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.

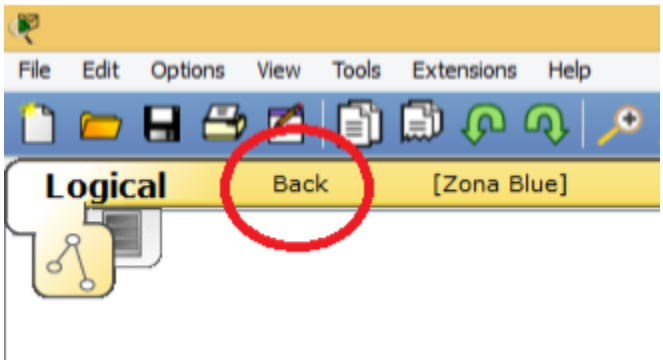
Atenție !

- 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*.

Mult succes!

Timp de lucru: 120 min.
Punctaj maxim: 100 puncte

Hint: Pentru a vedea echipamentele dintr-o zonă(cluster), selectați norișorul din interiorul zonei pe care doriți sa o vizualizați. Pentru a reveni la topologia initiala, dați click pe „Back" în colțul din stânga sus ca in ilustrația de mai jos:



Subiectul 1 – Pentagon Inc.

- Firma Pentagon Inc. și-a extins rețeaua cu un nou back-bone ultra-performant (cu fibră optică).
- Din eroarea unui administrator de rețea (aproape) toate configurațiile s-au pierdut.
- Sarcina voastră este să le refaceți, plecând de la un set de specificații.
- Studiați topologia și zonele în care ea este împărțită.
- Dacă există nelămuriri cu privire la topologie sau subiecte, adresați supraveghetorilor întrebări referitoare la acestea.
- **Atenție! Citiți cu atenție întregul text al unui exercițiu înainte de a-l rezolva. De cele mai multe ori există exemple pentru a clarifica cerințele sau există hint-uri pentru a vă conduce spre intuirea rezolvării.**

Subiectul 2 – Configurări de bază

- **Pe routerele din zona principală** (cele 5 routere de la R1 la R5) trebuie să:
  - Configurați hostname-ul (identic cu cel afișat pe topologie, Ex: pentru **R1** hostname=**R1**).
  - Configurați parola (secret) "**acadnet**" pe modul EXEC.
  - Configurați parola "**acadnet**" pe linia de consolă.
  - Configurați conectarea pe primele 7 linii VTY folosind userul **„admin"** și parola „**P3nt4g0n**"
  - Activați sincronizarea mesajelor pe linia de consolă de la sistemul de operare.
  - Dezactivați căutarea DNS.

Subiectul 3 – Subnetare

Zona	Subzona	Număr de host-uri	Observații
FinancialLayer	Angajați	40	-
	Guests	102	-
	Servers	5	-
CommunityZone	-	10	-
WorkZone	VLAN 100 - R&D	64	Se vor configura pe WorkRouter folosind Router-on-A-Stick
	VLAN 200 - IoT	26	
	VLAN 300 - Platform Analysis	100	
	VLAN 400 - Datacenter Solutions	15	Se vor configura pe WestLegacy Router folosind metoda clasică de inter-VLAN Routing
	VLAN 500 - HR	6	
Ultra-Secure	SQL Servers	7	-
	Data	12	-

- Pentru toate subneturile numărul de hosturi se referă la stațiile / device-urile terminale conectate în rețea.
- Prima adresă IP din fiecare subnet va fi rezervată pentru Default Gateway.
- DNS server, pentru toate device-urile va fi **10.0.2.58**.
- Subnetarea se face pe **10.0.0.0/8**

Subnetarea se va realiza cât mai eficient posibil, în ordine descrescătoare a numărului de hosturi, începând cu primele adrese disponibile. Numărul de adrese utilizabile (din tabel) **include** și adresa default-gateway-ului.

(Dacă aveți nelămuriri legat de această precizare, supraveghetorul vă poate da mai multe detalii.)

Subiectul 4 – Configurare adrese IP

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

1. Interfețele routerelor care sunt default gateway pentru rețeaua lor vor avea primul IP utilizabil din subnetul respectiv.

De exemplu: Pentru rețeaua **Data** (din **Ultra-Secure Zone**) din dreapta Routerului RSafe se comporta ca default gateway pentru hosturile din subrețeaua legate la Fa2/0 deci i se va da primul IP utilizabil.

2. Hosturile vor avea adresele imediat următoare, în corespondență cu indicele din numele lor.
3. Hosturile care în locul indice au specificat în nume identificatorul N, vor avea ultima adresă asignabilă din subnet.

Spre exemplu: În această zonă PC-ul 1 va avea alocată a 2-a adresă utilizabilă, PC2 a 3-a adresă, iar PCn ultima adresă asignabilă.

Configurați adrese IP pe routere și stații conform cu regulile de mai sus!

