A

Project Report

on

***Home wireless network and security***

IS

SUBMITTED IN PARTIAL FULFILMENT

FOR THR SUBJECT OF

***CS470-***  ***Network Engineering and Management***

***(MS-Computer Science)***

*Of*



**NORTHWESTERN POLYTECHNIC UNIVERSITY**

**47671 Westinghouse Dr, Fremont, CA 94539**

**Academic Year: Summer 2013**

**Course Instructor: Submitted by:**

Dr. Howard Liu Sonali Phatak

|  |  |  |
| --- | --- | --- |
| **INDEX** | | |
| **1** | **Introduction** | **3** |
| **2** | **Home wireless Network** | **4** |
| **3** | **design your home wireless** | **5** |
| **4** | **Outline of the process** | **10** |
| **5** | **Default Configuration Settings** | **11** |
| **6** | **Internet Protocol stack** | **13** |
| **7** | **Data link layer Security** | **15** |
| **8** | **Constant firmware update** | **17** |
| **9** | **stealth mode** | **18** |
| **10** | **TCP/UDP port scan** | **19** |
| **11** | **packet flood** | **21** |
| **12** | **DHCP, NAT, DNS and other protocols** | **22** |
| **13** | **encryption protocols** | **39** |
| **14** | **firewall** | **37** |
| **15** | **secure your wireless network** | **41** |
| **16** | **Conclusion** | **44** |

1. **Introduction :-**

This case study on the Home wireless network and security. It is with details and description. Security is most important part of networking, it describe wireless network security implementation at home. It also describes roles of the protocol on the networks.

For better understanding we use Packet and Traffic Capture Tool Wireshark, For browsing Google.

1. Home wireless network

This is my home wireless network.

****

**Netgear Wireless Internet Router**

**192.168.1.1 /26**

**Canon® PIXMA® MG5420 Wireless Inkjet Printer**

**192.168.1.6 /26**

**Lenovo IdeaPad Yoga 13**

**192.168.1.7/26**

**Apple imac desktop computer**

**192.168.1.10 /26**

**Xbox 360**

Xbox 360 120 GB

**192.168.1.9/26**

HD2 Windows phone

Internet

**Dell XPS 14 Ultrabook**

**192.168.1.8/26**

Comcast ISP

IP:24.6.188.137

Mask:255.255.248.0

GW:24.6.184.1

Modem

**s**

****

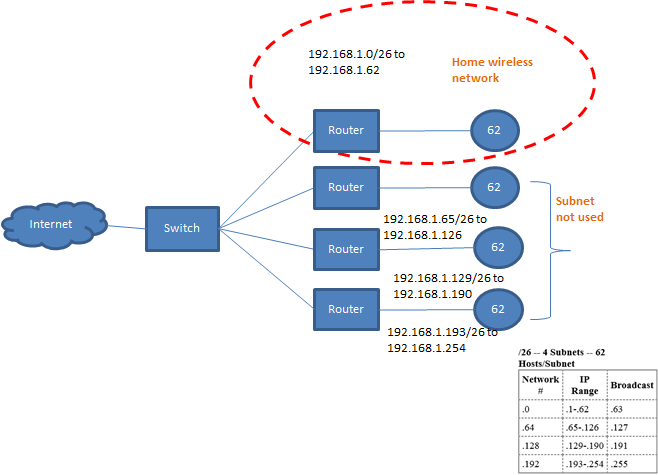
This diagram shows the home wireless network. In my Home network I use **NetGear N300 Wireless Router** to connect to the devices.

Q1. assume the number of devices need to be connected matches the last 2 digits of your student ID (or if the 2 digit number is less than 9, add 8 to your last two digit number);

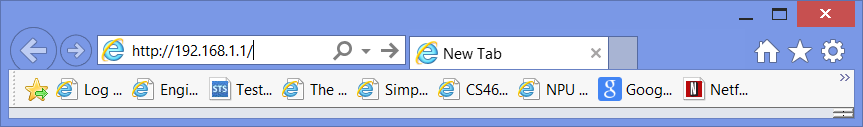
1. design your home wireless network and explain your rational behind your design;

**Assumption:** Maximum allowed devices on the Home network assumed to be 62 instead of 60 because of subnetting limitation

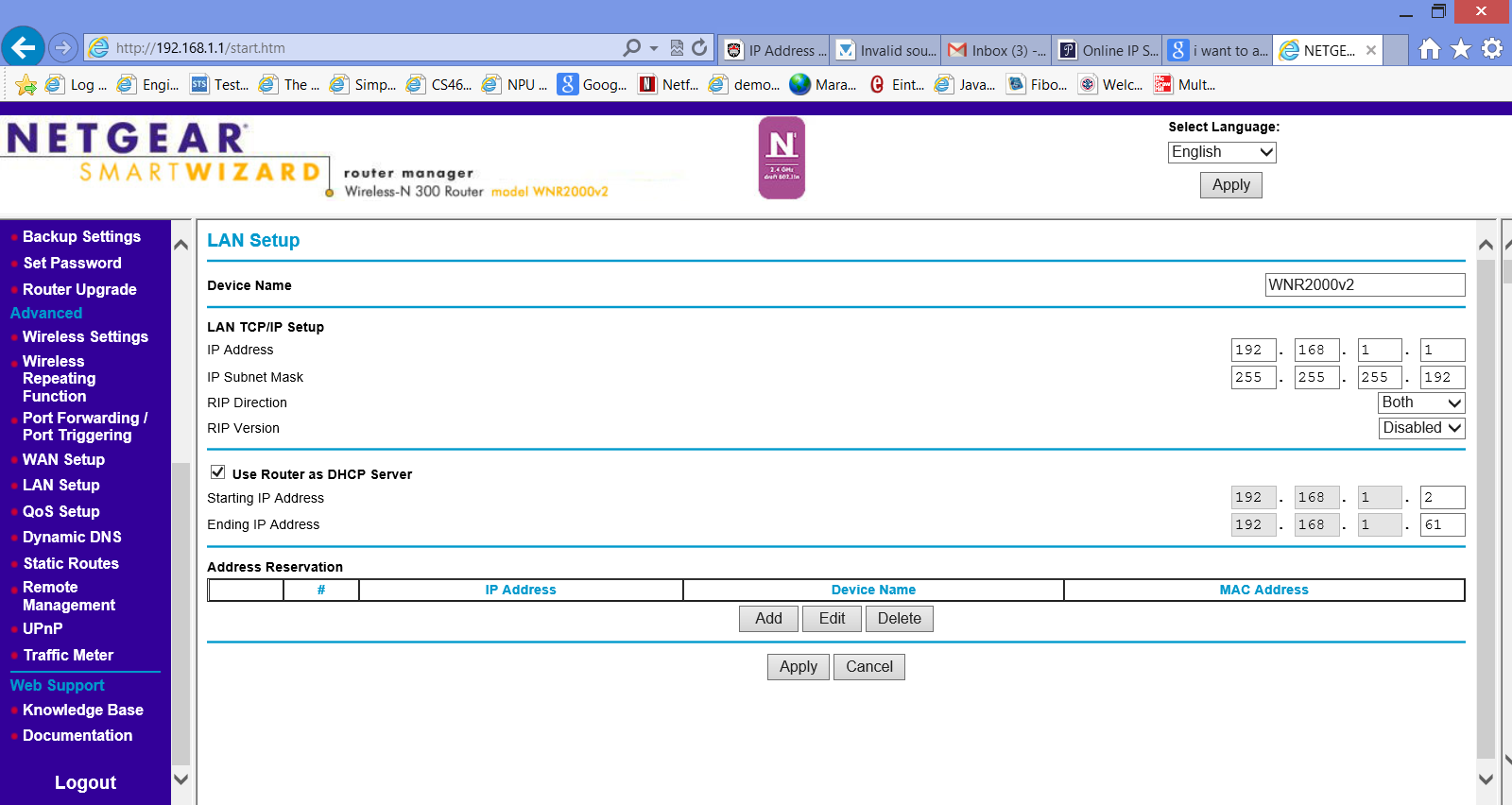
**Design:** The home wireless network is using one of the four subnets possible. The subet used (say Network A)uses a single wireless router. The Network A subnet could have maximum of 62 allowed host.



1. My student ID is 10260, so I have to assume I have 60 devices. for that in make changes in my home wireless network.
2. NetGear N300 Wireless Router is being used to setup the home network.
3. The network uses WIFI to connect devices to the router.
4. For changing the setting of router first enter in browser http://192.168.1.1



1. we have to provide username and password for your router after login, I made changes in the router configuration.
2. Go to the LAN setup-> IP address . My IP Address is 192.168.1.5. In my case I have to add 60 hosts.

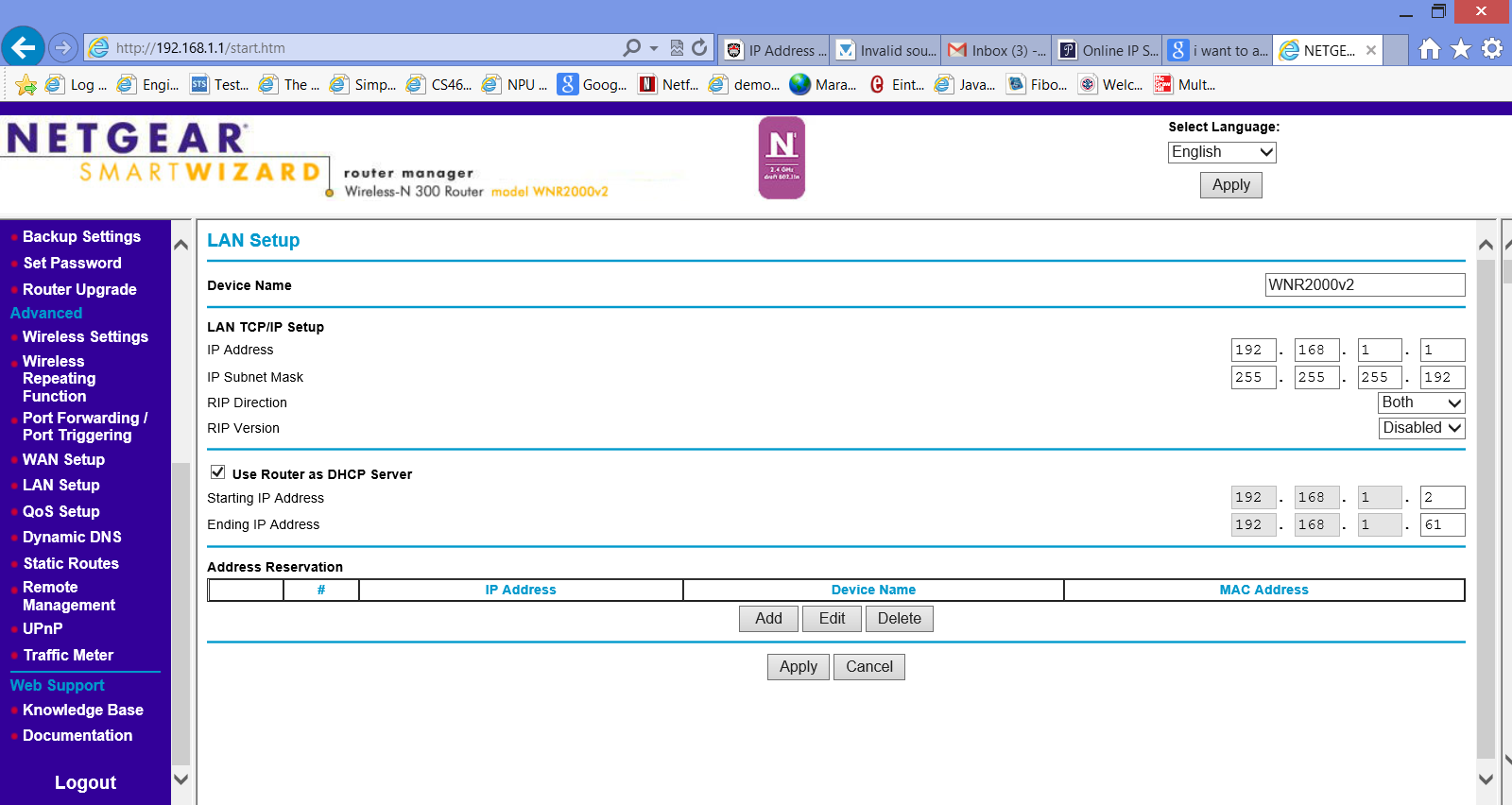


* **Host address range** :- 192.168.1.1 - 192.168.1.62
* **Subnet Id** :- 192.168.1.0
* **Broadcast Id** :- 192.168.1.63
* **Maximum subnets** :- 4
* **Subnet Mask** :- 255.255.255.192
* **First Octet Range :-** 192 – 223
* **Host per subnet :-** 62

**Q2.**  Outline the process you approach the network design, identify netmask, number of usable IP address; IP address range, subnet and broadcast address for each subnet;:

* **IP address range** :- 192.168.1.1 - 192.168.1.62
* **Subnet Id** :- 192.168.1.0
* **Broadcast Id** :- 192.168.1.63
* **Maximum subnets** :- 4
* **Subnet Mask** :- 255.255.255.192
* **First Octet Range :-** 192 – 223
* **Host per subnet :-** 62
* **number of usable IP address-**62

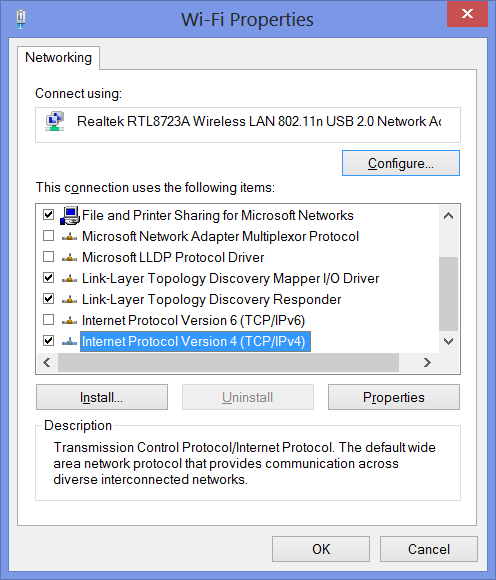
**DHCP server in router is configured to assign 192.168.1.2 - 192.168.1.61 (60 devices)**



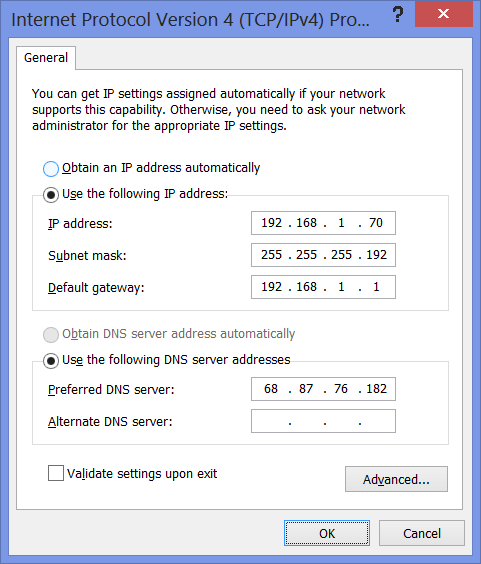
* DHCP automatically assigns IP address to any other devices which connect to my device within the range 192.168.1.1 to 192.168.1.62 so this set up can accommodate total of 60 wireless devices.

