Historical and Future Development of Internet Addresses. Identification, Address Resolution, Routing, Routers, Route tracing and Faultfinding

The Internet can be considered as "a collection of interconnected networks that use the Transmission Control Protocol / Internet Protocol suite" The Internet has its routes in experimental packet switching work which was conducted by the US Department of Defence Advanced Research Project Agency (ARPA). The research and development accomplish by ARPA resulted in the development of ARPANet. This network was responsible for the development of various aspects of the Internet such as file transferring, e-mail and remote terminal access to computers which became incorporated into the TCP / IP protocol. Most of this was done during the 60s and 70s and was later taken on by the Internet Architecture Board (IAB). The IAB is responsible for the development of Internet protocols and IP addressing. The IAB works in conjunction with the Internet Engineering Task Force (IETF), which in the past, has been in charge of developing such standards as IP version 4 and IP version 6. As development has occurred many different approaches have been taken to share information such as FTP, HTTP, STMP, IRC etc, which all have their unique way of sharing information but they can all be termed as the Internet as they use the basic underlying fundamentals of IP addressing and routing. I have used IP addressing and the Internet interchangeably.

An IP (Internet Protocol) address can be defined as "a unique identifier for a node or host connection on an IP network". A Protocol can be defined as "an agreed-upon format for transmitting data between two devices". Without an agreed format for transmitting data the very concepts of IP addressing could not exist as without a standard communication would be impossible between different protocols. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. Every IP address consists of two parts, one identifying the network and one identifying the node / host. Currently the Internet Protocol is running on IP version 4 (IPv4), which is a 32 bit addressing structure. An IP address is divided into a network number and a host number. Each number is separated from another number by a dot (decimal point). An example of a typical IP address maybe 182.26.183.123 however the highest IP address allowed in IP version 4 would be 255.255.255.255 as 255 is the maximum value which can be used in an IP address. The InterNIC board is responsible for assigning IP addresses and have broken them down into three main Classes (Class A, B and C). Class A IP addresses are only assigned to large organisations and countries. Such IP address have three bytes available for identifying hosts on one network / subnets. The first bit in Class A address must be zero (Figure 1), the first byte must be range from 1 to 127. Through the use of 7 bits for the network portion and 24 bits for the host portion of the address, 128 networks can exist with around a 16.78 million hosts on each Class A network. A Class B network use two bytes for the network identifier which are used to denote that it is a Class B network. As the two bits of the network portion are used to identify a Class B network, the network portion is reduced to a width of 14 bits and thus only 16384 networks can be assigned which can each have 65536 hosts. Class B addresses are often given to large organisations such as IBM which has tens of thousands of employees. Finally Class C addresses use three octets to identify the network as shown in figure 1. As 21 bits are used in Class C network more then 2 million distinct networks can supported (2^21 = 2097152) and on each network 256 hosts operate in

theory. Transmission Control Protocol (TCP), can be defined as “the suite of communications protocols used to connect hosts on the Internet”. TCP/IP uses several protocols, the two main ones being TCP and IP. The difference between an IP and TCP is that IP protocol deals only with data packets, while TCP enables two hosts to establish a connection and thus can exchange data.

IP addresses are key to how the Internet functions and without them addressing would be completely impossible under the current IP version 4 standard. IP addresses act as unique identifiers and every device wishing to use the Internet must be assigned one. Figure 2 helps to show what levels of the ISO OSI model IP and TCP protocols operate at. TCP can be thought of as the layer which contains the protocols to carry out various methods of data transfer while the IP address act much like a postal address which the protocols uses to identify where to send the packets and where the packets have come from. If we are to understand addressing, it is important to look at the TCP protocol header. Figure 3 demonstrates how the protocol header is made up. The main parts of the TCP protocol header is the sequence number which is used to identify the data segment being transported. That data field is also very important as it contains the data which is being transmitted to, two or more devices. However the TCP protocol can not work without the IP header which is the reason why both are paired together and called TCP / IP. Figure 4 shows the IP header which contains important information such as the destination address which contains the information of where the data is to be sent to, also the source address indicates where the data has come from which enables two devices to communicate with each other. The TCP protocol operates at the transport layer and the Internet protocol operates at the Internet layer of the ISO OSI model. This is very important as it helps to explain the various jobs each protocol is responsible for. For example at the application level such software runs such as FTP. The actual data which is being sent / received by the ftp will actually be contained in the TCP header while the IP header will only really be concerned with handling address mapping for the transmission of data between two or more hosts. A simple real life example could be that the address on a letter could be considered, as the IP address while the actual letter inside would be the data contained in the TCP header.

