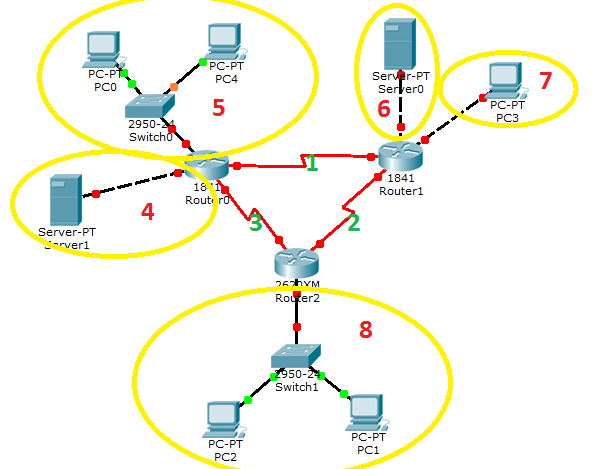
**DPT-III eksāmena jautājumi**

**Teorētiskā daļa - 6 no 1-74**

1. **Cik IP tīkli vai apakštīkli nepieciešami redzamajā tīkla topoloģijā?**

Skatāmies uz attēlu. Katram maršrutētāja izvadam/portam ir viens tīkls. Maršrutētāju kopējam savienojumam ir viens tīkls, kaut arī pēc iepriekšējā teikuma sanāk 2.

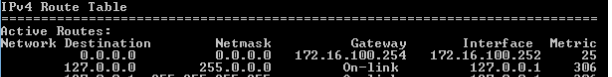


2. **Kam nepieciešama maršrutēšanas tabula?**

Maršrutēšanas tabula glabā informāciju par tieši un netieši pieslēgtajiem tīkliem. Tā norāda pa kuru ceļu, jāsūta pakete, lai tā nonāktu līdz galamērķim.

3. **Sniegt maršrutēšanas tabulas ieraksta paraugu?**

Windows (*route print*):



Cisco (*show ip route*):



4. **Kādu informāciju satur maršrutēšanas tabulas ieraksts?**

Galamērķa tīklu un tā masku, ceļu (vārteju - gateway) uz šo tīklu, interfeisu, caur kuru tas sasniedzams/pievienots un metrika – labākā ceļa noteikšanai. Mazāka metrika – īsāks ceļš vai lielāks joslas platums... Ceļam ar mazāku metriku tiek dota priekšroka.

5. **Kādu informāciju satur maršrutēšanas tabula?**

Vienu vai vairākus maršrutēšanas tabulas ierakstus... Skatīt 4. Punktu.

6. **Uz kuras iekārtas atrodas maršrutēšanas tabula?**

Uz maršrutētājiem un tīklā pieslēgtiem datoriem.

7. **Kā var aplūkot maršrutēšanas tabulu?**

Windows: **route print**

Cisco: **show ip route** (var arī no lietotāja „>” režīma)

8. **Sniegt maršrutētāja tīkla interfeisu piemērus?**

FastEthernet, Serial, Ethernet, Dot11Radio (tāds arī ir… Wireless)

9. **Kādus rezultātus sniedz "show ip route" komanda?**

parāda maršrutēšanas tabulas kuras atrodas uz maršrutētāja skatīt 3 jautājumu

**10. Kādas IP adreses jāpiešķir maršrutētāja tīkla kartēm?**

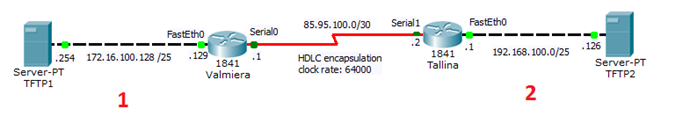
Nav īsti svarīgi.

Tāda adrese, kāda ir dotajam tīklam kas iet uz to portu.

11. **Kas ir statiskais maršruts?**

Maršrutēšana, kas nodrošina datu pārsūtīšanu to saņēmējam pa vienu un to pašu ceļu (maršrutu).

