TCP/IP AND INTERNET ADDRESSING

TCP/IP – (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)

TCP/IP is the most common networking protocol suite used in the world, each computer or node connected to the internet has its own 32-bit internet address (IP address) that uniquely identifies each computer from others.

INTERNET ARCHITECTURE

The internet architecture divides protocols into layers, each layer is responsible for a specific communication task. There are four basic layers that correspond with the OSI/RM:

- Network Access Layer
- Internet Layer
- Transport Layer
- Application Layer

OSI/RM AND INTERNET ARCHITECTURE LAYERS

OSI/RM Layer	Internet Architecture
Application	**APPLICATION**
Presentation	
Session	**TRANSPORT**
Transport	
Network	**INTERNET**
Data link	**NETWORK ACCESS**
Physical	

NETWORK ACCESS LAYER (*Data Link and Physical Layers*)

The network access layer corresponds to the Data link and Physical layers of the OSI and accepts higher layer datagrams and transmits them over the attached network, it handles all of the hardware details interfacing with network media, this layer consists of:

- Operating Systems device drivers.
- Corresponding NIC
- Physical connections

INTERNET LAYER (*Network layer*)

Corresponds to the network layer, is responsible for addressing and packet routing on TCP/IP networks, when a packet is passed down from the transport layer, it is encapsulated into an IP packet. The IP packet contains the routing information.

INTERNET LAYER PROTOCOLS

Internet Protocol	**IP**
Internet Control Message Protocol	**ICMP**
Internet Group Management Protocol	**IGMP**
Address Resolution Protocol	**ARP**
Reverse Address Resolution Protocol	**RARP**

TRANSPORT LAYER (*Transport and Session Layers*)

Corresponds to the transport and session layers, accepts application layer data (PDU's), provides the control of information flow between hosts using TCP and UDP.

TRANSPORT LAYER PROTOCOLS

Transmission Control Protocol	**TCP**
User Datagram Protocol	**UDP**

APPLICATION LAYER (*Presentation and Application Layers*)

Corresponds to the *Presentation and Application* layers, also known as the ***process layer***, interacts with the transport layer.

APPLICATION LAYER PROTOCOLS

Telnet	
File Transfer Protocol	**FTP**
Simple Mail Transfer Protocol	**SMTP**
Simple Network Management Protocol	**SNMP**

REQUEST FOR COMMENTS:

Request for comments are documents detailing information about protocols and standards, the higher the number, the more recent it is. STD 1 is known as (STD 0001) and is a live document since it is being continually updated.

PROTOCOL STATES

Before a protocol can become a standard it must pass through four maturity protocol states: Experimental, proposed, draft and finally standard, when it is accepted. The protocol must be recommended by the **IESG** (*Internet Engineering Steering Group*) of the **IEFT** (*Internet Engineering Task Force*).

MATURITY STAGES OF PROTOCOLS:

- **EXPERIMENTAL**
- **PROPOSED**
- **DRAFT**
- **STANDARD**

OTHER PROTOCOL STATES INCLUDE:

- **HISTORIC** - Legacy protocols or one that never made the grade!!
- **INFORMATIONAL –** Protocols developed outside the IESG/IETF.

PROTOCOLS BY LAYER IN THE INTERNET ARCHITECTURE:

APPLICATION	TRANSPORT	INTERNET	NETWORK ACCESS
HTTP	TCP	IP	ETHERNET
FTP	UDP	ICMP	TOKEN RING
TFPT		IGMP	FDDI
NNTP		ARP	ATM
SMTP		RARP	
SNMP			
DNS			
BOOTP			
DHCP			

COMMON PROTOCOLS:

INTERNET PROTOCOL (IP)

Internet protocol is responsible for IP addressing and performs routing functions, It selects a path for the data to travel to the destination IP address, it operates at the network layer of the OSI.

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP is the troubleshooting protocol for TCP/IP networks, it is used for error reporting from hosts and gateways.

