des protocoles de redondance du premier saut (first hop redundancy protocol)

4.0 Services IP - 10%

- 4.1 Configurer et vérifier inside source NAT (static et pools)
- 4.2 Configurer et vérifier NTP dans le mode client et le mode server
- 4.3 Expliquer le rôle de DHCP et de DNS au sein du réseau
- 4.4 Expliquer la fonction de SNMP dans les opérations réseau
- 4.5 Décrire l'utilisation des fonctionnalités de syslog features en ce inclus les facilities et niveaux
- 4.6 Configurer et vérifier DHCP client et relay
- 4.7 Expliquer le forwarding per-hop behavior (PHB) pour QoS comme classification, marking, queuing, congestion, policing, shaping
- 4.8 Configurer les périphériques pour un accès distant avec SSH
- 4.9 Décrire les capacités la fonction de TFTP/FTP dans un réseau

5.0 Sécurité de base - 15%

- 5.1 Définir les concepts clé de la sécurité (menaces, vulnerabilités, exploits, et les techniques d'atténuation)
- 5.2 Décrire les éléments des programmes de sécurité (sensibilisation des utilisateurs, formation, le contrôle d'accès physique)
- 5.3 Configurer l'accès aux périphériques avec des mots de passe
- 5.4 Décrire les éléments des politiques de sécurité comme la gestion, la complexité, et les alternatives aux mots de passe (authentications multifacteur, par certificats, et biométriques)
- 5.5 Décrire les VPNs remote access et site-to-site
- 5.6 Configurer et vérifier les access control lists
- 5.7 Configurer les fonctionnalités de sécurité Layer 2 (DHCP snooping, dynamic ARP inspection, et port security)
- 5.8 Distinguer les concepts authentication, authorization, et accounting
- 5.9 Décrire les protocoles de sécurité sans-fil (WPA, WPA2, et WPA3)
- 5.10 Configurer un WLAN en utilisant WPA2 PSK avec un GUI

6.0 Automation et Programmabilité - 10%

- 6.1 Expliquer comment l'automation impacte la gestion du réseau
- 6.2 Comparer les réseaux traditionnels avec le réseau basé contrôleur (controller-based)
- 6.3 Décrire les architectures basées contrôleur (controller-based) et software defined (overlay, underlay, et fabric)
  - 6.3.a Séparation du control plane et du data plane
  - 6.3.b APIs North-bound et south-bound
- 6.4 Comparer la gestion traditionnelle les périphériques campus avec une gestion des périphériques avec Cisco DNA Center
- 6.5 Décrire les caractéristiques des APIs de type REST (CRUD, verbes HTTP, et encodage des données)
- 6.6 Reconnaître les capacités des mécanismes de gestion des configuration comme Puppet, Chef, et Ansible
- 6.7 Interpréter des données encodées en JSON

Introduction

Ce premier volume du guide de préparation à la certification Cisco CCNA 200-301 est une première étape dans votre projet de formation. Il couvre les objectifs de la certification qui demeurent indispensables à la suite. Très théoriques, ces objectifs trouvent de nombreux cas d'application dans des exercices de lab.

L'objectif opérationnel de ce document est d'identifier les composants des topologies du réseau et de maîtriser l'adressage IPv4 et l'adressage IPv6, aussi bien en termes de calculs de masques et de sous-réseau. On aura également un aperçu des commandes et des procédures de diagnostic de la connectivité TCP/IP. L'ouvrage s'intéresse au célèbre IOS Cisco et au simulateur d'infrastructure GNS3.

Ce volume peut occuper une activité intellectuelle de 16 à 35 heures, voir plus.

Dans une première partie, on tentera d'acquérir les fondamentaux des technologies des réseaux tels que les modèles TCP/IP et OSI, les composants et les concepts d'architecture des réseaux d'accès LAN/WAN, dans le *Data Center* et dans le nuage (*cloud*) et, enfin, les rudiments pour manipuler les identifiants codés en décimal, en binaire et en hexadécimal.

Dans une seconde partie, on aborde la manière de se connecter aux périphériques Cisco comme des commutateurs (*switches*) ou des routeurs (*routers*) et à comprendre l'environnement en ligne de commande Cisco IOS. Cette partie n'est pas directement vérifiée dans l'examen, mais elle est indispensable pour entrer dans les opérations de configuration et de diagnostic dans les environnements réels ou simulés.

La troisième partie s'intéresse à la couche Internet en général, aux adresses IPv4 et aux masques de sous-réseau, au NAT, aux protocoles ICMP, ARP, UDP et TCP. A titre de diagnostic, on proposera plusieurs commandes de prise d'information et de l'observation de trafic TCP/IP.

La dernière partie de ce volume "fondamental" serait incomplet sans parler d'IPv6. IPv6 est un sujet fortement vérifié dans les certifications Cisco CCNA. Cette partie s'intéresse à la reconnaissance et à la validation des adresses IPv6, à leur configuration sur les interfaces, à leur vérification et à leur diagnostic. Enfin, on trouvera un propos sur la manière de concevoir des plans d'adressage IPv6.

Première partie Fondamentaux des réseaux

Les données que nos ordinateurs transmettent à travers les réseaux sont transportées sous la forme de signal binaire grâce à des protocoles de communications qui enveloppent et développent les informations originales en différentes couches. Des **protocoles LAN/WAN**, des **protocoles de la pile TCP/IP** et leurs **modèles de communication** rendent ces échanges possibles d'un point d'extrémité du globe à un autre de manière efficiente, sécurisée et peu coûteuse.

Certains **périphériques** tels que des commutateurs (*switches*) ou des routeurs (*routers*), des pare-feu (*firewalls*) ou encore des contrôleurs de réseaux locaux sans fil (*Wireless LAN controllers*) ainsi que les liaisons qui les interconnectent sont des composants matériels constitutifs des infrastructures de communications. Ces éléments construisent nos réseaux locaux domestiques et d'entreprise, de surveillance, de gestion, de paiement, nos centres de données, nos services à la clientèle, etc. et participent au déploiement de l'Internet. On représente les périphériques et leurs interconnexions par des **topologies** en forme de diagrammes. Les infrastructures de communication sont élaborées sur base d'**architectures** visant la robustesse, la sûreté et la haute disponibilité des données à travers le réseau grâce à des **modèles de conception**.

Les données sont transmises physiquement sous forme d'ondes électromagnétiques, sur des supports en cuivre (câble à paires torsadées, coaxial) ; sous forme d'ondes lumineuses, sur des supports comme l'air sur de courtes distances (ondes infra-rouges ou ultra-violettes) ou la fibre optique (laser/LED) ; sous forme d'ondes radio, à travers les airs sur de longues distances. Alors que nous avons l'habitude de parler en langues naturelles et à représenter les valeurs en base décimale, les ondes émises par les ordinateurs représentent des "bits de données" **codés en binaire ou en hexadécimal**.

Les services Internet fonctionnant avec la pile TCP/IP sont accessibles grâce à des technologies d'accès au réseau local (de type LAN) ou de type distant (pour des accès Internet, des inter-connexions de sites distants d'entreprise ou de centres de données ou encore avec des facilités VPN).

1. Protocoles et modèles de communication

Les protocoles du réseau peuvent être modélisés et catégorisés selon divers critères. On trouvera dans ce premier chapitre les principes fondamentaux sur les modèles de communication et leurs protocoles : définition, catégorisation, rôles, mise en couches, encapsulation et désencapsulation. On évoquera aussi les modèles OSI et TCP/IP, les technologies LAN, WAN et dérivés sans fil ainsi que les modèles de conception.

1. Définition d'un protocole de communication

Un protocole de communication est un ensemble de règles qui rendent les communications possibles, car les intervenants sont censés les respecter.

Les protocoles définissent une sorte de langage commun que les intervenants utilisent pour se trouver, se connecter l'un à l'autre et y transporter des informations.

Les protocoles peuvent définir toute une série de paramètres utiles à une communication :

- des paramètres physiques comme des modulations, des types de supports physiques, des connecteurs …
- le comportement d'un certain type de matériel,
- des commandes,
- des machines à état,
- des types de messages,
- des en-têtes qui comportent des informations utiles au transport.

2. Standardisation, régulation et interopérabilité

2.1. Organismes de standardisation

Les protocoles sont discutés et élaborés par des **organismes de standardisation**.

Les **protocoles TCP/IP** sont formalisés par l'Internet Engineering Task Force (IETF) dans des documents publics qui prennent le nom de RFC ("Requests For Comments"). On désigne ces documents par des numéros de références. Tous les RFCs ne sont pas nécessairement des standards. Leur statut au sein du processus de standardisation peut être : *Informational*, *Experimental*, *Best Current Practice*, *Standards Track* ou *Historic*.[1] L'IETF dépend de l'ISOC.

Les **protocoles LAN / WAN / PAN**[2] sont par contre formalisés par d'autres organismes comme l'IEEE (IEEE 802), l'ITU, par l'ANSI,etc.

2.2. Organismes de régulation et consortiums commerciaux

On prendra garde à distinguer ces organismes de standardisation de *consortiums commerciaux* comme la WiFi Alliance ou des *organismes étatiques nationaux et internationaux de régulation* comme le FCC, l'ETSI, l'IBPT, …

1. Pour un peu plus de détails sur les RFCs : fr.wikipedia.org et en.wikipedia.org.
2. Ces acronymes définissent des catégories de technologies physiques selon leur étendue : *Local* Area Network (LAN), *Wide* Area Network (WAN), *Personal* Area Network. Voyez plus bas.

Organismes de régulation, standardisation et compatibilité

Les organismes de régulation donnent les conditions d'usage des ondes sur l'espace public. Ce sont des organismes sous l'autorité des États qui s'entendent au niveau de l'Institution Internationale des Communications (ITU).

Les consortiums commerciaux tels que la "Wi-Fi Alliance" assurent que des matériels de fournisseurs respectant un standard comme IEEE 802.11 soient compatibles entre eux.

3. Nomenclature des protocoles

On peut catégoriser les protocoles sur base de différents critères comme la signalisation, la maintenance de la connexion, la fiabilité, selon les plans gestion, contrôle, donnée ou encore selon le type de technologie TCP/IP, LAN, WAN.

3.1. Signalisation

On désigne ici par "signalisation" tout message qui comprend des commandes utiles du protocole.

Un protocole à signalisation **In-Band** embarque la signalisation avec les données dans un même canal (HTTP).

Un protocole à signalisation **Out-of-Band** utilise une signalisation dans un protocole distinct (en téléphonie IP les protocoles SIP/SDP/RTP) ou un canal dédié (FTP).

3.2. Maintenance de la connexion

Un protocole **Orienté Connexion** est celui qui établit, maintient et ferme un canal au préalable de l'envoi des données (TCP, FTP).

Un protocole **Non Orienté Connexion** : Ethernet, IP, UDP, TFTP sont non orientés connexion et ne proposent aucun mécanisme de maintenance.

3.3. Fiabilité

Un protocole **Fiable** met en oeuvre des mécanismes de fiabilité tel que la reprise sur erreur, des accusés de réception, du contrôle de flux, etc. (TCP).

Un protocole **Non fiable** : Ethernet, IP, UDP, TFTP sont non fiables et ne proposent aucun mécanisme de fiabilité.

Les caractéristiques fiabilité et maintenance sont souvent associées, mais les deux caractéristiques peuvent être dissociées.

3.4. Plans

Les quatre plans "*Data*", "*Control*", "*Management*", "*Services*" sont des concepts pour identifier le "plan" des opérations sur un routeur (L3) ou un commutateur (L2) ou dans une architecture.

Le plan **Donnée (*Data plane*)** fait référence aux **fonctions et processus de transfert de paquets**. On y trouve des protocoles transportant des données des utilisateurs (HTTPS, FTP, RTP), l'encapsulation de données. La qualité de service (QoS), le filtrage sont aussi sur ce plan.

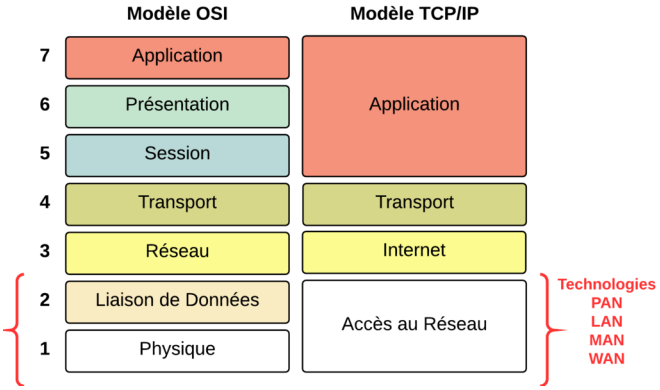
Le plan **Contrôle (*Control plane*)** concerne toutes les **fonctions de création des chemins** comme les protocoles de routage (OSPF, EIGRP, BGP) ou les protocoles LAN IEEE 802.1 (Spanning-Tree, Etherchannel, VLANs), les protocoles de redondance du premier saut FHRP (HSRP, VRRP, GLBP), etc. Ils émanent de l'infrastructure. Les protocoles de gestion d'infrastructure comme la résolution de noms (DNS), d'attributions d'adresses (DHCP, RA, DHCPv6), de voisinage (ARP/ND) peuvent être classés dans cette catégorie.

