**Network troubleshooting**

Network troubleshooting is primary done by network engineer or administrators to repair or optimize the network. It is generally done to recover and establish network or internet connection on end nodes or devices. Network troubleshooting can be done manually or automatically by using network Diagnostic tools.

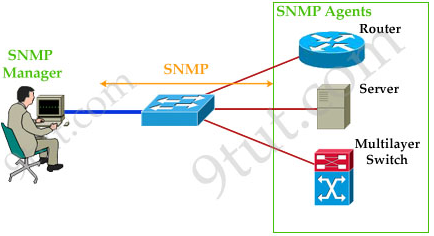
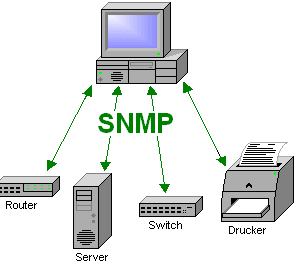


As a Good system administrator it is necessary to keep track of activities inside the network so in case if someone manages to penetrate inside the network system must be able to track it.

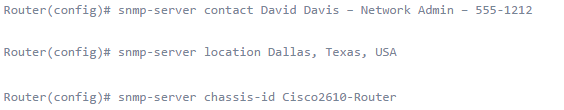
**SNMP (simple network management protocol)**

**The** simple network management protocol is a necessary toll for every network administrator it is the popular way to monitor the network performance of network devices including cisco routers, switches and PCs that are located inside your network. With an SNMP management station, you can graph the performance of network devices.

Further these devices can send alerts (trap) to management station if they found any unusual activity going on.



Once SNMP (simple network management protocol) is enabled on cisco Router or switch you may use any network monitoring tool like **CACTI** to see the flow of information and much more.



Next step is to configure SNMP so that it can be monitored by NMS(network management system). In order to use SNMP we have to create **community String** that as a password.

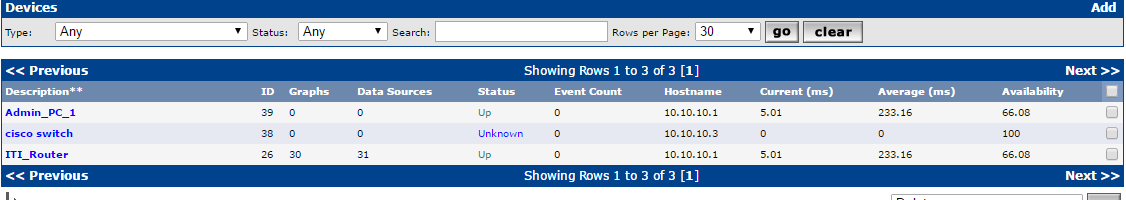


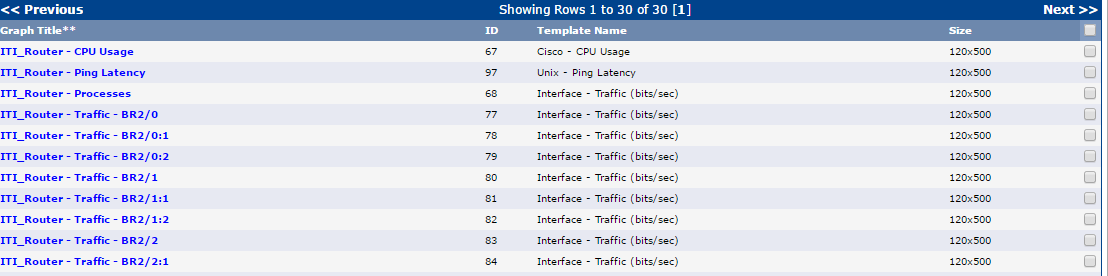
And then in order to send the notification to remote host the IP address of that host will be configured as.



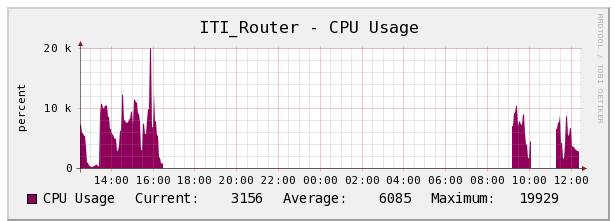
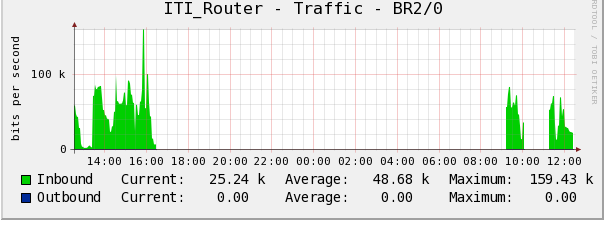
By enabling this all SNMP notification will be sent to **192.168.1.23**  host.

