1. K čemu slouží RIP protokol ve směrování, jak přibližně funguje?

RIP (Routing Information Protocol) je protokol ve směrování, který slouží k výměně směrovacích informací mezi směrovači v sítích s interním směrováním. RIP se používá k aktualizaci směrovacích tabulek směrovačů a k určení nejlepších cest pro směrování datových paketů. Funguje na základě periodické výměny aktualizačních zpráv, které obsahují informace o dostupných sítích a vzdálenostech k nim. RIP používá metriku hop count, což znamená, že se snaží minimalizovat počet směrovačů (hopů) na cestě k cílové síti.

2. Co je statické a adaptivní směrování, jaký je mezi nimi rozdíl?

Statické směrování je metoda, při které jsou směrovací záznamy ručně konfigurovány na směrovači a nezmění se automaticky. Směrovač používá tyto statické záznamy pro směrování datových paketů. Naopak adaptivní směrování je metoda, při které směrovače vyměňují si informace o sítích a provádějí automatický výpočet nejlepších cest na základě aktuální topologie sítě. Adaptivní směrovací protokoly, jako například RIP, OSPF nebo EIGRP, se používají pro dynamické aktualizace směrovacích tabulek.

3. Jaké má vlastnosti protokol TCP?

Protokol TCP (Transmission Control Protocol) je spojově orientovaný protokol transportní vrstvy. Jeho hlavní vlastnosti zahrnují spolehlivý přenos dat s potvrzováním, řízení toku dat, řízení spojení a mechanismus přesouvání paketů (retransmise) v případě ztráty nebo poškození dat.

4. Jaké má vlastnosti protokol UDP?

Protokol UDP (User Datagram Protocol) je nespojový protokol transportní vrstvy. Jeho hlavní vlastností je rychlý a jednoduchý přenos dat bez potvrzování doručení, řízení toku dat nebo mechanismů spolehlivosti. UDP je často používán pro aplikace, které vyžadují nízkou latenci a jsou méně citlivé na ztrátu dat, například hlasová nebo video komunikace.

5. Co je to u transportní vrstvy port, které porty znáte?

V transportní vrstvě se porty používají k identifikaci konkrétních aplikací nebo služeb, které komunikují na síti. Porty jsou číselné identifikátory, které jsou součástí transportních protokolů, jako je TCP a UDP. Příklady portů zahrnují HTTP (port 80), FTP (port 21), SSH (port 22), DNS (port 53) atd.

6. Definujte streamovaný přenos.

Streamovaný přenos (streaming) je forma přenosu dat, při které jsou data přenášena kontinuálně a přehrávána postupně, jakmile je dostupná určitá část dat. To umožňuje uživatelům přehrávat audio nebo video obsah bez nutnosti stahování celého souboru.

7. Definujte datagramový přenos.

Datagramový přenos je forma přenosu dat, při které jsou data rozdělena do menších bloků zvaných datagramy a přenášena samostatně. Každý datagram obsahuje potřebné informace pro doručení, jako je zdrojová a cílová adresa.

8. Popičte protokol TCP.

Protokol TCP je spojově orientovaný protokol, který poskytuje spolehlivý přenos dat. Používá potvrzování doručení, řízení toku dat, řízení spojení a mechanismus přesouvání paketů (retransmise) v případě ztráty nebo poškození dat. TCP je založen na spojení mezi dvěma koncovými body (počítači) a poskytuje spolehlivý přenos datových proudů bez ztráty, duplikace nebo přeházení paketů.

9. Popište protokol UDP.

Protokol UDP je nespojový protokol, který umožňuje jednoduchý přenos dat bez zajištění spolehlivosti. Neposkytuje žádné mechanismy pro potvrzování doručení, řízení toku dat ani přesouvání paketů. UDP je často používán pro rychlý přenos dat, jako jsou multimediální streamy nebo herní aplikace, které vyžadují nízkou latenci.

10. Popište hlavičku protokolu TCP.

Hlavička protokolu TCP obsahuje zdrojový a cílový port, číslo sekvence, číslo potvrzení, délku datového pole, příznaky (např. SYN, ACK, FIN), okno (window) pro řízení toku dat, kontrolní součet a nouzový pointer (urgent pointer). Tato informace se používá pro správné směrování a doručení dat.

11. Popište hlavičku protokolu UDP.

Hlavička protokolu UDP obsahuje zdrojový a cílový port, délku datového pole a kontrolní součet. UDP hlavička je jednoduchá a obsahuje minimální informace potřebné pro správné směrování dat.