I check this setting by giving large number than 62.

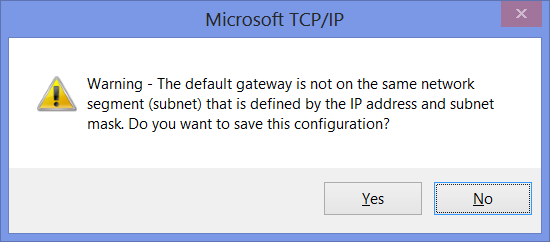
* Got to Control Panel->Network and Internet->Network Connections
* Write click Wifi -> select Wifi properties



* Click on Internet Protocol Version 4(TCP/IPv4)
* Write click properties then Internet Protocol Version4 window open

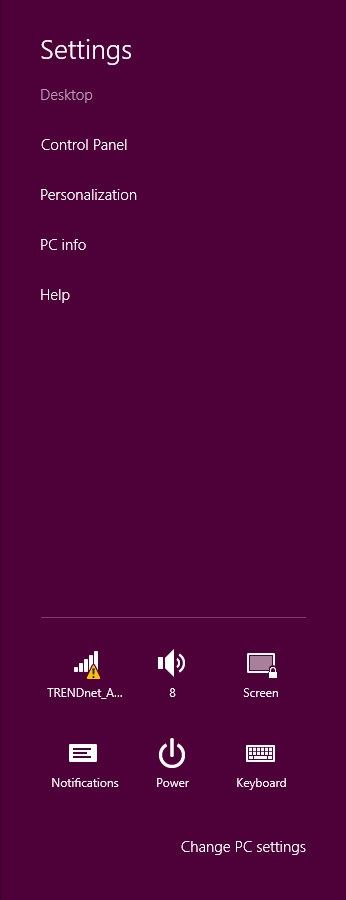


* Give IP address ,subnet mask ,default gateway,preferred DNS server
* When I give more than 62 in IP address

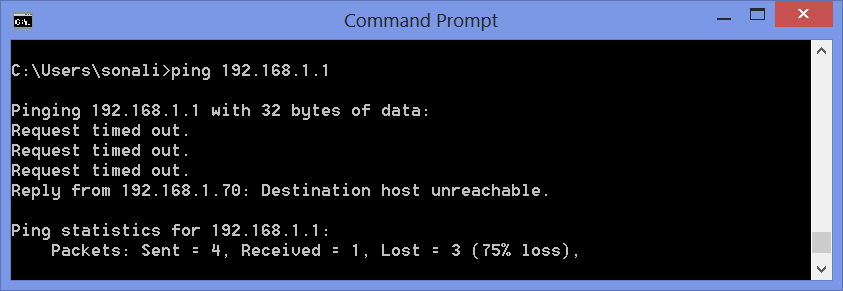


* It show me the error message.
* That means I can connect only 62 devices to my network.

If my IP address is already greater than 62. And I change the setting. Assign 62 devices.



Limited access



We cannot connect to the internet.

**Q3. What are your Default Configuration Settings :-**

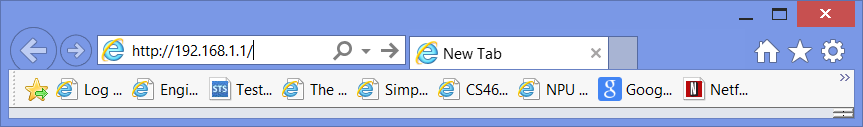
**Router Login URL** :-http://www. routerlogin.net or http://www.routerlogin.com

* **Login name** :- admin
* **Login password** :- password
* **Router Subnet:-** 255.255.255.0
* **Router LAN IP address:-** 192.168.1.1
* **Host Address Range :-** 192.168.1.1 - 192.168.1.254
* **Subnet ID :-** 192.168.1.0
* **Broadcast Address :-** 192.168.1.255
* **Maximum Subnets :-** 1
* **Hosts per Subnet:-**254

1. **Modify Default admin account password:-**

Steep:1 -Connect to your wireless network.

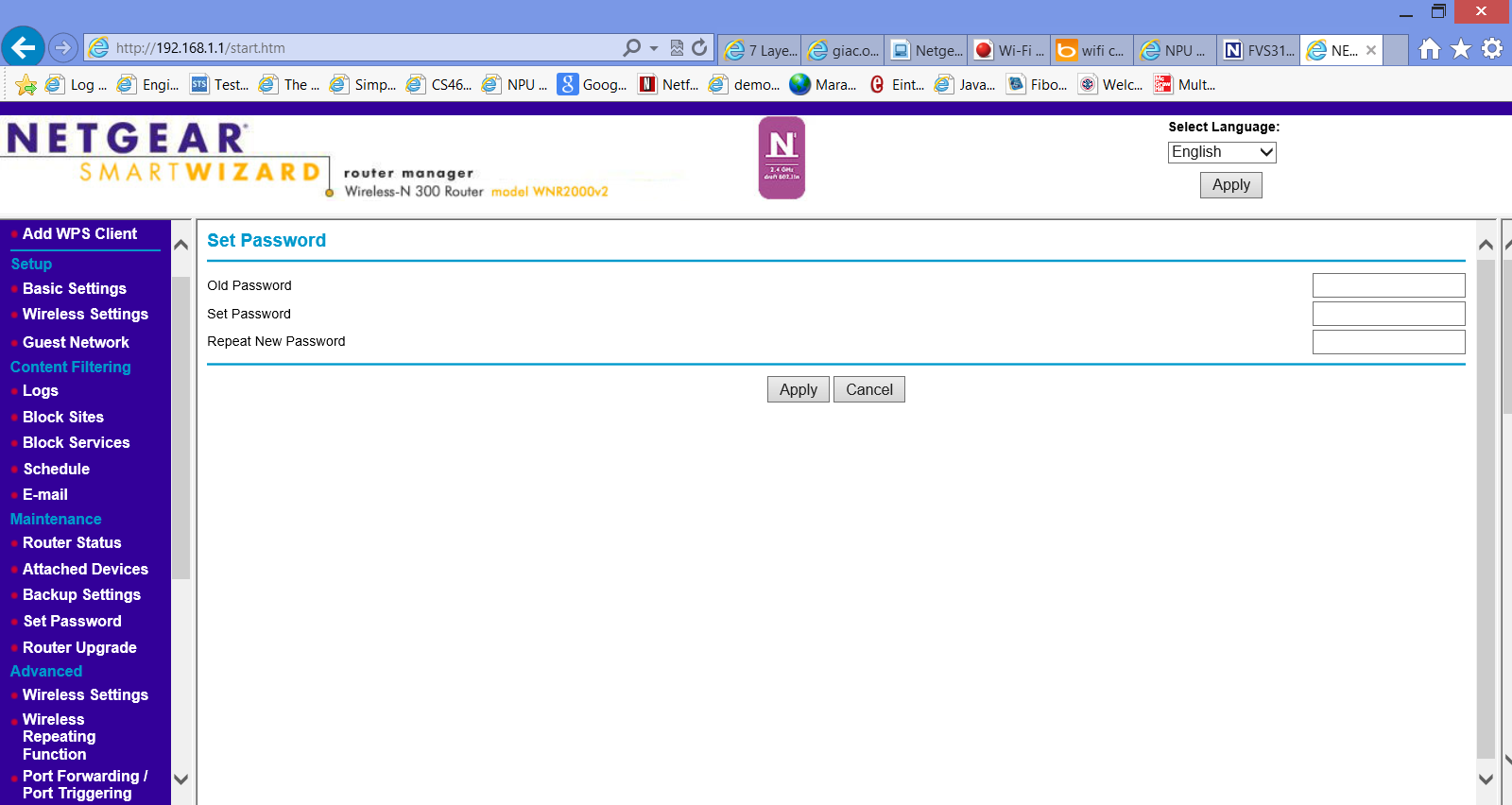
Steep:2 -Open your Web browser and type in the Web address <http://www.192.168.1.1>



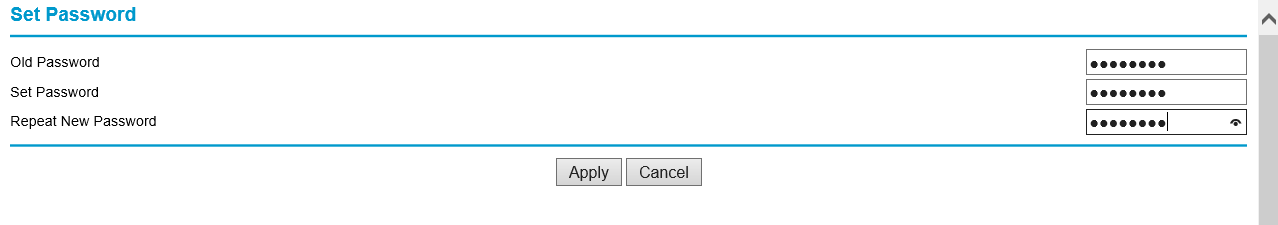
Steep:3- Press Enter

Steep:4 -Type in the user name and password

Steep:5 -The Router Manager window will display



Steep:6 -select the Set Password menu item



Steep: 7 -Type in the old password , type new password set password and retype new password.

Steep: 8 -Click the Apply button Then default password will be change.

**Q4. Security Per Internet Protocol stack:-**

**Secure protocols like HTTPS**

**TLS, SSL**

**Security provided at each layer**

Layer

Physical

Data link layer

Network

Transport

Application

**Network layer firewalls (packet filters),** **Stealth mode**

**MAC address filtering, constant firmware update**

**WEP, WPA like encryption for wireless data**

The functions of the five layers are:

**Application Layer:** security use **protecting Web applicatio**ns at the application layer. This layer uses end-to-end protocols, in which end systems are responsible for providing security for the application protocol. Secure HyperText Transport Protocol (SHTTP). The Secure Multipurpose Internet Mail Extensions (S/MIME) protocol was designed to build security functionality on top of the MIME protocol to be easily integrated into e-mail and messaging products. Use HTTPS protocol for more security purpose.

**Transport Layer:**

Transport layer security:- It has TLS (Transport layer security ),SSL These protocols use encryption keys to ensure private connections.

