**Тринадесето Национално състезание по компютърни мрежи**
**Практически казус**
**8. Април 2017**
**Време за работа: 75 минути**

Настоящият казус се състои от страници (включително тази заглавна страница) и задачи.
Общият брой точки е .
Времето за работа е 75 минути.
Настоящият казус е съобразен с програмата Packet Tracer версия 7.0
По време на работа записвайте файла си след всяка промяна.
В случай на проблем, запаметете конфигурациите на устройствата, запишете файла си и рестартирайте програмата.
Въвеждайте правилно зададените имена, пароли и съобщения, спазвайте указаните интерфейси за свързване и конфигуриране!
В противен случай автоматичната проверка няма да оцени направеното от Вас и може да доведе до излишно забавяне и объркване.
***По време на работа нямате право да използвате калкулатори.***

За всички устройства в топологията можете да използвате паролите, които са описани в Задача 1:

* Парола за привилигирован достъп **class**
* Парола за достъп през конзолната линия (console line) - **cisco**

**Задача 1.**Базова конфигурация.

Конфигурирайте базово маршрутизатор Varna:

* Име **Varna**
* Парола за привилигирован достъп **class**, съхранена след обработка с MD5 хеширащ алгоритъм.
* Парола **cisco** за достъп през конзолната линия (console line)
* Съобщение на деня с предупредителен характер **Authorized access only!**
* На интерфейс **Gigabit0/0** задайте втория използваем IPv4 адрес от транспортната мрежа Telco-Core - Varna (виж таблицата в задача [q:OSPF]).
* На интерфейс **Gigabit0/1** задайте първия използваем IPv4 адрес от локалната мрежа във Варна и първият използваем IPv6 адрес от мрежата 2001:acad:acad:1::/64 (броенето започва от 0, например нулев, първи и т.н.).

Конфигурирайте сигурен отдалечен достъп за управление на маршрутизатора чрез SSH:

* За име на домейн използвайте **13.nskm.bg**
* Генерирайте двойка публичен и частен RSA ключ с големина 2048 бита.
* Конфигурирайте версия 2 на SSH протокола.
* Създайте потребител **admin** с парола **admin321**, която да е съхранена след обработка с алгоритъма MD5.
* Конфигурирайте линиите за отдалечен достъп (vty lines) да приемат само SSH достъп, като използват локалната база с потребители.

**Задача 2.**Компанията експериментира с IPv6 свързаност в локалните мрежи в офиси Варна и Бургас. Свържете двата офиса посредством неизползваната серийна линия между тях, спазвайки следните изисквания:

* Конфигурирайте PPP протокол с CHAP автентикация между маршрутизатори Varna и Burgas. Използвайте **cisco** за парола.
* Използвайте първия адрес от мрежа 2001:acad:acad::/64 (започвайки броенето от 0) за интерфейса на маршрутизатор Varna, а за маршрутизатор Burgas - предпоследния.
* Конфигурирайте EIGRP, използвайки 64512 за номер на автономната система, така че компютрите в двата офиса да имат IPv6 свързаност помежду си.

**Задача 3.**Осигурете свързаност на компютър PC-IT и сървър Web. За целта са възможни два подхода.

Открийте и отстранете проблемите свързани с EIGRP в конфигурацията на маршрутизатор Operations. Конфигурирайте тунел между маршрутизатори IT и HQ и през него конфигурирайте път по подразбиране за маршрутизатор IT с административна дистанция 100 . В статичния път използвайте адреса на следващия маршрутизатор по пътя. Конфигурацията на тунела от страната на маршрутизатор HQ е завършена (не изисква промени), целта е маршруитзатор IT да получи конфигурация, чрез която да може да изгради тунел с маршрутизатор IT.

За осигуряване на желаната свързаност е достатъчно да се изпълни или условие (а) или условие (б). Намирането на решение и на двата проблема води до присъждане на 20 точки за задачата. Решението само на условие (а) или (б) носи съответно 15 или 10 точки.

