**Networking**

#Configure your own resolver name server.

#install Ubuntu bind package

Whois google.com

Dig google.com

Dig +tree google.com

telnet Microsoft.com 80

traceroute google.com #Show the google route table details

tcpdump #Show the history of websites recently accessed

netstat -p #All open ports details

dhcp #Used for private network creation in local and give IP each server

netstat -natpal | grep httpd # to find the assigned port of httpd

Check all IPtables Firewall Rules

iptables -L -n -v

iptables -t nat -L -v -n

* **-L** : List rules.
* **-v** : Display detailed information. This option makes the list command show the interface name, the rule options, and the TOS masks. The packet and byte counters are also listed, with the suffix ‘K’, ‘M’ or ‘G’ for 1000, 1,000,000 and 1,000,000,000 multipliers respectively.
* **-n** : Display IP address and port in numeric format. Do not use DNS to resolve names. This will speed up listing.

### Block Specific IP Address in IPtables Firewall

iptables -A INPUT -s xxx.xxx.xxx.xxx -j DROP

iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx -j DROP

### Unblock IP Address in IPtables Firewall

iptables -D INPUT -s xxx.xxx.xxx.xxx -j DROP

### Block Specific Port on IPtables Firewall

iptables -A OUTPUT -p tcp --dport xxx -j DROP

iptables -A INPUT -p tcp --dport xxx -j ACCEPT

### Allow Multiple Ports on IPtables using Multiport

# iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -j ACCEPT

# iptables -A OUTPUT -p tcp -m multiport --sports 22,80,443 -j ACCEPT

### Allow Specific Network Range on Particular Port on IPtables

iptables -A OUTPUT -p tcp -d 192.168.100.0/24 --dport 22 -j ACCEPT

### Block Facebook on IPtables Firewall

host facebook.com

facebook.com has address 66.220.15

whois 66.220.156.68 | grep CIDR

CIDR: 66.220.144.0/20 6.68

iptables -A OUTPUT -p tcp -d 66.220.144.0/20 -j DROP

### Setup Port Forwarding in IPtables

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j REDIRECT --to-port 2525

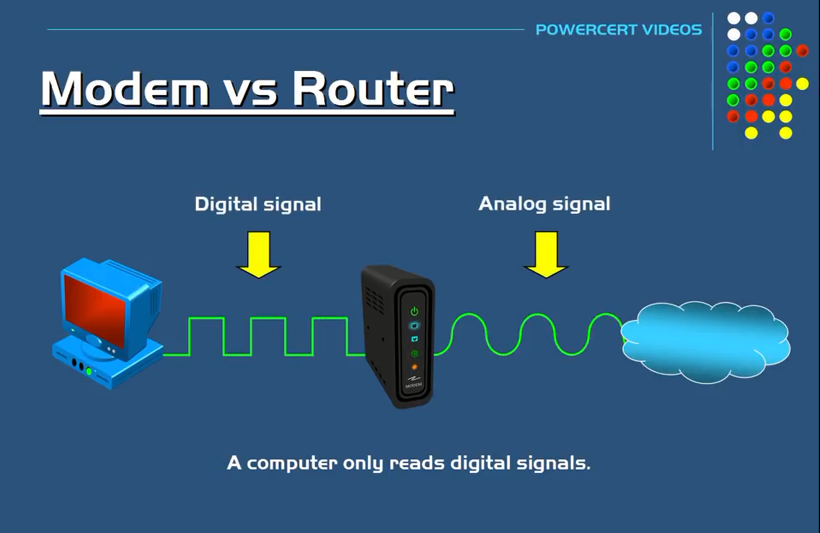
### Block Network Flood on Apache Port with IPtables

iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/minute --limit-burst 200 -j ACCEPT

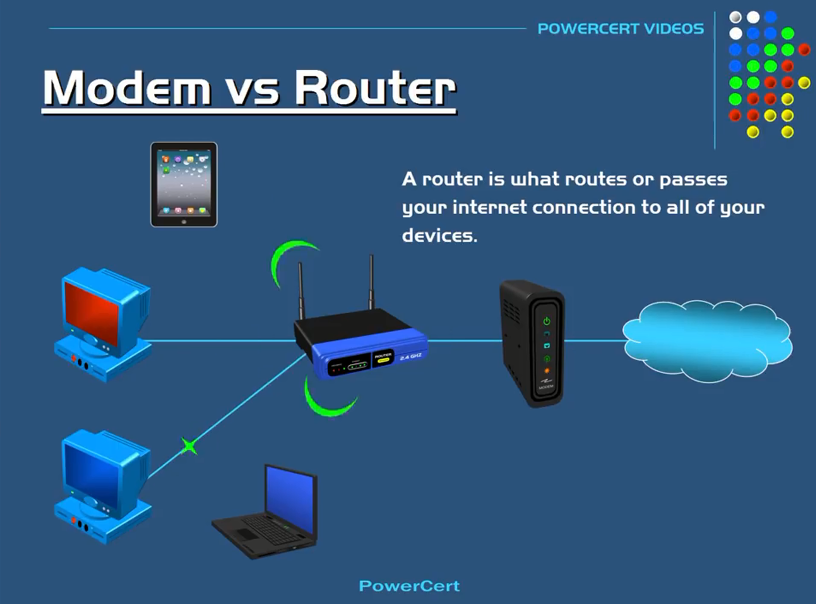
### Block Incoming Ping Requests on IPtables

iptables -A INPUT -p icmp -i eth0 -j DROP

**Modem: -**



**Router: -**



**Hub: -**

