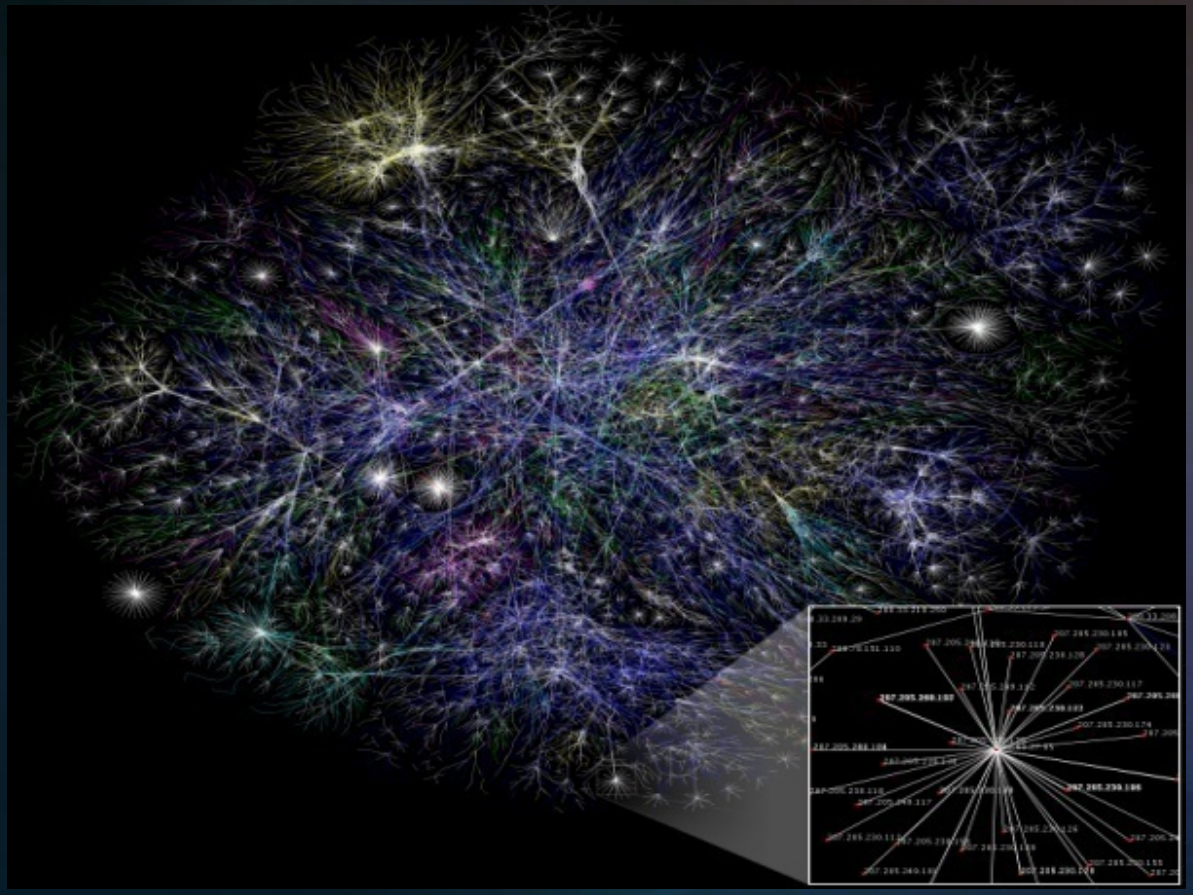
TCP/IP Networking in a Nutshell

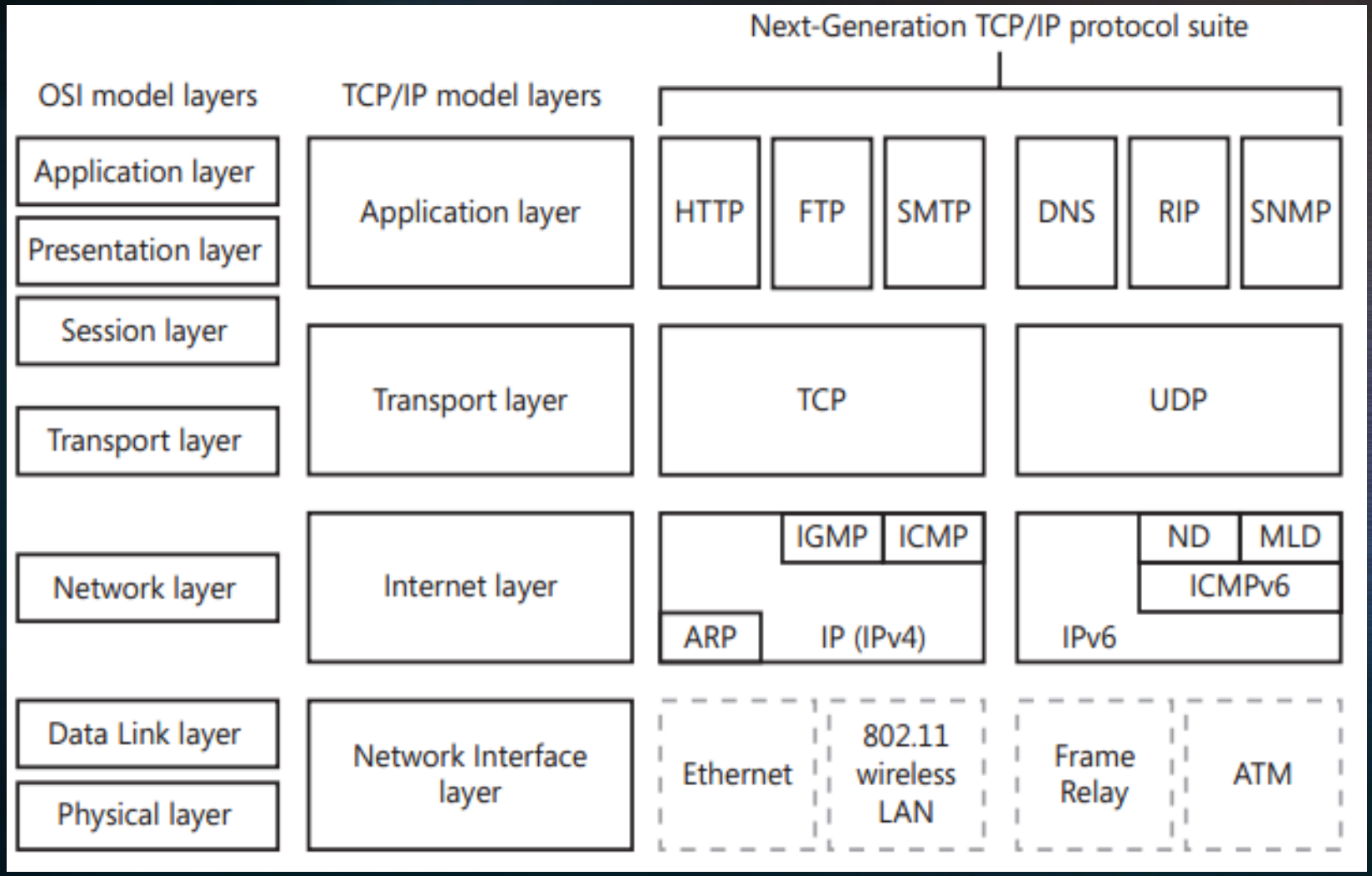


Tanmay Bhagwat

(Slides borrowed from Kevin Cleary and modified as required)

UB Cyber and Network Defense

TCP/IP Stack


Next-Generation TCP/IP protocol suite
OSI model layers
TCP/IP model layers
Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data Link layer
Physical layer
Application layer
Transport layer
Internet layer
Network Interface layer
HTTP
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IGMP
ICMP
ARP
IP (IPv4)
ND
MLD
ICMPv6
IPv6
Ethernet
802.11 wireless LAN
Frame Relay
ATM

What's a Server?

- Most communications on the internet are “Client / Server” based.