INTERNET GROUP MESSAGE PROTOCOL (IGMP)

IGMP is used for multicasting, it allows nodes to join (multicast-groups) and maintain membership in the group.

ADDRESS RESOLUTION PROTOCOL (ARP)

ARP translates IP addresses into MAC addresses.

REVERSE ADDRESS RESOLUTION PROTOCOL (RARP)

Translates MAC addresses, into IP addresses.

TRANSMISSION CONTROL PROTOCOL (TCP)

Provides session management between source and destination systems, ensures the reliable delivery of data, makes sure it is in the correct sequence and that no duplicate data is sent. TCP guarantee's delivery. Uses a handshaking process before commencing a session.

User Datagram Protocol (UDP)

Provides a datagram form of communication, sends packets with the best effort mode of delivery, does not guarantee delivery and has no flow control. No handshaking takes place to establish a reliable session.

Hypertext Transfer Protocol (HTTP)

Used to transmit HTML information (web pages) across the internet.

File Transfer Protocol (FTP)

Transfers files between computers on a network, FTP uses TCP.

Trivial File Transfer Protocol (TFPT)

Used for diskless workstations, TFPT uses UDP.

Telnet

Terminal emulation. A protocol that allows a user to remotely access another computer, as if he was at its terminal.

Network News Transfer Protocol (NNTP)

Allows sites to exchange news data, network news groups use NNTP.

Gopher

An old protocol that enabled uses to find resources on the internet, now replaced by web servers.

Simple Mail Transfer Protocol (SMTP)

Protocol used to send email messages.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Used for the management and administration of TCP/IP networks.

DOMAIN NAME SYSTEM (DNS)

Translates web address into IP addresses, FQDN (*Fully Qualified Domain Names*) are addresses that are registered.

BOOTSTRAP (BOOTP)

An alternative to RARP, enables diskless workstations, routers, etc to determine their IP at startup.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Assigns dynamic IP addresses to nodes and routers and servers at startup.

SESSION INITIATION PROTOCOL (SIP)

Initiates and manages sessions between two computers, it is responsible for setup, any modifications during the session and also session teardown or closure. Allows skype users to make calls on their PC's, these calls are made over a ***Soft Phone***, as it is the software acting like a phone, it can also apply to PDA's etc.

H.323

Provides consistency in audio, video and packet data transmissions, works over IP networks and defines the components, procedures, protocols and services required for multimedia communication over LANs and WANs.

DEMULTIPLEXING

Demultiplexing is the method a destination computer uses to process an incoming packet.

ROUTING

Routers forward packets from one physical network to another via the IP address in the packet, they choose the path over which to send packets and operate at layer 3 or the Network layer of the OSI/RM or the internet layer of the architecture layer.

DIRECT ROUTING

Direct routing is where computers on the same network are able to send packets without the need for a router. In an IEEE802.3 Ethernet TCP/IP network, the sending entity encapsulates the packet in an Ethernet frame, binds the destination address to an Ethernet address and then transmits the frame directly to its destination. ARP is an example.

The destination system is on the same physical network if the network portions of the source and destination addresses are the same. Direct routing actually has nothing on do with a router and one is not needed.

INDIRECT ROUTING

If two computers are on remote networks (not the same network or segment), they require a router for packet delivery, this is indirect routing, opposite to direct routing.

ROUTING PROCESS

Two processes:

- The host must know which router to use for the destination address, the router is the default gateway, the default gateway is the IP address of your local network.
- The router must know where to send the packet, the destination is determined by the routers routing information table.

ROUTING INFORMATION TABLE

The routing information table is a database maintained by a router. The table contains the location of all networks in relation to the routers location. When a packet arrives at the router, it examines the packets destination network and checks it against its table, it then determines where to send the packet and to which part of the network, or which other router to forward on the packet to its destination node.