**12. Cik statiskie maršruti būtu jānokonfigurē uz pasniedzēja norādītā maršrutētāja redzamajā tīkla topoloģija?**



**13. Kādi statiskie maršruti būtu jānokonfigurē uz pasniedzēja norādītā maršrutētāja redzamajā tīkla topoloģija?**

12. punkta attēlam:

* ip route 192.168.100.0 255.255.255.128 82.95.100.2 (uz maršrutētāja „Valmiera”)
* ip route 172.16.100.128 255.255.255.128 85.95.100.1 (uz maršrutētāja „Tallina”)

14. **Ar kādu komandu var nokonfigurēt statisko maršrutu?**

ip route network mask gateway

piem., **ip route 1.1.1.0 255.0.0.0 2.1.1.2**

15. **Kas ir noklusētais maršruts "default route" un kādās situācijās to izmanto?**

Visas paketes, kas jāsūta uz tīkliem, par kuriem nav ierakstu maršrutēšanas tabulā, tiek sūtītas caur noklusēto maršrutu (*default route*) – nākamo maršrutētāju (IP adrese) vai caur norādīto interfeisu.

16. **Sniegt noklusētā maršruta "default route" konfigurācijas piemēru!**

**ip route 0.0.0.0 0.0.0.0 Fa0/0**

Visas nezināmās paketes tiek sūtītas caur interfeisu *FastEthernet0/0*

17. **Kādās situācijās izvēlās statisko maršrutēšanu?**

Ja mūsu maršrutētājam ir pieslēgts tikai viens (cits) maršrutētājs. Nav jēgas konfigurēt maršrutēšanas, ja visi ceļi tāpat vedīs caur mums pieslēgto maršrutētāju.

18. **Kādi ir statiskās maršrutēšanas mīnusi?**

* Statiskā maršrutēšana neparedz rezerves ceļu veidošanu. „Nobrūkot” savienojumam, maršruts jāpārkonfigurē pašrocīgi;
* Sarežģīta konfigurēšana lielām tīkla topoloģijām;
* Pilnībā jāpārzina tīkla topoloģija (adminam).

19. **Kas ir dinamiskā maršrutēšana?**

Maršrutēšana, kas automātiski piemērojas datoru tīkla topoloģijas vai trafika izmaiņām.

Maršrutēšanas tehnika, kas nodrošina optimālu datu maršrutēšanu. Maršrutēšanas tabula tiek dinamiski atjaunota, balstoties uz pašreizējo tīkla situāciju – pieejamajiem ceļiem, tīkla slodzes, joslas platuma. Maršrutētāji savā starpā apmainās ar informāciju.

**20. Kādi ir dinamiskās maršrutēšanas plusi?**

· Maršrutēšanas tabula pielāgojas tīkla topoloģijai, dati tiek sūtīti dinamiski, rūteris izvēlas labāko maršrutu sūtīšanai.

**21. Kādi ir dinamiskās maršrutēšanas mīnusi?**

**22. Kādas ir dinamisko maršrutēšanas protokolu pamatfunkcijas?**

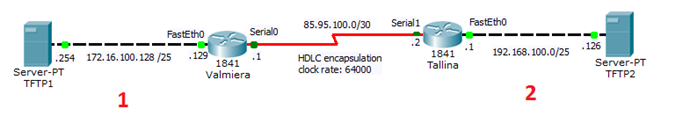
Dinamiski dalās ar informāciju rūteru starpā. Automātiski atjauno maršrutēšanas tabulu, ja mainās toploģija. Nosaka labāko ceļu uz galamērķi. Daloties ar maršrutēšānas tabulām, maršrutētāji ir spējīgi atklāt jaunus tīklus.

23. **Nosaukt četrus dinamiskās maršrutēšanas protokolus!**

RIP, OSPF, BGP, IGRP, [EIGRP](http://lv.wikipedia.org/wiki/EIGRP), IS-IS

24. **Kādi konfigurācijas ieraksti jāveic, lai uz pasniedzēja norādītā maršrutētāja darbotos dinamiskā maršrutēšana?**

* Konfigurē protokolus norādot tieši pieslēgtos tīklus, nevis galamērķi, kā statiskajiem maršrutiem.