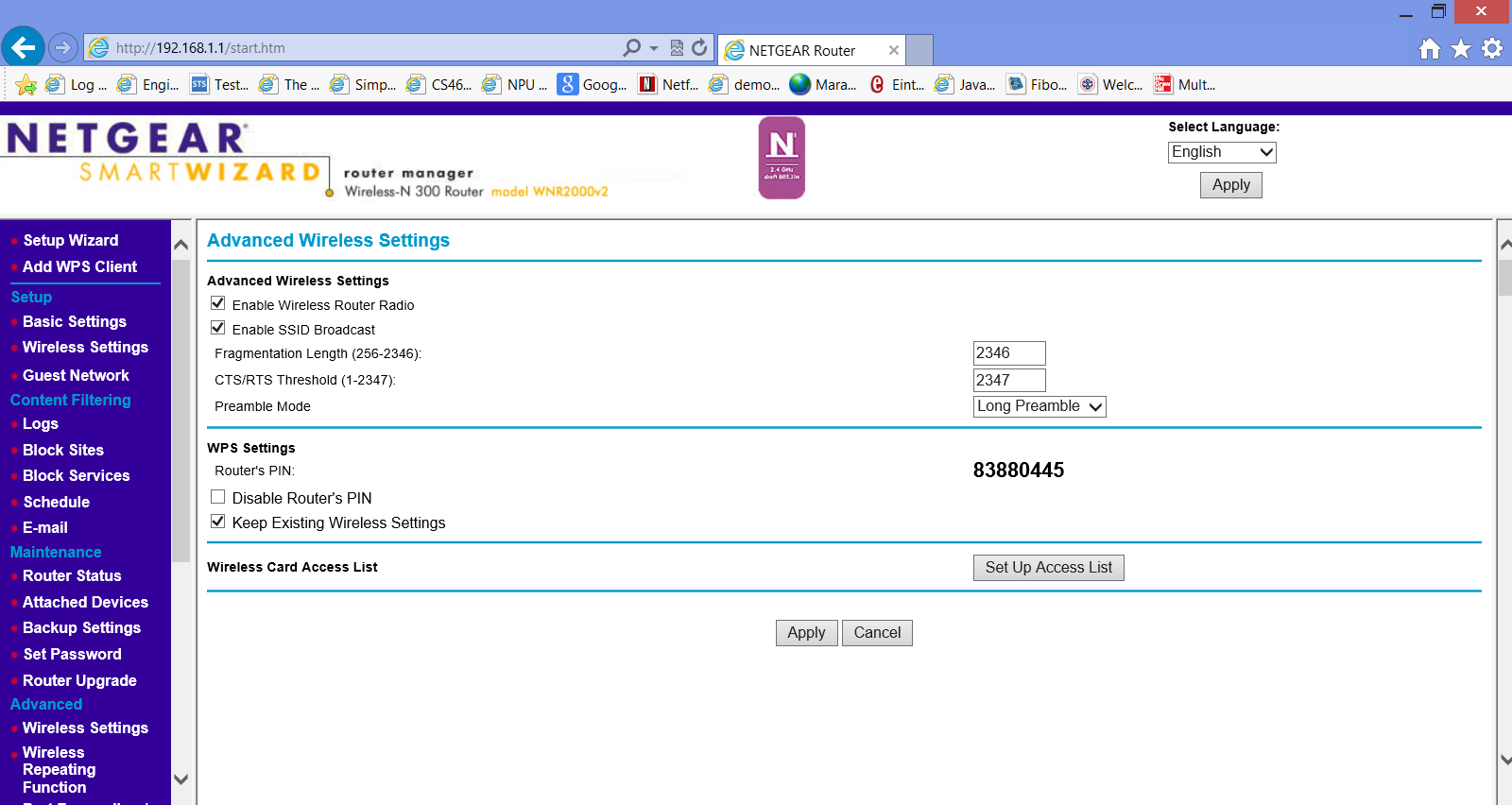
**Network Layer Security:**

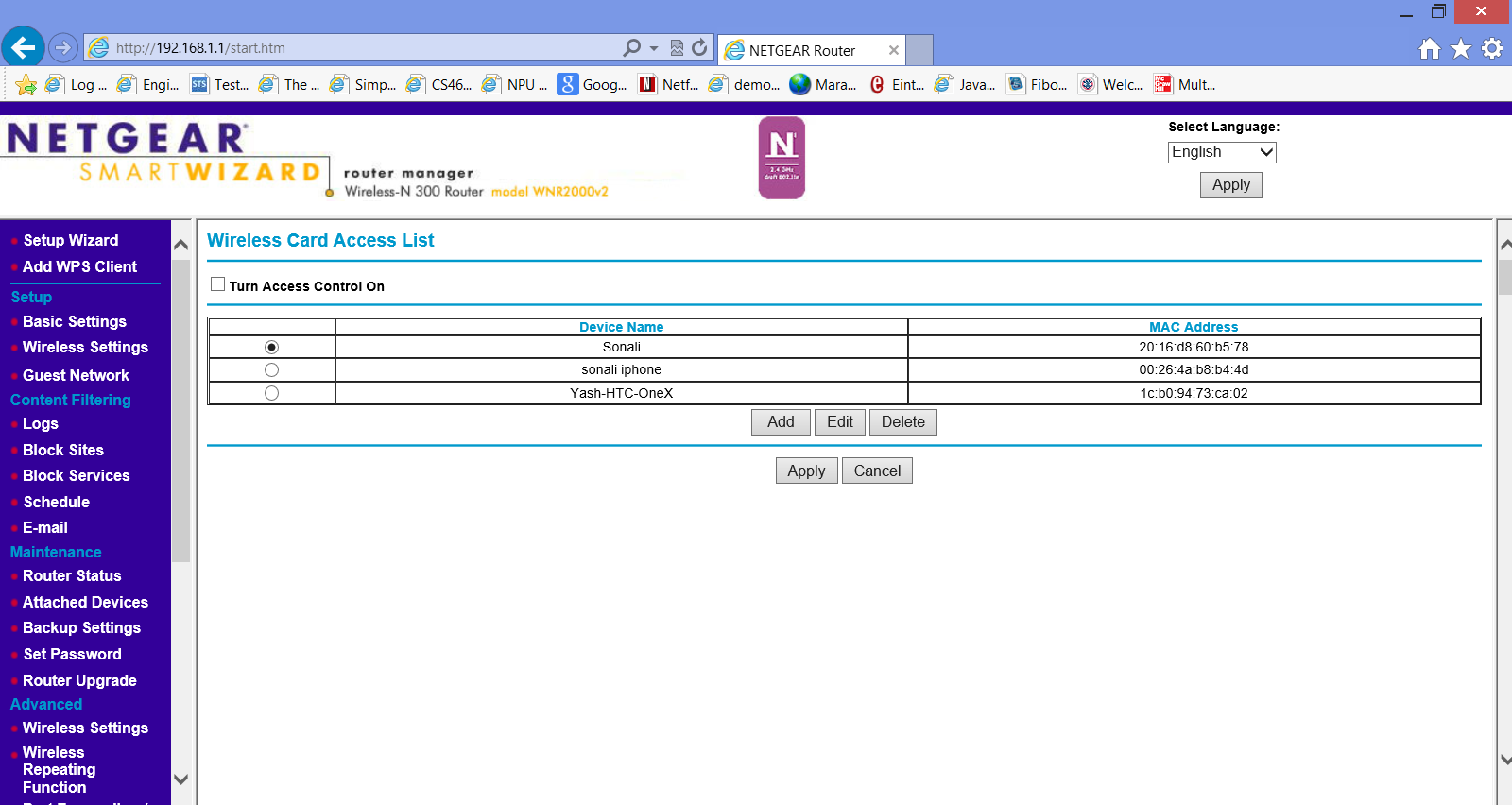
Network layer security:- **Network firewalls operate by blocking IP addresses, Routers is also provide network layer security.** Authenticates an IP address to the network is based on user of the system.

It protects all IP datagrams based on the source or destination address and Scope of data protection from system to gateway or endpoint.

**MAC layer (Data link) Security:-** The data link layer can done with port security, MAC address filtering, and wireless encryption.

1. MAC addresses filtering and -> Go to Advanced Wireless Settings -> [**Wireless Card Access List**](javascript:loadhelp('WLG_adv','access'))





Then add devices, then click apply.

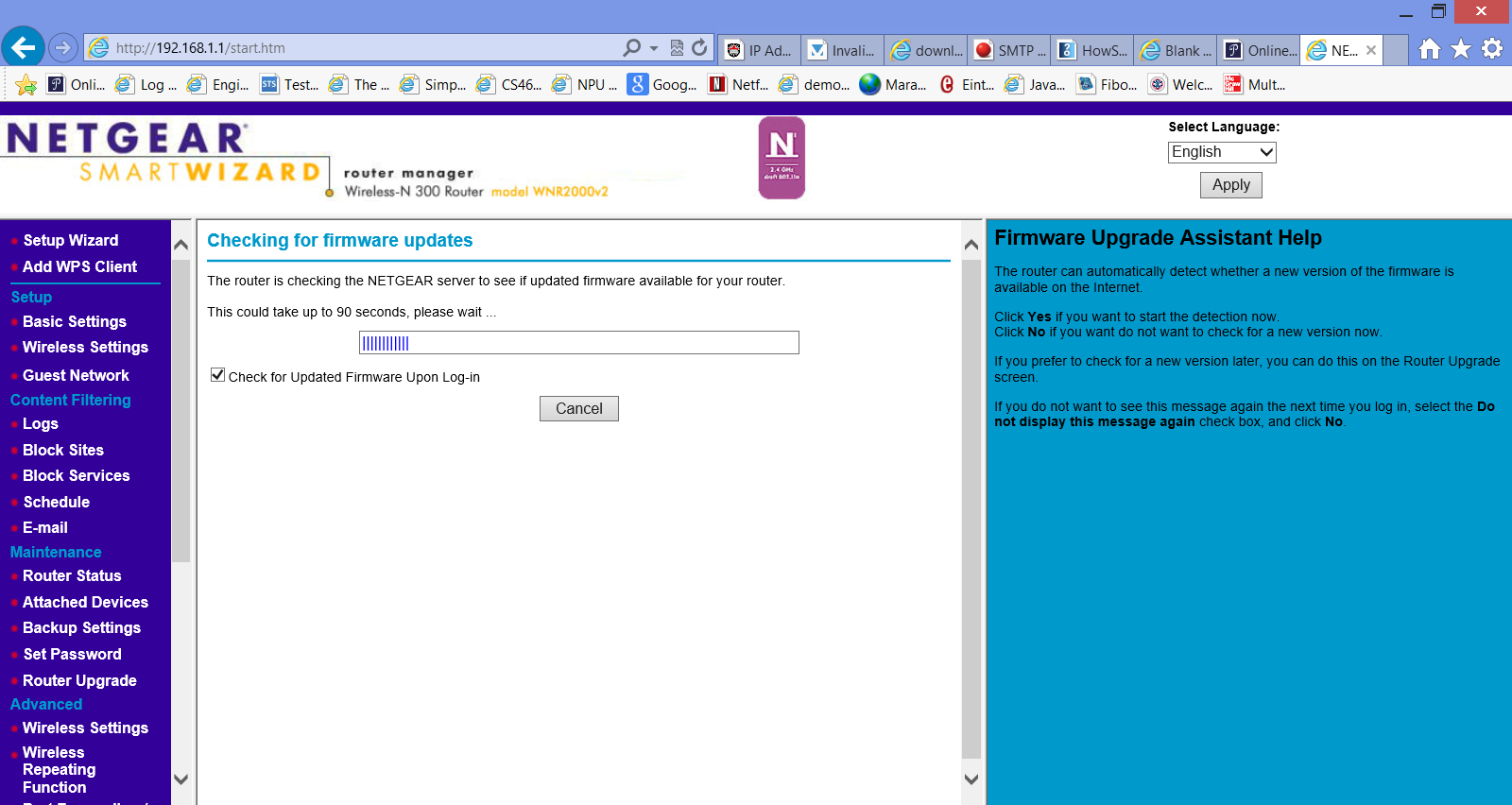
->This is for more security purpose, by default, any wireless PC that is configured with the correct SSID will be allowed access to the wireless network. For increasing security**, we can restrict access to the wireless network to allow only specific PCs based on their MAC addresses.**

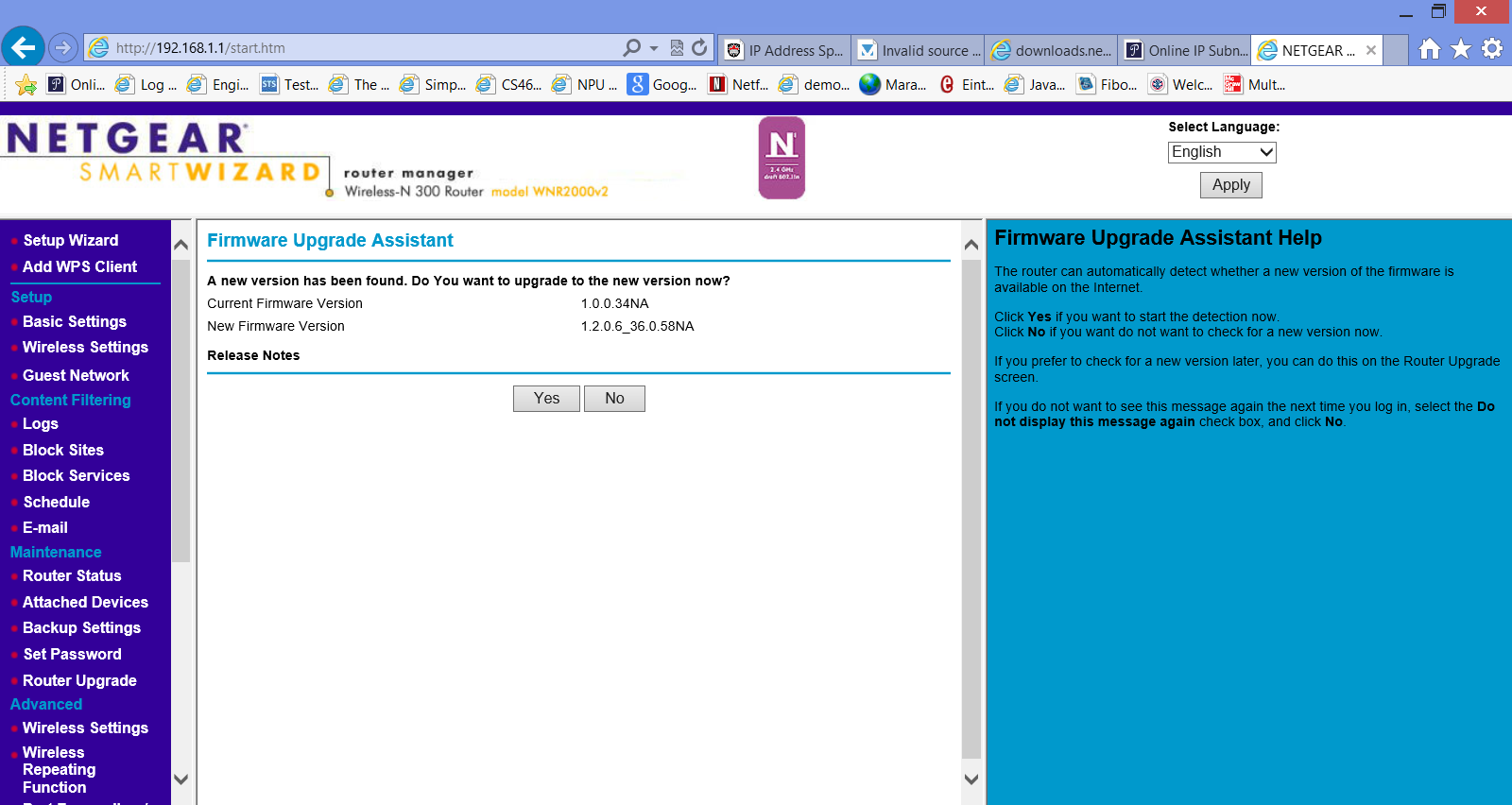
I add some devices giving device name and those devices have their MAC address. With the help of Access Control List, devices that are not on the list are not allowed to connect to my network.

