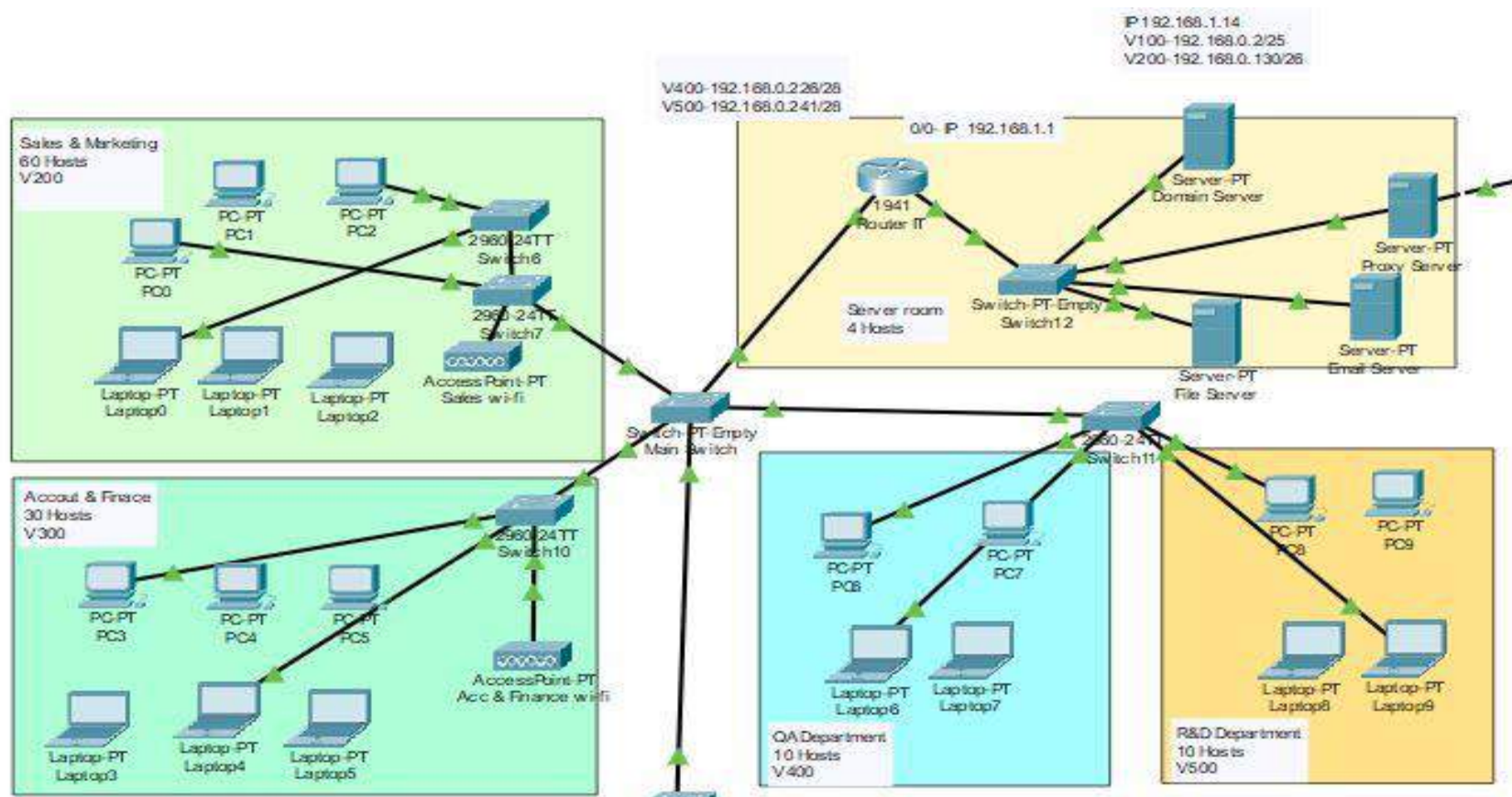


დავალება 2: ქსელის ადმინისტრატორს სურს გამართოს მოცემული ლოკალური ქსელი:

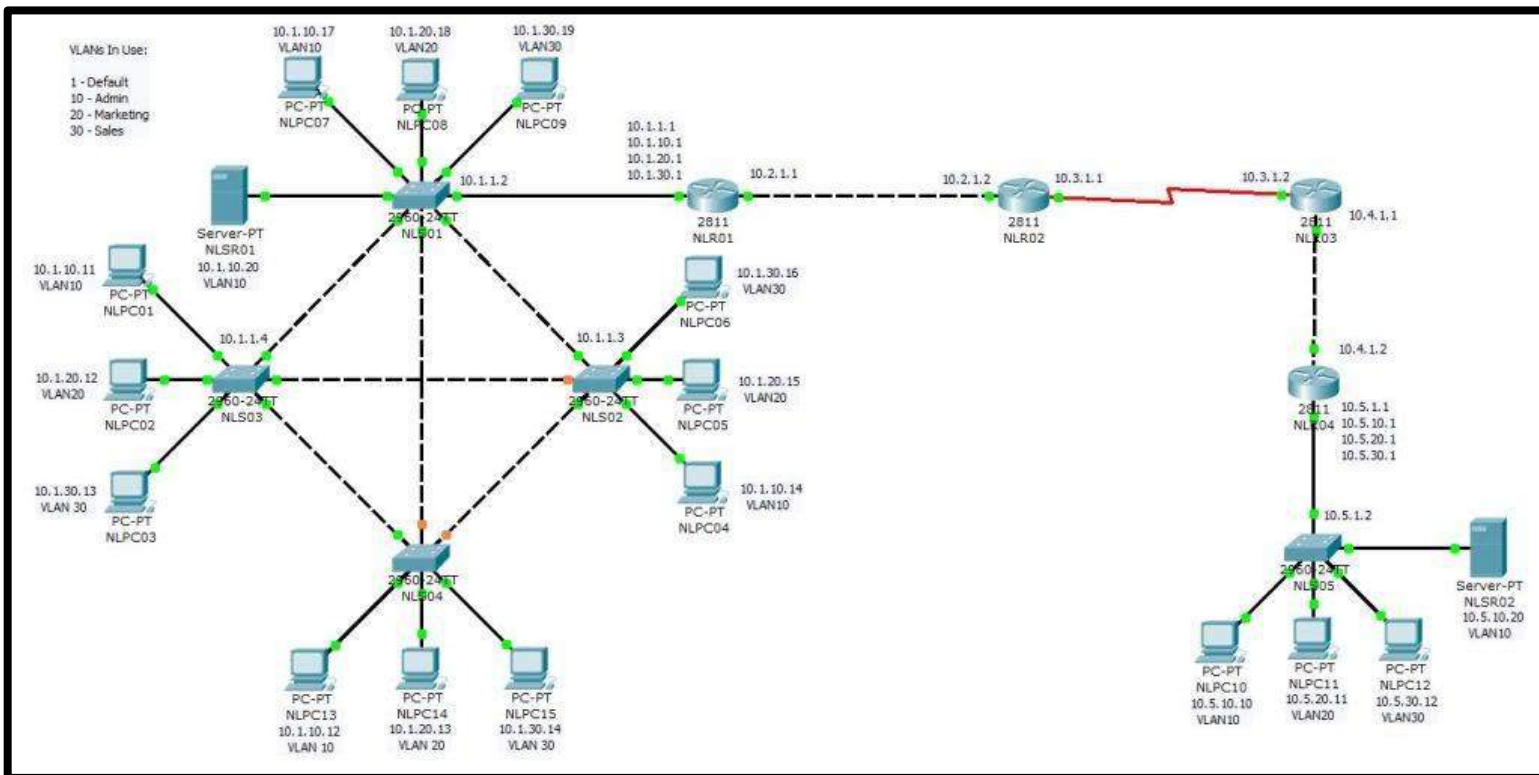
1. გამართეთ ლოგიკური და ფიზიკური ტოპოლოგია; გაწერეთ მოსამართები (მოცემულის თანახმად);
2. გამართეთ ველანები და დააკავშირეთ ისინი ერთმანეთთან;
3. დააკონფიგურირეთ სერვერები: Dns, Mail.
4. Account & Finance განყოფილებას აუკრძალეთ სხვა ქსელში გასვლა;
5. სასერვერო ოთახის სვიჩზე დააყენეთ ბაზისური უსაფრთხოება და პორტის უსაფრთხოება
6. როუტერზე დააკონფიგურირეთ NAT-ირება.
 - <inside global = 202.170.100.8/29>



