UNDERSTANDING NETWORKING WITH INTERNET TECHNOLOGIES

1. OBJECTIVE

To explore and understand the fundamentals of networking with TCP/IP protocol suite, i.e. the Internet technologies.

2. LABORATORY

Hardware Laboratory I (N4-1a-3).

3. EQUIPMENT

PC with Microsoft Windows OS, and access to the Internet.

4. DURATION

2 hours.

5. EXERCISE 1A: COMMUNICATION ARCHITECTURES

Enabling communications between different computers is too complex to be developed as a single large module. Hence, the task is being sub-divided into a number of small manageable modules/layers, and linked in a logical manner.

This led the International Organization for Standardization (ISO) to develop the Open Systems Interconnection (OSI) reference model where the communication functions are partitioned into a hierarchical set of seven layers.

However, the TCP/IP protocol suite developed earlier by the US Department of Defense (DoD) has gained commercial dominance and become the de facto standard. There is no official TCP/IP communication architecture as there is in OSI. Nevertheless, to facilitate understanding, we may loosely characterize TCP/IP as involving 5 layers.

Figure 1.1 illustrates the layers of the OSI and TCP/IP communication architectures, showing roughly the correspondence in functionality between the two.

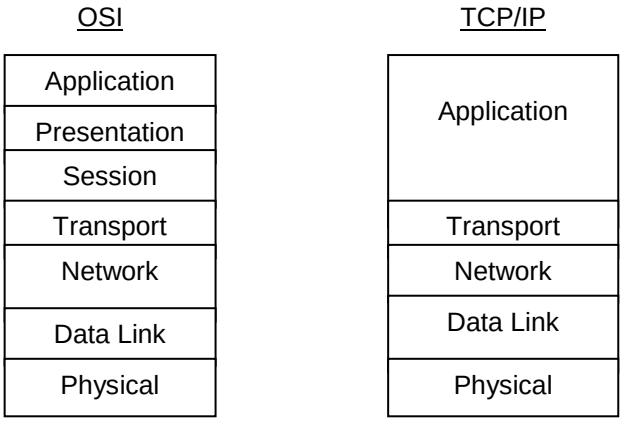


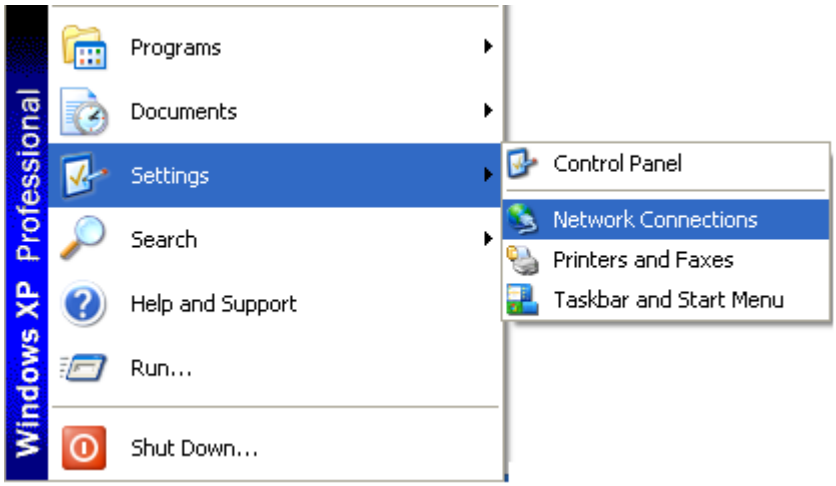
Figure 1.1: A Comparison of the OSI and TCP/IP Protocol Suite

Each layer in the TCP/IP protocol suite interacts with its immediate adjacent layers. At the source, the application layer makes use of the services provided by the transport layer. Similarly, the transport layer makes use of the services provided by the network layer, and it in turn makes use of the services provided by the data link layer. Ultimately, actual transmissions occur at the physical layer.