1. **Constant firmware update at link layer:-**

We do constant firmware update for updating firmware includes fixing bugs or adding new features to the device.

The router can automatically detect whether a new version of the firmware is available on the Internet. If new version available it display it.





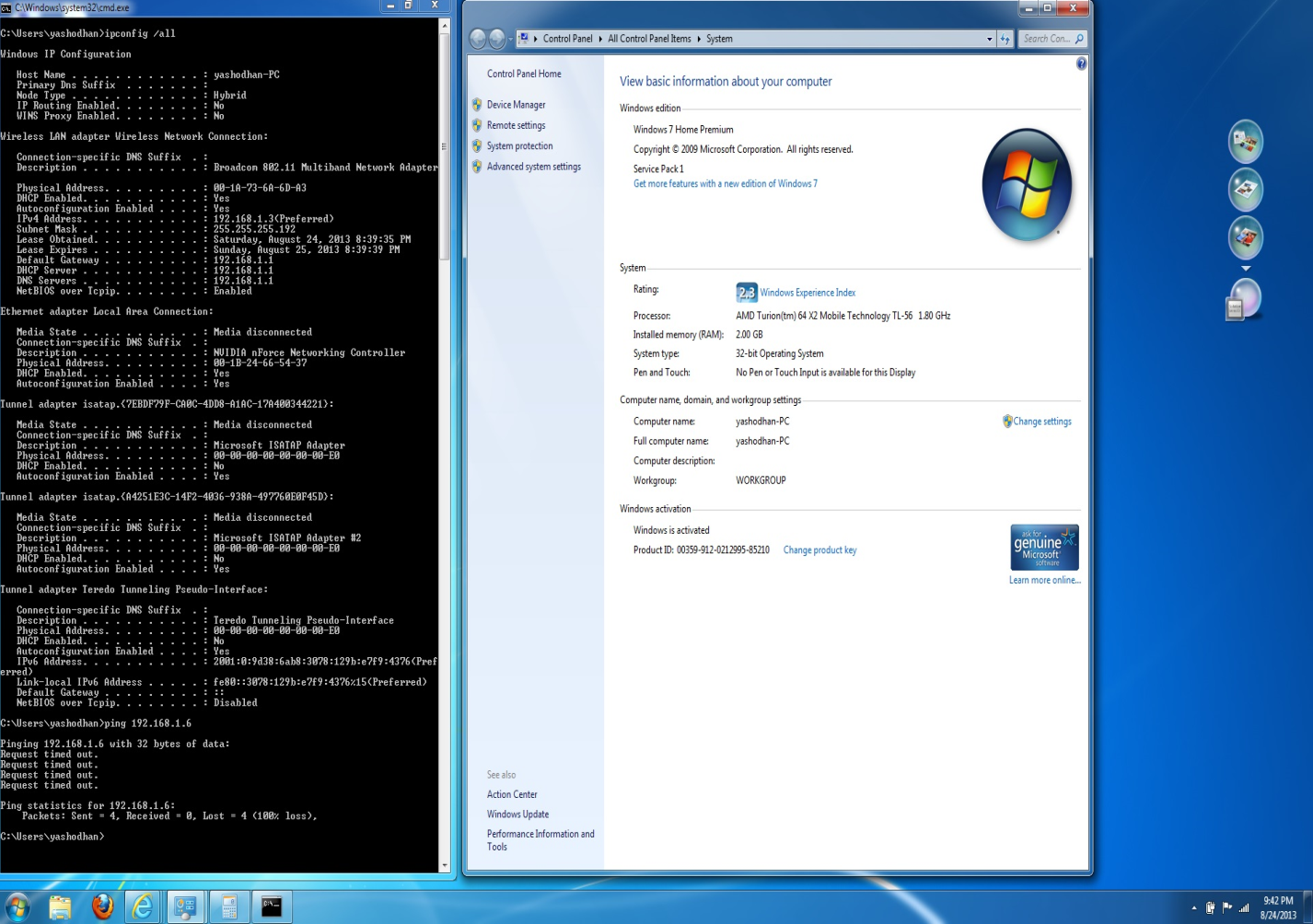
Firmware updates usually come from the manufacturer of the product (like router).

1. **what is stealth mode:-**

In this mode all activity initiated by the user is allowed. Activity such as remote connection to your computer, checking with the Ping utility, etc.

This means that your computer becomes "**invisible"** from the the others. Hackers cannot attack to your computer. The stealth mode is used for preventing all types of DoS (Denial of Service) attacks.

stealth mode is used in firewall to hide information of our computer from others like malicious user. Stealth mode in Windows Firewall with Advanced Security is designed to help protect against this attack. Stealth mode blocks outgoing ICMP unreachable and TCP reset messages for a port when no application is listening on that port.

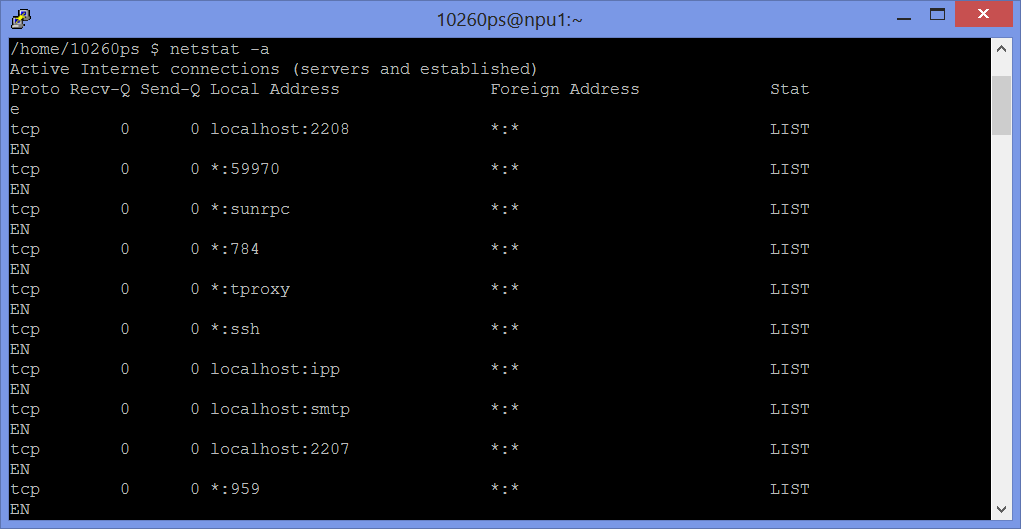


On Windows stealth mode is enabled by default. This is verified by trying to ping the local machine from another machine on the network (with IP 192.168.1.3). Local machine couldn’t be pinged as stealth mode is blocking ICMP response.

1. **What is TCP/UDP port scan**:-

:- firewall Detects TCP or UDP port scans and drops packet if detected.

**TCP port scan:-** TCP provides connection oriented services . In computer system running TCP/IP to determine which TCP and UDP ports are open and listening, which display all of the services that system running. If port is open OS completes its three way handshaking after that port scanner close that connection because Denial-of-service attack (Dos) cannot happen.



It display which process are which port(TCP/UDP) are listing.

TCP scanning can be implicitly specified with a “–sT” command line argument.

TCP Connect succeeds (three way TCP handshake completes) :- Port is open

TCP Connect fails (three way TCP handshake does not complete):- Port is closed

**UDP port scanning:-** UDP is connectionless protocol, there is no three way handshaking because of that UDP port scanning is more complex and it does not send the acknowledgement. If the port is open the packet is accepted and there is no response come .if UDP port is close and packet send to it the respond come with ICMP port unreachable message.

If the response is not come then port is open ,if response(Error message) come then the port is close.

1. **how to determine an invalid source/destination IP address:-**

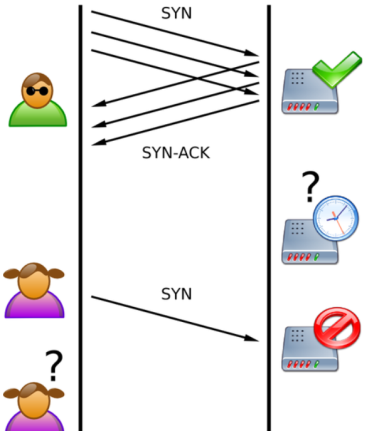
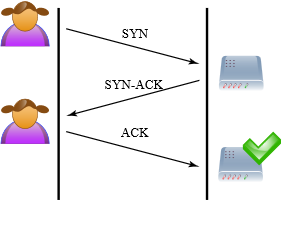
In network communication like sending email , transferring fails or requesting web page it need valid source and destination IP address. Source IP address defines sender and destination IP address defines receiver. Spoofed IP addresses means to gain unauthorized access to a system.

Scans inbound and outbound packets and drops packet if the IP source address is broadcast or multicast, the TCP destination IP address is not unicast, the IP source and destinationaddress are the same or an invalid IP source received from private/home network.

1. **what are packet flood (SYN/ICMP/other) and how to protect your network from such attacks:-**

Flooding is a routing algorithm, I this every packet is sent by every outgoing link but not in the arrival link.

SYN flood:- it is one type of denial-of-service attack, the attacker use fake IP address and send repeatedly SYN (synchronization) packets to the every port on the server, and consume the resources of the server.



3 way handshaking(normal) SYN(flood).

Image source: http://en.wikipedia.org/wiki/File:Tcp\_synflood.png

In three way handshaking Client sends SYN to server then Server sends SYN-ACK to client and client send ACK to server. This is the normal way but in SYN flood attack attacker sends repeatedly SYN and the ACK packet is never sent back by the client and that connection is a half-open connection. For preventing SYN attack we can use :-SYN Cookie and using Safe Reset

In SYN Cookies: - SYN Cookie, the firewall work as a proxy between the client and the server. There are two connections are established, one connection is between the client and firewall, and the another is between the firewall and the server. All the data packets send between the client and the server and it will be forwarded by the firewall.

IN SYN cookies: - a firewall use Safe Reset authentication.it check a client in first request, and normal services will not be affected even if the packets replied by the server to the client do not pass through the firewall. Safe Reset is like unidirectional proxy.

**Internet Control Message Protocol (ICMP) flood :-**  It is also called as ping flood and it is kind of Denial of Service attack that sends large amounts of ICMP packets to a machine for crash the transmission control protocol/Internet protocol (TCP/IP) stack on the machine.

Internet Control Message Protocol (ICMP) is a connectionless protocol it is used for IP operations, diagnostics, and errors. ICMP flood send large numbers of ICMP packets (ping packets) to the server and server cannot respond.

Firewall Detects any SYN, UDP, ICMP or other flood and stops them if it detected.

For securing our network from ICMP flood we have to disable IP-directed broadcasts to all of our routers and do this configuration.

1. Allow Ping –ICMP Echo-Request outbound and Echo-Reply messages inbound.

2. Allow Traceroute –TTL-Exceeded and Port-Unreachable messages inbound.

3. Allow Path MTU –ICMP Fragmentation-Df-Set messages inbound.

4. Block all other ICMP traffic.

These 4 steep provide a lot of network security.

**UDP flood attack:-** UDP provide unreliable services and it is connectionless protocol . UDP flood attack is also denial-of-service (DoS) attack. This attack sends large number of UDP packets.

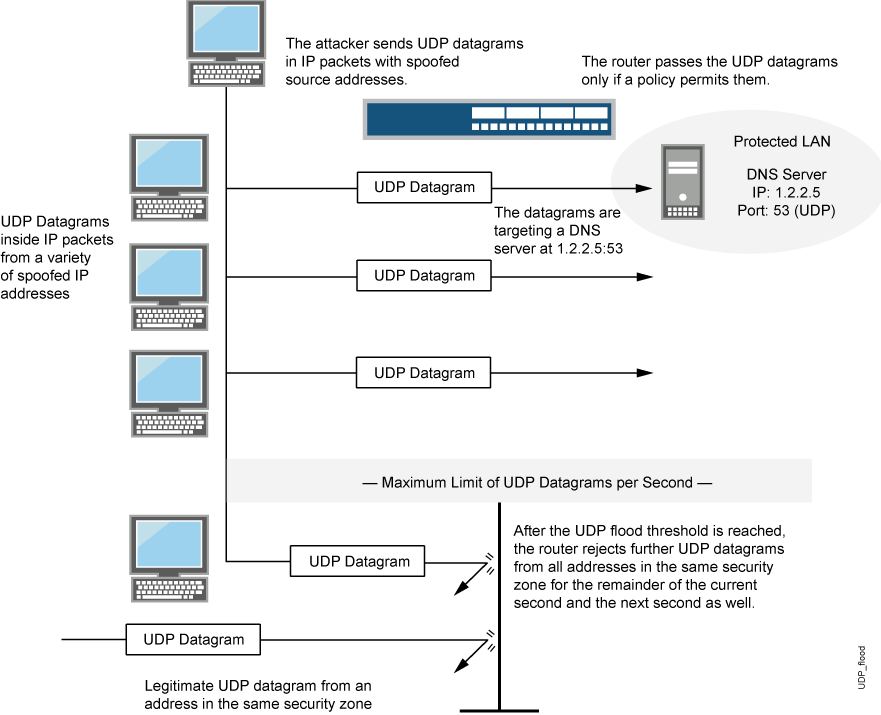


Image source:- http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60351.html

