## TABLE OF CONTENTS

### INTRODUCTION
- Module aim ............................................................................................................. 1
- Module abstract ...................................................................................................... 1
- Learning outcomes and assessment criteria ......................................................... 2
- Summary of learning outcomes and assessment criteria ....................................... 2
- Module content ...................................................................................................... 4
- Lectures .................................................................................................................. 5
- Class exercises and activities .................................................................................. 5
- Information resources .............................................................................................. 6
- Prescribed textbook ................................................................................................. 6
- Prescribed textbook for Networking Technologies .................................................. 6
- Recommended information sources ........................................................................ 6

### UNIT 1: TOPOLOGIES AND THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

- Learning objectives ............................................................................................... 15
- Supplementary reading ......................................................................................... 15
- Introduction ............................................................................................................ 16
  - 1.1 Key features of networks ................................................................................ 16
  - 1.2 Types of networks ........................................................................................... 16
  - 1.3 Network components ....................................................................................... 16
  - 1.4 Protocols ........................................................................................................... 18
  - 1.5 Clients and servers .......................................................................................... 18
  - 1.6 Server-based networks ...................................................................................... 18
    - 1.6.1 Advantages of server-based networks ....................................................... 19
    - 1.6.2 Disadvantages of server-based networks .................................................. 19
  - 1.7 Peer-to-peer networks ...................................................................................... 19
    - 1.7.1 Advantages of a peer-to-peer network ....................................................... 20
    - 1.7.2 Disadvantages of a peer-to-peer network .................................................. 20
  - 1.8 Network topologies ......................................................................................... 20
    - 1.8.1 Bus topology ............................................................................................. 21
    - 1.8.2 Star topology ............................................................................................. 22
    - 1.8.3 Ring topology ............................................................................................. 23
    - 1.8.4 Mesh topology ........................................................................................... 24
    - 1.8.5 Hybrid topologies ....................................................................................... 25
  - 1.9 Open Systems Interconnection (OSI) model .................................................... 26
    - 1.9.1 Network communication and the OSI model ............................................. 27
    - 1.9.2 The OSI model and network protocols ....................................................... 29
    - 1.9.3 OSI model layers ....................................................................................... 30
  - 1.10 TCP/IP protocol suite ..................................................................................... 33
    - 1.10.1 Link layer/network interface ..................................................................... 34
    - 1.10.2 Internet layer ............................................................................................. 34
    - 1.10.3 Transport layer .......................................................................................... 34
    - 1.10.4 Application layer ....................................................................................... 35
  - 1.11 Packet switching ............................................................................................. 35
  - 1.12 TCP/IP and Internet standards ....................................................................... 36
  - Concluding remarks .............................................................................................. 36
- Self-assessment ....................................................................................................... 36

### UNIT 2: ETHERNET

- Concluding remarks .............................................................................................. 37
UNIT 5: INTERNET PROTOCOL .................................................................................. 75

UNIT 4: BRIDGES AND SWITCHES ............................................................................ 63

Introduction ....................................................................................................... 86

Supplementary reading ...................................................................................... 85

Learning objectives ............................................................................................ 85

Test your knowledge .......................................................................................... 84

5.1 Datagram structure ...................................................................................... 76
5.2 IP addresses ................................................................................................. 76
5.2.1 Converting between binary and decimal format ........................................ 77
5.3 Subnet masks ................................................................................................. 77
5.3.1 ANDing ................................................................................................... 78
5.4 Configuring TCP/IP ..................................................................................... 79
5.4.1 Configuring TCP/IP under Windows ......................................................... 79
5.4.2 Configuring TCP/IP under Linux .............................................................. 80
5.5 ipconfig/ifconfig ....................................................................................... 81
5.6 IP routing basics .......................................................................................... 82
5.7 Internet Control Message Protocol (ICMP) and Ping ............................... 82
5.7.1 ICMP header ............................................................................................ 82
5.7.2 ICMP error types ...................................................................................... 83
5.7.3 Ping .......................................................................................................... 83

Concluding remarks .......................................................................................... 83

Self-assessment ................................................................................................. 83

Test your knowledge .......................................................................................... 83

UNIT 6: ADDRESSING SCHEMES ........................................................................... 85

Introduction ....................................................................................................... 86

6.1 Addressing schemes ..................................................................................... 86
6.1.1 Broadcast, multicast and unicast .............................................................. 86
6.1.2 Classful addressing .................................................................................. 86
6.1.3 Class D and E addresses ......................................................................... 87
6.1.4 Private addressing ................................................................................... 87
6.2 Creating subnets .......................................................................................... 88
6.2.1 Classful subnets ...................................................................................... 88
6.2.2 Classless subnets .................................................................................... 88
6.2.3 Planning an IP addressing scheme .......................................................... 89
6.3 Public Internet addressing ........................................................................... 89
6.3.1 Classful addressing .................................................................................. 90
UNIT 12: WIRED NETWORKS

### Introduction

#### Supplementary reading

#### Learning objectives

#### Test your knowledge

#### Self-assessment

#### Concluding remarks

---

UNIT 11: WAN TECHNOLOGIES

### Introduction

#### Supplementary reading

#### Learning objectives

#### Test your knowledge

#### Self-assessment

#### Concluding remarks

---

### Front Matter

#### 10.3 File Transfer Protocol (FTP)

#### 10.4 Email (SMTP/POP3/IMAP4)

#### 10.5 Conferencing and VoIP protocols

---

#### 11.4 Modern telecommunications networks

#### 11.5 Packet-switched WAN services

---

#### 11.6 Local loop services

#### 11.7 Installing modems

---

#### 12.1 Wiring standards
## UNIT 13: INSTALLING WIRELESS NETWORKS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1</td>
<td>Wi-Fi (IEEE 802.11)</td>
<td>150</td>
</tr>
<tr>
<td>13.1.1</td>
<td>Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)</td>
<td>150</td>
</tr>
<tr>
<td>13.1.2</td>
<td>IEEE 802.11 standards</td>
<td>150</td>
</tr>
<tr>
<td>13.1.3</td>
<td>Antenna types</td>
<td>150</td>
</tr>
<tr>
<td>13.2</td>
<td>Setting up a wireless network</td>
<td>151</td>
</tr>
<tr>
<td>13.2.1</td>
<td>Ad hoc and infrastructure modes</td>
<td>151</td>
</tr>
<tr>
<td>13.2.2</td>
<td>Roaming</td>
<td>152</td>
</tr>
<tr>
<td>13.2.3</td>
<td>Site surveys and channel configuration</td>
<td>152</td>
</tr>
<tr>
<td>13.2.4</td>
<td>Configuring an access point</td>
<td>153</td>
</tr>
<tr>
<td>13.3</td>
<td>Wireless security</td>
<td>155</td>
</tr>
<tr>
<td>13.3.1</td>
<td>War driving and war chalking</td>
<td>155</td>
</tr>
<tr>
<td>13.3.2</td>
<td>Wi-Fi authentication</td>
<td>156</td>
</tr>
<tr>
<td>13.4</td>
<td>Wireless WANs</td>
<td>157</td>
</tr>
<tr>
<td>13.4.1</td>
<td>Troubleshooting configuration issues</td>
<td>163</td>
</tr>
</tbody>
</table>
Introduction

Welcome to Networking Technologies (C_ITNT021.C_ITNT121), in which we provide a background to the basic components of networked systems from which all networking operations derive. This module also includes the evaluation of networks and network applications.

Module aim

To enable students to understand computer networking concepts, how they function and operate, and the protocols, standards and models associated with networking technology.

Module abstract

Understanding of the underlying principles of networking is of vital importance to all IT professionals in an environment that is increasingly complex and under continuous development.

Students will explore a range of hardware and technologies, culminating in the design and deployment of a networked system. Working with many technologies, this module informs the design, selection, implementation and support of a variety of network systems, including local area networks and larger scale, wider area networked systems. Supporting a range of units in the Higher National suite, this module underpins the principles of networks for all and enables students to work towards their studies in vendor units, if applicable.
Learning outcomes and assessment criteria

On successful completion of this module, you will:
1. Identify and explain networking principles and concepts
2. Discuss the role, purpose and specifications of key networking components
3. Discuss the functions and features of TCP/IP addressing, protocols and services
4. Identify and explain network services and WAN access technologies
5. Demonstrate the ability to implement and support networked systems

The following table outlines the assessment criteria that are aligned to the learning outcomes.

Summary of learning outcomes and assessment criteria

<table>
<thead>
<tr>
<th>Learning outcomes</th>
<th>Assessment criteria to pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>On successful completion of this module, you will:</td>
<td>You can:</td>
</tr>
<tr>
<td>1. Identify and explain networking principles and concepts.</td>
<td>1.1 Describe different types of network topologies and identify the key physical and logical network topologies.</td>
</tr>
<tr>
<td></td>
<td>1.2 Describe the functions of the layers of the OSI model and TCP/IP suite.</td>
</tr>
<tr>
<td></td>
<td>1.3 Describe the scope of IEEE 802 standards and the features of IEEE 802.3 (Ethernet).</td>
</tr>
<tr>
<td></td>
<td>1.4 Describe the properties of MAC addressing and ARP.</td>
</tr>
<tr>
<td></td>
<td>1.5 Discuss the use of packet sniffers/protocol analysers to capture and examine network traffic.</td>
</tr>
<tr>
<td></td>
<td>1.6 Discuss the functions, features and configuration of a network adapter.</td>
</tr>
<tr>
<td>2. Discuss the role, purpose and specifications of key networking components.</td>
<td>2.1 Describe the types and properties of different cables and connectors.</td>
</tr>
<tr>
<td></td>
<td>2.2 Describe the use of repeaters and media converters.</td>
</tr>
<tr>
<td></td>
<td>2.3 Examine the functionalities and characteristics of intranetworking components.</td>
</tr>
<tr>
<td></td>
<td>2.4 Describe the purposes and functions of VLANs and STP.</td>
</tr>
<tr>
<td>Learning outcomes</td>
<td>Assessment criteria to pass</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>On successful completion of this module, you will:</strong></td>
<td><strong>You can:</strong></td>
</tr>
</tbody>
</table>
| 3. Discuss the functions and features of TCP/IP addressing, protocols and services. | 3.1 Describe the format of IP addresses and datagrams, and the operation of subnet mask and the basics of IP routing.  
3.2 Configure TCP/IP on Windows and Linux hosts.  
3.3 Describe the operation of ICMP and related troubleshooting and configuration utilities.  
3.4 Discuss IP addressing schemes, including address classes, address ranges in private networks, configuring an IP address scheme for a private network, subnetting and classful addressing (supernetting).  
3.5 Discuss the methods for auto-configuring IP addressing information (DHCP and APIPA), including configuration of DHCP server and the use of Network Time Protocol (NTP).  
3.6 Identify IPv6 addressing schemes and describe the IPv6 address format and packet structure. |
| 4. Identify and explain network services and WAN access technologies. | 4.1 Describe the format of hostnames and FQDN, the process of name resolution, basic configuration for a DNS server and name resolution troubleshooting tools.  
4.2 Describe the functions of Web and file transfer application protocols and communications protocols.  
4.3 Distinguish between the types of switched networks.  
4.4 Identify technologies and protocols used to implement WANs.  
4.5 Describe and differentiate between types of local access network.  
4.6 Discuss the installation and configuration of dial-up and broadband modems. |
| 5. Demonstrate the ability to implement and support networked systems. | 5.1 Examine the installation of wired networks.  
5.2 Identify appropriate tools for network hardware installation and testing.  
5.3 Examine the installation of wireless networks.  
5.4 Describe effective troubleshooting procedures.  
5.5 Troubleshoot common connectivity scenarios. |

These outcomes are covered in the module content and they are assessed in the form of written assignments and semester tests. If you comply with and achieve all the pass criteria related to the outcomes, you will pass this module.

Learning and assessment may be performed across modules, at module level or at outcome level. Evidence may be required at outcome level, although opportunities exist for covering more than one outcome in an assignment.
Module content

1. Identify and explain networking principles and concepts.
   - Topologies and the OSI model: key features of networks, clients and servers, network topologies, the OSI model (physical layer, data link layer, network layer, upper layers), TCP/IP Protocol Suite
   - Ethernet: IEEE 802 standards, media characteristics, Media Access Control (MAC), Ethernet (IEEE 802.3), Ethernet media specifications, MAC addressing, Address Resolution Protocol (ARP), network adapters, protocol analyser

2. Discuss the role, purpose and specifications of key networking components.
   - Cabling and connectors: selecting network cable, twisted pair cable (UTP/STP/ScTP), other copper cable types, fibre-optic cable, repeaters, media convertors
   - Bridges and switches: hubs and bridges, switches, configuring a switch, Power over Ethernet (PoE), Virtual LANs (VLAN), Spanning Tree Protocol (STP)

3. Discuss the functions and features of TCP/IP addressing, protocols and services.
   - Internet protocol: Internet protocol basics, subnet masks, configuring TCP/IP, ipconfig/ifconfig, IP routing basics, ICMP and Ping
   - Addressing schemes: IP addressing schemes, creating subnets, public Internet addressing
   - DHCP, APIPA and NTP: static versus dynamic IP addressing, configuring DHCP, Network Time Protocol (NTP)
   - IPv6: IPv6 address format, IPv6 addressing schemes

4. Identify and explain network services and WAN access technologies.
   - Name resolution: hostnames, name resolution methods, configuring DNS servers, name resolution troubleshooting
• **Internet applications**: TCP/IP services, World Wide Web (HTTP), File Transfer Protocol (FTP), email (SMTP/POP3/IMAP), conferencing and VoIP protocols

• **WAN technologies**: WAN basics, telecommunications networks, modern telecommunications networks, packet-switched WAN services, local loop services, installing modems

5. **Demonstrate the ability to implement and support networked systems.**

• **Wired networks**: wiring standards, wiring distribution, distribution frames, wiring schemes, installing WAN links, cable testing tools, planning a SOHO network installation

• **Installing wireless networks**: Wi-Fi (IEEE 802.11), setting up a wireless network, wireless security, wireless WANs

• **Network troubleshooting**: troubleshooting procedures, troubleshooting common connectivity scenarios, troubleshooting internetworking infrastructure, troubleshooting configuration issues, troubleshooting internetworking infrastructure, troubleshooting services

**Lectures**

Each week has four compulsory lecture hours for all students. It is recommended that the lecture hours be divided into two sessions of two hours each, but this may vary depending on the campus.

Each week has a lecture schedule which indicates the approximate time that should be allocated to each activity. The week’s work schedule has also been divided into two lessons.

**Class exercises and activities**

Students will be required to complete a number of exercises and activities in class. These activities and exercises may also contribute to obtaining a pass; therefore, it is important that students are present in class so that they do not forfeit the opportunity to be exposed to such exercises and activities.

Activity sheets that are handed in should be kept by the lecturer so that they can be used as proof of criteria that were met, if necessary.
Information resources

You should have access to a resource centre or a library with a wide range of relevant resources. Resources can include textbooks and e-books, newspaper articles, journal articles, organisational publications, databases, etc. You can access a range of academic journals in electronic format via EBSCOhost. You have to consult the campus librarian to assist you with accessing EBSCOhost.

Prescribed textbook

Prescribed textbook for Networking Technologies

GTSLearning. 2014. Networking technology study notes.

Recommended information sources

Books


**Websites**


**NOTE**

- Web pages provide access to a further range of Internet information sources.
- Students must use this resource with care, justifying the use of information gathered.

**Using the Study Guide**

As we indicated earlier, the prescribed textbook is your main source of information for this module and the Study Guide serves as a guide to the prescribed textbook.

The purpose of the Study Guide is to facilitate your learning and help you to master the content of the prescribed textbook and other material. It helps you to structure your learning and manage your time; provides outcomes and activities to help you master said outcomes; and directs you to the appropriate sections in the prescribed textbook. It is, therefore, important that you start with the Study Guide.

The Study Guide has been carefully designed to optimise your study time and maximise your learning, so that your learning experience is as meaningful and successful as possible. To deepen your learning and enhance your chances of success, it is important that you read the Study Guide attentively and follow all the instructions carefully. Pay special attention to the course outcomes at the beginning of the Study Guide and at the beginning of each unit.

It is essential that you complete the exercises and other learning activities in the Study Guide as your course assessments (examinations, tests and assignments) will be based on the assumption that you have completed these activities.
The Study Guide accompanies the prescribed textbook and, therefore, it should be read in conjunction with such: it should **not** be deemed as a replacement for the prescribed text.

**Purpose**

The purpose of the Study Guide is to facilitate the learning process and to help you to structure your learning and to master the content of the module. The textbook covers certain themes in detail.

Where applicable, we give more simplified explanations in the Study Guide. It is important for you to work through both the prescribed textbook and the Study Guide attentively and to follow all the instructions set out in the Study Guide. In this way, you should be able to deepen your learning and enhance your chances of success.

**Structure**

The Study Guide is structured as follows:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Topologies and Open Systems Interconnection (OSI) model</td>
</tr>
<tr>
<td>2</td>
<td>Ethernet</td>
</tr>
<tr>
<td>3</td>
<td>Cabling and connectors</td>
</tr>
<tr>
<td>4</td>
<td>Bridges and switches</td>
</tr>
<tr>
<td>5</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>6</td>
<td>Addressing schemes</td>
</tr>
<tr>
<td>7</td>
<td>DHCP, APIPA and NTP</td>
</tr>
<tr>
<td>8</td>
<td>IPv6</td>
</tr>
<tr>
<td>9</td>
<td>Name resolution</td>
</tr>
<tr>
<td>10</td>
<td>Internet applications</td>
</tr>
<tr>
<td>11</td>
<td>WAN technologies</td>
</tr>
<tr>
<td>12</td>
<td>Wired networks</td>
</tr>
<tr>
<td>13</td>
<td>Installing wireless networks</td>
</tr>
<tr>
<td>14</td>
<td>Network troubleshooting</td>
</tr>
</tbody>
</table>

**GLOSSARY**

**BIBLIOGRAPHY**
Individual units
The individual units in the Study Guide are structured in the same way and each unit contains the following features, which should enhance the learning process:

<table>
<thead>
<tr>
<th>Unit title</th>
<th>Each unit title is based on the title and content of a specific outcome or assessment criterion (criteria) as discussed in the unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learning outcomes and assessment criteria</td>
<td>The unit title is followed by an outline of the learning outcomes and assessment criteria, which will guide your learning process. It is important for you to become familiar with the learning outcomes and assessment criteria, because they represent the overall purpose of the module as well as the end product of what you should have learnt in the unit.</td>
</tr>
<tr>
<td>Learning objectives</td>
<td>Learning objectives, which follow the learning outcomes and assessment criteria, are statements that define the expected goal of the unit in terms of the specific knowledge and skills that you should acquire as a result of mastering the unit content. Learning objectives clarify, organise and prioritise learning and they help you to evaluate your own progress, thereby taking responsibility for your learning.</td>
</tr>
<tr>
<td>Introduction</td>
<td>The prescribed reading section is followed by an introduction that identifies the key concepts of the unit.</td>
</tr>
<tr>
<td>Content</td>
<td>The content of each unit contains the theoretical foundation of the module and is based on the work of experts in the field of this module. The theory is illustrated by means of relevant examples.</td>
</tr>
<tr>
<td>Concluding remarks</td>
<td>The concluding remarks at the end of each unit provide a brief summary of the unit as well as an indication of what you can expect in the following unit.</td>
</tr>
<tr>
<td>Self-assessment</td>
<td>The unit ends off with a number of theoretical self-assessment questions that test your knowledge of the content of the unit.</td>
</tr>
</tbody>
</table>

Glossary
As you can see, we include a glossary at the end of the Study Guide. Please refer to it as often as necessary in order to familiarise yourself with the exact meaning of the terms and concepts involved in Networking Technologies.