Le plan **Gestion (*Management plane*)** est le plan des **fonctions de gestion et de surveillance des périphériques**. On y trouve des protocoles d'accès distant (AAA, RADIUS, SSH), de supervision (NTP, SYSLOG, SNMP), de transfert de fichier (FTP, TFTP, SSH/SCP/SFTP). On pensera aussi aux interfaces "API" Rest supportées par HTTP et/ou HTTPS qui permettent de contrôler du matériel et des solutions de type NFV / SDN.

Le plan **Services (*Services plane*)** est un cas spécifique du plan Données (*Data plane*) pour du trafic qui demande une transformation comme par exemple l'encapsulation en tunnels GRE, MPLS VPNs, le chiffrement/déchiffrement TLS/IPsec, le mécanisme QoS, etc.

4. Modèles de communication

Un modèle de communication en couches organise les communications entre les hôtes sous forme d'enveloppement hiérarchique. Chaque couche remplit une fonction spécifique à la communication et dispose de caractéristiques propres. Chaque couche utilise un protocole, soit un ensemble de règles de communication.



Comparaison des modèles TCP/IP et OSI

La couche est enveloppée dans la couche sous-jacente. On parle alors d'encapsulation.

On utilisera principalement le modèle TCP/IP pour expliquer les communications au niveau logique. Le modèle OSI n'a plus d'intérêt que dans sa distinction entre la couche L1 et la couche L2 au niveau de la couche d'accès au réseau.

4.1. Avantages d'un modèle de communication en couches

Un modèle de communication en couches dispose de plusieurs avantages :

- Il permet de mieux comprendre le véritable fonctionnement des communications. Il est **utile à l'apprentissage**.
- Il est **utile au diagnostic** et au dépannage.
- Il permet **de développer ou d'adapter** de nouvelles fonctionnalités sans à revoir l'ensemble du modèle. Les modifications peuvent intervenir uniquement sur le protocole de la couche concernée.
- **Il favorise l'interopérabilité** entre différents matériels, technologies et constructeurs. Il favorise la croissance du marché dans le secteur des infrastructures et de services IT.

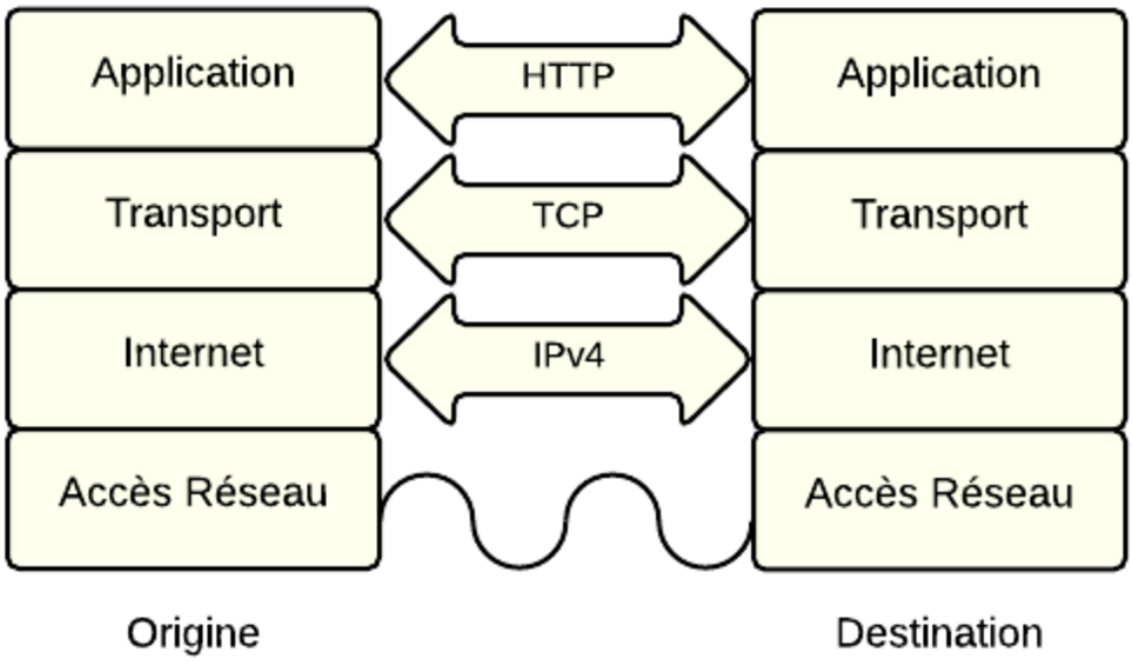
4.2. Modèles de communication utilisés dans ce document

On discutera dans ce document de quelques modèles de communication :

1. Le **modèle TCP/IP** qui implémente les technologies les plus courantes.
2. Le **modèle OSI** qui sert de référence académique et qui trouve des correspondances par rapport aux technologies TCP/IP, LAN et WAN.
3. Les **technologies LAN (Ethernet**, **Wi-Fi)** et **les technologies WAN (PPP**, **PPPoE**, **GRE**, **VPN)** qui disposent de leur propre modélisation au niveau des couches dites "basses", soit proches du signal physique dans les couches Physique (L1) et Liaison de données (L2).

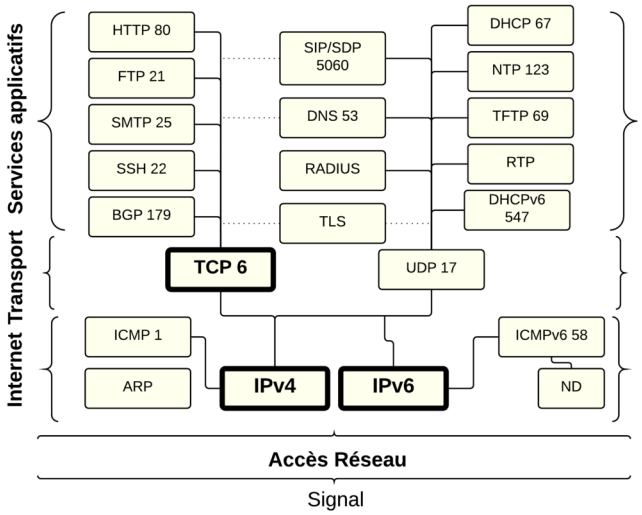
4.3 Protocoles TCP/IP

Les ***protocoles TCP/IP*** relèvent de la "logique", du *logiciel*, où d'une part, **l'Internet Protocol (IP)** identifie les noeuds de communication à travers l'interréseau et les meilleurs chemins, et où d'autre part, **TCP ou UDP** assurent la fonction de transport de bout en bout alors qu'un **protocole de couche application** rend un service de communication.



TCP/IP, communication d'égal à égal

C'est la technologie "Internet" qui utilise la pile des protocoles TCP/IP qui permet que des services comme Facebook, Google ou encore Amazon puissent fonctionner. C'est grâce à TCP/IP que nous pouvons tous les jours aller sur Internet.



Couches Internet, Transport et Application du modèle TCP/IP

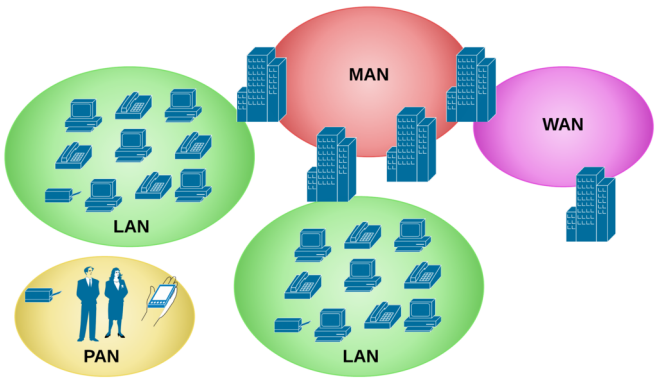
IP pour Internet Protocol, dans sa version 4 ou sa version 6, est celui qui permet d'identifier l'interface de communication de n'importe quels ordinateurs dans le monde et d'acheminer des paquets de données d'une extrémité du globle à une autre. TCP (Transmission Control Protocol) est celui qui permet de maintenir un canal fiable entre deux points IP. Son équivalent sans fiabilité et sans connexion est UDP (User Datagram Protocol). TCP et UDP transportent des protocoles applicatifs comme HTTPS ou DNS. Ces protocoles applicatifs sont utilisés par nos logiciels pour transporter des pages Web, des images, du son, bref n'importe quel type de données.

4.4. Protocoles LAN et WAN

Les ***technologies et protocoles LAN/WAN*** relèvent du *matériel/physique*. Elles assurent **le transport et la livraison physique** des données sur les liaisons locales avec les technologies :

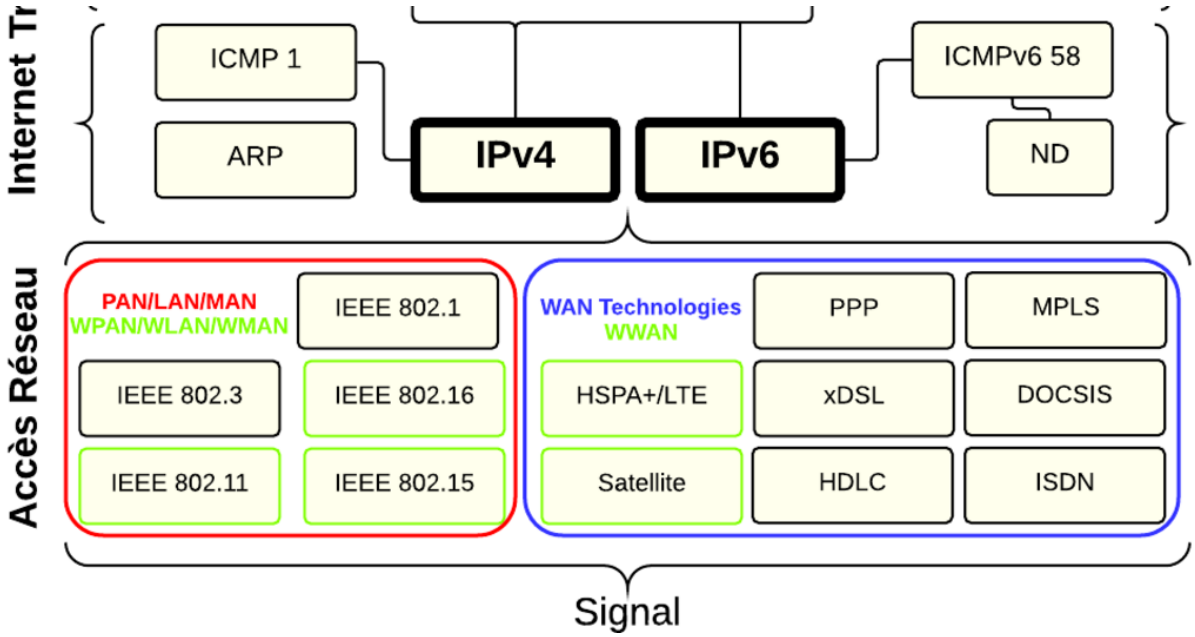
- **LAN** : Technologies au sein des réseaux locaux (confinés localement, rapides et permanents) : Ethernet, Wi-Fi, Bluetooth, WiMax, etc.
- **WAN** : Technologies qui interconnectent les routeurs, points intermédiaires de connectivité, plus lentes et couvrant de longues distances : xDSL/PPPoE, Metro-Ethernet, DOCSIS, LTE, 3G/4G/5G, Satelite, HDLC, Frame-Relay, ATM, … mais aussi les connexions VPN.

Ces technologies disposent de leur qualification “Wireless” avec WPAN, WLAN, WWAN.



Technologies LAN, WAN, PAN, WLAN, WPAN, WWAN

Les technologies LAN, WAN, PAN, WLAN, WPAN, WWAN sont dites des **technologies d’accès**, car elles permettent d’accéder aux réseaux qui autorisent des connexions de bout en bout d’une extrémité à l’autre du globe, *a priori* en TCP/IP.



Couches physiques et Liaison de données

Si cette distinction fondamentale LAN/WAN tient essentiellement à la portée des technologies ou à leur usage, ce sont aussi d’autres critères comme l’origine de leur standardisation qui les opposent dans les rôles ou leurs objectifs.