* RIP v2:

Valmiera (**config#**):

o router rip

o version 2

o network 172.16.100.128 *Tieši pieslēgtais tīkls*

o network 85.95.100.0 *Tieši pieslēgtais tīkls*

Tallina (**config#**):

o router rip

o version 2

o network 192.168.100.0 *Tieši pieslēgtais tīkls*

o network 85.95.100.0 *Tieši pieslēgtais tīkls*

* OSPF:

Valmiera (**config#**):

o router ospf *1* (<ID>) *ID drīkst atšķirties dažādiem maršrutētājiem*

o network 172.16.100.128 0.0.0.127 area **0**  *Tieši pieslēgtais tīkls*

o network 85.95.100.0 0.0.0.3 area **0** *Tieši pieslēgtais tīkls*

*Tieši pieslēgtais tīkls; inversā maska; area jāsakrīt visiem rūteriem, lai tie apmainītos ar info.*

Tallina (**config#**):

o router ospf *2*  *ID drīkst atšķirties dažādiem maršrutētājiem*

o network 192.168.100.0 0.0.0.127 area **0** *Tieši pieslēgtais tīkls*

o network 85.95.100.0 0.0.0.3 area **0** *Tieši pieslēgtais tīkls*

**25. Kā noskaidrot dinamisko maršrutēšanas protokolu izveidotos maršrutēšanas ierakstus?**

**KĀ?**

26. **Kas ir RIP?**

**Routing Information Protocol** (**RIP**) vēsturiski bija viens no biežāk lietotajiem maršrutēšanas protokoliem. Pārsvarā tas tiek lietots nelielos iekšējos tīklos.

RIP protokols sūta citiem maršrutētājiem pilnu maršrutēšanas informācijas tabulu katras 30 sekundes.

Ir trīs RIP protokola versijas: **RIPv1**, **RIPv2** un RIPng.

**RIPv1** izmanto *broadcast* adresi (255.255.255.255) maršrutēšanas informācijas nosūtīšanai.

**RIPv2** izmanto *multicast* adresi (224.0.0.9) maršrutēšanas informācijas nosūtīšanai.

27. **Kas ir EIGRP?**

**EIGRP** (angļu: *Enhanced Interior Gateway Routing Protocol*) ir dinamisks maršrutēšanas protokols.

EIGRP īsākā maršruta noteikšanai izmanto DUAL (angl. Diffusing update algorithm) mehānismu, kurā kopējā ceļa noteikšanai tiek izmantotas trīs veidu tabulas:

* kaimiņu iekārtu tabula – satur ierakstus (adresi) par katru maršrutētāju, kas ir fiziski pieslēgts konkrētajam maršrutētājam.
* topoloģijas tabula – satur ierakstus par visiem autonomās sistēmas maršrutiem. Ieraksti tiek iegūti no kaimiņu iekārtu tabulām.
* maršutēšanas tabula – satur ierakstus par labāko iespējamo maršrutu, kas tiek iegūti no topoloģiju tabulas.

28. **Kas ir IGRP?**

pilnā vārdā **Interior Gateway Routing Protocol** ir dinamiskās maršrutēšanas protokols

29. **Kas ir OSPF?**

Maršrutēšanas protokols, kas paredzēts lietošanai autonomajās sistēmās.

30. **Kas ir IGP un EGP? Kādās situācijās izmanto?**

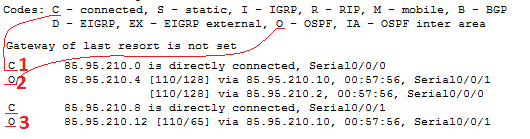
IGP - interior gateway protocol, EGP - exterior …

IGP - protokols, kuru izmanto maršrutētāja informācijas apmaiņai starp gateways (hosti ar rūteriem) autonomā sistēmā, piemēram, lokālajā tīklā.

EGP - protokols, kuru izmantot maršutētāja informācijas apmaiņai starp diviem kaimiņu gateway hostiem (kur katram hostam ir savs rūteris) autonomā sistēmā. To biežāk izmanto starp hostiem Internetā, kas satur maršūtēšanas tabulu.

