Protocole	*acronyme*	description	PORT	PROTOC
Adresse Ipv4	*Internet Protocol Address*	identifiant réseau propre à chaque appareil. Réglementé par l'ICANN (Internet Corpo AsignedName N°). Si l'ordinateur dispose de plusieurs interfaces, chacune d'elle aura une adresse IP spécifique (une interface peut disposer de plusieurs adresses IP). Chaque paquet transmis par le protocole IP contient l'adresse IP de l'émetteur, ainsi que l'adresse IP du destinataire. codée sur 32 bits attribués.		
adresse Ipv6	*Internet Protocol version 6*	protocole réseau sans connexion → couche 3 OSI. Composé de 8 groupes de 2 octets = 128 bits. Ecriture hexadécimale (base 16, 4bits pour une base) : 64bits/préfixe routage, 64bits/id d'interface . Différents types : lien-local (préfixe FE80/10, ND) / unicast global (unique au minde → Internet, préfixe / multicast (envoyé à tous les appareils du groupe) / anycast (envoyé uniquement au voisin le plus proche).		
AES	*Advanced Encryption Standard*	algorithme de chiffrement symétrique (128 ou 256 bits)		
APIPA	*Automatic Private Internet Protocol Addressing*	APIPA est le nom donné par Microsoft au protocole IPv4LL. Ce protocole, créé par IETF, permet de configurer automatiquement des adresses IP de portée lien. 169.254		
ARP	*address resolution protocol*	utilisé pour faire correspondre les adresses IP - qui opèrent au niveau 3 de l'OSI - aux adresses MAC du niveau 2 au sein d'un sous-réseau. Cette fonction est essentielle pour acheminer le trafic vers le bon ordinateur au sein d'un sous-réseau.		
BGP	*Border Gaterway Protocol*	échanger des informations de routage et d'accessibilité de réseaux entre Autonomous Systems		
BPDU	*Bridge Protocol Data Units*	messages envoyés périodiquement par les switches pour établir et maintenir la topologie en arbre sans boucles.		
CEPH		Ceph est une solution libre de stockage distribué qui propose trois protocoles en un avec : Bloc, Fichiers & Objet. Apporte évolutivité et redondance.		
DHCP	*Dynamic Host Configuration Protocol*	assurer la configuration automatique des paramètres IP d'une machine connectée à un réseau, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. 4 temps : discover/offer/request/ack	**67 et 68**	**UDP**
DNS	*Domain Name Systeme*	traduire noms de domaines en adresses IP	**53**	**UDP**
EAP	*Extensible Authentification Protocol (protocole d'identification et d'authentification et d'échange de clés)*	Mode authentifié entreprise. Utilise un serveur d'authentification (en général RADIUS, protocole AAA → bientôt Diameter) chargé de distribuer une clé à chaque utilisateur : norme 802.11i		
Echanges DB topologique		troisième protocole utilisé par OSPF		
EGP	*Exterior Gateway Protocol*	Portocole de routage dynamique. Par classe → EGP / sans classe → BGP		
EIGRP	*Enhanced Interior Gateway Routing Protocol*	Protocole (routage dyn) vectoriel de distance amélioré (Cisco), hybride distance / état de liaison (pas de cartographie complète du réseau comme OSPF). Utilise la métrique pour trouver le meilleur chemin entre 2 périph de couche 3. optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur. Augmente la disponibilité et la convergence. Envoi périodique de paquets HELLO. N° proto 88		
Ethernet		Technologie et protocole de communication et de connexion filaire aux LAN et WAN (cf 802.3)		

FLOODING	*Inondation*	prévenir les voisins des changements (protocole OSPF)		
FTP	*File Transfert Protocol*	communication destiné au partage de fichiers sur un réseau TCP/IP	**21**	**TCP**
HELLO		Vérifie les liaisons avec les voisins (protocole OSPF)		
HTTP	*HyperText Tranfert Protocol*	communication d'échange de données sur internet (pages web)	**80**	**TCP**
HTTPS	*Hypertext Transfer Protocol Secure*	combinaison du HTTP avec une couche de chiffrement TLS. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable	**443**	**TCP**
ICMP	*Internet Control Message Protocol (Couche 3)*	protocole que les périphériques d'un réseau utilisent pour communiquer les problèmes de transmission de données. L'une des principales façons de l'utiliser est de déterminer si les données atteignent leur destination et ce au bon moment. PING		
IG(R)P	*Interior Gateway (Routing) Protocol*	Protocole de routage dynamique. Peut être à vecteur de distance (avec classe : RIP v1, IGRP / sans classe = utilisation de MSRLV : RIP v2, EIGRP). Ou à état de lien (sans classe : OSPF, IS-IS)		
IMAP	*Internet Message Access Protocol*	permet d'accéder à ses courriers électroniques directement sur les serveurs de messagerie. Accessible pour plusieurs postes/personnes. Connexion continue avec serveur	**143**	**TCP**
Ipv6 ND	*Ipv6 Neighbor Discovery*	découverte du voisin (pas de broadcast, pas d'ARP). Basé sur ICMPv6		
ISCSI	*Internet Small Computer System Interface*	Protocole de stockage de données en réseau. Permet de relier les installations. L'autoriser sur le réseau TCP/IP. Encapsulation des commandes SCSI traditionnelles dans des paquets pouvant être acheminés par le réseau		
Kerberos		Système d'authentification (AD) par chiffrement symétrique	**88**	
L2TP	*Layer To Tuneling Protocol*	protocole de tunélisation de niveau 2. Combiné avec un autre protocole pour sécuriser la connexion		
LDAP	*Lightweight Directory Access Protocol*	interrogation et modification des services d'annuaire (évolution du protocole DAP). Repose sur TCP/IP. Il a évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs	**389**	**TCP**
LWAPP	*Lightweight Access Point Protocol*	contrôler plusieurs points d'accès sans fil Wi-Fi à la fois. Cela peut réduire le temps consacré à la configuration, à la surveillance et au dépannage d'un grand réseau. Le système permettra également aux administrateurs réseau d'analyser de près le réseau.		