5. Modèles de conception

Cisco Systems a contribué à la popularité des modèles de conception des réseaux. Ces modèles sont des guides de déploiement des infrastructures du réseau qui permettent aux organisations de rencontrer des objectifs de

performance et de disponibilité. On parle aussi d'architectures ou de topologie ou encore de *design* dans ce cadre. Les modèles de conception représentent la mise en oeuvre opérationnelle des protocoles du réseau dans l'infrastructure physique afin de contrôler au mieux le trafic et atteindre le niveau de service attendu par l'entreprise.

5.1. Modèles de conception traditionnels

On avait jusqu'en plus ou moins 2016 des modèles de déploiement respectant des architectures traditionnelles avec un modèle de conception hiérarchique et modulaire à trois couches : Access, Distribution et Core. Chaque couche assurant des rôles spécifiques sur l'objectif, les protocoles autorisés, les limites de la couche 2 et la couche 3, la sécurité, etc. Le chapitre ultérieur intitulé "Principes de conception LAN" évoque le sujet plus amplement.

Bien souvent, ces infrastructures sont difficiles à gérer et à faire évoluer. Elles demandent des interventions manuelles répétitives. Une vue unifiée de la surveillance et de la sécurité sont alors un véritable enjeu dans la gestion quotidienne de l'infrastructure ainsi que les reprises sur erreurs et la gestion des incidents.

Les architectures qui existent depuis longtemps deviennent difficiles à faire évoluer en demandant beaucoup d'interventions manuelles. Il n'est pas étonnant que l'environnement aie un impact sur les mentalités des professionnels en charge des infrastructures réseau.

Ces modèles sont toutefois toujours d'application dans les réseaux d'entreprise, ne fut-ce qu'en surcouche (*overlay*) d'une infrastructure physique sous-jacente – qui pourrait être conçue d'une autre manière.

5.2. Intent-Based Networks

"**Intent-Based Networks" (IBN)** est une nouvelle perspective de la gestion des réseaux dont l'acronyme est typiquement sorti des équipes marketing de chez Cisco. Les objectifs "Business" de l'organisation devraient être traduits en "policies" du réseau par les professionnels de l'informatique de telle sorte que le réseau puisse atteindre ces objectifs **de manière automatisée** et **à grande échelle**, à titre d'"intention".

Il s'agirait en fait de se rapprocher de plus en plus d'architectures offrant du "**Network as a Service" (NaaS)**. IBN demande une autre approche de la gestion de l'infrastructure avec d'autres interfaces que la ligne de commande (CLI) telle que la gestion à travers d'**APIs HTTP REST** avec des langages de programmation comme Python et des retours présentés en format **JSON**. Ces technologies sont déjà disponibles grâce à des déploiements de type **SDN ("Software Defined networks")** qui utilisent des **contrôleurs** pour centraliser la gestion de l'infrastructure.

Dans les offres des technologies WAN, on trouvera de plus en plus du "**Software Defined WAN" (SD-WAN)** voyant la connectivité WAN comme un service à la demande, prêt à la production et à l'évolutivité, comme par exemple commander à la demande des liaisons WAN entre deux villes d'un pays de manière "élastique". Son équivalent dans le LAN/WLAN (réseau local filaire et sans-fil) SD Access (SDA) apparaît dans les offres des fabricants. Avec SDN, le plan de contrôle et le plan data sont clairement distingués de telle sorte que les pratiques de gestion s'en trouvent modifiées.

Cette nouvelle vision du réseau a déjà eu pour conséquence de changer les infrastructures réseau du centre de données avec les concepts de fabrique (Fabric), de **topologie "Spine/Leaf"** (à deux niveaux) ou encore avec l'implémentation de protocoles comme VxLAN et l'intégration des réseaux SAN (de stockage, *Storage Area Network*, qui se distingue du LAN).

Aussi, avec IBN, on trouvera une multitude de propositions de déploiement du plan "contrôle" : dans le nuage, en local, embarqué sur les périphériques, etc. Les accès au réseau sans-fil devraient mieux s'intégrer aux infrastructures locales filaires, le "contrôle" pouvant disposer d'une vue abstraite des accès avec des politiques de sécurité unifiées.

Enfin, une nouvelle pratique fait son apparition avec celle de "**Network Assurance**" dans laquelle on retrouve des exigences de surveillance en temps réel avec des protocoles traditionnels, du *reporting* et des réponses automatiques. Concrètement, cela signifie que de nouvelles compétences en **programmation**, en **automation** et en gestion d'**infrastructures virtuelles** (locales ou dans le nuage) devront s'ajouter aux compétences des équipes en charge des réseaux, en plus de la connaissance des **nouvelles architectures** qu'ils devront gérer (ils n'en seront pas nécessairement les concepteurs initiaux).

6. Éléments clés à retenir

Les éléments clés à retenir concernant les protocoles et modèles réseau sont les suivants :

1. le rôle d'un protocole de communication réseau
2. les critères de distinction des protocoles (signalisation, connexion, fiabilité, plans)
3. la distinction entre les plans "donnée", "contrôle" et "gestion"
4. la distinction entre technologie d'accès et technologie Internet
5. la distinction entre technologies d'accès LAN et WAN
6. le concept de modèle en couche et d'encapsulation
7. le rôle des modèles de communication comme TCP/IP ou OSI
8. les modèles de conception de réseau
9. les concepts d'"Intent-Based Networks" (IBN) et de "Software Defined networks" (SDN)
10. le concept de topologie "Spine/Leaf"

En conclusion, un modèle de communication est une référence à maîtriser si l'on désire comprendre les technologies des réseaux.

Deuxième partie Cisco IOS CLI

Cette partie évoque le système d'exploitation Cisco IOS, la solution Open Source de simulation d'infrastructures informatiques GNS3. On se demandera malgré tout comment accéder à l'IOS avec une console physique, comment reprendre la main sur les routeurs et les commutateurs Cisco avec un "password recovery", avec une initiation à la méthode de configuration en ligne de commande IOS CLI.

2. Cisco IOS Internetwork Operating System

1. Introduction

Cisco IOS (Internetwork Operating System) est une famille de logiciels utilisée sur la plupart des routeurs et commutateurs Cisco Sytems. IOS dispose d'un ensemble de fonctions de routage (*routing*), de commutation (*switching*), d'interconnexion de réseaux (*internetworking*) et de télécommunications dans un système d'exploitation multitâche.

La plupart des fonctionnalités IOS ont été portées sur d'autres noyaux comme QNX (IOS-XR) et Linux (IOS-XE).

Tous les produits Cisco ne fonctionnent pas nécessairement sous Cisco IOS, comme les plateformes de sécurité ASA (dérivé Linux) ou les routeurs "carrier" qui fonctionnent sous Cisco IOS-XR.

2. Versions

La dénomination des versions Cisco IOS utilise des nombres et certaines lettres, en général sous la forme `a.b(c.d)e` où :

- `a` est le numéro de version **majeur**
- `b` est le numéro de version **mineur**
- `c` est le numéro de révision (release)
- `d` est le numéro de l'intérim (omit des révisions générales)
- `e` (aucune, une ou deux lettres) est l'identifiant du train comme aucun (Mainline), T (Technology), E (Enterprise), S (Service provider), XA est un train de fonctionnalités spécifiques, etc.

Rebuilds – Un rebuild est souvent une version corrective compilée d'un problème ou d'une vulnérabilité pour une version IOS donnée. Par exemple, 12.1(8)E14 est un Rebuild, le 14 signifiants le 14ème rebuild de 12.1(8)E.

Interim releases – Basé sur une production hebdomadaire.

Maintenance releases – Révision rigoureusement testées.

3. Trains

Un train est un véhicule fournissant un logiciel Cisco auprès d'un ensemble de plateformes et de fonctionnalités.

3.1. Jusqu'en version 12.4

Avant l'IOS release 15, les révisions étaient séparées en différents "trains", chacun contenant un ensemble de fonctionnalités. Les "trains" étant liés aux différents marchés et clients que Cisco voulait toucher.

- **The mainline train**, Version stable.
- **The T – Technology train**, Version en développement, prochaine version stable.
- The S – Service Provider train
- The E – Enterprise train
- The B – broadband train
- The X* (XA, XB, etc.)

3.2. Depuis 15.0

À partir de la version IOS 15, il n'y a plus qu'un seul train : le Train M/T.

4. Packaging / feature sets

La plupart des produits qui fonctionnent en Cisco IOS ont une ou plusieurs "feature sets" ou "packages", 8 pour les routeurs Cisco et 5 pour les switches Cisco.

Par exemple, pour un switch Catalyst les IOS sont disponibles en versions :

- "standard" : Routage IP de base
- "enhanced" : Full routage IPv4
- "advanced IP services" : Full routage IPv6

On peut trouver une fonctionnalité grâce au "Cisco Feature Set Browser" (Cisco Feature Navigator).

Avec les routeurs ISR 1900, 2900 and 3900, Cisco a révisé son modèle de licence. Les routeurs viennent avec une licence de base et celle-ci est étendue avec une fonctionnalité déjà native au logiciel par activation.

- **Data** : BFD, IP SLAs, IPX, L2TPv3, Mobile IP, MPLS, SCTP.
- **Security** : VPN, Firewall, IP SLAs, NAC.
- **Unified Comms** : CallManager Express, Gatekeeper, H.323, IP SLAs, MGCP, SIP, VoIP, CUBE(SBC).

On trouvera plus d'information sur les versions Cisco IOS dans l'article publié chez Cisco Press "An Overview of Cisco IOS Versions and Naming".

5. Cisco IOS

Le système d'exploitation Cisco IOS a été développé depuis les années 1980 pour des routeurs disposant de faibles ressources en RAM (256 Kb) et en CPU. La modularité dans l'architecture Cisco IOS a permis sa croissance sur du matériel toujours mieux adapté en fonctionnalités nouvelles.

Dans toutes les versions de Cisco IOS, le routage de paquets (*packet routing*) et la commutation de paquets (*packet switching*) sont des fonctions distinctes.

Le routage et les autres protocoles fonctionnent en tant que processus IOS et contribuent à la table "Routing Information Base (RIB)". Celle-ci subit un traitement pour produire la table finale "IP forwarding table (FIB, Forwarding Information Base)". La FIB est utilisée par la fonction de transfert (*forwarding*) du routeur.

Cisco IOS est construit selon une architecture monolithique. Il fonctionne comme une seule image et tous les processus partagent le même espace mémoire. Il n'y aucun mécanisme de protection entre les processus. En d'autres termes, un bug dans l'IOS peut potentiellement corrompre des données utilisées par un autre processus. Le noyau de l'IOS n'est pas préemptif.

Type	noyau	Mémoire
IOS	Monolithique, non-préemptif	mémoire partagée sans protection entre processus, pas de "swapping" ou "paging", plus de performance moins de sécurité

Plateformes fonctionnant en Cisco IOS monolithique.

Gamme de plateformes	Type de plateformes
Routeurs ISR G1 et ISR G2	Cisco 800, 1800, 1900, 2800, 3200, 3800, 2900, 3900, 3600 et 3700.
Commutateurs Cisco Catalyst	2970, 3560 3750, 4500, 4900 et 6500.
Routeur virtuel générique de lab	IOSv

6. Cisco IOS-XR

Pour les produits Cisco nécessitant de la haute disponibilité comme les Cisco CRS, les limites d'un IOS monolithique ne sont plus acceptables d'autant plus qu'un système d'exploitation d'un compétiteur comme JUNOS de Juniper de 10 à 20 ans son cadet ne connait pas ces limites grâce à sa base UNIX.

Une réponse de Cisco a été de concevoir une nouvelle version de Cisco IOS appelée Cisco IOS-XR (2006) offrant plus de modularité et une protection entre les processus, des "lightweight threads", de l'ordonnancement préemptif et la capacité de redémarrer indépendamment des processus qui ont échoué. IOS-XR utilise un micro-noyau tiers en temps réel ("a 3rd party real-time operating system microkernel") appelé QNX. Un bonne partie du code source de l'IOS a été réécrit pour profiter du nouveau noyau. L'avantage d'un micro-noyau est qu'il élimine tout processus qui n'est absolument pas nécessaire d'une part, et d'autre part qu'il les exécute ces processus comme des processus d'application.

Grâce à cette méthode, IOS-XR est capable d'atteindre le niveau de haute disponibilité que doivent atteindre les nouvelles plateformes. Même si les systèmes sont de conception franchement différente, ils sont très proches quant à leur usage.

Type	noyau	Mémoire
IOS-XR	third-party real-time operating system (RTOS) microkernel, QNX, multitâches préemptif, protection entre les processus, des "lightweight threads", de l'ordonnancement préemptif et la capacité de redémarrer indépendamment des processus qui ont échoué	mémoire dédiée et protégée.