The use of icons
Icons are used to highlight (emphasise) particular sections or points in the Study Guide, to draw your attention to important aspects of the work, or to highlight activities. The following icons are used in the Study Guide:

**Activity**
This icon indicates learning activities/exercises that have to be completed, whether individually or in groups, in order to assess (evaluate) your understanding of the content of a particular section.
Learning outcome alignment
This icon is used to indicate how individual units in the Study Guide are aligned to a specific outcome and its assessment criteria.

Supplementary reading
This icon indicates that you are expected to do some additional (supplementary) reading – i.e. you should obtain additional information by consulting relevant, external information sources.

Test your knowledge
This icon appears at the end of each unit in the Study Guide, indicating that you are required to answer self-assessment questions to test your knowledge of the content of the foregoing unit.

Alignment to prescribed textbook
The following table reflects the alignment between learning outcomes, assessment criteria, units in the Study Guide and chapters in the prescribed textbook.
## Study Guide/prescribed textbook alignment

<table>
<thead>
<tr>
<th>Learning outcome</th>
<th>Assessment criteria</th>
<th>Study Guide unit</th>
<th>Textbook chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LO1</strong> Identify and explain networking principles and concepts.</td>
<td>1.1 Describe different types of network topologies and identify the key physical and logical network topologies.</td>
<td>Unit 1</td>
<td>Module 1/Unit 1</td>
</tr>
<tr>
<td></td>
<td>1.2 Describe the functions of the layers of the OSI model and TCP/IP suite.</td>
<td>Unit 1</td>
<td>Module 1/Unit 1</td>
</tr>
<tr>
<td></td>
<td>1.3 Describe the scope of IEEE 802 standards and the features of IEEE 802.3 (Ethernet).</td>
<td>Unit 2</td>
<td>Module 1/Unit 3</td>
</tr>
<tr>
<td></td>
<td>1.4 Describe the properties of MAC addressing and ARP.</td>
<td>Unit 2</td>
<td>Module 1/Unit 3</td>
</tr>
<tr>
<td></td>
<td>1.5 Discuss the use of packet sniffers/protocol analysers to capture and examine network traffic.</td>
<td>Unit 2</td>
<td>Module 1/Unit 3</td>
</tr>
<tr>
<td></td>
<td>1.6 Discuss the functions, features and configuration of a network adapter.</td>
<td>Unit 2</td>
<td>Module 1/Unit 3</td>
</tr>
<tr>
<td><strong>LO2</strong> Discuss the role, purpose and specifications of key networking components.</td>
<td>2.1 Describe the types and properties of different cables and connectors.</td>
<td>Unit 3</td>
<td>Module 1/Unit 2</td>
</tr>
<tr>
<td></td>
<td>2.2 Describe the use of repeaters and media converters.</td>
<td>Unit 3</td>
<td>Module 1/Unit 2</td>
</tr>
<tr>
<td></td>
<td>2.3 Examine the functionalities and characteristics of intranetworking components.</td>
<td>Unit 4</td>
<td>Module 1/Unit 4</td>
</tr>
<tr>
<td></td>
<td>2.4 Describe the purposes and functions of VLANS and STPs.</td>
<td>Unit 4</td>
<td>Module 1/Unit 4</td>
</tr>
<tr>
<td>Learning outcome</td>
<td>Assessment criteria</td>
<td>Study Guide unit</td>
<td>Textbook chapter</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>LO3</td>
<td>Discuss the functions and features of TCP/IP addressing, protocols and services.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Describe the format of IP addresses and datagrams, and the operation of subnet mask and the basics of IP routing.</td>
<td>Unit 5</td>
<td>Module 2/ Unit 1</td>
</tr>
<tr>
<td>3.2</td>
<td>Configure TCP/IP on Windows and Linux hosts.</td>
<td>Unit 5</td>
<td>Module 2/ Unit 1</td>
</tr>
<tr>
<td>3.3</td>
<td>Describe the operation of ICMP and related troubleshooting and configuration utilities.</td>
<td>Unit 5</td>
<td>Module 2/ Unit 1</td>
</tr>
<tr>
<td>3.4</td>
<td>Discuss IP addressing schemes, including address classes, address ranges in private networks, configuring an IP address scheme for a private network, subnetting and classful addressing (supernetting).</td>
<td>Unit 6</td>
<td>Module 2/ Unit 2</td>
</tr>
<tr>
<td>3.5</td>
<td>Discuss the methods for auto-configuring IP addressing information (DHCP and APIPA), including configuration of DHCP server and the use of Network Time Protocol (NTP).</td>
<td>Unit 7</td>
<td>Module 2/ Unit 3</td>
</tr>
<tr>
<td>3.6</td>
<td>Identify IPv6 addressing schemes and describe the IPv6 address format and packet structure.</td>
<td>Unit 8</td>
<td>Module 2/ Unit 4</td>
</tr>
<tr>
<td>LO4</td>
<td>Identify and explain network services and WAN access technologies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Describe the format of hostnames and FQDN, the process of name resolution, basic configuration for a DNS server and name resolution troubleshooting tools.</td>
<td>Unit 9</td>
<td>Module 3/ Unit 1</td>
</tr>
<tr>
<td>4.2</td>
<td>Describe the functions of Web and file transfer application protocols and communications protocols.</td>
<td>Unit 10</td>
<td>Module 3/ Unit 2</td>
</tr>
<tr>
<td>4.3</td>
<td>Distinguish between the types of switched networks.</td>
<td>Unit 11</td>
<td>Module 3/ Unit 3</td>
</tr>
<tr>
<td>4.4</td>
<td>Identify technologies and protocols used to implement WANs.</td>
<td>Unit 11</td>
<td>Module 3/ Unit 3</td>
</tr>
<tr>
<td>4.5</td>
<td>Describe and differentiate types of local access networks.</td>
<td>Unit 11</td>
<td>Module 3/ Unit 3</td>
</tr>
<tr>
<td>4.6</td>
<td>Discuss the installation and configuration of dial-up and broadband modems.</td>
<td>Unit 11</td>
<td>Module 3/ Unit 3</td>
</tr>
</tbody>
</table>
**Concluding remarks**

At this point, you should be familiar with the module design and structure.

In Unit 1, we start by discussing topologies and the Open Systems Interconnection (OSI) model.
Unit 1: Topologies and the Open Systems Interconnection (OSI) model

Unit 1 is aligned with the following learning outcome and assessment criteria:

Learning outcome
LO1: Identify and explain networking principles and concepts.

Assessment criteria
AC1.1: Describe different types of network topologies and identify the key physical and logical network topologies.
AC1.2: Describe the functions of the layers of the OSI model and the TCP/IP suite.

Learning objectives
After studying this unit, you should be able to:

• Use basic terminology to describe different types of networks
• Understand what is meant by a topology and identify the key physical and logical network topologies:
  o Star
  o Mesh
  o Bus
  o Ring
  o Point-to-point/point-to-multipoint
  o Hybrid
  o Peer-to-peer/client-server
• Describe the functions of the layers of the OSI model
• Understand the basic features of the TCP/IP network protocol suite

Supplementary reading

Unit 1 adapted from:

Introduction

This unit describes the different topologies available, the different types of networks, the functions of the layers of the OSI model and the TCP/IP suite.

1.1 Key features of networks

Two or more computer systems linked together by some form of transmission medium that enables them to share information is called a network. A network provides services to its users. Historically, these services have included access to shared files, folders and printers and database applications. Modern networks are evolving to provide more services, including Web applications, Voice over IP (VoIP) and multimedia conferencing (GTSLearning, 2014).

1.2 Types of networks

Below are some terms that broadly define the scope of different types of networks:

- **Local Area Network (LAN):** a network that does not exceed a distance of 1.25 miles (2 km) from end to end
- **Campus Area Network (CAN):** a multi-building network that is limited in scope to a single geographical location and covering the same sort of distance as a LAN
- **Wide Area Network (WAN):** a network in which the distance exceeds 1.25 miles (2 km). It often comprises a series of LANs that have been joined together
- **Internet:** A worldwide network of networks based on TCP/IP protocol. It is not owned by a single company or organisation. The term ‘Internet’ is also used to describe any series of interconnected networks
- **Intranet:** It uses the same technologies as the Internet, but it is owned and managed by a company or organisation. Typically implemented as a LAN or WAN
- **Extranet:** an intranet that is also accessible to selected third-parties, such as customers or suppliers

(GTSLearning, 2014)

1.3 Network components

Below are some terms used to describe components of a network:

- **Node/host/station:** A node is any device that can communicate on the network and must have a unique address. ‘Host’ is often used in TCP/IP networking to mean the same thing as a node, while a node on a wireless network is known as a station.
- **Transmission media:** Information is always sent between nodes using some form of media, such as cable or wireless.
- **Intranetwork devices**: These are extra devices used by some networks to facilitate connections between nodes. A switch is an example of intranetwork device.

- **Segment**: It is part of a larger network that is linked together by an intranetwork device. All nodes on the same segment use the same type of transmission media and have the same bandwidth.

- **Backbone**: This term describes a fast link between other segments of a network. The backbone carries all the communications occurring between nodes in separate segments.

- **Internetwork devices**: Separate networks can be joined using internetwork devices such as routers. Such networks may use different types of transmission media and protocols.

- **Subnet**: This is a logical grouping of hosts within a single network. Subnets must use internetwork devices to communicate.

(GTSLearning, 2014)

The figure below is a demonstration of typical network boundaries. The entire network is connected to the wider Internet via a router. The router is also used to divide the network into two subnets. Within each subnet, a switch is used to allow nodes to communicate with one another and (through the router) the other subnet and the Internet. The link between each node and the switch is a segment. High bandwidth backbone segments are used between the router and the Internet and the router and the two switches:

![Figure 1: Network boundaries](Source: GTSLearning (2014))
1.4 Protocols

A protocol is a set of rules enabling systems to communicate. It generally defines the format in which data can be exchanged. Two of the most important functions of a protocol are to provide addressing and encapsulation. The addressing describes where data should go, whereas the encapsulation describes how data should be packaged for transmission. The basic process of encapsulation is for the protocol to add fields in a header to the payload that it receives from an application or other protocol (GTSLearning, 2014).

1.5 Clients and servers

Clients or workstations are computers on the network that allow users to request shared resources on servers. A server provides shared resources on the network and allows clients to access this information (GTSLearning, 2014).

The different types of servers include the following:

- **Network servers**: provide services that allow clients to join the network, such as name resolution, authentication or proxies
- **File and print servers**: share resources amongst clients
- **Application servers**: provide centralised processing. Some examples include virtual applications, Web applications and database platforms
- **Message servers**: provide email, chat and/or conferencing functionality
- **Media servers**: host streaming Audio/Video (A/V) applications

(GTSLearning, 2014)

1.6 Server–based networks

In this type of network, a dedicated central server (or servers) is used to provide access to resources. The first server-based Network-Operating System (NOS) for computers was developed by Novell and appeared as NetWare in 1985. Now, the most widely used server NOSs are Microsoft Server and UNIX/Linux. Figure 2 below shows a server-based network:
1.6.1 Advantages of server-based networks

- Performance
- Security
- Administration
- Scalability

1.6.2 Disadvantages of server-based networks

- High cost
- Complexity

1.7 Peer-to-peer networks

In a peer-to-peer network, each computer on the system is a ‘peer’ of the others and each may act as both a client and a server. This means that every user may share folders on his/her hard disk and also share peripherals, such as printers and scanners (GTSLearning, 2014). Figure 3 shows a peer-to-peer network.
1.7.1 Advantages of a peer-to-peer network
- Equipment and software costs are much lower.
- Installation and initial configuration is simple compared with server-based systems.

1.7.2 Disadvantages of a peer-to-peer network
- Peer-to-peer systems typically use machines of a lower specification than dedicated servers.
- They are difficult to manage, because they are based on the concept that each user is responsible for his/her own machine.
- There is a lack of security.

1.8 Network topologies
The network topology describes physical or logical structure or shape of the network. The physical topology describes the actual appearance or layout of the network, whereas the logical topology describes the flow of data through the network (GTSLearning, 2014).
In the simplest type of topology, a single link is established between two nodes. This is known as a point-to-point (or one-to-one) connection. Because only two devices share the connection, they are guaranteed a level of bandwidth (GTSLearning, 2014).

A multipoint (or multi-drop or point-to-multipoint) link is any connection between three or more devices. These multiple devices must share the available bandwidth.

Figures 4 and 5 depict point-to-point and multipoint connections, respectively.

![Figure 4: Point-to-point connection](Source: GTSLearning (2014))

![Figure 5: Multipoint connections](Source: GTSLearning (2014))

### 1.8.1 Bus topology

The simplest example of a bus topology is two computers directly connected by a single cable. ‘Physical bus’ means all nodes attach to one cable, whereas ‘logical bus’ means that all nodes connected to the same segment receive the same signals. The signal normally travels down the cable in both directions from the source and is received by all nodes connected to the cable. The bus is terminated at both ends of the cable to absorb the signal when it has passed all connected devices. This type of topology has a limited number of nodes, and faults cause widespread problems. It is obsolete as a physical topology. Wi-Fi is an example of a logical bus (GTSLearning, 2014).
1.8.2 Star topology

In a star network, each node is connected to a central point, typically an intranetwork or internetwork devices. The central point mediates communications between the attached nodes (GTSLearning, 2014).
1.8.2.1 Advantages of a star topology
- It is easy to reconfigure.
- It is easy to troubleshoot, because all data goes through a central point, which can be used to monitor and manage the network.
- Faults are automatically isolated to the media, node or intra-/internetwork devices.

1.8.2.2 Disadvantages of a star topology
- The central device/concentrator is a central point of failure.
- It requires more cable than a bus topology.

1.8.3 Ring topology
In this type of topology, computers are connected in a loop. The ring comprises a series of point-to-point links between each device. Signals pass from device to device in a single direction, with the signal regenerated at each device. It is no longer used on LANs, but remains current on WANs (GTSLearning, 2014).
1.8.3.1 Advantages of a ring topology

- A ring topology uses relatively little cable.
- It is simple to install.
- Two ring systems can be used to provide fault tolerance.

1.8.3.2 Disadvantages of a ring topology

- It is difficult to reconfigure.
- A media or device failure can affect all devices.
- It is difficult to troubleshoot.

1.8.4 Mesh topology

Mesh network topologies are commonly used in WANs. A mesh can be either full or partial. A full mesh is one in which each node is connected to every other node, whereas a partial mesh is one in which fewer physical links are needed. In a partial mesh, nodes relay (route) communications to provide interconnections between all nodes. It also provides redundancy and fault tolerance.

The architecture of the Internet is based on a mesh topology. To calculate the number of links required by a full mesh, the formula $n(n-1)/2$ is used, where $n$ is the number of nodes (GTSLearning, 2014).
1.8.5 Hybrid topologies

This is when two different topologies are combined within the same network to benefit from the advantages of both topologies.

1.8.5.1 Star-bus

This is a means of connecting star networks using a bus ‘backbone’ or ‘trunk’.
1.8.5.2 Star-wired ring

This is a physical star but logical ring topology. In this case, nodes are attached to the ring indirectly via an intermediary device, such as a Multistation Access Unit (MAU or MSAU).

![Figure 11: Star-wired ring](Source: GTSLearning (2014))

1.9 Open Systems Interconnection (OSI) model

The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model in 1977. It was designed to aid understanding of how a network system functions in terms of both the hardware and software components. The standard was published in 1983 as ISO 7498 (GTSLearning, 2014).
1.9.1 Network communication and the OSI model

For two computers to communicate, they must be running the same protocol. Each layer communicates with its equivalent layer on the other computer via the lower layers of the model. Each layer provides services for the layer above and uses the services of the layer below, as seen in Figure 13 (GTSLearning, 2014).
When a message is sent from one computer to another, it travels down the stack of layers on the sending computer, reaches the receiving computer using the transmission media and then passes up the stack on that computer. At each level (except the physical layer), a header is added to the data payload, forming a Protocol Data Unit (PDU). These headers are read by the corresponding layer on the other computer and provide control information (see Figure 14). This process is called encapsulation (GTSLearning, 2014).
1.9.2 The OSI model and network protocols

The OSI model is only intended to be a conceptual framework for discussing and designing protocols. Figure 15 below shows the OSI model layers with their associated protocols:

Figure 14: OSI header information

Source: GTSLearning (2014)
1.9.3 OSI model layers

A description of the layers of the OSI model is given below.

1.9.3.1 Physical layer

The physical layer of the OSI model is responsible for the transmission and receipt of bits from one computer to another computer. It specifies the following:
- Physical topology
- Mechanical specifications
- Bit transmission/encoding

Connectivity devices found at this layer include:
- Transceiver
- Media converter
- Repeater
- Hub
- Modem

(GTSLearning, 2014)
1.9.3.2 Data link layer

This layer is responsible for transferring data between devices. Other functions of this layer include:
- Addressing a frame to specific computers on the network (using their hardware addresses)
- Recognising when the destination address in a frame matches the hardware address of the installed network card and ignoring frames that do not match
- Error control, which allows the detection of errors
- The ability to control the data flow, which prevents fast transmitters from overwhelming slow receivers with data

(GTSLearning, 2014)

This layer has two sub-layers, called Media Access Control (MAC) and Logical Link Control (LLC), as seen in Figure 16.

![IEEE 802 sublayers](source: GTSLearning (2014))

The MAC sublayer defines the way in which multiple network adapters share a single transmission medium. It covers the following:
- Logical topology
- Contention/token passing
- Hardware addressing

The logical sub-layer is responsible for establishing and maintaining a link between communicating devices for the transmission of frames. This includes:
- Service level – connection-oriented or connectionless
- Flow control and error detection
Connectivity devices at the data link layer include:
- Network adapter
- Bridge
- Basic switch
- Wireless Access Point (AP)

(GTSLearning, 2014)

1.9.3.2 Network layer

The network layer is responsible for moving data around a network of networks, known as an internetwork or the Internet. Other functions of the network layer include:
- Network addressing
- Routing
- Fragmentation/reassembly
- Flow control
- Error control

(GTSLearning, 2014)

1.9.3.3 Transport layer

The transport layer is responsible for ensuring reliable data delivery so that packets arrive error-free and without loss. This layer accomplishes reliable delivery through the following mechanisms:
- Acknowledgement messages
- Orderly connection establishment and teardown
- Segmentation
- Flow control

(GTSLearning, 2014)

1.9.3.4 Session layer

Allows applications running on different computers to communicate using a connection that is called a dialogue. The session layer administers the process by establishing the dialogue, managing data transfer and then tearing down the session. Managing data transfer is called dialogue control. The three modes of dialogue control are: one-way, two-way alternate and two-way simultaneous (GTSLearning, 2014).

1.9.3.5 Presentation layer

This layer transforms data between the format required for the network and the format required for the application. It also supports data compression (GTSLearning, 2014).
1.9.3.6 Application layer

This layer provides support services to applications requiring network resources. One of the most utilised services provided by this layer is file transfer. Other services include network printing, electronic mail, directory lookup and database services (GTSLearning, 2014).

1.9.3.7 OSI model summary

![OSI model](image)

**Figure 17: OSI model**

Source: GTSLearning (2014)

1.10 TCP/IP protocol suite

Protocols are procedures or rules used by networked computers to communicate. A number of protocol suites have been used for LAN and WAN communications over the years. However, the overwhelming majority of networks have now converged on the use of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite (GTSLearning, 2014).
1.10.1 Link layer/network interface
This is the equivalent of the OSI physical and data link layer, as it defines the host’s connection to the network. Technologies used can be LAN-based (Ethernet or Wi-Fi) or WAN-based (T-carrier, ISDN or DSL) (GTSLearning, 2014).

1.10.2 Internet layer
This layer provides addressing and routing functions. It uses a number of protocols to ensure the delivery of packets (GTSLearning, 2014).