In CACTI now we can add The router that has be configured to send SNMP notification make sure you are using the right IP address of remote host that is running CACTI in this case it is **192.168.1.23.**



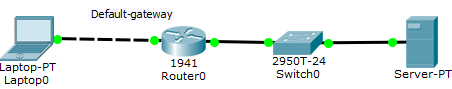
Following Graphs can be found by just clicking of devices that is added to use SNMP.

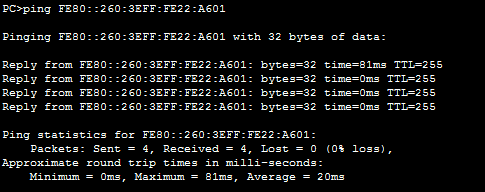
For example the CPU usage and traffic that is coming and going out looks like.



Checking connectivity to Default-gateway

Same like IPv4 network in IPv6 it is always good practice to check the connectivity to default-gateway .A default gateway is a point that acts as entrance to network and route the traffic of network station to outside network it must be configured properly in order for systems to communicate outside the network.



 And this connectivity can be checked by pinging from host to default-gateway Ip address.

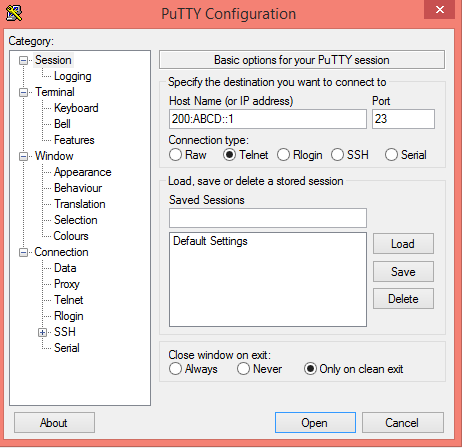
Making Telnet Access from Router

Same like IPv4 networks in IPv6 (internet protocol version six) telnet access can be made to remote access and to do that we can use command prompt (in window based operating system) Terminal(in Linux) ,CLI(command line interface in Cisco) and Putty. The procedure is same like IPv4 in the command line enter the command “**telnet ipv6 address”**



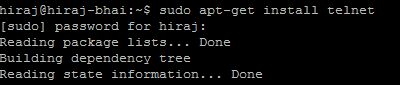
In case if you want to make telnet access from putty just put the IPV6 address of device with whom you want to make telnet connection and also from Linux terminal telnet access can be made.

In order to use the telnet services on cisco router or switches they must be enabled first the procedure will be same as discussed in previous chapters for Ipv4 (internet protocol version four)

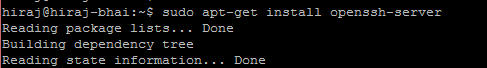


In order to enable telnet on Linux based system Go to terminal and enter the following command

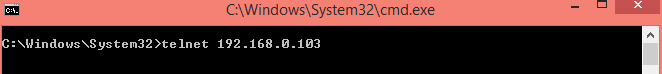
“Sudo apt-get install telnet” this command will install the telnet on the system and will enable the system to use the Telnet services.



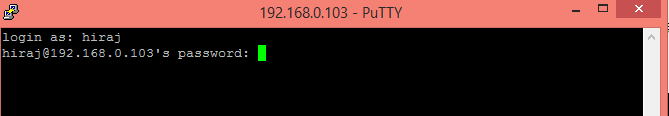
Or if you want to use the SSH (secure shell) services on Linux based system it can be enabled by entering these following command .

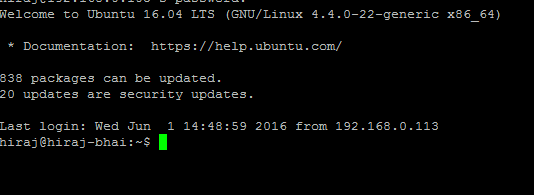


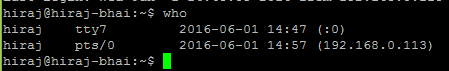
Once Telnet or SSH access has been enabled on Linux based operating system you can make remote access to the PC using any terminal and can install, uninstall , or can make changes remotely.



After making telnet or SSH connection it will ask about user name and password just provide the information and connection will be established.





If you are the one who is managing the network you must be able to keep track of who is having access to your Linux based Operating system or on cisco switch and Router. It can be checked by entering the “who” command. Thus by getting the information about devices that are having access these Devices can be blocked if they are un-authorized.

Domain Name system in IPv6

So with much information to be considered it is also import to consider DNS (domain name system) in IPv6 as in IPv4 if it is not properly configured you will not be able to have internet access because domain names will not be converted into IP addresses. There are two types of DNS server

1. **Primary DNS server**

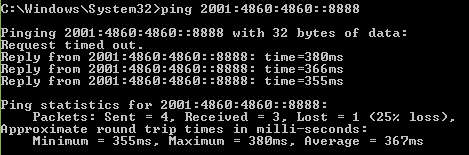
Primary DNS (domain name servers) reads data from the domain zone from a file located on the web server of hosting account. This server usually also sends information to secondary servers.