IGP izmanto RIP un OSPF protokolus, bet EGP - BGP border gateway protocol

31. **Izskaidrot pasniedzēja norādīto maršrutēšanas tabulas ierakstu!**



1. Tīkls 85.95.210.0 ir tieši pieslēgts. Izejas interfeiss – Serial0/0/0. Uz to norāda burts „C”.

2. Tīkls 85.95.210.4 ir pieejams caur:

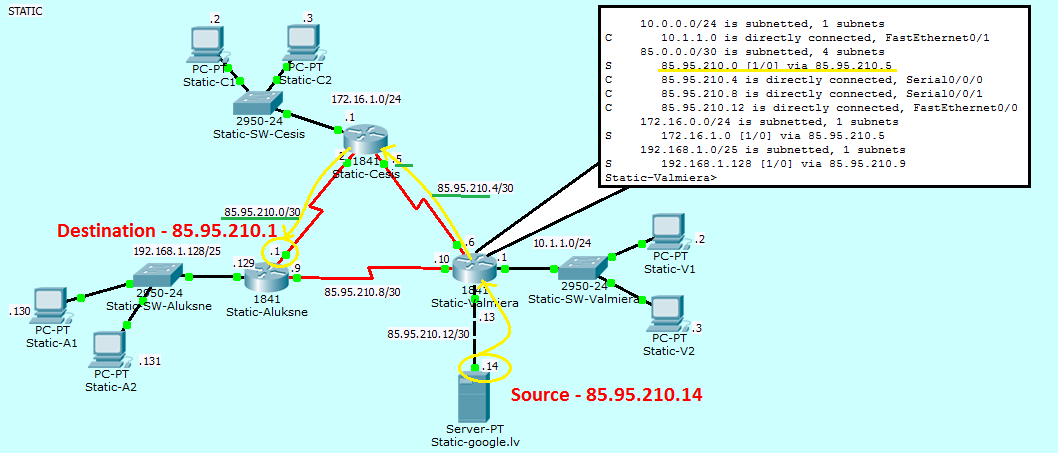
a. adresi 85.95.210.10, kas sasniedzama caur Serial0/0/1

b. adresi 85.95.210.2, kas sasniedzama caur Serial0/0/0.

Maršruts noskaidrots ar OSPF protokola palīdzību. Uz to norāda burts „O”

3. Tīkls 85.95.210.12 pieejams caur adresi 85.95.210.10, kas sasniedzama caur Serial0/0/1.

**32. Pa kuri ceļu tiks nosūtīta pakete norādītajā konfigurācijā un tīkla topoloģijā?**



Ar dinamisko maršrutēšanu var gadīties visādi brīnumi - grūti teikt, pa kuru ceļu klejos paketes.

**33. Kas ir maršrutēšanas protokolu metrika? Sniegt piemērus.**

Lēkājumu skaits (*hop-count*) - maršrutētāju skaits caur kuriem paketei jāiet, lai sasniegtu adresātu.

34. **Kāds ir slodzes dalīšanas "load balancing" mērķis?**

Optimizēt resursu izmantošanu, palielināt caurlaidību, samazināt reakcijas laiku, novērstu jebkuru resursu pārslodzi.

35. **Kad var izmantot slodzes dalīšanu "load balancing"?**

Slodzes dalīšanu var izmantot, ja caur dažādiem ceļiem, galamērķa adrese ir vienādā attālumā/ ar vienādām izmaksām, metrikām.

**36. Ko nozīmē tieši pieslēgtais "directly connected" tīkls?**

To, ka tīkls ir tieši pieslēgts pie kāda no maršrutētāja tīkla interfeisiem.

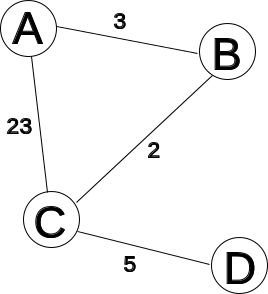
3**7. Kāpēc sūtot IP paketes procesā tiek izmantotas arī MAC adreses?**

*Būtībā, L2 Switch ir stulbs bez gala. Tas māk strādāt tikai ar MAC adresēm...*

38. **Kas ir ARP un kam tas nepieciešams?**

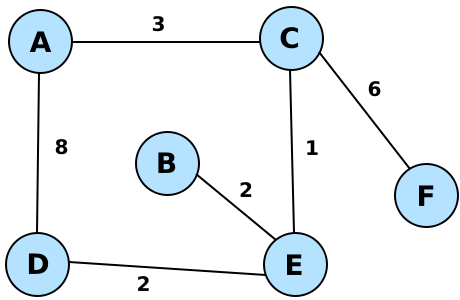
Address Resolution Protocol nepieciešams, lai noskaidrotu IP adresei atbilstošo iekārtas MAC adresi.

