

## Introduction

IP, the Internet Protocol, has its roots back in the 1960s and was originally developed as part of a research project funded by the Defence Advanced Research Projects Agency (DARPA), part of the US Department of Defence (DoD). Today, IP is well known as being the world's most widely used networking protocol.

Traditionally IP has been used in the support of transporting data. However due to a whole host of driving forces, IP is now seen as the protocol of today and the future to support not just data but multimedia traffic including voice and video. A term commonly applied to this bringing together of all communication needs into the one network is convergence.

This course looks at IP and its associated protocols in terms of the technology as well as how it is applied to real-life applications. In addition, we discuss many of the issues that need to be addressed when using and considering using IP.

## Live Equipment, Practical Exercises and Reviews

It is very important to us at HN Networks that the students on our courses receive training that allows them to learn most effectively. In order to achieve this, we include exercises and end-of-section and end-of-day review questionnaires within the course. The goal of the reviews is to provide a mechanism to reinforce the material covered during the course rather than simply testing how much a student has taken in on the first pass.

Live equipment, including various items of equipment including routers, servers and firewalls, is used to help consolidate the subjects learnt and give the students practical as well as theoretical skills.

## Who should attend the course?

This course is aimed at individuals who wish to develop a solid understanding of all aspects of IP technology. It will be beneficial for network managers, technicians, designers and consultants who are involved in supporting, managing, designing or implementing IP networks. A general understanding of data communication principles is recommended.

## Course Agenda

The following is an outline of the sections included in the course:

1. [Introduction to IP](#)
2. [The IP Layer](#)
3. [IP Support Protocols](#)
4. [Internet Control Message Protocol \(ICMP\)](#)
5. [Transport Layer Protocols](#)
6. [Application Layer Protocols](#)
7. [Routing with IP](#)
8. [IP Version 6 \(IPv6\)](#)
9. [Security and IP](#)
10. [Quality of Service \(QoS\) and IP](#)
11. [IP and Multi Protocol Label Switching \(MPLS\)](#)
12. [Voice over IP](#)

## Course Length

Three days.

## Course Section Descriptions

### 1 Introduction to IP

#### Protocol Concepts

- A brief overview of the layered approach to networking is covered. We look at the OSI model and the TCP/IP model and give a rationale for their use and an example of the TCP/IP model in action.

#### What is IP and where did it come from?

- IP stands for Internet Protocol, one of the many protocols in the commonly known TCP/IP suite.
- IP was developed as part of a research project funded by the Defence Advanced Research Projects Agency (DARPA), part of the Department of Defence (DoD) in the USA. This is why it is sometimes referred to as DoD IP. ARPANet (the forerunner of the Internet) was set up to link military CPUs together. The design was published in 1974 and the DoD eventually accepted it in 1979.

#### IP carried across various different types of network

- IP over Ethernet – We look at the two different Ethernet frame types including Ethernet 2 and IEEE 802.3 and how both can carry IP. We see that use of Ethernet 2 is, by far, most common.
- IP over Point-to-point Protocol (PPP) (optional)
- IP over Token Ring using IEEE 802.2 and Sub Network Access Protocol (SNAP) (optional)
- IP over Frame Relay (optional)
- IP over Asynchronous Transfer Mode (ATM) (optional)

### 2 The IP Layer

This section discusses the IP header with emphasis placed on IP addressing mechanisms. Extensive use of the live equipment will be made to demonstrate the subjects being explained. Exercises are used to further consolidate the students' knowledge.

- Introduction to the Internet Protocol (IP)
- OSI layer 3 functions
  - Path selection (routing), interaction with layer 2, network layer addressing, routing protocols
- The IP packet header
- IP addressing
  - Dotted decimal notation and binary view
  - Converting between dotted decimal notation and binary
  - Class A, Class B, Class C (Class D and Class E) addresses - The first octet rule
  - Network address masks
  - Converting IP addresses between decimal and binary format
- Subnetting
  - Subnet masks and prefix notation
  - Using the logical AND function to find network/subnet and host numbers
  - Subnetting on an octet boundary
  - Breaking the octet boundary

- How many subnets and hosts per subnet are available?
- Subnet zero and the all-ones subnet
- Calculating subnet number, subnet broadcast address and the range of host addresses in a subnet using binary.
- Calculating subnet number, subnet broadcast address and the range of host addresses in a subnet without using binary.
- IP subnetting guidelines to meet a given design requirement
- Variable Length Subnet Masking - VLSM
- Classless Inter-Domain Routing - CIDR
- Private Addressing
- Network Address Translation (NAT) and Port Address Translation (PAT)
  - Static NAT
  - Dynamic NAT
  - Port Address Translation (PAT)
- Section summary and end-of-section review questions

### **3 IP Support Protocols**

- This section looks at some protocols and other aspects that are used to support the IP protocol.
- Address Resolution Protocol (ARP)
  - How ARP works
  - What does ARP do?
  - Proxy ARP
- Internet Control Message Protocol (ICMP)
- Dynamic Host Configuration Protocol (DHCP)
  - DORA – Discover, Offer, Request, Ack
  - DHCP Renewal, Release and Refusal
  - DHCP Inform 1
  - DHCP Decline and ARP Duplicate Address Test (DAT)
  - DHCP/BOOTP Relay
- Name systems
  - The Hosts file on Windows/UNIX/LINUX systems
  - The Domain Name System
- Section summary and end-of-section review

### **4 Internet Control Message Protocol (ICMP)**

- Internet Control Message Protocol (ICMP)
  - ICMP - Echo request and echo reply
  - ICMP - Destination unreachable

- Network unreachable
- Host unreachable
- Protocol unreachable
- Port unreachable
- Fragmentation needed and DF bit set (Can't fragment)
  - Maximum Transmission Unit (MTU) and Fragmentation
- ICMP - Time exceeded
- ICMP - Redirect
- Section summary and end-of-section review questions

## 5 Transport Layer Protocols

This section examines the host-to-host layer of the TCP/IP model and compares the two protocols that operate at this layer.