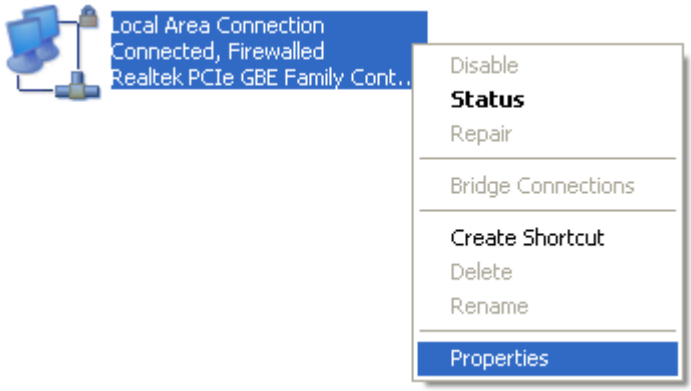
At the destination, each layer delivers data up to the next higher layer.

The Internet is built on the foundation of the TCP/IP protocol suite. Microsoft Windows OS is Internet-ready, so it must have the TCP/IP suite implemented.

Open the Network Connections Panel in Windows OS by clicking on the Start button, and select the Settings ► Network Connections option as follows:



Next, right-click on the Local Area Connection and select the Properties option as follows:



A list of communication modules installed in the Internet-ready Windows OS will be shown. Classify the following installed communication modules into their appropriate layers in the TCP/IP architecture:

Internet Protocol (TCP/IP) :
Realtek PCIe GBE Family Controller :

6. EXERCISE 1B: ADDRESSING

Several levels of addressing are used in the TCP/IP protocol suite.

First, each network device/computer attached to a network such as LAN (Local Area Network) must be allocated a unique address. Examples IEEE 802.3 Ethernet using the 48-bit addresses. We refer to such addresses as physical addresses or MAC addresses.

To facilitate global communications between different devices/computers using different MAC addresses in different networks, there is a need to have another common logical addressing format, and each and every device/computer must be assigned a unique address associated with this format. In the TCP/IP architecture, this is referred to as an IP address.

Typically, a computer will support multiple processes or applications. Once communication packets arrive at a destination computer, they must be delivered to the correct process. Each process therefore needs another unique address/identifier, referred to as port number.

Based on your understanding of the addressing, classify the use of the following addresses into their appropriate layers in the TCP/IP architecture:

Port number :
IP address :
MAC address :

7. EXERCISE 1C: PHYSICAL/MAC/ETHERNET ADDRESSES

Nowadays, almost all LANs are using Ethernet technology, which is also known as IEEE 802.3 standard.

The Ethernet address consists of 48-bit and is divided into two fields: the first 24 bits consist of an Organizationally Unique Identifier (OUI) assigned to a vendor by the IEEE (which is why they are also called vendor codes). The Ethernet vendor combines their 24-bit OUI with a unique 24-bit value that they generate to create a unique 48-bit address for each Ethernet interface they build.

Determine the MAC address of your laboratory PC:
[Hint: explore the use of ***ipconfig*** command in DOS prompt by typing ***ipconfig /?*** for available usage options and syntax]

MAC Address :
Manufacturer :
[Hint: http://standards.ieee.org/develop/regauth/oui/public.html]

8. EXERCISE 1D: IP ADDRESSES

To prevent conflicts, IP addresses are centrally coordinated by IANA (http://www.iana.org), operated by ICANN (http://www.icann.org/). The role of IANA is to allocate IP addresses from the pool of unallocated addresses to the five RIRs (Regional Internet Registries) according to their needs.

Registry	Area Covered
AfriNIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Internet Service Providers (ISPs) and organizations/companies which are members of these RIRs are then able to obtain a range of IP addresses for their use.

IP address, specifically IPv4 address, is 32-bit long, and is usually written as dotted decimal notation. For example, the IP address 11000000 11100100 00010001 00111001 is written as 192.228.17.57.

Traditionally, IP addresses are divided into five classes A, B, C, D and E. Classes A, B and C are for normal use and are shown in Figure 1.2. Classes D and E are for multicast and future use respectively.

