# TPG: **IP routing**

## Online course specification

**Target audience:**
This "IP routing" course is designed for those who are, or intend to be, involved in the planning, installation, or maintenance of Internet Protocol (IP) networks.

**Course aim:**
To describe the role, facilities, and operation of the various protocols that discover routes over an IP network and to describe methods of increasing the efficiency and security of the routing process.

**Course level:** Advanced
*An explanation of PTT course levels is given at the end of this document*

**Pre-requisites:**
An understanding of the principles of the Internet Protocol and routing. It is recommended that PTT's "IP Networks" course is studied before attempting this course.

**Course structure:**
The course consists of the following 8 modules:

1. Course introduction
2. RIP route discovery
3. Principles of OSPF
4. OSPF facilities
5. EIGRP route discovery
6. IP addressing
7. EGP and BGP route discovery
8. Routing security

**Module 1**: Introduction

Module aim: To summarise the aims of each module and introduce the navigation and learning facilities provided by the course.

**Module 2**: RIP route discovery

Module aim: Describe the use, operation and limitations of the distance vector routing protocol, RIP.

After completing this module, a trainee will be able to:

- review the principles of connectionless operation of a network based on the Internet Protocol (IP).
- introduce the principles of distance vector route discovery.
- describe the role of the Routing Information Protocol (RIP).
- describe the format of a RIP routing table.
- describe how routers build and update their routing tables in a network using RIP.
- explain how routing loops can be produced in a RIP-based network.

- describe how the use of split horizon and hold down timers can reduce the possibility of routing loops.
- compare the facilities provided by RIP v1, RIP v2 and RIPng

**Module 3**: Principles of OSPF

Module aim: Describe the use and operation of the link state routing protocol, OSPF.

After completing this module, a trainee will be able to:

- explain the principles and advantages of a link state routing protocol.
- describe the role of OSPF link state advertisements in building a router's topological database.
- describe the process of build a routing table from information in a topological database.

**Module 4**: OSPF facilities

Module aim: Describe the hierarchical routing and traffic engineering facilities offered by the link state routing protocol, OSPF.

After completing this module, a trainee will be able to:

- explain that the OSPF protocol allows routing tables to be built using other criteria apart from hop count.
- describe how the bandwidth cost metric is calculated.
- explain the significance of the OSPF-TE Traffic Engineering extensions to OSPF.
- explain the concept of an autonomous system (AS).
- explain that an OSPF-based AS can be divided into areas, giving advantages.
- explain the concept of a backbone area and a stub area.
- describe the role of an Area Border router and AS Boundary router.
- compare the facilities of the various versions of OSPF

**Module 5**: EIGRP route discovery

Module aim: Describe the principles of operation of the EIGRP route discovery protocol and compare its benefits with those of OSPF.

After completing this module, a trainee will be able to:

- explain that EIGRP was designed by Cisco to overcome the limitations of their distance vector protocol.
- explain the role of, the relationship between, and the types of information held in, the three types of database maintained by EIGRP on each router in a network.
- explain that EIGRP routers only exchange routing information when a network change occurs.
- explain how EIGRP combines values of least bandwidth and total delay to compute the cost of a path.
- explain the concepts of, and relationship between, successor, feasible distance, feasible successor and reported distance.
- describe how a router using EIGRP recovers from the loss of a successor path.
- explain how EIGRP avoids routing loops.
- compare the characteristics and facilities of RIP, OSPF and EIGRP.

**Module 6**: IP addressing

Module aim: Describe how IP addressing has evolved to improve the efficiency of routing and address allocation.

After completing this module, a trainee will be able to:

- explain the need to make more efficient use of IP addresses and to reduce the size of routing tables.
- describe the role and principles of subnetting with reference to the format and distribution of subnet masks.
- describe the role, advantages and principles of variable length subnet masking (VLSM).
- describe the principles and advantages of route summarisation with reference to OSPF areas.
- describe the principles of Classless Inter-Domain Routing (CIDR) and its role in improving the efficiency of IP address allocation.
- describe the advantages of IPv6 addressing with reference to the number of available addresses and the inclusion of a subnet identifier.
- explain the use of route summarisation with IPv6 addresses.

**Module 7**: EGP and BGP route discovery

Module aim: Describe and compare protocols that advertise routing information between autonomous systems.

After completing this module, a trainee will be able to:

- describe the role of the Exterior Gateway Protocol (EGP).
- describe the limitations of EGP with reference to routing loops and interconnected autonomous systems.
- describe the role and advantages of the Border Gateway Protocol (BGP).
- describe the role and principles of Interdomain traffic engineering with BGP
- describe the role of the various BGP path attributes.
- describe the role and principles of Interdomain traffic engineering with BGP
- explain the redistribution of routing information between interior and exterior routing protocols and the need for route filtering and summarisation.

**Module 8**: Routing security

Module aim: Describe the various ways in which a route discovery protocol can be misused for fraudulent or malicious purposes and explain how this misuse can be guarded against.

After completing this module, a trainee will be able to:

- explain that a hacker can send out false routing updates to either divert or disrupt traffic.
- describe methods of injecting false routing information into routers' address tables.
- explain how access lists, route filtering and modification of the time to live process can minimise the risk of routing update misuse.
- explain and compare the role of hashing and encryption.
- explain how MD5 uses hashing to authenticate the sender of routing updates.
- explain the role of the IPsec protocol in protecting transmitted routing updates.
- explain the role of digital certificates in authentication and encryption of routing updates.
- describe how the Resource Public Key Infrastructure (RPKI) ensures only a valid user of an IP address can originate an advertisement of a route to their address.
- explain how the BGPsec protocol ensures the validity of every autonomous system in a path to an IP address.

**Course access requirements:**
To access the course, a computer running a browser such as Google Chrome, Safari etc is required. The computer should have Internet access. A screen resolution of at least 1024x768 is necessary.

**Learning facilities:**
This online course employs interactive simulations, hypertext links to an online glossary and multiple-choice question sessions to fully involve the trainee in the learning experience. Each module provides revision links to previously studied, relevant topics. A record of progress and level of achievement is recorded for each trainee. Once studied as a structured, assessed course, the content can be browsed for revision or reference.

**PTT course levels:**
PTT online courses are categorised by one of three levels according to the depth of treatment they provide:

1. **Introductory:**

   PTT Introductory courses are designed for those with no previous experience or knowledge of telecommunications. These courses provide an overview of telecommunications or discuss the fundamentals of electronic communications. The study of general science at secondary (high) school is a typical pre-requisite for PTT Introductory courses.
   PTT Introductory courses are suitable for those joining the telecommunications sector particularly those in an apprenticeship programme.

2. **Intermediate:**

   PTT Intermediate courses are designed for technicians and engineers requiring an understanding of a certain aspect of telecommunications. Those planning to study an Intermediate course should have an understanding of the basic principles of electronic communications.
   The depth of treatment provided by Intermediate courses is typically equivalent to level 3 of a UK national vocational qualification (NVQ). PTT Intermediate courses can be used to support the attainment of a Communications Technology NVQ at level 3.

3. **Advanced:**

   PTT Advanced courses are designed for those who require an in-depth treatment of a certain aspect of telecommunications. Such courses are suitable for system designers as well as those who will be responsible for the maintenance of the system described in the course.
   Those planning to study a PTT Advanced course should have a background in telecommunications, and an understanding of telecommunications fundamentals and the principles of the type of telecommunications system described in the course.

PTT
October 2019

© Formactual Projects Limited t/a PTT