higher education & training

Department:
Higher Education and Training
REPUBLIC OF SOUTH AFRICA

NASIENRIGLYN

NASIONALE SERTIFIKAAT (BEROEPSGERIG)

DATA KOMMUNIKASIE EN NETWERKING
NKR VLAK 4

10 November 2022

Hierdie nasienriglyn bestaan uit 7 bladsye.

Kopiereg voorbehou

AFDELING A

VRAAG 1

1.1 B
1.2 A
1.3 D
1.4 C
1.5 D
1.6 A
1.7 C
1.8 C
1.9 B
1.10 C

(10 × 1) **[10]**

VRAAG 2

2.1 D
2.2 F
2.3 K
2.4 L
2.5 B
2.6 I
2.7 C
2.8 J
2.9 A
2.10 E

(10 × 1) **[10]**

TOTAAL AFDELING A: 20

AFDELING B

VRAAG 3

3.1 3.1.1

- Skakelaar – koppel toestelle in ’n LAN netwerk.✓
- Brandmuur – laat netwerkverkeer gebaseer op beleid toe of weier toegang ✓OF beskerm ’n LAN van eksterne bedreigings. ✓
- Draadlose roeteerder – word vir roetering gebruik ✓ OF word gebruik om ’n netwerk aan die internet te koppel ✓ OF word gebruik om netwerke te skei. ✓
- Bediener – word gebruik om hulpbronne te berg ✓ OF ’n rekenaar wat inligting en dienste aan kliënte verskaf. ✓

(4)

3.1.2 ’n Brandmuur is ’n sekuriteitstoestel of sagteware wat gebruik word om netwerke te beskerm en beveilig ✓ maar ’n skakelaar word gebruik om toestelle in ’n LAN te koppel. ’n Brandmuur filter inkomende en uitgaande verkeer gebaseer op organisasie se sekuriteit. ✓ (2)

3.2

- Simpleks:✓ Kommunikasie is eenrigting. Slegs een van die twee toestelle op ’n skakel kan stuur, die ander kan slegs ontvang. Die simpleks modus kan die hele kapasiteit van die kanaal gebruik om data in een rigting te stuur.✓
- Halfdupleks:✓ Elke stasie kan stuur en ontvang, maar nie terselfdertyd nie. Wanneer een toestel stuur, kan die ander een slegs ontvang ✓ en omgekeerd.
- Volledig dupleks:✓ Albei stasies kan terselfdertyd stuur en ontvang. In volle dupleks modus deel seine wat in een rigting gaan die kapasiteit van die skakel met seine wat in ’n ander rigting gaan.✓ (3 × 2) (6)

[12]

VRAAG 4

4.1 ’n Virtuele LAN (VLAN) stel ’n mens in staat om gebruikers in afsonderlike uitsaai-domeine✓ te verdeel.✓ VLANs verbeter sekuriteit, segmentering en buigsaamheid. Elke VLAN op ’n skakelaar tree op asof dit ’n afsonderlike fisiese brug is.✓ Die skakelaar stuur pakkies slegs na poorte waaraan dieselfde VLAN toegewys is. ✓ Dit verminder netwerkverkeer.✓ VLANs benodig ’n hooflyn (trunk) om veelvuldige skakelaars te oorspan (span). Elke hooflyn kan verkeer vir veelvoudige VLANs dra.✓ (Enige 4 × 1) (4)

4.2 Gebruikersaanvaardingstoetsing (UAT)✓ is een van die laaste stadiums van die sagteware-ontwikkelingslewensiklus. Dit staan soms bekend as eindgebruikertoetsing.✓ Soos die naam suggereer word UAT uitgevoer op ’n produk deur die eindgebruikers van die produk vir goedkeuring vir produksievrystelling.✓ (Enige 2 × 1) (2)

4.3 4.3.1 A – Oop stelsels tussenverbinding (OSI)
B – Transmissiebeheerprotokol/Internetprotokol OF TCP/IP (2)