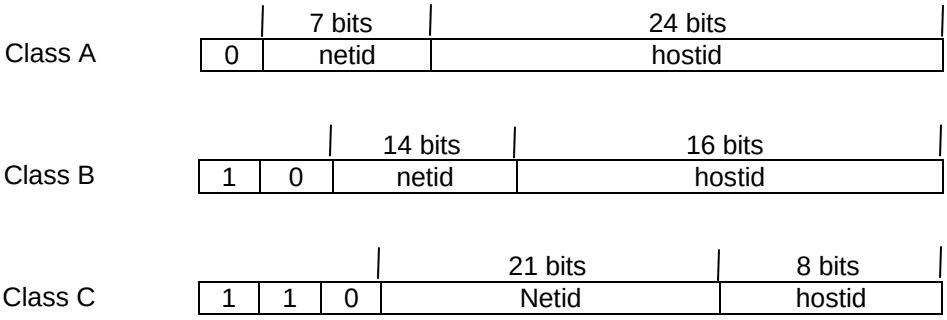


Figure 1.2: Classes of IP Addresses

With the depletion of IPv4 addresses, the above classful addressing is mostly outdated. Instead, the concept of Classless Inter-Domain Routing (CIDR) addressing is now widely used:

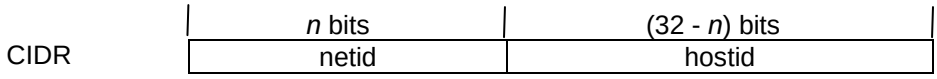
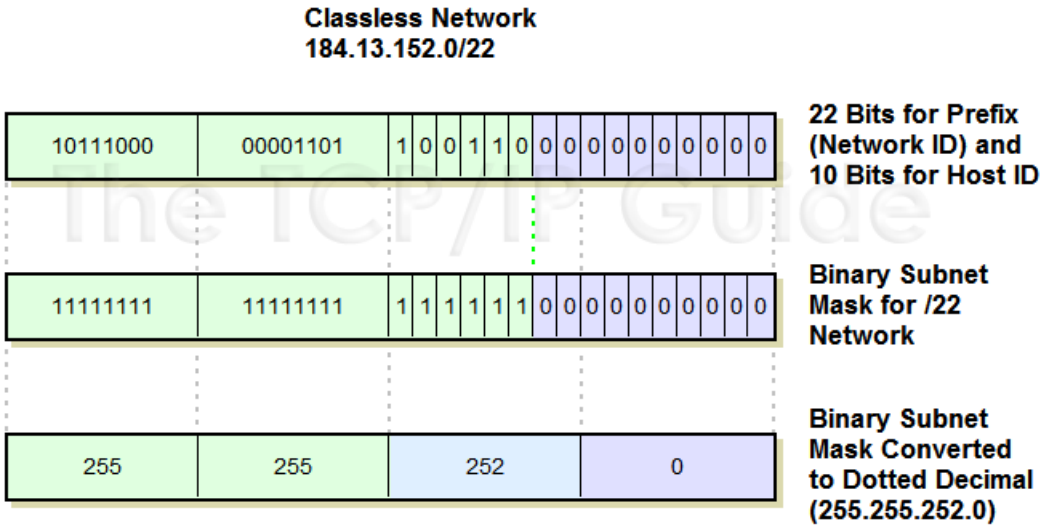


Figure 1.3: CIDR IP Addresses

In contrast to fixed length netid in classful addressing, CIDR allows variable length netid. Hence, there is an additional requirement for a 32-bit network mask (also known as subnet mask) to indicate the length of netid - with all bits corresponding to netid set to '1's, and remaining bits corresponding to hostid set to '0's; e.g.:



What is the range of IP addresses allocated to NTU?
[Hint: whois search @ http://wq.apnic.net/apnic-bin/whois.pl]

NTU IP address range :

In addition, there are special uses of certain IP addresses. Using the notation:

IP address ::= { <netid>, <hostid> }

Determine the special uses of the following IP addresses:
[Hint: RFC 1918, RFC 5735]

{ 127, <any> } :
{ 172.21, <any> } :

9. EXERCISE 1E: DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Once an organization has obtained a block of addresses, it can assign individual IP addresses to the host and router interfaces in its organization. A system administrator may manually configure the IP addresses into the host, but more often this task is done by using the Dynamic Host Configuration Protocol (DHCP). DHCP allows a host to obtain (be allocated) an IP address automatically as shown in Figure 1.4.