Plateformes IOS-XR :

- Cisco CRS-1 Carrier Routing System (CRS),
- CRS-3 Carrier Routing System,
- ASR9000 Series routers,
- Cisco XR 12000 Series routers pour service provider core networks,
- IOS-XRv

Cisco CRS 16-Slot Back-to-Back (2+0) System

Source de l'image : Cisco CRS 16-Slot Back-to-Back (2+0) System

7. Cisco IOS-XE

L'IOS-XE utilise des composants d'architecture qui l'améliore et le différencie par rapport à un noyau IOS traditionnel. Toutefois, la ligne de commande Cisco IOS CLI (Command Line Interface) et les procédures de configuration sont très proches de telle sorte que les opérateurs puissent passer de l'un à l'autre facilement. Il fonctionne sur des machines physiques dédiées ou virtuelles avec des processeurs Intel 64 bits.

IOS-XE ajoute la stabilité grâce à l'abstraction de la plateforme supportée par un **noyau Linux**. Le noyau Linux et ses pilotes sont les seuls composants de l'architecture IOS-XE qui disposent d'un accès direct au matériel en fournissant une stabilité supplémentaire.

Le noyau Linux permet d'exécuter des processus sur de multiples processeurs. Les librairies logicielles permettent à des applications de fonctionner sur le même matériel. L'exécution de Wireshark sur un Superviseur Catalyst 4500 est un exemple.

Tous les protocoles de routage sont des démons appelés *IOSd* qui fonctionnent comme des processus distincts.

IOS-XE supporte des architectures Intel 64 bits permettant une exploitation de la mémoire vive au-delà de 4 Go (limite associée aux architectures 32 bits). Le noyau attribue de la mémoire vive aux processus IOSd. Les IOSd attribuent alors une taille de mémoire configurable et les utilisent pour diverses fonctions de l'IOS.

Plateformes IOS-XE

- ASR1000
- CSR1000v
- Cisco ASR 900 Series
- Catalyst 4000 Series Supervisor 7

Gamme Cisco ASR1000

Source de l'image : Gamme Cisco ASR1000

Cisco Systems et le programme de la certification CCNA nous invitent à nous intéresser à la programmation des infrastructures réseau à partir de Cisco IOS-XE comme par exemple sur https ://developer.cisco.com/site/ios-xe/.

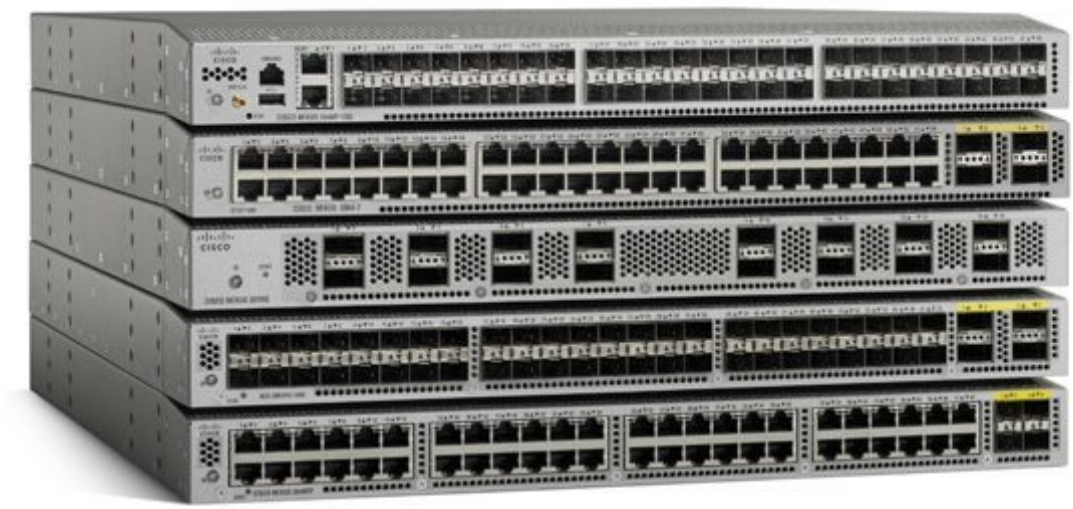
8. Cisco NX-OS

Cisco a fabriqué un système d'exploitation de prochaine génération pour le *data center* pour un maximum d'évolutivité et de disponibilité des applications. NX-OS est une évolution du système d'exploitation industriel Cisco Storage Area Network Operating System (SAN-OS) Software et fonctionne avec une base Wind River Linux[1].

Plateformes IOS NX :

- Cisco Nexus 3000,
- Cisco Nexus 5000,
- Cisco Nexus 7000,
- Cisco Nexus 9000,
- Cisco 9k series routers,
- NX-OSv

1. https ://en.wikipedia.org/wiki/Cisco_NX-OS



Cisco Nexus 3000

Source de l'image : Cisco Nexus 3000

9. Cisco ASA OS

La gamme "Adaptive Security Appliance" (ASA) est celle des pare-feu chez Cisco. Cisco ASA Software est le système d'exploitation développé sur ces plateformes. Il fonctionnait sous d'anciennes plateformes comme Cisco PIX, Cisco VPN 3000, Cisco IPS 4200. L'interface Cisco AS-OS est très proche de celle des plateformes IOS.

- http ://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html
- http ://www.cisco.com/c/en/us/products/security/virtual-adaptive-security-appliance-firewall/index.html
- https ://docs.gns3.com/appliances/cisco-asav.html

Gamme Cisco ASA

Source de l'image : Gamme Cisco ASA

10. Cisco IOx

L'environnement applicatif Cisco® IOx combine l'exécution d'applications IoT dans le brouillard, une connectivité sécurisée avec le logiciel Cisco IOS® et des services puissants pour une intégration rapide et fiable avec les capteurs de l'Internet des objets (IoT) et le nuage. En apportant la capacité d'exécution d'applications à la source des données IoT, les clients surmontent les difficultés liées aux volumes élevés de données et à la nécessité d'une réactivité du système automatisée en temps quasi réel. Cisco IOx offre une gestion et un hébergement cohérents pour tous les produits d'infrastructure réseau, y compris les routeurs, les commutateurs et les modules de calcul Cisco. Cisco IOx permet aux développeurs d'applications de travailler dans l'environnement familier des applications Linux avec leur choix de langages et de modèles de programmation avec des outils de développement open-source familiers.[2]

Cisco IOx peut être activé sur les plateformes suivantes :

- Cisco 800 Series Industrial Integrated Services Routers
- Cisco Industrial Ethernet 4000 family of switches
- Compute Module for Cisco 1000 Series Connected Grid Routers
- Cisco IR510 WPAN Industrial Router

En termes d'architecture matérielle, à titre d'exemples, les routeurs matériels IR829 et IR809 utilisent le même processeur Intel Rangeley double coeur, avec 2 Go de mémoire DDR3, 8 Mo de mémoire SPI Bootflash et 8 Go (4 Go utilisables) de mémoire flash eMMC.[3]

2. Cisco IOx Data Sheet.
3. Documentation>IOx>IR8xx Platforms

L'hyperviseur, fourni par LynxWorks, fonctionne sur le matériel baremetal sur lequel l'IOS et un OS invité (par exemple Linux) fonctionnent comme deux machines virtuelles (VM) séparées.

L'hyperviseur présente le matériel sous-jacent aux machines virtuelles (IOS et OS invité) comme un sous-ensemble du matériel physique réel – ce qui permet la virtualisation imbriquée (*Netsed virtualization*). La configuration de l'hyperviseur permet de déterminer quels périphériques doivent être affectés à quelle VM. Les VM accèdent à une unité centrale virtuelle, à des zones de mémoire préconfigurées, à un stockage sur disque flash prédivisé et à d'autres périphériques matériels. LynxSecure Separation Kernel v. 5.1 a été sélectionné comme hyperviseur.

Chaque périphérique PCI peut être détenu exclusivement par une VM dans l'architecture de l'hyperviseur. Toutefois, l'IOS et le système d'exploitation invité doivent accéder à certains périphériques partagés, par exemple la mémoire flash eMMC. La solution est un serveur de périphériques virtuels (VDS), qui est une VM distincte possédant des périphériques partagés. L'IOS et le système d'exploitation invité accèdent aux dispositifs virtuels émulés dans l'hyperviseur. L'hyperviseur et le VDS coordonnent ensuite l'accès aux dispositifs partagés. Le VDS fournit également des canaux de communication entre les VM, en utilisant des interfaces Ethernet émulées.

L'IOS agit comme une passerelle vers les ressources réseau pour la partition Linux, en utilisant l'adresse IP et une connexion de commutateur virtuel fournie à l'hyperviseur. IOS et Linux fonctionnent chacun comme un système d'exploitation invité de l'hyperviseur.

Le chemin réseau de IOXVM à IOS est disponible via une liaison Ethernet émulée entre eux. Le protocole IPv4 ou IPv6 peut être exécuté sur la liaison Ethernet.

L'IOXVM exécute le CAF et d'autres éléments de l'infrastructure IOx sur le Linux hôte et héberge toutes les applications LXC.

On imagine donc que des machines virtuelles Qemu/KVM ou des containers Docker puissent être intégrés au plus proche des clients dans le matériel réseau.

Vous pouvez commencer avec Cisco IOx à partir de la page "What is IOx ?"

11. Sources du document

- Pearson VUE, An Overview of Cisco IOS Versions and Naming
- Cisco CRS
- https ://developer.cisco.com/site/ios-xe/
- https ://en.wikipedia.org/wiki/Cisco_ASA
- "What is IOx ?"

Troisième partie Protocole IPv4

Tous les ordinateurs qui se connectent à ce qu'on appelle communément l'Internet sont identifiés de manière certaine par une adresse Internet (IP). Cette partie s'intéresse à la couche Internet en général, aux adresses IPv4 et aux masques de sous-réseau, au NAT, aux protocoles ICMP, ARP, UDP et TCP.

A la fin de la partie, à titre de diagnostic, on proposera plusieurs commandes de prise d'information et de l'observation de trafic TCP/IP.

La couche Internet est celle qui permet à deux ordinateurs situés à n'importe quel endroit du monde de communiquer directement entre eux. Les routeurs utilisent l'adressage du protocole IPv4 ou celui du protocole IPv6 pour acheminer les paquets jusqu'à leur destination. La gestion des adresses IP est confiée à des organismes régionaux (les RIRs). Actuellement le protocole le plus utilisé est IPv4. IPv6 et le NAT (la traduction d'adresses) sont des solutions à l'épuisement des adresses IPv4.

Même si la certification Cisco CCNA n'exige pas la connaissance des en-têtes IPv4 ou IPv6 (ni d'aucun autre protocole), il est utile de distinguer les différences entre ces en-têtes et de les comparer d'un protocole à l'autre. Par contre, il est inimaginable de se présenter à un examen Cisco ou à un entretien d'embauche dans le domaine des réseaux sans maîtriser l'adressage IPv4 et ses mécanismes de découpage.

Enfin, IPv4 est aidé par deux protocoles pour la résolution d'adresses et le contrôle : ARP et ICMP au niveau de la couche 3 (L3). Enfin, les protocoles TCP et UDP de la couche Transport des modèles OSI et TCP/IP, vus de manière comparative, font partie des sujets vérifiés dans la certification CCNA.

3. La couche Internet du modèle TCP/IP

La couche Internet est celle qui permet à deux ordinateurs situés à n'importe quel endroit du monde de communiquer directement entre eux. Les routeurs utilisent l'adressage du protocole IPv4 ou celui du protocole IPv6 pour acheminer les paquets jusqu'à leur destination. La gestion des adresses IP est confiée à des organismes régionaux (les RIRs). Actuellement le protocole le plus utilisé est IPv4. IPv6 et le NAT (la traduction d'adresses) sont des solutions à l'épuisement des adresses IPv4.

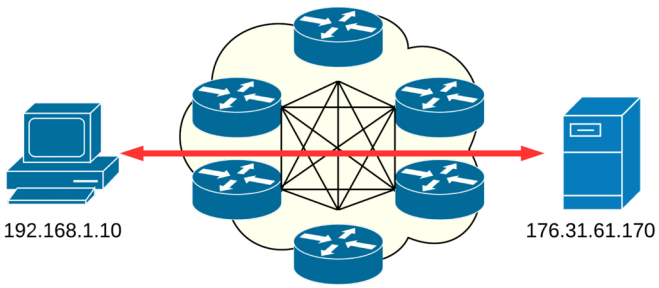
1. Définition de la couche Internet

1. La couche Internet est celle qui s'occupe d'adresser globalement les interfaces : elle remplit une fonction d'**adressage**.