- OSI layer 4 functions
- Connection oriented vs connectionless protocols
- Reliable and un-reliable protocols
- The use of port numbers
- Transmission Control Protocol (TCP)
  - The TCP header
  - Connection-opening and closing
  - Segmentation of data and data sequencing
  - Error recovery
  - Flow control using windowing
- User Datagram Protocol (UDP)
  - The UDP header

## 6 Application Layer Protocols

This section looks at some of the more popular application layer protocols.

- Telnet – Virtual terminal operation giving interactive access to remote systems.
- File Transfer Protocol (FTP) – Used to transfer files across an IP network along with extensive facilities for remote functions such as directory manipulation, file deletion etc...
- Trivial File Transfer Protocol (TFTP) – Used to transfer files across an IP network in a very simple fashion (i.e. with limited functionality).
- Simple Mail Transfer Protocol (SMTP) – Electronic Mail achieved simply.
- Post Office Protocol (POP) – A protocol that client e-mail applications use to retrieve mail from a mail server via an IP network such as the Internet.
- HyperText Transfer Protocol (HTTP) – The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

- HyperText Mark-up Language (HTML) – The basic language that provides the formatting capabilities on typical web pages.
- Simple Network Management Protocol (SNMP) – Here we look at the most common protocol used for the management of devices in an IP network.

## 7 Routing with IP

In this section, we deal with the routing function of IP and the devices used to achieve this. Examples of routers will be set up and we will demonstrate how they operate.

- Routing
  - What does a router do
  - Routing tables
  - Static routing and its configuration
  - Summary Route
  - Floating Static Routes and Load Sharing
  - Default routes
- Routing protocols
  - Routed vs. Routing Protocols
  - Dynamic Routing Protocols
  - Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP)
  - Routing Metrics
  - Types of Dynamic Routing Protocol
    - Distance Vector routing protocols
      - Routing Information Protocol (RIP) Version 1
      - RIP Version 2
      - Interior Gateway Routing Protocol (IRGP)
    - Link-State Routing Protocols
      - Open Shortest Path First (OSPF)
      - Integrated Interior System to Interior System (IS-IS)
    - The Internet EGP - Border Gateway Protocol (BGP)
  - Classful and Classless routing
  - Classful and Classless Routing protocols
  - Route summarisation
- Autosummarisation
- Section summary and end-of-section review questions

## 8 IP Version 6 (IPv6)

Here we look at IPv6, the development of a new protocol designed to replace IPv4.

- IPv6 addressing

- Types of IPv6 address
  - Unicast
  - Multicast
  - Anycast
- Types of unicast addresses
  - Global addresses
  - Link local addresses
  - Unique local addresses
  - Special addresses
  - IPv4 compatible addresses
- IPv6 interface identifiers
- IPv6 packet header format
- IPv6 extension headers
- ICMPv6
- Neighbour discovery
- IPv6 autoconfiguration
- DNS enhancements for IPv6

## 9 Security and IP

Rapid development of communications across networks such as the Internet has brought about the need for significant security mechanisms to protect client protocols of IP. This section has a look at what IP security is all about and how it may be achieved.

- Overview of security and IP
- Network Address Translation (NAT) and Port Address Translation (PAT)
- Access lists in routers
- IP Security (IPSec)
- Firewalls

## 10 Quality of Service (QoS) and IP

IP was never really intended for the support of applications that demanded QoS. Today, however, things have changed completely. With the demand for such applications as voice and video over IP (and others), quality of service is an important requirement. There are a number of approaches to delivering QoS and this section explores them.

- Quality of Service with IP
- QoS by using IP over ATM
- Integrated services and the Resource Reservation Protocol (RSVP)
- Differentiated services - Diffserv

## 11 IP and Multi Protocol Label Switching (MPLS)

The original intent of MPLS was to provide a technology that provided the performance of layer 2 switching yet did so based on layer 3 (IP) information. While MPLS does achieve this goal, it is no longer viewed as the only benefit to be gained from MPLS. Other key benefits include the simplicity with which Virtual Private Networks (VPNs) may be implemented as well as the ability to support Quality of Service (QoS) and perform traffic engineering.

- Introduction to MPLS
- MPLS defined
- Routing protocol overview
- Label Distribution Protocol (LDP)
- Traffic engineering with MPLS
- QoS and MPLS
- VPNs and MPLS

## 12 Voice over IP

This section looks at how Voice over IP works as well as looking at some of the issues surrounding it. Live equipment will be used to demonstrate voice over IP operation.

- Why VoIP? A view from a business perspective as to why voice over IP may be an appropriate technology to deploy in many voice related applications
- A look at voice over IP as deployed across the Internet or across a private IP network.
- A look at some of the standards for voice over IP:
  - H.323 and related protocol
  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP) and Megaco / H.248
  - Cisco SCCP (Skinny Call Control Protocol)
- A look at some of the devices that may be used to implement a voice over IP network
  - IP phones
  - Power to the IP phone - powered Ethernet
  - Gateways
  - Call control systems
  - IP enabled voice switches (PBX and public network switches)
- A look at some of the challenges of deploying voice over IP
- Section summary and end-of-section review questions

### End of Training Outline