

**Vizsgakérdések az Infokommunikációs szolgáltatások és alkalmazások című tárgyhoz
(2010/2011 tavaszi félév)**

1. NGN hálózati koncepció, NGN ALL-IP architektúra, NGN átmenet, az IMS szerepe. Konvergencia folyamatok, FMS, FMC, IMS alkalmazások.
 2. IMS architektúra, az egyes elemek szerepe. Az UMTS architektúra fejlődése, az IMS megjelenése.
 3. Kapcsolatvezérlési protokollok, soroljon fel néhány protokollt. Ismertesse a H.323 protokollt, hasonlítsa össze a SIP protokollal. A SIP architektúra elemei, SIP azonosítás
 4. SIP protokollüzenetek. Az üzenet részei, kérés-válasz modell, a legfontosabb SIP kérések és válaszok. A legfontosabb fejléc mezők (pl. record-route). Az SDP.
 5. IMS regisztráció és hívásfelépítés (folyamatábra alapján), IETF és 3GPP SIP koncepció összehasonlítása.
 6. QoS biztosítási lehetőségek az IMS-ben. Intserv és Diffserv modell, PDP.
 7. Hitelesítés, Engedélyezés, Számlázás (AAA) az IMS-ben, a Diameter protokoll, a felhasználói profil.
 8. IMS számlázás. A számlázás fajtái, a számlázás feladatai. Miben különbözik az Immediate Event Charging és Event Charging with Unit Reservation.
 9. IMS szolgáltatások: a presence szolgáltatás (általános bemutatás, elemei, példák). Milyen további IMS alkalmazásokat ismer? Milyen előnyökkel jár egy alkalmazásfejlesztési platform alkalmazása?
 10. Transzport protokollok. A szállítási réteg feladatai, alkalmazások típusai, vezeték nélküli és mobil hálózatok jellemzői. Hasonlítsa össze a TCP, DCCP és SCTP protokollok tulajdonságait.
 11. Transzport protokollok. Mi a multihoming, illetve a multistreaming? Mi a torlódásszabályozás? Mi a forgalomszabályozás? Különböző alkalmazástípusokhoz, milyen transzport protokollt javasolt választani? Ismertesse az UDP, RTp/RTCP protokollokat.
 12. Web Privacy. Hogyan fejlődtek a nyomkövetéses támadások legalapvetőbb technikái? Sorolja fel ezeket a technológiákat, és röviden írja le, hogyan működnek! Mi az alapelve a History Stealing támadásnak? Mutassa meg, hogy ha a cél a felhasználó profiljának beazonosítása, akkor hogyan hajtaná végre!
- Milyen anonimizáló szolgáltatás típusokat ismer? Mutasson meg ezek között kapcsolatot, és mindegyiket írja le a jellemzőivel!

13. Közösségi hálók. Sorolja fel, milyen főbb szereplők érintettek a közösségi hálók privátszférát érintő kérdéseiben, és hogy ezek a szereplők milyen motivációval és lehetőségekkel bírnak! Milyen támadás típusokat ismer, amit harmadik felek hajthatnak végre? Hasonlítsa is össze a leírt típusokat!

Írja le egy ismert félig-aktív támadás típus működési elvét! Mi a hátránya ennek a módszernek, és a gyakorlatban miért nehezen alkalmazható?

14. Ismertesse az IPv4 és az IPv6 fejléc-struktúráinak különbségeit! Mutassa be az IPv4 legfontosabb hátrányait, hiányosságait! Hogyan kezeli az IPv6 az Internet felhasználóinak egyre növekvő számát? Mire szolgál az IPv6-ban a Destination Option kiegészítő fejléc?

15. Milyen IPv6-os címtípusokat ismer? Mi váltja az IPv6-ban az IPv4-es ARP és RARP funkciókat? Hogyan működik az IPv6-os állapotmentes (stateless) autokonfiguráció? Mi az a Path MTU discovery és hogyan működik az IPv6-ban?

16. Hogyan csoportosíthatók az IPv4-IPv6 együttélést megvalósító módszerek? Mit nevezünk anycast kommunikációnak, és hogyan támogatja az IPv6 ezt a kommunikáció típust? Hogyan működik a broadcast átvitel IPv6-ban? Milyen ICMPv6 üzeneteket ismer?

17. Mit mondott Bruce Schneier a biztonságról? Milyen lépésekre lehet bontani a körforgást? Miért támadnak a támadók? Definiálja a következőket: Sértetlenség, Hitelesség, Letagadhatatlanság. Definiálja a következőket: Bizalmasság, Távoli azonosítás.

18. Milyen két nagy csoportra osztjuk a támadásokat? Jellemezze ezeket. Milyen passzív támadástípusokat ismer? Mi jellemzi a passzív támadásokat? Milyen aktív támadástípusokat ismer? Mi jellemzi az aktív támadásokat? Mi az a DoS támadás? Ismertessen két DoS típusú támadást! Mi az a Social Engineering?