IP addresses can be assigned to be static or dynamic. However it must be remembered that the initial assignment of IP addresses will be carried out by InterNIC. This is too unsure that the same IP is not given to for example two FTP servers. No two computers can use the same IP address. However, one computer (or device) may have several IP addresses. An example of this might be that a computer that serves as a host for multiple services in which case each service may have one or more IP addresses. If the same IP was being used by two web servers it would be impossible to determine where to send a request. Once an IP address / addresses have been given to an organisation how they are assigned is up to the administration of the network. An ISP (Internet Service Provider) for example may have a pool of addresses which it may assign dynamically as each person logs on. This address would then become their address while they are connected. Once they disconnect from the ISP the IP address they were using goes back into the pool. This is called dynamic assignment of IP addresses. As these are assigned by the network administration it may be difficult to predict the exact IP address and quite unlikely to be the same next time you connect. It is important to take into account that dynamic assignment is only possible up to a certain point. This is because an organisation will be given a set number of IP

addresses such as a class C IP address. In such a case it will only be able to assign 254 addresses at any given time. This would limit the assignment of IP address, as truly dynamic assignment would be mean the organisation would be free to assign any IP it chooses. In contrast a static IP address is given to say a web server where the IP address will always be the same. It will not change if the server is connected to the net or not. Nevertheless if the server is not connected it will not be possible for other networks to access it because the data stored on the web server will not be connected to the Internet. The purpose of such an activity depends on what the IP addresses is used for. If for example a company sets up a FTP server it would want the address to constant as it would be pointless if the address was forever changing as employees would have to have up to date information about the servers IP address in order to access it. However in the case of the ISP users only need the IP for a short space of time and thus it would be pointless giving each user his / her own IP if a pool of IP addresses can be shared amused users. Security is also an issue as dynamic assignment may prevent attacks on a system because the hacker will have to discover the new IP address of the server he / she was previously hacking into.

IP addresses must be assigned to a network in order for the network to communicate on the Internet but this does not take into account the practical side of implementing IP addresses. The address resolution protocol (ARP) is a protocol used by the Internet Protocol network layer protocol to map IP network addresses to the hardware addresses. The protocol operates below the network layer as a part of the OSI link layer, and is used when IP is used over Ethernet. Therefore IP addresses must be mapped onto Medium Access Control (MAC) addresses in order to assign certain IP addresses to certain devices within the network. A MAC address can be defined as “a hardware address that uniquely identifies each node of a network”. In IEEE 802 networks, the Data Link Control layer of the OSI Reference Model is divided into two sub layers, which are the Logical Link Control layer and the Media Access Control layer. The MAC layer interfaces directly with the network media. This means that each different type of network media requires a different MAC layer. The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a local computer to a remote computer / server. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address. Basically ARP can be thought of as the protocol which translates IP addresses into MAC addresses which enables data from an external networking via the Internet to reach its destination.

Domain Name System (or Service) can be defined as “an Internet service that translates domain names into IP addresses”. Domain names are alphabetic which makes them easier to remember. However the Internet is based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.wmin.ac.uk might translate into an IP address such as 213.83.195.65. A Domain Name Server performs the translation of English words into to 32 bit IP addresses. The DNS system can be viewed as its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address

match has been found. Each network normally has its own its own Domain Name Server, and when communication is established between the such servers on a TCP/IP networks connected to the Internet are referred to as a Domain Name Service (DNS). There are six top level domain names which are .com, .edu, .gov, .mil, .net, and .org. However DNS can be used for other IP address unrelated to the HTTP protocol such as ftp, mail servers (SMTP / POP3), news (for UseNet servers) etc.

It is of up most importance to understand how networks communicate with each other to be able to understand how routing is carried out on the Internet. Routing can be defined as “the internetworking and processes of moving a packet of data from its source to its destination”. Routing is usually performed by a dedicated device called a router. It is a key feature of the Internet because it enables data to pass from one computer to another and eventually reaching the target machine (destination). The Internet could not exist without routing as in theory if different networks could not send and receive data they could not operate as an Internet which is basically many smaller networks connected to form one massive grid. Internet routing devices have also been known to be called gateways. In today's terminology, however, the term gateway refers specifically to a device that performs application-layer protocol translation between devices. There are two main types of gateways, which perform different functions in terms of routing on the Internet. An interior gateways are devices that perform protocol functions between machines or networks under the same administrative control or authority, such as a corporation's internal network. An example may be data being transfer from one area of the network to another or an internal message board system. These are sometimes known as autonomous systems which can be thought of as a collection of networks (routers), administered by a single authority which use the same Interior Gateway Protocol (IGP) to route packets. Exterior gateways perform protocol functions between independent networks. Such an example may include may include the action of sending an e-mail to someone outside the organisation as the data packets would have to pass internally until they can be delivered by a mail server (SMTP) to there destination. However we are mainly only concerned which exterior gates as this is the method used for networks to communicate with the Internet.