Each time it sends a packet to another router, it is called a ***hop***.

DYNAMIC ROUTING AND STATIC ROUTING

Static routers have routing tables that require manual configuration and updating, they may not be able to forward a packet if its destination network has not been manually configured or entered into its table.

Dynamic routing involves routers that have a dynamic routing table that is updated automatically. These routers communicate with other dynamic routers to calculate routes automatically using protocols such as RIP and OSPF. When a route changes, the routers automatically update their tables.

ROUTING PROTOCOLS

INTERIOR ROUTING PROTOCOLS – Are used within an organisational network, **RIP, RIPv2** and **OSPF**.

EXTERIOR ROUTING PROTOCOLS – Used outside an organisational network, *Exterior Gateway Protocol* (**EGP**) and *Border Gateway Protocol* (**BGP**)

ROUTING INFORMATION PROTOCOL (RIP)

RIP is commonly implemented on small to medium LANs, it only maintains the best route to destination, old route information is replaced by new code every time the network topology changes. RIP selects routes based on the lowest hop count, or the closest path between source and destination nodes.RIPv2 is more efficient that RIPv1.

OPEN SHORTEST PATH FIRST (OPSF)

IN OPSF no emphasis is placed upon factors like available bandwidth, multiple connections or security, it is an interior routing gateway protocol.

OPSF includes the following:

- **Routing information table updates** – reduces traffic saves bandwidth.
- **Service routing** - multiple routes to a destination.
- **Load balancing** - All routes cost the same, even distribution of traffic over all routes.
- **Network areas** – Ability to partition network areas.
- **Authenticated exchanges** – All exchanges are authenticated using OSPF.

PORT NUMBERS

When a packet arrives at the destination node, it is passed to the transport layer which determines the packets port number. TCP and UDP packets both contain source and destination port numbers in their packet headers. Port numbers are assigned by ICANN.

ICANN (*Internet Corporation for Assigned Names and Numbers*)

Port numbers fall under three primary categories:

- **WELL KNOWN** – Between (0 and 1023)
- **REGISTERED** – Between (1024 and 49151)
- **DYNAMIC** – Between (49152 and 65535)

Well known are controlled by ICANN and require administrative permissions , registered are also known as ephemeral do not require admin permissions, dynamic are private port numbers and are not registered or controlled by ICANN.

INTERNET ADDRESSING

ICANN issues all internet addresses ensuring each user has a unique IP address. Internet addresses contain a network portion and a host portion.

Network portion – 208.157.24.*111 –host portion*

The network portion is 208.157.24 *.111 is the host portion*

An IP address is a 32 bit dotted decimal, each field has 8bits or 1 byte and can range between 0 – 255.

SUBNET MASK.

Each system in a TCP/IP network must be configured with an IP address and a subnet mask. The subnet mask determines which part of the address is used as the network address and which part is used to identify the host.

Subnet mask: 255.255.255.0

It works very much like addressing a letter, the network part would be your city or state, and the host part would be your house and street number.

Subnet mask serve the following purposes:

- Distinguish the network and host portions of an IP address.
- Specifying whether an address is local or remote.

The subnet mask tells a system which bits of the IP address are the network or subnetwork and which bits are the host.

Subnet masks also specify whether a destination address is local or remote, it is used to ‘mask’ the network portions of the address so only the host part remains. This allows a computer to determine whether a destination address is intended for a computer on the same local network, or a remote location.

ANDING

A subnet mask indentifies whether the destination address is local or remote through a process called ANDing. The network portion of an IP address can be determined by using the ***Boolean AND*** operation with the internet address and the subnet mask.

When a computer starts up it uses the ANDing function with its local IP address and subnet mask, when it sends data to a destination address, it uses the ANDing function again with the destination address and subnet mask. If these values match the initial ANDing result, the data is destined for the local network, if it does not match, it is destined for a remote host.

