Lab 6

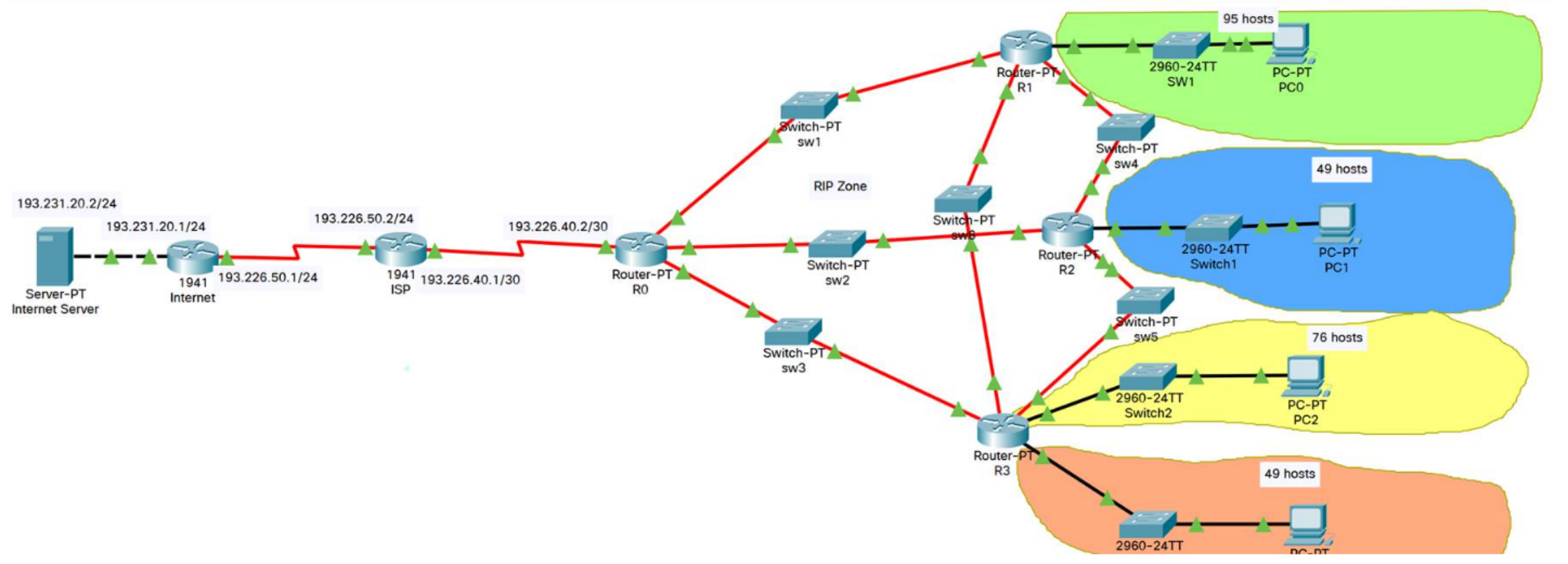
In the diagram bellow we represent an organization network (right of Router-PT R0) connected to its ISP (router 1941 ISP). The router 1941 Internet and Server-PT Internet Server represent the Internet and some server in Internet.
Some of the IP addresses are given and already allocated like in the figure (internet part and up to the organization router external IP public IP address). We can observe in the figure that the organization has three subnetworks, each linked to the main router (R0) by an intermediate router (R1, R2 and R3).
Use Packet Tracer to create a network topology like the one bellow and setup IP Addressing and setup manual and dynamic (RIP *Routing Internet Protocol*) such that:

