Secțiunea rețele de calculatoare, clasele 11 - 12

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

NOTA: Ce nu este îngroșat în tabel este deja configurat în topologia inițială.

Echipament	Interfața	Adresa IP	Masca de rețea	Default Gateway
S11	**VLAN 11**	**10.10.11.11**	**255.255.255.192**	**10.10.11.1**
S12	**VLAN 11**	**10.10.11.12**	**255.255.255.192**	**10.10.11.1**
S13	**VLAN 11**	**10.10.11.13**	**255.255.255.192**	**10.10.11.1**
S14	**VLAN 11**	**10.10.11.14**	**255.255.255.192**	**10.10.11.1**
R1	**Gig0/0.8**	**10.10.8.1**	**255.255.255.0**	**N/A**
R1	**Gig0/0.9**	**10.10.9.1**	**255.255.255.0**	**N/A**
R1	**Gig0/0.10**	**10.10.10.1**	**255.255.255.128**	**N/A**
R1	**Gig0/0.11**	**10.10.11.1**	**255.255.255.192**	**N/A**
R1	**Se0/0/0.2**	**172.16.12.1**	**255.255.255.252**	**N/A**
R1	**Se0/0/0.3**	**172.16.13.1**	**255.255.255.252**	**N/A**
R2	G0/0	172.16.32.1	255.255.255.0	N/A
R2	Loopback0	172.16.40.1	255.255.255.0	N/A
R2	**Se0/0/0.1**	**172.16.12.2**	**255.255.255.252**	**N/A**
R2	**Se0/0/0.3**	**172.16.23.1**	**255.255.255.252**	**N/A**
R3	**Se0/0/0.1**	**172.16.13.2**	**255.255.255.252**	**N/A**
R3	**Se0/0/0.2**	**172.16.23.2**	**255.255.255.252**	**N/A**
R3	**Se0/0/1**	**141.85.85.2**	**255.255.255.252**	**N/A**
PC0	FastEthernet	10.10.8.254	255.255.255.0	10.10.8.1
PC1	FastEthernet	10.10.9.254	255.255.255.0	10.10.9.1
PC2	**FastEthernet**	**DHCP**	**DHCP**	**DHCP**
PC3	**FastEthernet**	**DHCP**	**DHCP**	**DHCP**
Laptop	**FastEthernet**	**DHCP**	**DHCP**	**DHCP**
WebServer	FastEthernet	172.16.32.2	255.255.255.0	172.16.32.1
DNSServer	FastEthernet	172.16.32.3	255.255.255.0	172.16.32.1
cisco.com	FastEthernet	141.85.85.6	255.255.255.252	141.85.85.5
R4	S1/0	??	255.255.255.252	N/A
Teleworker	FastEthernet	??	255.255.255.0	N/A

A. Configurarea VLAN-urilor

1. Pe fiecare din switch-urile S11, S12, S13 și S14 creați VLAN-urile 8, 9, 10 și 11, denumindu-le și configurându-le pe interfețele Fa0/6-24 în modul access, conform tabelului:

VLAN	Nume	Porturi de acces asociate pe S11-S14	Retea asociata
8	IT	FastEthernet 0/17-24	10.10.8.0/24
9	Sales	FastEthernet 0/9-16	10.10.9.0/24
10	Native	Nativ pe trunk-uri	10.10.10.0/25
11	Management	Fa0/6-8	10.10.11.0/26

2. Configurați interfața de management și adresa de default gateway pentru fiecare dintre S11, S12, S13, respectiv S14, conform tabelului de adrese IP.

B. Securizarea switchurilor din rețeaua locală

1. Securizați accesul la S11 și S12 astfel:

- accesul pe liniile VTY să fie posibil exclusiv prin SSH cu următoarele setări:
  - nume de domeniu **acadnet.ro**
  - user **Admin** și parola **letmein**
  - cheie de lungime minimă **1024**
  - SSH versiunea 2
  - maxim 2 încercări de introducere a parolei în SSH
  - timeout de 60 de secunde la autentificare eșuată în SSH
- parola secretă de intrare în modul privilegiat să fie cisco
- parolele din configurația curentă să apară criptate

Testați conectarea prin SSH între oricare două switch-uri, folosind adresele IP configurate pe interfețele de management la subiectul **A**.

