

TQJ: Exterior IP routing

Online course specification

Target audience:

This "Exterior 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 protocols that discover routes between IP networks 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 operation of networks based on the Internet suite of protocols including route discovery. It is recommended that PTT's "IP Networks" course is studied before attempting this course. It is also recommended that the companion course "Interior IP routing" is studied before attempting this course.

Course structure:

The course consists of the following 4 modules:

1. IP addressing
2. EGP and BGP route discovery
3. Routing security
4. Trusted routing

Module 1: 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.
- define the meaning of, and relationship between, autonomous systems, routing domains, and OSPF areas.
- 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).
- explain how the use of CIDR improves the efficiency of IP address allocation and routing.
- describe the advantages of IPv6 addressing with reference to the number of available addresses and the inclusion of a subnet identifier.

Module 2: 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.
- explain the requirement for, and role of, route filtering and summarisation.

Module 3: 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, modification of the time to live process, and anti-spoofing methods can minimise the risk of routing announcement misuse.
- explain the role and principles of hashing in the verification of the source of a routing announcement.
- explain the role, principles, and advantages of asymmetric encryption in protecting the security of transmitted routing announcements.
- explain how MD5 uses hashing to authenticate the sender of routing announcements.
- explain the role of the IPsec protocol in protecting transmitted routing announcements.

Module 4: Trusted routing

Module aim: Describe the various methods taken to improve the security of the global routing system and the role of the various organisations involved in encouraging and implementing the use of those methods.

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

- explain the role and principles of digital certificates and digital signatures in verifying the identity of the source of routing announcements.
- describe how the Resource Public Key Infrastructure (RPKI) allows the verification that a valid user of an IP address has originated an advertisement of a route to their address.
- explain how the BGPsec protocol ensures the validity of every autonomous system on a path to an IP address.
- describe the role of Internet routing registries in allowing co-operation between network operators with the aim of improving the security of the global routing system.
- describe the role of the Mutually Agreed Norms for Routing Security (MANRS) initiative with reference to the actions stipulated in its implementation guide.

Course access requirements:

To access the course, a computer/tablet running a browser such as Chrome, Safari, Edge etc is required. The device should have an active Internet connection and a screen resolution of at least 1024x768.

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
February 2024

© Formactual Projects Limited t/a PTT