To be able to explain how routing is conducted on the Internet routers must be investigated. The underlying technology must be understood as to how data packets are received and sent by the router. They operate at the network layer of the ISO OSI model, which basically means that their main activity is to examine network addresses and make decisions about whether or not data on a network should remain on the network or if it should be transmitted to a different network. Headers of data packets are examined and the source / destination are determined by the router and the data packet is forwarded or retained accordingly. Routers are not concerned as to what is being transmitted but where the data should be sent. Therefore a router will not prevent a DoS attack as the data is only transmitted and not examined and thus the receiving host is responsible for data analysis. In simple terms a router operates by learning about disruptions and delays on network segments from other routers and store continuously updated information about routes availability. Route status can change based on traffic volumes, hardware malfunctions, and planned outages. Most routers do not know the location of every location of every router and routers are being added to the Internet on a frequent basis.

There are various ways in which data packets are transmitted via the Internet. Figure 5 shows how a router would send and received data packets using switching. A router possibly may have a configuration table which holds such information as how connections lead to particular groups of addresses, which connections prioritise over others and rules for handling both routine and special cases of traffic. Packet data, such as an e-mail message, travels over a system known as a packet-switching network. The raw data is broken up into packages of about 1,500 bytes long. Each of these packages includes information on the source, destination and checksums to ensure that the data packet is not corrupted in any way. Once the router has examined the data pack the router will decide the best route for the data packet to travel down. In figure 5 the router actually determine the best course of action for the data packet but the switches are responsible for diverting the data packet to its destination. It is important to bear in mind that the route chosen is likely to be the most efficient but that does not necessarily mean the shortest. For example a certain part of the network might be very heavily loaded with huge amounts of request, thus it may make more sense for the data packet to be sent around the congested area.

Under windows and Unix there are several ways in which it is possible to trace data packets and connections between the local network and the Internet. Under windows there is a facility called "TRACERT" (Trace Route). This command is a diagnostic utility that demonstrates the path the data packet takes to reach its destination. In figure 6 I have traced the route a data packet will take from my computer to, two different website. At the top of figure 6 I have carried out a trace on wmin.ac.uk and on the left the IP address is shown for www.wmin.ac.uk, which has been converted by DNS into its number form. The numbers of the left hand side indicate how many hops the data packet had to go through and the addresses associated with each number is the IP of the router. The data packet passed through 15 hops, as the last hope is not included as it is the destination address. I also carried out the same procedure for www.yahoo.com to demonstrate that the data packet has travels in a totally different direction, which is indicated by it passing through different routers. In this case both data packets went through 15 hops but depending on the network and the location of the server the number could change. The traceroute function can useful to test the path for example to a website to determine if there are any problems making a connection which has happen in the case of www.wmin.ac.uk as the destination was not reachable.

Various problems can occur and error detection must be put in place to ensure that data packets reach their destination error free. Transmission mediums can suffer from several factors, which can cause a data packet to contain errors. Machinery is prone to break down which can effect how data is send and received by a network. White noise is always present on networks as they are in effect electronic circuits. Due to thermal motions of electrons within circuits data can be corrupted and even such things as magnets and physical damage maybe cause data packets to be corrupted or destroyed. Thus it is important to have checks in place, which make sure that data reaches its rightful destination. There are two main types of data transmission, which are Asynchronous and Synchronous transmission. Depending on the type used to transmit data various methods of detection and correction can be implemented. The main difference between the two types of technique is the way in which they transmit data packets, as Asynchronous sends data packets in short pulses while Synchronous transmission sends the data in a continuous stream. As both techniques are very

different from each other they both use different methods of error detection. Asynchronous tends to use more traditional methods of data checking such as parity checking and block checking while Synchronous maybe use Cyclic codes. The actual header in the data packet contains an error detecting mechanism called a checksum. The checksum allow the IP to detect datagrams with corrupted headers and discard them and relevant steps will be taken to request the data packet again.