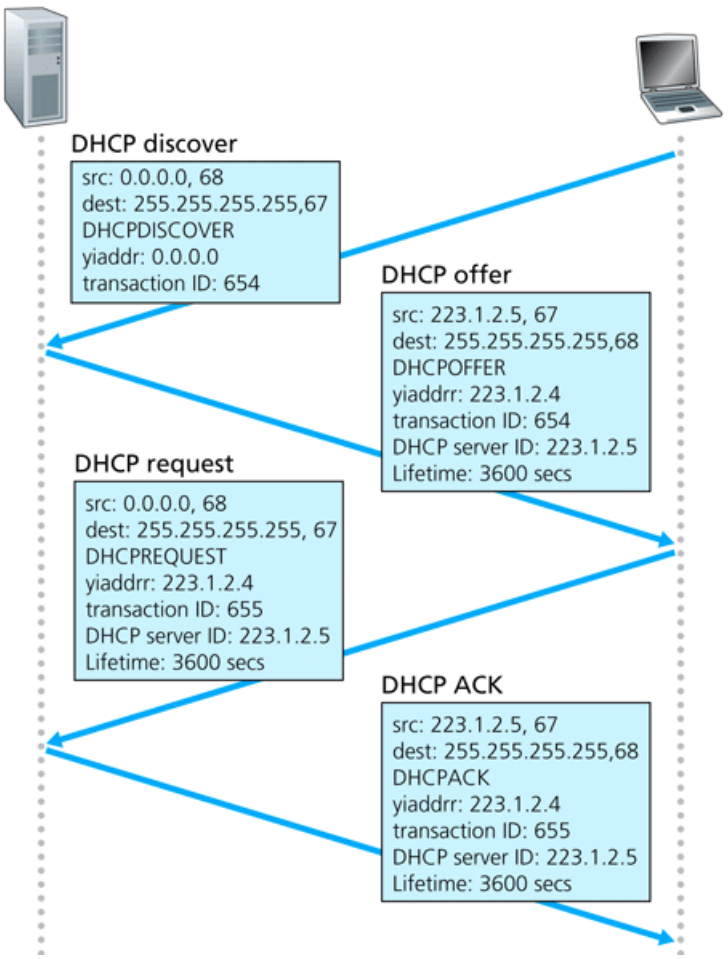


Figure 1.4: Dynamic Host Configuration Protocol (DHCP)

Determine the following for your laboratory PC:
[Hint: use ***ipconfig*** command]

DHCP Enabled :
DHCP Server :
IP Address :
Network/Subnet Mask :

ipconfig shows your real IP address assigned by ISP/organization. If your PC is behind a NAT (Network Address Translation), your assigned IP address is hidden by the NAT. Visit any of the following websites to check your IP address:

- http://whatismyipaddress.com
- http://www.whatismyip.com
- http://checkip.org

Is the reported IP address the same as your assigned IP address? What is the reported IP address?

IP address of the computer :
IP address seen on the website :

Who is the owner of the IP address reported by the website?

10. EXERCISE 1F: PORT NUMBERS

Presuming data has been correctly delivered to the destination network device/computer, port number is then used to deliver it to the correct process.

How do you know the port number? The direct way will be to obtain it from whoever is running the server process; just like you need to obtain your friend's phone number before you can give a call.

For the purpose of providing common services to any client, IANA/ICANN is also managing and controlling a range of port numbers from 0-49,151. Each common service is assigned a unique number known as well-known port.

For example, most web servers are running at well-known port 80. As a result, there is no requirement for us to indicate port number during web surfing since our browser is configured to automatically contact port 80.

Some of the common services in TCP/IP are listed below. Determine their well-known ports:
[Hint: RFC 1700, RFC 3232]

TELNET	:
Simple Mail Transfer Protocol (SMTP)	:
Quote of the Day Protocol	:
Domain Name Service (DNS)	:
Hyper-Text Transfer Protocol (HTTP)	:

11. EXERCISE 1G: DOMAIN NAMES

It is hard to remember everyone's IP address. The Domain Name System (DNS) makes it easier by allowing a familiar string of letters (the domain name) to be used instead of the arcane IP address. So instead of typing 192.0.32.8, you can type www.iana.org. It is a 'mnemonic' name that makes addresses easier to remember.

In the Domain Name System (DNS) naming of computers there is a hierarchy of names. The root is unnamed. Under the root is a set of what is called top-level domain names (TLDs). These are the generic TLDs (gTLDs) such as .edu, .com, .net, .org, .gov, .mil, and .int, and the two letter country code TLDs (ccTLDs) such as .sg from ISO-3166. Under each TLD there may be created a hierarchy of names.