2. Securizați porturile de acces din intervalul Fa0/6-24 de pe S13 și S14, astfel încât:

- să poată fi învățate maxim 2 adrese MAC pe fiecare port de acces
- adresele MAC învățate să fie salvate în configurația switch-ului
- la tentativa de a încălca această politică de securitate, portul să arunce traficul de la adresa MAC care încălca politica și să emită un avertisment în consola administratorului
- Porturile de acces care nu sunt conectate la niciun echipament trebuie să fie închise administrativ.

C. Configurarea EtherChannel

1. Configurați pe S11, S12, S13 și S14 interfețele FastEthernet0/1-4 și Gigabit0/1-2 în modul trunk, cu VLAN-ul nativ 10. Permiteți explicit numai VLAN-urile prezente în tabelul de mai sus pe aceste interfețe de trunk.

2. Configurați interfețele de trunk ale S11-14 astfel încât să **negocieze PortChannel LACP** cu switchurile adiacente, ca în tabelul de mai jos. Porturile PortChannel rezultate trebuie configurate în modul trunk cu VLAN-ul nativ 10, permițând explicit numai VLAN-urile 8, 9, 10, 11.

IMPORTANT! Pentru ca interfețele fizice de trunk să nu fie dezactivate pe timpul configurării pe caz de eroare (inconsistența temporară a PortChannel cu interfețele fizice), dați comanda "shutdown" pentru a le dezactiva manual și abia la terminarea configurațiilor de EtherChannel reactivați-le cu "no shutdown".

PortChannel	Porturi echipament	Porturi echipament
1	S11: Fa0/1, Fa0/2	S12: Fa0/1, Fa0/2
2	S13: F0/1, Fa0/2	S14: Fa0/1, Fa0/2
3	S11: Gi0/1, Gi0/2	S13: Gi0/1, Gi0/2
4	S12: Fa0/3, Fa0/4	S13: Fa0/3, Fa0/4
5	S11: Fa0/3, Fa0/4	S14: Fa0/3, Fa0/4
6	S12: Gi0/1, Gi0/2	S14: Gi0/1, Gi0/2

D. Spanning Tree Protocol peste EtherChannel

1. Configurați STP în modul Rapid PVST+ pe switch-urile S11-14.

2. Configurați STP pentru load-balancing între S11 și S12. Pentru asta, urmăriți ca:
   - S11 să fie root bridge pentru VLAN-urile 8 și 10
   - S11 să fie secondary root bridge pentru VLAN-urile 9 și 11
   - S12 să fie root bridge pentru VLAN-urile 9 și 11
   - S12 să fie secondary root bridge pentru VLAN-urile 8 și 10

3. Configurați porturile de acces active pe S13 și S14 astfel încât tranziția la starea de forwarding să fie mai accelerată în STP (ajutând la scăderea timpului de conectare la rețea a End-device-urilor).

4. Configurați porturile de acces active pe S13 și S14 astfel încât să fie blocate la primirea unui Bridge Packet Data Unit (BPDU), pentru a preveni atacuri asupra algoritmului STP din partea unui PC exploatat de un atacator.

E. Router on a stick

1. Configurați interfața Gigabit0/0 a lui R1 cu subinterfețe pentru rutarea inter-VLAN pentru VLAN-urile 8, 9, 10 și 11, folosind tabelul de adresare IP de mai sus. VLAN-ul 10 trebuie configurat ca VLAN nativ.

2. Configurați interfața F0/5 a lui S11 ca trunk pe care să permiteți explicit VLAN-urile configurate pe subinterfețele Gi0/0 ale lui R1. VLAN-ul 10 trebuie configurat ca VLAN nativ.

F. Server DHCP

1. Configurați R1 ca DHCP server cu 3 pool-uri de adrese, câte unul pentru fiecare dintre rețelele VLAN 8, 9 și 11. Trebuia ca P3, PC4 și Laptop să poată fi configurați dinamic cu adresa IP, masca de rețea, default gateway și adresa lui DNSServer drept server de DNS**.**
2. Excludeți **primele 10 adrese** din fiecare pool DHCP. Pentru VLAN11 excludeți și adresele interfețelor de management ale switchurilor.