**39. Distances vektora "distance vector" dinamiskie maršrutēšanas protokolu piemēri un to pamatīpašības?**

**Piemērs:**

Informē blakus esošo tīklu par topoloģijas izmaiņām

**40. Link-state dinamiskie maršrutēšanas protokolu piemēri un to pamatīpašības?**

**Piemērs:**

Ir viens no galvenajiem tīkla protokoliem, kuru izmanto pakešu pārslēgšanā, izmanto OSPF un IS-IS, princips ir tāds, ka link-state network izveido karti, kurā parāda visus punktus, kuriem ir pieslēgušies citi punkti.

**41. Kāda ir "classless" un "classful" maršrutēšanas atšķirība?**

classless- ip adrešu lielumu nosaka pēc subnet maskas. Piemēram ip adrese var būt no 172.16.1.0 - 255 jo subnet maska ir 255.255.255.0

classful- ip adrešu lielumu nosaki pats un no tā izriet kāda būs subnet maska. Piemēram 172.16.1.2 subnet maska būs 255.255.0.0, un lai kā gribētos nevarēs ietekmēt subnet maskas lielumu.

**42. Kam maršrutēšanas tabulas ierakstā domāta "administartive distance" vērtība?**

Domāts lai rūteris izvēlētos labāko ceļu, ja ir sniegti vairāki ceļi par vienu

**43. Kas ir maršrutēšanas protokolu konverģences laiks, kas to veido?**

Topoloģiju izmaiņu ātrums.

**44. Raksturo periodiskos un trigerētos maršrutēšanas protokolu ziņojums!**

periodiskie maršrutēšanas ziņojumi- izmanto RIP v1 un nenēsā līdzi subnet informāciju, un nav nekādas aizsardzības pret izstūtītajiem un ienākošajiem ziņojumiem, tas nozīmē, ka tīkls ir viegli apdraudējams.

trigerētie- izmanto RIP tīklā un jabūt nokonfigurētam no abām pusēm.

**45. Kas ir maršrutēšanas cilpas, kā tās rodas?**

maršrutēšanas cilpas ir kad divi punkti domā ka ceļš uz galamērķi iet caur otru punktu. pieņemsim mums ir punkts A un punkts B viņi abi grib tikt uz punktu C un abi domā ka sākuma punkts ir pretējais punkts. B domā ka sākuma punkts ir no A un otrādi. tādejādi veidojot mūžīgu ciklu.

**46. Raksturot galvenos paņēmienus maršrutēšanas cilpu novēršanai!**

RIPS izmanto Split horizontal, route poisining un holdown timer šīs ir tīkla migrācijas

Tīkliem [BGP](http://en.wikipedia.org/wiki/BGP), [EIGRP](http://en.wikipedia.org/wiki/EIGRP), [DSDV](http://en.wikipedia.org/wiki/DSDV), [Babel](http://en.wikipedia.org/wiki/Babel_%28protocol%29)- ir izveidots speciāls algoritms, kurš neļauj izveidoties Cilpām

Tīkliem [OSPF](http://en.wikipedia.org/wiki/OSPF) or [IS-IS](http://en.wikipedia.org/wiki/IS-IS)- Cilpa izgaist tiklīt pievienojas jauni tīkli, Cilpas nav ilgākas par dažām sekundēm

**47. Kas ir VLSM un CIDR? Kam to izmanto?**

VLSM (*Variable Length Subnet Masks*)- VLSM atļauj elastīgu un līdz ar to ekonomisku dalīšana apakštīklos (*subnetting*), kā arī prefiksu apkopošanu (*prefix aggregation*).

Šos abus sūdus izmanto ipv6

CIDR(*Classless Inter-Domain Routing*)- tā ir ip un apakštīklu sadales metode, kura ļauj sadalīt tīklus elastīgāk nekā ipv4. CIDR izmanto VLSM

48. **Kas ir "wildcard" maska? Kur to izmanto?**

Wildcard maska ir inversā maska. Iegūst no 255 atņemot katru tīkla maskas oktetu. Izmanto konfigurējot OSPF un ACL.

|  |  |
| --- | --- |
|  | 255.255.255.255 |
| - | 255.255.128.0 |
|  | 0.0.127.255 |

**49. Raksturo simetrisko un asimetrisko komutāciju!**

Simetriskā komutācija- Viss iet kā viens ports ja viens ir pieslēgts 100mb/s portam tad pārējie arī būs ar šādu ātrumu

asimetriskā komutācija- tiek pārslēgti porti attiecīgi pēc vajadzības viens var būt pieslēgts 100mb/s portam un otrs 1000mb/s tīklam un tas nodrošina lielāku tīkla ātrumu un tādejādi datu pāraidīšana notiek daudz plūstošāk.