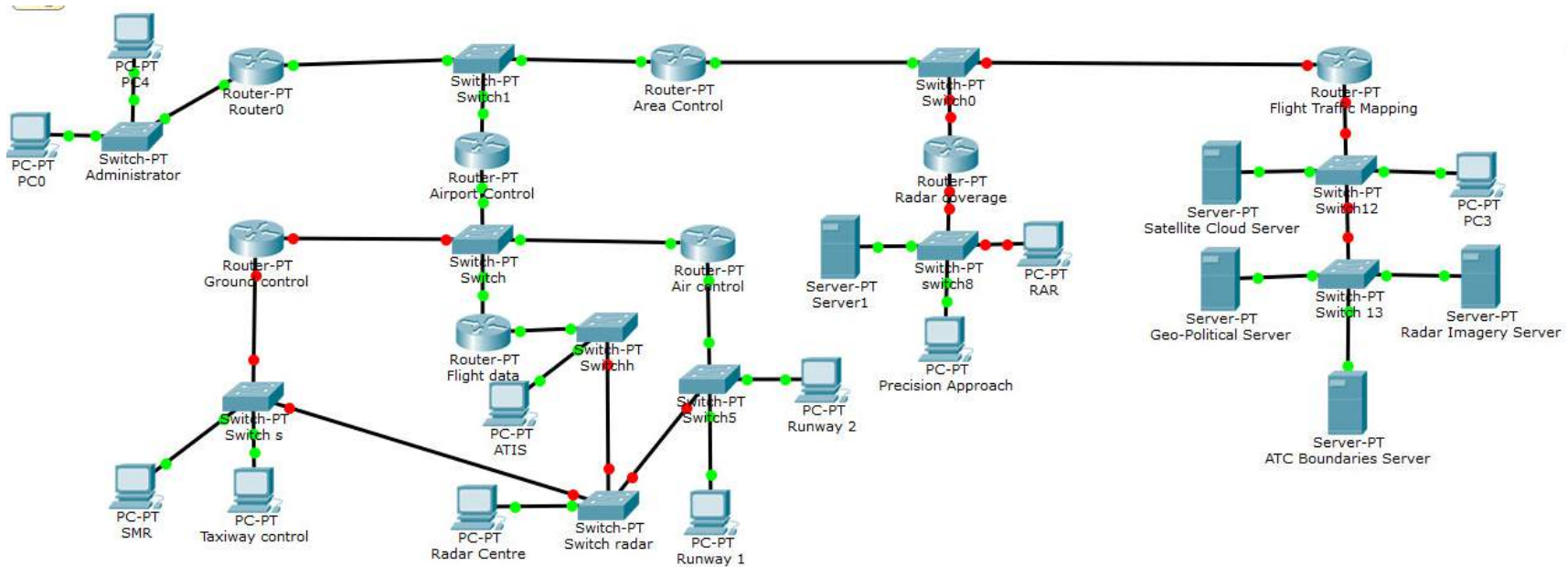
დავალება 4: ააგეთ ნახაზზე ნაჩვენები ტოპოლოგია.

1. შექმენით VLAN-ები ნახაზზე ნაჩვენები წესით
2. დააკონფიგურირეთ მარშრუტიზაციის პროტოკოლი
3. შექმენით ACL ისე, რომ Sales განყოფილება ვერ გადიოდეს გარე ქსელში (შიდა ქსელის სხვა VLAN-ებთან ჰქონდეს კავშირი)
4. გარე ქსელში გასასვლელად გამოიყენეთ NAT-ირება (NAT-ისთვის გამოიყენეთ ნებისმიერი გლობალური მისამართები)
5. ყველა სხვა კომპიუტერები თავისუფლად უნდა პინგავდნენ როგორც შიდა ასევე გარე ქსელის კომპიუტერებს.

