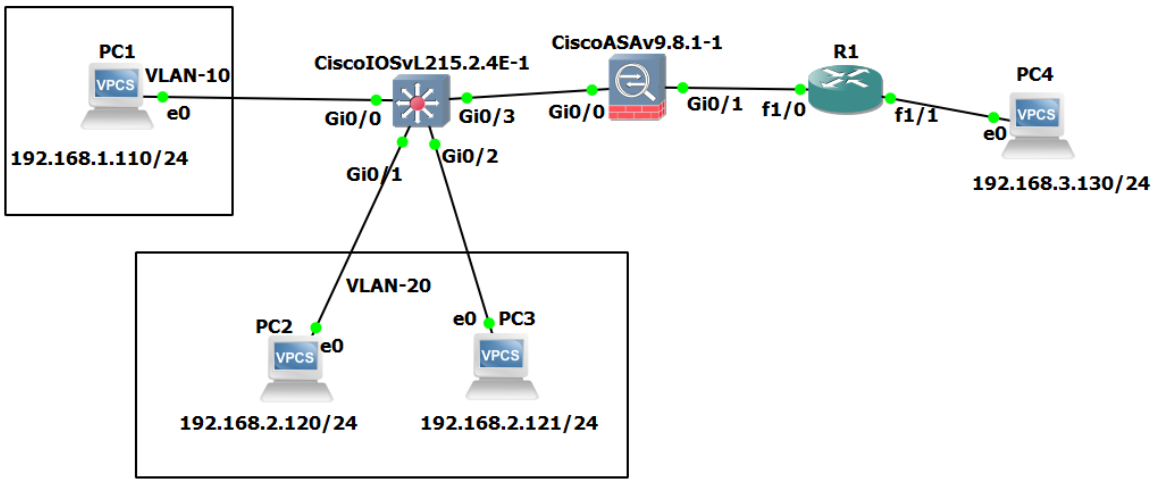
CNOSS. LAB 1

The second network scheme was configured using GNS3 software with device templates downloaded from the net.



Firstly, names for each PC were set, then IP addresses:

```
VPCS> set pcname PC1

PC1> ip 192.168.1.110/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.110 255.255.255.0 gateway 192.168.1.1

PC1>
```

```
VPCS> set pcname PC2

PC2> ip 192.168.2.120/24 192.168.2.1
Checking for duplicate address...
PC2 : 192.168.2.120 255.255.255.0 gateway 192.168.2.1

PC2>
```

```
VPCS> set pcname PC3

PC3> ip 192.168.2.121/24 192.168.2.1
Checking for duplicate address...
PC3 : 192.168.2.121 255.255.255.0 gateway 192.168.2.1

PC3>
```

```
Press '?' to get help.

VPCS> set pcname PC4

PC4> ip 192.168.3.130/24 192.168.3.1
Checking for duplicate address...
PC4 : 192.168.3.130 255.255.255.0 gateway 192.168.3.1

PC4>
```

Also, we should save configuration for next startups to have everything on place:

```
PC1> save
Saving startup configuration to startup.vpc
.  done

PC1>
```

I set hostname and created vlan-10 and vlan-20:

Vlan-10 ->PC1(192.168.1.110/24)

Vlan-20 ->PC2(192.168.2.120/24), PC3(192.168.2.121/24)

```
S1(config)#vlan 10
S1(config-vlan)#name vlan010
S1(config-vlan)#vlan 20
S1(config-vlan)#name vlan020
S1(config-vlan)#end
S1#s
*Apr 16 08:53:48.498: %SYS-5-CONFIG_I: Configured from console by consolehow vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/2, Gi0/3, Gi0/0, Gi1/0
                                                 Gi1/1, Gi1/2, Gi1/3, Gi2/0
                                                 Gi2/1, Gi2/2, Gi2/3, Gi3/0
                                                 Gi3/1, Gi3/2, Gi3/3
10   vlan010                           active
20   vlan020                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

S1#
```