  - A client is typically a desktop computer or smart device.
  - Servers are the destinations for many client initiated connections
  - Servers are computers with a dedicated task.
- Clients and servers typically live on separate networks.
- Other communication models can include:
  - Peer-to-peer
  - Grid
  - Distributed

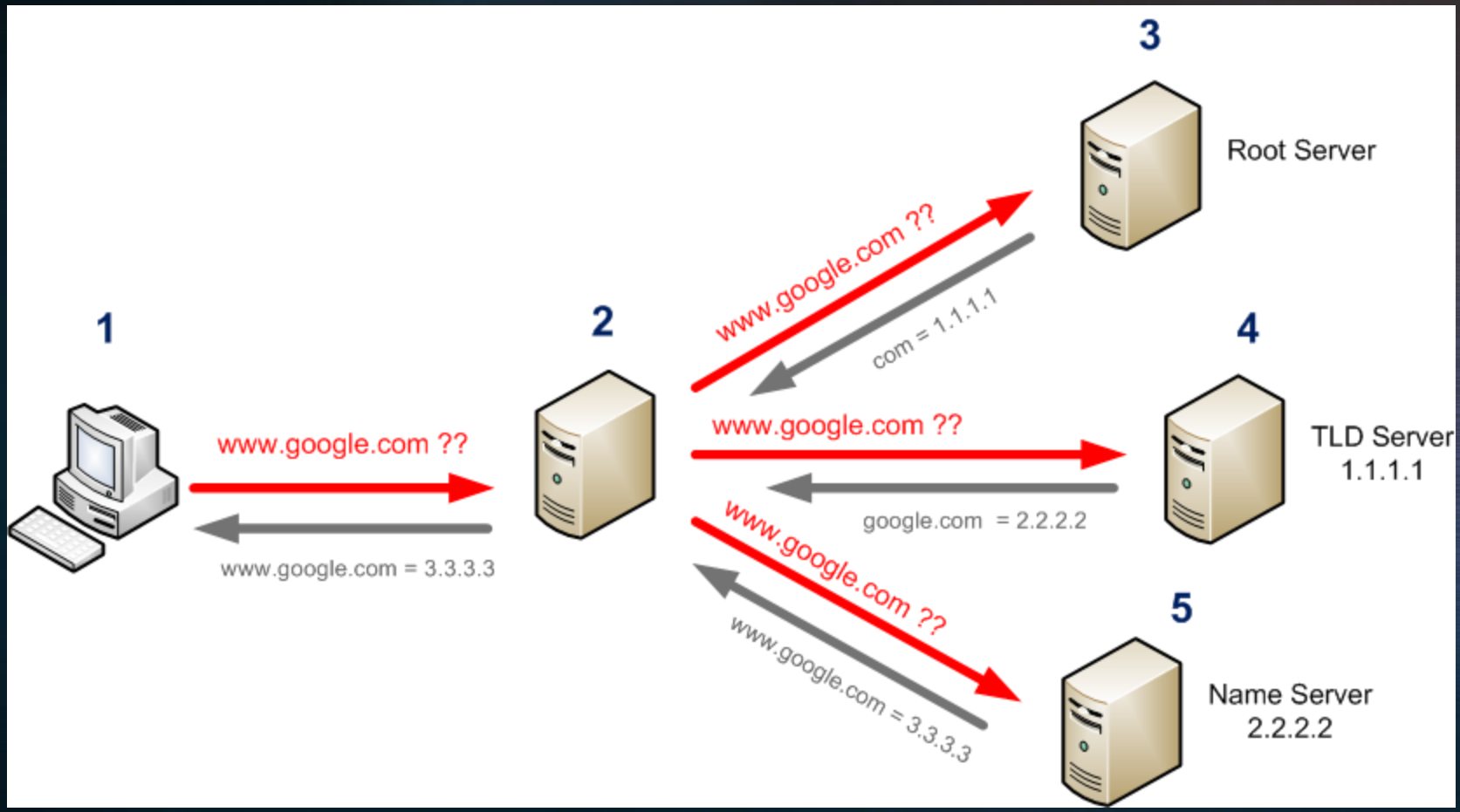
Domain Name System (DNS)

- DNS to translate domain names such as “google.com” to an IP addresses such as “74.125.226.206”.
  - It’s easier to memorize and type domain names than IP addresses.
- Getting a domain name involves registering the name you want with an organization called the “Internet Corporation for Assigned Names and Numbers” (ICANN) through a domain name registrar.