**50. Kādu papildu funkcionalitāti nodrošina Layer3 komutators salīdzinot ar Layer2 komutatoru?**

* zems latentums
* drošība
* aparatūras balstīta pakešu sūtīšāna
* augstas veiktspējas pakešu pārslēgšana
* datu plūsmas uzskaite
* ātrgaitas mērogojamība

**51. Kādas ir hierarhiska tīkla priekšrocības un hierarhiskā modeļa līmeņi?**

Samazināt nepieciešamību pēc visu ierīču aptaujas.

52. **Kādas būtiskas funkcijas nodrošina mūsdienu komutatori bez klasiskās kadru komutācijas?**

Nodrošina maršrutētājam līdzīgas funkcijas, tie var atbalstīt tos pašus maršrutēšanas protokolus kā tīkla rūteris. Mūsdienu komutatori, kā Layer 3 switch darbojas ar paketēm.

53. **Kas ir VLAN, kam to izmanto? īsti nezinu vai pareizi**

**virtual local area network ,** lai palielinātu drošību tīklā, regulētu datu plūsmu, notiektu dažādas piekļuves tiesības

54. **Sniegt VLAN izmantošanas piemēru!**

Piemēram pie viena switcha ir pieslēgti datori ,kurus var iedalīt 2 grupās, 1. grupa datori kurus izmanto studenti, 2. grupa datorus kurus izmanto pasniedzēji ar VLAN palīdzību var nodrošināt ka studenti nevarēs piekļūt pasniedzēju datoriem un pasniedzēji no saviem datoriem nevarēs piekļūt studentu datoriem.

**55. Kā noskaidrot vai komutators atbalsta VLAN funkcionalitāti?**

Apskatoties uzstādījumos, konfigurācijās

**56. Kas ir "trunk" tīklos kuros izmanto VLAN tehnoloģiju?**

Trunk ir protokols, kurš nesā informāciju par visiem switchiem VLAN tīklā

**57. Pēc kāda principa notiek VLAN definēšana?**

Ieraksta VLAN ID numuru un nosaukumu.

Piešķir tam portu.

Pievieno trunk ar pārējiem switchiem

58. **Kam izmanto inter-VLAN maršrutēšanu?**

Lai nodrošinātu saziņu/komunikāciju starp dažādiem VLANiem.

59. **Kas ir STP, kam tas nepieciešams?**

Spanning Tree Protocol. Izmanto Layer 2 cilpu likvidēšanai – porti, kuros atrastas cilpas, tiek izslēgti.

*Ja kas, STP ir arī Shielded Twisted Pair – ekranētais vītais pāris.*

**60. Kā noskaidrot vai komutators spēj apstrādāt Layer2 cilpas?**

**61. Kāpēc būtu nepieciešams uz maršrutētāja izmantot "sub-interfaces" kādai no Ethernet tīkla kartēm?**

**62. Kas ir NAT? Kam to izmanto?**

Tīkla protokols IPv4, kurš atļauj vairākām ierīcēm pieslēgties publiskam tīklam izmantojot vienu un to pašu IPv4 adresi.

**63. Uzskaitīt NAT izmantošanas variantus!**

Statisks NAT- ir izveidota tabulu, kurā glabājas katra lietotāja piešķirtā IP adrese ar ārējo adresi(katru adresi vajag pašam vadīt iekšā)

dinamisks NAT- Rūteris katram lietotājām piešķir adreses pats.

Vienas adreses NAT-IR tikai viena aktīva IP adrese, lai sazinātos ar internetu no citas adreses rūteris sūta pieprasījumu šādā formā x.x.x.x:y--for example, 10.0.0.1:100 would be IP address 10.0.0.1, port 100

**64 Kādi ir NAT izmantošanas galvenie ieguvumi?**

Droši vien lai atomātiski sakonektētos visi lietotāji ar internetu, bez iestatīšanas.