2. Elle détermine les meilleurs chemins à travers les inter-réseaux : elle remplit une fonction de **routage**.

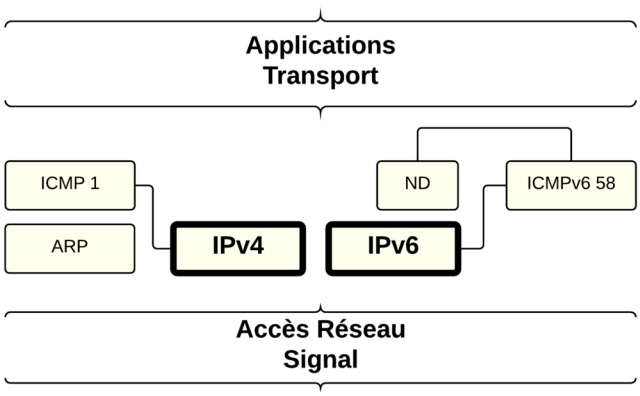
Elle utilise un des protocoles Internet (IPv4 ou IPv6). Ceux-ci ont pour caractéristique communes de fonctionner en mode **non fiable** et en mode **non connecté**.

En bref, la couche Internet est celle qui permet à ces deux ordinateurs de communiquer directement entre eux via un inter-réseau probablement à l'échelle du globe : à travers l'Internet.



La couche Internet est celle qui permet à ces deux ordinateurs de communiquer directement entre eux via un interréseau.

2. Modèle TCP/IP : couche Internet



Modèle TCP/IP : couche Internet

3. Protocoles de couche Internet

IPv4 et IPv6 sont accompagnés d'autres protocoles comme ARP, ICMP et ICMPv6 :

- La couche Internet remplit aussi le rôle de **résolution d'adresses** : **ARP** (RFC826) en IPv4 et **Neighbor Discovery (ND)** (RFC4861) en IPv6.
- IPv4 dispose d'**ICMP** (RFC792) et IPv6 d'**ICMPv6** (RFC443) pour du **diagnostic et des messages d'erreurs**.
- IPv4 et IPv6 sont aidés par des **protocoles de routage** pour maintenir le routage Internet (**BGP**, **OSPF**, **EIGRP**)

  Avec ICMPv6 qui embarque des fonctions de **configuration du réseau**, **d'autoconfiguration des interfaces** et de **maintenance de relations de voisinage**, soit **l'autoconfiguration automatique sans état** (Stateless Address Autoconfiguration)RFC4862), la couche 3 (L3, Internet/Réseau) maîtrise nativement la gestion de cet adressage de 128 bits. Un marché s'ouvre pour exploiter les nouvelles fonctionnalités d'IPv6 en termes de gestion (IPAM, IP Address Management).

4. Protocoles Internet

Quelle que soit leur version, IPv4 ou IPv6, les "*Internet Protocols*" répondent à quelques principes majeurs :

- d'une **communication de bout en bout** : Les adresses d'origine et de destination utilisées pour adresser les machines communicantes sont joignables de bout en bout
- du **meilleur effort** : Les paquets sont acheminés sans garantie quant à leur acheminement, Méthode de qualité de service **(QoS)** par défaut.
- Il est aussi **réputé "non-fiable"** : **Sans mécanisme de fiabilité** (pas de contrôle de flux, pas d'accusés de réception, pas gestion des erreurs, il est néanmoins robuste)
- Il est "**non orienté connexion**" : Un protocole "orienté connexion" est celui qui établit, maintient et termine une communication.
- **Unicité des adresses** : les adresses Unicast sont censées être uniques dans un Interréseau. Les adresses Multicast sont ces adresses uniques qui peuvent être adressées à plusieurs noeuds, même à travers un interréseau (IPv6).

Par ailleurs, les protocoles IP présentent d'autres caractéristiques :

- IP fait le **lien ENTRE** *l'infrastructure qui transporte les données* ET *les services offerts*. Il est donc **central et critique**.
- Le NAT (NAT44, NAT66, NAT444, CG-NAT, NAT64, tous types de NAT) **contrevient au principe d'une communication de bout en bout** empêchant d'exploiter pleinement le potentiel de TCP/IP. Si le NAT est indispensable dans l'exploitation des réseaux IPv4, on envisagera toute solution NAT avec mesure. On privilégiera des solutions et des architectures basées sur du matériel et des protocoles de sécurité et "applicatifs" comme des *proxys*.
- Des fonctionnalités/modèles de **Qualité de Service (QoS)** autres que le "meilleur effort" peuvent être mises en oeuvre.
- Selon le service utilisé, **TCP** prend en charge les fonctionnalités de fiabilité.
- Sur le plan physique, **la couche sous-jacente (Accès Réseau)** peut éventuellement aussi prendre en charge des mécanismes de fiabilité.

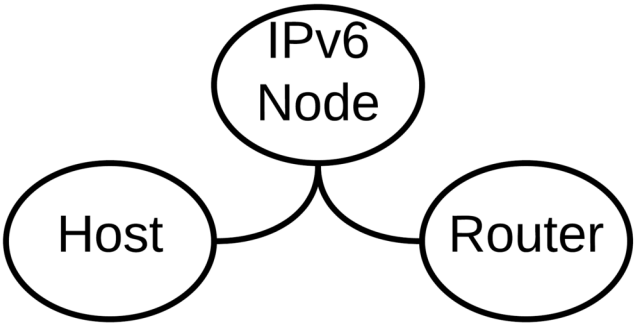
Sur le plan fondamental, un "*Internet Protocol*" est un protocole qui permet :

- D'acheminer des paquets de données d'une extrémité à l'autre de l'interréseau,
- à travers des réseaux distincts (donc différents) interconnectés entre eux.

Les routeurs transfèrent le trafic d'une origine à une destination et prennent leurs décisions sur base des adresses IP contenues dans les paquets.

5. Internet : rôles

Au niveau de la couche 3 (L3), pour les protocoles IP, les hôtes TCP/IP sont reconnus comme des "noeuds" (*nodes*) qui peuvent prendre un des deux rôles : hôte terminal (*end host*) ou routeur (*router*).



IPv6 voit deux rôles : hôte terminal et routeur.

- Les hôtes terminaux qui disposent de une ou plusieurs interfaces attachées à un lien.
- Les routeurs qui disposent de plusieurs interfaces attachées à des liens et qui transfèrent le trafic qui ne leur est pas destiné. Ils prennent leurs décisions sur base de leur table de routage. Le routeur examine les en-têtes IP au niveau du champ d'adresse de destination pour prendre ses décisions de routage. Il filtre (il ne transfère pas) le Broadcast.

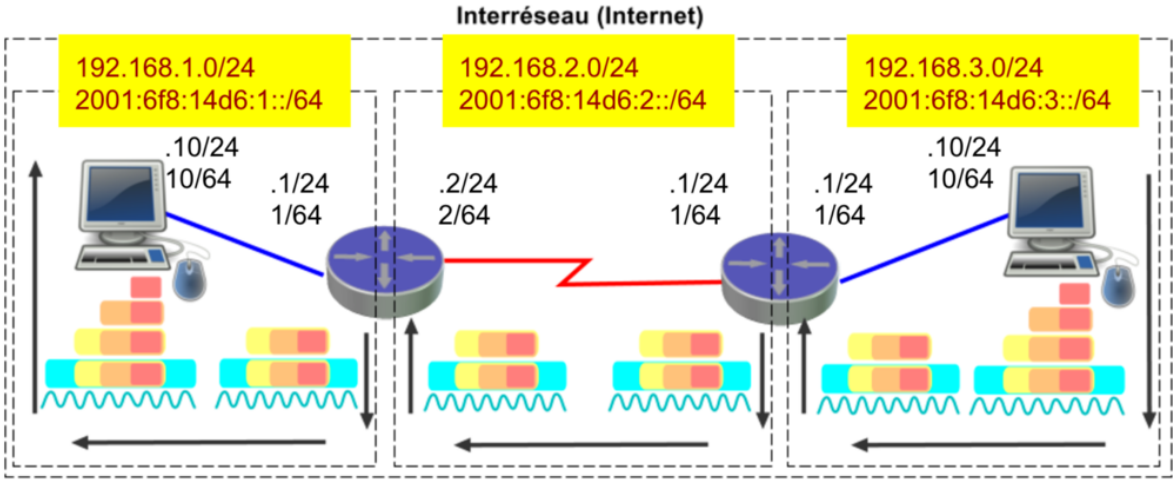
6. Routeur IP

- Seuls les routeurs sont capables de transférer les paquets d'une interface à une autre.
- Un routeur transfère le trafic qui arrive sur l'une de ses interfaces en fonction de l'adresse IP destination trouvée dans le paquet ; précisément il compare cette destination à une entrée de sa table de routage qui dispose de toutes les destinations d'un inter-réseau.
- Un routeur transfère le trafic qui ne lui est pas destiné, par définition.
- Un routeur limite les domaines de Broadcast sur chacune de ses interfaces.
- Un routeur échange avec ses voisins des informations concernant les différentes destinations (des réseaux à joindre) grâce à des protocoles de routage.

  De plus, de manière obligatoire en IPv6, les routeurs configurent le réseau.

7. Routage entre domaines IP

- Deux noeuds IP (hôtes terminaux, interfaces, cartes réseau, PC, smartphone, etc.) doivent appartenir au même réseau, au même domaine IP pour communiquer directement entre eux.
- Quand les noeuds IP sont distants, ils ont besoin de livrer physiquement (L2) leur trafic à une passerelle, soit un routeur.
- D'une extrémité à l'autre de l'inter-réseau, les adresses IP ne sont pas censées être modifiées (sauf NAT) par les routeurs. Par contre, le paquet est désencapsulé /réencapsulé différemment au niveau de la couche Accès (L2) au passage de chaque routeur.



Cheminement d'un paquet d'une extrémité à l'autre d'un inter-réseau.

8. Organisation des adresses IP

IPv4 offre un espace d'adressage de 32 bits, soit un espace de 2 EXP 32 adresses, aujourd'hui épuisé.

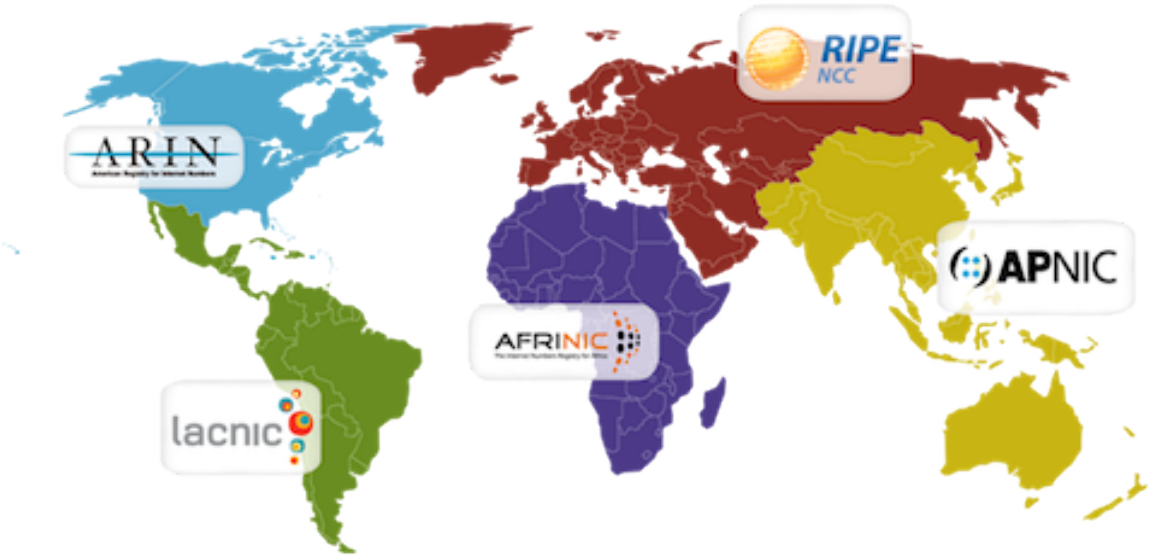
IPv6 offre quant à lui un emplacement de 128 bits pour l'adressage, soit un espace de 2 EXP 128 adresses.

Ce sont des adresses organisées de manière hiérarchique sur base géographique (globe/continent/pays/Fournisseur d'Accès Internet/Client).

Ces attributions d'adresses s'organisent comme suit :

1. La gestion de l'espace d'adresses est confiée par l'IANA aux différents RIRs (*Regional Internet Registries*) comme le RIPE-NCC, l'APNIC, ...
2. Les RIRs confient des blocs à des LIRs (*Local Internet Registries*), des ISP (FAI, Fournisseur d'Accès Internet) ou des grandes entreprises.
3. Les ISP (FAI) offrent des services de connectivité à leurs clients finaux (EU, *End Users*).

NB : Toute demande d'adresse IP doit être justifiée par un projet et une continuité.