1.10.3 Transport layer
The transport layer provides communication between the source and destination computers and breaks application layer information into packets. The two methods of data delivery provided by TCP/IP are connection-oriented and connectionless (GTSLearning, 2014).
1.10.4 **Application layer**

This is the layer at which TCP/IP services (high-level protocols) can be run (such as FTP, HTTP and SMTP).

1.11 **Packet switching**

Prior to the development of packet switching, any two computers wanting to communicate had to open a direct channel (known as a circuit). If this circuit was broken, the computers would stop communicating immediately. Packet switching introduced the ability for one computer to forward information to another. In this type of switching, data is broken into packets that can take any path to their destination. It is described as robust, as it can recover from link failures automatically (GTSLearning, 2014).

![Packet switching networks](source)

*Figure 19: Packet switching networks*

Source: GTSLearning (2014)

The figure above shows an example of an Internet system. A packet being sent from Network A – D may be sent via Network C (the quickest route). If this route becomes unavailable, the packet is routed using an alternate route (e.g. A-F-E-D).
1.12 TCP/IP and Internet standards

Examples of TCP/IP and Internet standards include:
• Internet Society (ISOC)
• Internet Architecture Board (IAB): The IAB governs three groups; namely, the Internet Research Task Force, Internet Engineering Task Force and Internet Assigned Numbers Authority
• Request For Comments (RFC)

(GTSLearning, 2014)

Concluding remarks

In this unit, we learned that networks are categorised by size and topology. They comprise nodes, transmission media, intra- and internetwork devices and protocols. Physical and logical topologies include client/server, peer-to-peer, point-to-point, point-to-multipoint, star, bus, ring, mesh and hybrid. The OSI model was also discussed. We learned that it is used to analyse network functions in layers (physical, data link, network, transport, session, presentation and application). It is important to be able to relate network hardware and protocols to the appropriate OSI layer. Lastly, we learned that the TCP/IP protocol suite is the basis of the Internet and is used for many LANs and private WANs. It uses a simpler four-layer model compared with OSI (link, Internet, transport application).

Self-assessment

Test your knowledge

1. Describe the functions of the layers of the OSI model.
2. Describe the functions of the layers of the TCP/IP suite.
3. Describe any three network topologies.
4. Distinguish between client/server and peer-to-peer networks.
5. Describe the concept ‘packet switching’.
Unit 2: Ethernet

Unit 2 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**  
LO1: Identify and explain networking principles and concepts.

**Assessment criteria**  
AC1.3: Describe the scope of IEEE 802 standards and the features of IEEE 802.3 (Ethernet).  
AC1.4: Describe the properties of MAC addressing and ARP.  
AC1.5: Discuss the use of packet sniffers/protocol analysers to capture and examine network traffic.  
AC1.6: Discuss the functions, features and configuration of a network adapter.

**Learning objectives**  
After studying this unit, you should be able to:  
- Understand the purpose and scope of IEEE 802 standards  
- Understand the properties of transmission media and data signalling  
- Describe the features of IEEE 802.3 (Ethernet)  
- Describe the properties of MAC addressing and ARP  
- Select, install and configure a network adapter  
- Understand the use of packet sniffers/protocol analysers to capture and examine network traffic

**Supplementary reading**  
**Unit 2 adapted from:**  
Introduction
Over the years, a number of protocols, standards and products have been developed for technologies that work at the physical and data link layers of the OSI model. The most important of these are the Institute of Electrical and Electronics Engineers (IEEE) 802 Standards, published by the LAN/MAN Standards Committee of the IEEE.

2.1 IEEE 802 Standards

2.1.1 IEEE 802.2 (logical link control)
The IEEE 802.2 Standards divide the data link layer of the OSI model into two sub-layers, called the Logical Link Control (LLC) and the Media Access Control (MAC), as discussed in Unit 1. The LLC is used with other protocols, such as 802.3 and 802.11, which are conceived as operating at a MAC sub-layer and the physical layer. The LLC protocol provides error control, flow control and a standard network layer service interface, regardless of lower level protocols (GTSLearning, 2014).

2.1.2 IEEE 802.3 (Ethernet)
Ethernet is now the only widely supported standard for cabled LANs. IEEE 802.3 describes functions operating at the MAC sub-layer (frame format, contention, addressing) and the physical layer (signalling and media specifications) (GTSLearning, 2014).
2.2 Media characteristics

Transmission media are the physical paths through which electromagnetic signals travel to allow nodes to communicate with one another. The transmission media used for a network can be classified as cabled or wireless. In terms of cable, there are those that use electrical (unshielded twisted pair) and those that use light (fibre optic) to transmit information. In terms of wireless, microwave or radio links are used (GTSLearning, 2014).

2.2.1 Signalling

A signal can be either analogue or digital. The figure below provides a representation of the two forms of signals.

![Figure 21: View of digital and analogue signals](Source: GTSLearning (2014))

An analogue signal is characterised by a continually changing wave, while the digital signal is a signal that is in a discrete state. Digital signals are transmitted as a series of pulses. When used for computer networking, both types of signals can be used to represent binary information. Digital signalling is better suited to transmitting this type of data, as it is easier to convert from the data to the signal and back again, and the conversion process suffers fewer errors from noise and interference. Analogue signalling is used by computer modems that are connecting over the telephone network (GTSLearning, 2014).
2.2.1.1 Bandwidth
The bandwidth of transmission media is the range of frequencies supported, measured in hertz. Two ways of allocating bandwidth in a transmission medium are:

- **Baseband transmission**: uses complete bandwidth of the media as a single transmission path
- **Broadband transmission**: can divide the available media bandwidth into a number of transmission paths

The term ‘bandwidth’ is also used to describe the amount of data that can be transferred through the media in a given amount of time, which is bit rate or speed (GTSLearning, 2014).

2.2.1.2 Signalling speed
Signalling speed is the rate at which information is sent over the media, measured in MHz (millions of clock cycles per second) (GTSLearning, 2014).

2.2.1.3 Digital encoding
An encoding scheme is applied to convert the binary data into representative electromagnetic signals. A symbol is some property of the signalling system that can be used to represent a value. One of the critical problems of encoding digital signals is that of bit timing (GTSLearning, 2014).

2.2.1.4 Distance
Each media type can support a given data rate over a defined distance, only. **Attenuation** and **noise** affect the maximum supported distance of a specific media type. Attenuation is the progressive loss of signal strength, measured in decibels (dB). Noise is anything that is transmitted within, or close to, the medium that is not the intended signal (GTSLearning, 2014).

2.3 Media Access Control (MAC)
Media Access Control (MAC) is the methodology used to determine when devices are allowed to communicate using the network.

2.3.1 Contention and collision domains
In a contention-based system, each network device within the same collision domain competes with the other connected devices for use of the transmission media. The contention protocols are called Carrier Sense Multiple Access (CSMA) protocols. There are two types of CSMA protocols. These are: **CSMA/CD (with Collision Detection)** and **CSMA/CA (with Collision Avoidance)** (GTSLearning, 2014).
2.3.2 Switched networks
Contention-based access methods do not scale to large numbers of nodes within the same collision domain. This problem is overcome by using switches as intranetworking devices. Using a switch means that each port is in a separate collision domain (GTSLearning, 2014).

2.3.3 Half duplex, full duplex and bonding
The term ‘half duplex transmissions’ is used to refer to a device that can transmit or receive, but cannot do both at the same time. ‘Full duplex’ means that a device can transmit and receive simultaneously. ‘Bonding’ refers to aggregating multiple links into a single high-speed connection (GTSLearning, 2014).

2.3.4 Broadcast
When transmitting signals, it is useful to have a mechanism to transmit the same signal to multiple nodes. ‘Broadcast traffic’ refers to signals sent to all of the nodes within the same area (broadcast domain). Conversely, signals intended for receipt by a single node are called unicast (GTSLearning, 2014).

2.4 Ethernet (IEEE 802.3)
Ethernet was first used commercially by DEC, Intel and Xerox (DIX) in the late 1970s. It was standardised by IEEE as 802.3 in 1983. Ethernet uses a logical bus topology wired as a star topology, baseband signalling and CSMA/CD method for MAC (GTSLearning, 2014).

2.4.1 Ethernet frames
The basic format of an Ethernet frame is shown in Table 1 below:

<table>
<thead>
<tr>
<th>Table 1: Construction of an Ethernet frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)

2.5 Ethernet media specifications
Ethernet media specifications are named using a three-part convention. This describes:
- The data rate (Mbps)
- The signal mode (baseband or broadband)
- A designator for the media type
### 2.5.1 10 BASE-T

'10 Base-T' denotes an implementation that works at 10 Mbps, uses a baseband signal and uses twisted-pair cabling. 10 Base-T network systems use 4-pair unshielded or shielded twisted-pair copper wire cabling. A pair consists of two insulated wires wrapped around one another. One pair is used to transmit and one pair to receive, while the other two pairs reduce crosstalk and interference. With compatible network adapters and switches, 10 Base-T supports full duplex operation (hub-based Ethernet supports half-duplex only) (GTSLearning, 2014).

### 2.5.2 Fast Ethernet (802.3u)

This is based on the same CSMA/CD protocols that define traditional Ethernet, but it reduces the duration of time that each bit is transmitted by a factor of ten, by using higher frequency signals and improved encoding methods. This raises the packet speed from 10 Mbps to 100 Mbps. Fast Ethernet allows only one or two hubs, though this does not apply if the hubs are stacked using a proprietary backplane. It also introduced autonegotiation protocol to allow devices to choose the highest supported connection parameters. Fast Ethernet codes a 16-bit data packet into a signal which advertises its service capabilities. This is called Fast Link Pulse (FLP) (GTSLearning, 2014).

### 2.5.3 Gigabit Ethernet

This builds on the standards defined for Ethernet and Fast Ethernet. The speed that can be used is 10 times that of Fast Ethernet. In June 1998, the IEEE approved the Gigabit Ethernet standard over fibre (LX and SX) and shielded copper (CX) as IEEE 802.3z. The various fibre standards are collectively called 1000Base-X. The following year, the IEEE approved 1000Base-T, a standard using Cat 5e or Cat 6 copper wiring. This is defined in IEEE 802.3ab (GTSLearning, 2014).

### 2.5.4 10G (Gigabit) Ethernet

This multiplies the nominal speed of Gigabit Ethernet by a factor of 10. 10G is not deployed in many office networks, as the cost of the equipment is high. The major applications of 10G Ethernet are:

- Increasing bandwidth for server interconnections and network backbones
- Replacing existing switched public data networks based on proprietary technologies with simpler Ethernet switches

10G Ethernet is standardised under a number of publications with letter designations (starting with 802.3ae), which are periodically collated. 10G works only with switches in full duplex mode (GTSLearning, 2014).
2.6 MAC addressing

Each Ethernet network adapter has a unique hardware address known as the MAC address. A MAC address typically consists of 48 binary digits (6 bytes). The format of the number differs depending on the system architecture. An Ethernet card address is often displayed as 12 digits of hexadecimal with colon or hyphen separators or no separators at all (for example, 00:60:8c:12:3a:bc or 00608c123abc). The IEEE gives each card manufacturer a range of numbers and they hard code every card produced with a unique number from their range. This is called the Burned In Address (BIA). The first six hex digits (3 bytes or octets) represent the manufacturer (the Organisationally Unique Identifier [OUI]); the last six digits are the serial number (GTSLearning, 2014).

2.6.1 Unicast and broadcast

A unicast transmission is a transmission in which the frame is directed to a single destination card. In shared Ethernet, all adapters receive the frame, but they ignore it if it is not addressed to them. In a switched Ethernet, however, only the destination card receives the frame (GTSLearning, 2014).

A broadcast transmission is a transmission in which the frame is directed at every card in the same broadcast domain. The computer broadcasting the data uses the MAC address ff:ff:ff:ff:ff:ff. See Figure 22 below:

![Figure 22: Checking the destination of a frame](source: GTSLearning (2014))
In Figure 22 above, Computer A sends a frame of data to Computer B. Computer B recognises its own MAC address and copies the frame for processing. Computers C and D ignore the frame, as the destination address does not match their own. This type of communication is called **unicast**, as there is a single destination card (GTSLearning, 2014).

### 2.7 Address Resolution Protocol (ARP)

The TCP/IP suite includes the Address Resolution Protocol (ARP) to perform the task of resolving an IP address to a hardware address.

#### 2.7.1 Local address resolution

1. Once it is determined that an IP address is a local address, the source host checks its ARP cache for the required hardware address of the destination host.
2. If not present in the cache, the ARP builds a request, which is then broadcast onto the network.

*Figure 23: Local address resolution*

Source: GTSLearning (2014)
3. The broadcast is processed by all the hosts on the local network (or subnet), but unless the request contains its own IP address, most hosts ignore the request.
4. If the target host recognises its own address, it updates its cache with the MAC address of the source host. It then replies to the source host.
5. The source host receives the reply, updates its cache table and communication is established.

(GTSLearning, 2014)

2.7.2 Remote address resolution

If the host is on a remote network, then the local host must use a router (for default gateway) to forward the packet. Therefore, it must determine the MAC address of the gateway using ARP (GTSLearning, 2014).

1. The sending host determines the IP address of the default gateway (router). The host then examines its ARP cache for the necessary IP address/MAC address mapping of the gateway.
2. If the mapping for the gateway address is not located, then an ARP request is broadcast for the default gateway’s IP address.
3. Hopefully, the router will respond to the request by returning its hardware address. The sending host then sends the packet to the default gateway to deliver to the remote network and the destination host.

Figure 24: Remote address resolution

Source: GTSLearning (2014)
4. At the router, IP determines whether the destination is local or remote. If local, it uses ARP for the address resolution. If remote, it checks its route table for an appropriate gateway to the remote network. (GTSLearning, 2014)

2.7.3 Optimising address resolution
ARP broadcasts can generate traffic on a network, which can reduce performance. To optimise this process, the results of an ARP broadcast are initially held in a cache. If the entry is used within the timeout period, the entry is held in the cache for a few minutes before it is deleted. The cache is an area reserved in memory that contains the IP address and the associated hardware address (GTSLearning, 2014).

2.7.4 ARP
The ARP utility can be used to perform a number of functions related to the ARP cache, such as:
- `arp -a` or `arp -g` views the ARP cache contents. Use with `IPAddress` to view the ARP cache for the specified interface, only.
- `arp -s IPAddress MACAddress` adds an entry to the ARP cache. Under Windows, `MACAddress` needs to be entered, using hyphens between each hex byte.
- `arp -d *` deletes all entries in the ARP cache; can also be used with `IPAddress` to delete one entry, only.

2.7.5 Reverse Address Resolution Protocol (RARP)
The Reverse Address Resolution Protocol (RARP) resolves an IP address from a given MAC address.

2.8 Network adapters
The component responsible for physically connecting the node to the transmission medium is known as the network adapter, network adapter card or Network Interface Card/Controller (NIC). This device is responsible for moving data from the computer to the network, and also from the network to the computer (GTSLearning, 2014).
2.8.1 Function of a network adapter

The following occur when a network card transmits data:

- The data arrives at the network card via the computer’s **Input/Output (I/O) bus**. The card’s **driver** handles communications between data processed on the card and the Operating System’s (OS’s) protocol stack. Card drivers are usually based on one of two standard Application Programming Interfaces (API): Network Driver Interface Specification (NDIS) or Open Data Link Interface (ODI).
- The data is placed in the **buffer** where it can be stored if a bottleneck builds up because the network card is unable to process the data quickly enough.
- The **transceiver** converts the bit stream used by the computer to the required format for the transmission media.
- The media connector physically joins the network card to the transmission media to allow the data to depart.

The other function performed by the network card is **addressing** data to other network cards and recognising data destined for it (GTSLearning, 2014).

2.8.2 Features of network adapters

The following represent the main features that differentiate the different models of network adapters:

- Network support
- Form factor
- Multi-port NICs
• TCP Offload Engine (TOE)
• Parallellisation and virtualisation support
• SNMP agent
• Remote booting

(GTSLearning, 2014)

2.8.3 Configuring a network adapter

Computer hardware devices need to use certain computer resources to function. These are generally the Interrupt Request Channel (IRQ), Input/Output Port (I/O Port) and Memory Address (GTSLearning, 2014).

Each Operating System provides a method for installing and configuring devices. Generally, this takes place as part of the setup process for the Operating System, but it is also possible to add drivers once the system has been installed (GTSLearning, 2014).

2.8.3.1 Software configuration

Plug-and-Play compliant cards will install and configure themselves. If necessary, resources can be configured manually using Device Manager (or the equivalent) (GTSLearning, 2014).

2.8.3.2 Vendor configuration

Some older network cards which do not support Plug-and-Play configuration will need to be configured using drivers from a vendor-supplied utility disk (GTSLearning, 2014).

2.8.3.3 Hardware configuration

Some very old network adapters support configuration via switches and jumpers on the NIC. It is unlikely that you will encounter many of these.

2.8.4 Protocol analyser

A protocol analyser (or packet sniffer or network analyser) performs packet capture and analysis. The analyser can be implemented on special hardware or installed as software on a PC host. Protocol analysers can decode a captured frame to reveal its content in a readable format. The capabilities of different products vary widely but, in general terms, protocol analysers can perform the following functions:

• Identify the most active computers on the network
• Isolate computers producing erroneous packets and rectify the problem
• Filter traffic and capture packets meeting certain criteria
• Baselining
- Generate frames and transmit them onto the network to test network devices and cabling
- Monitor bandwidth usage by hosts, applications and protocols
- Trigger alarms when certain network conditions fall outside ‘normal levels’

(GTSLearning, 2014)

2.8.4.1 Promiscuous mode and sniffing switched Ethernet

By default, a network card can only receive packets that are directed to that card or broadcast messages. Most packet sniffers can make a network adapter work in promiscuous mode, so that it receives all traffic within the Ethernet broadcast domain, whether it is intended for the host machine or not (GTSLearning, 2014).
Concluding remarks
In this unit, we discussed the different LAN products based on IEEE 802.3 (Ethernet). We also discussed MAC addresses and their format, and the functions and features of network adapters. Finally, we determined that protocol analysers, such as Wireshark, allow for the capture and analysis of frames sent to, and received by, a network node.

Self-assessment

Test your knowledge

1. What is attenuation?

2. Describe how the two contention protocols work.

3. Describe the functions of a network adapter.

4. Describe the functions of a protocol analyser.

5. Describe the features of network adapters.

6. Distinguish between analogue and digital signals.
Unit 3: Cabling and connectors

Unit 3 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO2: Discuss the role, purpose and specifications of key networking components.

**Assessment criteria**
AC2.1: Describe the types and properties of different cables and connectors.
AC2.2: Describe the use of repeaters and media converters.

**Learning objectives**
After studying this unit, you should be able to:
- Describe the types and properties of different cables and connectors:
  - Twisted pair
  - Coax
  - Fibre optic
  - Serial
- Understand the use of wiring standards when selecting cable for different applications
- Understand the use of repeaters and media converters

**Supplementary reading**

**Unit 3 adapted from:**
Introduction
When designing a network, one important component is network cable. This unit will discuss the different network cables that are available, and how to use wiring standards when selecting a network cable for different applications. The use of different types of cable connectors will also be discussed. In addition, the functionalities of repeaters and media converters will be analysed in this unit.

3.1 Selecting network cable
When selecting a suitable media for a network, the following should be considered:
- Cost
- Ease of installation
- Transmission speed
- Duplex
- Distance
- Noise immunity
- Security

(GTSLearning, 2014)

3.2 Twisted pair cable (Unshielded Twisted Pair/Shielded Twisted Pair/Screened Twisted Pair)
Twisted pair is a type of copper cable that has been extensively used for telephone systems and data networks. One pair of insulated wires twisted together forms a twisted pair and two or four twisted pairs form a twisted pair cable. The pairs are twisted to reduce external interference and crosstalk. **Crosstalk** is a phenomenon whereby one wire causes interference in another as a result of their close proximity (GTSLearning, 2014).