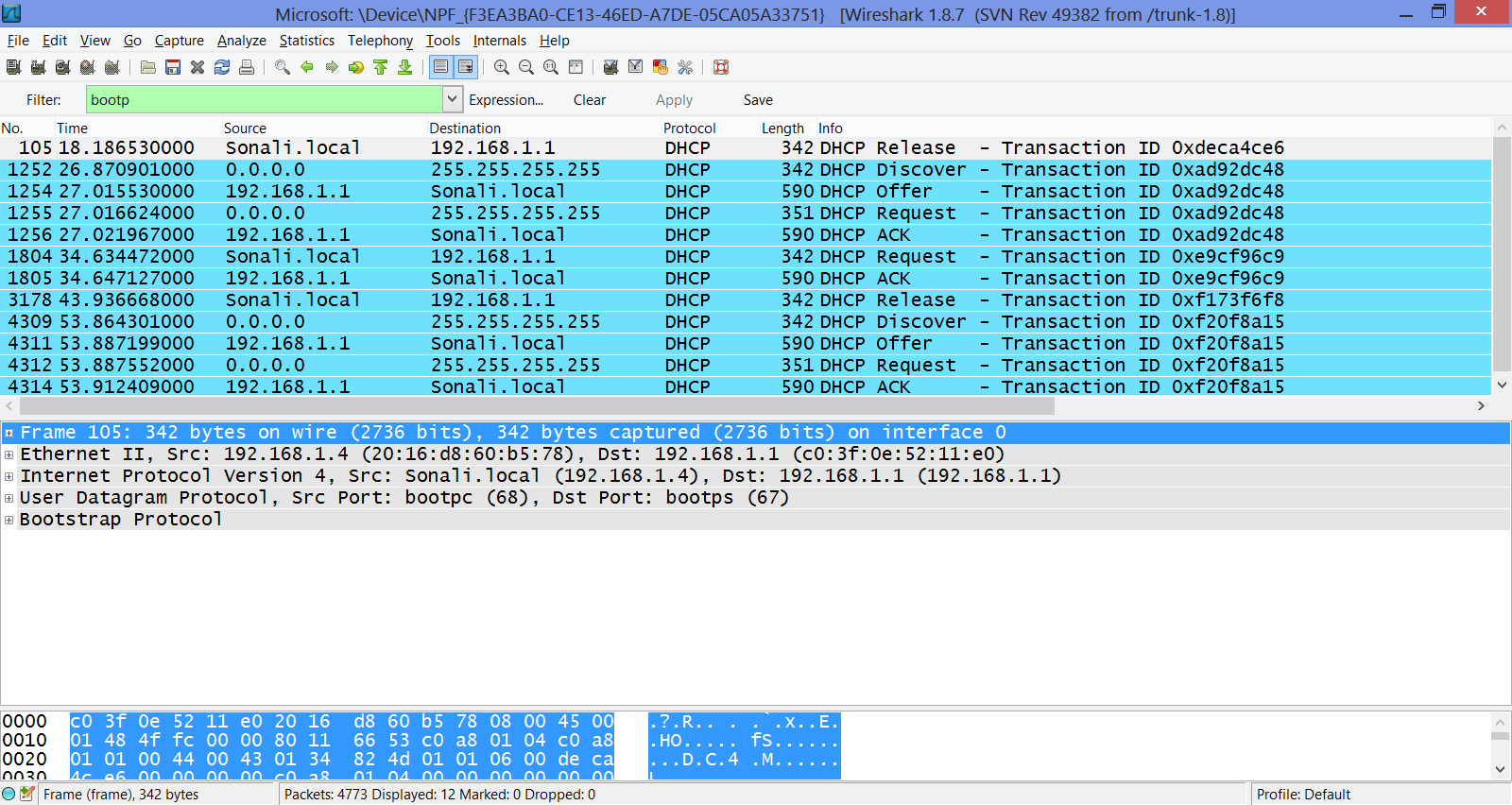
Q5. **Roles of Protocols**

1. **DHCP:-** DHCP is TCP/IP based network protocol, it assign a unique IP address to each computer. An IP address is a unique numeric identifier that identifies computers on the network. The Dynamic Host Configuration Protocol (DHCP) is a service that can be implemented to automatically assign unique IP addresses to DHCP clients.

DHCP runs at the application layer of the TCP/IP protocol stack to provide the following functions in TCP/IP networks:

* Dynamically assign IP addresses to DHCP clients.
* Allocate the following information to DHCP clients:
* Subnet masks information.
* Default gateway IP addresses.
* Domain Name System (DNS) IP addresses.
* Windows Internet Naming Service (WINS) IP addresses.

In Wirshark this capture show the DHCP requests and responses.



A host uses DHCP to getting an IP address, a host’s IP address is not confirmed until the last four-message exchange. If the For each of the fourDHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and Destination IP addresses.

In this capture the communication and IP address are:

Discover source address 0.0.0.0 Destination address 255.255.255.255

Offer source address 192.168.1.1 Destination address 192.168.1.4

Request source address 0.0.0.0 Destination address 255.255.255.255

Ack DHCP address 192.168.1.1 Destination address 192.168.1.4





DHCP ACK

DHCP REQUEST

DHCP OFFER

DHCP DICOVER

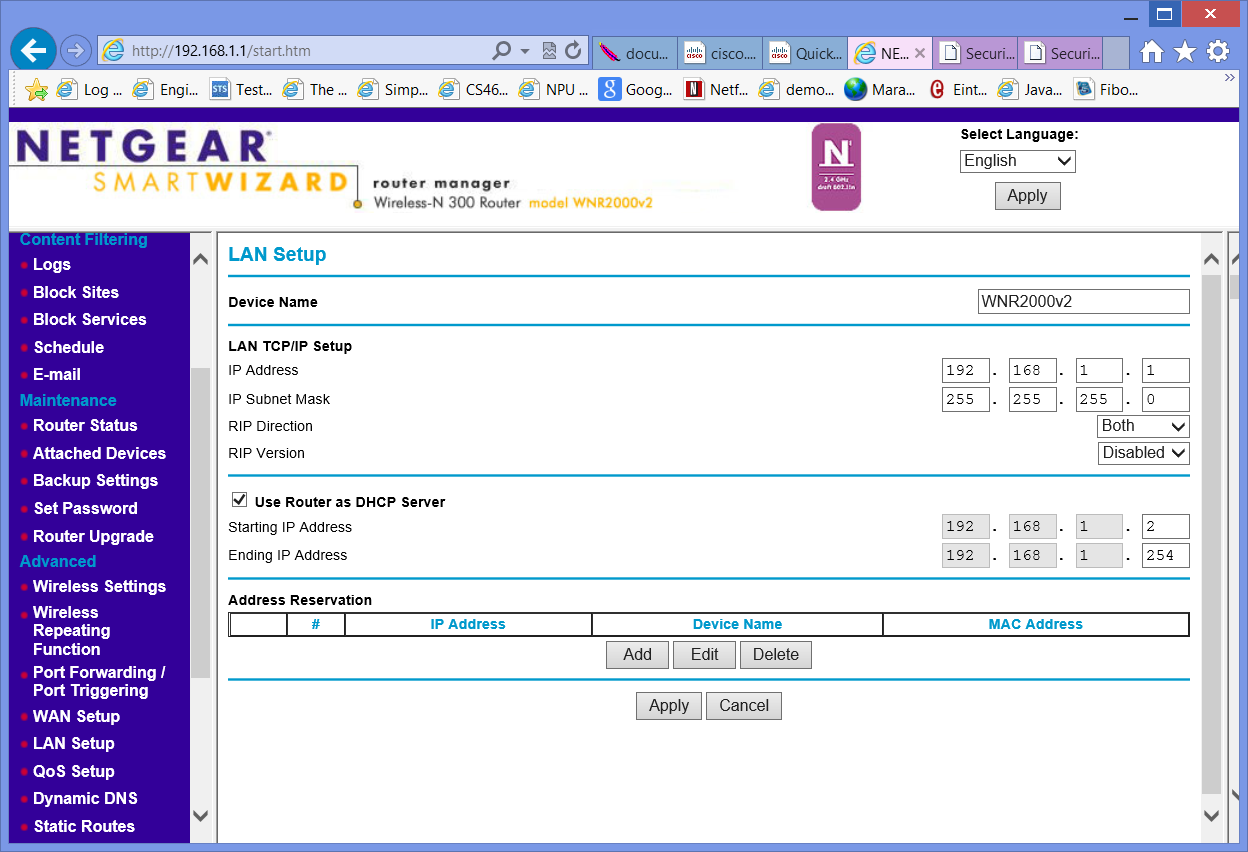
Client

Server

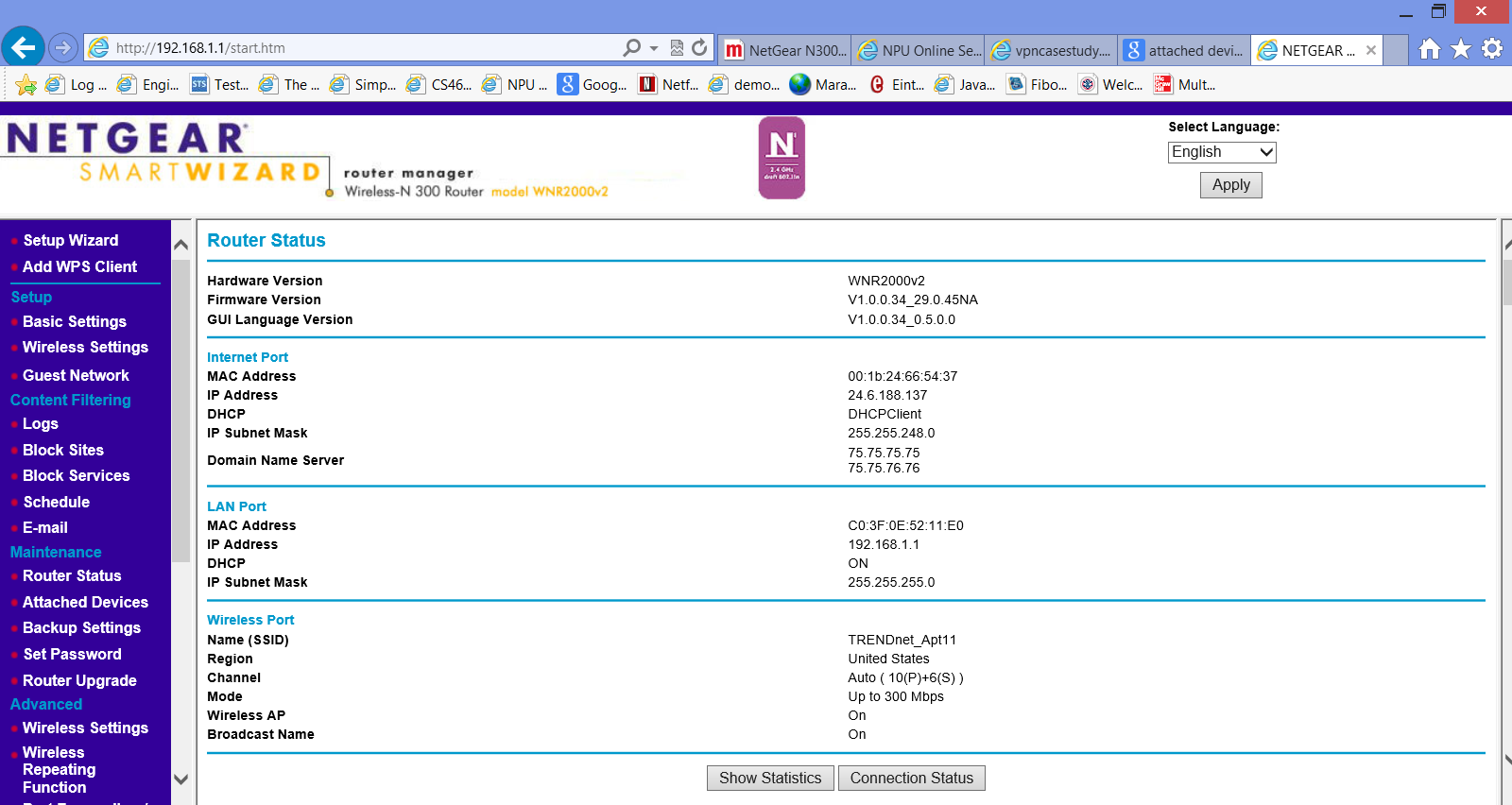
In home network, we can configure the DHCP server in NETGARE (my wireless router)

* Select LAN setup
* Select Router as DHCP server
* For the Starting IP Address, enter the first available host address in IP address range.
* Ending IP address, last available host address in IP address range.
* Then select apply

DHCP is a first come, first serve protocol. We can control how many IPs are assigned to the DHCP server. If we disable it, we have to statically assign IP address to each computer, or if we have a DHCP server .This goes for wired and wireless. Any connection on our network has an IP address.



Detailed information about router status which we selected ->

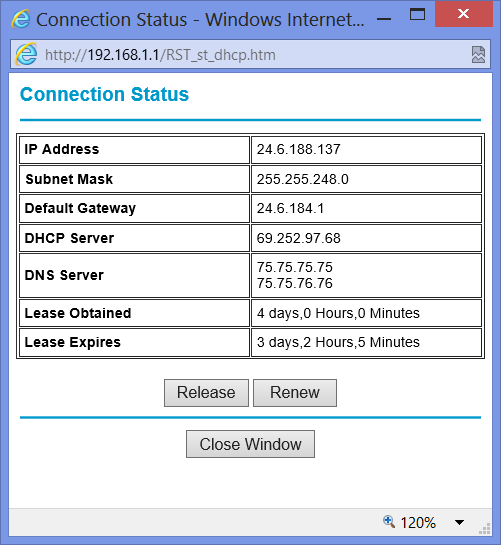


**Internet Port:** it display the current settings which we set in the Basic Settings screens.

**LAN Port**: - display mac address , IP address, subnet mask.

**Wireless Port:** These are the current settings, as set in the Wireless

• Security Options. The wireless security type (NONE, WEP, WPA-PSK, WPA2-PSK, WPA-PSK+WPA2-PSK).