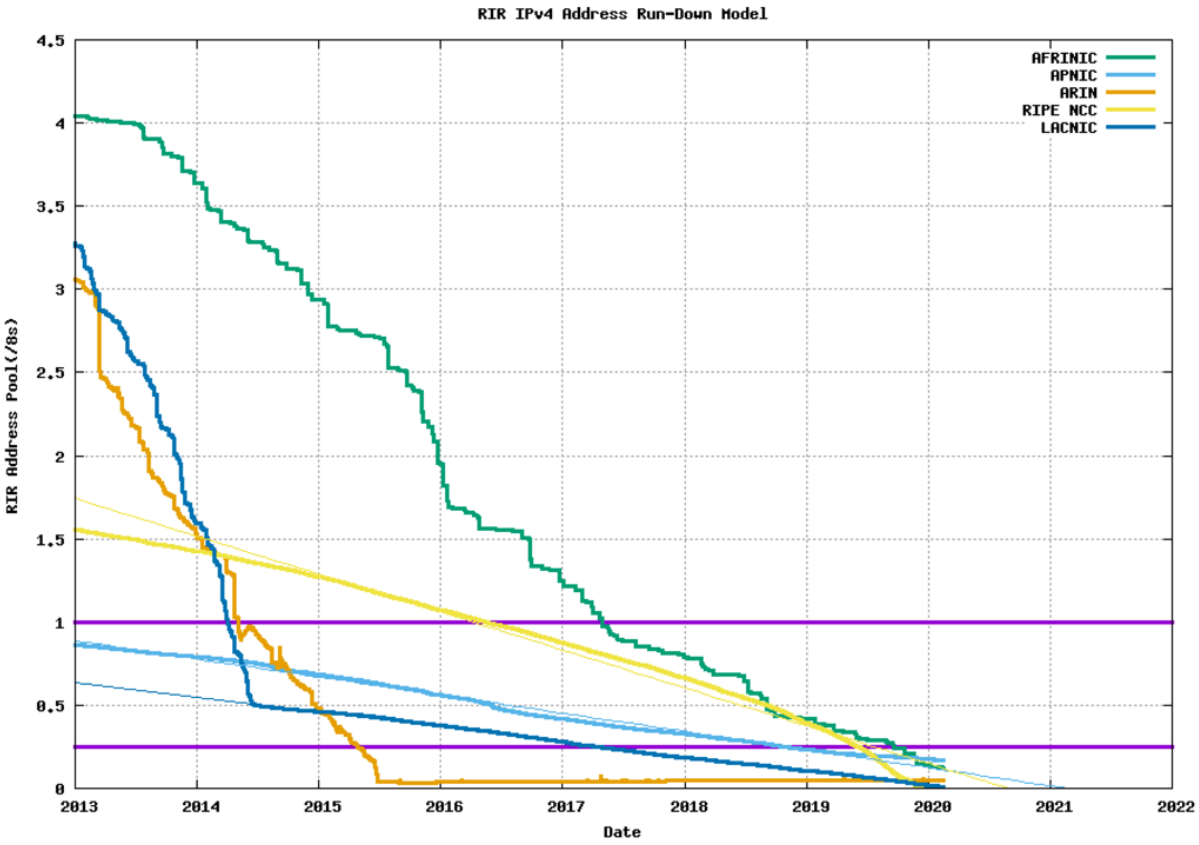
[RIRs (Regional Internet Registries)](https ://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/)

9. Epuisement des adresses IPv4

Pour l'instant, la grande majorité des ressources Internet sont disponibles en IPv4. L'épuisement des adresses IPv4 (publiques) est l'épuisement du "pool" d'adresses IPv4 non allouées par les RIRs. Étant donné qu'il y a moins de 4,3 milliards d'adresses disponibles, l'épuisement a été anticipé depuis la fin des années 1980, alors que l'Internet a connu une croissance spectaculaire dès sa commercialisation. Cet épuisement est l'une des raisons du développement et du déploiement de son protocole successeur IPv6.

IPv6 est proposé et est déjà déployé dans les réseaux des opérateurs et des grands fournisseurs de contenu. Il se déploie progressivement dans les centres de données et sur les connexions domestiques. Toutefois peu d'entreprises le déploient dans leur LAN malgré sa présence *de facto*[1].

1. IPv6 est activé et fonctionne par défaut dans toute solution d'entreprise Microsoft Active Directory.

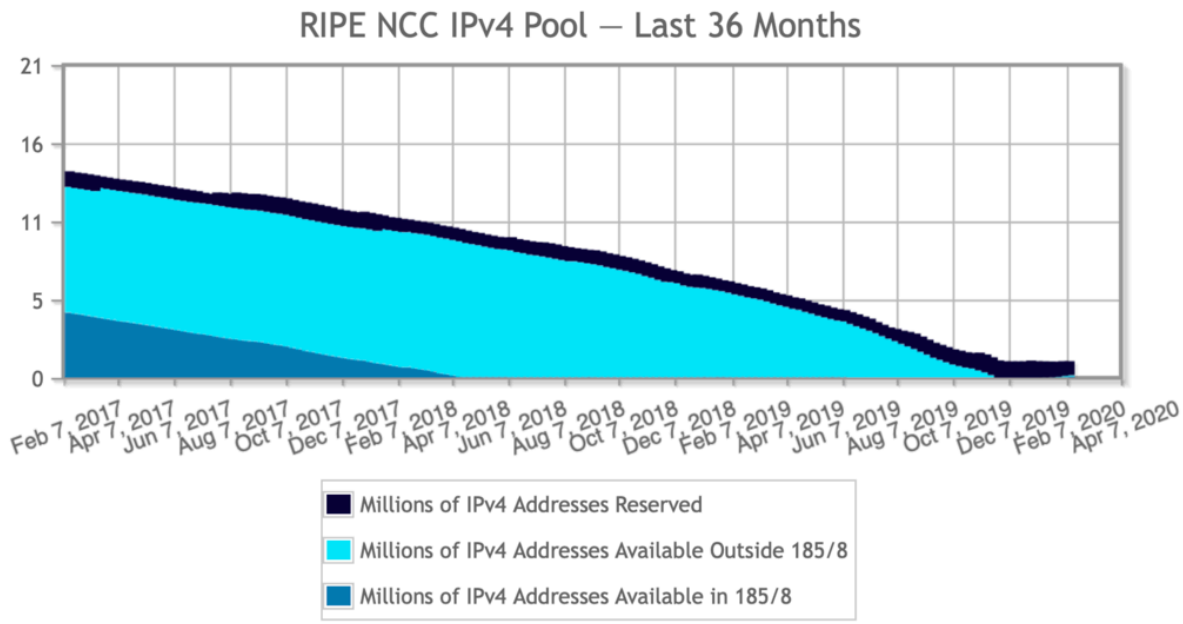


[Projection de Geoff Huston sur l'évolution des pools d'adresses IP par RIR](https ://ipv4.potaroo.net/)

Source de l'image : Projection de Geoff Huston sur l'évolution des pools d'adresses IP par RIR

Le 17 avril 2018, le RIPE-NCC vient d'attribuer son dernier bloc IPv4 185/8 en blocs /22 seulement aux LIRs disposant déjà de blocs IPv4/IPv6. En conséquence :

- Les nouveaux entrants sont exclus d'IPv4.
- Trafic illégal d'adresses IPv4 prévisible.
- Cela signifie concrètement le début d'une impossibilité à déployer largement des services TCP/IPv4 au niveau global.

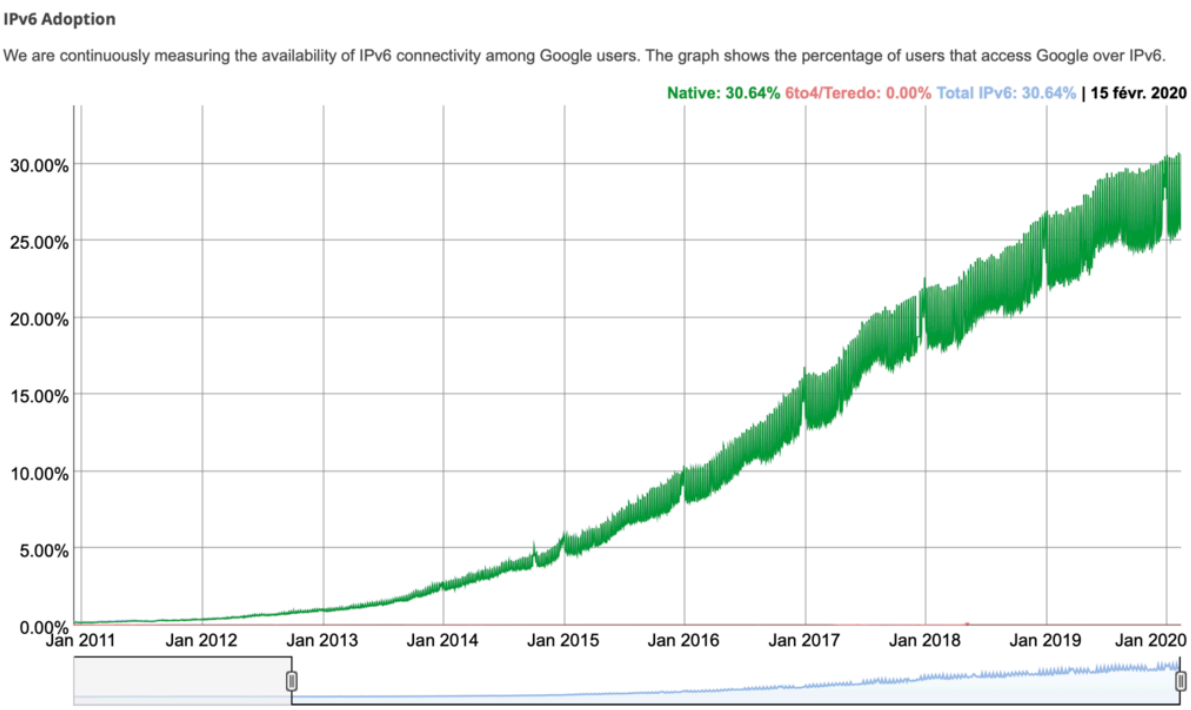


[RIPE NCC IPv4 Available Pool](https ://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion/ipv4-available-pool-graph)

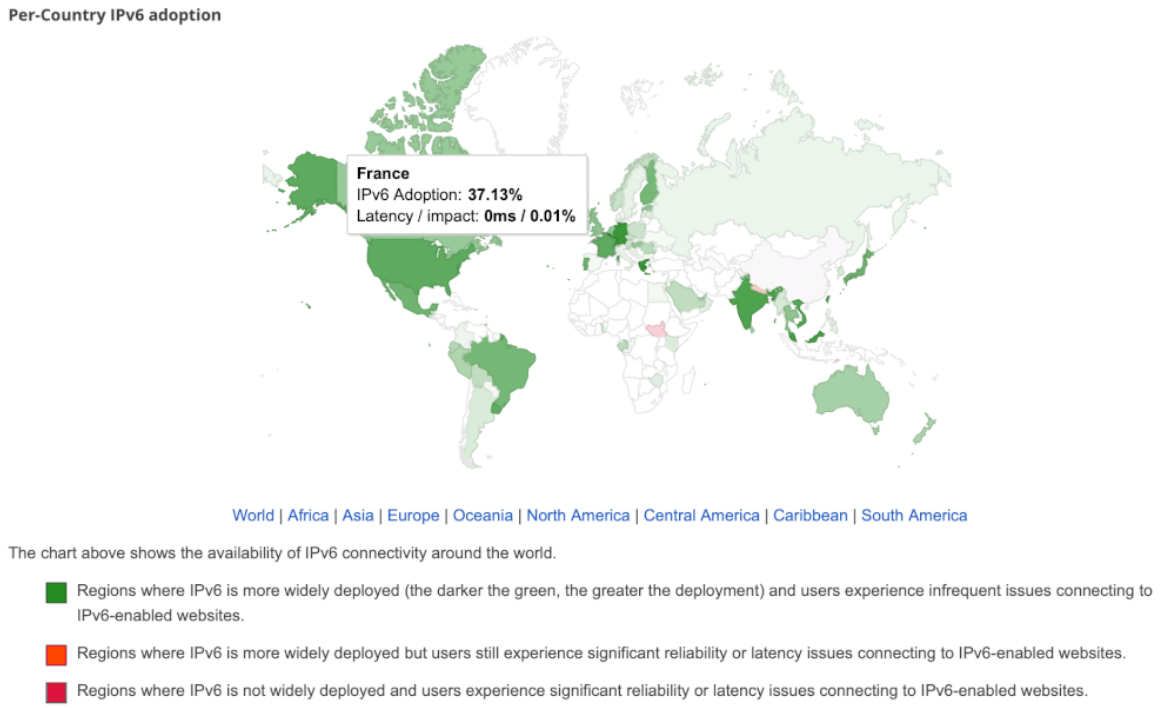
D'ici mai 2020, le RIPE-NCC pourra encore attribuer 9,3 millions d'adresses qui étaient réservées et qui ont été récupérées.

10. Transition vers IPv6

Étant donné que toutes les attributions d'adresse IPv4 sont épuisées à terme, IPv6 doit être déployé. Mais quel est le taux d'adoption d'IPv6 dans le Monde ?