3.2.1 Unshielded Twisted Pair (UTP)
Most twisted pair cable which is used is Unshielded Twisted Pair (UTP). The reason for this is that it is used in many telephone systems. Modern buildings are often ‘flood-wired’ using this cabling. This involves laying cabling to every location in the building that may need to support a telephone or computer. These cables can then be used for either the telephone system or the data network (GTSLearning, 2014).
3.2.2 Shielded Twisted Pair (STP)
Each pair was surrounded by a braided shield. This shielding (around each pair) and/or screening (around all pairs) reduces interference. Shielded Twisted Pair (STP) was used in old Token Ring networks, but it is also a generic term for any type of screening/shielding. Screened cable is usually designated as ScTP or F/UTP or FTP. Modern fully screened and shielded cable is referred to as S/FTP (GTSLearning, 2014).

3.2.3 Twisted pair cabling connectors (RJ-45/RJ-11)
Twisted pair cabling uses RJ-45 and RJ-11 connectors. RJ stands for Registered Jack.

RJ-45 connectors are used with 4-pair (8 wire) cables. The connectors are also referred to as 8P8C, referring to: 8-position/8-contact. This means that all eight ‘potential’ wire positions are supplied with contacts, so that they can all carry signals if needed. RJ-45 is used for Ethernet twisted-pair cabling (GTSLearning, 2014).
The smaller RJ-11 connectors are used with 2- or 3-pair UTP. Typically, only one pair carries the dial tone and voice circuit. The other pair is usually unused, but can be deployed for a secondary circuit. RJ-11 connectors are used for telephone systems (GTSLearning, 2014).

3.2.4 TIA/EIA CAT standards
The American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) have created categories for UTP to simplify selection of a suitable quality cable. Table 2, below, shows the different categories for UTP.
### Table 2: TIA/EIA CAT standards

<table>
<thead>
<tr>
<th>Cat</th>
<th>Frequency (MHz)</th>
<th>Capacity (Mbps)</th>
<th>Maximum distance</th>
<th>Network application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>–</td>
<td>1</td>
<td>–</td>
<td>Voice only</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
<td>10</td>
<td>100 m (328 ft)</td>
<td>10BASE-T (Ethernet)</td>
</tr>
<tr>
<td>5</td>
<td>100</td>
<td>100</td>
<td>100 m (328 ft)</td>
<td>100BASE-TX (Fast Ethernet)</td>
</tr>
<tr>
<td>5e</td>
<td>100</td>
<td>1000</td>
<td>100 m (328 ft)</td>
<td>1000BASE-T (Gigabit Ethernet)</td>
</tr>
<tr>
<td>6</td>
<td>250</td>
<td>1000+</td>
<td>100 m (328 ft)</td>
<td>1000BASE-T (Gigabit Ethernet)</td>
</tr>
<tr>
<td>6A</td>
<td>500</td>
<td>10 Gbps</td>
<td>100 m (328 ft)</td>
<td>10BASE-T (10G Ethernet)</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)

### 3.2.5 Advantages of twisted pair cabling
- The use of telephone systems technology means that network reconfiguration is simple.
- It can be installed relatively easily.
- It is relatively inexpensive.
- It supports full-duplex signalling.

### 3.2.6 Disadvantages of twisted pair cabling
- Both UTP and STP formats suffer high attenuation levels.
- Twisted-pair is sensitive to Electromagnetic Interference (EMI) and eavesdropping, especially if unshielded.

### 3.3 Other copper cable types
UTP predominates in terms of modern networking applications, but a number of other copper wire cable and connector types are available (GTSLearning, 2014).

#### 3.3.1 Coaxial cable
Coaxial cable is made of two conductors that share the same axis. The core conductor of the cable is made of copper wire and is enclosed by plastic insulation. A wire mesh which serves both as shielding from EMI and as ground, surrounds the insulating material. A tough plastic sheath protects the cable. These cables are categorised using the Radio Grade (RG). In most cases, Bayonett-Neill-Concelman, British Naval Connector, or Barrel Nut Connector (BNC) connectors are crimped to the ends of the cable. Some coax installations use screw-down **F-connectors** (GTSLearning, 2014).
3.3.2 Serial cable

All network technologies transfer data in serial, but ‘serial cable’ generally refers to the original asynchronous serial transmission standard – one of the oldest and simplest in computing. ‘Asynchronous’ means that there are no timing signals. Each byte of data is identified by start and stop signals. The computer serial port is obsolete, but the use of a serial connection remains current in networking as a means of establishing an ‘out-of-band’ connection to the console port of a network appliance.
On older devices, the console port may be labelled the ‘management or admin’ port. The console port connection on the appliance can use either a DB-9/DB-25 port or standard RJ-45 jack. In this latter scenario, a console cable featuring an RJ-45 plug on one end and a 9-pin serial connector on the other is used for connection to the terminal (GTSLearning, 2014).

![Figure 34: Console cable](image)

Source: GTSLearning (2014)

### 3.4 Fibre-optic cable

Copper wire carries electrical signals, which are subject to interference and attenuation. Fibre-optic cable uses pulses of infrared light for signalling, which are not susceptible to interference, cannot be intercepted and suffer far less from attenuation. Fibre-optic cabling supports much higher bandwidth and cable runs (GTSLearning, 2014).

A single optical fibre is constructed from three elements:
- Core
- Cladding
- Buffer
3.4.1 Categories of fibre cable
Fibre-optic cables are specified using the mode, composition (glass/plastic) and core cladding. The two main categories of fibre-optic cables are:
- Single-Mode (SMF or Monomode)
- Multimode (MMF)

3.4.2 Installation of fibre-optic cables
Fibre optic can be installed in a star topology with the use of a switch. Long-distance cables are typically laid as trunks or rings with repeaters or amplifiers between cable segments to strengthen the signal (GTSLearning, 2014).

3.4.3 Fibre-optic cable connectors
The different types of fibre-optic cable connectors are:

- **Straight Tip (ST):**
  - Push-and-twist locking mechanism

- **Ferrule Connector (FC):**
  - Screw-in attachment

- **Subscriber Connector (SC):**
  - Push/pull design attachment
  - Lucent or Local Connector (LC) is similar to SC, but is half the size

- **Mechanical Transfer Registered Jack (MTRJ):**
  - Small form-factor duplex connector with a snap-in design
3.4.4 Advantages of fibre-optic cable

- Immune to interference and eavesdropping
- Supports high bandwidths
- Low attenuation
- Can be used in hazardous conditions
- Smaller and lighter than copper cable
- Ideal for space-limited situations
- No requirement to reinstall the cable over the life of the building

(GTSLearning, 2014)

3.4.5 Disadvantages of fibre-optic cable

- Very expensive
- More difficult to install than twisted-pair for LAN applications

3.5 Repeaters

A repeater is used to amplify the signal and, consequently, extend the maximum allowable distance for a medium type. Repeaters can work either as amplifiers or as signal regenerators.

The main characteristics of repeaters are as follows:

- Repeaters work at the physical layer of the OSI model.
- All segments connected with a repeater must use the same access method; therefore, it is not possible to combine, for example, Ethernet and Asynchronous Transfer Mode (ATM) segments using a repeater. A repeater has no frame conversion capability.
- Repeaters are intranetwork connectivity devices and so segments that are connected by a repeater are treated as belonging to the same network and are in the same collision domain.
- A repeater has little intelligence.

(GTSLearning, 2014)

3.6 Media converters

Media converters are used to convert one cable type to another. These components alter the characteristics of one type of cable to match those of another. Media converters work at the physical layer of the OSI model (GTSLearning, 2014).

The following media conversions are typical:

- Single mode fibre to Ethernet
- Multimode fibre to Ethernet
- Fibre to coaxial
- Single mode to multimode fibre
Concluding remarks
In this unit, we discussed the different network cables and how wiring standards are used when selecting a network cable for different applications. Furthermore, the use of connectors for the different types of cable was discussed. The unit concluded with the characteristics and functions of repeaters and media converters.

Self-assessment

Test your knowledge

1. What is crosstalk?
2. Describe the principal characteristics of repeaters.
3. Distinguish between UTP and STP.
4. Identify the advantages and disadvantages of twisted pair cabling.
5. Describe the categories of fibre-optic cable.
6. Identify the advantages of fibre-optic cable.
Unit 4: Bridges and switches

Unit 4 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO2: Discuss the role, purpose and specifications of key networking components.

**Assessment criteria**
AC2.3: Examine the functionalities and characteristics of intranetworking components.
AC2.4: Describe the purposes and functions of VLANs and STP.

**Learning objectives**
After studying this unit, you should be able to:
- Install and configure intranetworking components:
  - Hubs
  - Bridges
  - Switches
- Describe the purposes and functions of VLANs
- Understand the use of STP to prevent switching loops

**Supplementary reading**

Unit 4 adapted from:
**Introduction**

In this unit we will be discussing hubs, switches and bridges. We will also investigate the purpose and functions of Virtual Local Area Networks (VLANs) as well as the use of Spanning Tree Protocol (STP).

### 4.1 Hubs

Hubs are the central point of connection for Ethernet segments configured in a star topology. A hub regenerates and transmits signals over all ports. All ports on a hub are in the same collision domain. Another name for a hub is multiport repeater or concentrator. Hubs work at the physical layer of the OSI model (GTSLearning, 2014).

![Figure 40: Hub](source: GTSLearning (2014))

### 4.2 Bridges

A bridge is a device that provides communications between two or more segments. A bridge extends the maximum distance of network, but it may also be used to segment the network and reduce traffic (GTSLearning, 2014).

#### 4.2.1 Features of bridges

- Bridges work at the data link layer since they need to understand the MAC addresses within frames.
- Most bridges are only able to link segments of the same type (e.g. Ethernet to Ethernet).
- Bridges can be used to link different cable types.
Bridges are legacy devices that are used to segment networks and reduce contention. Segments at either side of a bridge are in separate collision domains but the same broadcast domain (GTSLearning, 2014).

### 4.2.2 Bridge operation

A bridge works in the following manner:

1. Computer A sends a signal to Computer D. Note that the frame contains a source hardware address of MA and a destination hardware address of MD.
2. The bridge listens to all traffic on all attached segments and, consequently, receives the signal at Port 1.
3. The bridge reads the destination frame and, using its port address table, determines the port to which the network card with hardware address MD is attached. The bridge is able to locate the hardware address MD in its port: MAC address table and transmits the signal out of Port 2, only.
4. If no record of the hardware address exists or the frame is a broadcast or multicast, then the bridge forwards the frame to all segments, except the source segment.

(GTSLearning, 2014)
4.3 Switches

Ethernet networks implemented with a bus or hubs rely on a contention-based technology to access the network. Devices can only transmit on the network when it is free. As more devices are added to the network, there is a greater chance of collisions. This problem can be overcome by moving from a ‘shared Ethernet’ system to ‘switched Ethernet. This involves the replacement of hubs and bridges with switches (GTSLearning, 2014).

![Figure 42: HP ProCurve 24-port switch](source: GTSLearning (2014))

4.3.1 Switch operation

A switch performs the same sort of function as a bridge, but can provide many more ports. Each port is a separate collision domain. In effect, the switch establishes a point-to-point link between any two nodes. This is called **microsegmentation**. The basic mode of operation for a switch is called ‘store-and-forward’ (GTSLearning, 2014). This works as follows:

![Figure 43: Switch operation](source: GTSLearning (2014))
1. Computer A transmits a frame intended for Computer B.
2. The switch receives the frame into a port buffer and obtains the destination MAC address from the Ethernet frame. The port buffer holds frames until they can be processed. The switch can also perform error checking on the frame, using Cyclic Redundancy Check (CRC).
3. The switch uses its MAC address table to look up the port connected to the destination MAC address.
4. The switch uses its high-speed backplane to send the frame out on Port 3 for Computer B to receive.
5. None of the other connected devices see any activity on the network while this process takes place. Therefore, these other devices are able to transmit and receive at the same time.

A switched network means that each port is in a separate collision domain. Collisions can only occur if the port is operating in a half-duplex mode and, even then, collisions only affect the segment between the port and that adapter (GTSLearning, 2014).

### 4.3.2 Building the MAC address table

If a MAC address cannot be found in the MAC address table, then the switch acts like a hub and transmits the frame out of all the ports (except for the incoming port). This is called **flooding** (GTSLearning, 2014).

The switch builds the MAC address table by analysing incoming frames for a source MAC address. It can then add a MAC address entry against the particular port number. Entries remain in the table for a period before being flushed. The address table is implemented as Content Addressable Memory (CAM), a special type of memory optimised for searching rather than random access (GTSLearning, 2014).

### 4.3.3 Switch models

Different models of switches exist with different ports. The market is dominated by Cisco’s Catalyst Series, but other notable vendors include HP (ProCurve), Nortel, Foundry and 3Com (GTSLearning, 2014).

### 4.3.4 Configuring a switch

Some switches, such as unmanaged switches, do not offer any configuration options or interface. Managed switches often support more complex functions, including configuring VLANs, port authentication, load balancing, Quality of Service (QoS), traffic shaping and filtering. These functions can be accessed via the switch’s management interface (GTSLearning, 2014).
A switch may support the following interfaces:
- Console port
- Management port
- Simple Network Management Protocol (SNMP)

A switch may also support autoconfiguration using a Dynamic Host Configuration Protocol (DHCP) server to obtain addressing information and a Trivial File Transfer Protocol (TFTP).

4.3.5 Autonegotiation

Switches usually support a range of Ethernet standards so that older and newer network adapters can all be connected to the same network. In most cases, the port on the switch is set to autonegotiate speed and full or half duplex operation, but a static configuration can be applied manually if necessary (GTSLearning, 2014).

4.3.6 Diagnostics

Most managed switches will provide diagnostic information through the management interface, as seen in Figure 45 below.
4.3.7 MAC address filtering

MAC filtering means specifying which MAC addresses are allowed to connect to a particular port. This can be done by specifying a list of valid MAC addresses, but this ‘static’ method is difficult to keep up to date and is relatively error-prone (GTSLearning, 2014).

4.3.8 Port mirroring

Switch does not allow sniffing across ports. Port mirroring copies all packets sent to one or more source ports to a mirror (destination) port. On a Cisco switch, this is called Switched Port Analyser (SPAN). The mirror port would be used by network analyser or Intrusion Detection System (IDS) (GTSLearning, 2014).
4.3.9 Power over Ethernet (PoE)

Power over Ethernet (PoE) supplies electrical power to devices over Ethernet cable. PoE is suitable for IP phones, wireless access points, thin clients and so on.

PoE is defined in two IEEE standards:
- **802.3af**: Powered devices can draw up to about 13W over the link.
- **802.3at (PoE+)**: Powered devices can draw up to about 25W over the link.

PoE switches are referred to as Power Sourcing Equipment (PSE). If an existing switch does not support PoE, a device called a **power injector** can be used (GTSLearning, 2014).

4.4 Virtual LANs (VLAN)

‘Virtual LAN’ simply means that through the use of switching technologies, different groups of computers on the same cabling can appear to be in different LANs, creating two or more VLANs (GTSLearning, 2014).

Benefits of VLANs include: traffic management, improved performance and security. A VLAN is described as a separate broadcast segment. A busy segment can be broken into two distinct groups, each chatting amongst themselves. The separation of these groups into separate VLANs will reduce the impact of each group’s traffic on the other group (GTSLearning, 2014).

In Figure 47, for example, ports 1 through 10 and 11 through 20 could be configured as two separate VLANs, typically each with their own subnet address.
VLANs are defined by the IEEE 802.1Q standard. Under 802.1Q, traffic is defined by a VLAN tag inserted in the Ethernet frame between the source address and Ethertype fields. The tag contains information about the VLAN ID and priority. The Ethertype value is set to identify the frame as 802.1Q (GTSLearning, 2014).
### Table 3: Construction of an 802.1Q Ethernet frame

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination MAC</th>
<th>Source MAC</th>
<th>802.1Q Tag</th>
<th>Length/type</th>
<th>Payload</th>
<th>CRC</th>
</tr>
</thead>
</table>

Source: GTSLearning (2014)

#### 4.4.1 VLAN trunking protocol

The interconnections between switches are referred to as trunks. When VLANs are also configured on the switches, trunking means that a VLAN can be configured across more than one switch device without having to manually configure the VLANs on each device. The protocol governing this data exchange would either be Cisco’s VLAN Trunking Protocol (VTP), Generic Attribute Registration Protocol (GARP) or VLAN Registration Protocol (GVRP) (GTSLearning, 2014).

Under VTP, switches can be grouped into management domains, identified by a domain name. Within these groups, switches are assigned the roles of either VTP server or VTP client.

‘Pruning’ refers to removing broadcasts related to particular VLANs from a trunk to preserve bandwidth (GTSLearning, 2014).

#### 4.4.2 Spanning Tree Protocol (STP)

Multiple paths between switches (or bridges) provides fault tolerance, but if there are multiple paths between switches, broadcast traffic can loop and be rebroadcast by each switch. STP prevents switching loops by designating a single active path from any one device to the one designated as the root bridge. STP is defined in the 802.1D MAC Bridges standard. This is a means for the bridges to organise themselves into a hierarchy. The bridge at the top of the hierarchy is the root bridge. STP is now more likely to be implemented as 802.1D-2004/802.1W or Rapid STP (RSTP). The rapid version creates outages of a few seconds or less. In RSTP, the blocking, listening and disabled states are aggregated into a discarding state (GTSLearning, 2014).

Where VLANs are implemented, a modified version of STP must be used. If a trunk port to multiple VLANs were to be blocked, all the VLANs on that trunk would be denied access to the rest of the network. Some means must be established to disable links on a per-VLAN basis. Originally, this was accomplished using Cisco’s Per-VLAN STP Protocol (PVST), but it is now implemented using Multiple Spanning Tree Protocol (MSTP), defined in 802.1Q (GTSLearning, 2014).

### Concluding remarks

In this unit, we learned that hubs are legacy devices that are used as the network concentrator to implement a star topology. We also learned that
bridges can be deployed with hubs to divide a network into smaller collision domains, reducing the effect of contention. Hubs and bridges have been replaced by Layer 2 switches to eliminate the effect of collisions. VLANs can be used to aggregate and sub-divide networks into a different logical topology.

Self-assessment

Test your knowledge

1. What is PoE?
2. What is the function of STP?
3. What methods can be used to allocate a particular host to a VLAN?
4. How do bridges operate?
5. How do switches operate?
Unit 5: Internet protocol

Unit 5 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO3: Discuss the functions and features of TCP/IP addressing, protocols and services.

**Assessment criteria**
AC3.1: Describe the format of IP addresses and datagrams, and the operation of subnet mask and the basics of IP routing.
AC3.2: Configure TCP/IP on Windows and Linux hosts.
AC3.3: Describe the operation of ICMP and related troubleshooting and configuration utilities.

**Learning objectives**
After studying this unit, you should be able to:
- Describe the format of IP addresses and datagrams
- Understand the operation of a subnet mask and the basics of IP routing
- Configure TCP/IP on Windows and Linux hosts
- Describe the operation of ICMP and related troubleshooting and configuration utilities

**Supplementary reading**
Unit 5 adapted from:

**Introduction**
At the network layer, the Internet Protocol (IP) provides packet addressing and routing for all higher level protocols within the TCP/IP suite. It provides best-effort delivery of an unreliable and connectionless nature.
The two main versions of IP are versions 4 and 6. IPv4 is currently in widespread use, but IPv6 provides a much larger address space.

5.1 Datagram structure

IP datagrams encapsulate data from the transparent layer, adding a number of fields.