12. Popište, jak vzniká spojovaný přenos.

Spojovaný přenos v TCP probíhá pomocí třícestného stisknutí ruky (three-way handshake). První počítač (klient) pošle SYN paket s počátečním číslem sekvence na druhý počítač (server). Server odpoví SYN-ACK paketem s číslem potvrzení a číslem sekvence. Klient nakonec odpoví ACK paketem s potvrzením přijetí čísla sekvence. Tím je navázáno spojení mezi klientem a serverem a mohou být přenášena data.

14. Co to je a co všechno zahrnuje v UDP datagramu kontrolní součet?

V UDP datagramech je obsažen kontrolní součet (checksum), který slouží k detekci chyb v přenášených datech. Kontrolní součet je vypočítán z datagramu a kontrolního pole. Při příjmu datagramu je kontrolní součet opětovně vypočítán a porovnán s přijatým kontrolním polem. Pokud se kontrolní součty neshodují, znamená to, že došlo k chybě v datovém přenosu.

15. Jak se zabezpečuje u TCP spolehlivost?

Spolehlivost u protokolu TCP je zajištěna pomocí potvrzování doručení. Při přenosu datových paketů mezi počítači je každý přijatý paket potvrzen (ACK) přijímacím počítačem. Pokud odesílatel neobdrží potvrzení doručení paketu v určitém časovém intervalu, předpokládá se, že došlo k ztrátě paketu a je znovu odeslán. Tím je zajištěna spolehlivost a doručení dat v pořadí.

16. Co má společného TCP a UDP hlavička?

Hlavička protokolu TCP obsahuje zdrojový a cílový port, číslo sekvence, číslo potvrzení, délku datového pole, příznaky (např. SYN, ACK, FIN), okno (window) pro řízení toku dat, kontrolní součet a nouzový pointer (urgent pointer). Tato informace se používá pro správné směrování a doručení dat.

17. Hlavička protokolu UDP obsahuje zdrojový a cílový port, délku datového pole a kontrolní součet. UDP hlavička je jednoduchá a obsahuje minimální informace potřebné pro správné směrování dat.

18. Jak probíhá u TCP navazování spojení?

U TCP (Transmission Control Protocol) probíhá navazování spojení pomocí tzv. Three-Way Handshake, což je třífázový proces mezi klientem a serverem. Tento proces slouží k synchronizaci komunikace a navázání spolehlivého spojení mezi oběma stranami.

Klient pošle serveru paket s nastaveným příznakem SYN (synchronizace) a náhodným číslem sekvence. Tímto paketem klient žádá server o navázání spojení.

Server odpovídá klientovi paketem s nastavenými příznaky SYN a ACK (potvrzení) a náhodným číslem sekvence a potvrzení. Tímto paketem server potvrzuje přijetí žádosti o navázání spojení a zároveň žádá klienta o potvrzení.

Klient odpovídá serveru paketem s nastaveným příznakem ACK a potvrzením. Tímto paketem klient potvrzuje přijetí odpovědi serveru.

Po dokončení tohoto Three-Way Handshake je spojení mezi klientem a serverem navázáno. Klient i server si vytvoří informace o spojení, jako jsou čísla sekvencí a potvrzení, které jsou důležité pro správný přenos dat. Spojení je nyní připraveno na přenos dat.

Navazování spojení TCP zajišťuje spolehlivost a řízení toku dat mezi klientem a serverem. Three-Way Handshake umožňuje oběma stranám komunikace synchronizovat se a ustanovit společné parametry pro přenos dat, což je klíčové pro správnou a spolehlivou komunikaci přes TCP protokol.

19. Jak funguje záplavové směrování?

Klient pošle serveru paket s nastaveným příznakem SYN (synchronizace) a náhodným číslem sekvence. Tímto paketem klient žádá server o navázání spojení.

20. Jak funguje metoda zpětného učení (jako varianta směrování)?

Server odpovídá klientovi paketem s nastavenými příznaky SYN a ACK (potvrzení) a náhodným číslem sekvence a potvrzení. Tímto paketem server potvrzuje přijetí žádosti o navázání spojení a žádá klienta o potvrzení.

21. Jak funguje source routing (jako varianta směrování)?

Klient odpovídá serveru paketem s nastaveným příznakem ACK a potvrzením. Tímto paketem klient potvrzuje přijetí odpovědi serveru.