**Connection Status**:- It display the information about our current connection. like IP address, Subnet Mask, Default Gateway, DHCP server, DNS server ,Lease obtained, Lease Expires.

Lease Time: - A DHCP lease is an amount of time that an IP address is offered to our device.

**DHCP lease process :-**



The DHCP lease of my device lease obtains 4 days and it will expire in 3 day 2 hours 5 min.

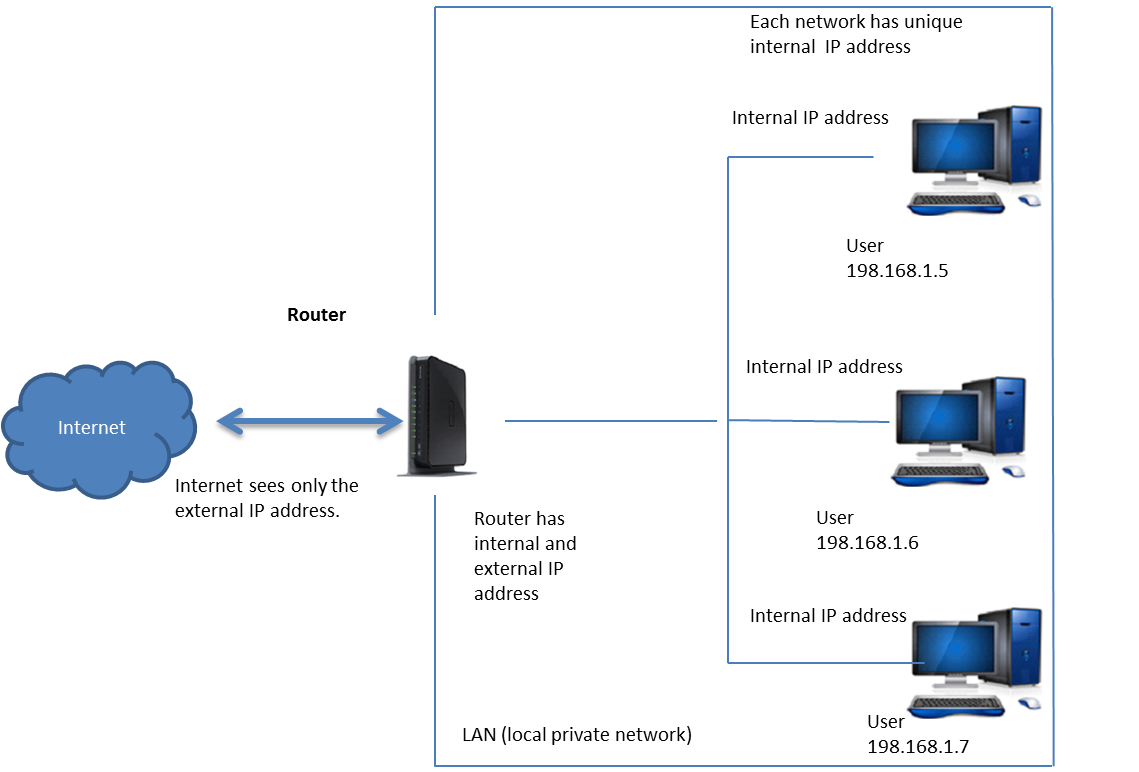
1. **NAT :-** Network address translation (NAT) is play an important role. It designed for IP address conservation.

The private network has its own IP address, **NAT operates on a router, it has both internal (private)IP address and external IP address** .it connecting two networks together, and translates addresses into legal addresses, before setting connection or transferring data packets to another network. it provide security.

In local area network each network user has its own unique internal IP address and Internet sees only the external IP address.

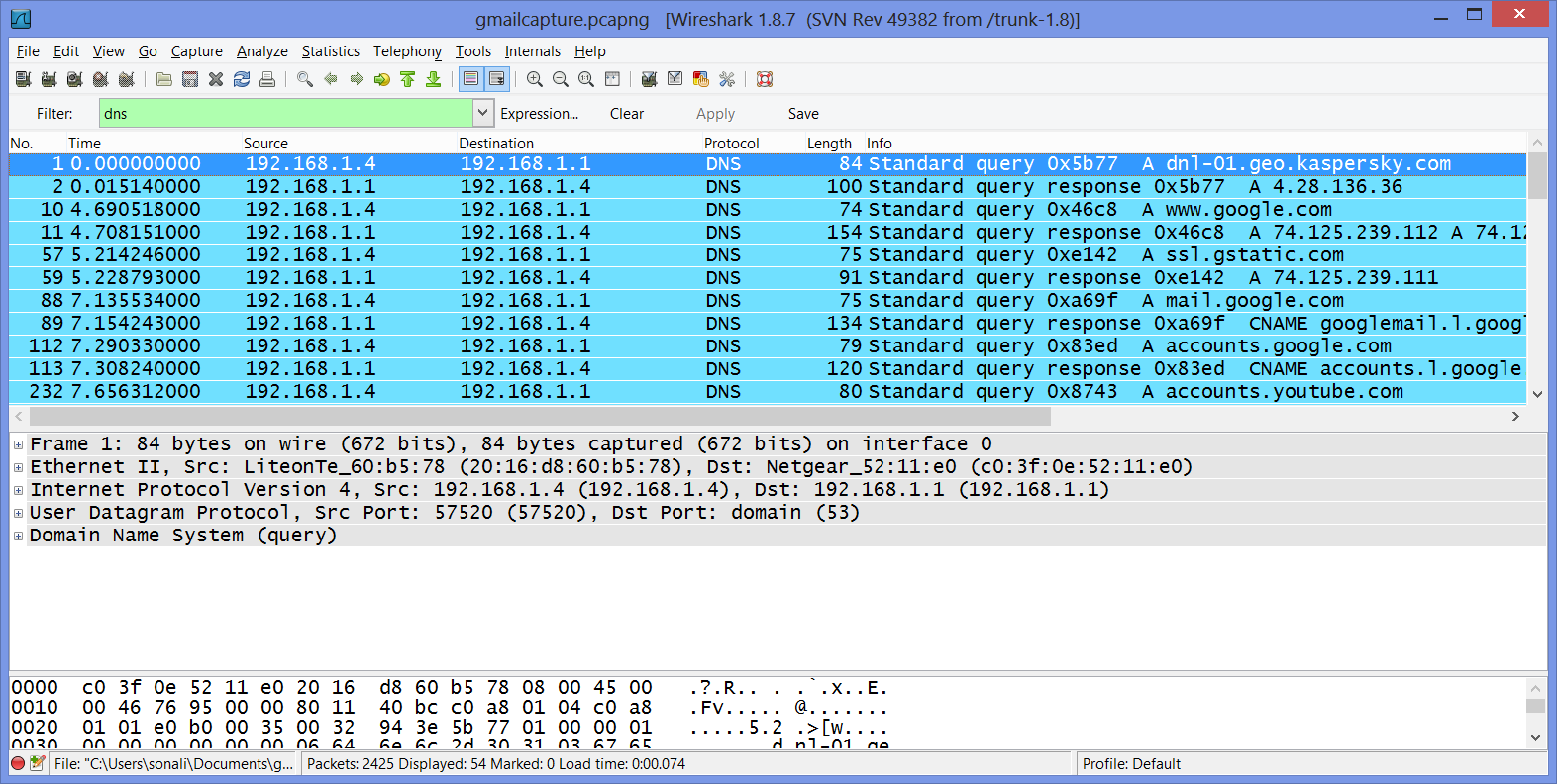
NAT can display only one address for the entire network to the outside world. Nat provides more security because it hides the entire internal network behind that address. Main important function of NAT is it provides security and address conservation. NAT is implemented in remote-access environments.

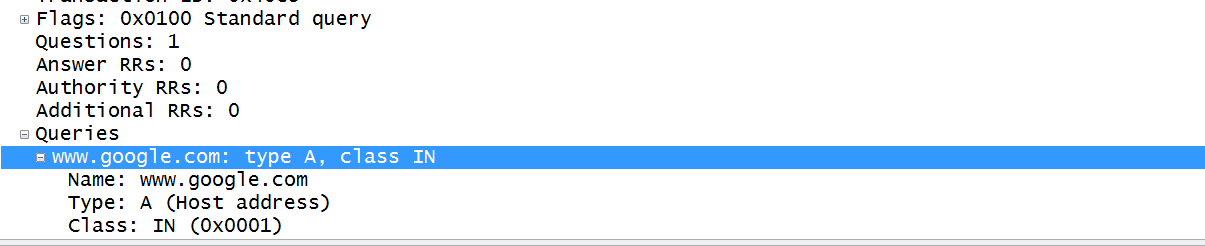
a router act as an agent between the Internet (or public network) and a local network (or private network). That means router need only one IP address for representing the multiple computers to the network.

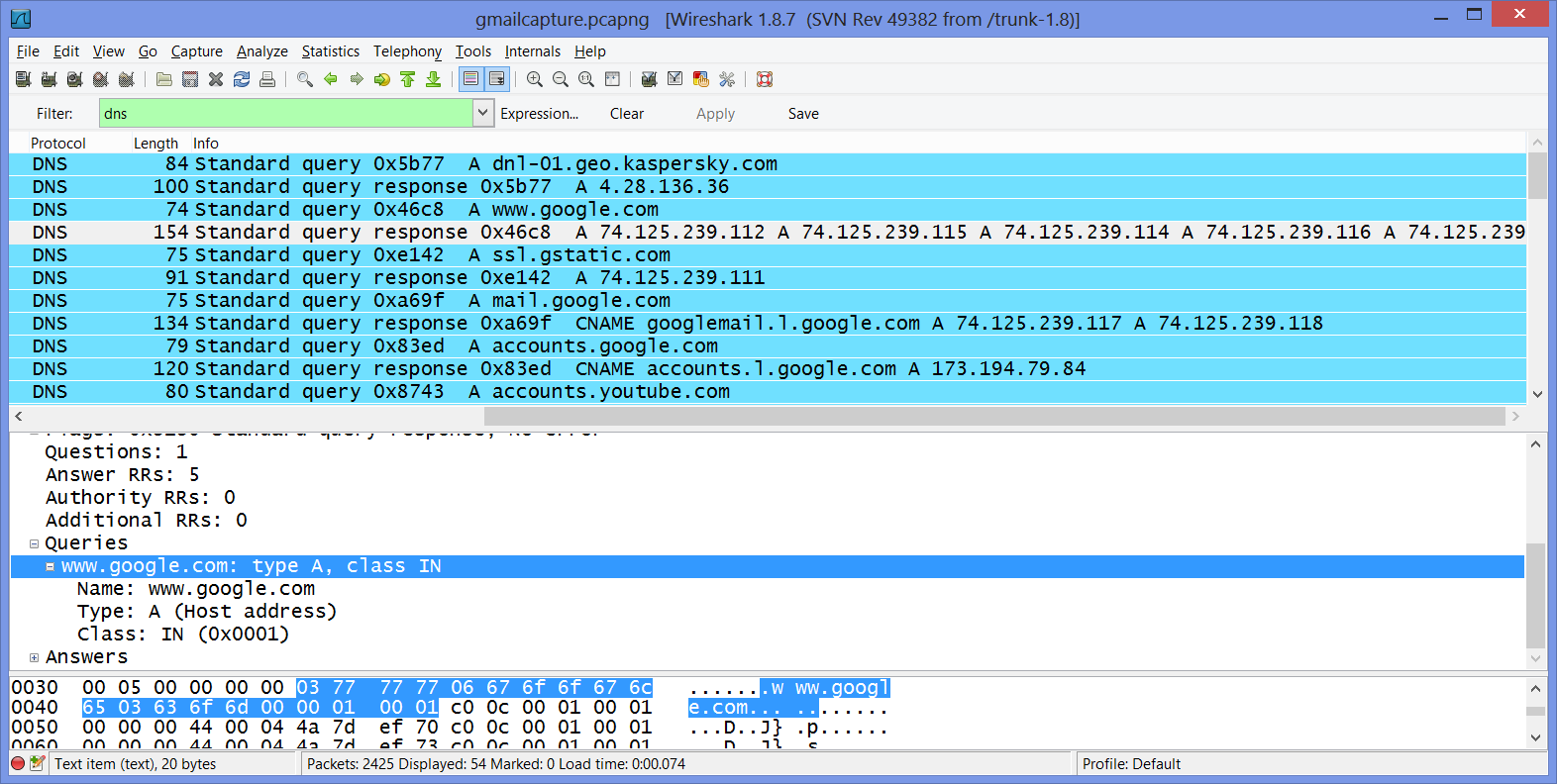


1. **DNS:-** DNS is application protocol Domain name server is used for managing domains ,names of the websites. When we type names of any website in to the web browser DNS automatically find the address on the internet .mostly we enter the name of website we don’t know the IP address of that website. e.g. http://www.google.com/, we don’t know the IP address of google.com. DNS looks for the corresponding IP address for that site and establish connections between Web browsers and Web servers. It is like "phone book of the Internet”.