![Figure 49: IP datagram](source: GTSLearning (2014))

5.2 IP addresses

At the TCP/IP Internet layer of the OSI model, a unique number, known as an IP address, is used to identify each host. The IP address provides two pieces of information (GTSLearning, 2014):
- The network ID
- The host ID

An IP address is 32 bits long and is used within an IP packet to define the source and destination of the packet. IP addresses are usually displayed in dotted decimal notation. This notation requires each octet to be converted to a decimal value. The decimal numbers are separated using a period (example of an IPv4 address is 192.16.1.1) (GTSLearning, 2014).
5.2.1 Converting between binary and decimal format

Binary to decimal conversion
Convert the octet 10110101 into its equivalent decimal number.

\[
\begin{array}{cccccccc}
128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
\hline
128 \times 1 & 64 \times 0 & 32 \times 1 & 16 \times 1 & 8 \times 0 & 4 \times 1 & 2 \times 0 & 1 \times 1 \\
\end{array}
\]

The decimal number is equal to:
\[128 + 0 + 32 + 16 + 4 + 0 + 1 = 181\]

5.2.1 Decimal to binary conversion
Convert the decimal number 199 into its equivalent binary number.

\[
\begin{array}{cccccccc}
128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\
128 \times 1 & 64 \times 1 & 32 \times 0 & 16 \times 0 & 8 \times 0 & 4 \times 1 & 2 \times 1 & 1 \times 1 \\
\hline
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
\end{array}
\]

The binary number is 11000111.

5.3 Subnet masks
An IP address consists of a network ID and host ID. A subnet mask is applied to identify the network and host portions within a single IP address (GTSLearning, 2014).

‘Default’ masks are used to refer to old IP address classes. The default subnet masks for each of the main IP address classes are shown in Figure 52 below.
5.3.1 ANDing

To work out a network ID, given an address and mask in decimal, convert to binary and back, as shown in Figure 53 below.

<table>
<thead>
<tr>
<th>Source IP (172.30.15.12)</th>
<th>10101100</th>
<th>00011110</th>
<th>00001111</th>
<th>00001100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask (255.255.0.0)</td>
<td>11111111</td>
<td>11111111</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>Destination IP (172.31.16.101)</td>
<td>10101100</td>
<td>00011111</td>
<td>00010000</td>
<td>01100101</td>
</tr>
<tr>
<td>IP address (172.30.15.12)</td>
<td>10101100</td>
<td>00011110</td>
<td>00001111</td>
<td>00001100</td>
</tr>
<tr>
<td>Mask (255.255.0.0)</td>
<td>11111111</td>
<td>11111111</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>Network ID (172.30.0.0)</td>
<td>10101100</td>
<td>00011110</td>
<td>00000000</td>
<td>00000000</td>
</tr>
</tbody>
</table>
5.4 Configuring TCP/IP

An IP address that is unique on the internetwork to which the host is attached and a subnet mask is the minimum information required for the configuration of the TCP/IP protocol. If the host has more than one network interface, then each must be configured with a unique IP address and a subnet mask. A default gateway (router) address must be provided if the host is required to communicate with remote networks (GTSLearning, 2014).

5.4.1 Configuring TCP/IP under Windows

TCP/IP can be configured in Windows either by using automatic address configuration or static configuration.

![Figure 54: Configuring IP](source: GTSLearning (2014))
5.4.2 Configuring TCP/IP under Linux

In Linux you can either use a graphical utility to configure the adapter, set the values in a configuration file, or use the command-line tool `ifconfig`.

![Figure 55: Configuring DNS suffix](image)

Source: GTSLearning (2014)

![Figure 56: Using Yet another Setup Tool (YaST) to configure the network in SUSE Linux Enterprise Server](image)

Source: GTSLearning (2014)
5.5 ipconfig/ifconfig

The `ipconfig` program is used to verify TCP/IP configuration on Windows-based systems.

![Figure 57: Using ipconfig](Source: GTSLearning (2014))

UNIX and Linux hosts provide a command called `ifconfig`, which provides similar output to the `ipconfig` program of Windows.

![Figure 58: Using ifconfig](Source: GTSLearning (2014))
5.6 IP routing basics

The default gateway is the IP address of a router on the same subnet as the host. Messages destined for other subnets are sent to the default gateway address by the source host.

When a message is sent using IP, the following steps occur:
- The IP will attempt to establish a connection with the destination host by IP address.
- The destination network address is compared with that of the source.
- It is possible that, due to limitations in the underlying network, IP may fragment the packet into more manageable pieces.
- IP then calculates a checksum (to use for error detection) and sends the packet. A data link protocol (such as Ethernet) encapsulates this into one or more frames and transmits them over the network.
- If the datagram has been routed, at the gateway, the Time to Live (TTL) is decreased by at least one. This could be greater if the router is congested. When TTL is zero, the packet is discarded. This prevents badly addressed packets from permanently circulating the network.
- The router then determines what to do with the datagram by repeating the steps described from the second step onwards. If the message is destined for yet another network, the process is repeated to take it to the next stage, and so on.

(GTSLearning, 2014)

Routes to other subnets can be manually configured or learned by a routing protocol. Discovered routes are held in a routing table.

5.7 Internet Control Message Protocol (ICMP) and Ping

The Internet Control Message Protocol (ICMP) is used to report errors and send messages about the delivery of a packet. It can also be used to test TCP/IP networks (GTSLearning, 2014).

5.7.1 ICMP header

An ICMP message is encapsulated within a single IP datagram. The fields of an ICMP message are:
- Code
- Checksum
- ID/Sequence
- Address
- Data

(GTSLearning, 2014)
5.7.2 ICMP error types
ICMP messages are grouped into different types. The most commonly encountered are:
- Echo request/reply
- Destination unreachable
- Time exceeded
- Source quench
- Redirect

(GTSLearning, 2014)

5.7.3 Ping
The Ping program sends a configurable number and size of packets to a destination host. The packet contains ICMP data. The Ping utility can be used to provide essential information when troubleshooting a TCP/IP network (GTSLearning, 2014).

![Figure 59: Troubleshooting with Ping](Source: GTSLearning (2014))

5.7.3.1 Interpreting Ping output
- Reply from, round trip time and packet loss:
  - Detect whether a link is slow or experiences packet loss
  - Use tracert to identify where on the route there is a problem
• Destination unreachable:
  o No route to host
  o Check IP configuration
  o Check router (default gateway)
• No reply/timed out:
  o Host/interface is down
  o Host cannot route reply
  o Firewall has been implemented

(GTSLearning, 2014)

Concluding remarks
The Internet Protocol (IP) provides Layer 3 addressing, allowing for logically distinct networks. IPv4 clients are configured with an IP address and subnet mask; the subnet mask defines the network and host ID portions of the IP address. A Windows host is configured via network connection properties while Linux hosts use ifconfig and route. Ipconfig/ifconfig is used for various troubleshooting and configuration tasks; there are differences between Windows and Linux versions. ICMP delivers a status message and allows for connectivity testing (Ping utility).

Self-assessment

Test your knowledge

1. Once installed, how would you check the TCP/IP configuration?

2. On a UNIX host, which TCP/IP parameters must be defined for routing to be able to take place?

3. Describe the ICMP error types.

4. Describe the fields of an IP datagram.

5. Identify the two pieces of information provided by an IP address.
Unit 6: Addressing schemes

Unit 6 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO3: Discuss the functions and features of TCP/IP addressing, protocols and services.

**Assessment criteria**
AC3.4: Discuss IP addressing schemes, including address classes, address ranges in private networks, configuring an IP address scheme for a private network, subnetting and classful addressing.

**Learning objectives**
After studying this unit, you should be able to:
- Understand IP addressing schemes, including address classes, subnetting and classless addressing (supernetting)
- Identify address ranges for private networks
- Configure an IP address scheme for a private network

**Supplementary reading**

Unit 6 adapted from:
**Introduction**

As described in Unit 5, the combination of an IP address and subnet mask can be used to describe network ID and a host ID. Addressing schemes describe different ways of configuring IP addressing to suit different types and sizes of networks.

### 6.1 Addressing schemes

Addressing schemes describe different ways of configuring IP addressing to suit different types and sizes of networks (GTSLearning, 2014).

#### 6.1.1 Broadcast, multicast and unicast

- **Unicast** is when an IPv4 host sends a packet to another single host (or destination host). This is a one-to-one approach.
- **Broadcast** is when the local host sends a packet to all hosts on the local subnetwork. This one-to-all approach.
- **Multicast** represents a group of computers, programmed to respond to a particular address. This is a many-to-many approach.

  (GTSLearning, 2014)

#### 6.1.2 Classful addressing

Classful addressing allocates a network ID based on the first octet of the IP address. The network IDs are divided into three classes, defining different sizes of networks (GTSLearning, 2014).
6.1.3 Class D and E addresses

Class D addresses are multicast addresses and range between 224.0.0.0 and 239.255.255.255.

Class E addresses are experimental/reserved addresses which range between 240.0.0.0 and 255.255.255.255.

6.1.4 Private addressing

A private network will typically use a private addressing scheme to allocate IP addresses to hosts.

Address ranges that are not routable over Internet:
- 10.0.0.0 to 10.255.255.255
- 169.254.0.0 to 169.254.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Hosts on the private network must use Network Address Translation (NAT) or proxy mechanisms to access the Internet (GTSLearning, 2014).
6.2 Creating subnets

Most organisations sub-divide their networks into different logical groups. These groups are called subnetworks or subnets. Organisations need to do this for the following reasons:

- Excessive broadcast traffic is created when there are more hosts on the same network.
- WAN links normally forms separate networks.
- It is useful to divide a network into logically distinct zones for security and administration

(GTSLearning, 2014)

6.2.1 Classful subnets

When working with classful addresses, the default subnet mask can be modified to allow a single network to be divided into a number of subnets. To do this, additional bits of the IP address have to be allocated to the network address rather than the host ID (GTSLearning, 2014).

![Figure 61: Internetwork addressing (Class B address)](source)

![Figure 62: Subnet addressing](source)

6.2.2 Classless subnets

In a classless addressing scheme, the network ID is determined not by the range into which the first octet of the IP address falls, but by the length of the network prefix. The network prefix can still be represented as a subnet mask. Alternatively, the prefix can be written in slash notation:

- \(/nn\) – number of bits in the mask. This is more compact and easy to understand.
• New (unofficial) meaning for address ‘classes’:
  o Class A network = /8
  o Class B network = /16
  o Class C network = /24

6.2.3 Planning an IP addressing scheme

Before choosing an addressing scheme, consider the following:
• Whether you need a public or private addressing scheme
• How many networks you need
• How many subnetworks you need
• How many hosts per subnet you need

Additional addressing rules to consider:
• Network ID cannot be 127
• Network and/or host IDs cannot be all 255 (all 1’s in binary)
• Network and/or host ID cannot be 0 (all zeros in binary)
• Host ID must be unique in the network
• Network ID must be unique on the Internet

The process of designing the scheme is as follows:
• Work out how many subnets are needed:
  o Must be a power of 2
  o Exponent (the value of ‘n’ in $2^n$) is the number of bits to add to the default network prefix
• Check that subnets allow for sufficient hosts ($2^n-2$ where ‘n’ is number of host bits).
• Work out the subnets – deduct the least significant octet in the mask from 256.
• Work out the next subnet ID, which will be the lowest subnet value higher.
• Work out the host ranges for each subnet:
  o Take the subnet address and add a binary 1 to it for the first host
  o Take the next subnet ID and deduct two binary digits from it

6.3 Public Internet addressing

When an organisation wants to connect to the Internet, it must apply for a range of public addresses via an Internet Service Provider (ISP) (GTSLearning, 2014).
6.3.1 Classful addressing

In the classful addressing system, an organisation was allocated a network address from a suitable class (A, B, C). Under this classful system, almost all Class B addresses became allocated. This shortage of network addresses prompted the development of IPv6, which uses 128-bit IP addresses. However, the deployment of IPv6 has been extremely delayed, so a series of stopgap measures have been introduced over the years. The earliest were the use of subnetting and private address ranges to hide the complexity of private local networks from the wider Internet. Another significant measure was the introduction of supernetting or Classless Interdomain Routing (CIDR) in 1993 (GTSLearning, 2014).

6.3.2 Supernetting

Supernetting allocates network bits for use as subnet/host bits. In supernetting, addresses must be adjacent blocks. Supernetting allows for a more flexible, hierarchical system of network addressing, with efficient routing between networks on the Internet. CIDR collapses entries into single network routing prefix for routers that are external to the network (GTSLearning, 2014).

![Figure 63: Supernetting](source: GTSLearning (2014))

Concluding remarks

IPv4 traffic can be unicast, broadcast or multicast. Classful addressing uses a system of fixed network IDs based on the first octet of the IP address. Variable length subnet masks allow for subnets and supernetting (CIDR). IPv4 provides public and private addressing schemes. Privately addressed hosts can use some type of NAT or proxy to communicate over the Internet.
Self-assessment

Test your knowledge

1. If a host is configured with the IP address 10.0.10.22 and a mask 255.255.255.192, what is the broadcast address of the subnet?

2. How many hosts/subnets would the addressing scheme in Question 1 support?

3. Distinguish between unicast, broadcast and multicast.

4. Identify the IP address classes and their address ranges.

5. Identify three reasons why organisations sub-divide their networks.
Unit 7 is aligned with the following learning outcome and assessment criterion:

**Learning outcome**
LO3: Discuss the functions and features of TCP/IP addressing, protocols and services.

**Assessment criterion**
AC3.5: Discuss the methods for auto-configuring IP addressing information (DHCP and APIPA), including configuration of DHCP server and the use of Network Time Protocol (NTP).

**Learning objectives**
After studying this unit, you should be able to:
- Understand methods for autoconfiguring IP addressing information (DHCP and APIPA)
- Configure a DHCP server
- Understand the use of Network Time Protocol (NTP) to synchronise system clocks across a network

**Supplementary reading**

Unit 7 adapted from:

**Introduction**
In this unit we will be discussing the different methods for autoconfiguring IP addressing information, as well as how to configure a DHCP server. At the end of the unit, we explore how to use Network Time Protocol (NTP) to synchronise system clocks across a network.
7.1 Static versus dynamic IP addressing

Originally, all the parameters required by TCP/IP were configured manually (static configuration). Every machine was allocated an appropriate IP address, a subnet mask and a default gateway (router) for its network. This type of configuration was complex (GTSLearning, 2014).

Over the years, several mechanisms have been employed to provide a client autoconfiguration service for TCP/IP.

7.1.1 BOOTP

One of the first autoconfiguration mechanisms was Reverse Address Resolution Protocol (RARP). This allows a host to obtain an IP address from a server configured with a static list of MAC:IP mappings (GTSLearning, 2014).

RARP can only be used to obtain an IP address, which is inadequate for most implementations of TCP/IP. Consequently, the Bootstrap Protocol (BOOTP) was developed as a means of supplying a full set of configuration parameters (IP address, subnet mask, default gateway, DNS addresses, and so on). The additional parameters are provided in an executable boot file downloaded to the host using Trivial File Transfer Protocol (TFTP) (GTSLearning, 2014).

The main problem with BOOTP is that it depends on a static configuration file mapping IP addresses to MAC addresses. This problem was addressed by the development of BOOTP into the Dynamic Host Configuration Protocol (DHCP) (GTSLearning, 2014).

7.1.2 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) assigns configurations to hosts dynamically. A host is configured to use DHCP by specifying in the TCP/IP configuration that it should automatically obtain an IP address (GTSLearning, 2014).
7.1.2.1 DHCP client initialisation

The DHCP client initialisation process can be seen in Figure 57 below.

![DHCP Client Initialisation Process Diagram]

**Figure 64: The Dynamic Host Configuration Protocol (DHCP) process**

Source: GTSLearning (2014)
7.1.3 Automatic Private IP Addressing (APIPA)

Automatic Private IP Addressing (APIPA) was developed by Microsoft as a means for clients that are configured to automatically obtain an address that could not contact a DHCP server to communicate on the local subnet. APIPA uses the address range 169.254.1.0 – 169.254.254.255. These addresses are from one of the address ranges that are reserved for private addressing. It then performs an ARP broadcast to check that the address is currently unused; if it is in use, the host selects another address and repeats the broadcast, and so on.

This type of addressing is called link-local in standards documentation. Link-local can also be implemented by Bonjour on Mac OS X and Avahi or mDNSResponder on Linux (GTSLearning, 2014).

7.2 Configuring DHCP

A DHCP server must be allocated a static IP address and configured with the following information:

- A range of IP addresses to allocate (scope)
- A lease period plus renewal (T1) and rebinding (T2) timers
- A subnet mask to allocate
- Other optional information to allocate, such as default gateway and DNS address(es)

(GTSLearning, 2014)
7.2.1 DHCP scopes and leases

A scope is a range of IP addresses that a DHCP server allocates to clients, along with associated IP configuration settings known as DHCP options. Along with scope, you also need to define a lease period. A long lease period means that the client does not have to renew the lease as frequently, but the DHCP server’s pool of IP addresses is not replenished (GTSLearning, 2014).

7.2.2 DHCP options

Typical DHCP options include:
- The default gateway
- The IP address of DNS servers
- The DNS suffix (domain name) to be used by the client
- Other useful server options, such as time synchronisation (NTP), file transfer (TFTP), or VoIP proxy.

(GTSLearning, 2014)

7.2.3 DHCP reservations

With DHCP, clients do not retain the same IP addresses over time. However, there are some cases where it would be better for some hosts to retain their IP addresses (e.g. network printers or wireless access points). One solution is to configure these devices statically, using IP addresses outside the DHCP scope. While this solution works, it loses the benefits of central configuration.
An alternative approach is to create a DHCP reservation. This is a mapping of a MAC address to a specific IP address. When the DHCP server receives a request from a given MAC address, it always provides the same IP address. This is also called static or fixed address assignment (GTSLearning, 2014).

### 7.3 Network Time Protocol (NTP)

Many applications on networks are time dependent and time critical (such as authentication and security mechanisms, scheduling applications, or backup software). Network Time Protocol (NTP) provides a channel of transport through which to synchronise these time-dependent applications. NTP works over UDP on Port 123 (GTSLearning, 2014).

![Figure 67: Configuring the time settings within SUSE Linux](Source: GTSLearning (2014))
Concluding remarks

DHCP is a method for a client to automatically request IP configuration information from a server. A DHCP service can be configured to run on a Windows/Linux server, or can be provided by most types of switches and routers. In Windows, if a client cannot contact a DHCP server, it uses an APIPA (link local) address that allows for communication on the local network. NTP is used to synchronise the time across various network devices and applications.

Self-assessment

Test your knowledge

1. Describe the DHCP client initialisation process.
2. Describe the functions of NTP.
3. What is the advantage of having a DHCP server in a TCP/IP network?
4. Distinguish between static and dynamic IP addressing.
5. Identify and explain the mechanisms that have been employed to provide a client autoconfiguration service for TCP/IP.
Unit 8: IPv6

Unit 8 is aligned with the following learning outcome and assessment criterion:

**Learning outcome**
LO3: Discuss the functions and features of TCP/IP addressing, protocols and services.

**Assessment criterion**
AC3.6: Identify IPv6 addressing schemes and describe the IPv6 address format and packet structure.

**Learning objectives**
After studying this unit, you should be able to:
- Describe the IPv6 address format and packet structure
- Identify IPv6 addressing schemes

**Supplementary reading**

*Unit 8 adapted from:*

**Introduction**
This unit will introduce us to the IPv6 address format and packet structure, and also identify the different IPv6 addressing schemes.

**8.1 IPv6 address format**
In IPv4, the addressing scheme is based on a 32-bit binary number. 32 bits can express $2^{32}$ unique addresses (in excess of four billion). Inefficiencies in the addressing scheme and growing demand for addresses in Asia mean that the available IPv4 address supply is close to exhaustion (GTSLearning, 2014).
NAT and private addressing have provided a ‘stopgap’ solution to the problem, but NAT does not work well with modern applications, such as VoIP and conferencing (GTSLearning, 2014).