When an IP address is broken down into binary notation, which portions of the address equal all 1's determines whether it is a local or remote address.

If an IP address was: 131.226.85.1

and the subnet mask is 255.255.0.0

Binary = 10000011 11100010 01010101 00000001

Local subnet mask = 11111111 11111111 00000000 00000000

If the ANDing result is different to that of the local network, a router will be used, it is the same, a router will not be used. If the data is sent locally, there is no need for a router.

If the results were different, the data would be sent to a remote location and obviously a router would be used.

1 and 1 =1, anything else is zero.

INTERNET ADDRESS CLASSES

There are **3,720, 314, 628** possible IP addresses, to give them structure IP address classes are divided into five classes based on the first byte of the address, the five classes range from **A, B, C, D,** and **E**.

IP ADDRESS CLASSES

Address Class	IP Address Range
Class A	0.0.0.0 to **127**.255.255.255
Class B	**128**.0.0.0 to **191**.255.255.255
Class C	**192**.0.0.0 to **223**.255.255.255
Class D	**224**.0.0.0 to **239**.255.255.255
Class E	**240**.0.0.0 to **247**.255.255.255

CLASS A (FIRST BYTE) 0 TO 127

Class A addresses use the first byte for the network portion and the last three for the host portion. The first byte can range from 0 – 126, 127 is a loopback address.

0.0.0.0 to 126.255.255.255

Class A has the potential for 126 networks with 16,777, 214 host on each.

CLASS B (FIRST TWO BYTES) 128 TO 191

Class B addresses use the first two bytes for the network portion and the last two bytes for the host portion, they range from 128 to 191.

128.0.0.0 to 191.255.255.255

CLASS C (FIRST THREE BYTES) 192 TO 223

Class C use the first three bytes as the network portion and the last byte for the host portion. They range from:

192.0.0.0 to 223.255.255.255

CLASS D (ALL FOUR BYTES) 224 TO 239

Class D addresses are used for multicasting, they use all four bytes as the network address and there is no host address portion. They range from:

224 to 239 for all four bytes. (all network portions)

CLASS E (RESERVED FOR FUTURE USE) 240 TO 247.

DEFAULT SUBNET MASKS FOR IP ADDRESS CLASSES

The default subnet mask is the simplest of all, by default each b-bit field is turned on(255 –all binary ones) or off (0- all binary zeros), depending on the address class (A, B or C). Class D and E have no hosts and therefore do not require subnet masks.

STANDARD IP CLASSES AND SUBNET MASKS

Class	Addresses Range	Standard Subnet Mask
Class A	1.0.0.0 to 126.0.0.0	255.0.0.0
Class B	128.0.0.0 to 191.0.0.0	255.255.0.0
Class C	192.0.0.0 to 233.0.0.0	255.255.255.0

PRIVATE IP ADDRESSES

Many organisations do not use standard IP address ranges and to save money instead use private IP addresses. These address are usually used within the enterprise when nodes do not require internet access.

Private IP address ranges cannot be sent across routers, only internal company routers. Internet and external routers are configured to ignore and discard any packets containing private IP address ranges. This prevents network leakage.

PRIVATE IP ADDRESS

Class	Private IP Address Range	Subnet Mask	CIDR Notation
Class A	vv10.0.0.0 to 10.255.255.255	255.0.0.0	10/18
Class B	172.16.0.0 to 172.31.255.255	255.254.0.0	172.16/12
Class C	192.168.0.0 to 192.168.255.255	255.255.0.0	192.168/16

Class B and C do not use standard subnet masks.

PRIVATE IP ADDRESSES AND NETWORK ADDRESS TRANSLATION

For addresses in this range to be sent across the network they require the use of **NAT** (*Network Address Translation*), NAT allows the router or firewall or (appliance) to reconfigure the packet and replace the private IP with a routable one for the internet. Proxy servers which work at the application layer of the OSI can also perform this function.