Similar to IP addresses, domain names need to be unique. IANA is also the central coordinator for it, specifically for the gTLDs and ccTLDs.

A central Internet Registry (http://www.internic.net) has been designated to manage gTLDs. On the other hand, individual countries typically manage their respective ccTLDs; e.g. SGNIC (http://www.nic.net.sg/) is managing the domain names under .sg. For scalability, many commercial companies are accredited as domain name registrars to offer domain name registration services to users.

How do you register/buy a domain name under .sg, e.g. myweb.per.sg?
[Hint: http://www.nic.net.sg]

12. EXERCISE 1H: DOMAIN NAMES/IP ADDRESSES TRANSLATION - DOMAIN NAME SYSTEM (DNS)

Now, Internet host can be identified in two ways: by a domain name or by an IP address. However at the network/Internet layer, only IP address is recognized. So domain name needs to be translated to IP address, and is achieved with the implementation of Domain Name Service (RFC 1034, 1035) at the application layer.

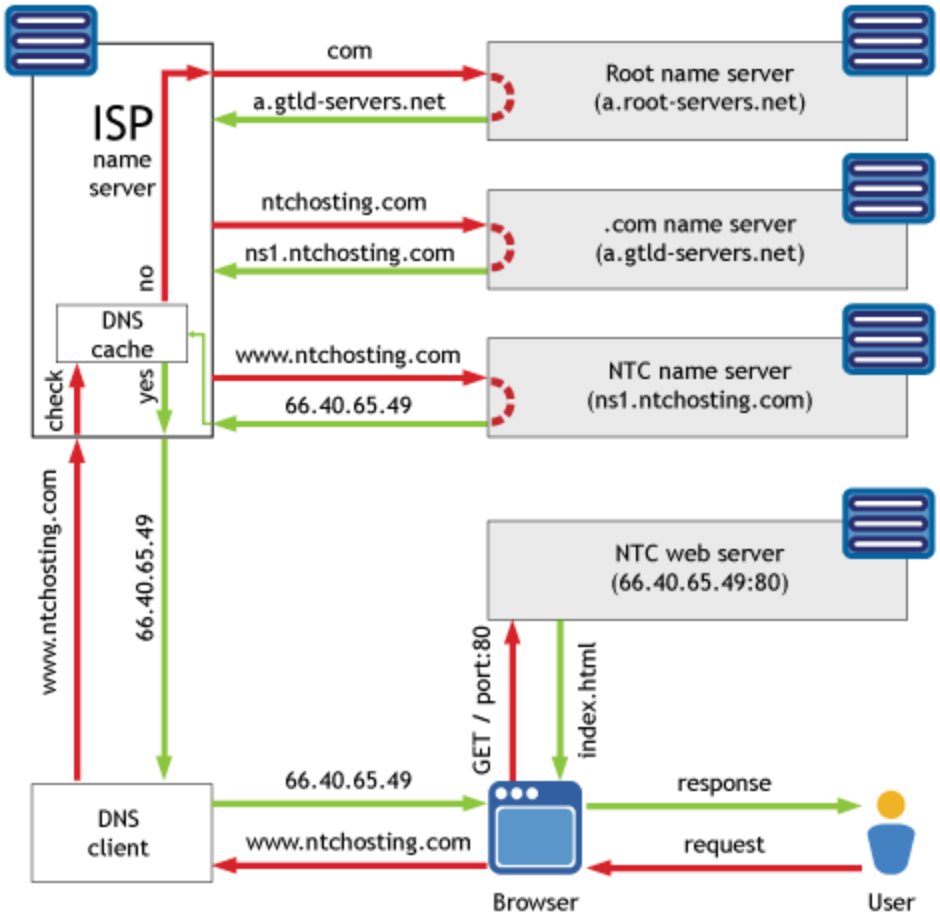
At the heart of the DNS are 13 special computers, called root servers. They are coordinated by IANA and are distributed around the world. All 13 contain the same vital information – this is to spread the workload and back one another up. The root servers contain the IP addresses of all the TLD registries – both the global registries such as .com, .org, etc. and the country-specific registries such as .sg, etc.