HINT: Legăturile dintre Routere sunt deja configurate (excepție R5-ISP)
HINT: Anumite configurări pe echipamente sunt de asemenea făcute

Excepţii:

1. Echipamentele din **Community Zone** primi adrese IP dintr-o zonă de adrese private prin DHCP.
2. Toate echipamentele din **ISP** sunt deja preconfigurate pentru voi. Conectarea către ISP se face printr-o subnet **/30** nedocumentat. Pentru aflarea acesteia va trebui să folosiți **CDP**.
3. Echipamentele din Subzona Guests din zona Financiar își vor lua adresele IP prin DHCP de la serverul de DHCP din zonă. (Atenție: adresa de pe router trebuie configurată de voi)
4. Interfețele routerelor din WorkZone către rețele vor fi configurate în modul următor: WorkRouter va avea interfața în modul router on a stick cu vlan-urile 100,200 și 300; WestLegacyRouter va avea fiecare interfața în modul access pentru vlan-urile 400 și 500.

Subiectul 5 – Community Zone

- În pauzele de lucru, programatorii Pentagon Inc. depedenți de Internet se relaxează în zona de Community. Aici există o rețea largă de AP-uri open, pentru ca semnalul Wi-fi să fie mereu bun.

- Problema semnalată este că, atunci când un număr mare de leneși se strâng în zona de Community pool-ul de IP-uri se epuizează și nu se mai pot conecta utilizatori noi.

- Pentru a rezolva problema, trebuie să configurați DHCP pe CommunityNatRouter folosind adrese IP din zona **192.0.0.0/10** pentru a fi date in rețea.

- Configurați NAT pentru rețeaua transmisă prin DHCP, astfel încât ruterul să poată suporte 70000 de conexiuni simultan. Puteți folosi adrese din zona 12.0.0.0/8 pentru zona de outside.

Detalii DHCP:

- Pool-ul DHCP va include toate adresele din LAN-ul cu același nume, exceptând adresa routerului. Denumirea acestuia rămâne la alegerea voastră.
- Odată cu configurațiile de IP și Mască de rețea host-urile vor primi și adresa default gateway și a serverului de DNS.
- DNS-ul va fi **10.0.2.58**.

Subiectul 6 – Security for Financial Zone

Într-un mod nefericit, departamentul de financiar al firmei se învecinează cu serverul public de Web și zona pentru vizitatori.

Din acest motiv, este necesar să folosim ACL-uri pentru a asigura controlul accesului în această zonă.

Ruter Financiar are deja configurate ACL-uri. Faceti configuratile necesare fară a șterge sau a adăuga comenzi pe interfețe, astfel încât comportamentul obținut să fie cel descris în afirmațiile următoare:

- Toată lumea trebuie să aibă acces la **DNS** și **Public Web**.
- Angajații din zona Financiar trebuie să fie singurii ce au acces la serverul Financiar.
- LazyGuy este un angajat al departamentului Financiar, care însă pierde mult timp accesând site-ul public al companiei. El nu va mai avea acces la serverul public de web.

Subiectul 7 – Work Zone

- Zona **Work Zone** este compusă din mai multe departamente ale căror fluxuri de trafic trebuie izolate folosind VLAN-uri.
- Schema de adresare este cea specificată la **subpunctul 2**.
- Pentru configurarea Inter-VLAN Routing veți folosi:

– Router-on-a-Stick pentru rețelele direct conectate la routerul WorkRouter

- Metoda Legacy (folosind interfețe în modul access) pentru rețelele conectate la routerul WestLegacyRouter.

Toate legăturile trebuie configurate în modul corespunzător, pentru a asigura funcționarea rețelei. Legăturile de tip trunk vor permite doar VLAN-urile necesare.

- Respectarea ID-urilor VLAN-urilor este obligatorie.
- Nu este obligatoriu sa setați numele VLAN-urilor.
- Pentru realizarea conectivității între rețelele acestei zone folosiți un protocol de rutare (diferit de OSPF) la alegerea voastră.

Subiectul 8 – Port Security

Configurati in zona Ultra-Secure Zone:

- Switch-ul 3 astfel încat SqlServer 1 să fie singurul aparat care poate fi conectat la portul Fa0/2 al switch-ului.
- Switch-ul 9 astfel încât pe portul Fa0/2 sa se conecteze maxim 2 aparate diferite, și in caz de acest număr este depășit portul sa se închidă.

Subiectul 9 - ISP

- Routerului R5 îi vei configura o rută default către Internet/ISP (specificată prin intermediul interfeței de ieșire).
- Configurația OSPF peste routerele din rețea astfel încât sa avem conectivitate end-to-end, unde nu este limitata de exercițiile anterioare.
- Propagați ruta definită mai sus în rețea.

Subiectul 10 – TROUBLE

La acest exercițiu va trebuie să rezolvați anumite probleme apărute în rețeaua voastră datorită unor configurări eronate. Erorile sunt enumerate mai jos:

- În zona Ultra-Secure Zone DataPC1 nu are acces în afara rețelei
- În zona Work Zone legătura între Switch8 și Switch10 este down
- În zona WorkZone IoT1 nu poate comunica cu restul echipamentelor
- Echipamentele din zona **Community Zone** nu pot comunica cu echipamentele din celelalte zone