The reasons for having private IP Addresses in the enterprise include:

- Conservers unique IP addresses (IPv4)
- Gives the enterprise greater flexibility for expansion
- Prevents IP clashes for external connectivity

CLASSLESS INTERDOMAIN ROUTING (CIDR)

IP addresses are no longer assigned based on classes, they are assigned according to specific ranges, each range is assigned a specific subnet mask presented in Classless Interdomain Routing notation, or CIDR notation.

CIDR notation uses the following format:

Address block/prefix

In this format the address block is given and a number is given for the prefix. The prefix designates the number of bits used by the subnet mask, as an example the following ranges would be noted as follows:

55.66.77.88 to 55.66.88.99 = 55.66.77.88-55.66.88/24

In this notation ICANN is able to assign a custom subnet mask to any range of addresses, this also allows conservation of IP addresses because they can assign a specific number of addresses instead of ranges.

INTERNET PROTOCOL VERSION 6 (IPV6)

IPv6 uses a 128-bit addressing scheme which allows for approximately 340 undecillion addresses, (a significantly larger address pool than IPv4) it fixes the current shortcomings with IPv4 and requires less admin and overhead and reduces routing table problems.

The shortcomings of IPv4 are follows:

- Limited address space (4.2 billion addresses)
- Lack of security -native encryption and authentication mechanisms
- Speed problems – network routers have to disassemble transmissions
- Configuration problems

IPv6 is far less dependent than IPv4 on routers which also reduces the burden on routers, this increases network efficiency.

System Configuration and IP Addressing

The administrator can configure systems to IP addresses in two ways:

Static Address Assignment – the administrator manually enters IP address information, or manually assigns addresses.

Automatic Address Assignment-Clients are configured to automatically obtain IP address information for a DHCP server, clients can also self-assign an APIPA in the absence of a DHCP server.

Loopback Address

The local loopback address is used for troubleshooting and is a class A address which ranges from 127.0.0.0 to 127.255.255.255. It is used for testing and functionality by using the **PING** command (*Packet Internet Groper).*

For UNIX and Windows systems, the loopback address is listed in the host file and is typically 127.0.0.1 with the assigned name local host. The host file contains mappings of IP addresses to host names. This file can be accessed by: C drive\Windows\System32\Drivers\etc\hosts.

Broadcast Address

Broadcast addresses send messages to all network hosts, this kind of addressing is used to send messages to only destination addresses, so the host portion of then IP address determines where the packets are sent.

There are four types of broadcast address types:

- **Limited Broadcast** (used at computer start-up, address is 255.255.255.255 and request a dynamic address from a DHCP server.
- **Net-directed broadcast** (netid.255.255.255), broadcast to all host
- **Subnet-directed broadcast** (only one subnet gets messages)
- **All-subnets-directed broadcast** (all subnets get broadcast).

NETWORK AND SPECIAL-CASE SOURCE ADDRESSES

The special-case source IP address of a computer is all zeros (0.0.0.0), when it initialises at start-up, it request an IP address from a DHCP server or BOOTP server, which then assigns it an address.

The special-case source address can also specify a host on the network during initialisation, the network portion of an address might be all zeros but the host portion might be ones: 0.0.0.11

NORMAL TCP/IP WORKSTATION CONFIGURATION

A network host must have at least an IP address and a subnet mask to communicate on a network. WAN communication requires at least an IP address, a subnet mask and a default gateway.

The basic configuration parameters for a workstation are:

- IP address
- Subnet mask (determines the network and host portions of the address, also whether a destination address is local or remote)
- Default gateway (modem/router)
- DHCP client

TCP/IP SERVICES

Service	Function
DNS	Domain Name System, a name resolution service, resolves domain names to IP addresses, resolves host names to IP addresses and can also resolve IP addresses to host names.
DHCP	Automatic assignment of IP address and subnet mask at initialisation or computer start-up, may also be sent DNS server IP address.
APIPA	Client self assignment of private IP address if it fails to receive one from a DHCP server, if range begins with 169.254 it is APIPA.