Ports gi0/0,gi0/1,gi0/2 are set as mode access ports because connections through these ports will carry only traffic for single vlan at any time, in contrary, port gi0/3 is set as trunk port and traffic for both vlans will be gone via this port:

```
Switch(config)#int gi0/0
Switch(config-if)#swi
Switch(config-if)#switchport
Switch(config-if)#sw
Switch(config-if)#switchport mode acc
Switch(config-if)#swi
Switch(config-if)#switchport access vlan 10
```

```
Switch(config)#int gi0/1
Switch(config-if)#swi
Switch(config-if)#switchport
Switch(config-if)#swi
Switch(config-if)#switchport mode ac
*Apr 18 01:20:57.543: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int gi0/2
Switch(config-if)#swi
Switch(config-if)#switchport
Switch(config-if)#swi
Switch(config-if)#
*Apr 18 01:21:17.234: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
Switch(config-if)#swi
Switch(config-if)#switchport mode access
Switch(config-if)#switc
Switch(config-if)#switchport acces
Switch(config-if)#switchport access vlan 20
```

```
Switch(config)#int gi0/3
Switch(config-if)#switc
Switch(config-if)#switchport
Switch(config-if)#sw
Switch(config-if)#switchport mode tru
Switch(config-if)#switchport mode trunk
Switch(config-if)#
*Apr 18 03:26:24.353: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
Switch(config-if)#swi
Switch(config-if)#switchport tru
Switch(config-if)#switchport trunk al
Switch(config-if)#switchport trunk allowed vla
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#end
```

Port g0/0 was splitted into two sub-interfaces to assign gateway to them and vlan-id:

```
ciscoasa(config)# int g0/0
ciscoasa(config-if)# no nameif
ciscoasa(config-if)# no security-level
ciscoasa(config-if)# no ip address
ciscoasa(config-if)# no shut
ciscoasa(config-if)# int g0/0.10
ciscoasa(config-subif)# nameif inside-10
ciscoasa(config-subif)# vlan 10
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-subif)# int g0/0.20
ciscoasa(config-subif)# nameif inside-20
ciscoasa(config-subif)# vlan 20
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip address 192.168.2.1 255.255.255.0
```

Routing info of networks also were added:

```
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set

C        10.10.10.0 255.255.255.0 is directly connected, outside-3
L        10.10.10.2 255.255.255.255 is directly connected, outside-3
C        192.168.1.0 255.255.255.0 is directly connected, inside-10
L        192.168.1.1 255.255.255.255 is directly connected, inside-10
C        192.168.2.0 255.255.255.0 is directly connected, inside-20
L        192.168.2.1 255.255.255.255 is directly connected, inside-20
S        192.168.3.1 255.255.255.255 [1/0] via 10.10.10.1, outside-3
```

Now, from ASA we can ping PCs in vlan:

```
ciscoasa# ping 192.168.1.110
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.110, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
ciscoasa# ping 192.168.2.120
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.120, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/18/30 ms
```

The network 3.0/24 is outside so by default the security is 0, which will limit PCs and other devices to send packets to inside:

```
ciscoasa(config-if)# int g0/1
ciscoasa(config-if)# nameif outside-3
INFO: Security level for "outside-3" set to 0 by default.
ciscoasa(config-if)# ip address 10.10.10.2 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# end
ciscoasa# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/10/10 ms
```

Then I assigned corresponding IPs to router's interfaces:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f1/1
R1(config-if)#ip address 192.168.3.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int f1/0
R1(config-if)#ip address 10.10.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#end
R1#
*Apr 18 05:13:18.979: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 192.168.3.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
R1#
```

And added routes for other networks:

```
R1(config)#ip route 192.168.1.0 255.255.255.0 f1/0
R1(config)#ip route 192.168.2.0 255.255.255.0 f1/0
```

To allow pinging from inside to outside NATs were created which connect inside-10 vlan to outside-3 and inside-20 vlan to outside-3. By default, ICMP packets are drop in firewall so to permit pass through firewall “inspect icmp” command was run:

```
ciscoasa(config)# object network in1-out
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside-10,outside-3) dynamic interface
ciscoasa(config-network-object)# object network in2-out
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside-20,outside-3) dynamic interface
ciscoasa(config-network-object)# policy-
ciscoasa(config-network-object)# policy-m
ciscoasa(config-network-object)# policy-map global
ciscoasa(config-network-object)# policy-map global_policy
ciscoasa(config-pmap)# clas
ciscoasa(config-pmap)# class inspection_defau
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# end
```

For security reasons, cisco firewall drops packages with source’s security level lower than destination’s. One way to enable bidirectional icmp from outside network to inside vlan is to set security level 100 for all interfaces and sub-interfaces and allow same security level connection.

```
ciscoasa(config)# same
ciscoasa(config)# same-security-traffic per
ciscoasa(config)# same-security-traffic permit inter
ciscoasa(config)# same-security-traffic permit inter-interface
```