TCP – transmission control protocol – connection orientated

UDP – user datagram protocol - connectionless

IP – Internet Protocol

Hostname – c:\> hostname <enter> (netbios)

## Routing – Public vs Private

**Private IP Address Ranges – Non-Routable**

Class A - 10.0.0.0 to 10.255.255.255 / Subnet 255.0.0.0 / CIDR 8

Class B – 172.16.0.0 to 172.31.255.255 / Subnet 255.255.0.0 / CIDR 16

Class C – 192.168.0.0 to 192.168.255.255 / Subnet 255.255.255.0 / CIDR 24

192.168.1.1 IP -> host

255.255.255.0 -> subnet

AND

8 7 6 5 4 3 2 1

128 64 32 16 8 4 2 1

1 1 0 0 0 0 0 0 = 192

1 1 1 1 1 1 1 1 = 255

192.168.1.0 => network ID

192.168.0.1 -> another host

255.255.255.0 -> the another’s subnet

AND

192.168.0.0 => another network ID

They are in different subnets (LANs) thus they would need a router in order to communicate

**Special Ranges**

Class D – 224.0.0.0 (Multicast)

Class E – 240.0.0.0 (Broadcast)

Loopback/Localhost – 127.0.0.0

## Other Related Protocol

DNS (port 53) – Domain Naming System – FQDN to IP and visa versa

MAC – 6 hex values separated (48 bit) – or colon (first 3 UOI, last ULANMAC address)

ARP – Address resolution protocol – maps IP to MAC address and visa versa

ICMP – Internet control & messaging protocol – ping / tracert / route print

SMTP (port 25/587) - Simple Mail Transfer Protocol (email client to email server & between servers)

POP3 (port 110) - Post Office Protocol 3 (download email from email server to email client)

IMAP4 (port 143) - Internet Mail Access Protocol 4 (manage email on email server)

SNMP (port 161/162) - Simple Network Management Protocol (manage network intelligent devices)

HTTP (port 80) - Hypertext Transfer Protocol (transport html related traffic from server)

HTTPS (port 443) - Hypertext Transfer Protocol Secure (uses SSL/TLS)

FTP (port 20/21 - TFTP 69) - File Transfer Protocol (file transfer in the clear/unencrypted)

SSH (port 22) - Secure Shell (cryptographically enhanced remote terminal)

Telnet (port 23) – Remote shell to service

DHCP (port 67/68 BOOTP) - Dynamic Host Configuration Protocol (D.O.R.A.D.R.IN – BOOTP)

DHCPv6 (port 546/547)

NTP (port 123) - Network Time Protocol (important to avoid time-skew, 5min threshold on AD)

IKE (port 500) - Internet Key Exchange (certificate-based authentication – Windows)

RPC (port 530) - Remote Procedure Call

LDAP (port 389/636) - Lightweight Directory Access Protocol (Windows AD)

## Commands for Diagnostics & Maintenance

Ipconfig /all

Ping 127.0.0.1

Ping (in general)

Tracert www.google.co.za

Route print

Arp -a

Netstat

Nslookup