MPLS	*Multi Protocol Label Switching*	Technique de commutation : peut assurer l'étanchéité des VPN sur le nuage. Réseau virtuel hermétiquement fermé mais partagé sur nuage. Technologie conçue pour améliorer la vitesse et l'efficacité du transfert des données. Distribue plusieurs réseau virtuel entre eux. Lien dédié qui fourni QoS le long du chemin unique		
NFS	*Network File System*	transferts de fichiers par le réseau principalement utilisé sur les systèmes Linux/Unix, (compatible avec Windows et MacOS). L'utilisateur accède à des fichiers stockés sur un serveur distant, fonctionne selon le mode client/serveur (open source).	**2049**	**TCP**
NTP	*Network Time Protocol*	protocole de synchronisation de réseau, permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure	**123**	**UDP**

OSPF	*Open Shortest Path First*	algorithme à état de lien (base de donnée de la topo du réseau) → chemin le plus efficace. Organisation en zones logique → routeur de bordure de zone (ABR). 3 protocoles utilisés : Hello, flooding, échanges DB topologique. Algo Dijkstra SPF. Convergence rapide, conso ressources élévé, complexe. N° proto 89. À l'intérieur de chaque zone, certains routeurs joueront un rôle particulier : DR (designated router) / BDR (Backup Designated Router)		
POP3		Contrairement aux protocoles modernes qui utilisent la synchronisation bidirectionnelle, le POP3 ne prend en charge que la synchronisation unidirectionnelle de l' e-mail, ce qui permet aux utilisateurs de télécharger des e-mails d'un serveur vers un client.	**110**	**TCP**
PPP	*Point to Point Protocol*	communication ordinateur –> modem vers FAI, réseau téléc		
PPTP	*Protocol Point to Point*	ancien protocole VPN. Pas de cryptage		
RADIUS	*Remote AuthenticationDial-In User Service*	protocole client-serveur permettant de centraliser des données d'authentification		
RDP	*Remote Desktop Protocol*	Protocole de communication réseau sécurisé développé par Microsoft, permet de contrôler des ordinateurs à distance. Permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services. Des clients existent pour la quasi-totalité des versions de Windows, et pour d'autres systèmes d'exploitation, comme les systèmes GNU/Linux	**3389**	**TCP**
ReFS	*Resilient File System*	système de fichiers de Microsoft le plus récent. Il a été conçu pour optimiser la disponibilité des données, s'adapter efficacement aux jeux de données volumineux sur diverses charges de travail et garantir l'intégrité des données avec une résilience face aux altérations		
RIP (v2)	*Routing Information Protocol (v2)*	routage à vecteur de distance : se base sur nb de sauts. Max 15 sauts. Convergence lente si réseau complexe. Quasi obsolète. V2 = sans classe (variable)		
RTP / RTCP	*Real-Time Transport (Control) Protocol*	chargés de l'acheminement des données et du contrôle qualité (tel, streaming...). SRTP ajoute Secure → authentif+chiffrement AES		
SDP	*Session Description Protocol*	défini les paramètres d'une communication téléphonique. Encapsulé par le SIP		
SCCP	*Skinny Call Control Protocol*	point d'accès TFTP aux téléphones pour récupérer leur fichier de configuration. Le protocole VoIP ici n'est pas SIP, mais un protocole propriétaire de Cisco. Plus léger. Numéro d'identification : commande « option 150 ip 192.168.10.1 ».		