The Internet is always changing and growing and as technology advances so will the various ways addressing and data packets are transmitted. Over the past 5 years or so the Internet has experienced a massive boom in popularity as more and more people are now using it on a daily basis. One of the major problems in the near future will be the exhaustion of the IPv4 address space. IP version 4 (IPv4), is a 32-bit addressing system which means that in total there are only 4,294,967,296 (2^{32}) IP addresses available for use on the whole internet. This may seem like a huge number of addresses but they are being taken up at an alarming rate. With many new countries and organisations in developing and third world countries being introduced to the Internet on a daily basis it is not uncommon for an individual to have several different IP address as they might have there own Internet connection at home and use the internet from work. The address shortage problem is made worse as IP address space is often efficiently allocated. Such an example maybe that a Internet Service Provider may have a set amount of IP address but when the network is only running at half capacity, half the IP addresses will not be in use which in theory could be used for another task. Any major problem facing the Internet is caused by routing tables growing to unmanageable sizes. As more networks join the Internet, routing table/topology change and become ever more complex. Processing power if now a concern as routers may not be able to cope with the sheer volume of processes / data. Such a problem can not be solved by adding more router as the network in the wide sense will become more complicated. Core routers would have to be taken out which would make various parts of the Internet unusable.

Measures have been thought up to deal with such problems above. IP version 6 (IPv6) is the latest effort to resolve Internet addressing problems. IPv6 replaces the 32-bit address structure of IPv4 with a 128-bit addressing structure, which in turn would increase address space by a factor of 2^{96}. This vastly increases the amount of available IP addresses, which can be allocated. IPv6 is designed as an evolution from IPv4, rather than a complete change to the current structure of the Internet. However changes have been made to the IPv4 header in IP6 which will increase the speed in which routers can process the data. This is effect will make processing more efficient as it will cut down on the routers CPU cycles and thus enabling a higher packet per second (PPS) processing rate to be obtained. The major problem with IPv6 is that it will take many years for it to be successfully implemented as it requires hardware and Internet standards to be updated. The Internet Engineering Task Force is responsible for developing the next generation of the Internet Protocol such as IPv6. It is important to remember that both IPv4 and IPv6 both need to be standards in order for the all the networks on the Internet to work as one and freely exchange data packets.

The future of IP addressing remains to be seen as new technology is being developed at an alarming rate. A totally new break through in transmitting data maybe be discovered but as yet it would be far to assume IP version 6 as the immediate future for IP addressing. Many factors have to be taken into account but one thing that

remains clear is that the Internet is forever growing and changing and this will produce various growing pains which must be anticipated and swift concise measures must be taken to ensure the functionality of the Internet as a whole.

Figure 1:

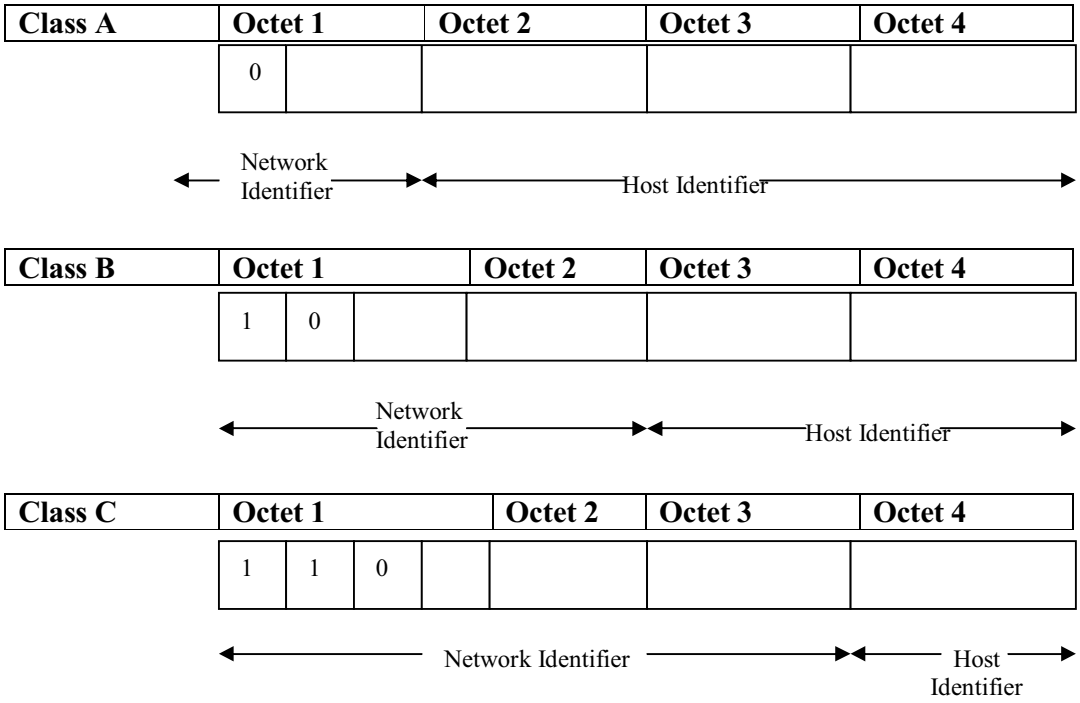

Figure 2: The TCP / IP Protocol Architecture.

Application Layer	HTTP, FTP, TELEMET, DNS, SMTP	DNS, SNMP, RIP, RADIUS	Ping		
Internet Layer	TCP	UDP	ICMP	OSPE	
Transport Layer	IP				ARP
Network Interface Layer	Ethernet / 802.3, Token Ring, ISDN, ATM, PPP, HDLC, xDSL etc etc				

Figure 3: TCP Header Format

2	Source Port
2	Destination Port
4	Sequence Number
4	Acknowledgment Number
2	Data Offset / Control Flags
2	Window
2	Checksum
2	Urgent Power
	Data

Figure 4: IP Header Format

Version	Headers Length
Type Of Service	
Total Length	
Identification	
Fragment Offset	
Time to Live	
Protocol	
Checksum	
Source Address	
Destination Address	
IP Options	

Figure 5: Router and switch.