Domain Name System (DNS)

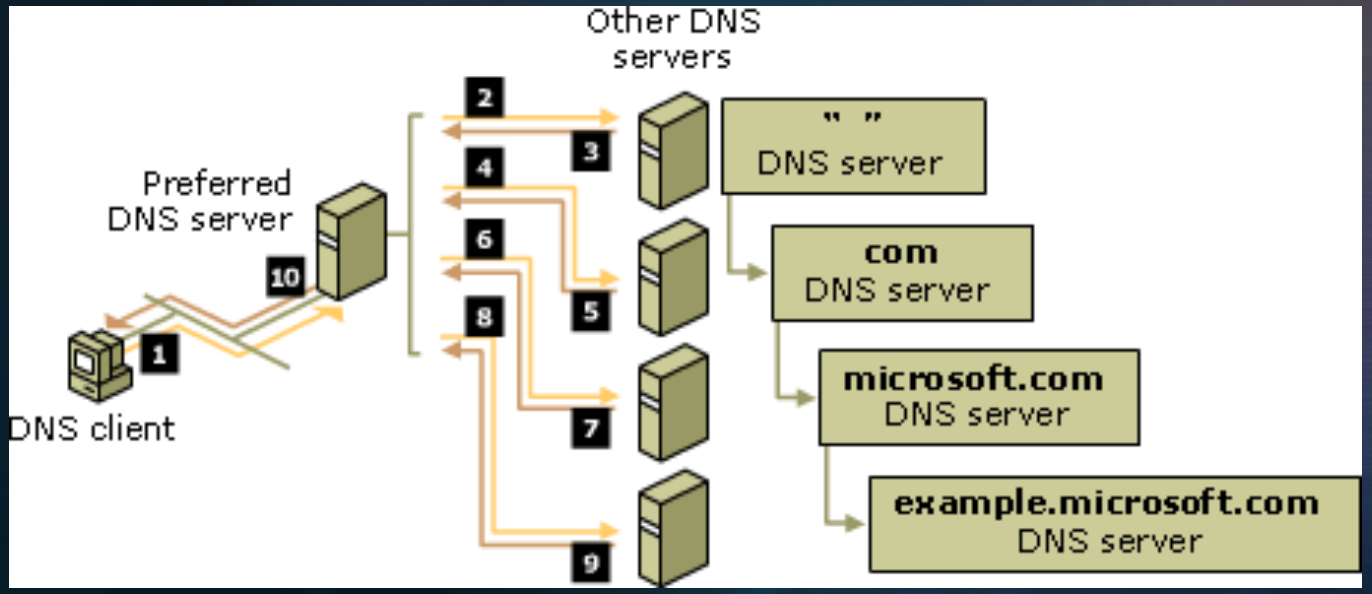
- Consider www.google.com
  - .com is called the “top level domain”.
  - Google is the second level domain.
  - www is the host name.
- Domain Name lookup is an iterative process.
  - Doman Name servers are arranged in a hierarchal fashion, ex: “www.bbc.co.uk”.
  - Distributed sub-domain servers all manage small portions of IP addresses.
  - There are 13 root servers globally that resolve top level domain names.

Domain Name System (DNS)



Domain Name System (DNS)

- A local DNS server will temporarily cache entries for greater speed upon subsequent lookups.
- Each name server only knows of its own small portion of its domain.



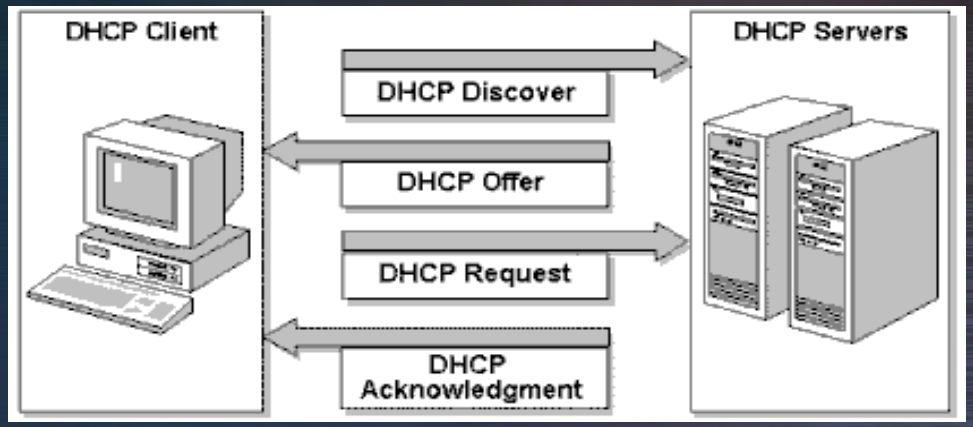
- DNS is an connectionless protocol
- DNS has been weaponized in recent years with what are called amplification attacks.

Dynamic Host Control Protocol (DHCP)

