Ports réseau essentiels

Ports logiques utilisés par les protocoles et services réseau

Port	TCP / UDP	Protocole / service	À quoi ça sert ?	Comment ça fonctionne ?	Exemple concret	À retenir
20	TCP	**FTP Data**	Transfert des données FTP.	En FTP actif, ce port transporte réellement les fichiers entre le client et le serveur.	Téléchargement ou envoi d'un fichier via FTP.	**FTP 20 = données**
21	TCP	**FTP Control**	Contrôle de la session FTP.	Le client s'y connecte pour envoyer les commandes : identification, navigation, demande de transfert.	Connexion à un serveur FTP et parcours des dossiers.	**FTP 21 = commandes**
22	TCP	**SSH**	Connexion distante sécurisée.	Communication chiffrée pour administrer une machine en ligne de commande.	Connexion à un serveur Linux à distance.	**SSH = accès distant sécurisé**
25	TCP	**SMTP**	Envoi et transfert d'e-mails.	Utilisé surtout entre serveurs de messagerie pour transmettre les messages.	Un serveur mail transmet un message à un autre serveur.	**SMTP = mail, TCP 25**
53	UDP / TCP	**DNS**	Traduction d'un nom de domaine en adresse IP.	UDP est le plus courant ; TCP est utilisé pour certaines réponses volumineuses ou transferts de zone.	google.com → adresse IP.	**DNS = nom → IP**
67	UDP	**DHCP serveur**	Attribution automatique de la configuration réseau.	Le serveur DHCP écoute sur 67 et fournit IP, masque, passerelle et DNS ; le client utilise 68.	La box donne automatiquement une adresse IP à un PC.	**DHCP serveur = 67**
69	UDP	**TFTP**	Transfert simple de fichiers.	Protocole léger, sans authentification, souvent utilisé pour PXE ou fichiers de configuration.	Transfert d'une image de démarrage ou d'une configuration.	**TFTP = UDP 69**
80	TCP	**HTTP**	Accès à un site web non chiffré.	Le navigateur contacte le serveur web sur le port 80 ; les échanges ne sont pas chiffrés.	Accès à un site en http://	**HTTP = web non sécurisé**
109	TCP	**POP2**	Ancien protocole de réception d'e-mails.	Ancienne version de POP, aujourd'hui obsolète et très rarement utilisée.	Ancien système de messagerie.	**POP2 = ancien**
110	TCP	**POP3**	Récupération des e-mails depuis un serveur.	POP3 télécharge les messages sur le client ; ils peuvent ensuite être supprimés du serveur selon la configuration.	Récupérer ses mails avec un logiciel de messagerie.	**POP3 = récupérer les mails**

Pour bien comprendre

Notions clés

Port réseau / logique : numéro qui identifie un service ou une application sur une machine.
Adresse IP : indique quelle machine reçoit les données.
Port : indique quel service reçoit les données.
Couche OSI : les ports sont liés à la couche 4.

Exemple de communication

192.168.1.25:52344 → 93.184.216.34:80
192.168.1.25 = IP du client
52344 = port temporaire du client
93.184.216.34 = IP du serveur
80 = port HTTP du serveur

À retenir

IP = machine concernée
Port = service concerné
TCP/UDP = manière dont la communication est transportée

Ports réseau essentiels - suite

Ports logiques utilisés par les protocoles et services réseau

Port	TCP / UDP	Protocole / service	À quoi ça sert ?	Comment ça fonctionne ?	Exemple concret	À retenir
123	UDP	**NTP**	Synchronisation de l'heure des machines.	Le client interroge un serveur NTP pour régler automatiquement son horloge système.	Un PC, un serveur ou un routeur synchronise son heure.	**NTP = heure, UDP 123**
143	TCP	**IMAP**	Consultation et synchronisation des e-mails.	Les e-mails restent sur le serveur et se synchronisent entre plusieurs appareils.	Lire ses mails sur téléphone et ordinateur avec les mêmes dossiers.	**IMAP = mails synchronisés**
161	UDP	**SNMP**	Supervision des équipements réseau.	Un outil de supervision interroge les équipements pour récupérer leur état, interfaces ou compteurs.	Surveiller un switch, un routeur, une imprimante ou un serveur.	**SNMP = supervision, UDP 161**
389	TCP	**LDAP**	Interrogation d'un annuaire.	Un client interroge un serveur d'annuaire pour rechercher utilisateurs, groupes ou objets.	Active Directory utilise LDAP pour consulter l'annuaire.	**LDAP = annuaire, TCP 389**
443	TCP surtout / UDP avec QUIC	**HTTPS**	Accès à un site web sécurisé et chiffré.	HTTPS utilise généralement TCP avec TLS ; avec HTTP/3, il peut utiliser UDP via QUIC.	Accès à un site en https://	**HTTPS = web sécurisé**
500	UDP	**ISAKMP / IKE**	Négociation des paramètres d'un VPN IPsec.	ISAKMP/IKE établit une association de sécurité avant le chiffrement IPsec.	Mise en place d'un VPN site-à-site entre deux pare-feux.	**ISAKMP/IKE = IPsec, UDP 500**
995	TCP	**POP3S**	Récupération sécurisée des e-mails.	POP3S est la version chiffrée de POP3 avec TLS/SSL.	Un client mail récupère les messages d'une boîte en connexion sécurisée.	**POP3S = POP3 sécurisé**
1194	UDP surtout / TCP possible	**OpenVPN**	Création d'un accès VPN sécurisé.	Le client OpenVPN contacte le serveur et crée un tunnel chiffré ; UDP est fréquent pour la performance.	Connexion sécurisée à un réseau d'entreprise.	**1194 = OpenVPN**

