Tentafrågor Effektiviserad drift av datorsystem

Fråga: I vilket OSI-lager jobbar SNMP?
Svar: OSI lager 7, applikationslagret

Fråga: Vad är en SNMP trap?
Svar: Enheter som övervakas av SNMP skickar normalt bara information till övervakningsservern först när den fått en förfrågan om det. En trap, kan dock skickas av enheten till övervakaren om ett visst kriteria uppfyllts utan att övervakaren bett om det.

Vilket transportprotokoll använder SNMP för traps?
Svar: UDP

Fråga: Vad medför detta för nackdel?
Svar: Eftersom UDP inte upprättar en anslutning mellan avsändaren och mottagaren och istället bara skickar iväg paketet och hoppas det kommer fram så finns det ingen garanti att paketet kommit fram. Konsekvensen blir att traps kan gå förlorade utan att någon märker det.

Fråga: Vad använder SNMP för port(ar)?
Svar:
161 (Här tar SNMP-agenter emot förfrågningar.)
162 (Här tar Managers emot Trap och InformRequest PDU:er.)
10161 (Används för de krypterade förfrågningarna.)
10162 (Här tar Managers emot Trap och InformRequest PDU:er som skickas i krypterad form.)

Fråga: Hur är ett OID uppbyggt?
Svar: Varje OID har en variabel associerad till den och dessa är sedan organiserade enligt en trädstruktur (hierarkisk struktur).
Den fulla sökvägen till ett specifikt OID skulle kunna vara: 1.3.6.1.4.1.2681.1.2.102. Det sista talet, i det här fallet 102,
hittas om man först går till 1, vidare till 3, vidare till 6, vidare till 1 och så vidare. Alla dessa siffror representerar kategorier.
Varje OID är unikt och de första i ordningen är standardiserade på vad de representerar.

Fråga: Vilka try typer av communitys har SNMP?
Svar: Read-Only, Read-Write och Trap.

Fråga: Vad brukar standardnamnen vara för SNMP-community Read-Only och Read-Write?
Svar: Read-Only = Private, Read-Write = Public

Fråga: Varför vill man inte att SNMP cummunitynamnen ska skickas i klartext på nätverket?
Svar: För att communitynamnet även används som ett lösenord i SNMP och sniffas detta upp kan en attack utföras.

Fråga: Vad används MIB:s till?
Svar: För att översätta alla OIDs från siffrorkoder till namn på vad de representerar. Utan dem förstår inte en människa vad som representerar vad.