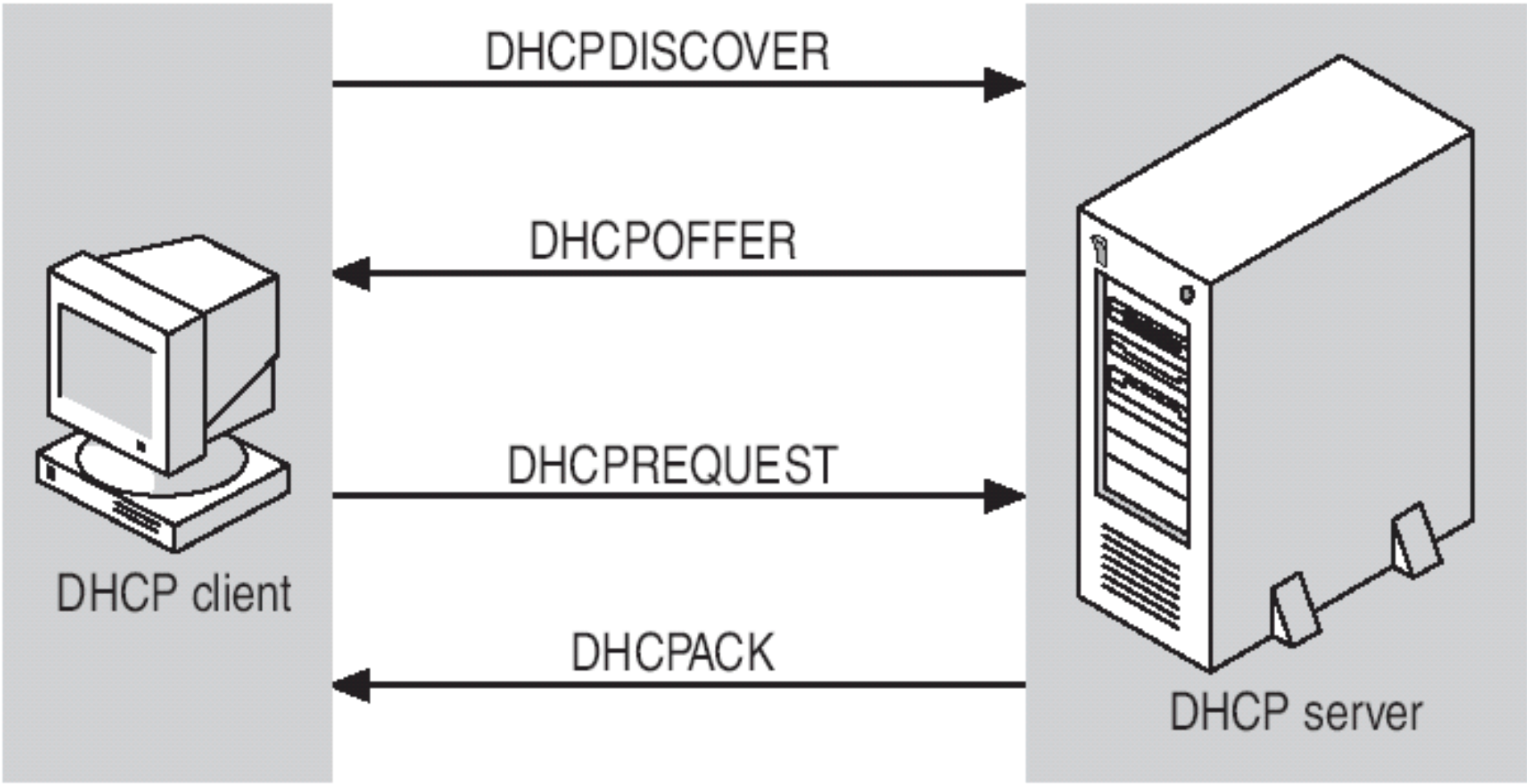
- Server Addresses are said to be "**static**". These addresses do not change over time and are usually manually set by someone.
- Workstations or home PCs tend to have "**dynamic**" addresses. These addressed are managed or "leased" by a central authority known as DHCP.
- DHCP will set all the network parameters your PC needs to communicate on a network.
- DHCP hides details of the IP protocol from users.

Setting IP Addresses

- Dynamic Host Control Protocol (DHCP) – takes care of assigning your networked devices their needed networking parameters. Such as:
  - IP Address
  - Gateway Address
  - Subnet Mask
  - DNS Servers
  - Other valuable information
  - makes it possible to hide network level details from normal everyday users.



- When you connect to a home network or “UB_Secure” your computer ask that network’s DHCP server for the needed network information.
- This functionality is embedded on most home routers.


DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACK
DHCP client
DHCP server

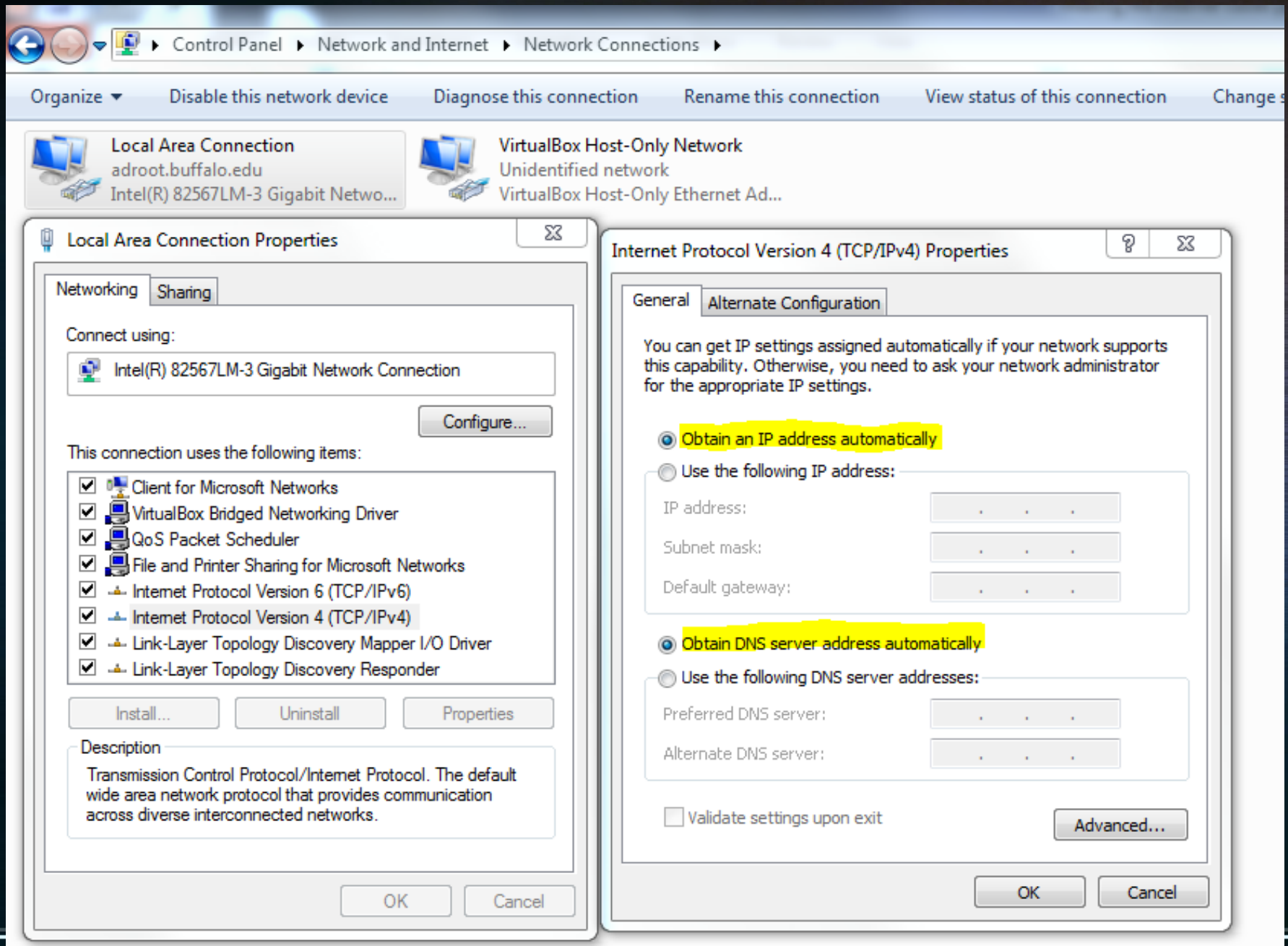
Dynamic Host Control Protocol (DHCP)