6. სერვერებზე დააყენეთ პორტის უსაფრთხოება



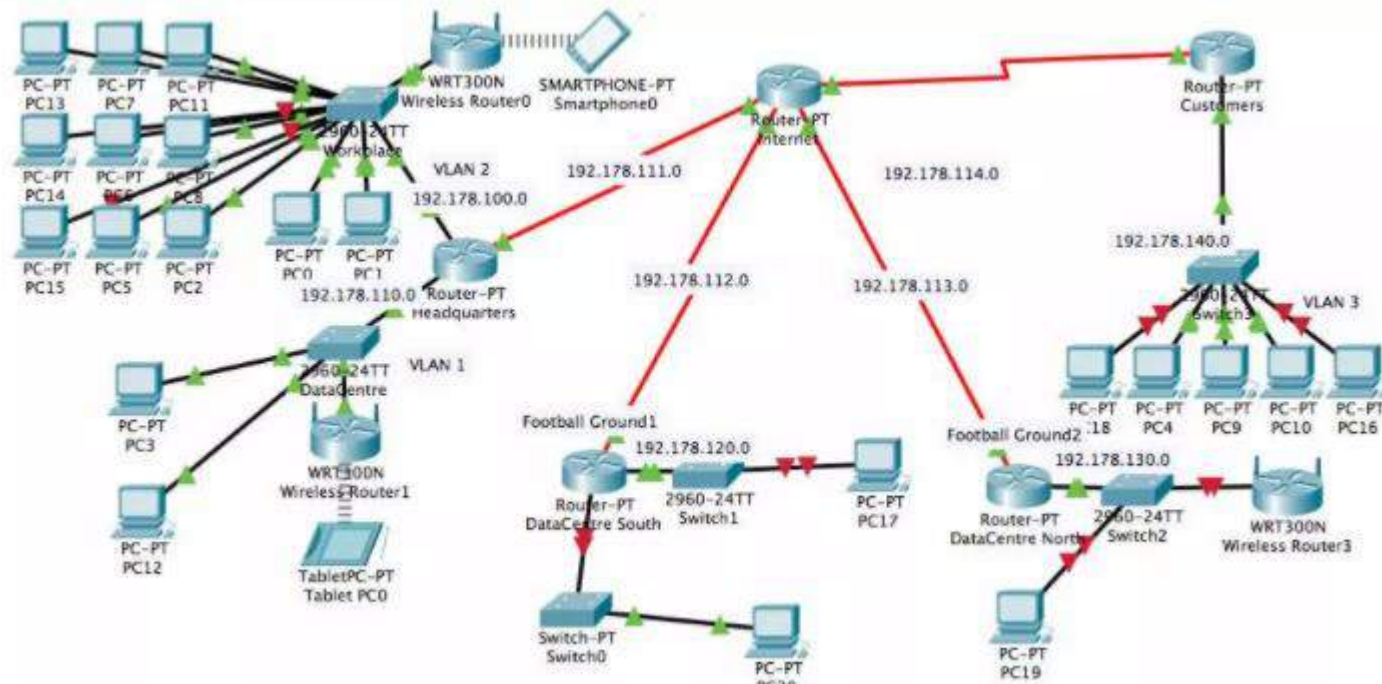
1. დააკონფიგურირეთ მისამართები შიდა ქსელიდან (გამოიყენეთ ქვექსელები) და გაწერეთ ცხრილის სახით
2. მარშუტიზაცია გაწერეთ დინამიურად. როუტერებს შორის გამოიყენეთ /30 მასკა.
3. NAT -ირებისთვის დინამიურად გაწერეთ ნებისმიერი მისამართები Flight Traffic Mapping როუტერზე
4. სერვერებზე დააყენეთ პორტის უსაფრთხოება
5. სერვერ 1-ზე დააყენეთ ვებ გვერდი www.google.com.
6. PC0 აუკრძალებს ვებ გვერდის ნახვას; სერვერებს აუკრძალებს ინტერნეტში გასვლა.
7. ქსელურ მოწყობილობებზე გამართეთ ბაზისური უსაფრთხოება (გაწერეთ ცხრილის სახით)



1. დააკონფიგურირეთ მისამართები (იხე როგორც ნახაზზეა ნაჩვენები)

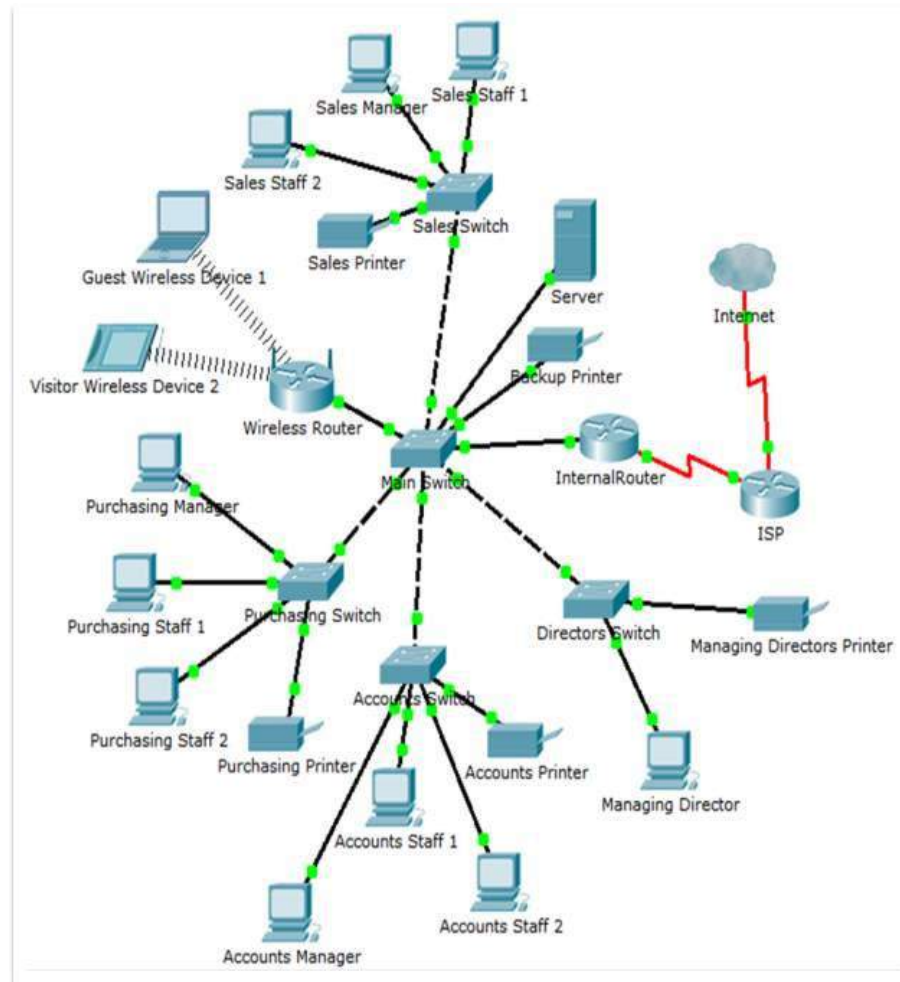
1. დააკონფიგურირეთ მისამართები (იხე როგორც ნახაზზეა ნაჩვენები)

