

## Introduction

This course is designed for those who require a good understanding in the areas of Ethernet and TCP/IP technologies. Much emphasis is given to practical demonstrations, reviews, exercises and hands-on practice giving an interesting learning experience and consolidated knowledge of the subjects taught.

## 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, both for demonstrations and hands-on exercises, 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 those wishing to gain a good understanding of the operation, configuration and applications on Ethernet and TCP/IP. While not mandatory, a reasonable understanding of general networking concepts would be helpful.

## Course Agenda

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

1. Layered Communication Models: OSI and TCP/IP Models
2. Ethernet Fundamentals
3. LAN Switching Fundamentals
4. Virtual LANs (VLANs) and Trunking
5. Internet Protocol (IP) Fundamentals
6. Other layer 3 functions:
7. Routing IP, Static Routing and Routing Protocols
8. Network Design and Implementation Hands-on exercises
9. Internet Control Message Protocol (ICMP)
10. Transport Layer Protocols – Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) Fundamentals
11. Application Layer Protocols
12. Firewalls
13. IP and Multi Protocol Label Switching (MPLS)
14. Voice over IP (VoIP)

## Course Length

**Four** days.

## Course Section Descriptions

### 1 Layered Communication Models: OSI and TCP/IP Models

- Introduction to layered models
- Benefits of Using a Layered Model
  - Open Systems Interconnection (OSI) Model
- Application, Presentation, Session, Transport, Network, Datalink, Physical
- TCP/IP Model
  - Application, Transport, Internetwork, Network Interface
  - TCP/IP Data Encapsulation
- OSI vs TCP/IP
- Section summary and end-of-section review questions

### 2 Ethernet Fundamentals

- Introduction to Ethernet
- Ethernet and the OSI model
  - Layer 1 functions
  - Layer 2 functions -
    - Arbitration, Addressing (MAC), Error Detection (FCS), Encapsulated data identification
- The various forms of cabled Ethernet
  - The older Ethernet standards - 10BASE5 (Thick Ethernet) and 10BASE2 (Thin Ethernet) (brief)
  - Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP)
  - Fibre-optic
- UTP forms of Ethernet:
  - 10BASE-T
  - 100BASE-T (Fast Ethernet)
  - 1000BASE-T (Gigabit Ethernet)
  - 10Gigabit Ethernet and beyond
- Ethernet frame formats:
  - Ethernet V2
  - IEEE 802.3
  - Sub Network Access Protocol (SNAP)
- Ethernet addresses - The MAC address - Physical/Unicast, Multicast and Broadcast
- Carrier Sense Multiple Access with Collision Detect (CSMA/CD)
- Performance limitations as a result of collisions
- Methods to reduce collisions
  - LAN switching
  - Full-duplex Ethernet
- Wireless LANs - IEEE 802.11
- Introduction to the Ethernet LAN Analyser with hands-on exercises
- Section summary and end-of-section review questions

### 3 LAN Switching Fundamentals

- Introduction to bridging and switching
  - Separation of collision domains - LAN segmentation
- Overview of transparent bridging
- Ethernet switching:
  - MAC address learning
  - Forwarding and filtering of frames
  - Broadcast, multicast and unknown unicast frame handling
  - Cut-through switching / Fragment-free switching / Store and forward switching
  - Full duplex operation
  - Auto-negotiation
- Loops in bridged/switched networks
  - The problem
  - The solution - Spanning Tree Protocol (STP)
  - The IEEE 802.1d Spanning Tree Protocol explained
    - Ports and The Spanning Tree
    - Root Bridge election
    - Root Port selection
    - Designated bridge and Designated Port selection
    - Bridge (Switch) Port States
  - Responding to network changes
  - The IEEE 802.1w Rapid Spanning Tree Protocol
    - Port Roles
      - Root port, designated port, alternate port, backup port and disabled port
    - Port States
    - Rapid Convergence
- Section summary and end-of-section review questions

### 4 Virtual LANs (VLANs) and Trunking

- Overview of VLAN concepts and operation
- Trunking between switches
  - IEEE 802.1Q
  - Trunking Between a Switch and a Router
- VLAN configuration on the Cisco 2950
- VLAN trunking configuration on the Cisco 2950
- Hands-on exercises of configuring and testing VLANs
- Section summary and end-of-section review questions

## 5 Internet Protocol (IP) Fundamentals

- 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

## 6 Other Layer 3 Functions

- 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

## **7 Routing IP, Static Routing and Routing Protocols**

- 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 Network Design and Implementation Hands-on Exercises**

- Network design using Ethernet switches and IP routers
- Implementation of network design using static routing
- Network tools used to troubleshoot issues with the network
- Implementation of network design using automatic routing protocols

## 9 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

## 10 Transport Layer Protocols – Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

- 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
- Section summary and end-of-section review questions

## 11 Application Layer Protocols

- Overview of some applications used with TCP/IP and UDP/IP
  - File Transfer Protocol (FTP)
  - Telnet
  - Simple Mail Transfer Protocol (SMTP)
  - Domain Name System (DNS)
  - Trivial File Transfer Protocol (TFTP)
  - Hypertext Transfer Protocol (HTTP)
  - Post Office Protocol - version 3 (POP3)
  - Simple Network Management Protocol (SNMP)
- Section summary and end-of-section review questions

## 12 Firewalls

- Overview of firewalls
- Network address translation and port address translation
- Access control lists (ACL) – Access lists
- Virtual Private Networks (VPNs)
- Section summary and end-of-section review questions

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

- Introduction to MPLS
- MPLS defined
- Routing protocol overview
- Label Distribution Protocol (LDP)
- Traffic engineering with MPLS
- QoS and MPLS
- VPNs and MPLS
- Section summary and end-of-section review questions

## 14 Voice over IP

- 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