SCP	*Secure Copi*	transfert sécurisé de fichiers entre deux ordi utilisant le protocol de communication SSH. Le terme SCP désigne aussi bien le programme scp que le protocole. Fourni par package openssh-clients	**22**	**TCP**
SFTP	*SSH File Transfer Protocol*	programme de transfert de fichiers similaire à FTP, mais les transferts sont effectués au travers d'un tunnel SSH chiffré et il peut également utiliser l'authentification par clé publique. Fourni par package openssh-clients		
SIP	*Session Initial Protocol*	protocole qui porte la VoIP. Trunk SIP : Ce sont les canaux utilisés pour raccorder une architecture ToIP au central téléphonique de l'opérateur. C'est la version IP des lignes téléphoniques Numéris.	**5060 5061-sec**	**TCP UDP**
SMB	*Server Message Block*	largement utilisé pour partager des fichiers entre différents systèmes d'exploitation, y compris Windows, ce qui le rend idéal pour des environnements hétérogènes	**139 / 445**	**TCP**
SMTP	*Simple Mail Transfer Protocol*	transférer le courrier électronique vers les serveurs de messagerie électronique	**25**	**TCP**
SNMP	*Simple Network Management Protocol*	protocole de supervision (remonté d'infos) qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance	**161 / 162**	**UDP**

SPB	*Shorted Path Bridging*	Créer et configurer le réseau avec autorisation du routage multi-chemin (+ actif). Topologie de couche 2. Remplace STP		
SSH	*Secure Shell*	protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un analyseur de paquets pour voir ce que fait l'utilisateur	**22**	**TCP**
SSL	*Secure Sockets Layer*	protocole de sécurité Internet basé sur le chiffrement. 1995 Netscape → confidentialité, authentification et intégrité des données dans les communications Internet. Algoritme de chiffrement par bloc. Devenu TLS		
STP	*Spanning-Tree-Protocol*	empêcher formation de boucles dans le réseau éthernet commuté. Elit switch racine = point de ref. Puis chemin le plus court vers racine → root port (autres ports fermés contre boucles). Echange config via BPDU. Réévaluation si changement de topologie		
SYSLOG		service de journaux d'événements d'un système informatique (centralisation logs). Permet de faire un rapport de journalisation de l'ensemble de l'infrastructure au niveau des multiples événements qui ont lieu. C'est aussi le nom du format qui permet ces échanges. Partie cliente et partie serveur. Existe logiciel Syslog. CNIL/RGPD et ANSSI	**6514 / 514**	**TCP UDP**
TCP	*Transmission Control Protocol (couche 4)*	Connection orientée (fiable), séquencement, full-duplexe « 3 way handle » (syn/syn-ack/ack) : http(s), smtp, nfs, smb, ssh telnet, rdp, ldap		
TELNET		communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte. Créé en 1969, telnet est un moyen de communication très généraliste et bi-directionnel	**23**	**TCP**
TFTP	*Trivial File Transfer Protocol*	protocole simplifié de transfert de fichiers. ne gère pas le listage de fichiers, et ne dispose pas de mécanismes d'authentification, ni de chiffrement. Il faut connaître à l'avance le nom du fichier que l'on veut récupérer. De même, aucune notion de droits de lecture/écriture n'est disponible en standard	**69**	**UDP**
TLS	*Transport Layer Security*	successeur de SSL		
UDP	*User Datagram Protocol (couche 4)*	connexion non orientée (non fiable), pas de séquencement, « fire and forget » : dns, snmp, ntp, tftp, streaming		
URL	*Uniform Ressource Locator*	adresse web permettant d'accéder à des ressources internet : proto://préfix.nomdedomaine.TLD		
VMFS	*Virtual Machine File Système*			
VRRP	*Virtual Router Redundancy Protocol*	Protocole de redondance du routeur virtuel. Joue tous les rôles actifs lorsque le routeur principal est en arrêt		
WEP	*Wired Equivalent Privacy*	protocole de sécurité plus ancien et moins sécurisé. Il utilise des clés de chiffrement statiques		
WPA/ WPA2/WPA3	*Wi-Fi Protected Access*	protocoles de sécurité sont plus avancés et plus sûrs que le WEP. WPA, WPA2 et WPA3 utilisent des méthodes de chiffrement plus robustes comme TKIP (Temporal Key Integrity Protocol) pour WPA et AES (Advanced Encryption Standard) pour WPA2. Mode authentifié (srv Radius)/mode personnel (PSK)		
WPS (PSK)	*Wi-Fi Protected Setup (Pre-Shared Key)*	Mode personnel (sans serveur d'authenf). Protocole de configuration simplifié conçu pour faciliter l'ajout de nouveaux périphériques réseaux à un réseau Wi-Fi sécurisé. Il vise à simplifier le processus de connexion en éliminant la saisie manuelle de la clé de sécurité dans le gestionnaire de réseaux sans fil. Sans serveur d'authentification, les utilisateurs partagent la même clé (passphrase) comme avec le WEP		

ZFS	*Zebibyte File System*	système de fichiers open source sous licence CDDL. Ttrès haute capacité de stockage, l'intégration de beaucoup de concepts que l'on trouve sur d'autres systèmes de fichiers, et la gestion de volume		