- A new client broadcasts a DHCP discover message to a local subnet.
- A DHCP server responds with a DHCP offer message that contains an IP address for lease to the client.
- When the offer message is received, the client selects the offered address by replying to the server with a DHCP request.
- The offering server sends a DHCP acknowledgement message (DHCPACK) , approving the lease.
  - Other DHCP option information is included in the acknowledgement.
  - Once the client receives acknowledgment, it configures its TCP/IP properties using the information in the reply

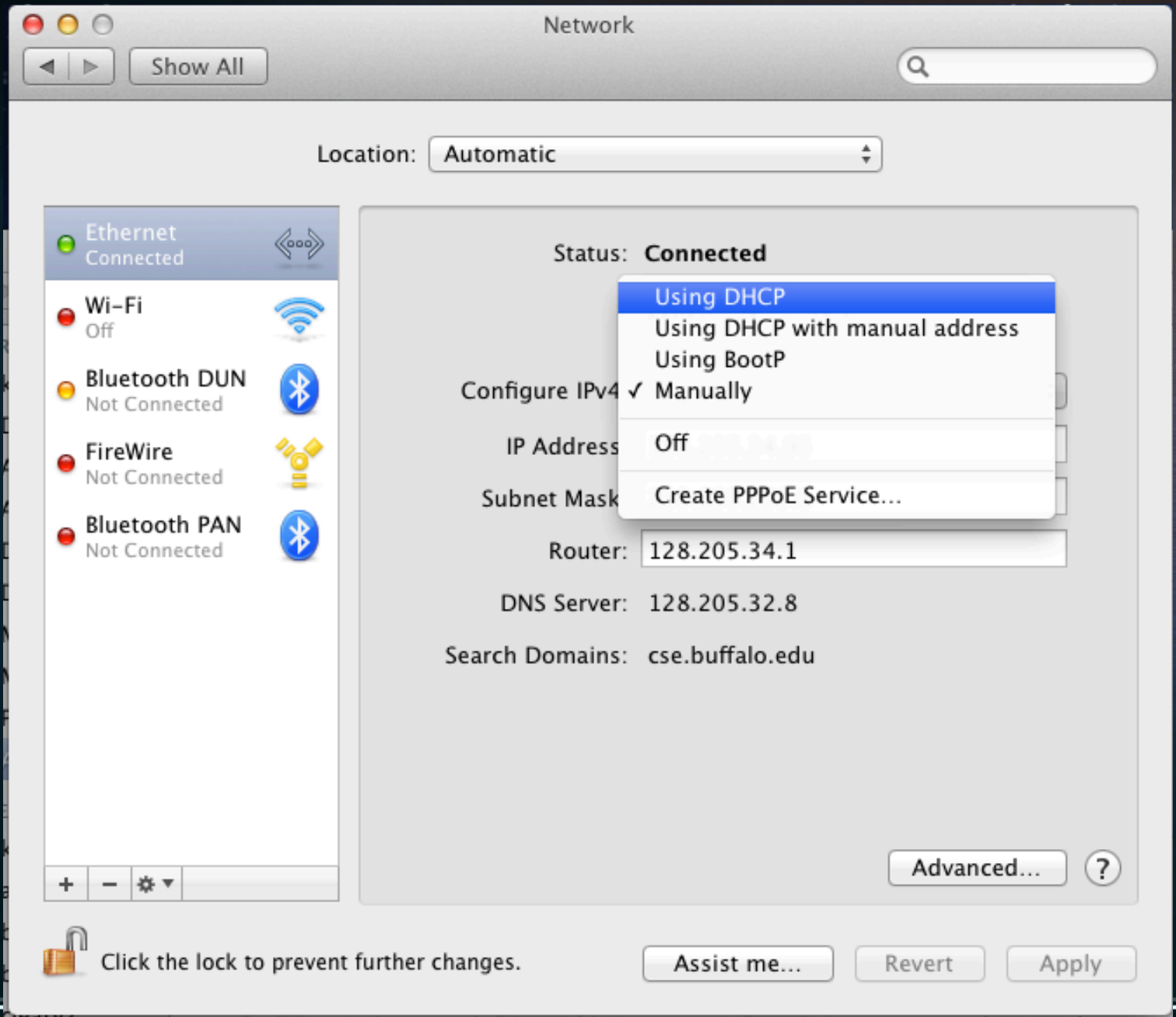
Dynamic Host Control Protocol (DHCP)

- What happens when :
  - There is no server to answer your request?
    - Your client will guess its own address and assign an "Automatically Assigned IP Address" (AAIPA).
    - You will know this is happening if your machines IP address starts with a "169….".
  - The wrong DHCP server answers?
    - This could be a type of attack known as a "Rogue DHCP".
    - A bad guy could route traffic through a malicious host.