**Задача 4.**Конфигурирайте комутаторите Telco-Core, Telco-North и Telco-South спрямо следните изисквания:

* Създайте следните виртуални мрежи на трите комутатора:

| **Номер на VLAN** | **Име на VLAN** | **Адресно пространство** |
| --- | --- | --- |
| 10 | Varna | 172.16.10.0/30 |
| 20 | Burgas | 172.16.20.0/30 |
| 30 | SOHO | 172.16.30.128/28 |
| 100 | HQ | 172.16.100.0/30 |
| 200 | Management | 172.16.200.0/25 |
| 999 | Blackhole | — |

* Конфигурирайте SVI интерфейси на комутатор Telco-Core във VLAN Varna, Burgas, HQ и Management. Използвайте първия възможен адрес от съответната мрежа.
* Конфигурирайте интерфейси за управление на комутатори Telco-North и Telco-South във VLAN Management. Използвайте съответно предпоследния и последния използваем адрес от съответната мрежа. Уверете се, че комутаторите ще бъдат достижими от отдалечени мрежи, като за шлюз по подразбиране използвайте адреса на комутатор Telco-Core в същия VLAN.
* Агрегирайте връзките Fa0/3 и Fa0/4 между комутаторите Telco-North и Telco-South в **Portchannel 1**, така че и двете страни да опитат договаряне с Link Aggregation Control Protocol.
* Конфигурирайте в режим “trunk” следните интерфейси, като използвате VLAN 999 за “native”, спрете DTP и позволите само VLAN-ите с адресно пространство, посочени в таблицата в началото на въпроса, да преминават през тях:

| **Комутатор** | **Интерфейс** |
| --- | --- |
| Telco-Core | Fa0/1, Fa0/2, Gi0/1 |
| Telco-North | Fa0/1, Po1 |
| Telco-South | Fa0/2, Po1 |

* Според таблицата конфигурирайте в подходящ режим съответните портове на комутаторите и ги присъединете към определените виртуални мрежи:

|  | **VLAN 10** | **VLAN 10** | **VLAN 20** | **VLAN 999** |
| --- | --- | --- | --- | --- |
| Telco-North | Fa0/24 |  |  | Всички неизползвани портове |
| Telco-South |  | Fa0/24 |  | Всички неизползвани портове |
| Telco-Core |  |  | Fa0/24 | Всички неизползвани портове |

* На трите комутатора спрете динамичния режим на портовете, които не са членове на нито една от използваните виртуални мрежи, и ги изключете.

**Задача 5.**Довършете конфигурацията на маршрутизатор HQ спрямо следните изисквания:

* Интерфейс **Gigabit0/1** конфигурирайте като “trunk”.
* Създайте подинтерфейси във VLAN 30 и 100 и ги конфигурирайте с последните използваеми адреси в съответните мрежи от таблицата в задача [q:OSPF].

**Задача 6.**Конфигурирайте OSPF в зона 0 и процес 1 за маршрутизаторите и мрежите описани в таблицата:

| **Устройство** | **Мрежа** | **Описание** |
| --- | --- | --- |
| HQ | 172.16.30.128/28 | Транспортна мрежа HQ - SOHO |
| HQ | 172.16.100.0/30 | Транспортна мрежа Telco-Core - HQ |
| Telco-Core | 172.16.10.0/30 | Транспортна мрежа Telco-Core - Varna |
| Telco-Core | 172.16.20.0/30 | Транспортна мрежа Telco-Core - Burgas |
| Telco-Core | 172.16.100.0/30 | Транспортна мрежа Telco-Core - HQ |
| Telco-Core | 172.16.200.0/25 | Management мрежа |
| Varna | 172.16.10.0/30 | Транспортна мрежа Telco-Core - Varna |
| Varna | 172.16.11.0/24 | Локална мрежа Варна |
| Burgas | 172.16.20.0/30 | Транспортна мрежа Telco-Core - Burgas |
| Burgas | 172.16.21.0/24 | Локална мрежа Бургас |

* Обявете съществуващия на маршрутизатор HQ път по подразбиране в OSPF процеса.
* Погрижете се маршрутизатори HQ, Varna и Burgas никога да не участват в избора на DR и BDR в OSPF процеса.