G. Frame Relay

1. Configurați Frame Relay cu subinterfețe point-to-point pe R1, R2 și R3 folosind adresarea din tabelul de adrese. Configurați subinterfețele cu DLCI-uri corespunzător informațiilor de mai jos:

- R1 folosește DLCI 102 pentru a ajunge la R2 și 103 pentru R3
- R2 folosește DLCI 201 pentru R1 și 203 pentru R3
- R3 folosește DLCI 301 pentru R1 și 302 pentru R2

H. OSPF peste Frame Relay

1. Configurați OSPF pe R1, R2 și R3 folosind router-id-urile 1.1.1.1, 2.2.2.2, respectiv 3.3.3.3.
Introduceți rețelele de pe subinterfețele Frame Relay în aria 0 din OSPF.
2. Configurați R2 astfel încât să redistribuie rețelele de pe Gi0/0 și de pe Loopback 0 ca rețele externe procesului de OSPF.
3. Configurați OSPF pe R1 astfel încât rețelele de pe VLAN 8-11 să fie propagate în aria 1.
4. Configurați OSPF pe R1 pentru agregarea rețelelor VLAN8-11 ca o singura ruta propagata din aria 1 în aria 0.

I. Point-to-Point Protocol cu autentificare CHAP

1. Configurați PPP cu autentificare CHAP pe interfața lui R3 către Internet. Hostname-ul echipamentului la care R1 se conectează pentru a ajunge în Internet este **“ISP”**, iar parola CHAP este **“cisco”.**
2. Adăugați pe R3 o rută statică default cu interfața de ieșire către ISP și propagați ruta în OSPF.

J.New Branch inital set-up (Tunele GRE)

1. Telework-erul este în un nou Branch al companiei sale. Router-ul R4 nu a fost configurat. Conectați-vă prin consolă de la Teleworker și configurați pe R4. Aflați în mod remote IP-ul asignat de ISP pentru R4 pe S1/0.
2. Configurați un tunel GRE între R3 și R4 folosind interfețele lor către ISP ca suport pentru tunel și spațiul 172.16.33.0/30 pentru adresarea tunelului.
3. Configurați un LAN între R4 și Teleworker, de mărime /24, din spațiul de adrese 10.0.0.0/8, care să nu facă overlap cu alte rețele preconfigurate.
4. Realizați configurațiile necesare astfel încât prin acest tunel GRE să existe acces de la Teleworker catre PC-urile 0-4, WebServer și DNSServer.

