Secțiunea rețele de calculatoare, clasele 9 - 10

Înainte de a începe rezolvarea subiectelor va trebui să semnați digital activitatea Packet Tracer atașată cu numele vostru.

Din Meniul *Options* selectați *User Profile* (sau Ctrl+Shift+u) și introduceți:

- Numele vostru complet în câmpul de nume.
- Orașul și liceul vostru în câmpul *Additional Info*.
  (adresa de email este opțională)

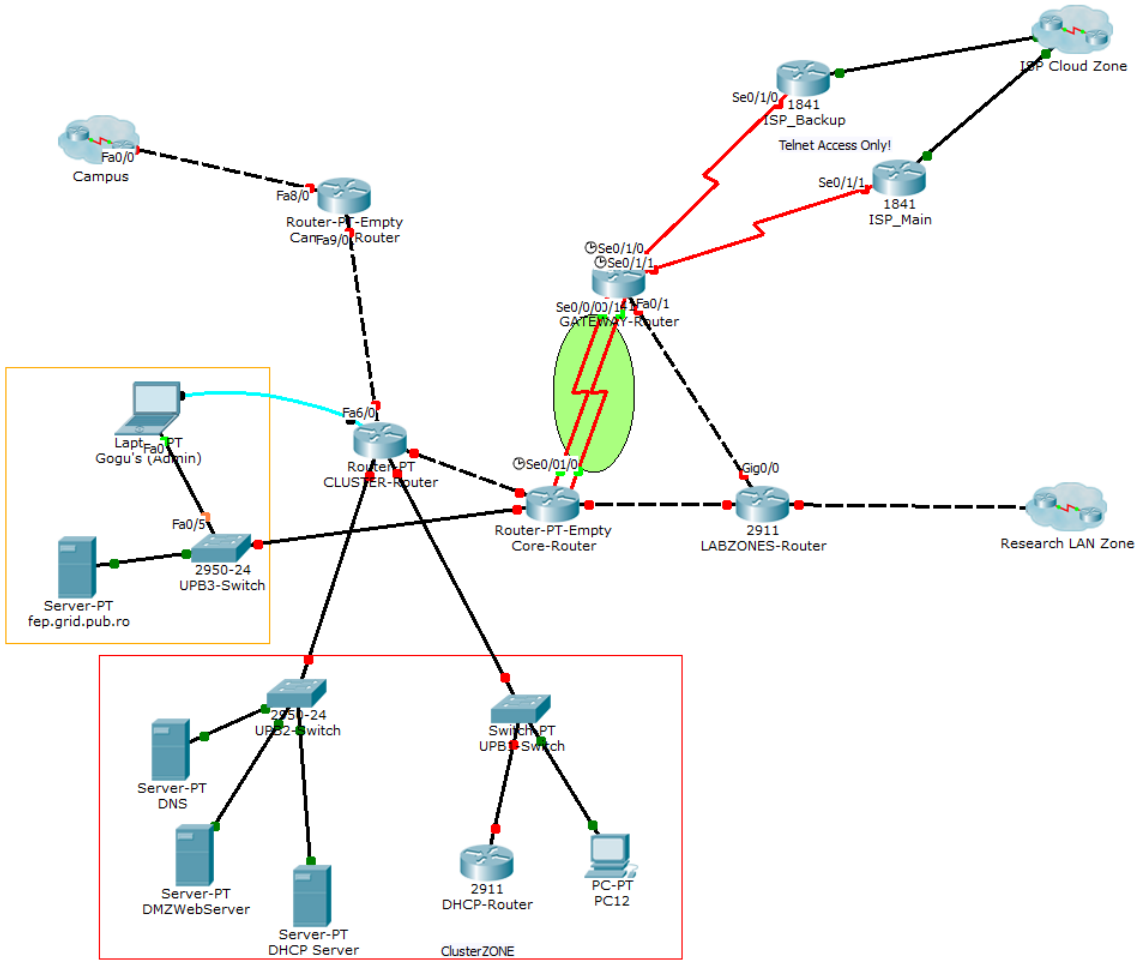
Odată ce apăsați OK, activitatea se resetează și veți pierde tot ce ați lucrat până în acest moment.

Atenție !

- Nu aveţi voie să utilizaţi telefonul mobil, PDA-ul sau orice alt dispozitiv electronic.
- Salvați frecvent progresul vostru, atât pe echipamentele virtuale, cât și pe fișierul cu activitatea voastră. Încărcați fișierul în locul specificat de pe *www.acadnet.ro* pentru a vă asigura că aveți o copie sigură și acolo. Va fi luată în considerare doar ultima variantă trimisă. Dacă are loc o cădere de curent sau alt eveniment neprevăzut riscați ***să pierdeți tot ce ați lucrat până la acel moment!***
- Este recomandat să utilizaţi facilitatea de help a IOS-ului (prin tasta **?**), autocomplete-ul (prin tasta TAB), comenzile *show* şi *debug*.
- Înainte de a declara o cerinţă terminată faceţi verificări pentru a fi siguri că aţi rezolvat corect subiectul.
- Verificaţi configuraţia iniţială a echipamentelor înainte de a începe lucrul.
- Nu aveţi voie să utilizaţi nici un alt site în afara celui oficial, *www.acadnet.ro*.
- Acolo unde vi se cere setarea sau folosirea unei parole sau a unei chei folosiți „**acadnet**”. Orice altă parolă folosită va rezulta în imposibilitatea validării exercițiului și în ***pierderea întregului punctaj pe acel exercițiu!***

Mult succes!