Scattered across the Internet are thousands of computers – called Local Name Servers. These are located strategically within Internet Service Providers (ISPs) or institutional networks. They are used to respond to a user's request to resolve a domain name – that is, to find the corresponding IP address. When a local name server cannot immediately satisfy a query from a client (because it does not have a record for the hostname being requested), it behaves as a DNS client and queries one of the root name servers.

However the root name server may not have a record for the queried hostname. Instead, the root name server will know the IP address of an authoritative name server that has the mapping for that particular hostname.

By definition, a name server is authoritative for a host if it always has a DNS record that translates the host's hostname to that host's IP address. Actually, each host is required to have at least two authoritative name servers, in case of failures. The authoritative name server is then queried by the root name server or the local name server for the translation. Many name servers act as both local and authoritative name servers.

Let us take a look at an example: suppose that a user is accessing the web site, http://www.ntchosting.com. Here is the sequence of steps:



1. Browser machine launches the DNS client to send a request to the local name server to resolve the IP address of the web site.
2. If the local name server does not have the domain name in its cache, it issues a request to one of the root name servers.
3. The root name server looks up its table and returns the name server responsible for .com domain.
4. The local name server contacts the .com domain name server.
5. The .com domain name server looks up its table and returns the name server responsible for ntchosting.com domain.
6. The local name server then contacts the ntchosting.com domain name server.
7. The ntchosting.com name server looks up its table for www.ntchosting.com and returns the corresponding IP address.
8. The local name server returns the IP address to the browser via DNS client.
9. Finally, the browser is able to contact the web site.

Determine the followings:

Local DNS servers for your laboratory PC :
[Hint: ipconfig]
Authoritative DNS servers for ntu.edu.sg :
[Hint: whois search @ http://www.nic.net.sg]

What is the IP address of domain name www.ntu.edu.sg?
[Hint: explore the use of ***nslookup*** command in DOS prompt]

For efficiency reason, DNS search results are cached temporarily. What is the command to show the entries in the DNS cache? What is the command to clear the entries in the DNS cache? [Hint: explore the use of ***ipconfig*** command]

13. EXERCISE 1J: PROPRIETARY MICROSOFT WINS

Conceptually, the purpose of Windows Internet Name Service (WINS) is to resolve names to IP addresses similar to DNS. However, WINS is proprietary and is only supported in Microsoft Windows environment. In addition, names in WINS, also called NetBIOS names, are flat (i.e. unlike domain names which are hierarchical) and can only be up to 15 characters long.

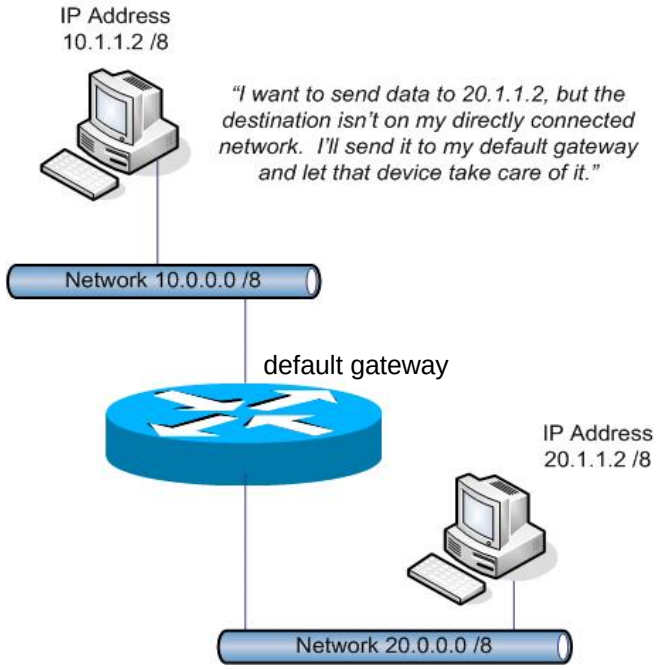
In organisations running Windows environment like NTU, it is common to see WINS in addition to DNS. In this case, when a name needs to be resolved, DNS is tyically being queried first. If not successful, e.g. the given name is a non-existent domain name, then WINS will be queried.