- R0, R1, R2,R3 routers and their interconnecting subnetworks to R0 have public IPs subnetted from **193.226.40.0/28** (193.226.40.0/30 is the global R0 external network).
- Interconnexion networks between R1-R2- R3 have IPs allocated from 10.0.0.0/28 !
- The green subnetwork contains 95 hosts, the blue subnetwork contains 49 hosts, the yellow subnetwork contains 76 hosts and the orange subnetwork contains 49 hosts. All these IPs are allocated from the range **192.168.0.0/23**.
- All local LANs green subnetwork, blue subnetwork, yellow subnetwork, orange subnetwork can access each other without NAT – only through routing. Routing between R0, R1, R2, R3 and local LANs should be implemented using RIP and be dynamic.
- Setup NAT access on R1, R2, R3 such that all colored LANs can access the Internet using their router's public IP. R1,R2, R3 are not accessible from Internet and do not have access to Internet.
- Routers R0, R1, R2,R3 are linked with Fiber and are all instances of an empty PT-router to which one adds three fiber network adapters and two gigabit copper network adapters and one serial link. They are connected through PT-Switches that have at least two fiber network ports each.
- The Server-PT Internet Server implements a public HTTP/HTTPS service and an FTP service and has its default router set trough 193.231.20.1/24.
- R0 has as default gateway/router the ISP router and the ISP router has as default gateway 193.222.50.1 (1941 Internet). The 1941 Internet router has as default gateway the Server-PT Internet Server (193.231.20.2)
- Router 1941 ISP should manually route to the organization only range 193.226.40.0/28 !
- All routing in the RIP zone (organization network) should be implemented using RIP v2 -including the default routes to Internet. (see notes bellow)
- No private IP networks should be directly accessible from the outside of the organization network.
- No private IPs should be able to escape in Internet from the local networks. If NAT is deactivated on one of the routers – the border organization router should define an external access policy (access-list + access-group on the external interface that blocks that traffic)

-

CHECKLIST: If your implementation is correct, you should be able to: **(this is your checklist)**

1. Have correct addressing in all networks where you allocated Ips
2. Ping or traceroute from any internal PC to any other organization PC (without having its address nated) and access any server/router in Internet through NAT.
3. Access HTTP and FTP services from all computers in all networks.
4. On R0 if you disconnect any single or two links towards any of R1,R2, R3 – you should see that RIP adapts and redirects traffic from the colored networks towards internet via the remaining available paths. NAT should still be working. Check that with traceroute or in Simulation mode !
5. If you disconnect links between any combination of R0, R1, R2, R3, while there is still a working path – RIP should adapt and direct traffic accordingly. Check that with traceroute or in Simulation mode.
6. Check what happens if you allow auto-summarization enabled on R0, R1, R2, R3 ! Explain !
7. If NAT is deactivated on any of the internal routers (R1,R2,R3) the private IPs should not escape outside the organization – R0 should block them.


193.231.20.2/24
193.231.20.1/24
193.226.50.2/24
193.226.40.2/30
193.226.50.1/24
193.226.40.1/30
Server-PT
Internet Server
1941
Internet
1941
ISP
Router-PT
R0
Switch-PT
sw1
Switch-PT
sw2
Switch-PT
sw3
RIP Zone
Router-PT
R1
Switch-PT
sw6
Router-PT
R2
Router-PT
R3
Switch-PT
sw4
Switch-PT
sw5
95 hosts
2960-24TT
SW1
PC-PT
PC0
49 hosts
2960-24TT
Switch1
PC-PT
PC1
76 hosts
2960-24TT
Switch2
PC-PT
PC2
49 hosts
2960-24TT
PC-PT