**65. Kas ir RIR un to funkcija?**

RIR ir reģionālais interneta reģistrs, tas ir institūts, kura galvenais uzdevums ir pāraudzīt interneta adresses attiecīgajos reģionos, viņi arī pārvalda piešķirtās IP adreses un domeinus.

**66. Kas ir un kam izmanto "port-forwarding"?**

Atļauj kādam attālākam datoram pievienoties lokālajam tīklam

**67. Kas ir ACL, kam to izmanto?**

ACL-access control list, nosaka, kuras ip adresses īpašnieki vai porta numuri drīkst piekļūt tīklam un veikt darbības

**68. Raksturot standarta ACL!**

Standarta ACL filtrē adreses pēc tā avota, tas ir tā ka viņš var atrast tikai tīkla vai hosta avotu, bet nevarēs atrast paketes galamērķi.

**69. Raksturot paplašināto "extended" ACL!**

var pārbaudīt gan galamērķi gan avota adreses

**70. Kas ir ugunsmūris, kādi principi nodrošina tā pamatfunkcionalitāti?**

Ugunsmūris ir aparatūra vai programmatūra, kura pārbauda informāciju, kas ienāk no interneta vai tīkla, un atkarībā no ugunsmūra iestatījumiem to bloķē vai arī ļauj ienākt datorā.

**71. Kāda vadlīnija jāņem vērā tīklā izvietojot standarta ACL?**

ACL ieraksti tiek pārskatīti no augšas uz leju, un kad tiek atrasts īstais vairs nekas netiek meklēts

**72. Kāda vadlīnija jāņem vērā tīklā izvietojot paplašināto "extended" ACL?**

Rūteris nevar filtrēt trafiku, kuru ir pats radījis

**73. Kādā secībā rakstīt ACL konfigurācijas ierakstus?**

R1(config)#**ip access-list standard 1**

R1(config-std-nacl)#**deny host 192.168.1.49 log**

R1(config-std-nacl)#**permit any log**

R1(config-std-nacl)#**exit**

**74. Raksturot kas tiek realizēts pasniedzēja norādītajos ACL konfigurācijas ierakstos!**

Standarta: 

Atļauj visas paketes kas nāk no 192.168.30.0/24 tīkla. Pārējās tiek bloķētas.

Paplašinātā:

Atļauj visas paketes no 192.168.30.0/24 tīkla, kas izmanto 80 TCP portu (*HTTP*). Pārējās tiek bloķētas.

**Praktiskā daļa - 1 no...**

75. PT pieslēgt un nokonfigurēt norādītajā segmentā datoru!

76. PT pieslēgt maršrutētājam jaunu LAN tīkla segmentu un nokonfigurēt statisko maršrutēšanu!

77. PT pieslēgt maršrutētājam jaunu LAN tīkla segmentu un nokonfigurēt dinamisko maršrutēšanu!

78. PT pieslēgt un nokonfigurēt tīkla segmentam DHCP serveri! Nodemonstrēt tā darbību!

79. PT pieslēgt un nokonfigurēt tīkla segmentam HTTP serveri! Nodemonstrēt tā darbību!

80. PT pieslēgt un nokonfigurēt tīkla segmentam DNS serveri! Nodemonstrēt tā darbību!

81. PT piešķirt esošam VLAN papildu porttu!

82. PT nodefinēt uz komutatora divus VLAN!

83. PT izveidot "trunk" savienojumu starp komutatoriem!

84. PT izveidot Layer2 rezerves ceļu!

85. PT izveidot Layer3 rezerves ceļu!

86. PT nokonfigurēt NAT kādam no topoloģijā norādītajiem tīkla segmentiem!

87. PT nokonfigurēt ACL, lai realizētu pasniedzēja norādītos tīkla pakalpojumu ierobežojumus!

88. PT nodrošināt savienojumu starp dažādiem VLAN!

89. Sadalīt tīklu apakštīklos pēc pasniedzēja norādījumiem! Drīkst izmantot Subnet Calculator programmatūru.

**Praktiskā daļa - visiem!**

90. PT diagnosticēt problēmu kāpēc nav sasniedzams norādītais dators!

(iespējamās problēmas: ip, gw, sm, route,port status, media u.c.) - obligāti iekļautais jautājums