Determine the following for your laboratory PC:
[Hint: use ***ipconfig*** command]

NetBIOS/Host name :
Primary WINS server :
Secondary WINS server :

14. EXERCISE 1K: DEFAULT GATEWAY

Except for computers on the same LAN which can be reached directly, a source computer will usually not know how to send messages to a destination computer outside its own network. Hence, there is a need for a default gateway which your computer relies on when it does not know how to reach a destination computer as shown below:



Typically, the default gateway is a router, which will have its own routing table to know how to route communication packets to the destination, possibly via other intermediate routers.

Determine the IP address of the default gateway for your laboratory PC:
[Hint: use ***ipconfig*** command]

Default gateway :

15. EXERCISE 1L: IP ADDRESS/PHYSICAL ADDRESS TRANSLATION - ADDRESS RESOLUTION PROTOCOL (ARP)

To reach from a source computer on a LAN to another, ultimately it is the 48-bit Ethernet address that is required. So far, the source computer only knows the name/IP address and port number of the destination computer, how does it know the Ethernet address of the destination computer?

RFC 826 specifies the Address Resolution Protocol (ARP) converting IP addresses to 48-bit Ethernet address for transmission on the Ethernet LAN, and works as follows:

ARP sends an Ethernet frame called an ARP request to every host on the network. This is called broadcast. The ARP request contains the IP address of the destination host and is asking 'if you are the owner of this IP address, please respond to me with your hardware address'.

The destination host's ARP receives this broadcast, recognizes that the sender is asking for its IP address, and replies with an ARP reply. This reply contains the IP address and the corresponding Ethernet address.

The ARP reply is received and the data can now be sent.

Similar as DNS cache, for efficiency reason, an ARP cache is also maintained, which contains the recent mappings of IP addresses to Physical/MAC addresses. The normal expiration time of an entry in the ARP cache is 2 minutes from the time the entry is created.

To show the entries in the ARP cache, explore the use of ***arp*** command in DOS prompt by typing ***arp -?*** .

What is the physical address of default gateway?

16. EXERCISE 1M: NETWORK REACHABILITY – *PING* COMMAND

"Ping", developed by Mike Muuss in 1983, is a common computer network tool used in the Internet to test the reachability of a particular computer in a network. It provides a test on whether a computer can be reached from another. If so, it measures some statistic information about the connectivity, such as round-trip time and packet loss rate.

Ping has been used by many worms and viruses to find target on the Internet for infection. As such, many firewalls blocks ICMP "echo request". Consequently, ping may fail to report a positive reachability when crossing firewalls. However, it is still useful when testing the network connectivity of a computer in some cases.

Ping can also be used to debug the network configuration. The debugging procedure may consist of the following steps.

STEP 1: ping 127.0.0.1
Do you get a positive reachability result? If not, TCP/IP component in your computer is not working or installed.

STEP 2: ping your IP address.
Do you get a positive reachability result? If not, your network configuration may not be properly setup.

STEP 3: ping the default gateway
Do you get a positive reachability result? If not, the default gateway is incorrect or not working.

STEP 4: ping the DNS server(s)
Do you get a positive reachability result? If not, the DNS servers are incorrect or not working.

STEP 5: ping your host name
Do you get a positive reachability result? If not, the DNS resolution is not working.

At this point, you can assure that the basic network configurations are properly set on your computer.

Now, ***ping*** your neighbour's PC.

Run the ***arp*** command again. Do you see your neighbour's PC listed? Why? What is the physical address of your neighbour's PC?

17. EXERCISE 1N: TRACE ROUTE – *TRACERT* COMMAND

Often we want to find the list of routers a packet traverses from a source to a destination. Identifying the path helps troubleshoot the network, particularly routers. The network tool that provides this function is named “tracert”. Simply type ***tracert*** followed by the destination hostname, a list of IP addresses of the routers will be displayed showing the path that a packet is routed from your computer to the destination. In the list, the last record shows the destination IP address, others are IP addresses of routers.

Similar to ping, tracert may be blocked by firewalls for security reasons. Hence, tracert may fail to find the destination.

Now, ***tracert*** to your local DNS servers. How many routers are separating your laboratory PC and the local DNS servers in your network?

Run the ***arp*** command again. Can you find the physical address of the DNS servers? Why?