Netwerkbeheer

a. *Waarom* is netwerkbeheer noodzakelijk ?
b. Aan welke *randvoorwaarden* moeten oplossingen voor netwerkbeheer beantwoorden ?
c. Beschrijf het model dat de *functionele eisen* voor netwerkbeheer vastlegt. Geef van elke categorie de meest typische aspecten.

A)

1. **Op financieel vlak:** een goed beheerd en gedocumenteerd netwerk laat toe om de *pro-actief* het aantal incidenten, waardoor bepaalde diensten voor gebruikers onbeschikbaar zijn, te verminderen. Dit leidt tot hogere productiviteit en lagere globale kosten.

2. **Op technisch vlak:** potentiele probleemsistuaties en punten die voor verbetering in aanmerking komen, zijn in een strikt beheerde omgeving makkelijker te identificeren. Een goed beheerde infrastructuur kan veel beter reageren op veranderende randvoorwaarden en doelstellingen, zoals uitbreiding van capaciteit, diensten en gebruikers.

3. **Op vlak van beveiliging:** het aanbieden van de juiste diensten aan de juiste personen is onmogelijk zonder dat de volledige verzameling bronnen correct geïnventariseerd en strict beheerd wordt. Indien onbevoegde personen toch toegang zouden krijgen tot bepaalde elementen, dan is herstel van de gevontroleerde toestand veel vlugger mogelijk dan in een onbeheerde omgeving.

4. **Op professioneel vlak:** de toekomstperspectieven van het globale bedrijf hangen voor een groot deel af van de goed beheerde informatica-structuur. Ook de jobvoldoening is veel groter als ze het gevoel hebben dat ze de componenten onder controle hebben.

B)

- Het begrip netwerkinfrastructuur moet men in zeer ruime zin interpreteren. Alle componenten die een essentiële bijdrage leveren komen in aanmerking: netwerkkaarten, modems, hubs, bridges, switches, routers, werkpost/server-systemen. Ook meer ordinaire element, zoals sensoren,… Netwerkbeheer omvat niet alleen het beheer van hardware componenten, maar ook van software toepassingen zoals print spoolers, DNS-, mail-, DCHP-, WWW- en databankservers.
  Daarom moeten beheersystemen kunnen omspringen zowel met een ruime waaier netwerkprotocollen als met diverse media en randapparatuur.

- **Netwerkbeheer moet zoveel mogelijk gecentraliseerd gebeuren** (vanaf één enkel management station(NMS)). Bij een volledig gecentraliseerd beheer is het management station vak zelf een bottleneck (vooral indien er vele duizenden componenten gemonitord moeten worden). Daarom kiest men vaak voor een *gedistribueerde* aanpak. Voordeel: het netwerkbeheer zelf hoeft niet onderbroken te worden als de software of hardware van het NMS faalst

- **Netwerkbeheer moet een beperkte impact hebben op de kosten en belasting van het netwerkinfrastruur.** Daarom moet ze steunen op eenvoudige principes en gebruik maken van eenvoudige implementaties.

- **Systemen voor netwerkbeheer moeten modulair implementeerbaar zijn**

- **Netwerkbeheersystemen moeten gebruik maken van een bestaande protocolstack.** Zo zijn ze zo weinig mogelijk afhankelijk van hogere procolniveau's en blijven ze routeerbaar.

C)

Het X.700 model (ISO) heeft een hele reeks functionele eisen waaraan een efficiënte managementstrategie moet beantwoorden gebundeld in 5 gebieden.
Een compleet netwerkbeheerssysteem moet aan alle aspecten van alle gebieden voldoen.

5 gebieden:

1. Configuratie beheer: omvat 2 doeleinden:
    - Configuratie van de hardware infrastructuur
      Dit komt vooral neer op een gedetailleerde inventaris (locatie en functie) van alle systemen en hun componenten.
      Dit proces wordt dikwijls geautomatiseerd mbv discovery procedures.
    - Configuratie van de software
      meer complex

    Belangrijkste aandachtspunten:
    - *Change management:* onmiddellijk beschikbare en precieze informatie over alle wijzigingen + mogelijkheid om dezelfde configuratiewijzing toe te passen op een groep componenten.

    - *Asset management:* een overzicht van alle netwerkcomponenten die kunnen vervangen worden + de planning om verouderde elementen te vervangen door nieuwe technologie.

2. Accouting beheer:
    - *Value assessment:* kent elke netwerkcomponent een bepaalde waarde toe die kenmerkend is voor de belangrijkheid ervan.

    - *Usage auditing:* het precies bijhouden wie op welk ogenblik welke netwerkbronnen gebruikt.

3. Performantie beheer heeft als doel een netwerkinfrastructuur aan te bieden met de hoogst mogelijke niveaus van betrouwbaarheid, beschikbaarheid en throughput.
   Taken: uittesten van media, simulatie, planning, tuning, opsporen van bottlenecks en baselining (periodiek meten van de belasting van diverse componenten en dit uitgemiddeld over een bepaalde tijdsspanne)

4. Security beheer: ervoor zorgen dat de diverse netwerkbronnen enkel door geautoriseerde gebruikers benaderd kan worden en (pogingen tot) inbreuken

rapporteren en herstellen.

Voorbereidende stappen:

- *Value assessment:* elk type data een waarde toekennen

- *Risk management:* inschatting van de gevolgen van eventuele blootstelling of corruptie.

5. Foutopvolging: zoveel mogelijk pro-actief vermijden van fouten en het zo vlug mogelijk detecteren en rapporten van fouten.
   Rapportering: wegschrijven van events in logbestanden, automatisch aanmaken van trouble tickets, genereren van een alarm.
   Ook analyseren van de oorzaak en remedies.