Dynamic Host Control Protocol (DHCP)



Dynamic Host Control Protocol (DHCP)

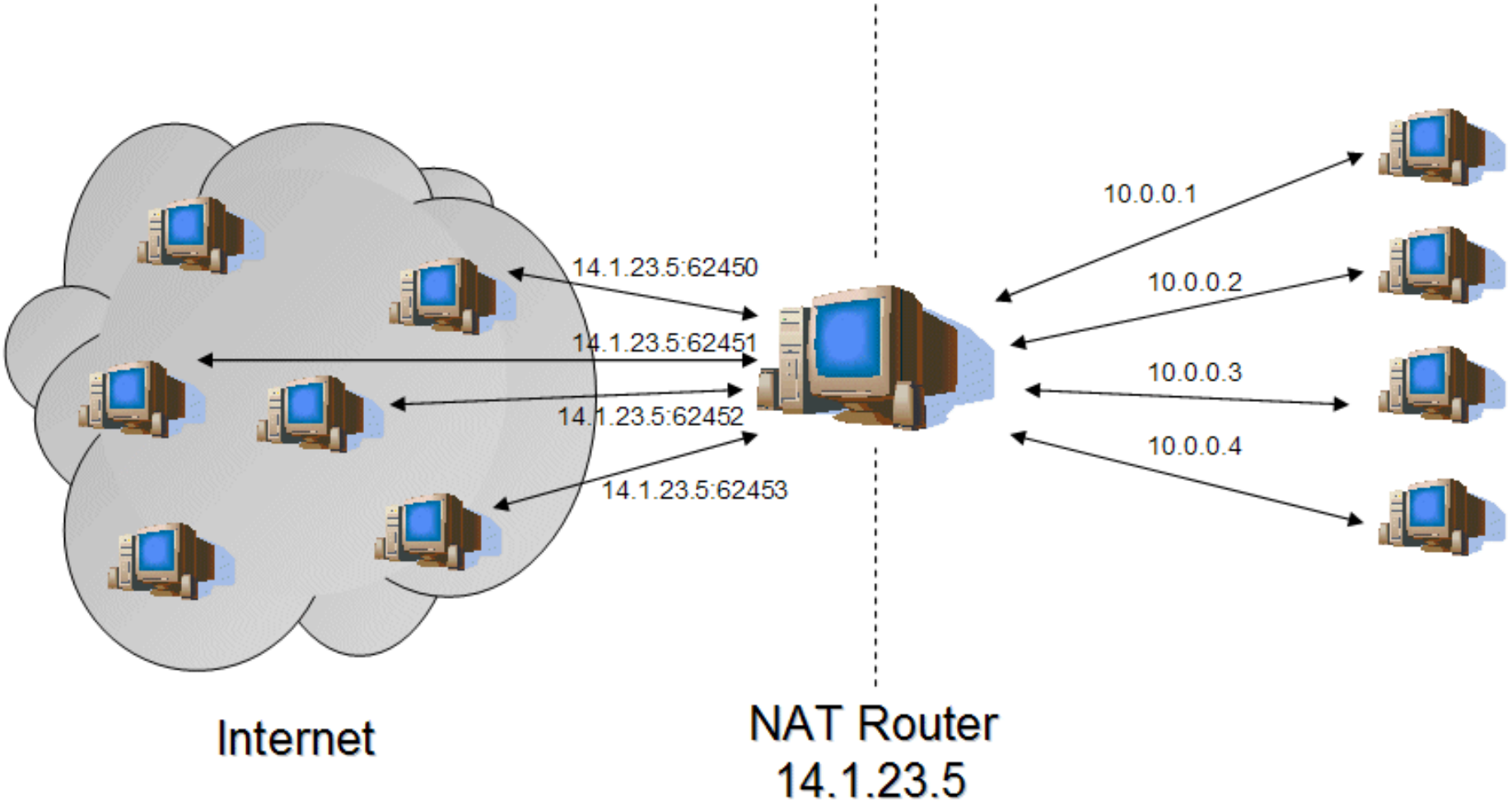


Home Networks

- What are home routers?
  - A Switch?
  - A Gateway?
  - A Firewall?
  - A Server?
  - A DSL/Cable Modem?

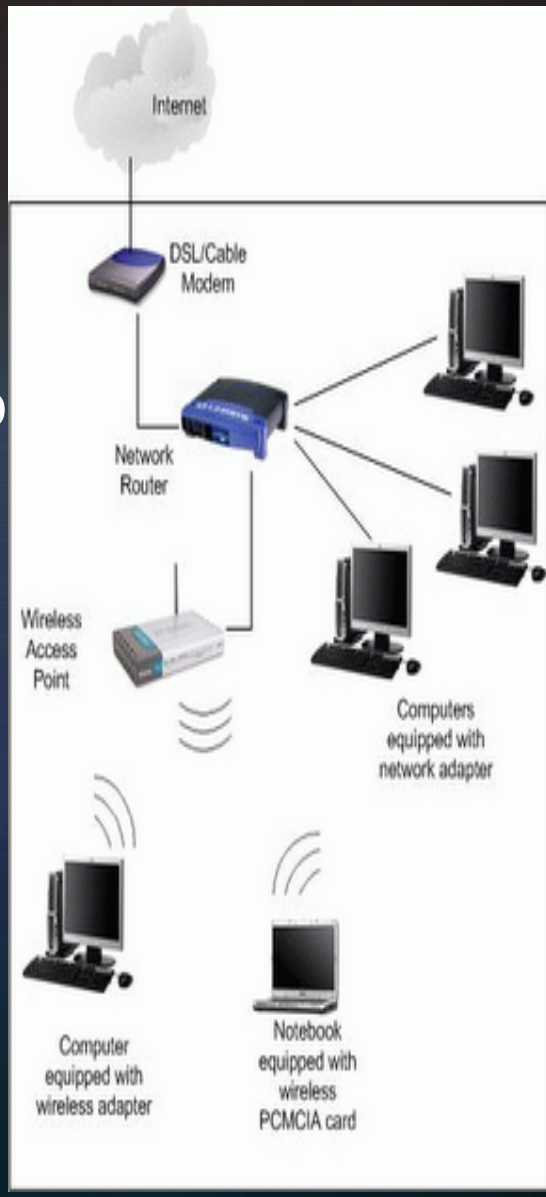
Home Routers

- Most Home Routers will function as a Network Address translation Firewall, or NAT.