IP Next Generation or IPng (IPv6) provides a long-term solution to the problem of address space exhaustion. Its 128-bit addressing scheme has space for 340 undecillion unique addresses (GTSLearning, 2014).

To interpret IPv6, you must understand hexadecimal notation. Hex is a convenient way of referring to the very long addresses. Hexadecimal has 16 characters (0…9, A, B, C, D, E, F) compared to binary’s 2. Therefore, it only takes 1 hexadecimal character to represent 4 binary characters. Values are arranged in 8 x 16-bit (double byte) blocks separated by colons; for example, 2001:0db8:0000:0000:0abc:0000:0def0:1234. Where a double-byte contains leading zeros, they can be ignored. Thus, the address above would become: 2001:db8::abc:0:0def0:1234 (GTSLearning, 2014).

8.2 IPv6 addressing schemes

An IPv6 address is divided into two main parts:
- The first 64 bits are used as a network ID.
- The second 64 bits designate a specific interface.

Network addresses are written using CIDR notation, where /nn is the length of the routing prefix in bits. Within the 64-bit network ID, as with CIDR, the length of any given network prefix is used to determine whether two addresses belong to the same network (GTSLearning, 2014).

Like IPv4, IPv6 defines a number of addressing schemes. These are unicast, multicast and anycast (GTSLearning, 2014).

8.2.1 Unicast addressing

A unicast address identifies a single network interface. IPv6 unicast addressing is scoped; a scope is a region of the network. Global scopes provide the equivalent of public addressing schemes in IPv4, while link local schemes provide private addressing. The parts of a global address are as follows:
- The first 3 bits (001) indicate that the address is within the global scope.
- The next 45 bits are allocated in a hierarchical manner to regional registries and from them to ISPs and end users.
- The next 16 bits identify site-specific subnet addresses.
- The final 64 bits are the interface ID.

(GTSLearning, 2014)
Link local addresses are used by IPv6 for network housekeeping traffic. Link-local addresses span a single subnet. Nodes on the same link are called neighbours. Link-local addresses start with a leading fe80, while the next 54 bits are set to zero and the last 64 bits are the interface ID (GTSLearning, 2014).

8.2.2 Multicast addressing
A multicast address identifies multiple network interfaces. Unlike IPv4, IPv6 routers must support multicast. The parts of a multicast address are subdivided as follows:
- 8-bit multicast scope (11111111 or ff in hex)
- 4-bit flag
- 4-bit scope (link-local/global)
- 112-bit group ID

Link-local multicast replaces broadcast.

(GTSLearning, 2014)

8.2.3 Anycast addressing
An anycast address also identifies multiple addresses. Anycast is used where a message must be sent to any member of a group, but not necessarily to all of them. The packet is sent to the member of the group physically closest to the transmitting host. Anycast is principally used for routing protocol traffic (GTSLearning, 2014).

8.2.4 Reserved addresses
The 0000::/8 block is reserved for special functions. Within this block, two special addresses are defined:
- Unspecified (:)
- Loopback (::1)

(GTSLearning, 2014)

Concluding remarks
IPv6 uses longer addresses (128-bit) with variable length network prefixes and a 64-bit host ID, derived from the MAC address or randomly assigned. IPv6 supports global, link-local and unique private address schemes, and unicast, multicast and anycast addressing.
Self-assessment

Test your knowledge

1. In IPv6, how is the loopback address best expressed?

2. In IPv6, how would you distinguish a unicast address with global scope from other addresses?

3. If assigned a single global IPv6 address prefix, how many bits are available for subnetting?

4. What type of IPv6 address is not routable?

5. What is anycast?
Unit 9: Name resolution

Unit 9 is aligned with the following learning outcome and assessment criterion:

Learning outcome
LO4: Identify and explain network services and WAN access technologies.

Assessment criterion
AC4.1: Describe the format of hostnames and FQDNs, the process of name resolution, basic configuration for a DNS server and name resolution troubleshooting tools.

Learning objectives
After studying this unit, you should be able to:
- Describe the format of hostnames and Fully Qualified Domain Names
- Understand the process of name resolution using HOSTS and DNS
- Identify basic configuration parameters for a DNS server
- Use name resolution troubleshooting tools

Supplementary reading

Unit 9 adapted from:

Introduction
In this unit we will explore the format of hostnames and Fully Qualified Domain Names (FQDNs), as well as the process of name resolution using HOSTS and DNS. We will further identify the basic configuration parameters for a DNS server and name resolution troubleshooting tools.
9.1 Hostnames
A hostname is an alias assigned to a computer by the administrator. A hostname:
- Can contain letters, numbers and hyphens
- Cannot be all numbers
- Cannot start or end with a hyphen
- Is not case sensitive

9.2 Fully Qualified Domain Name (FQDN)
To avoid the possibility of duplicate hostnames on the Internet, a Fully Qualified Domain Name (FQDN) is used to provide a unique identity for the host. An example of a FQDN might be mole.riverbank.com. The FQDN is made up of the hostname and one or more domain names (a domain suffix). In the example, the hostname is ‘mole’ and the domain suffix is ‘riverbank.com’. This domain suffix consists of the domain name ‘riverbank’ within the top level domain ‘.com’ (GTSLearning, 2014).

FQDNs must follow certain rules:
- The hostname must be unique within the domain.
- The total length of the FQDN must be 255 characters or less.
- The FQDN supports alphanumeric and hyphen characters only. A label cannot begin or end with a hyphen.
- FQDNs are not case sensitive.

9.3 Name resolution methods
To make use of these user-friendly names, there has to be a system for resolving a FQDN to its IP address and also for ensuring that the names are unique. The Internet uses a system called Domain Name System (DNS), but before DNS was available, a HOSTS file was used (GTSLearning, 2014).

9.3.1 Name resolution using the HOSTS file
HOSTS was a text file containing a list of IP > hostname or FQDN mappings which was distributed manually between network administrators.

It has long been replaced by DNS, but each host is still installed with HOSTS file:
- Windows
  - %SystemRoot%\System32\drivers\etc\hosts
- Linux
  - /etc/hosts
Administrators can configure static mappings in HOSTS, and these take precedence over DNS (GTSLearning, 2014).

### 9.3.2 Domain Name System (DNS)

Domain Name System (DNS) is a hierarchical system for resolving names to IP addresses. At the top of the DNS hierarchy is the root, which is often represented by a period (\(.\)). There are 13 root level servers (A to M).

Immediately below the root lies the Top Level Domain (TLD). There are several types of TLDs, but the most prevalent are generic (\(.com\), \(.org\), \(.net\), \(.info\), \(.biz\)), sponsored (\(.gov\), \(.edu\)) and country code (\(.uk\), \(.ca\), \(.de\)) (GTSLearning, 2014).

TLD’s are managed by ICANN and regional registries. Domains can be registered within an appropriate TLD (GTSLearning, 2014).

![Figure 68: DNS hierarchy](source: GTSLearning (2014))
9.3.3 Name resolution using DNS

The resolution process takes place as follows:

1. The client (resolver) in **grommet.co.uk** queries its local name server for the IP address of the host **www.widget.com**.
2. The name server checks its own zone database for the record.
3. It is not authoritative for the domain, so the name server queries a root server for the required IP address.
4. The root server checks its zone, finds that it is not authoritative for the requested record and passes the name server in grommet.co.uk, the IP address of a name server in the **.com** domain.
5. The originating name server queries the designated name server in **.com**, which does not have the required information.
6. However, it does have the IP address of name servers in the **widget.com** domain. It passes these to the originating name server.
7. The **grommet.co.uk** name server queries the name server in **widget.com**.
8. Because the name server is authoritative, it passes the required record back to the originating server.
9. The server caches the result and passes the requested IP address to the client.
10. The client establishes a session with the **www.widget.com** server.
9.4 Configuring DNS servers

DNS is essential to the function of the Internet. Windows Active Directory and Linux networks also require a DNS service to be running correctly (GTSLearning, 2014).

9.4.1 Zones

Name servers maintain the DNS namespace in zones. A name server can maintain:
- Primary zone
- Secondary zone

A server that does not maintain a zone (primary or secondary) is referred to as a cache-only server (GTSLearning, 2014).

9.4.2 Resource records

A zone will contain resource records, which will allow computers and services to be resolved into IP addresses.

<table>
<thead>
<tr>
<th>Record</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA</td>
<td>Start Of Authority</td>
<td>Identifies the name server that is authoritative for the zone plus contact information and a serial number (for version control).</td>
</tr>
<tr>
<td>A</td>
<td>Address</td>
<td>A host name mapped to an IPv4 address.</td>
</tr>
<tr>
<td>AAAA</td>
<td>Address</td>
<td>A host name mapped to an IPv6 address.</td>
</tr>
<tr>
<td>NS</td>
<td>Name Server</td>
<td>Identifies name servers in the zone.</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer</td>
<td>An IP address mapped to a host name. This is used for reverse lookups, which are a useful security feature.</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical Name</td>
<td>Defines an alias for a particular host (for example, the true name of a web server could be masked as the alias www).</td>
</tr>
<tr>
<td>MX</td>
<td>Mail eXchanger</td>
<td>Identifies a mail server for the domain. Multiple servers are often provided for redundancy. Each server is given a preference value. The lowest numbered server is preferred.</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)
9.5 Name resolution troubleshooting

A number of command line tools are available to troubleshoot name resolution on Windows and Linux hosts and networks (GTSLearning, 2014).

9.5.1 nslookup

You can troubleshoot DNS with the **nslookup** command, either interactively or from the command prompt.

*Nslookup ComputerName –DNSServer -Option*

![Figure 70: Using nslookup](source: GTSLearning (2014))

9.5.2 Domain Information Gopher (dig)

DNS **Domain Information Gopher (dig)** allows you to query a name server directly and retrieve any of the information known about the domain name.
9.5.3 Nbtstat

The **nbtstat** (NetBIOS over TCP/IP statistics) utility is used to provide NetBIOS status information when using TCP/IP.
Concluding remarks

A computer can be configured with a hostname to provide simpler means for users to identify the system on the network. An FQDN provides a unique identity for hosts communicating on an Internet. Name resolution services, such as DNS, map IP addresses to hostnames and FQDNs. Nslookup and dig can be used to troubleshoot DNS, while nbtstat is useful for NetBIOS troubleshooting.

Self-assessment

Test your knowledge

1. What is a generic top-level domain?
2. What characters are allowed in a DNS hostname?
3. What type of DNS record resolves IPv6 addresses?
4. What is a PTR DNS record used for?
5. What command would you use to view cached NetBIOS name entries?
Unit 10: Internet applications

Unit 10 is aligned with the following learning outcome and assessment criterion:

**Learning outcome**
LO4: Identify and explain network services and WAN access technologies.

**Assessment criterion**
AC4.2: Describe the functions of Web and file transfer application protocols and communications protocols.

**Learning objectives**

After studying this unit, you should be able to:

- Describe the functions of Web and file transfer application protocols:
  - Web (HTTP)
  - HTTPS (HTTP Secure)
  - FTP
- Describe the functions of communications protocols:
  - Email (SMTP, POP3, IMAP)
  - VoIP/streaming video (SIP, RTP)

**Supplementary reading**

**Unit 10 adapted from:**

Introduction
In this unit we will be discussing the functions of some Web and file transfer application protocols as well as the functions of communications protocols.

10.1 TCP/IP services
The services that form part of the TCP/IP protocol suite are mostly client-server protocols and applications. Client-server applications are based around a centralised server that stores information and waits for requests from clients (GTSLearning, 2014).

10.2 World Wide Web (HTTP)
The World Wide Web (WWW) is a TCP service running over the Internet. The foundation of Web technology is the HyperText Transfer Protocol (HTTP). HTTP enables clients to request resources from an HTTP server. HTTP is usually used to serve HyperText Markup Language (HTML) web pages (GTSLearning, 2014).

10.2.1 Forms and interactivity
HTTP also features forms mechanisms (GET and POST) whereby a user can submit data from the client to the server. HTTP is a stateless protocol; this means that the server preserves no information about the client during a session (GTSLearning, 2014).

10.2.2 Error codes
HTTP also has a system of codes that provide feedback on the status of the request by the client. There are many codes, broadly grouped into the following ranges:
- 2xx – request successful
- 3xx – redirect to another Uniform Resource Identifier (URI)
- 4xx – client error (notably 403 – Forbidden and 404 – Not Found)
- 5xx – server error

(GTSLearning, 2014)

10.2.3 Establishing a website
Most organisations have an online presence, represented by a website. In order to run a website, it must be hosted on an HTTP server connected to the Internet. The main server platforms are Internet Information Server (Windows) and Apache (Linux and Windows) (GTSLearning, 2014).
10.2.4 HTTP Secure (HTTPS)
It is a subset of HTTP that allows for a secure dialogue between a client and a server. This security is provided using a server-side certificate. A certificate is a digital proof of identity. The certificate, issued by a digital Certificate Authority (CA), provides assurance (GTSLearning, 2014).

10.2.5 Structure of the Uniform Resource Identifier (URI)
The Uniform Resource Identifier (URI) is used as the addressing scheme of the Internet. A URI has a fixed structure comprising up to six components. The following example shows the structure of a URI used for HTTP and explains the various components:

http://www.w3.org:80/docs/uri/about.htm?query=information#top
(Scheme://Authority/LocalPath?Query#Anchor)

- Scheme is http, though other URI schemes exist
- Authority is:
  - The FQDN or IP address of the server
  - The server port (80 for HTTP or 443 for HTTPS by default)
- Local path is the directory (and file) on the server
- Query is an optional part to pass to a script or Web application running on the server
- Anchor is an optional part specifying an ID within a document
(GTSLearning, 2014)

10.3 File Transfer Protocol (FTP)
File Transfer Protocol (TP) is a connection-oriented protocol using TCP that is especially useful for transferring files between different Operating Systems. The WWW service has replaced most functions of FTP, although only FTP allows you to copy files from a client computer to a server. FTP is also more efficient than HTTP for the transfer of files (GTSLearning, 2014).

10.3.1 FTP clients
The FTP client may take a number of forms:
- Most installations of TCP/IP include a command line client interface. The commands PUT and GET are used to upload and download files, respectively.
- Dedicated GUI clients allow you to connect to servers, browse directories and upload and download files.
- Internet browsers allow you to connect to an FTP service and download files.
(GTSLearning, 2014)
10.3.2 Active versus passive FTP

A client connects to TCP Port 21 on FTP server. The control port is used to transfer commands and status information, but not for data transfer.

In active mode, the client sends a PORT command specifying its chosen data connection port number and the server opens the data connection between the chosen client port and Port 20 on the server (GTSLearning, 2014).

![Figure 73: FTP in active mode](Source: GTSLearning (2014))

In passive mode, the client opens a data port and sends the PASV command to the server’s control port. The server then opens a random high port number and sends it to the client using the PORT command. The client then initiates the connection between the two ports (GTSLearning, 2014).

![Figure 74: FTP in passive mode](Source: GTSLearning (2014))

Active FTP poses a configuration problem for some firewalls, as the server is initiating the inbound connection but there is no way of predicting which port number will be used (GTSLearning, 2014).
10.3.3 **Trivial File Transfer Protocol (TFTP)**

Trivial File Transfer Protocol (TFTP) is a connectionless protocol (using UDP Port 69) that provides file transfer services. It does not provide the guaranteed delivery offered by FTP and is, therefore, only suitable for transferring small files. It supports reading (GET) and writing (PUT) files, but not directory browsing, file deletion, or any of the other features of FTP (GTSLearning, 2014).

10.4 **Email (SMTP/POP3/IMAP4)**

Electronic mail enables a person to compose a message and send it to another user on their own network, or anywhere in the world, via the Internet.

An Internet email message has a fixed format containing two parts:
- Message headers:
  - From, To, Reply To, Subject
- Body:
  - Contains any plain ASCII text
  - Attachments can be encoded using Multipurpose Internet Mail Extensions (MIME)
  - Most clients also support HTML formatting

An Internet email address is always of the form: LocalPart@DomainName; for example, sender@widget.com.

The domain name represents the domain of which the email server is a member and the local part of the email address refers to the mailbox. A mailbox usually refers to a user, although it may also refer to other recipients, such as a distribution list (GTSLearning, 2014).

10.4.1 **Simple Mail Transfer Protocol (SMTP) protocol**

The Simple Mail Transfer Protocol (SMTP) specifies how mail is delivered from one system to another. SMTP is used in the following situations:
- For delivering messages from the email client to the SMTP server
- For transferring messages from one SMTP server to another

The SMTP server for the domain is registered on the DNS using a Mail Exchange (MX) record. SMTP is not used for transferring the message from the recipient’s SMTP server to its email client, because it requires that both source and destination are online to make a connection. The SMTP server retries at regular intervals before timing out and returning a Non-Delivery Report (NDR) to the sender (GTSLearning, 2014).
10.4.1.1 SMTP commands
SMTP can be operated from a Terminal Emulation (Telnet) command prompt.

10.4.1.2 Non-Delivery Reports (NDR)
SMTP has a system of codes that provide feedback on the status of the request made by the client in the form of an NDR. There are many codes, broadly grouped into the following ranges:
- 2.x.x – request successful and/or informational messages
- 3.x.x – more information required
- 4.x.x – temporary error
- 5.x.x – permanent error

(GTSLearning, 2014)

10.4.2 Post Office Protocol (POP3)
Post Office Protocol (POP3) is designed to allow mail to be downloaded to the recipient’s email client at his/her convenience. A POP3 client application, such as Microsoft Outlook or Mozilla Thunderbird, establishes a TCP connection to the POP3 server. This is generally a different service running on the same machine as the SMTP server. The user is authenticated and the contents of his or her mailbox are downloaded for processing on the local computer (GTSLearning, 2014).

Figure 75: Configuring mailbox access protocols on a server
Source: GTSLearning (2014)
10.4.3 Internet Message Access Protocol (IMAP)

While POP3 is widely used, it does have limitations, some of which are addressed by IMAPv4. Clients connect over Port 143 (993 for SSL). They authenticate themselves, then retrieve messages from the designated folders. SMTP is still needed to support mail delivery. Internet Message Access Protocol (IMAP) is a retrieval protocol, only (GTSLearning, 2014).

The differences between POP3 and IMAP are that POP3 is primarily designed for dial-up access; the client contacts the server to download its messages, then disconnects. IMAP, on the other hand, supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously (GTSLearning, 2014).

10.4.4 Internet mail flow

The following process shows how an email message is sent from a typical corporate mail gateway (using Microsoft Exchange mail server) to a recipient with dial-up Internet access:

- The email client software on the sender’s computer sends the message to the Exchange email server using Microsoft’s Message Application Programming Interface Protocol (MAPI). The mail server puts the message in a queue, waiting for the next SMTP session.
- When the Exchange SMTP server starts to process the queue, it first contacts a DNS server to resolve the recipient’s address to an IP address for the email server.
- It then uses SMTP to deliver the message to this email server.
- The message is put in the message store on the recipient’s gateway. To retrieve it, the recipient uses his or her mail client software to connect with the mailbox on the server, using POP3 (Port 110) or IMAP (Port 143). (GTSLearning, 2014)

10.5 Conferencing and VoIP protocols

Voice over IP (VoIP), Web conferencing and Audio/Visual (A/V) conferencing solutions are becoming more popular as the technologies that support them become viable. The main challenges that these applications have in common is that they transfer real-time data and must create point-to-point links between hosts on different networks (GTSLearning, 2014).

The protocols designed to support these applications cover one or more of the following functions:

- Session control
- Data transport
- Quality of Service (QoS) (GTSLearning, 2014)
10.5.1 Voice over IP (VoIP)

Voice over IP (VoIP) can be a cost-effective way of providing telephony services to end users over corporate IP networks, or even public IP networks such as the Internet. It provides integration with the fixed and mobile telephone networks, allowing calls to be placed from computer to landline or from mobile phone to laptop (GTSLearning, 2014).