THE HOST FILE

The host file maps DNS host names with IP addresses, it is installed whenever you install the TCP/IP suite or stack. The files in the host file are editable. The host file resides under ***the System32/Drivers/etc*** hosts file under the Windows directory.

DNS CONFIGURATIONS

HOST NAME – the name of your computer on the network

DOMAIN NAME – a domain to which your computer belongs

DNS SERVER – the DNS servers must be identified to provide the SND service to all computers on the network.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

DHCP automatically assigns IP addresses to clients in a TCP/IP environment when they initialise, it also assigns the subnet mask and the default gateway and the DNS server information if required.

DHCP assigns these addresses on a lease basis, usually the leased IP address will expire at some point so it can then be assigned to another node. If you have trouble connecting in a DHCP environment, you can renew the lease to request new TCP/IP credentials. The syntax is:

ipconfig/ release and once it is released, type ***ipconfig/ renew***.

The DHCP server has a pool of IP addresses which it can assign to computers on the network, this pool consists of a range of IP addresses that were input by the network administrator in to the DHCP server.

In this kind of environment clients are DHCP clients and the DHCP servers operate under a dynamic addressing scheme.

RECONFIGURING A COMPUTER WITH A RESERVED IP ADDRESS

1. Click Start/Control Panel/Network and Sharing Centre
2. Right-click Local Area Connection
3. Select Properties
4. Select the Protocol (IPv4/IPv6)
5. Click Properties for that Protocol
6. Click Use the following IP Address
7. Enter the appropriate IP address and Subnet Mask
8. Click OK and Close

NETWORK DIAGNOSTIC TOOLS

TCP/IP has the following tools for troubleshooting:

- *Ping*
- *Tracert and Traceroute*
- *Route*
- *Netstat*
- *Ipconfig and ifconfig*
- *Arp*
- *Network analysers*

THE PING COMMAND

Packet Internet Groper or 'PING' test's connectivity between source and destination systems, you can either ping and IP address or a host name.

The ping command uses two ICMP types:

echo request (ICMP 8) and ***echo reply (ICMP 0)***

The ping returns a result that either proves connectivity or it can also show that DNS is working by pinging a host name.

It is common practise to first ping an IP address to test connectivity, then ping a host name to ensure DNS is working properly.

To ping an IP address open the command prompt and type ‘ping’ then the IP address or host name, as below:

Because a reply was received, a connection exists between the node sending the request and the computer with the IP address of 10.0.0.138.

You can stop the ping request by pressing : **CTRL + C**

If you can ping the host by IP address but not by host name, a problem exist with name resolution, if you cannot ping the host by either method, a connectivity problem exists.

You can test your local connectivity by using the loopback ping which is ping 127.0.0.1, if it returns a successful ping, you have good connectivity.

Additional ping commands:

- Ping –n - specifies the number of echo packets (default is 4)
- Ping –i - specifies TTL (Time To Live)
- Ping –l - Specifies buffer size (default is 32)
- Ping –a - Resolves an IP address to a host name

It may be impossible to ping systems outside the enterprise since many firewalls will have ICMP disabled, ICMP is a security risk if left to operate.

TRACERT AND TRACEROUTE COMMANDS

The traceroute utility can determine the path between the source and destination systems, it also provides information on roundtrip propagation time between each router and the source system.

When problems located far from your local network are causing you connectivity problems outside your network, you can use the tracert command to locate such failures. Pressing CTRL + C halts tracert.

Tracert is syntax for ***Windows***

Traceroute is syntax for ***Linux/Unix***

The output shows the sequence of routers the packets cross and the route they take, it also shows the number of hops, which is 14. Usually 30 hops is the maximum.

The tracert tries each path three times and reports a round trip time for each stage.

