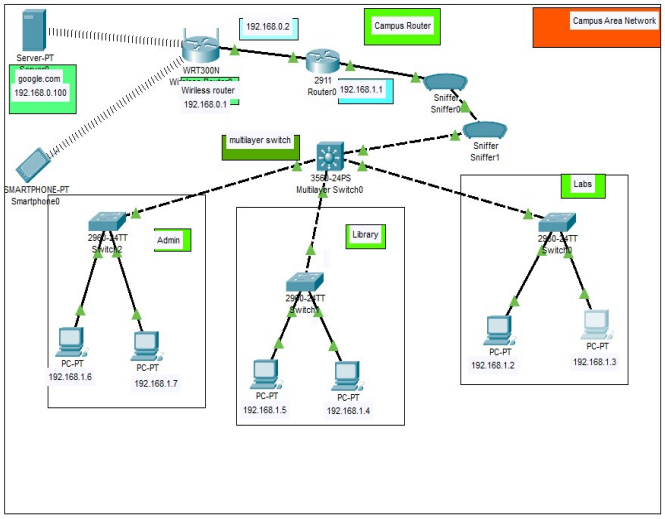

Campus Area Nerwork :

==========
NETWORK TOPOLOGY CREATION:
==========
steps1: creating a topology which is same as your campus.

step2: creating three network based on the campus requirement

step3 : choose a multilayer switch to connect multiple network to a router
and that router than connect to a wireless router from which our campus
get internet and access stuff on internet like show in digram google.com

step4: configure each device with there ip address and default getways so
that the campus network can access the internet from outside.

In this topology , SRMIST Delhi NCR Campus networks essential network
configures such as LAB, LIBRARY,LABS

==========
DATA OR ACCESS OF EXTERNAL NETWORK:
==========

Whenever a person respective to network domain will try to access the google.com
than for this topologies the same things goes via IP address when user ping the IP
from the command promt or also type the IP address in the web browser than it will
redirect to you to respective web page.

At first time when topolgies created, when a user want to
access the any other network device in the campus or want to access the internet that time the packet which
broadcast to every network which connect to the switch when a respective node reply to the packet than sw
MAC address in the MAC TABLE.

==========
flow of the packet travel from source to destination
==========
let say we user of pc with ip address 192.168.1.6 and want to access the google.com(192.168.0.100) so we
1. go to network switch(layer 2 device of OSI model) than this switch transmit to nearest router (layer 3 devi
2. this router is also connect to a wireless router which enable internet to access external network.
3. once the request is successful reach to destination than it response to request

Now to analyaze how the packet will traval and what are the commpent are require inorder to send data secu

==========
PACKET TRANSMISSION AND HEADER INFORMANTION:
==========
we can refer to TCP/IP model
==========
encapsulation of data/payload :
==========
application layer(layer-1)->Data will generated
transport layer (layer 2)->Data will divided into segments by adding transport header
internet layer (layer 3)->segments are converted into packets by adding network header
network access (layer 4)->packet are converted into frame by adding frame header and trailer to packets

decapsulation of data/payload :
==========
t dject opposite of encapsulation
layer 4-> frame and trailer are separeted and formward to upper layer
layer 3-> network header is separeated and forward to upper layer.
layer 2-> transport header is seperated and forward to upper layer.
layer 1 -> actual data/payload is get by application layer and corresponding response is given.

==========
PACKET SNIFFER:
==========

let assume you want to know about how the data packets of various field or header informantion

you can use Packet Sniffer which will not effect the packet transmission from source to destination
but able to retrieve essential information such port no., protocol, etc.
in our topologies we add two packet snipper between multilayer switch and router to see the incoming and ou

packet sniffer able two retrieve information about almost all the protocol header such UDP ,TCP,SMTP,etc.

while looking into this header we can able to see the source address and destination address of data packet t

in my topologies
==========
I send the data packet through the device with IP 192.168.1.2 to analyze the packet flow and retrieve header
source Ip:192.168.1.2
destination Ip: 192.168.0.100
version : 4
header lenght: 5
flages information
checksum value
TTL field
fragement fields
---
this are the essential information that are very crucial
if attacker want to use this information than they can use as
to show ourself as a legitmate device and request for a crucial
information.

==========
outcome of packet sniffer:
==========
This is all I learn when I was doing packet sniffing through
the packet sniffer because unless attacker can't affect the transmission of packet but the information is get by
lead future problem such security of data. and it might get information about network topologies and as well as

---