4.3.2

OSI (Oop stelsels tussenverbinding)	**TCP/IP (Transmissiebeheerprotokol/ Internetprotokol)**
• Dit is ’n generiese, protokol-onafhanklike standaard wat as ’n kommunikasiepoort tussen die netwerk en eindgebruiker funksioneer.	• Dit is gebaseer op standaard protokolle waaróm die internet ontwikkel het. Dit is ’n reeks protokolle. Dit wil sê, ’n boks protokolle.
• Die vervoerlaag (transport layer) lei direk na die vervoerlaag van die TCP/IP	• Die vervoerlaag (transport layer) lei direk na die OSI vervoerlaag.
• Dit volg ’n vertikale benadering.	• Dit volg ’n horisontale benadering.
• Dit het ’n afsonderlike aanbiedingslaag (presentation layer) en ’n sessielaag (session layer).	• Dit het nie ’n afsonderlike aanbiedingslaag (presentation layer) en ’n sessielaag (session layer) nie.
• Die applikasielaag spesifiseer funksies van applikasies. Dit wil sê, dit verskaf spesifikasies vir gebruikerskoppelvlak.	• Die TCP/IP applikasielaag sluit ’n aantal protokolle in wat spesifieke funksionaliteit aan ’n verskeidenheid eindgebruiker-applikasies verskaf.
• Die netwerklaag spesifiseer roetering en logiese addresseringsfunksies.	• Die netwerklaag word die internetlaag.
• Dit is ’n verwysingsmodel waaróm netwerke gebou word. Gewoonlik word dit as ’n leidingshulpmiddel gebruik.	• Op ’n manier is dit die implementering van die OSI model.
• Die fisiese en dataskakel-lae is afsonderlike lae.	• OSI laag 1 en 2, die fisiese en dataskakels lei na die TCP/IP netwerk toegangslaag (access layer).
• Die OSI model se laag 5, 6 en 7 word gebruik as verwysings vir applikasie-sagteware-ontwikkelaars en -verkopers om produkte te produseer wat op netwerke werk.	• Oor die algemeen moet applikasie-ontwikkelaars die funksies van laag 5 en 6 in hulle applikasies inkorporeer.
• Dit definieer dienste, koppelvlakke en protokolle baie duidelik en tref ’n duidelike onderskeid tussen hulle. Dit is protokol-onafhanklik.	• Dienste, koppelvlakke en protokolle word nie duidelik geskei nie. Dit is ook protokol-afhanklik.
• Dit het sewe lae.	• Dit het vier lae.

Aanvaar antwoorde in die vorm van ’n paragraaf
✓ vir elke duidelik omskryfde eienskap van elke model
(Enige 8 × 1) (8)
[16]

VRAAG 5

5.1 Kabel A – Enkel-modus optiese veselkabel
Kabel B – Multimodus optiese veselkabel
(Antwoord moet die woorde 'optiese vesel' bevat)(2 × 2) (4)

5.2
- Die kabel maak dit moontlik dat veelvoudige strale lig daardeur beweeg.
- Dit het ’n groter kern.
- Hierdie kabel word gebruik in korter afstand in vergelyking met enkelmodus kabels.
- Dit gebruik ’n LED as die ligbron.
- Dit het groter verspreiding. Dit wil sê, groter verstrooiing van strale lig. Meestal gebruik in LANs. (Enige 4 × 1) (4)

5.3 Netwerksekuriteit bestaan uit drie verskillende kontroles naamlik fisiese netwerksekuriteit ✓ wat ontwerp is om te verhoed dat ongemagtigde personeel fisiese ✓ toegang tot netwerkkomponente soos roeteerders, kabelkaste (cabling cupboards) en so aan kry. Beheerde toegang, soos slotte, biometriese bekragtiging en ander toestelle moet gebruik word ✓; tegniese netwerksekuriteit ✓ wat data beskerm wat op die netwerk geberg word of wat in transito is deur, in of uit die netwerk. ✓ En administratiewe netwerksekuriteit ✓ wat bestaan uit sekuriteitsbeleide en -prosesse ✓ wat gebruikersgedrag beheer, insluitend hoe gebruikers gemagtig en bekragtig word en ook die data beperk waartoe elke gebruiker toegang het.✓

(Enige 6 × 1) (6)
[14]

VRAAG 6

6.1
- Plaaslike gebruikersprofiel: word die eerste keer geskep wanneer ’n gebruiker op ’n rekenaar aanteken. Die plaaslike gebruikersprofiel word op ’n rekenaar se plaaslike hardeskyf geberg. Enige veranderings wat aan die plaaslike gebruikersprofiel gemaak word, is spesifiek tot die rekenaar waarop veranderings gemaak word.
- Swerwing (roaming) gebruikersprofiel: ’n Kopie van die plaaslike profiel word op ’n gedeelde bediener gekopieer en geberg. Hierdie profiel word afgelaai elke keer wat ’n gebruiker op enige rekenaar op die netwerk aanteken en enige veranderings aan ’n swerwing gebruikersprofiel word gesinchroniseer met die bediener se kopie wanneer uitgeteken word.
- Verpligte gebruikersprofiel: ’n Tipe profiel wat administrateurs kan gebruik om sekere instellings vir gebruikers te spesifiseer. Slegs stelseladministrateurs kan veranderings aan verpligte gebruikersprofiele maak. Veranderings aan wat deur die gebruiker aan tafelrekenaar-instellings gemaak word, gaan verlore wanneer die gebruiker afteken.
- Tydelike gebruikersprofiel: ’n Tydelike profiel word enige tyd uitgereik wat ’n fouttoestand verhoed dat die gebruiker se profiel gelaai kan word. Tydelike profiele word aan die einde van elke sessie uitgewis en veranderings wat die gebruiker aan hulle tafelrekenaar-instellings gemaak het, gaan verlore wanneer die gebruiker afteken. (Enige 3 × 2) (6)

