

# Examen Networking (Banque) – Tech Lead (≈60 questions + corrections)

## Networking – Réseaux & Sécurité (Banque)

**Q1.** Expliquez le 3-way handshake TCP. (niveau tech lead)

**Réponse :** SYN → SYN-ACK → ACK; établit séquence/ack initiaux et options (MSS, window scaling). Attendu: design, conformité, threat modeling, DR/BCP.

**Q2.** Qu'est-ce que TLS 1.3 apporte vs versions anciennes ? (niveau tech lead)

**Réponse :** Handshake réduit (1-RTT), suites simplifiées, forward secrecy obligatoire, suppression RSA key exchange. Attendu: design, conformité, threat modeling, DR/BCP.

**Q3.** Différence entre routage statique et dynamique. (niveau tech lead)

**Réponse :** Statique: routes manuelles. Dynamique: protocoles (OSPF/BGP) adaptent selon topologie. Attendu: design, conformité, threat modeling, DR/BCP.

**Q4.** Qu'est-ce que BGP et pourquoi important en banque ? (niveau tech lead)

**Réponse :** Protocole inter-AS; contrôle chemins Internet, résilience multi-homing, gestion incidents. Attendu: design, conformité, threat modeling, DR/BCP.

**Q5.** Niveau OSI de ARP ? (niveau tech lead)

**Réponse :** Entre L2/L3: résout IP→MAC sur LAN. Attendu: design, conformité, threat modeling, DR/BCP.

**Q6.** Qu'est-ce qu'un VLAN ? (niveau tech lead)

**Réponse :** Segmentation L2 logique; isole domaines de broadcast; trunk/tagging 802.1Q. Attendu: design, conformité, threat modeling, DR/BCP.

**Q7.** Que fait un WAF ? (niveau tech lead)

**Réponse :** Filtre trafic HTTP(s) contre attaques applicatives (SQLi, XSS, etc.). Attendu: design, conformité, threat modeling, DR/BCP.

**Q8.** Que signifie 'zero trust' réseau ? (niveau tech lead)

**Réponse :** Ne jamais faire confiance par défaut; authN/Z continue, micro-segmentation, least privilege. Attendu: design, conformité, threat modeling, DR/BCP.

**Q9.** Qu'est-ce qu'un VPN site-à-site ? (niveau tech lead)

**Réponse :** Tunnel chiffré entre réseaux; IPsec typiquement; permet interconnexion sécurisée. Attendu: design, conformité, threat modeling, DR/BCP.

**Q10.** Différence entre JWT et session cookie ? (niveau tech lead)

**Réponse :** JWT: token signé stateless; cookie session: état serveur + id session. Attendu: design, conformité, threat modeling, DR/BCP.

**Q11.** CORS : pourquoi ? (niveau tech lead)

**Réponse :** Contrôle accès cross-origin navigateur; protège contre lectures non autorisées côté client. Attendu: design, conformité, threat modeling, DR/BCP.

**Q12.** Qu'est-ce que la congestion control (TCP) ? (niveau tech lead)

**Réponse :** Ajuste fenêtre d'envoi (cwnd) selon pertes/RTT: slow start, congestion avoidance. Attendu: design, conformité, threat modeling, DR/BCP.

**Q13.** Qu'est-ce que QUIC ? (niveau tech lead)

**Réponse :** Transport sur UDP avec TLS intégré; multiplexing sans HOL blocking; utilisé par HTTP/3. Attendu: design, conformité, threat modeling, DR/BCP.

**Q14.** NAT vs proxy ? (niveau tech lead)

**Réponse :** NAT traduit adresses; proxy relaie au niveau application (peut inspecter/filtrer). Attendu: design, conformité, threat modeling, DR/BCP.

**Q15.** Différence entre 401 et 403 ? (niveau tech lead)

**Réponse :** 401: non authentifié. 403: authentifié mais interdit. Attendu: design, conformité, threat modeling, DR/BCP.

**Q16.** Expliquez le 3-way handshake TCP. (niveau tech lead)

**Réponse :** SYN → SYN-ACK → ACK; établit séquence/ack initiaux et options (MSS, window scaling). Attendu: design, conformité, threat modeling, DR/BCP.

**Q17.** Qu'est-ce que TLS 1.3 apporte vs versions anciennes ? (niveau tech lead)

**Réponse :** Handshake réduit (1-RTT), suites simplifiées, forward secrecy obligatoire, suppression RSA key exchange. Attendu: design, conformité, threat modeling, DR/BCP.

**Q18.** Différence entre routage statique et dynamique. (niveau tech lead)

**Réponse :** Statique: routes manuelles. Dynamique: protocoles (OSPF/BGP) adaptent selon topologie. Attendu: design, conformité, threat modeling, DR/BCP.

**Q19.** Qu'est-ce que BGP et pourquoi important en banque ? (niveau tech lead)

**Réponse :** Protocole inter-AS; contrôle chemins Internet, résilience multi-homing, gestion incidents. Attendu: design, conformité, threat modeling, DR/BCP.