Timp de lucru: 120 min.
Punctaj maxim: 130 puncte


ISP Cloud Zone
Se0/1/0
1841
ISP_Backup
Telnet Access Only!
Se0/1/1
1841
ISP_Main
Fa0/0
Campus
Fa8/0
Router-PT-Empty
Fa9/0
Se0/1/0
Se0/1/1
Se0/0/0
Fa0/1
GATEWAY-Router
Fa6/0
Router-PT
CLUSTER-Router
Se0/0/1
Gig0/0
Router-PT-Empty
Core-Router
2911
LABZONES-Router
Research LAN Zone
Fa0/5
2950-24
UPB3-Switch
Server-PT
fep.grid.pub.ro
Server-PT
DNS
Server-PT
DMZWebServer
Server-PT
DHCP Server
2911
DHCP-Router
PC-PT
PC12
ClusterZONE

Subiectul 1 - The Initial Sorcery

- Acomodează-te cu topologia și cu zonele în care ea este împărțită.
- Acum este momentul să adresezi supraveghetorilor primele nelămuriri (dacă există) despre formularea cerințelor.
- Aţi fost desemnat să fiţi administrator de reţea pentru topolgia curentă. Unul dintre primele taskuri este să realizaţi recuperarea parolei (prin schimbare) în zona ClusterZone pe Routerul CLUSTER-Router prin consolă, întucât trebuie să puteţi accesa toate echipamentele.
- Celelalte configurații de pe router trebuie să rămână neschimbate momentan.

Subiectul 2 - Name the Gods

Subnetaţi cât mai optim spaţiul de adresă **141.141.128.0/18** astfel încât să se respecte cerinţele menţionate în tabelul de mai jos.

Zona	Subzona	Număr de adrese utilizabile necesare	Observații
Campus	Mediator Zone	1022	
	Hostpot	5	Nu se referă la zona de NAT
Research LAN Zone	East Reseach Zone	56	DHCP
	West Research Zone	63	DHCP
	Admin Zone	60	DHCP
	Special Zone	75	DHCP
Cluster Zone	Servers	53	Subrețeaua ce cuprinde cele 3 servere
	FEP	241	Subreteaua serverului fep.grid.pub.ro
	DHCP	126	

Subnetarea se va realiza cât mai eficient posibil, în ordine descrescătoare a numărului de hosturi, începând cu primele adrese disponibile. Pentru reţelele punct-la-punct se vor aloca ultimele reţele disponibile, descrescator, urmărind topologia de la stânga la dreapta. Numărul de adrese utilizabile (din tabel) **include** și adresa default-gateway-ului.

Asignaţi IP-uri pe echipamente, urmărind regulile şi excepţiile.

Excepţii:

a. Echipamentele din Reserch LAN Zone vor primi IP-uri prin DHCP, având ca server DHCP serverul local din Admin Zone
b. Zona ISP Cloud Zone a fost preconfigurată pentru voi
c. Capetele interfeţelor seriale de pe ISP_Main şi ISP_Backup au fost configurate cu IP-uri dintr-o clasă pe care va trebui să o aflaţi mai tarziu.

d. Interfeţele seriale dintre routerul GATEWAY-Router şi CORE-Router au fost configurate.

Regulile de asignare a IP-urilor pe echipamente sunt următoarele.

1. Dacă există servere în reţea, acestea vor avea primele adrese folosite din subreţea - prioritate 1 - prioritate maximă
2. Dacă există rutere, acestea vor avea prioritate 2.
3. Hosturile vor avea ultimele adrese alocabile, indiferent de prioritate şi de ce alte echipamente există în subreţea.
4. Dacă există mai multe echipamente de acelaşi tip în aceeaşi subreţea, primul IP se va aloca echipamentului de mai la stânga şi celui mai de sus.

Subiectul 3 - The First Enlightenment

Realizaţi configurări iniţiale, pentru toate echipamentele de rețea din topologie, exceptând echipamentele din zona ISP Cloud Zone:

- Configurați hostname (identic cu cel afișat pe topologie, Ex: pentru R1 hostname=R1)
- Configurați parola (secret) pe modul EXEC.
- Configurați parola pe linia de consolă și pe liniile VTY. Activați cererea parolei la accesarea lor.
- Activați sincronizarea mesajele pe linia de consolă de la sistemul de operare.
- Dezactivați căutarea DNS.

Subietul 4 - Crack the Research Zone:

Asiguraţi-vă că LABZONES-Router şi RESEARCH-Router vor forma adiacenţă EIGRP AS 200 astfel încât LABZONES-Router să afle de reţelele acomodate de RESEARCH-Router, respecând următoarele:

1. Asiguraţi-vă că echipamentele terminale primesc IP prin DHCP de pe Serverul din aceeasi zona, DHCP-Server. Configuraţi serverul de DHCP.