2. Workplace როუტერი დაყავით სეგმენტებად (ველანები) და განახორციელედ მათ შორის კომუნიკაცია
3. განახორციელეთ ქსელებს შორის მარშრუტიზაცია.
4. NAT -ირებისთვის გამოიყენეთ Internet როუტერი და დინამიურად გაწერეთ ნებისმიერი მისამართები. ასევე გაწერეთ დეფაულტ მარშრუტი.
5. როუტერებს აუკრძალეთ როუტინგ ცხრილის გაგზავნა შიდა ქსელისკენ
6. Lan 3 ქსელს აუკრძალეთ ინტერნეტში გასვლა
7. Lan 1 ქსელს აუკრძალეთ Lan 3-ში გასვლა.



დავალება 12: ააგეთ ნახაზზე ნაჩვენები ტოპოლოგია.

1. დაგეგმეთ მისამართები შიდა ქსელიდან და ააგეთ შესაბამისი ცხრილი.
2. შიდა ქსელი გაყავით ველანებად (სტაფი1, 2, მენეჯერი) და უზრუნველყავით მათ შორის კავშირი)
3. გაწერეთ მარშუტიზაცია. გამოიყენეთ შიდა ქსელი და /30 მასკა. როუტერებს აუკრძალეთ შიდა ქსელში ცხრილის გაგზავნა.
4. სერვერზე დააყენეთ ვებ გვერდი და სტაფ 1-ის კომპიუტერებს აუკრძალეთ ამ ვებ გვერდის ნახვა
5. დირექტორის კომპიუტერზე დააყენეთ პორტის უსაფრთხოება.
6. შიდა ქსელის ბოლო როუტერზე გაწერეთ დეფაულტ მარშუტიზაცია და ნატირება (ნებისმიერი მისამართით).
7. როუტერებზე დააყენეთ ბაზისური უსაფრთხოება და ააგეთ შესაბამისი ცხრილი.



დავალება 13: ააგეთ ნახაზზე ნაჩვენები ტოპოლოგია.

1. დააკონფიგურირეთ მისამართები ნახაზზე ნაჩვენები ქსელების მისამართების მიხედვით
2. კომპიუტერის ლაბორატორიის მისამართები გაწერეთ დინამიურად და ამისთვის გამოიყენეთ როუტერ 2.
3. მარშუტიზაცია გაწერეთ სტატიკურად
4. NAT -ირებისთვის დინამიურად გაწერეთ ნებისმიერი მისამართები და დააყენეთ იგი როუტერ 0-ზე
5. როუტერ 0 არის ბოლო როუტერი რომლიდანაც ხდება ინტერნეტ ქსელში გასვლა. დააყენეთ დეფაულტ მარშუტი.
6. Other ლაბორატორიას აუკრძალეთ ყველა ხვა შიდა ქსელში შესვლა, თუმცა შეუძლია ინტერნეტში გასვლა

7. Switch3 კომპიუტერებზე გაწერეთ პორტის უსაფრთხოება.
8. სერვერებზე დააყენეთ ვებ და დნს სერვისები. ცომპიუტერის ქსელს აუკრძალეთ ამ ვებ გვერდის ნახვა