Home Networks

- Home Routers are connected to the internet through an Internet Service Provider (ISP).
  - An ISP provides you a way to connect to their own WAN, providing access to the Internet.
  - An ISP will provide you a modem or home router to connect through their preferred transmission medium.
    - Sometimes these devices must be connected to a local switch to form your own LAN

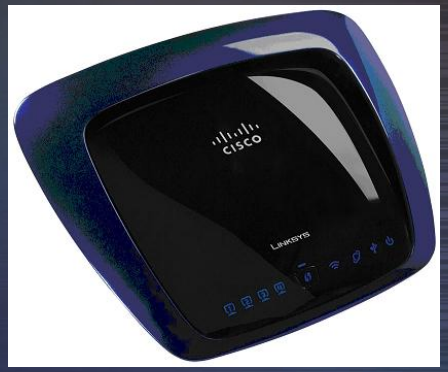


Home Routers

- Most Home Routers will function as a Network Address Translation Firewall (NAT).
  - NAT allows a single device, such as a home router, to act as an agent between the Internet (public network) and a local (private) network.
  - Only a single, unique, IP address is required to represent an entire group of internal or private computers, such as a home network.
  - In a home setup, a NAT firewall allows several home devices to share a single IP provided by an ISP
  - NATs help to hide the internal setup of your network.

Home Networks

- Home Routers provide a combination of:
  - IP address routing (gateway)
  - Network address translation (NAT)
  - DHCP functions
  - DNS
  - Firewall functions
  - LAN connectivity like a Network switch
  - Modem Functionality
  - Some allow you to connect an external USB or E-Sata drive as a means of providing shared storage.



Netcats

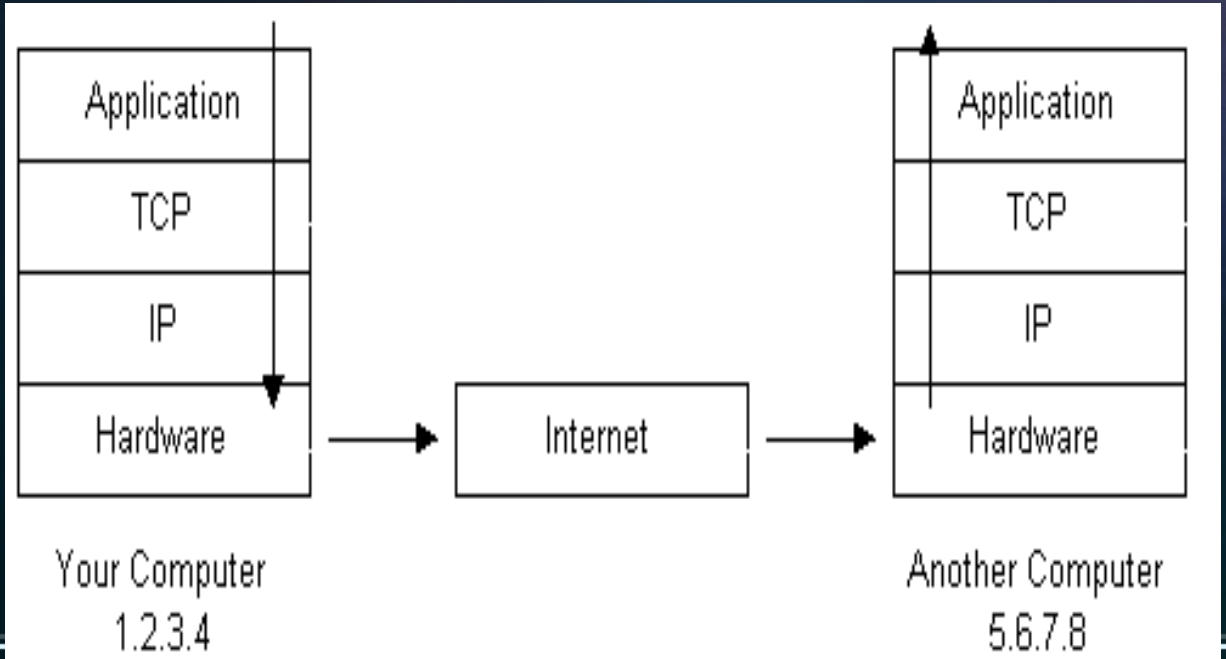
- https://www.youtube.com/watch?v=frnoxPi0uGs
- Learn more: Leo Tindall YouTube

WireShark

Extra Material

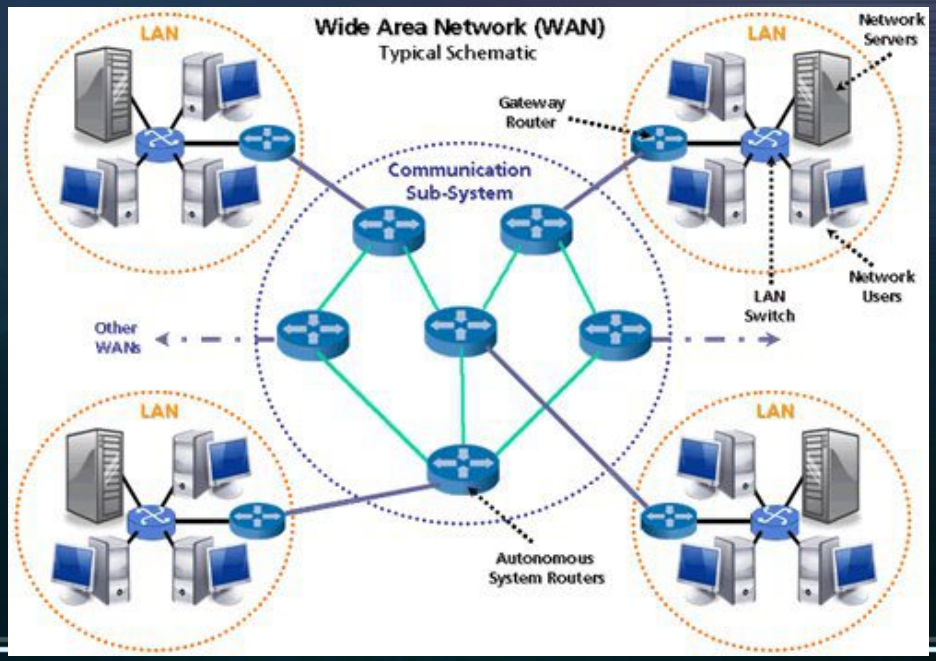
The Hardware Layer

- The “hardware“ layer (sometimes called the “Link Layer”) of the internet is in charge of transmitting data over a physical medium.
- The physical medium for transmitting data can take on many forms and is implemented with a wide variety of technologies, both wired and wireless.