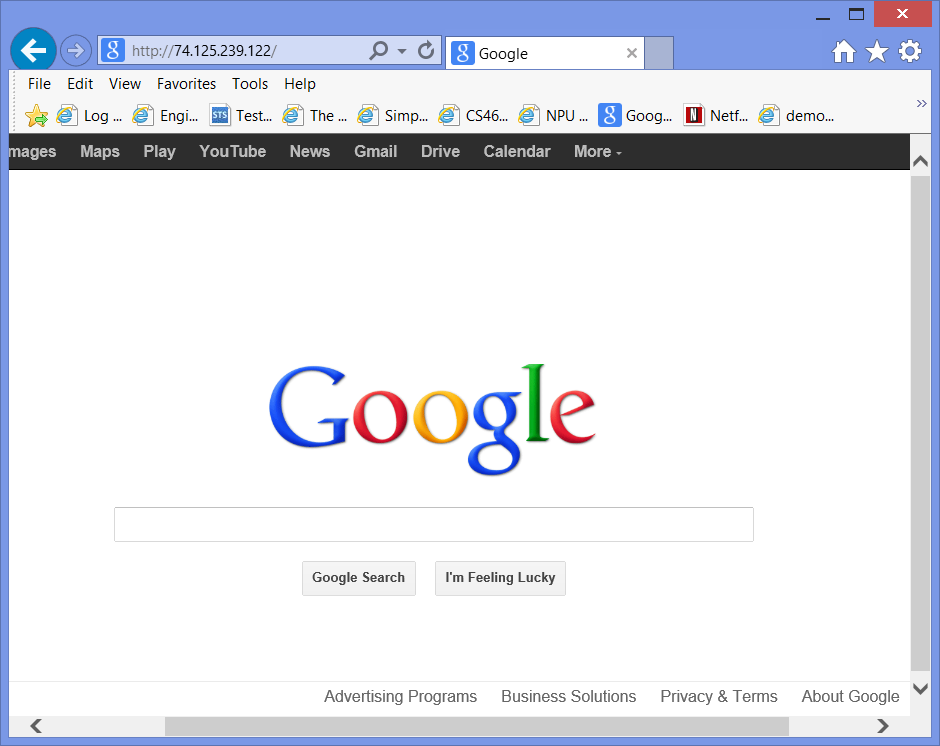
In wireshark:-



I enter google.com in web browser and DNS send query to find port number of google.com. 

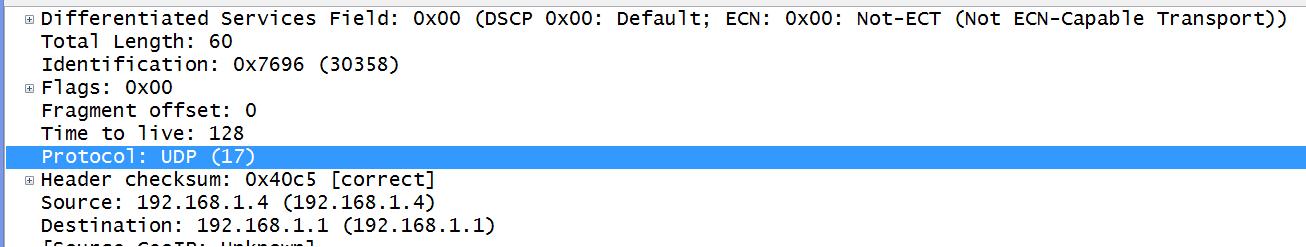


Response comes with IP address. Capture shows different IP address of google.com. 74.125.239.122, 74.125.239.114, 74.125.239.116, 74.125.239 .if we enter any of these IP address in web browser Google page will open.

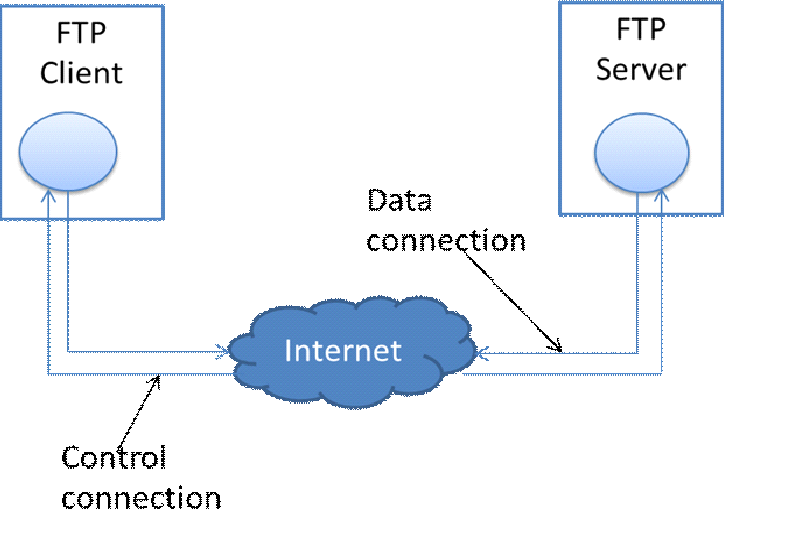


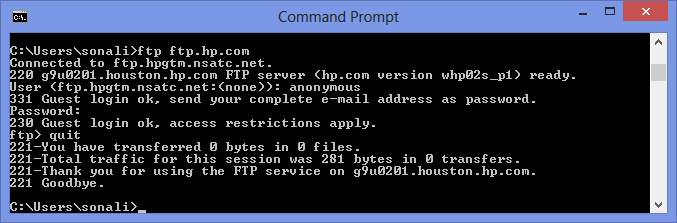
I enter 74.125.239.122 the Google.com open.

DNS use TCP/UDP as its transport protocol.



1. **FTP:-** File Transfer protocol is application layer protocol, standard network protocol, uses TCP/IP protocol. Ftp use for transferring files between computer on the internet. Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail.

****



FTP is built on client-server architecture and uses separate control and data connections between the client and the server. For secure data transmission that hides the username and password, and encrypts the content, FTP is secured with SSL/TLS ("FTPS"). SSH File Transfer Protocol ("SFTP") is sometimes also used instead, but is technologically different .FTP is used to transfer files.

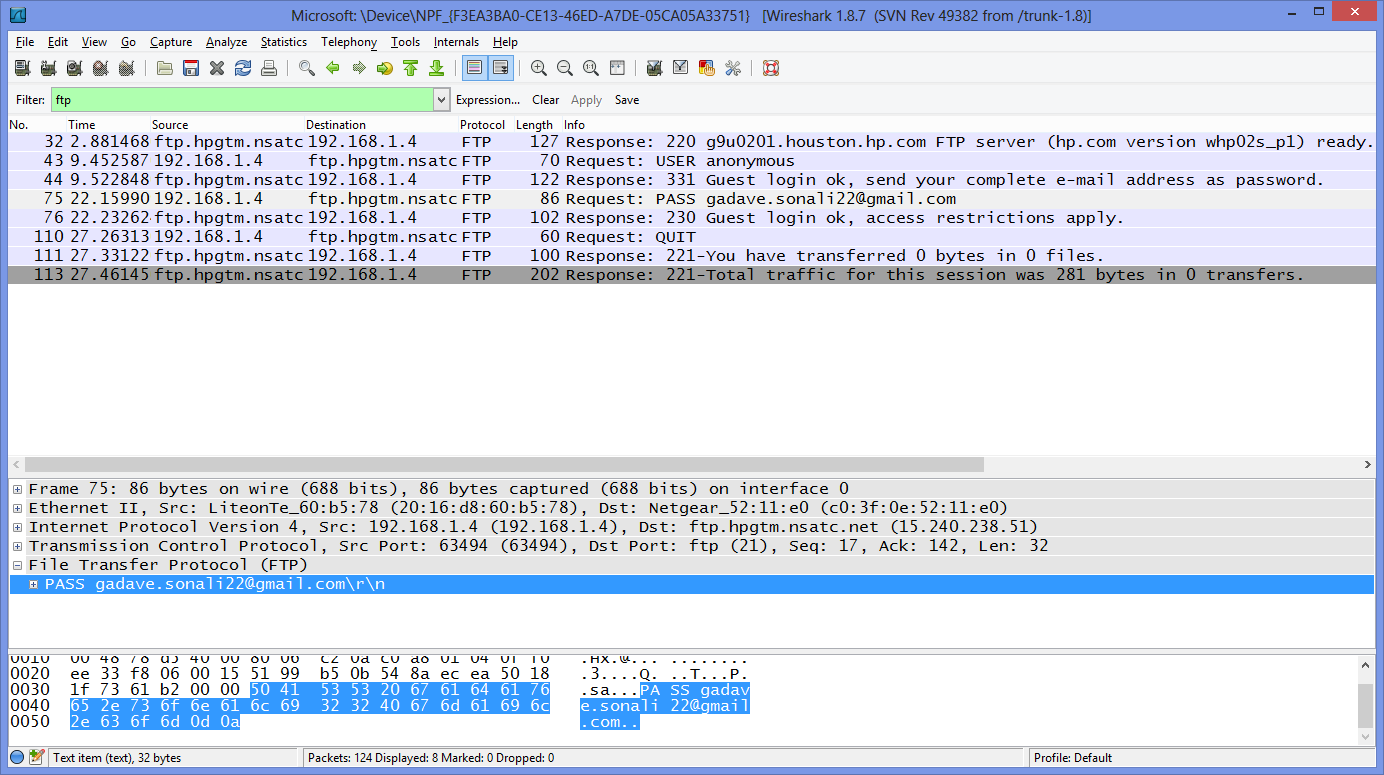
Protocol dependencies

Ftp uses 2 parallel TCP connections for transferring data

1. Control connection
2. Data connection

**Example traffic**

**Capture Filter**



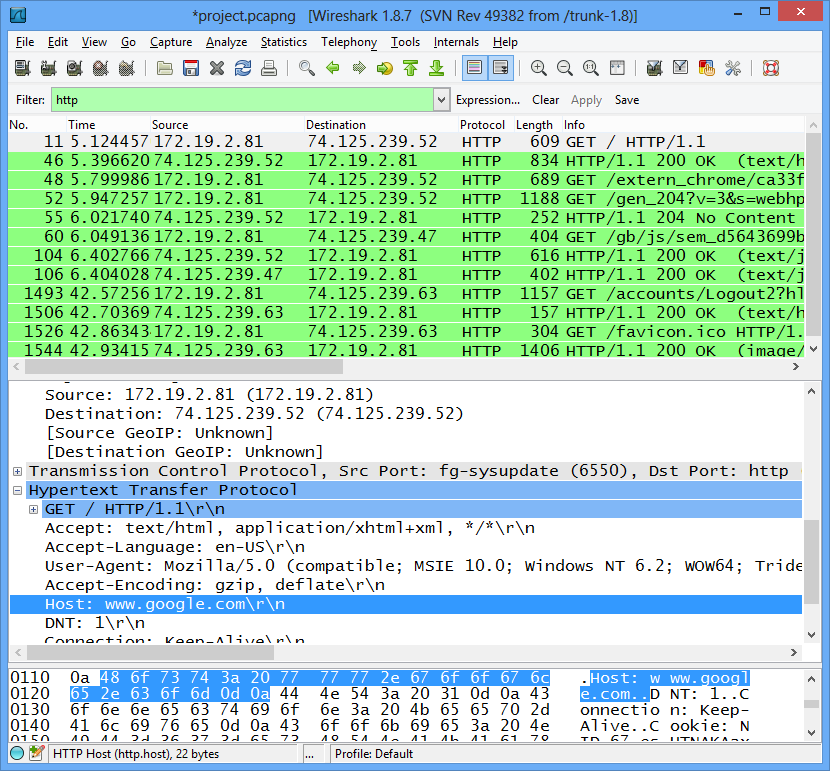
1. **HTTP:-** Hypertext Transfer Protocol. HTTP defines how messages transmitted. For example, when we enter a URL in your browser, sends an HTTP command to the Web server directing it to get and the requested Web page.

HTTP is **stateless**: each command is executed independently, does not keep record.

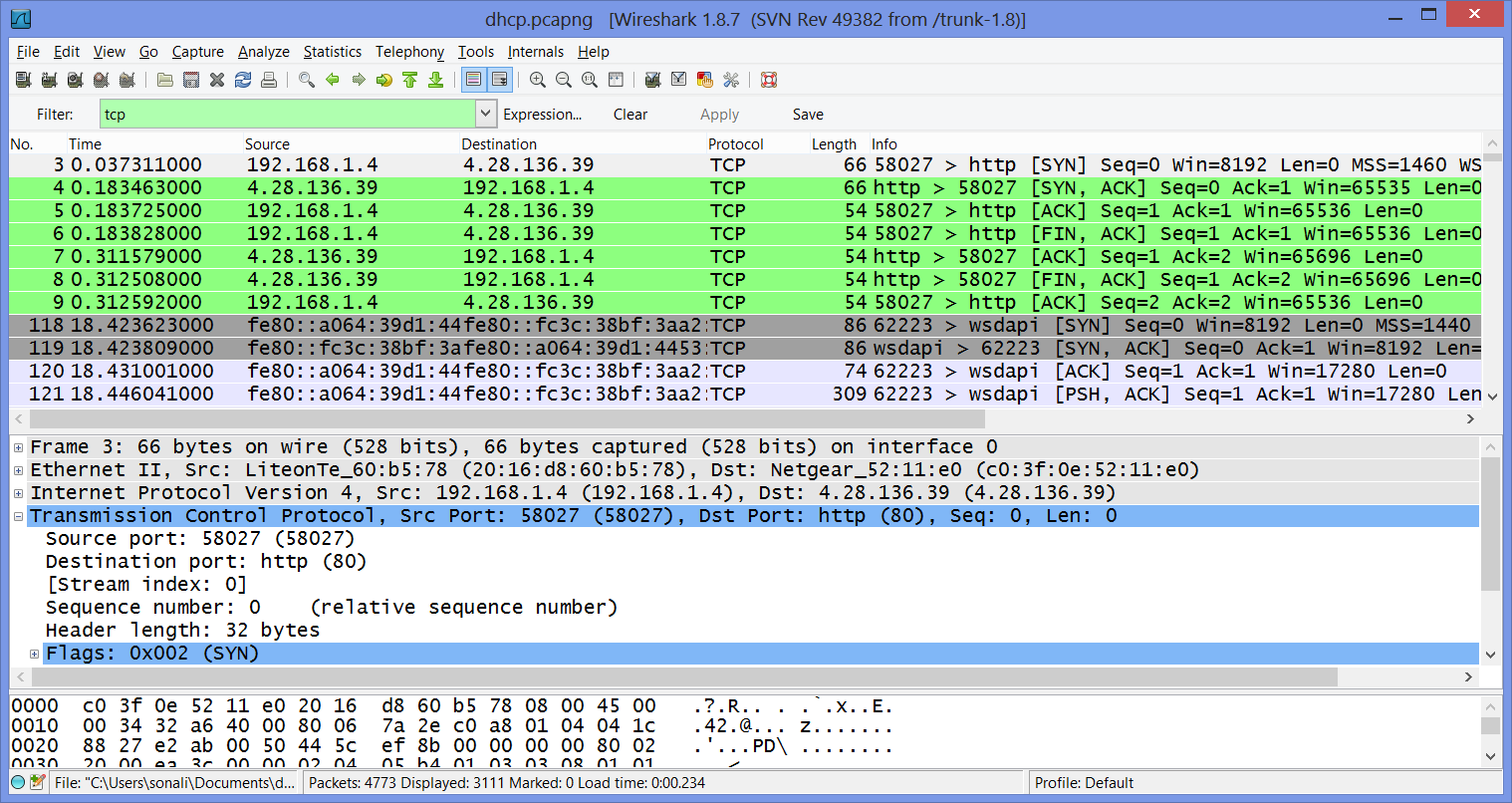
HTTP is **connectionless:** After a request is made, the client disconnects from the server and waits for the response. The server must re-establish the connection after it processes the request.