Pour bien comprendre

Repères utiles

DNS utilise surtout UDP 53, mais TCP 53 existe aussi.
DHCP : serveur 67, client 68.
HTTPS : TCP 443 en classique, UDP 443 avec HTTP/3 et QUIC.

Mémo des pièges

SMTP = mail, TCP 25.
SNMP = supervision, UDP 161.
TFTP = transfert simple, UDP 69, sans authentification.

Lien avec la couche 7

Les ports sont en couche 4, mais les services comme DNS, HTTP, SSH ou LDAP se comprennent aussi comme services de couche 7.

Ports réseau essentiels - suite et fin

Ports logiques utilisés par les protocoles et services réseau

Port	TCP / UDP	Protocole / service	À quoi ça sert ?	Comment ça fonctionne ?	Exemple concret	À retenir
1433	TCP	**Microsoft SQL Server**	Connexion à une base de données SQL Server.	Une application ou un client SQL envoie des requêtes au moteur SQL Server. À filtrer par pare-feu.	Connexion d'une application métier à une base SQL Server.	**1433 = SQL Server**
1512	TCP / UDP	**WINS**	Résolution de noms NetBIOS en adresse IP.	Ancien service Windows qui associe un nom NetBIOS à une IP. Largement remplacé par DNS.	Ancien réseau Windows.	**WINS = ancien NetBIOS → IP**
1701	UDP	**L2TP**	Création d'un tunnel VPN L2TP.	L2TP transporte le tunnel. Il est souvent associé à IPsec car L2TP seul ne chiffre pas tout.	Connexion VPN L2TP/IPsec.	**1701 = L2TP**
3074	TCP / UDP	**Xbox Live / jeux**	Certains services de jeux en ligne.	Utilisé pour les services Xbox, matchmaking, parties en ligne et certains échanges liés au NAT.	Jeu en ligne sur console.	**3074 = Xbox / jeux**
3260	TCP	**iSCSI**	Accès à du stockage via le réseau.	Transporte des commandes SCSI sur IP ; un stockage distant apparaît comme un disque local.	Connexion à une baie de stockage iSCSI.	**3260 = stockage iSCSI**
3306	TCP	**MySQL / MariaDB**	Connexion à une base de données MySQL.	Une application envoie des requêtes SQL au serveur MySQL/MariaDB. À éviter d'exposer directement sur Internet.	Site web relié à une base MySQL.	**3306 = MySQL**
3389	TCP / UDP	**RDP**	Accès Bureau à distance Windows.	Permet une session graphique distante. TCP est classique ; UDP peut améliorer la fluidité. Port sensible à sécuriser.	Prendre la main sur un poste Windows à distance.	**3389 = Bureau à distance**
8080	TCP	**HTTP alternatif / proxy**	Accès à un service web alternatif.	Utilisé quand le port 80 n'est pas utilisé, pour un proxy, une application web ou une interface de test.	Interface web d'une application sur le port 8080.	**8080 = HTTP alternatif**
8443	TCP	**HTTPS alternatif**	Accès à un service web sécurisé alternatif.	Comme HTTPS avec TLS, mais sur un port alternatif, souvent pour interfaces admin ou applications web.	Interface d'administration sécurisée en 8443.	**8443 = HTTPS alternatif**

Pour bien comprendre

Ports sensibles

Bases de données, RDP, iSCSI, VPN et interfaces web d'administration doivent être filtrés strictement.

Pare-feu

Ouvert : un service écoute sur ce port.
Filtrer : autoriser uniquement les IP nécessaires.
Exposer : rendre accessible depuis un autre réseau ou Internet.

Mémo sécurité

Éviter d'exposer directement sur Internet : 1433, 3306, 3260, 3389.
Pour RDP ou bases de données : privilégier VPN, filtrage IP et MFA si possible.

IP = quelle machine ? • Port = quel service ? • Pare-feu = qui a le droit d'entrer ?