Connecting to LANs and WANs

- The Hardware layer defines how:
  - We connect devices to LANs
    - Wired
      - Ethernet (NICs and Switches)
    - Wireless
      - Wifi (802.11 B/G/N)
  - We connect LANs to WANs
    - Wired (Broadband)
      - Modem*
      - DSL
      - Cable
      - Fiber Optic
    - Wireless
      - Satellite
      - 4G (Cell service)



Connecting to LANs - Ethernet

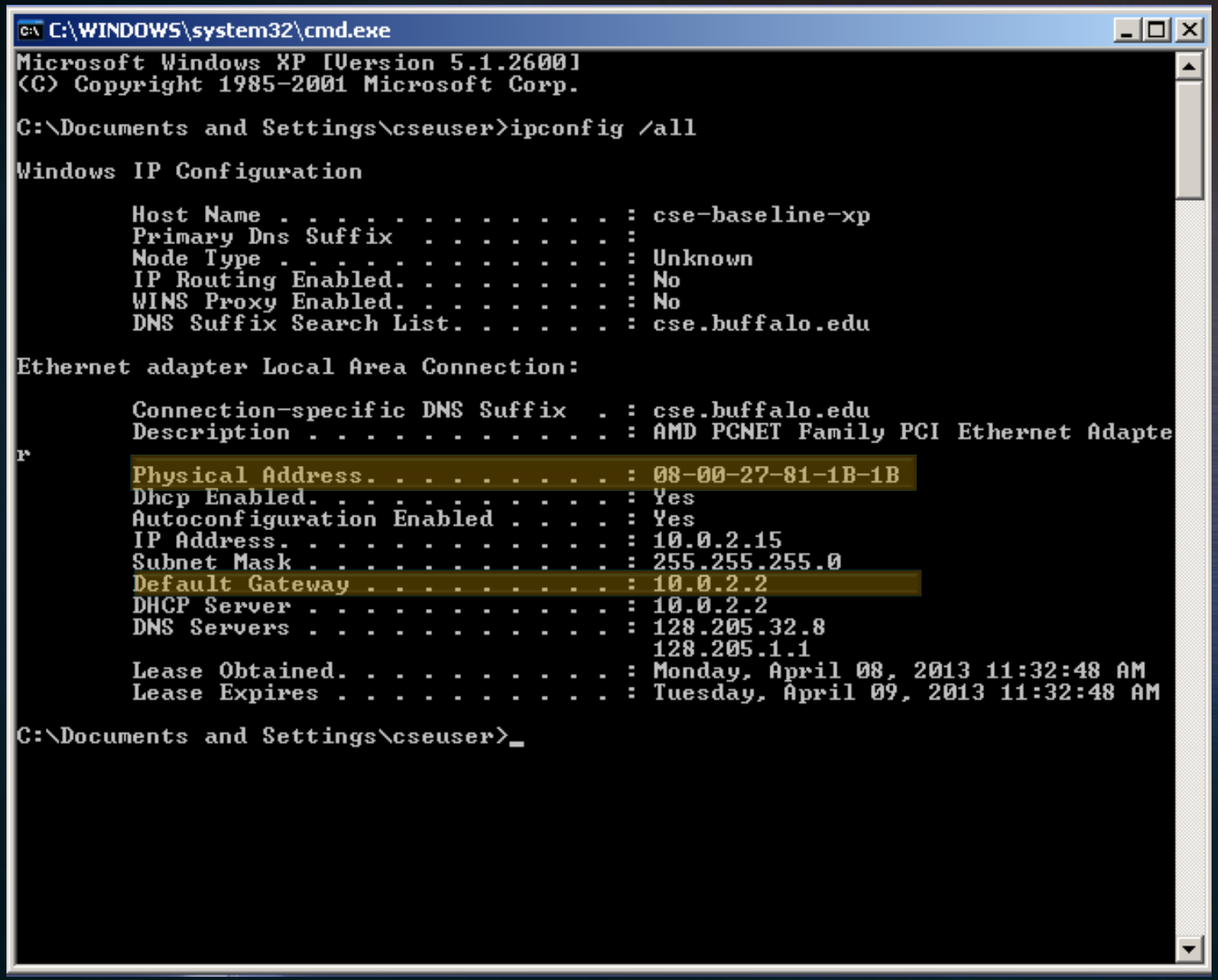
- The Ethernet can be thought of as:
  - Hardware communication devices
  - Topologies of devices being used
- Common Ethernet speeds are around 1000Mb/s (1000Base-T) also called gigabit.
- Most Ethernet devices such as network interface cards and switches have the ability to negotiate the highest available speed.
- Power over Ethernet (PoE) allows the transmission of power through an Ethernet network cable. This is useful for things like VOIP phones.

Connecting to LANs - Ethernet

- Switches - devices that physically connect multiple computers together to form a subnet.
  - Switches use a star topology and work by joining electrical pathways together, so that devices can talk to each other.
  - Hubs look similar to switches but use a ring topology, relying on each member node to pass along a packet of information.
  - More advanced switches support Virtual Local Area Networks, VLANS, SPANing, TAPing, port filtering, etc…

The Hardware Layer

- All machines have a Hardware address called a “MAC” address, or “Media Access Control Address”.
  - address is hardcoded on the network interface card (NIC) and usually cannot be changed.
  - The MAC address is used when delivering messages along a subnet.
- It is possible for a MAC address to have multiple IP addresses bound to it.
- The binding between MAC and IP address is handled through “Address Resolution Protocol” (ARP).


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\cseuser>ipconfig /all
Windows IP Configuration
Host Name . . . . . : cse-baseline-xp
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cse.buffalo.edu
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : cse.buffalo.edu
Description . . . . . : AMD PCNET Family PCI Ethernet Adapte
r
Physical Address. . . . . : 08-00-27-81-1B-1B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
DHCP Server . . . . . : 10.0.2.2
DNS Servers . . . . . : 128.205.32.8
128.205.1.1
Lease Obtained. . . . . : Monday, April 08, 2013 11:32:48 AM
Lease Expires . . . . . : Tuesday, April 09, 2013 11:32:48 AM
C:\Documents and Settings\cseuser>

The Hardware Layer

- Your machine will only use ARP to communicate with other devices on your own subnet.