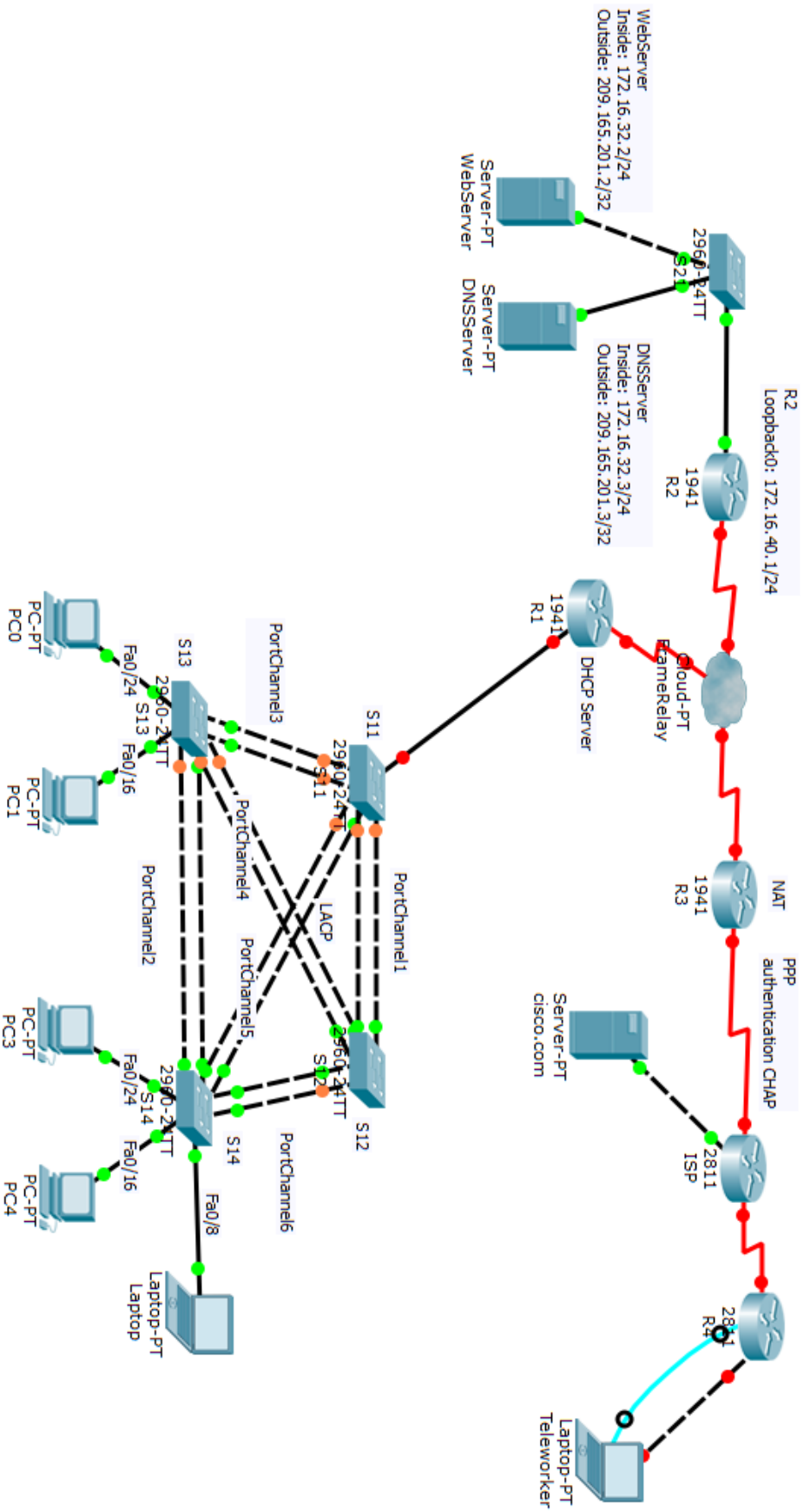
K. NAT static și PAT

1. Configurați NAT pe R3 astfel încât WebServer și DNSServer să acceseze serverul cisco.com (141.85.85.6) cu adresele IP sursă translatate static la 209.165.201.1, respectiv 209.165.201.2.

2. Configurați PAT (port address translation) pe R3 pentru a translata IP-urile sursă **numai** pentru traficul IP din VLAN-urile 8-11 către rețeaua 141.85.85.0/30. Translatarea se va face la adrese din rețeaua 209.165.134.0/30.

L. Configurare ACL pentru interzicerea accesului cisco.com

1. Verificați că aveți conectivitate în ambele sensuri între serverul cisco.com și WebServer. Configurați un access-list pe R3 care să blocheze traficul TCP de la serverul cisco.com catre WebServer. Restul traficului IP este permis.


WebServer
Inside: 172.16.32.2/24
Outside: 209.165.201.2/32
Server-PT
WebServer
Server-PT
DNSServer
DNSServer
Inside: 172.16.32.3/24
Outside: 209.165.201.3/32
2960-24TT
S21
R2
Loopback0: 172.16.40.1/24
1941
R2
1941
R1
DHCP Server
Cloud-PT
FrameRelay
1941
R3
NAT
PPP
authentication CHAP
Server-PT
cisco.com
2811
ISP
2811
R4
Laptop-PT
Teleworker
PC-PT
PC0
PC-PT
PC1
PC-PT
PC3
PC-PT
PC4
Laptop-PT
Laptop
S13
2960-24TT
S13
S11
2960-24TT
S11
S14
2960-24TT
S14
S12
2960-24TT
S12
Fa0/24
Fa0/16
Fa0/24
Fa0/16
Fa0/8
PortChannel1
PortChannel2
PortChannel3
PortChannel4
PortChannel5
PortChannel6
LACP