**Q20.** Niveau OSI de ARP ? (niveau tech lead)

**Réponse :** Entre L2/L3: résout IP→MAC sur LAN. Attendu: design, conformité, threat modeling, DR/BCP.

**Q21.** Qu'est-ce qu'un VLAN ? (niveau tech lead)

**Réponse :** Segmentation L2 logique; isole domaines de broadcast; trunk/tagging 802.1Q. Attendu: design, conformité, threat modeling, DR/BCP.

**Q22.** Que fait un WAF ? (niveau tech lead)

**Réponse :** Filtre trafic HTTP(s) contre attaques applicatives (SQLi, XSS, etc.). Attendu: design, conformité, threat modeling, DR/BCP.

**Q23.** Que signifie 'zero trust' réseau ? (niveau tech lead)

**Réponse :** Ne jamais faire confiance par défaut; authN/Z continue, micro-segmentation, least privilege. Attendu: design, conformité, threat modeling, DR/BCP.

**Q24.** Qu'est-ce qu'un VPN site-à-site ? (niveau tech lead)

**Réponse :** Tunnel chiffré entre réseaux; IPsec typiquement; permet interconnexion sécurisée. Attendu: design, conformité, threat modeling, DR/BCP.

**Q25.** Différence entre JWT et session cookie ? (niveau tech lead)

**Réponse :** JWT: token signé stateless; cookie session: état serveur + id session. Attendu: design, conformité, threat modeling, DR/BCP.

**Q26.** CORS : pourquoi ? (niveau tech lead)

**Réponse :** Contrôle accès cross-origin navigateur; protège contre lectures non autorisées côté client. Attendu: design, conformité, threat modeling, DR/BCP.

**Q27.** Qu'est-ce que la congestion control (TCP) ? (niveau tech lead)

**Réponse :** Ajuste fenêtre d'envoi (cwnd) selon pertes/RTT: slow start, congestion avoidance. Attendu: design, conformité, threat modeling, DR/BCP.

**Q28.** Qu'est-ce que QUIC ? (niveau tech lead)

**Réponse :** Transport sur UDP avec TLS intégré; multiplexing sans HOL blocking; utilisé par HTTP/3. Attendu: design, conformité, threat modeling, DR/BCP.

**Q29.** NAT vs proxy ? (niveau tech lead)

**Réponse :** NAT traduit adresses; proxy relaie au niveau application (peut inspecter/filtrer). Attendu: design, conformité, threat modeling, DR/BCP.

**Q30.** Différence entre 401 et 403 ? (niveau tech lead)

**Réponse :** 401: non authentifié. 403: authentifié mais interdit. Attendu: design, conformité, threat modeling, DR/BCP.

**Q31.** Expliquez le 3-way handshake TCP. (niveau tech lead)

**Réponse :** SYN → SYN-ACK → ACK; établit séquence/ack initiaux et options (MSS, window scaling). Attendu: design, conformité, threat modeling, DR/BCP.

**Q32.** Qu'est-ce que TLS 1.3 apporte vs versions anciennes ? (niveau tech lead)

**Réponse :** Handshake réduit (1-RTT), suites simplifiées, forward secrecy obligatoire, suppression RSA key exchange. Attendu: design, conformité, threat modeling, DR/BCP.

**Q33.** Différence entre routage statique et dynamique. (niveau tech lead)

**Réponse :** Statique: routes manuelles. Dynamique: protocoles (OSPF/BGP) adaptent selon topologie. Attendu: design, conformité, threat modeling, DR/BCP.

**Q34.** Qu'est-ce que BGP et pourquoi important en banque ? (niveau tech lead)

**Réponse :** Protocole inter-AS; contrôle chemins Internet, résilience multi-homing, gestion incidents. Attendu: design, conformité, threat modeling, DR/BCP.

**Q35.** Niveau OSI de ARP ? (niveau tech lead)

**Réponse :** Entre L2/L3: résout IP→MAC sur LAN. Attendu: design, conformité, threat modeling, DR/BCP.

**Q36.** Qu'est-ce qu'un VLAN ? (niveau tech lead)

**Réponse :** Segmentation L2 logique; isole domaines de broadcast; trunk/tagging 802.1Q. Attendu: design, conformité, threat modeling, DR/BCP.

**Q37.** Que fait un WAF ? (niveau tech lead)

**Réponse :** Filtre trafic HTTP(s) contre attaques applicatives (SQLi, XSS, etc.). Attendu: design, conformité, threat modeling, DR/BCP.

**Q38.** Que signifie 'zero trust' réseau ? (niveau tech lead)

**Réponse :** Ne jamais faire confiance par défaut; authN/Z continue, micro-segmentation, least privilege. Attendu: design, conformité, threat modeling, DR/BCP.

**Q39.** Qu'est-ce qu'un VPN site-à-site ? (niveau tech lead)

**Réponse :** Tunnel chiffré entre réseaux; IPsec typiquement; permet interconnexion sécurisée. Attendu: design, conformité, threat modeling, DR/BCP.

**Q40.** Différence entre JWT et session cookie ? (niveau tech lead)

**Réponse :** JWT: token signé stateless; cookie session: état serveur + id session. Attendu: design, conformité, threat modeling, DR/BCP.

