

PORTS AND PROTOCOLS

USEFUL PORTS

APPLICATION/PROTOCOL	TCP/UDP	PORT NUMBER
FTP File Transfer Protocol	TCP	20/21
TELNET	TCP	23
SSH Secure Shell	TCP	22
DNS Domain Naming Service	TCP/UDP	53
DHCP Dynamic Host Configuration Protocol	UDP	67/68
TFTP Trivial FTP	UDP	69
HTTP Hypertext Transfer Protocol	TCP	80
HTTPS HTTP Secure	TCP	443
SMTP Simple Mail Transport Protocol	TCP	25
NetBIOS	TCP	137, 138, 139
LDAP Lightweight Directory Access Protocol	TCP	389
Secure LDAP	TCP	636
RDP Remote Desktop Protocol	TCP	3389
NTP Network Time Protocol	UDP	123
POP3 Post Office Protocol 3	TCP	110
IMAP4 Internet Mail Access Protocol 4	TCP	143
SNMP Simple Network Management Protocol	UDP	161
Kerberos	UDP/TCP	88

USEFUL APPLICATION PROTOCOLS

DNS – Domain Naming Service/System. Resolves FQDN to IP Address (and reverse)

ARP – Address Resolution Protocol. Resolves IP addresses to MAC addresses

RARP – Reverse ARP. Resolves MAC addresses to IP addresses

DHCP – Issues IP Addresses to DHCP Clients

(APIPA – 169.254.x.x /16 – Automatic Private IP Addressing – DHCP Client self assigns if no DHCP server is available)

TELNET – Terminal Emulation. Remote connection (insecure)

SSH – Secure Shell – Used to secure connections:

- SFTP
- SC
- SCP

SSL/TLS – Secure Socket Layer/Transport Layer Security – Used to authenticate and secure connections:

- HTTPS
- FTPS
- SSTP (VPN)

SNMP – Simple Network Management Protocol – Used to identify and log device errors and conditions

ICMP – Internet Control Message Protocol – Used to swap control information between systems for maintenance

- PING
- Tracert
- PathPing

Kerberos – Authentication and Authorization system which uses tickets issued by the Key Distribution Center (KDC)

IGMP – Internet Group Management Protocol – used as a communication protocol for multicast messages and information