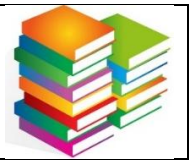


Les principaux protocole réseau



Un protocole réseau est un ensemble de règles permettant aux équipements de communiquer. Plusieurs protocoles travaillent ensemble pour transporter une même information.

Par exemple, pour consulter un site web, un ordinateur peut utiliser DNS pour trouver son adresse IP, TCP pour établir une communication fiable et HTTPS pour échanger avec le site de manière chiffrée.

Identifier et joindre les équipements

Protocole	Rôle principal	Exemple
Ethernet	Transporte les trames sur un réseau local, en utilisant des adresses MAC	Un poste communique avec un serveur à travers un commutateur.
ARP	Retrouve l'adresse MAC correspondant à une adresse IPv4 sur le réseau local	« Qui possède l'adresse 192.168.10.10 ? »
IP	Adresse les paquets et permet leur acheminement entre réseaux	Un paquet ping utilise des requêtes et des réponses ICMP.
ICMP	Transporte des messages de diagnostic et d'erreur réseau	La commande ping utilise des requêtes et des réponses ICMP

A retenir : une adresse MAC sert à la livraison sur le lien local, une adresse IP sert à identifier une interface et à acheminer les paquets entre réseaux.

Pour joindre un équipement situé sur un autre réseau, un poste recherche généralement l'adresse MAC de sa passerelle et non celle du destinataire distant.

Transporter les données

Protocole	Fonctionnement	Usages courants
TCP	Etablit une connexion, remet les données dans l'ordre et restransmet les données perdues	http/1.1, http/2, SSH, mesagerie
UDP	Envoie des datagrammes sans établissement préalable de connexion ni garantie intégrée de livraison ou d'ordre	DNS, DHCP, certains flux audio et vidéo

Pour reconnaître une connexion TCP, l'ouverture de la connexion compte trois étapes :

1. SYN : le client demande une connexion
2. SYN,ACK : Le serveur accepte et répond
3. ACK : Le client confirme

Autres indicateurs :

- ⇨ FIN : demande de fermeture normale de la connexion
- ⇨ RST : interruption ou refus de la connexion
- ⇨ Retransmission : nouvel envoi de données pouvant résulter d'une perte réseau

Attention : Une connexion TCP réussie ne signifie pas que l'utilisateur a réussi à s'authentifier. Le serveur peut accepter la connexion puis refuser les identifiants.

A. BÉGER

Fournir les services réseau

Les ports ci-dessous sont les ports habituels d'un serveur. Le client utilise généralement un port temporaire. Un service peut être configuré sur un autre port.

Protocole	A quoi sert-il ?	Port(s) habituel(s)
DNS	Associe un nom de domaine à une adresse IP	UDP ou TCP 53
DHCP	Attribue automatiquement une configuration IPv4 (adresse, masque, passerelle, DNS)	UDP 67
HTTP	Echange des pages web, fichiers et données sans chiffrement intégré	TCP 80
HTTPS	Protège les échanges HTTP par chiffrement et authentification du serveur	443 TCP UDP pour HTTP/3
SSH	Permet l'administration distante sécurisée d'un équipement	TCP 22
FTP	Transfère des fichiers, sans chiffrement dans sa forme classique	TCP 21
SMTP	Transporte et soumet les courriels	TCP 25
IMAP	Permet de consulter et synchroniser une boîte de messagerie	TCP 143 (993 avec TLS implicite)

A retenir :

- ⇨ DNS cherche une adresse, DHCP fournit une configuration réseau
- ⇨ HTTPS protège la communication, mais ne garantit pas que le site est honnête
- ⇨ SFTP utilisé pour transférer des fichiers via SSH (différent de FTP !)

Lire un échange HTTP

Une requête est envoyée par le client. Une réponse est renvoyée par le serveur.

Les méthodes courantes :

Méthode	Signification habituelle	Exemple
GET	Demander une ressource	Consulter /actualites ou télécharger /exports/clients.csv
POST	Envoyer des données à traiter	Envoyer un formulaire de connexion vers /login

La méthode POST ne chiffre pas les données : avec HTTP en clair, leur contenu peut être lisible dans une capture.

Les codes de réponses utiles :

Code	Signification	Interprétation
`200 OK`	La requête a été traité avec succès	Vérifier le contenu pour savoir ce qui a réellement réussi
`301/302`	Redirection	Le serveur renvoie vers une autre adresse
`401 Unauthorized`	Autorisation invalide	Les identifiants peuvent être absents, invalides ou expirés
`403 Forbidden`	Accès refusé	Le serveur refuse l'accès à la ressource
`404 Not Found`	Ressource introuvable	L'adresse demandée n'a pas été trouvée
`500 Internal Server Error`	Erreur interne du serveur	Le traitement a rencontré un problème côté serveur

Un cookie de session peut permettre au serveur de reconnaître un utilisateur entre plusieurs requêtes. Dans Wireshark, `Set-Cookie` apparaît dans une réponse et `Cookie` dans les requêtes suivantes.

Repérer une activité inhabituelle

Un indice doit être interprété dans son contexte.

Observation	Hypothèse à examiner
Nombreux essais de connexion rapprochés	Recherche automatisée d'identifiants ou application mal configurée
Refus répétés, puis authentification réussie	Accès potentiellement obtenu après plusieurs essais
Téléchargement important après connexion	Export légitime ou récupération inhabituelle de données
Connexions vers de nombreux ports	Inventaire tehcnique ou recherche de services accéssibles
Nombreuses retransmissions TCP	Pertes réseau, congestion ou problème de capture, pas forcément une attaque

Méthode d'analyse : identifier la source et la destination, observer le protocole, reconstituer la chronologie et citer les trames qui justifient la conclusion.

Une capture montre des communications. Elle ne permet pas à elle seule, d'identifier la personne derrière un poste ni de prouver son intention.