[IPv6 Adoption sur base des statistiques de Google](https ://www.google.com/intl/en/ipv6/statistics.html)



[Adoption IPv6 par pays selon Google](https ://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption)

Vu que les hôtes terminaux ne peuvent utiliser que l'un ou l'autre des deux protocoles IP, on peut considérer que l'Internet IPv6 est un second Internet dont l'architecture va progressivement supplanter IPv4.

Cette phase de transition "duale" pourrait durer jusqu'à 10 ans et plus. Stéphane Bortzmeyer écrivait ceci en première phrase de son article du 7 juin 2018 intitulé "Aurait-il fallu faire IPv6 « compatible » avec IPv4 ?" : *Le déploiement du protocole IPv6 continue, mais à un rythme très réduit par rapport à ce qui était prévu et espéré. À cette vitesse, on aura encore de l'IPv4 dans 20 ou 30 ans.*

11. Généalogie IPv4/IPv6

D'un point de vue généalogique, IPv6 est un "vieux" protocole qui entre seulement maintenant dans sa phase de déploiement global. En réalité, la pénurie d'adresses a été prévue dès la mise en oeuvre commerciale d'IPv4 à la fin du XXème siècle. Au même moment, un nouveau protocole IPv6 est conçu. Entretemps, il fait l'objet de nombreuses expérimentations locales et globales.

Période	Protocoles Internet
1981	IPv4 Classes d'adresses (RFC791).
1985	Masques de sous-réseaux (RFC950).
1993	CIDR-VLSM (RFC4632).
1994	NAT (RFC1631 rendu obsolète par RFC3022).
1996	Adressage privé (RFC1918).
1995-1998	IPv6 (RFC2460).
World IPv6 Launch Day (2012)	La plupart des fournisseur d'accès Internet, des fabricants de matériel réseau grand public et des entreprises Web à travers le monde ont activé de manière permanente le protocole IPv6 pour leurs produits et service.
2017	RFC8200 : IPv6 passe de statut "DRAFT STANDARD" à "INTERNET STANDARD".

Depuis 2012, nous sommes entrés dans une longue période de transition de la **double pile IPv4/IPv6** qui pourrait durer plus de 10 ans.

Il n'est plus envisagé de manière crédible de traduire le nouveau protocole dans l'ancien, IPv6 dans IPv4, autrement que pour dépanner ou bricoler. Par contre, l'inverse, c'est-à-dire traduire l'ancien protocole dans le nouveau,

IPv4 dans IPv6, annonce la prochaine étape de transition. Les solutions NAT64/DNS64 offrent la possibilité d'un déploiement local "IPv6 Only" tout en rendant encore accessible certaines ressources "seulement IPv4". Ce scénario n'est pas encore globalement d'actualité même si le cas a déjà fait l'objet d'expérimentations convaincantes[2]. Une solution NAT64/DNS64 est encore certainement aujourd'hui une solution coûteuse pour une entreprise et relèverait plutôt d'une responsabilité d'opérateur[3] et de gestionnaires de centres de données.

12. Nouveautés IPv6

D'un point de vue strictement technique, on peut considérer qu'IPv6 est le résultat amélioré de notre longue expérience d'IPv4. D'un point de vue comparatif, IPv4 et IPv6 sont à la fois si semblables et tellement différents. Quelles sont les nouveautés en IPv6 par rapport à IPv4 ?

- Adressage incommensurablement étendu sur 128 bits
- Le Broadcast disparaît au profit du Multicast
- Plus besoin de NAT, *a priori*
- ARP disparaît au profit de Neighbor Discovey (ICMPv6)
- Entrée DNS IPv6 AAAA
- **Le routeur configure le réseau**
- Adressage automatique local obligatoire
- Autoconfiguration automatique sans état seulement, DHCPv6 seulement ou les deux pour autant de préfixes à distribuer.
- Plug-and-Play par défaut
- DHCPv6-PD, solutions IPAM
- Reprise en main de la sécurité des accès, des régles de filtrage, de l'architecture sécurisée

2. IPv6-only at Microsoft : "Hopefully, migrating to IPv6 (dual-stack) is uncontroversial at this stage. But for us, moving to IPv6-only as soon as possible solves our problems with IPv4 depletion and address oversubscription. But it also moves us to a simpler world of network operations where we can concentrate on innovation and providing network services, instead of wasting energy battling with such a fundamental resource as addressing."
3. RFC7269.

Quatrième partie Adressage IPv6

IPv6 est un sujet fortement vérifié dans les certifications Cisco CCNA. Cette partie s'intéresse à la reconnaissance et à la validation des adresses IPv6, à leur configuration sur les interfaces, à leur vérification et à leur diagnostic. Enfin, on trouvera un propos sur la manière de concevoir des plans d'adressage IPv6.

L'adressage IPv6 est codé en hexadécimal. Une telle étendue sur 128 bits nécessitait une représentation plus efficace que celle d'IPv4 (décimale pointée). Toutefois, l'usage de l'hexadécimal peut être un frein à l'acceptation et à la compréhension du protocole auprès de certains. Il s'agit d'un résistance que l'on peut facilement dépasser si on s'y intéresse le temps de la lecture de ces quelques articles.

On apprendra à identifier, à écrire et à vérifier des adresses : les adresses Unicast et Multicast et parmi elles les adresses Loopback (Node-Local), Link-local, Global Unicast, Unique Local, Well-Know Multicast, et Sollicited-Node Multicast. On apprendra aussi à distinguer le préfixe et l'identifiant d'interface et à envisager le contrôle sur la construction de l'adresse. Enfin, on ne manquera pas de démontrer la souplesse de l'adressage en matière de découpage de blocs d'adresses.

4. Introduction aux adresses IPv6

On commencera par définir ces identifiants IPv6 encore trop peu connus. Ensuite, on apprendra à écrire, à simplifier et à valider une adresse IPv6.

1. Terminologie IPv6

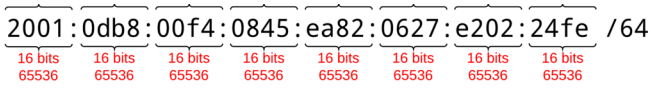
- Un **lien** (*link*) est le support physique (ou la facilité telle un tunnel) de communication entre deux noeuds au niveau de la couche 2 liaisons de données/accès réseau (technologies LAN/WAN).
- Deux **noeuds** sur le même lien sont voisins (neighbors).
- Une **interface** est l'attachement d'un noeud au lien.
- Une **adresse** est un identifiant pour une interface (Unicast) ou pour un ensemble d'interfaces (Multicast). Une interface peut avoir plusieurs adresses IPv6 et être inscrite dans plusieurs groupes Multicast.
- Un **préfixe** désigne l'appartenance à un domaine IPv6.
- Le masque donne l'étendue du domaine IP : il se note après l'adresse et une barre oblique / ("slash"). Il indique le nombre de bits fixes dans une adresse.

2. Définition et étendue d'une adresse IPv6

On rappellera utilement que le protocole IPv6 doit être activé volontairement sur les interfaces des routeurs Cisco contrairement aux systèmes d'exploitation courants comme Windows ou Linux pour lesquels IPv6 est activé par défaut.

Les adresses IPv6 sont des identifiants uniques d'interfaces :

- codés sur 128 bits
- et notés en hexadécimal en 8 mots de 16 bits (4 hexas) séparés par des " :".



Exemple d'adresse IPv6 Global Unicast

Le **masque** identifie la partie fixe d'une adresse qui correspond aussi au numéro de réseau de 64 bits (le préfixe). Le **préfixe** est l'élément commun à toutes les adresses d'une même plage (au sein d'un réseau).

Par exemple, pour l'adresse "Global Unicast" `2001:0db8:00f4:0845:ea82:0627:e202:24fe/64` dans son écriture extensive :

```
2001:0db8:00f4:0845:ea82:0627:e202:24fe/64
---- ---- ---- ---- ---- ---- ---- ---- --
16b  16b  16b  16b  16b  16b  16b  16b
------------------- ------------------- --
    Préfixe          Interface ID       Masque
```

Le **préfixe** ou la première adresse de la plage est `2001:0db8:00f4:0845::/64`. Le `/64` correspond aux 64 premiers bits de l'adresse que l'on peut aisément compter.

- Contrairement à IPv4, cette première adresse peut être attribuée à une interface.
- Une adresse IPv6 configurée sur une interface dispose dans 99,999 % des cas d'un masque par défaut de 64 bits noté `/64`.
- *A priori*, plus de calculs de masque exotique. La consigne est contraire à celle d'IPv4 conservatrice : "Jusqu'au gaspillage, réalisez des connexions en IPv6 !"
- Les 64 derniers bits appelés *identifiants d'interface* identifient l'interface dans le réseau.

À partir de l'exemple précédent, la valeur `ea82:0627:e202:24fe` correspond à l'identifiant d'interface.

La plage du bloc IPv6 s'étend sur 2 EXP 64 possibilités d'adresses, de la première adresse à la dernière :

```
2001:0db8:00f4:0845:0000:0000:0000:0000/64
2001:0db8:00f4:0845:ffff:ffff:ffff:ffff/64
---- ---- ---- ---- ---- ---- ---- ---- --
16b  16b  16b  16b  16b  16b  16b  16b
------------------- ------------------- --
    Préfixe          Interface ID       Masque
```

Les 64 premiers bits sont identiques pour toutes les adresses d'un même bloc (`2001:0db8:00f4:0845`). Les 64 derniers bits varient de `0000:0000:0000:0000` à `ffff :ffff :ffff :ffff`. Cette dernière partie de 64 bits est appelée **Identifiant d'interface (IID Interface Identifier)**. Elle sert à identifier les interfaces au sein du réseau.

3. Ecriture résumée

Heureusement, on peut résumer l'écriture d'une adresse IPv6. Les systèmes sont obligés d'accepter ces simplifications d'écriture.

Par exemple, pour l'adresse "Global Unicast" `2001:0db8:00f4:0845:ea82:0627:e202:24fe/64` dans son écriture extensive :

```
2001:0db8:00f4:0845:ea82:0627:e202:24fe
---- ---- ---- ---- ---- ---- ---- ----
16b  16b  16b  16b  16b  16b  16b  16b
------------------- -------------------
    Préfixe          Interface ID
```

Voici l'écriture résumée qui respecte deux règles faciles à retenir :

- Les zéros en en-tête de chaque mot peuvent être optimisés ;
- Une seule fois seulement, une suite consécutive de mots tout-à-zéro peut être résumée par `::`.

```
2001:0db8:00f4:0845:ea82:0627:e202:24fe
```

```
2001:-db8:--f4:-845:ea82:-627:e202:24fe
```

```
2001:db8:f4:845:ea82:627:e202:24fe
```

Ou encore l'adresse `fe80:0000:0000:0000:bb38:9f98:0241:8a95` peut être résumée en `fe80::bb38:9f98:241:8a95` :

```
fe80:0000:0000:0000:bb38:9f98:0241:8a95
```

```
fe80:----:----:----:bb38:9f98:-241:8a95
```

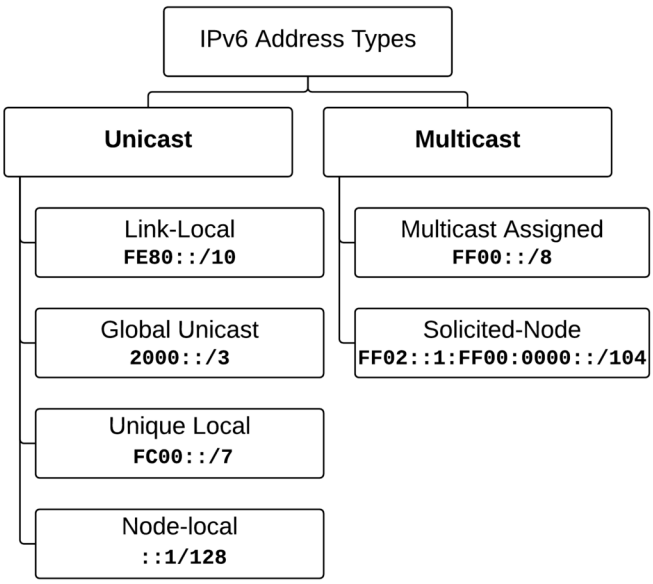
```
fe80::bb38:9f98:241:8a95
```

4. Types d'adresse IPv6

En IPv6, il y a pas mal de nouveautés en matière d'adresses :

- Le Broadcast disparaît d'IPv6. Il est remplacé par l'adressage Multicast plus fin.
- Une adresse préexiste toujours sur chaque interface activée en IPv6.
- Les adresses IPv6 rétablissent la connectivité globale (publique).
- Le NAT en IPv6 ne semble pas indispensable. Il est même déconseillé.
- Des adresses privées IPv6 restent néanmoins utiles pour transporter du trafic privé (sur des lignes privées, dans des tunnels VPN)

On trouvera plusieurs types d'adresse IPv6.