ROUTE COMMAND

The route command is used to display and manually configure the routes in a routing table, it is available on many operating systems including Linux and Windows Vista and Server 2008. This command also provides additional options that allow you to add and delete routes.

NETSTAT COMMAND

The netstat (network statistics) command works in all TCP/IP operating systems, it displays the contents of network related data structures including the state of sockets. A ***socket*** is the end point of a connection (either end) which includes the TCP or UDP port used and the IP address, used for communication between a client and a server.

The netstat command also displays information about packets processed by your system on the network. It displays all the active connections currently running on a system.

There are several switches for netstat:

netstat –a displays the current connections and listening ports.

IPCONFIG COMMAND

The ipconfig (*internet protocol configuration*) command displays the Windows IP configuration, by default this command displays only the IP address, subnet mask and default gateway.

The ipconfig command comes with several switches or options, one very commonly used is the ipconfig/all command which provides extra information related to the computers network and NIC .

The ipconfig command can also release and renew lease obtained from a DHCP server, the syntax for lease release and renewal is:

Ipconfig/release

Ipconfig/renew

IFCONFIG COMMAND

The ifconfig (interface configuration) command is the Linux/UNIX equivalent of the ipconfig command, it displays the hardware and software configurations of the NIC.

IFCONFIG COMMAN

D

ARP COMMAND

Arp resolves software (IP addresses) to hardware (MAC) address, it displays the MAC address of systems on the network. Common syntax is: ***arp –a***, displays physical addresses, ***arp –d IP address*** deletes IP's

NETWORK ANALYSERS

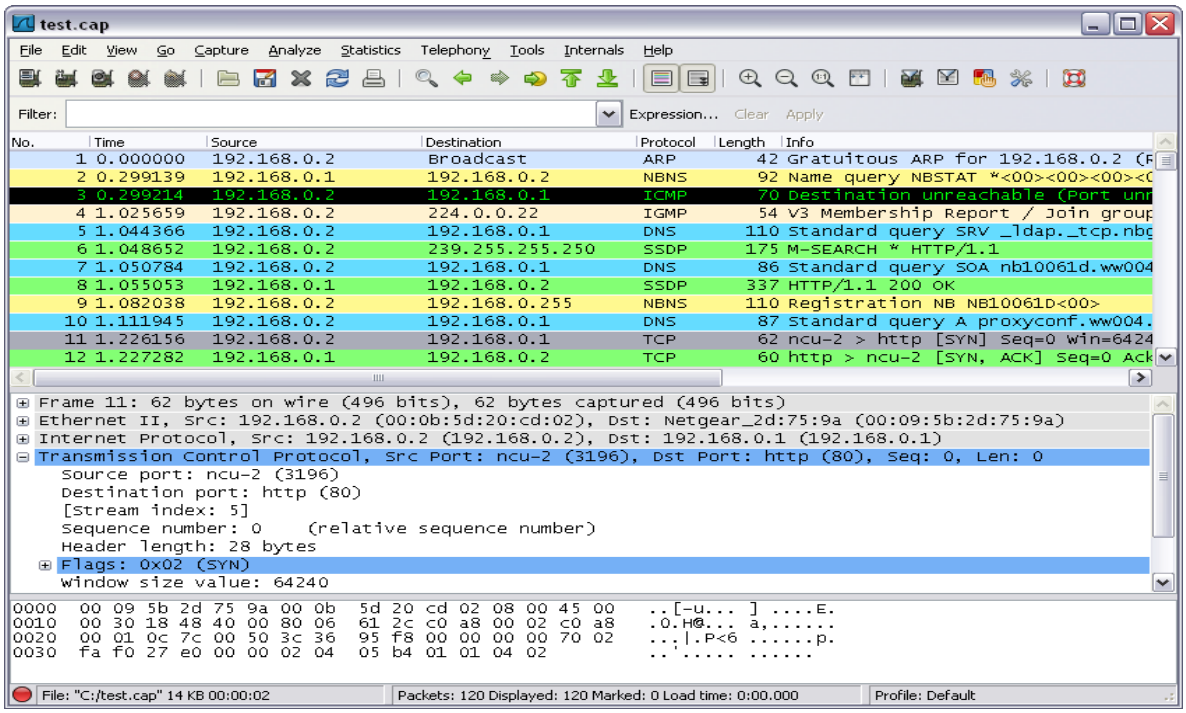
Network analysers allow administrators to troubleshoot and manage networks, they are also known as 'packet sniffers'. Data or packets are captured and you can then view its contents including the Ethernet header that has the source and destination address of both nodes.