2. Routerul REASERCH-Router va trimite una sau mai multe rute sumarizate eficient pe interfața conectată la LABZONES-Router

3. Configuraţi o rută default către routerul ISP_Main de pe LABZONES-Router

4. Redistribuiţi ruta default de pe LABZONES-Router în EIGRP astfel încât să ajungă la RESEARCH-Router.

5. Pasivizaţi interfeţele pe care consideraţi necesar să nu ajungă updateuri de rutare.

Subiectul 5 - The Mighty Catch:

Zona **ISP Cloud Zone** a fost preconfigurată pentru voi cu IP-uri din poolul **200.200.200.208/18.** NU aveţi acces la echipamentele din această zonă decât remote, prin telnet. Dacă aţi configurat corect adresarea reţelei, vă veţi putea conecta prin telnet pe routerele ISP_Main şi ISP_Backup.

Inspectaţi protocoalele de rutare care rulează în zona.

1. Inspectaţi DR-ul şi BDR-ul din zona de OSPF. Asiguraţi-vă că DR-ul va fi întotdeauna ISP_Main.

2. Asiguraţi-vă că routerul FarAway nu va participa la procesul de alegere DR BDR

3. Routerul Cr01 nu formează adiacentă cu restul routerelor. Aflaţi de ce şi faceţi modificările necesare astfel încat să se formeze adiacenţa.

4. Asiguraţi-vă că se realizează equal cost load balancing în OSPF, între routerele Ultimate-Router şi Route-Sever, care au direct conectate trei legături.

5. Asiguraţi-vă că interfeţele de Loopback din această zonă nu primesc update-uri OSPF, dar reţelele corespunzătoare sunt anunţate, ca şi până acum în procesul de OSPF.

Subiectul 6 – NAT for Guests:

În zona de Hotspot a Campusului, folosiți un spațiu de **adrese private** la alegere pentru a asigura, cu un număr minim de adrese publice alocate, accesul utilizatorilor la Internet.

- Capacitatea maximă a NAT-ului este de 1000 de utilizatori

- Adresarea end-device-urilor se va face dinamic, folosind ca DHCP-server routerul DHCP-Router din ClusterZone.

- Adresele IP private nu se vor anunța în cadrul niciunui protocol de rutare și nu vor apărea sub nicio formă în tabelele de rutare a celorlalte routere.

Subiectul 7 – ACLs That Keep The Hackers Out:

Pentru securitatea rețelei, implementați următoarele politici:

- Utilizatorii din zona de Hotspot a campusului pot accesa numai resursele web publice (din Internet sau oferite de către serverul DMZWebServer). Accesul la toate serviciile ce

nu contribuie la asigurarea acestei facilități va fi restricționat într-un mod cât mai eficient.

- Accesul la clusterul fep.grid.pub.ro se va putea face doar prin SSH/Telnet, numai din zonele de Campus și LabZone (nu și din Internet).
- Din zona administratorului de sistem, toate serviciile vor fi accesibile, în pofida oricărei alte politici impuse.
- Analizați topologia pentru posibile politici reziduale (din cadrul configurației inițiale) care se suprapun cu cele de mai sus și corectați-le.

Subiectul 8 – Oh, infamous deeds :

Configuraţi următoarele, în zona ClusterZone:

1. Folosind protocolul OSPF asiguraţi-vă că aveţi conectivitate între toate echipamentele din zona ClusterZone. Folosiţi area 245.
2. Pasivizaţi interfeţele care se concteză la echipamente terminale şi unde nu este necesar să ajungă update-uri de routare.
3. Configuraţi routerul CORE-Router cu o rută default către GATEWAY-Router, pe seriala Serial0/1/1. Aveţi grijă ca această rută să fie redistribuită în OSPF Area 245.
4. Configuraţi serverul DNS astfel încât să realizeze translatarea DNS a adreselor pentru serverele fep.grid.pub.ro şi DMZWebServer.pub.ro

Subiectul 9 – Accessing the WAN:

Configurați conexiunea către ISP astfel încât legătura dintre Gateway și ISP_Backup să rămână inactivă (cel puțin din punctul de vedere a traficului împins) atât timp cât legătura dintre ISP_Main este funcțională. ISP-ul cunoaște deja zona de IP-uri alocate rețelei și redirecționează în mod corespunzător traficul către rețeaua locală.

Subiectul 10 – This bag is not connected yet:

Asiguraţi conectivitatea end-to-end a echipamentelor, luând în considerare următoarii paşi:

1. Inspectaţi legăturile Seriale dintre CORE-Router şi GATEWAY-Router şi rezolvaţi problemele de conectivitate dintre acestea.

2. Pentru a asigura conectivitatea între zonele principale, folosiţi RIPv2 cu autentificare MD5 între CAMPUS-Router, CLUSTER-Router, CORE-Router, LABZONES-Router şi GATEWAY-Router.

3. Asiguraţi conectivitatea end-to-end folosind alte rute rute statice sau default, dacă este necesar, fără a modifica configuraţiile realizate până acum.