Request message:- GET /path/to/file/index.html HTTP/1.0

Response message:- HTTP/1.0 200 OK or HTTP/1.0 404 Not Found



1. **TCP:-** Transfer control protocol is transport layer protocol. TCP provides a connection oriented, reliable, byte stream service. TCP includes a flow-control, congestion-control, Multiplexing, Full Duplex.



TCP is connection oriented protocol meaning that it has to establish a connection between Host and Server before it starts sending anything(data). So the three way handshake is needed to establish a reliable connection. The handshake allows the server and client to agree on properties that provides security as well as reliability.

2 Syn- Ack

1 Syn

3 Ack

Established

Host B

Host A

1. Client sends SYN to server

2. Server sends SYN-ACK to client.

3. Client send ACK to server

**Firewall**:- A firewall is one type of system ,it is designed to prevent unauthorized access and prevent our network from attack. We can implement a firewall in hardware or software form, or a combination of both. Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet. All the data, information and messages which we enter in our private network is pass through the firewall to outside network. The firewalls examine each message and blocks and maintain specified security. Firewall is designed to protect network traffic and connections. It is an mediator between private and public network.

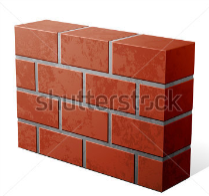
🡪In firewall setting we can set some setting for secure our network

* Excessive Session Detection
* TCP/UDP Port Scan
* Invalid Source/Destination IP address
* Packet Flood (SYN/UDP/ICMP/Other)
* Invalid TCP Flag Attacks (NULL/XMAS/Other)
* Invalid ICMP Detection.

**Types of firewalls:**

Packet filtering: In packet filtering the system examines each every packet which is send to outside the network or coming in inside network .that information is accepted or rejected it is based on user-defined rules(which we define ). It is susceptible to IP spoofing.

* Circuit-level gateway implementation: This process applies security provided when a TCP or UDP connection is established. Once the connection establish, packets can flow between the hosts without further checking.
* proxy server: A proxy server is a type of gateway that hides the true network address of the computer from the network. A proxy server connects to the Internet, makes the requests for pages, connections to servers And receives the data first and send it to the computer. The firewall capabilities lie in the fact that a proxy can be configured to allow only certain types of traffic to pass (e.g., HTTP files, or web pages). Proxy server slowing performance of the network.



LAN (local private network)

Internet

**Router**

Internet

Router

Firewall

**Comparison of password encryption protocols such as WEP, WPA/WPA2:** There are many wireless protocol are develop for security purpose, like WEP,WPA AND WPA2.

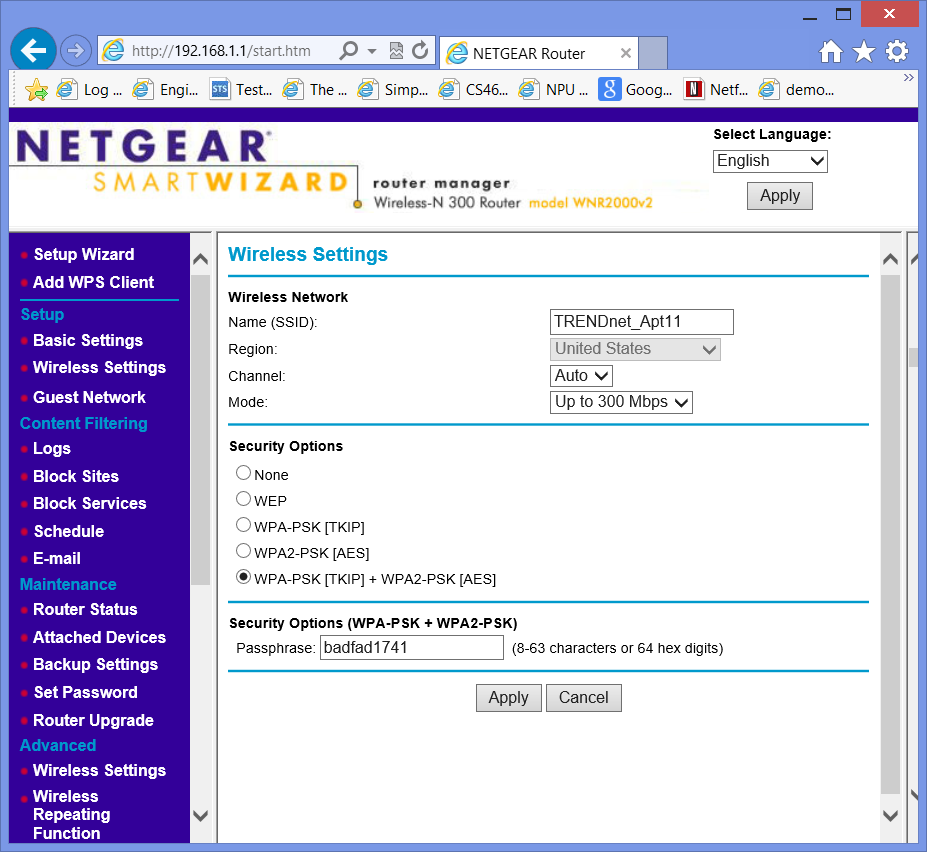
* **Wired Equivalent Privacy (WEP):** Wired Equivalent Privacy is security protocol for wireless local area network (WLANs),WLANS are over radio waves. WEP was designed to provide the same level of security as wired networks .WEP is providing security by encrypting data over **radio waves.** It is protected as it is transmitted from one end point to another. WEP is not very secure, it is difficult to configure, and is easily broken. WEP is used at the two lowest layers of the OSI model which are data link and physical layer. It therefore does not offer end-to-end security.

->In WEP we can manually or automatically program the four data encryption keys. These values are identical on all PCs and Access Points in your network. We can provide one paraphrase for automatic encryption.

* **Wi-Fi Protected Access (WPA):** WPA is a security technology for Wi-Fi wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). WEP has some weakness because of that WPA was developed. Most current WPA implementations use a **preshared key** (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates. WPA is better than WEP.

It is security encryption with presheared key.

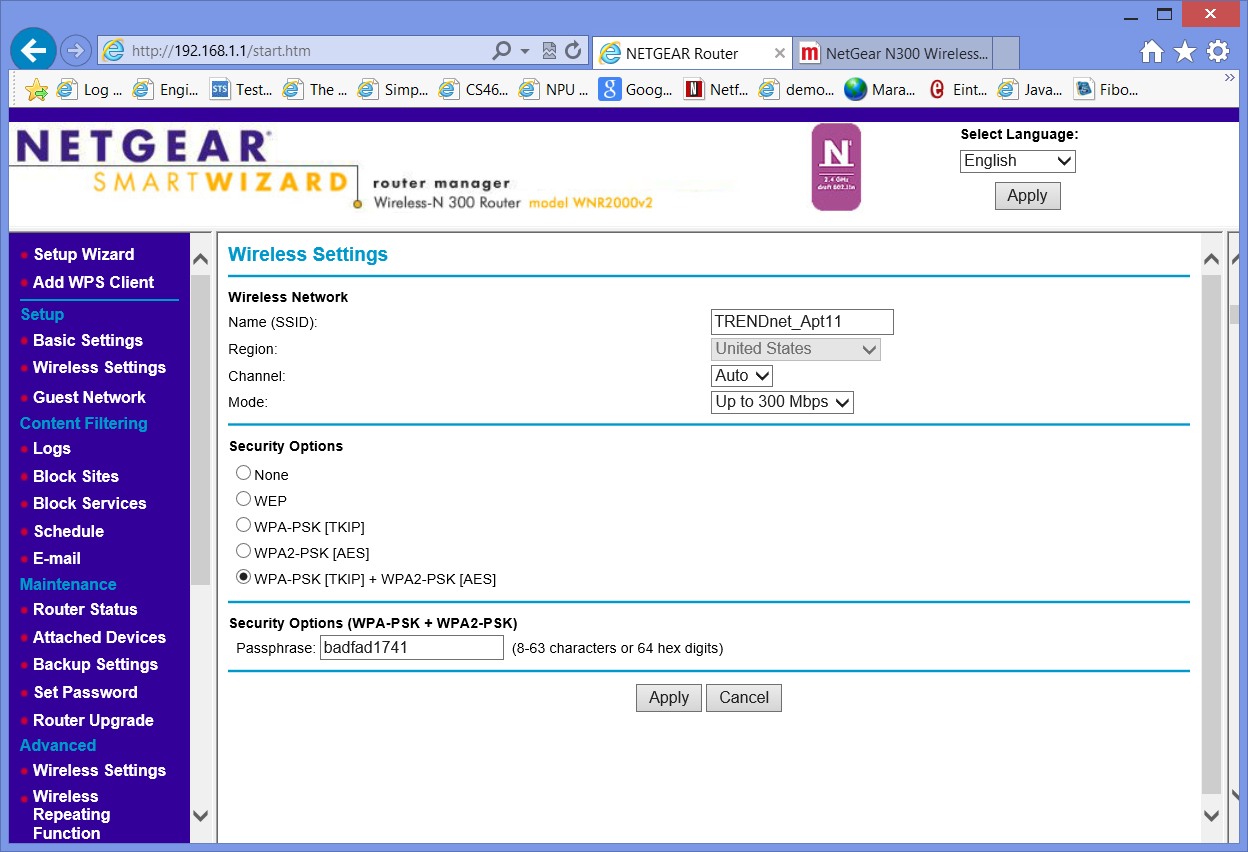
* **Wi-Fi Protected Access version 2 (WPA2):** Wireless Protected Access was designed as a replacement for the older and less secure Wireless Encryption Protocol (WEP). Based on the 802.11i wireless security standard. The most significant enhancement to WPA2 over WPA is the use of the **Advanced Encryption Standard (AES) for encryption**. WPA2 also improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires.

I am using WPA-PSK [TKIP] + WPA2-PSK [AES] for secure my home wireless network. 

**Physical Layer Security:** Physical layer passing actual data/information by physical medium and between two physical locations. The physical layer is a wire ,hub . **The physical layer can be secured by protecting access to network cables and ports.**

**To conduct your online research to see what you can do to secure your wireless network at physical layer beyond physical access restriction;**

I am using NetGear N300 Wireless Router.



Wireless settings:- I will change my wireless settings. I

**Wireless Network**:-

Name:-This (TRENDnet\_Apt11) is the name of my account ,same name must be assigned to all wireless devices in my network.

Region:-displays the region

Channel:-This field determines which operating frequency will be used.

Mode:- I select Up to 300 Mbps mode Up to 300 Mbps. This mode has a maximum Wireless speed of up to 300 Mbps.

**Security Options:-**

This is important setting for security.it has, None, WEP(Wired Equivalent Privacy),WPA-PSK [TKIP] ,WPA2-PSK [AES] ,WPA-PSK [TKIP] + WPA2-PSK [AES] .

*Security Encryption (WPA-PSK + WPA2-PSK)* :-

Wi-Fi Protected Access with Pre-Shared Key, use WPA-PSK standard encryption with TKIP encryption type, Wi-Fi Protected Access version 2 with Pre-Shared Key, use WPA2-PSK standard encryption with the AES encryption type. This option Allow the clients using either WPA-PSK [TKIP] or WPA2-PSK [AES].

This selection allows clients to use either WPA (with TKIP, broadcast packets also use TKIP.) or WPA2 (with AES). If selected, encryption must be TKIP + AES. The WPA passphrase (Network key/password) must also be entered. My password is badfad1741,To reach maximum wireless performance, the 11N clients must connect to this router using WPA2-PSK(with AES) .

Create a WLAN security policy.

**Secure the WLAN:**

–> Modify the default SSID.

–> Use strong encryption.

–>use authentication between the client and the network.

–> Use VPNs or WEP combined with MAC address control lists to secure business-specific devices.

–> Use identity networking in combination with VLANs to restrict access to network resources.

–> Ensure management ports are secured.

–> Use lightweight access points as which are not store security information locally.

–> Physically hide or secure access points to prevent tampering.

Secure the wired network :

–>enable wireless IPSs to prevent rogue access points and other wireless threats.

protect external threats:

**Conclusions:-**

**Commercial Wireless router can be configured to design home wireless network (WLAN) to cater the user requirements such as number of devices that can connect to network, private IP address range, add security to wireless medium using authentication and encryption.**

**Home wireless network can be made more secure by adding firewall (enabling one provided by the device OS).**

**Source:**

**Books: -** computer networking a top-down approach

<http://support.netgear.com/>. Wikipedia

http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html

http://cisco.com