**Задача 7.**Конфигурирайте маршрутизатор Varna да работи като DHCP сървър за локалните мрежи в офисите Варна и Бургас според таблицата към задача [q:OSPF]. За имена на DHCP адресните пространства използвайте съответно **Varna** и **Burgas** Започнете раздаването от десетия използваем адрес и конфигурирайте да бъдат раздавани не повече от 100 адреса. Настройте маршрутизаторBurgas да пренасочва DHCP заявките от локаната си мрежа към по-близкия до него интерфейс на маршрутизатор Varna.

**Задача 8.**Защитете портовете на комутаторите в офисите Варна и Бургас, в които са включени компютри. Позволете максимум 10 MAC адреса на порт. Изберете такъв режим на защита, при който в случай на нарушение портът блокира нерегламентирания трафик и остава включен, без да генерира Syslog съобщения. Подсигурете физическите адреси на компютрите да присъстват в текущата конфигурация на комутатора. Изключете всички неизползвани портове.

**Задача 9.**Конфигурирайте **Rapid STP** на комутаторите Telco-HQ, Telco-North и Telco-South така че да постигнете посочените по-долу приоритети. Конфигурирайте портове Fa0/24 на устройствата като “edge” портове.

| **Комутатор** | **VLAN 10** | **VLAN 20** | **VLAN 30** | **VLAN 100** | **VLAN 200** |
| --- | --- | --- | --- | --- | --- |
| Telco-Core | 32778 | 32788 | 4126 | 4196 | 4296 |
| Telco-North | 4106 | 8212 | 20510 | 24676 | 28872 |
| Telco-South | 8202 | 4116 | 24606 | 28772 | 20680 |

**Задача 10.**Конфигурирайте безжичния маршрутизатор SOHO, както следва:

* Конфигурирайте статично получаване на адрес за Internet интерфейса. IP адресът е осмият използваем от мрежата, в която е свързан Internet интерфейса на безжичния маршрутизатор, като Default Gateway е съответният интерфейс на HQ
* За вътрешната мрежа, конфигурирайте следните настройки:
	+ Вътрешния интерфейс с адрес и маска: **172.16.40.1/24**.
	+ Динамично раздаване на адреси, започващо от **172.16.40.10**.
	+ Максимален брой адреси за раздаване: **90**.
	+ Включете възможността за отдалечено конфигуриране на маршрутизатора, като използвате парола **cisco123**.
* За безжичната мрежа, конфигурирайте следните настройки:
	+ Име на безжичната мрежа (SSID): **NetRocks** с възможност за изпращане на “beacons”
	+ Алгоритъм за защита WPA2 Personal с парола (Passphrase): **cisco123** безжична свързаност на Mobile-Worker към маршрутизатора SOHO.

**Задача 11.**Конфигурирайте NAT правила за трафика, прекосяващ маршрутизатор HQ според следните изисквания:

* Конфигурирайте интерфейсите на маршрутизатора като вътрешни или външни за NAT според това дали са конфигурирани с публичен или частен IP адрес.
* Създайте стандартен, наименован списък за контрол на достъпа (ACL) с име **NAT-ACL**. В него с единствено твърдение (entry) обобщете адресите, необходими на офисите Варна, Бургас и безжичните клиенти на SOHO маршрутизатора.
* Създайте NAT правила, които да транслират трафика от адресите в гореописания списък за контрол на достъпа с адреса на изходящия интерфейс.
* Уверете се, че имате достъп от компютрите PC-Varna, PC-Burgas и Mobile-Worker както до PC-IT, така и до сървър Web

**Задача 12.**Конфигурирайте списък за контрол на достъпа на маршрутизатор HQ според следните изисквания:

* Дефинирайте разширен списък за контрол на достъпа с име **Block-Mobile**.
* На компютрите, клиенти на безжичната мрежа, предоставяна от SOHO маршрутизатора, забранете SSH достъпа до Management мрежата. Правилото не трябва да засяга останалия трафик.
* Приложете списъкът на най-подходящия интерфейс на маршрутизатора спрямо най-добрите практики.