Theory

Network routing using RIP (**R**outing **I**nformation **P**rotocol) is performed by having each router advertise to the other routers the networks *it knows* about. This information is propagated to neighboring routers allowing them to learn trough which routers they can route packets addressed to a given destination. Routers are told which network to advertise as being capable of reaching. Neighboring routers use this information to learn the next hops for reaching a given network. Once the information is propagated through the entire infrastructure, each router learns the network topology and its state. Whenever a link goes down, the negative information (some networks do not get advertised anymore to their neighbors) is also spread throughout the network. Using RIP one can let the dynamic state of the network at all moments be reflected into the routing tables of the routers allowing for dynamic path changing. The way RIP works and build its network graph is presented during the lectures. Packet Tracer implements RIPv1 which is only classfull and RIPv2 (classless). You should use RIPv2 in order to handle CIDR addressing.
In order to ***distribute the default routing information*** inside the organization – one should activate the option (default-information originate) on the router situated at the edge of the organization towards Internet (R0 in our case). This allows the internal routers to dynamically choose their default routes according to the state of the links.
RIP performs network **auto summarization** (address aggregation) by default which is not always desirable when using subsegments of former classfull addresses.

Notes:

Router Configuration

For any equipment configuration try to setup things in the config tab and watch the equivalent commands as you should have enter them in order to accomplish the same task in the bottom side of the window. There are things that cannot be configured from the graphical user interface. In order to learn new commands try the help system "?". After any part of a command entered, placing a "?" shows the remaining parameters and their explanation. Usually a user needs administrative privileges (or entering privileged mode) in order to apply any new configuration changes to a router. The command to enter privileged mode is ***enable***.
From privileged mode – most of configuration changes need a special mode that is entered by using the command:
config t – as configure terminal – which enters configuration mode. You need to type CTRL+Z or exit .
In order to make router settings changes permanent one needs to copy the *current running configuration* into the *startup configuration*. The command to accomplish this is copy running-config startup-config. Upon reboot the router will keep its configuration.

RIP – configuration

In order to configure RIPv2 on a router we need to:

#go in admin mode, configuration
enable
config t

#enable RIP protocol on the router
route rip

#enable RIPv2
version 2

#specifiy the networks that we advertise to remote routers one by one
network 192.168.0.0
network 10.0.1.0
network 10.0.2.0

#tell router to not advertise the networks on the links where RIP is not activated or were routes shoult not be propagated.Ex. outside of R0 and inside green subnetwork, blue subnetwork, yellow subnetwork, orange subnetwork.
Passive-interface Serial 0/0/0

#on R0 enable propagation of the default route towards the other routers through RIP. This allows propagation of the default routes to all other organization routers and allow them to choose dynamically their routes towards Internet.
default-information originate

#because we use CIDR adressing we disable auto-summary (aggregation of routing networks that RIP does not always perform correctly)
no auto-summary

#go back to normal admin mode context
exit
exit
all done for RIP at this point
#in order to see the routes that are learned we can show the global routing table
show ip route

#to see info on what routes RIP learned
show ip rip database

NAT – configuration

Access lists are a mechanism that helps selecting IP traffic according to some rules (IP addresses – source or destination and protocol) either for implementing a basic packet filtering (firewall) or to be selected for some action. You will need to use them to select which communicating parties are candidate to NAT from each local network. Extended access-lists contain multiple rules read in order and having the first matching rule apply the fate of the packet.

#to select traffic that won't be affected where the access list is applied put use deny. To allow traffic to be selected use permit. Both versions use a source and destion specifiers. Select to not apply to = deny traffic from 192.168.0.0-192.168.0.127 to 192.168.0.0-192.168.0.255. The list bellow selects traffic between 192.168.0.0/25 to all other IPs except the range 192.168.0.0/24.

conf t
ip access-list extended nat
10 deny ip 192.168.0.0 0.0.0.127 192.168.0.0 0.0.0.255
select to traffic between 192.168.0.0-192.168.0.127 and everything else
20 allow ip 192.168.0.0 0.0.0.127 any

If you use this list as source for NAT – only some pairs or combintions will suffer NAT depending on how you describe them in the access list.

Packet Filtering – configuration

Packet filtering is implemented using acess-lists at the interface level. On each interface the **access-group** directive allows filtering traffic **in** or **out** according to the rules defined in an access list.

conf t
interface Serial 0/0
ip access-group fw-out out