1. Secondary DNS server

Secondary DNS servers are also known slave server or simple slave receives zone data from primary server automatically.

A Secondary server can be configured inside the network all devices that are connected inside the network will make DNS query to that server that is located inside thus it will increase the efficiency and performance of network.

In order to check your connectivity to **Google DNS server** just use this command.

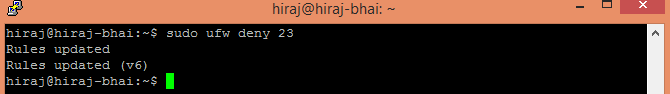


**Firewall in Linux based Operating System**

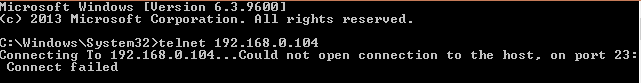
Same like in window based OS (operating system) in Linux based operating system it is always recommended to use Firewall in order to block un-intended traffic or to block certain type of traffic.in Linux UFW(un complicated firewall) is used it provides much more user friendly framework for managing net filter and command-line interface for working with firewall.

Other than that you can use command line as well some GUI(graphical user interface) that make its incredibly simple to use.

For example if you want to block telnet access to your Linux device enters the following command.



23 is port number that is used for Telnet access while port number 22 is dedicated for SSH connection. As from the above syntax Telnet is denied if you try to telnet the device connection will be refused by the remote host.



If want to allow Telnet access to remote host enter this command



The other basic available arguments for UFW (UN complicated firewall includes)

* Allow
* Deny
* Reject
* Limit

In order to enable UFW (uncomplicated fire wall) on your Linux device enter “Sudo ufw enable” without quote.



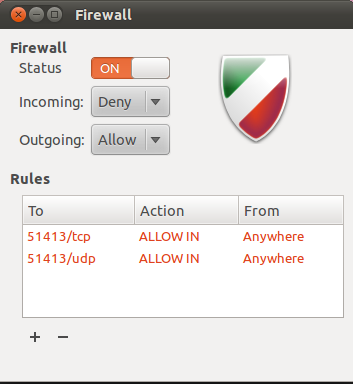
Or it can be disabled by the “Sudo ufw disable” command.



**GUFW is the GUI (graphical user interface) version of UFW that**  can also be used if you are newbie to Linux OS(operating system) . In order to install the GUFW just use this simple command

“**Sudo apt-get install gufw”**





Quick Quiz

1. SNMP is a protocol that is used for network management and it stand for?
2. **Simple network management protocol**
3. **Simply not my problem**
4. **Standard news management packet**
5. **Simple network message protocol**

Answer: A... SNMP stand for simple network management protocol

1. Which command is used to check how many connections are open on Linux machine?
2. Who
3. Whom
4. Sudo apt-get install
5. None of the above

The command **who** is used to check the connections.

1. In window based Operating we use **ipconfig**  to get IP address information in Linux which command is used to perform the same function?

1. Ifconfig
2. Ipconfig
3. Nslookup
4. Route

Answer: in Linux based Operating system “ifconfig” is interchangeable with ipconfig.

1. Can we enable Telnet and SSH both services on one device?
2. Yes
3. NO

Answer: Both services can be used at the same time.

1. Which command is used to install telnet on Linux?
2. Sudo apt-get install telnet
3. Sudo apt-get install talnet
4. Sudo apt-get add telnet
5. Sudo apt-get purge telnet

Answer: **Sudo apt-get install telnet**

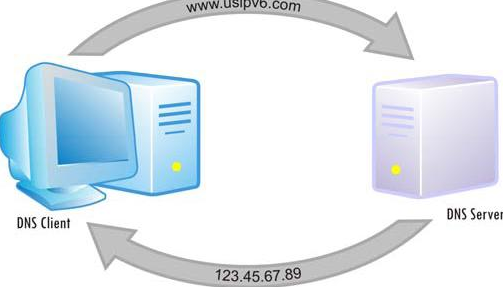
1. Which command is used to enable SSH service on Linux based operating system?
2. Sudo apt-get install openssh
3. Sudo apt-get install openssh-server
4. Sudo apt-get install SSH
5. None of the above

Answer: Sudo apt-get install openssh-server

1. Write down two types of DNS (Domain name system)?
2. Primary DNS
3. Secondary DNS

1. Write down three Differences between Primary and secondary DNS (domain name system)?

|  |  |
| --- | --- |
| **Primary DNS** | **Secondary DNS** |
| It is Authoritative server for the zone. | It is backup DNS server. |
| It can read/write copy of DNS server | It can only read the copy of DNS server |
| One DNS server can have one primary DNS server | There can be up to 255 secondary DNS servers. |



1. Write dow the three advantages of OSI(open system inter conenction model) ?
2. It prevents changes from one layer to take affect on other layers
3. Standardrization of network components allows multiple vendor development
4. It allows different types of hardware and software to communicate with each other.
5. **Write down the advantages of each Layer in OSI model ?**