10.5.2 Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP)

Session Initiation Protocol (SIP) sits at the session layer of the OSI model and is implemented in instant messaging, Web and A/V conferencing, and IP telephony solutions, primarily as a signalling control. SIP is used to establish, manage and terminate communication sessions. SIP typically uses TCP ports 5060 and 5061 (GTSLearning, 2014).

While SIP provides session management features, the actual delivery of real-time data uses different protocols. The principal one is Real-time Transport Protocol (RTP). RTP uses a temporary UDP port to open a media stream. The data is packetised and tagged with control information (GTSLearning, 2014).

Concluding remarks

Websites and applications use HTTP to transfer data and are accessed via URIs. FTP and TFTP can be used for file transfer. SMTP is used for mail delivery, while POP3 and IMAP4 are means of accessing a mailbox on a remote server. Real-time applications, such as VoIP, use session protocols such as SIP, along with data transfer protocols such as RTP.

Self-assessment

Test your knowledge

1. What distinguishes TFTP from FTP?

2. If HTTP uses connection-oriented TCP transport, why is it described as stateless?

3. What happens if a message sent via SMTP cannot be delivered?
4. What protocol would enable a client to manage mail subfolders on a remote mail server?

5. Which TCP/IP connectivity utility provides bidirectional file transfers between TCP/IP hosts?
Unit 11: WAN technologies

Unit 11 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO4: Identify and explain network services and WAN access technologies.

**Assessment criteria**
AC4.3: Distinguish between the types of switched networks.
AC4.4: Identify technologies and protocols used to implement WANs.
AC4.5: Describe and differentiate between the types of local access networks.
AC4.6: Discuss the installation and configuration of dial-up and broadband modems.

**Learning objectives**
After studying this unit, you should be able to:
- Distinguish circuit- and packet-switched networks
- Understand the provision of telecoms networks and the Internet
- Identify technologies and protocols used to implement WANs (PDH (T-carrier/E-carrier), SONET/SDH, Passive Optical Network, 10G Ethernet, frame relay, ATM, MPLS)
- Describe and differentiate between types of local access networks (dial-up/PSTN, dedicated/leased lines, ISDN, DSL, HFC, FTTx, broadband over powerline)
- Install and configure dial-up and broadband modems/multifunction network devices

**Supplementary reading**

Unit 11 adapted from:
Introduction
Wide Area Network (WAN) technologies support data communication over greater distances than LANs. In this unit, we will be looking at the different network types, identify the technologies and protocols used to implement WANS, learn about the different types of local access networks and learn how to install modems.

11.1 WAN basics
WANs use different technologies, including copper cables, fibre-optic cables, microwave transmitters and satellites. WAN links usually provide low bandwidth levels compared with LANs, although faster technologies are becoming available at cost-effective pricing (GTSLearning, 2014).

Most remote connectivity methods involve the use of ‘public networks’. WAN connection services are often leased from a service provider; typically, a Telecommunications Company (telco), because dedicated links are too expensive and complex for most organisations to implement and maintain (GTSLearning, 2014).

11.2 Switched networks
Switching is the process used to connect source and destination nodes and the process by which the data is forwarded at intermediary points. It is more efficient for connecting multiple locations than a dedicated line. The two types of switched networks are:
- Circuit switching
- Packet switching

(GTSLearning, 2014)

11.2.1 Circuit switching
Circuit switching enables a temporary dedicated path to be established between two locations, such as two routers. A connection is established as follows:
- The source router requests the connection.
- The destination router signals readiness to receive data.
- The source and destination routers exchange communication parameters for the connection.

(GTSLearning, 2014)

Once the connection is established, all communications are sent on the same path. At the end of the communication, the connection is broken down and the path becomes available for another connection to use (GTSLearning, 2014).
Circuit switched networks provide guaranteed bandwidth, but, on the downside, they make inefficient use of the transmission media, since a dedicated channel cannot be used when it is not in use (GTSLearning, 2014).

![Figure 76: Circuit switched networks provide a dedicated path between nodes](source: GTSLearning (2014))

### 11.2.2 Packet switching

Packet switching technology was developed on the basis that subscribers share the network infrastructure and pay only for the bandwidth that they use. It is more cost-effective and provides more efficient use of network infrastructure than circuit-switched network (GTSLearning, 2014).

In this type of network, data is broken into small numbered chunks that contain addressing and other information, such as the packet sequence number. The packet size is kept small, for two reasons:

- The small packets can be processed by the switches and routers more quickly to keep the switch availability high and prevent them from becoming blocked.
- If a packet arrives in a damaged state, then only a small amount of data must be re-transmitted.

(GTSLearning, 2014)

There are two forms of packet switching. These are:

- Connectionless or datagram packet switching
- Connection-oriented or virtual circuit packet switching
11.2.3 WAN topologies

Many WAN links are point-to-point; that is, a single link to connect two sites. Sometimes organisations need to link two of their sites. This can be done by creating a full mesh or a partial mesh. This type of topology is expensive and it creates duplication. A cheaper alternative is a hub and spoke topology (GTSLearning, 2014).

11.3 Telecommunications networks

Public networks are owned by telecommunications companies and provide WAN services to organisations. Interoperability between telcos is often guided by standards set by the International Telecommunication Union (ITU). The Internet Engineering Task Force (IETF) develops standards for communications over the Internet, but is mostly focused on network, transport and application layer protocols (GTSLearning, 2014).

11.3.1 Public Switched Telephone Network (PSTN)

The basis of Public Switched Telephone Network (PSTN) is a circuit-switched network, but the infrastructure can also carry packet switched data services.

The different zones of a PSTN are:
- Customer Premises Equipment (CPE)
- Local loop
- Local exchange
- Trunk offices
11.3.2 The Internet

The major infrastructure behind the Internet is the fibre-optic trunks which are maintained by the major telecommunications providers. The interconnection between these trunk lines is called Network Access Points (NAPs), which are administered by first-tier Network Service Providers (NSPs) (GTSLearning, 2014).

Tier 2 Internet Service Providers (ISPs) connect to the NAPs, then provide downstream transit to tier 3 ISPs or directly to customer networks or to lower tier ISPs and resellers. Customers connect to the ISP’s network via a local Point Of Presence (POP) and their communications are then switched or routed to the appropriate destination (GTSLearning, 2014).

Tier 2 and 3 ISPs are also likely to pool services within an Internet eXchange Point (IXP).
11.3.3 PDH/DSx (or T-Carrier)
The first generation of Digital Signalling (DS) to be implemented on telecommunications networks was the Plesiochronous Digital Hierarchy (PDH) or T-carrier system. PDH-enabled voice traffic should be digitised for transport around the core network. It is based on Time Division Multiplexing (TDM) (GTSLearning, 2014).

11.4 Modern telecommunications networks
The second generation of digital transmissions standards is known as the Synchronous Digital Hierarchy (SDH), as standardised by the ITU or Synchronous Optical Network (SONET), as standardised by ANSI (GTSLearning, 2014).

11.4.1 Synchronous Optical Network (SONET)
Synchronous Optical Network (SONET) was developed to carry ATM traffic and provide a standard transport mechanism for the various proprietary PDH fibre-optic networks that had been installed over the years. As such, SDH/SONET is principally a physical layer standard which defines infrastructure, line speeds, and so on. There is an SDH/SONET frame format, but this is designed to transport frames from higher level protocols rather than to provide any sort of addressing capability (GTSLearning, 2014).
SHD/SONET also uses TDM but, unlike PDH, it is synchronous. The nodes in the SDH/SONET infrastructure are usually Add-Drop Multiplexers (ADM). SDH/SONET is now the mainstream standard for telecommunications trunk lines (GTSLearning, 2014).

11.4.2 Dense Wave Division Multiplexing (DWDM)

Wave Division Multiplexing (WDM) is a means of making more use of the bandwidth available in a fibre-optic cable. Dense WDM (DWDM) involves transmitting multiple wavelengths (colours) of light down the same fibre and also allowing for bidirectional communication across the same fibre. Each wavelength forms a channel with a data rate of up to 10 Gbps and a single fibre can currently support a few hundred channels (GTSLearning, 2014).

Telcos have used DWDM to maximise the capacity of long-distance fibre-optic trunks and the technology supports the higher optical carrier (OCx) rates. This use of both SONET and DWDM is called overlay model. This is being standardised by the ITU as the Optical Transport Network (OTN) (GTSLearning, 2014).

11.4.3 Passive Optical Network (PON)

Passive Optical Network (PON) technology uses unpowered optical components to split the light beam, enabling a point-to-multipoint technology to be implemented. In PON networks, a single data stream is split and delivered to multiple downstream nodes. Upstream communication is handled separately using some form of multiplexing, such as TDM or DWDM (GTSLearning, 2014).

11.4.4 10G Ethernet WAN PHY

The WAN PHY specifications in the Ethernet 10G standard are designed to be interoperable with SONET OC-192 and DWDM. For some applications, the use of DWDM can make the overlaying of SONET seem unnecessary. An alternative architecture consists of 10G Ethernet/IP running directly on DWDM links, where each wavelength channel is a 10G Ethernet link. This is called a peer-to-peer model (GTSLearning, 2014).

11.5 Packet-switched WAN services

The principal packet-switched technologies in use in WANs are:
- Frame relay
- Asynchronous Transfer Mode (ATM)
- Multiprotocol Label Switching (MPLS)

(GTSLearning, 2014)
11.5.1 Frame relay

Frame relay evolved from X.25. It provides data packet forwarding for services running over T-carrier lines, ISDN, or even dialup. Frame relay uses variable-length packets up to 4096 bytes and it can encapsulate data from higher-level protocols, including TCP/IP (GTSLearning, 2014).

X.25 was based on the use of analogue equipment and, therefore, required error checking and correction information to be transmitted and calculated at each node, creating a substantial overhead (GTSLearning, 2014).

Frame relay makes use of connection-oriented virtual circuits that avoid fragmentation and re-assembling of packets. Virtual circuits are either permanent (PVC0) or switched (SVC) (GTSLearning, 2014).

With frame relay, overheads on the network are reduced. Frame relay provides mechanisms for the service provider to perform congestion control and maintain available bandwidth to an agreed service level, providing QoS for latency-sensitive applications such as VoIP (GTSLearning, 2014).

11.5.2 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) uses a cell switching technology. A cell is a small (53 byte), fixed-length packet that contains 48 bytes of data and 5 bytes of header information. ATM was designed for both LAN and WAN environments. It is designed to make highly efficient use of the available bandwidth, with switches used to multiplex data simultaneously from multiple sources onto the network. The header information identifies the virtual circuit required for the cell to reach its destination and also allows bandwidth to be dedicated to particular data. The use of virtual circuit means that the packets arrive in order and can be processed quickly (GTSLearning, 2014).

Figure 80: Asynchronous Transfer Mode (ATM) switch

Source: GTSLearning (2014)
Figure 80 above shows an example of a switch allocating additional bandwidth to data source 3, while continuing to provide some bandwidth to the other data sources (1 and 2). ATM combines the bandwidth guarantee of circuit switching with the efficient use of bandwidth provided by circuit switching (GTSLearning, 2014).

ATM becomes less efficient when transporting protocols with large frame sizes or PDUs, as the small cell size means that a substantial overhead is introduced in disassembling and reassembling packets (GTSLearning, 2014).

11.5.3 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) was developed by Cisco from ATM as a means of providing traffic engineering (congestion control), Class of Service (CoS) and Quality of Service (QoS) within a packet-switched, rather than a circuit-switched, network (GTSLearning, 2014).

MPLS achieves a marriage of Layer 3 based routing with Layer 2 based switching. Where frame relay and ATM provide connection-oriented transfer by establishing a virtual circuit, MPLS establishes connections via Label Switched Paths (LSPs) enabled by a mesh network of Label Switched Routers (LSRs). One of the benefits of MPLS is that ATM switches can usually be re-engineered to act as LSRs, reducing initial deployment costs by retaining existing hardware (GTSLearning, 2014).

![Figure 81: Multiprotocol Label Switching (MPLS) topology](source:image)

Source: GTSLearning (2014)
11.6 Local loop services

While technologies such as SDH/SONET, ATM and MPLS enable traffic to be carried over telecommunications trunks, the trickiest part of providing services to subscribers tends to be the connection over the local loop. Various technologies have been developed to provide fast ‘broadband’ connections over the local loop (GTSLearning, 2014). These services are briefly described below.

11.6.1 Dial-up services

The most basic means of establishing a data network connection over the POTS is the dial-up modem. While this offers only very low bandwidth, it remains an almost universally supported fall-back option when no other means of making a connection is available. A dial-up link connection is typically established using the Point-to-Point Protocol (PPP). The main disadvantages of this system are low data transfer rates and error-prone links (GTSLearning, 2014).

![Figure 82: Legacy dial-up Small Office/Home Office (SOHO) Internet access technology](source: GTSLearning (2014))

11.6.2 Dedicated/leased lines

A dedicated or leased line provides a permanent connection that links two locations using any variety of technologies. A dedicated line is owned by a company. These dedicated lines establish a connection without any delay and offer a faster and more reliable service, as the line quality is always consistent (GTSLearning, 2014).

Digital leased lines use devices called Channel Service Units or Data Service Units (CSUs/DSUs) instead of modems used for analogue systems. CSU/DSU converts the Ethernet frames from the router to the frame format and digital signalling supported by the WAN environment (GTSLearning, 2014).
11.6.3 Integrated Services Digital Network (ISDN)
Integrated Services Digital Network (ISDN) is a digital version of the local loop. It is a digital circuit-switched technology for voice, video and data. ISDN is a dial-up service billed for line rental and usage. ISDNs are most commonly used for interconnection of LANs and remote users to businesses. The two classes of ISDN are:
- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

(GTSLearning, 2014)

11.6.4 Digital Subscriber Line (DSL)
Digital Subscriber Line (DSL) is a technology for transferring data over voice-grade telephone lines. DSL uses the higher frequencies available in a copper telephone line as a channel of communication. The use of a filter prevents contaminating voice traffic with noise. The use of advanced modulation and echo cancelling techniques enable high-bandwidth, full-duplex transmissions (GTSLearning, 2014).

The main drawback of DSL is that as a copper-wire technology, it suffers from attenuation. The maximum range of a DSL modem is typically about 3 miles, but the longer the connection, the greater the deterioration in data rate. Various flavours of DSL exist, notably:
- Symmetrical DSL (SDSL)
- Asymmetrical DSL (ADSL)
- Symmetrical High Speed DSL (G.SHDSL)
- Very High Bitrate DSL (VDSL)

(GTSLearning, 2014)

11.6.5 Hybrid Fibre Coax (HFC)
A cable Internet connection is usually available along with a cable telephone/television service. These networks are often described as Hybrid Fibre Coaxes (HFCs), as they combine fibre-optic core network with coax links to customer premises equipment, but are more simply described as cable. The cable operators and telcos are competing with one another to provide ‘triple play’ networks and the investment in fibre-optic links has given the cable operators something of an advantage (GTSLearning, 2014).

11.6.6 FTTx
Traditional phone companies and cable television operators want to provide the same sort of converged ‘triple play’ services to consumers. The major obstacle to doing this is bandwidth in the ‘last mile’, where the wiring infrastructure is generally not good (GTSLearning, 2014).
The most expensive solution is Fibre To The Premises (FTTP) or its domestic variant, Fibre To The Home (FTTH). The essential point about both of these implementations is that the fibre link is terminated on Customer Premises Equipment (CPE). These make use of Wideband Division Multiplexing (WDM) to create a Passive Optical Network (PON) where signals from multiple sources are carried over a single fibre link (GTSLearning, 2014). There are three types of PONs:
  - ATM PON (APON)
  - Ethernet PON (EPON)
  - Gigabit PON (GPON)

Other solutions can variously be described as Fibre To The Node (FTTN) or Fibre To The Curb (FTTC) (GTSLearning, 2014).

### 11.6.7 Broadband Over Powerline (BPL)

Broadband Over Powerline (BPL) overlays a higher frequency carrier signal on the lines and uses this to transfer data. In fact, BPL is also known as Powerline DSL (PDSL). BPL is much less widely deployed than DSL or HFC (GTSLearning, 2014).

### 11.7 Installing modems

The term ‘modem’ means Modulator/Demodulator, originally referring to a device that converts between analogue and digital signal transmissions. The term modem is now widely used to refer to any type of SOHO remote connectivity appliance, even when such appliances do no actual modulation. These include ISDN, DSL, cable and satellite modems (GTSLearning, 2014).

#### 11.7.1 Analogue modems

Most laptops still come with built-in modems and they are also widely available either as PCI cards or external devices, connected via a serial or USB port. The modem is connected to an analogue phone point by 2-pair cable with RJ-11 connectors (GTSLearning, 2014).

#### 11.7.2 ISDN adapters

An ISDN connection would typically be facilitated through a Terminal Adapter (TA). The TA may be an external appliance or a plug-in card for a PC or compatible router. The TA is connected to the ISDN network via a Network Terminator (NT1) device. The ‘U’ port on the NT1 is connected to the ISDN wall jack. The ISDN-enabled router may then either be connected to a hub or switch or support direct connections from ISDN devices. A separate NT1 appliance can provide a connection for up to seven devices, known as Terminal Equipment (TE). TE1 devices can connect directly to the NT1; TE2 devices require a TA (GTSLearning, 2014).
11.7.3 DSL modems

A DSL adapter is installed as customer premises equipment, typically as some sort of combined router and hub/switch. These multifunction network devices are universal in the SOHO market. They provide Ethernet ports for connection to computers and switches on the LAN, and a WAN port for connection to the phone line. Alternatively, a USB adapter can be installed to make the connection for a single computer. A filter must be installed to separate voice and data signals (GTSLearning, 2014).

![Figure 83: WAN port to the right of 4xEthernet ports on a wireless router/DSL modem](source)

![Figure 84: Configuring ADSL connection settings for an ISP using PPPoA (ATM)](source)
11.7.4 Hybrid Fibre Coax (HFC)/cable modems

Installation of a cable modem follows the same general principles as for a DSL modem. Generally, the cable modem is interfaced to the computer through an Ethernet or USB adapter and with the access provider’s network by a short segment of coax (GTSLearning, 2014).

Concluding remarks

Public WANs make more use of circuit-switching technologies than LANs. Telecoms core infrastructure and the Internet is supported by fibre-optic trunk links, mostly using SDH/SONET, WDM or Metro Ethernet. WAN links can be used to run a number of packet-switched data services, including Frame Relay, ATM, MPLS and Ethernet. T-carrier and E-carrier describe a number of service levels for providing leased or dedicated access lines to subscribers. Other subscriber access technologies include ISDN, DSL and cable access. The demarc represents the end of an access provider’s cabling. WAN links can be implemented using a number of devices, from CSUs/DSUs for leased lines, through to dial-up modems, through to DSL/cable/satellite adapters and routers.

Self-assessment

Test your knowledge

1. What is the main advantage of circuit-switched networks?
2. What is multiplexing?
3. What is an Internet eXchange Point (IXP)?
4. What distinguished ATM from Ethernet?
5. What is the difference between IP and MPLS routing?
6. Distinguish between the different ‘flavours’ of DSL.
Unit 12: Wired networks

Unit 12 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO5: Demonstrate the ability to implement and support networked systems.

**Assessment criteria**
AC5.1: Examine the installation of wired networks.
AC5.2: Identify appropriate tools for network hardware installation and testing.

**Learning objectives**

After studying this unit, you should be able to:
- Understand the application of wiring standards to network design and installation
- Specify and install elements of wiring distribution, such as cabling, cross-connects and wall outlets
- Install and configure components for WAN links (smart jack/demarc and CSU/DSU)
- Identify appropriate tools for network hardware installation and testing
- Make an installation plan to accommodate the customer requirements and constraints for a typical SOHO network

**Supplementary reading**

*Unit 12 adapted from:*

Introduction
In this unit we will be discussing the different wiring standards, elements of wiring distribution, hardware installation and testing tools.