If a computer on the network is sending error messages, you can identify it and determine the problem, a common network analyser is wireshark, from www.wireshark.org. Hackers and attackers also use wireshark.

Network analysers help troubleshoot a network by:

- **Monitoring network traffic to identify network trends** - Baselines and trends can be created and compared to traffic flow.
- **Identifying network problems and sending alert messages**
- **Testing network connections**

WIREHSHARK



TROUBLESHOOTING CONSIDERATIONS

DNS NAME RESOLUTION:

Have you entered the correct address for a DNS server, if you can ping the IP but not the host name, it is a DNS problem.

HOST FILE CONFIGURATION:

Is the host file up-to-date and accurate, many systemts check this file for name resolution before communicating with a DNS server.

STATIC AND DYNAMIC ADDRESSING:

Determine how host are configured to obtain IP addresses, try and keep all host configured with either manual configuration – static addressing,(not recommended in enterprise environments) or have them use a DHCP server or APIPA.

DEFAULT GATEWAY AND SUBNET MASK:

Be sure you have specified the correct IP address and subnet mask, make sure the default gateway is set with the correct IP address. The subnet mask helps determine whether an address is local or remote.

Use the network diagnostic tools to determine whether the problem exists on the client side or the server side, if you cannot ping another computer on your local network, it is probably a client-side connectivity problem.

If you can ping the default gateway but cannot ping an address external to the router or (default gateway), there might be a problem with the router – check the router settings.

Always ensure the correct username and password has been entered.

Always check cables and connectors first!!

ADSL AND CABLE MODEM TROUBLESHOOTING

Most home-based modems are intended for a single system, you can attach others systems via means of a router, it can be:

- Windows or Linux system with two NICs hosting network service to another computer, Windows uses ***Internet Connection and Sharing*** and ***Linux uses iptables***.
- A dedicated router or firewall

You require a cross-over cable to connect a modem to a router. Always check for basic connectivity first, ping a local IP and then try to ping a host name. You want to rule out any problems with DNS.

Ping the default gateway, use a different computer or connect one directly to the gateway, this provides information about if the problem exists with the gateway itself.

Check all cables and connectors, including power cables!

It is also a good idea before you do anything to power down all devices and then power up and boot up the system, sometimes that's all it takes.

Power down the modem as well and allow it time to re-initialise and check for lights and activity, make sure the DSL light is on if it's a DSL modem, ensure the lights for each port are working (indicating activity) if a cable is plugged i and attached to a computer. Swap out cables also.

Check with the ISP as the problem may be external to your network and at the ISP end of things, ring them if in doubt.

SYNTAX FOR WINDOWS AND LINUX

Windows Syntax	Linux Syntax
ping	
tracert	traceroute
route	
Ipconfig	Ifconfig
netstat	
arp	

PROTOCOLS AND LAYERS

APPLICATION	TRANSPORT	INTERNET	NETWORK ACCESS
HTTP	TCP	IP	ETHERNET
FTP	UDP	ICMP	TOKEN RING
TFPT		IGMP	FDDI
NNTP		ARP	ATM
SMTP		RARP	
SNMP			
DNS			
BOOTP			
DHCP			
SIP			