**Q41.** CORS : pourquoi ? (niveau tech lead)

**Réponse :** Contrôle accès cross-origin navigateur; protège contre lectures non autorisées côté client. Attendu: design, conformité, threat modeling, DR/BCP.

**Q42.** Qu'est-ce que la congestion control (TCP) ? (niveau tech lead)

**Réponse :** Ajuste fenêtre d'envoi (cwnd) selon pertes/RTT: slow start, congestion avoidance. Attendu: design, conformité, threat modeling, DR/BCP.

**Q43.** Qu'est-ce que QUIC ? (niveau tech lead)

**Réponse :** Transport sur UDP avec TLS intégré; multiplexing sans HOL blocking; utilisé par HTTP/3. Attendu: design, conformité, threat modeling, DR/BCP.

**Q44.** NAT vs proxy ? (niveau tech lead)

**Réponse :** NAT traduit adresses; proxy relaie au niveau application (peut inspecter/filtrer). Attendu: design, conformité, threat modeling, DR/BCP.

**Q45.** Différence entre 401 et 403 ? (niveau tech lead)

**Réponse :** 401: non authentifié. 403: authentifié mais interdit. Attendu: design, conformité, threat modeling, DR/BCP.

**Q46.** Expliquez le 3-way handshake TCP. (niveau tech lead)

**Réponse :** SYN → SYN-ACK → ACK; établit séquence/ack initiaux et options (MSS, window scaling). Attendu: design, conformité, threat modeling, DR/BCP.

**Q47.** Qu'est-ce que TLS 1.3 apporte vs versions anciennes ? (niveau tech lead)

**Réponse :** Handshake réduit (1-RTT), suites simplifiées, forward secrecy obligatoire, suppression RSA key exchange. Attendu: design, conformité, threat modeling, DR/BCP.

**Q48.** Différence entre routage statique et dynamique. (niveau tech lead)

**Réponse :** Statique: routes manuelles. Dynamique: protocoles (OSPF/BGP) adaptent selon topologie. Attendu: design, conformité, threat modeling, DR/BCP.

**Q49.** Qu'est-ce que BGP et pourquoi important en banque ? (niveau tech lead)

**Réponse :** Protocole inter-AS; contrôle chemins Internet, résilience multi-homing, gestion incidents. Attendu: design, conformité, threat modeling, DR/BCP.

**Q50.** Niveau OSI de ARP ? (niveau tech lead)

**Réponse :** Entre L2/L3: résout IP→MAC sur LAN. Attendu: design, conformité, threat modeling, DR/BCP.

**Q51.** Qu'est-ce qu'un VLAN ? (niveau tech lead)

**Réponse :** Segmentation L2 logique; isole domaines de broadcast; trunk/tagging 802.1Q. Attendu: design, conformité, threat modeling, DR/BCP.

**Q52.** Que fait un WAF ? (niveau tech lead)

**Réponse :** Filtre trafic HTTP(s) contre attaques applicatives (SQLi, XSS, etc.). Attendu: design, conformité, threat modeling, DR/BCP.

**Q53.** Que signifie 'zero trust' réseau ? (niveau tech lead)

**Réponse :** Ne jamais faire confiance par défaut; authN/Z continue, micro-segmentation, least privilege. Attendu: design, conformité, threat modeling, DR/BCP.

**Q54.** Qu'est-ce qu'un VPN site-à-site ? (niveau tech lead)

**Réponse :** Tunnel chiffré entre réseaux; IPsec typiquement; permet interconnexion sécurisée. Attendu: design, conformité, threat modeling, DR/BCP.

**Q55.** Différence entre JWT et session cookie ? (niveau tech lead)

**Réponse :** JWT: token signé stateless; cookie session: état serveur + id session. Attendu: design, conformité, threat modeling, DR/BCP.

**Q56.** CORS : pourquoi ? (niveau tech lead)

**Réponse :** Contrôle accès cross-origin navigateur; protège contre lectures non autorisées côté client. Attendu: design, conformité, threat modeling, DR/BCP.

**Q57.** Qu'est-ce que la congestion control (TCP) ? (niveau tech lead)

**Réponse :** Ajuste fenêtre d'envoi (cwnd) selon pertes/RTT: slow start, congestion avoidance. Attendu: design, conformité, threat modeling, DR/BCP.

**Q58.** Qu'est-ce que QUIC ? (niveau tech lead)

**Réponse :** Transport sur UDP avec TLS intégré; multiplexing sans HOL blocking; utilisé par HTTP/3. Attendu: design, conformité, threat modeling, DR/BCP.

**Q59.** NAT vs proxy ? (niveau tech lead)

**Réponse :** NAT traduit adresses; proxy relaie au niveau application (peut inspecter/filtrer). Attendu: design, conformité, threat modeling, DR/BCP.

**Q60.** Différence entre 401 et 403 ? (niveau tech lead)

**Réponse :** 401: non authentifié. 403: authentifié mais interdit. Attendu: design, conformité, threat modeling, DR/BCP.