

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. [Transport Layer Protocols](#)
5. [Application Layer Protocols](#)
6. [Routing with IP](#)
7. [IP Version 6 \(IPv6\)](#)
8. [Security and IP](#)
9. [Quality of Service \(QoS\) and IP](#)
10. [IP and Multi Protocol Label Switching \(MPLS\)](#)
11. [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.
- MAC Addresses
- IP over Token Ring using IEEE 802.2 and Sub Network Access Protocol (SNAP)
- IP over Point-to-point Protocol (PPP), Serial Line IP (SLIP), CSLIP and CPPP
- IP over Frame Relay
- IP over Asynchronous Transfer Mode (ATM)

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.

- IP version 4 addresses have an instantly recognisable format, called dotted decimal notation
- How IP addresses are allocated
- Network and host addressing
- Address classes and the first octet rule
- Public IP address space vs. private IP address space
- Address masks and subnet masks
- Subnetting in detail including subnet guidelines and exercises
- Variable Length Subnet Masking (VLSM)
- Classless Inter-Domain Routing (CIDR)

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)
 - Default Gateway and Default Router
 - Reverse Address Resolution Protocol (RARP)
 - Internet Control Message Protocol (ICMP) provides some of the error handling functionality that is missing from IP itself. The well known Ping facility and the not so well known Traceroute facility will be used to demonstrate the operation of ICMP.
 - Boot Protocol (BOOTP)
 - Dynamic Host Configuration Protocol (DHCP)
 - Domain Name System (DNS) – Including a look at domain naming, zones and name servers, Resource Records and a look at an example of domain name resolution.
-

4 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.

- Transport layer addressing – Ports and Sockets
 - Transmission Control Protocol (TCP) – This is a Transport layer (layer 4) protocol that provides a reliable data delivery service to the higher layer protocols, such as FTP, and other applications that cannot tolerate the loss or corruption of information.
 - User Datagram Protocol (UDP) – This is an unreliable data communications protocol that adds very little overhead to the IP layer. It is used to support applications that themselves probably support their own error correction such as the Trivial File Transfer Protocol (TFTP).
-

5 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.
-

6 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.

Why use routers

- Routing is the process by which two communicating end stations use the optimum path across an internetwork. A router provides the routing function.

The principles of routing

- Routing occurs at the Network layer of the OSI model, or the Internet layer of the TCP/IP model. Here we discuss what a router actually does and how it does it.

Router topology

- What does a router network look like? A variety of scenarios can be catered for using routers, from the very simple to the very complex.

Basic Router Configuration

Here we look at the routing table in more depth and discuss static routing.

Routing Protocols

- Routing vs routed protocols
 - Interior and exterior gateway protocols (IGP and EGP)
 - Routing metrics
 - Routing algorithm types – Distance Vector and Link State protocols
 - Distance Vector routing protocols – Here we look at how distance vector protocols operate and discuss some of the pros and cons of their use.
 - Link State routing protocols – Here we look at how Link State routing protocols operate and compare them to Distance Vector techniques.
 - Routing Information Protocol (RIP) – A look at how RIP works.
 - Open Shortest Path First (OSPF) – A look at how OSPF works.
 - Border Gateway Protocol (BGP) – A look at how BGP works.
-

7 IP Version 6 (IPv6)

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

- Design goals of IPv6
 - IPv6 packet header format
 - IPv6 extension headers
 - IPv6 addressing
 - Aggregatable Global Unicast Address Structure
 - ICMPv6
 - Neighbour discovery and autoconfiguration
 - IPv4 and IPv6 interworking
-

8 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
-

9 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
-

10 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
-

11 Voice over IP

A particularly significant application topic today is that of 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.

- Introduction to Voice over IP
 - A look at H.323 – Terminal equipment, Gatekeepers and Gateways
 - A look at H.225.0 and H.245
 - How speech, DTMF, signalling etc.. is carried in IP packets
 - What are the issues of supporting voice over IP?
 - A look at Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP)
-

End of Training Outline

HN Networks

HN Networks specialises in delivering training in Datacommunication and Telecommunication technologies.

We offer a range of standard training courses as well as providing a customisation service where we will specifically tailor a course to a particular client's needs.

To find out about our current range of training courses, please refer to our web site at:

<http://www.hn-networks.co.uk>

Alternatively, please feel free to call us on +44 (0) 1628 622187 if you wish to discuss your training requirements or simply need further information.