Types d'adresse IPv6

On distingue principalement les adresses **Unicast** des adresses **Multicast**.

Le RFC intitulé IP Version 6 Addressing Architecture (RFC 4291) indique les adresses dans lesquelles un hôte IPv6 doit se reconnaître :

- Une adresse Link-local sur chaque interface.
- Des adresses Unicast ou Anycast qui ont été configurées sur les interfaces du noeud.
- L'adresse de Loopback.
- Les adresses All-Nodes Multicast.
- L'adresse Solicited-Node Multicast pour chacune des adresses Unicast ou Anycast.
- Les adresses Multicast des groupes joints par le noeud.

Adresses Unicast

Une adresse Unicast est une adresse qui désigne une seule destination.

Parmi les adresses IPv6 Unicast, on trouve plusieurs classes réservées à certains usages.

- **Node-Local** `::1/128` : adresse de bouclage.
- **Link-Local** `fe80::/10` : adresse obligatoire et indispensable au bon fonctionnement du protocole.
- **Global Unicast** `2000::/3` : adresse publique.
- **Unique Local** `fc00::/7` (c'est le préfixe `fd00::/8` qui est utilisé) : adresse privée (aléatoire).

Une adresse **Anycast** ne se distingue pas d'une adresse Unicast ; ce terme "Anycast" désigne une adresse de livraison qui atteindra sa destination par une technique de routage au plus proche ou au plus efficient.

On remarquera aussi : **Unspecified** `::/128` : route non spécifiée, et **Default Route** `::/0` : route par défaut.

Adresses Multicast

Une adresse Multicast est une adresse qui désigne potentiellement plusieurs destinations. Les adresses Multicast remplacent utilement les adresses de Broadcast.

On trouvera deux types d'adresse Multicast que l'on reconnait par leur préfixe `FF00::/8` :

- **Well-Know Multicast** : adresses Multicast bien connues
- **Solicited-Node Multicast** : adresses utilisées dans la découverte de voisinage (ND)

Concrètement, plusieurs interface du réseau et de l'inter-réseau se mettent à l'écoute d'une adresse Multicast, c'est-à-dire qu'elles seront potentiellement plusieurs à accepter du trafic à destination de cette adresse Multicast (si il leur est livré par les commutateurs).

5. Méthodes de configuration des interfaces

Une adresse IPv6 attribuée à une interface est constituée d'un préfixe de 64 bits et d'un identifiant d'interface de 64 bits.

Un identifiant d'interface peut être créé de différentes manières :

- statiquement : `2001:db8:14d6:1::1/64`, `2001:db8:14d6:1::254/64`, `fe80::101`, par exemple.
- par autoconfiguration (SLAAC) en utilisant l'une de ces trois méthodes :
  1. MAC EUI-64, par défaut (RFC 4291)

2. tirage pseudo-aléatoire, par défaut chez Microsoft, Ubuntu, Mac OSX (RFC 4941)
3. CGA, peu implémenté (RFC 3972)

- dynamiquement : DHCPv6 (RFC 3315) stateful, si le client est installé et activé (par défaut sur Microsoft Windows et Mac OSX)

Une interface IPv6 peut accepter plusieurs adresses dans un même préfixe mais aussi dans des préfixes distincts. L'idée est d'améliorer finement les politiques de routage et de filtrage en fonction de ces adresses.

6. Autoconfiguration Automatique

Comment les adresses parviennent-elles à se configurer toutes seules ? Le routeur du réseau local envoie régulièrement des messages "Neighbor Discovery" (ND) (ICMPv6 type 134), appelés des "Router Advertisements" qui poussent ces paramètres de configuration auprès des machines du réseau local. C'est le routeur IPv6 qui configure le réseau et de manière très fine. Les interfaces s'autoconfigurent selon la méthode SLAAC (*Stateless Address Autoconfiguration*) qui implique un trafic "Neighbor Discovery" (ND) de vérification avec l'usage des adresses Link-Local et du Multicast (NUD et DAD).

Si le Broadcast disparait, ARP est remplacé par ND (ICMPv6). Ce n'est pas anodin et cette nouveauté mérite attention.

DHCPv6 est un nouveau protocole qui se décline en deux formules (avec et sans état) et qui peut se combiner à la méthode SLAAC d'autoconfiguration brièvement décrite ci-dessus. Cette dernière est juste activée par défaut sur tout hôte IPv6. L'usage de DHCPv6 nécessite un logiciel client DHCPv6 (déjà présent sous Windows et Mac) sur l'ordinateur client. Il est conseillé d'utiliser pleinement DHCPv6 dans un réseau bien géré. Il n'y a aucune obligation à laisser les hôtes terminaux s'autoconfigurer.

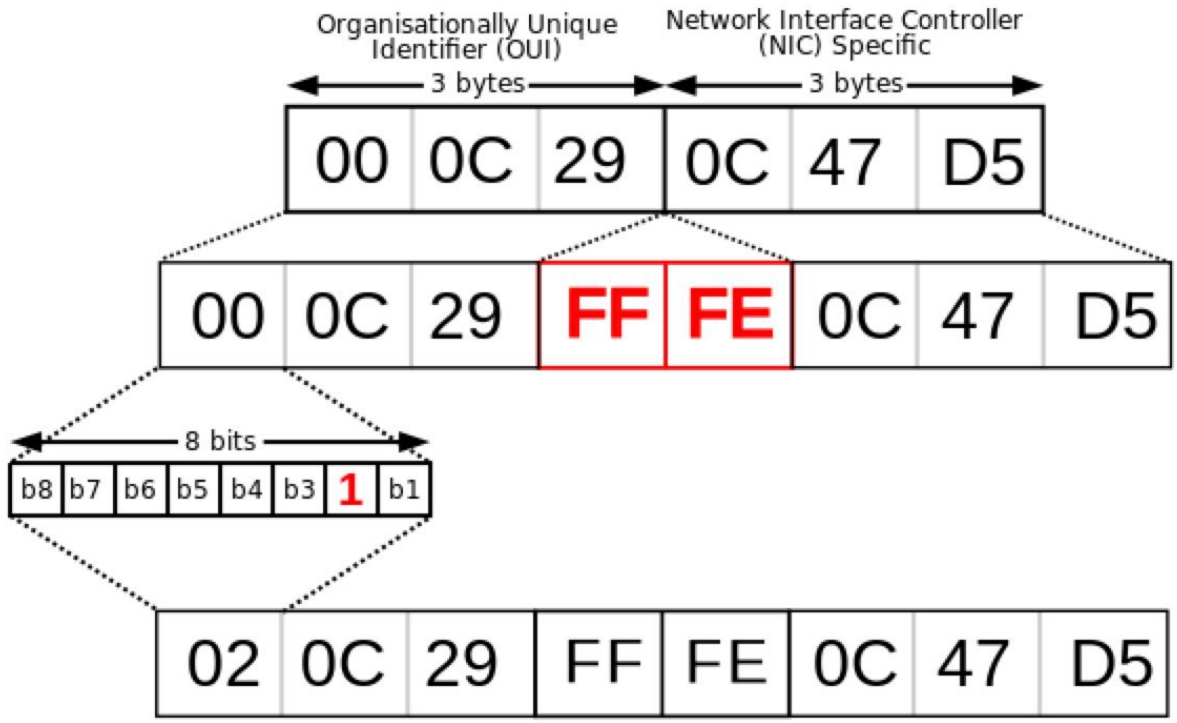
Enfin, c'est sans parler des comportements et configurations particulières sur Cisco IOS ou autres ou encore des stratégies et techniques de transition, DNS, la sécurité, le développement de code avec de l'IPv6.

7. Autoconfiguration des identifiants d'interface

Identifiant d'interface MAC-EUI64 "Modified"

MAC EUI-64 est une est des méthodes de configuration automatique des ID d'interface qui se fonde sur l'adresse MAC IEEE 802 (48 bits).

On passe d'une adresse codée sur 48 bits à 64 bits en insérant 16 `FF :FE` au milieu de l'adresse MAC entre les 24 premiers bits et les 24 derniers bits. De plus, la méthode exige que le 7ième bits de poids fort de l'adresse soit inversé passant de la valeur "Local" à "Universal" d'où ce terme "EUI64 Modified".



MAC-EUI 64 Modified

Pour compléter le propos, on ne manquera pas d'observer les paramètres acquis par une station Linux Debian 7 qui offre un service plus "standard" dans les mêmes conditions :

```
root@debian:~# ifconfig
eth0      Link encap:Ethernet  HWaddr b8:27:eb:59:70:f3
          inet adr:192.168.1.119  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fd26:44e1:8c70:fd00:ba27:ebff:fe59:70f3/64 Scope:Global
          adr inet6: fe80::ba27:ebff:fe59:70f3/64 Scope:Lien
          adr inet6: 2001:db8:acaf:fd00:ba27:ebff:fe59:70f3/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:93310 errors:0 dropped:49 overruns:0 frame:0
          TX packets:76990 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:11548535 (11.0 MiB)  TX bytes:14021689 (13.3 MiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:17546 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17546 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:1199358 (1.1 MiB)  TX bytes:1199358 (1.1 MiB)
```

On trouvera sur cet ordinateur deux interfaces `eth0` et `lo`. La sortie donne la portée de chaque adresse IPv6.

L'interface `eth0` connectée au réseau local ne démarre pas par défaut un client DHCPv6, ce n'est pas erreur. Sur cette interface, on trouvera les trois types d'adresses. Pour chacune, l'identifiant d'interface est identique. Il est généré par la méthode MAC-EUI64 (méthode par défaut). MAC-EUI64 est une méthode standardisée qui vise à obtenir un identifiant d'interface de 64 bits à partir d'une adresse MAC de 48 bits. Aussi, ce n'est pas une erreur mais le comportement par défaut.

```
fe80::ba27:ebff:fe59:70f3
2001:db8:acaf:fd00:ba27:ebff:fe59:70f3
fd26:44e1:8c70:fd00:ba27:ebff:fe59:70f3
```

Avez-vous aperçu le souci de confidentialité ? On retrouve l'adresse MAC de l'interface dans l'identifiant d'interface de cette adresse. Cette portion significative de l'adresse permet d'identifier de manière certaine l'interface quel que soit son préfixe. De plus, les 24 premiers bits de l'adresse MAC (ici `b8:27:eb`) identifient le matériel ; à vous de le retrouver.

Soit la méthode MAC-EUI64 insère 16 bits manquants **`FFFE`** après les 24 premiers bits de l'adresse MAC (OUI, *Organizationally Unique Identifier*) dont le 7e bit a été inversé :

de `b8:27:eb :59:70:f3`, on passe à `ba27:ebff :fe59:70f3`

16 bits ont été ajoutés et la valeur du deuxième hexa est passée de `8` à `a` soit augmenté de 1 bit. Ce renversement signifie que l'adresse est "administrée localement".

Il est possible de modifier ce comportement par défaut quel que soit le système d'exploitation.

Privacy Extensions for Stateless Address Autoconfiguration in IPv6

Alors que la méthode de configuration des interfaces par défaut obligatoire est la méthode MAC-EUI64, les hôtes Windows et Linux domestiques préfèrent la méthode "Privacy Extension" (Privacy Extensions for Stateless Address Autoconfiguration in IPv6).

Cette méthode autoconfigure deux identifiants d'interface pour une durée limitée dans chaque préfixe :

- **Une adresse "publique"** (c'est-à-dire non secrète) pour les serveurs, enregistrés dans un serveur DNS par exemple, qui est utilisée pour accepter des connexions directes entrantes venant d'autres machines. Des pare-deux dans le chemin pourraient bloquer ce trafic.
- **Une adresse "temporary"** utilisée comme "bouclier" sur l'identité des clients quand ils débutent une connexion.

On trouvera des exemples de ces adresses et identifiants d'interfaces autoconfigurés "Privacy Extensions" dans la page Prise d'information IPv6.

8. Résumé

Manque adresse loopback

Link-Local	Global Unicast	Unique Local
L'adressage Link-Local (Unicast) se reconnaît par : un préfixe `FE80::/10` et un identifiant d'interface de 64 bits autoconfiguré (MAC-EUI64 ou aléatoire) ou fixé (Cisco)	Préfixe : `2000::/3` (`2000::/4`)	Préfixe : `FC00::/7` (`FD00::/8`) adressage privé avec 40 bits de préfixe aléatoire
Est obligatoire sur toutes les interfaces quand IPv6 est activé	optionnel	optionnel
Ces destinations ne sont jamais transférées par les routeurs !	Connectivité de bout en bout nécessaire	fonctionne dans un interréseau privé
Ces adresses sont utilisées dans le trafic de gestion comme ND, SLAAC, avec les protocoles de routage.	Trafic vers l'Internet	Trafic sur des lignes privées (physiques ou virtuelles).

Révisions

Architecture

- Spine-leaf, ACI
- On-premises et cloud, Cloud