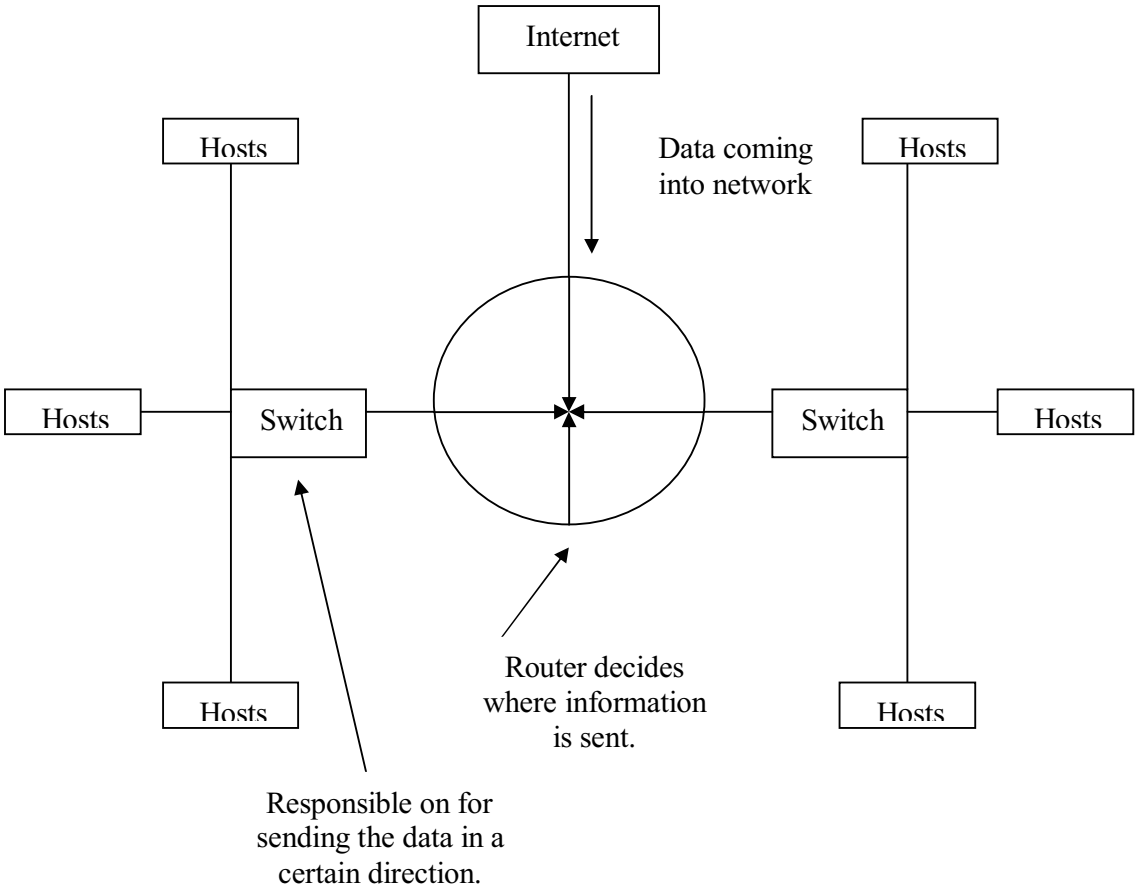

Figure 6: Traceroute

```
Tracing route to isls-web4.wmin.ac.uk [161.74.55.211]
over a maximum of 30 hops:

  1  1101 ms   982 ms   957 ms  rt-loh24a.proxy.aol.com [195.93.34.233]
  2   943 ms   957 ms   997 ms  support12-loh-G3-0.proxy.aol.com [195.93.34.252]

  3  1001 ms   983 ms   970 ms  access11-loh-P3-3.router.aol.com [195.93.36.109]

  4   956 ms   957 ms   958 ms  pop4-loh-P3-0.atdn.net [66.185.146.69]
  5   984 ms   997 ms  1417 ms  bb1-loh-P0-2.atdn.net [66.185.146.64]
  6  1008 ms   957 ms   959 ms  pop2-loh-P0-0.atdn.net [66.185.136.241]
  7   942 ms   970 ms   958 ms  Level3.atdn.net [66.185.143.90]
  8  1010 ms  1469 ms  1902 ms  212.113.3.5
  9  1978 ms   944 ms   958 ms  195.50.116.206
 10  1010 ms   957 ms   958 ms  london-bar4.ja.net [146.97.37.85]
 11   281 ms   301 ms   301 ms  po6-0.lond-scr.ja.net [146.97.35.129]
 12   301 ms   353 ms   288 ms  po0-0.london-bar1.ja.net [146.97.35.2]
 13   306 ms  1010 ms   366 ms  ulcc-gsr.lmn.net.uk [146.97.40.34]
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *     194.83.101.98  reports: Destination net unreachable.

Trace complete.

C:\WINDOWS>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [64.58.76.229]
over a maximum of 30 hops:

  1  1100 ms   957 ms   957 ms  rt-loh24a.proxy.aol.com [195.93.34.233]
  2   916 ms   353 ms  1023 ms  support12-loh-G3-0.proxy.aol.com [195.93.34.252]

  3   340 ms   538 ms   339 ms  access12-loh-P3-3.router.aol.com [195.93.36.125]

  4   298 ms   287 ms  1680 ms  pop5-loh-P2-0.atdn.net [66.185.146.89]
  5   348 ms   656 ms   301 ms  bb2-loh-P0-3.atdn.net [66.185.146.82]
  6   290 ms   301 ms   301 ms  pop2-loh-P1-0.atdn.net [66.185.136.243]
  7   483 ms   301 ms   288 ms  CandW.atdn.net [66.185.143.94]
  8   301 ms   813 ms  1075 ms  zcr2-ge-2-1-0.Londonlnt.cw.net [166.63.222.146]

  9   751 ms   302 ms   299 ms  bcr2.Thamesside.cw.net [166.63.210.62]
 10   382 ms   957 ms   419 ms  dcr1-loopback.Washington.cw.net [206.24.226.99]

 11   880 ms  1429 ms  1562 ms  bhr1-pos-10-0.Sterling1dc2.cw.net [206.24.238.16
6]
 12   396 ms   380 ms   380 ms  csr12-ve241.Sterling2dc3.cw.net [216.109.66.91]

 13   391 ms  1167 ms   380 ms  csr11-ve241.Sterling2dc3.cw.net [216.109.66.90]

 14   386 ms   379 ms   380 ms  216.109.84.162
 15   381 ms   788 ms   382 ms  216.109.120.190
 16   389 ms   683 ms  1482 ms  w8.dcx.yahoo.com [64.58.76.229]

Trace complete.
```

BIBLIOGRAPHY

- **Data and computer communications 6th edition by William Stallings.**
- **Handbook of data communications and networks by Bill Buchanan.**
- **Internetworking with TCP/IP principles, protocols and architectures 4th edition by Douglas E.comer.**
- **The Essential Guide to Networking by Jim Keogh**