6.2 Toegangsbeheer is ’n metode om toegang tot ’n stelsel of fisiese of virtuele hulpbronne te beperk.✓ Dit is ’n proses waardeur gebruikers toegang tot en sekere regte/voorregte tot stelsels, hulpbronne of inligting kan kry.✓ Toegangsbeheer is ’n sekurieitstegniek wat beheer het oor wie verskillende aspekte kan besigtig, wat besigtig kan word en wie hulpbronne in ’n rekenaaromgewing kan gebruik.✓ Dit is ’n fundamentele konsep in sekuriteit wat risiko vir die besigheid of organisasie verlaag.✓ (4)

6.3 ’n Nutsprogram is stelselsagteware✓ wat gebruikers help om hulle rekenaars te ontleed, konfigureer, monitor of help in stand hou.✓ (2)

6.4 Dit moet koppelings ✓, kommunikasies en dienste verskaf. ✓ (2)

6.5 ’n Drukwerktou is ’n lys drukker uitsettake ✓ wat in ’n gereserveerde geheue-area gehou word.✓ Dit handhaaf die mees onlangse status✓ van alle aktiewe en hangende druktake.✓ (4)
[18]

VRAAG 7

7.1 Netwerkkapasiteitsbeplanning is die proses om ’n netwerk vir benutting, bandwydte, operasies, beskikbaarheid en ander netwerkkapasiteits-beperkings ✓ te beplan.✓ Dit is ’n tipe netwerk of IT bestuursproses✓ wat netwerkadministrateurs help in die beplanning vir netwerkinfrastruktuur en -operasies in lyn met huidige en toekomstige operasies.✓ (4)

7.2
- Datatransmissietempo
- Hoeveel die netwerk gebruik word
- Die aantal verlore of foutiewe pakkies (3 × 2) (6)

7.3 Pakkieskakeling breek databoodskappe in pakkies op wat terselfdertyd oor beskikbare kringe tussen die bron en die bestemmingstoestel gestuur word.✓ Pakkieskakeling stel nie ’n kring tussen kommunikasietoestelle daar nie.✓ (2)

7.4 7.4.1 Om te verhoed dat ’n gebruiker toegang tot stelsels of data kry deur ’n gemagtigde gebruiker se rekening te gebruik, implementeer twee-faktor bekragtiging.✓ Dit vereis dat ’n gebruiker ’n tweede stuk identifiserende inligting bykomend tot ’n wagwoord verskaf.✓ Installeer ’n brandmuur. ✓

OF

Enkripteer sensitiewe korporatiewe data op rus of soos dit oor ’n netwerk beweeg deur geskikte sagteware of hardeware tegnologie te gebruik.✓ Op daardie manier sal krakers nie in staat wees om toegang tot vertroulike data kry nie.✓

7.4.2 Om binnebedreigings op te spoor en te verhoed, implementeer bespeidware-skandeerprogramme, antivirus programme, brandmure en ’n streng data rugsteun- en argiveringsroetine.✓ Jy kan werknemers en kontrakteurs ook oplei om sekuriteitsbewus te wees voordat hulle toegang tot die korporatiewe netwerk kry.✓

OF

Implementeer werknemer-monitering sagteware✓ om die risiko van dataoortredings en die diefstal van intellektuele eiendom te verminder deur nalatige, ontevrede of kwaadwillige binnekringlede te identifiseer. ✓

7.4.3 Beskerming teen uitvissingsaanvalle begin deur gebruikers in te lig om uitvissingsboodskappe te identifiseer.✓ Daarbenewens kan ’n poort- e-posfilter baie massa-geteikende e-posse ondervang en die getal uitvissings- e-posse wat gebruikers se inmandjies beland verminder.✓

(3 × 2) (6)

7.5 Wye-gebied-netwerk (2)

[20]

TOTAAL AFDELING B: 80
GROOTTOTAAL: 100

Kopiereg voorbehou