12.1 Wiring standards
In 1991, the Electronic Industries Association (EIA) introduced the EIA 568 specification. The standard is called Commercial Building Telecommunications Wiring Standard and was the first non-proprietary networking scheme for network designers (GTSLearning, 2014).

<table>
<thead>
<tr>
<th>Type</th>
<th>US (ANSI/TIA/EIA)</th>
<th>EU/UK (CENELEC)</th>
<th>ISO (ISO/IEC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial/office</td>
<td>568</td>
<td>EN 50173-2</td>
<td>11801</td>
</tr>
<tr>
<td>Data centre</td>
<td>942</td>
<td>EN 50173-5</td>
<td></td>
</tr>
<tr>
<td>Industrial</td>
<td>1005</td>
<td>EN 50173-3</td>
<td>24702</td>
</tr>
<tr>
<td>Residential</td>
<td>570</td>
<td>EN 50173-4</td>
<td>15018</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)

12.2 Wiring distribution
Computer network cabling is often installed in the same manner as a telephone installation.

12.2.1 Basic wiring scheme
The main components of a simplified structured wiring scheme are as follows:
- The computer has a network adapter installed with a socket for an RJ-45 connector.
- A patch cable is used to link the network card into a wall outlet with an external RJ-45 port. This must be stranded cable so that it is flexible.
- Behind each wall jack is an Insulation Displacement Connector (IDC).
- In the computer room, the cable is wired into more IDCs in a patch panel.
- Finally, another patch cable connects the RJ-45 port on the front of the patch panel to a free port on the switch.

(GTSLearning, 2014)
12.2.2 Structured cabling system

The structured cabling system is ANSI/TIA/EIA 568 standard. TIA 568 identifies the following subsystems within the cabling system:

- **Horizontal cabling**: It connects user work areas to the nearest horizontal cross-connect/distribution frame.
- **Backbone cabling**: It connects horizontal cross-connects to the main cross-connect.
- **Work area**: It is the space where user equipment is located and connected to the network.
- **Telecommunication room/equipment room**: It houses horizontal cross-connects. This is the termination point for the horizontal cabling along with a connection to backbone cabling.
- **Entrance facilities/demarc**: Special types of equipment rooms marking the point at which external cabling is joined to internal cabling. The demarcation point is where the access provider’s network terminates and the organisation’s network begins.
- **Administration**: Administration schemes are described in the TIA 606 standard. This defines a system of identifiers to use to describe the elements of the network and manage configuration changes. These are often called MACs (Moves, Adds, Changes).

(GTSLearning, 2014)
There are several options for securely routing cable. These are:
- Conduit
- Trays/J-hooks/caddies
- Staples
- Cable ties
- Cable management

(GTSLearning, 2014)

Some of the main design considerations for equipment closets are:
- Position
- The space should be of sufficient size to accommodate equipment
- Equipment should be installed in wall-mounted or free standing racks
- There should be a controlled environment (Heating, Ventilation, Air Conditioning [HVAC])
- Lighting should not be in close proximity to equipment
- The area must have an adequate power supply
- Entry to the space must be controlled and restricted to authorised personnel

(GTSLearning, 2014)

12.3 Distribution frames

A distribution frame is another way of describing a cross-connect. It is a passive device allowing the termination and cross-connection of cabling. These can be installed in a hierarchy:
- **Main Distribution Frame (MDF):** terminates external cabling and distributes backbone cabling to intermediate or horizontal cross-connects
- **Intermediate Distribution Frame (IDF):** optional level of hierarchy for distributing backbone cabling

Wiring is terminated using a punch-down block.

(GTSLearning, 2014)

12.3.1 Block

The 110 block is a type of IDC supporting 100 MHz operation (Cat 5) and better. ‘110 block’ can describe both a punch-down format and a distribution frame (or wiring block) (GTSLearning, 2014).

12.3.2 RJ-45 patch panel

A patch panel is a type of cross-connect that uses modular jacks and connectors.
12.3.3 Wiring tools and techniques

In order to ensure tidiness during cable installation, adhere to the following:
- Adhere to the specified standard.
- Leave cables out of sight, securely fastened, and routed and labelled.
- Test everything.
- Document the installation.
- Identify the paths which the cable will take.
- Install cable management components along the path and drill any access points through walls and ceilings.
- Patch panels, wall jacks and patch cords should all be wired to the same standard.
- Starting at the patch panel, label the end of the cable with the appropriate jack ID and then run it through to the work area.
- Leaving enough slack at both ends to make the connection, cut the cable and label the other end with the appropriate ID.
- Repeat for all the other cable runs! Use ties and cable management to keep the cable runs neat and tidy.
- When all the cable is in place and properly labelled, you can make the terminations to the patch panel and wall jacks.

(GTSLearning, 2014)

12.3.4 Plenum versus non-plenum cable

A plenum space is a void in a building designed to carry Heating, Ventilation and Air Conditioning (HVAC) systems.

Special fire safety requirements for electrical cable are laid in plenum spaces. Plenum-safe cables are marked CMP or MMP, while non-plenum cables are marked CMG/MMG or CM/MP. Non-plenum cabling uses Polyvinyl Chloride (PVC) jackets and insulation. Cabling that passes between two floors is referred to as riser (GTSLearning, 2014).
12.3.5 Termination tools

The range of tools that you require will, of course, depend on the cabling work that you do, but the following can be considered typical:

- Wire stripping/cutting
- Punch-down:
  - Terminate cable to Insulation Displacement Connector (IDC)
  - Formats (66, 110, Krone)
- Crimpers:
  - Attach jack (e.g. RJ-45) to patch cable
  - Avoid excessive untwisting
- Fibre-optic tools
- Cable pulling
- Labelling
- Cable testers
- Essentials

(GTSLearning, 2014)

12.4 Wiring schemes

Each conductor in a 4-pair data cable is colour-coded. Each pair is assigned a colour (blue, orange, green or brown). The first conductor in each pair has a predominantly white insulator with strips of the colour; the second conductor has an insulator with the solid colour (GTSLearning, 2014).

The ANSI/TIA/EIA 568 standard defines two methods for terminating Ethernet connectors: T568A and T568B. The wiring for T568B is shown in Figure 87 below.
Ethernet and Fast Ethernet use only two pairs in the cable: one to transmit (Tx) and the other to receive (Rx). Gigabit and 10G Ethernet use all four pairs, transmitting and receiving simultaneously (Bix) through the use of improved signal encoding methods (see Table 6 below):

**Table 6: T568A and T568B standards**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Wire colour (T568A)</th>
<th>Wire colour (T568B)</th>
<th>10/100 Mbps</th>
<th>1/10 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Green/white</td>
<td>Orange/white</td>
<td>Tx+</td>
<td>BixA+</td>
</tr>
<tr>
<td>2</td>
<td>Green</td>
<td>Orange</td>
<td>Tx-</td>
<td>BixA-</td>
</tr>
<tr>
<td>3</td>
<td>Orange/white</td>
<td>Green/white</td>
<td>Rx+</td>
<td>BixB+</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td>Blue</td>
<td></td>
<td>BixC+</td>
</tr>
<tr>
<td>5</td>
<td>Blue/white</td>
<td>Blue/white</td>
<td></td>
<td>BixC-</td>
</tr>
<tr>
<td>6</td>
<td>Orange</td>
<td>Green</td>
<td>Rx-</td>
<td>BixB-</td>
</tr>
<tr>
<td>7</td>
<td>Brown/white</td>
<td>Brown/white</td>
<td></td>
<td>BixD+</td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td>Brown</td>
<td></td>
<td>BixD-</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)
12.4.1 Crossover cable, T1 crossover cable, loopback cable

A **crossover cable** is created by wiring the connectors at each end differently, so that Tx on one connector goes directly to Rx on the other connector and vice versa (Tx/Rx reversed). The cable itself is UTP (GTSLearning, 2014).

Another type of crossover cable, called **T1 crossover**, can be used to directly connect two ISDN PRI interfaces together, typically to simulate a WAN link for testing purposes. This cable is also made up of ordinary UTPs with RJ-45 connectors (GTSLearning, 2014).

A **loopback cable** is used to test a port. It involves connecting pin 1 to pin 3 and pin 2 to pin 6. This can be done by either rewiring the jack or twisting the relevant pairs together on a cable stub. Alternatively, you can buy a prefabricated loopback plug (GTSLearning, 2014).

12.5 Installing WAN links

Establishing a WAN link means terminating the access provider’s cabling at some point in your premises, then attaching modem and/or routing equipment to that line (GTSLearning, 2014).

12.5.1 Demarcation point (demarc)

The point at which the access provider’s network terminates is called the **demarcation point** (or demarc). Access equipment that is provided or leased by the customer and installed at their site is referred to as Customer Premises Equipment (CPE). The demarc point represents the end of the telco’s responsibility for maintaining that part of the network.

A demarc extension refers to cabling that has to be run through the customer premises. A telco will run cabling to the Minimum Point Of Entry (MPOE), which is the most convenient place for the cabling to enter the building (GTSLearning, 2014).

12.5.2 Installing leased lines

A CSU/DSU describes equipment used to terminate leased or dedicate digital lines, such as T-carrier, ISDN, frame relay and so on. The function of a CSU/DSU is to provide voice and data services over these links. The line from the telco is usually terminated at a smart jack or Network Interface Unit (NIU), which contains line testing facilities for the telco to use. The DSU encodes the signal from Data Terminal Equipment (DTE) (GTSLearning, 2014).
12.6 Cable testing tools

The best time to verify wiring installation and termination is just after you have made all the connections. This means that you should still have access to the cable runs. A number of tools are available to perform tests on the physical characteristics of a cable link (GTSLearning, 2014). Some cable testers are described below.

12.6.1 Multimeters and wire map testers

Multimeters and wire map testers are used to check physical connectivity. The primary purpose of a multimeter is to test electrical circuits, but they can test for the continuity of any copper wire, the existence of a short and the integrity of a terminator. Many multimeters perform the same functions as a wire map tester. Wire map testers can identify the following problems: continuity, shorts and transpositions (GTSLearning, 2014).

12.6.2 Tone generator and probe

Tone generators and probes are used to trace a cable from one end to the other. This may be necessary when the cables are bundled and have not been labelled well. This device is also known as a ‘Fox and Hound’ or ‘toner and probe’. The tone generator is used to apply a signal to the cable, to be traced where it is used to follow the cable over ceilings and through ducts (GTSLearning, 2014).

12.6.3 Time-Domain Reflectometer (TDR)

Time-Domain Reflectometers (TDRs) are used to measure the length of a cable run and are able to locate open and short circuits, kinks/sharp bends and other imperfections in cables that could affect performance (GTSLearning, 2014).

12.6.4 Cable certifiers

Cable certifiers measure installed cable against a defined standard. They report attenuation, noise and crosstalk, etc. (GTSLearning, 2014)

12.6.5 Butt set

A butt set is a telephone handset that connects to telephone wires using crocodile clips rather than a modular jack. Butt sets can only be used to test analogue phone lines, but most have digital circuit detectors and cut-outs and built-in DSL filters (GTSLearning, 2014).
12.6.6 Environmental monitor

Heat increases the attenuation of copper data cabling. Spaces housing data equipment and cabling should be kept at an ambient temperature of between 18-24°C and at a relative humidity of 30-55%. This would normally be maintained by the building HVAC system, with environmental monitors to measure temperature and relative humidity in each space (GTSLearning, 2014).

Monitors are also available to check that the power supply is operating at the correct current and voltage. These devices are capable of alerting an administrator in the event of brownouts or surges (GTSLearning, 2014).

Network-enabled monitors can be connected to switches or connected to a computer via USB and integrated with network management software to provide an alert if environmental conditions change (GTSLearning, 2014).

12.7 Planning a SOHO network installation

Many networks are smaller, however, and may not use a typical wiring scheme. These types of networks are often called Small Office Home Office (SOHO) networks. Installing and maintaining these SOHO networks presents different challenges to the enterprise LAN environment (GTSLearning, 2014).

When planning a SOHO network installation, the following factors should be taken into consideration:

- Cable runs
- Device types
- Equipment limitations
- Environmental limitations
- Compatibility requirements

(GTSLearning, 2014)

Concluding remarks

Wiring standards provide a framework for installing a network infrastructure that will provide ROI over 10-15 years. Structured cabling uses main and horizontal cross-connects with backbone and work area cabling wired in a hierarchical star. Cross-connects come in various formats, with 110 block patch panels being the most popular for LANs. Installing cabling plant requires a professional attitude and a good toolkit. Devices used to test cable installations include multimeters, toner and probe, TDR/OTDR, cable certifiers and protocol analysers.
Self-assessment

Test your knowledge

1. What role do cross-connects play in a structured cabling system?

2. What is cable management?

3. Name a typical use of an IDF.

4. What is the significance of different IDC formats when planning a wiring job?

5. What function does a smart jack serve?

6. What cabling faults would a wire map tester detect?
Unit 13: Installing wireless networks

Unit 13 is aligned with the following learning outcome and assessment criteria:

Learning outcome
LO5: Demonstrate the ability to implement and support networked systems.

Assessment criteria
AC5.3: Examine the installation of wireless networks.

Learning objectives
After studying this unit, you should be able to:
• Distinguish between different IEEE 802.11 Wi-Fi standards
• Distinguish between ad hoc and infrastructure WLANs
• Perform a site survey and install and configure APs
• Configure wireless client devices
• Describe methods of securing and authenticating wireless connections
• Describe and differentiate wide area wireless networks

Supplementary reading

Unit 13 adapted from:

Introduction
In this unit, we will examine the different IEEE 802.11 Wi-Fi standards, ad hoc and infrastructure WLANs, installation of Access Points (Aps) and wireless client devices, methods of securing and authenticating wireless connections and the differences between wide area wireless networks.
13.1 Wi-Fi (IEEE 802.11)

IEEE 802.11 is the Wireless LAN (WLAN) standard that dominates business networking. Data is encoded into a radio carrier signal by using a modulation scheme such as Quadrature Amplitude Modulation (QAM) or Phase Shift Keying (PSK). The original 802.11 Wi-Fi standard worked at only 1 Mbps, but there are other revisions with different signalling and transmission techniques (GTSLearning, 2014).

13.1.1 Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

The IEEE 802.11 standard uses Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). Under CSMA/CA, when a station receives a frame, it performs error checking, and if the frame is complete, it responds with an Acknowledgement (ACK). If the ACK is not received, the transmitting station resends the frame until timing is out. 802.11 defines a Virtual Carrier Sense flow control mechanism to reduce collision. A station broadcasts a Request To Send (RTS) with the source and destination and the time required to transmit. The receiving station responds with a Clear To Send (CTS) and all other stations in range do not attempt to transmit within that period (GTSLearning, 2014).

13.1.2 IEEE 802.11 standards

Table 7, below, shows all the 802.11 standards with their transfer rates, channel width, Radio Frequency (RF) band and range.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Transfer rates (Mbps)</th>
<th>Channel width (MHz)</th>
<th>RF band (GHz)</th>
<th>Range (metres) indoors and outdoors</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>1 or 2</td>
<td>20</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td>802.11a</td>
<td>Up to 54</td>
<td>20</td>
<td>5</td>
<td>35 and 120</td>
</tr>
<tr>
<td>802.11b</td>
<td>Up to 11</td>
<td>20</td>
<td>2.4</td>
<td>40 and 170</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 and higher</td>
<td>20</td>
<td>2.4</td>
<td>40 and 170</td>
</tr>
<tr>
<td>802.11n</td>
<td>108 and higher</td>
<td>20 or 40</td>
<td>2.4 or 5</td>
<td>70 and 250</td>
</tr>
</tbody>
</table>

Source: GTSLearning (2014)

13.1.3 Antenna types

Most wireless devices have simple omnidirectional vertical rod-type antennas, which can receive and send a signal in all directions. To extend the signal range, you can use an antenna focused at a specific point; this is referred as unidirectional antenna (GTSLearning, 2014).
13.2 Setting up a wireless network

A WLAN can be configured in peer-to-peer or hub mode and you need to plan carefully to ensure a strong signal and effective security parameters (GTSLearning, 2014).

13.2.1 Ad hoc and infrastructure modes

802.11 compliant wireless links can be configured in different modes:

- Ad hoc ‘peer-to-peer’ or an ‘independent basic service set’
- Infrastructure:
  - Stations connect via base stations (access points [APs])
  - An AP plus attached stations is a Basic Service Set (BSS)
  - The MAC address of the AP is the BSSID
  - Each WLAN has a Service Set Identifier (SSID) or network name
  - Multiple BSSs with the same SSID form an Extended Service Set (ESS) (GTSLearning, 2014)
13.2.2 Roaming

Clients can roam between access points with the same SSID when the APs are connected by a wired network (distribution system). When the client detects that it is no longer receiving a good signal, it checks for another signal with the same SSID on other channels (GTSLearning, 2014).

13.2.3 Site surveys and channel configuration

When considering Wireless Access Point (WAP) placement, a device supporting the Wi-Fi standard should have a maximum indoor range of up to about 30m, though the weaker the signal, the lower the data transfer rate. During site surveys and channel configuration, consider the following:

- Identify placement of APs to implement and secure WLAN:
  - Determine number of users to support and usage patterns.
  - Identify environmental obstructions.
- Check signal strength in different areas.
- Use non-overlapping channels (e.g. 1, 6, 11).
- Check coverage once APs have been installed.

(GTSLearning, 2014)
13.2.4 Configuring an access point

The example below shows configuration settings on a 3Com OfficeConnect wireless AP, designed for SOHO. This device is also a 4-port network switch and ADSL-enabled router, providing a connection to the Internet. The appliance is configured via a Web (HTTP) interface (GTSLearning, 2014).
The following settings must be configured on the 3Com wireless AP:
- Channel
- Extension Channel
- Frequency
- SSID (Service Set ID)
- SSID Broadcast
- Wireless Mode

(GTSLearning, 2014)

To prevent snooping, you should enable encryption on the connection as shown in Figure 92.

![Figure 92: Configuring encryption](Source: GTSLearning (2014))

On the **Advanced** tab, you can set the Beacon Interval. The beacon is a special management frame broadcast by the AP to advertise the WLAN.
13.3 Wireless security

WLANs are subjected to data emanation or signal leakage. On a WLAN, there is no simple way to limit the signal within defined boundaries. It will propagate to the extent of the antenna's broadcast range, unless blocked by some sort of shielding or natural barrier. Data emanation means that packet sniffing a WLAN is trivially easy if you can get within 30m (GTSLearning, 2014).

13.3.1 War driving and war chalking

War driving is the practice of driving around with a wireless-enabled laptop scanning for insecure WLANs. War chalking is the practice of marking little symbols to advertise the presence of an open and exploitable AP (GTSLearning, 2014).

Due to these techniques, the crucial step in enforcing wireless security is to enable encryption. There are three schemes of encryption:

- **Wired Equivalent Privacy (WEP):**
  - There are two versions of this type of encryption (version 1 and version 2).
  - Many tools exist to crack WEP security.
  - Weak authentication due to pre-shared key.

- **Wi-Fi Protected Access (WPA/WPA 2)/Temporal Key Integrity Protocol (TKIP):**
  - Version 1 improves on WEP and allows stronger authentication (EAP).
  - Version 2 fully implements 802.11i WLAN security standard.
  - The main difference to WPA is the use of Advanced Encryption Standard (AES) for encryption.

  (GTSLearning, 2014)
13.3.2 Wi-Fi authentication

In order to secure a WLAN, you need to be able to confirm that only valid users are connecting to it. WLAN authentication comes in three forms:

- Pre-Shared Key (PSK) (group authentication)
- 802.1X/EAP/WPA Enterprise:
  - Strong authentication (multifactor)
  - Network directory authorisation
- Open

(GTSLearning, 2014)

![OfficeConnect ADSL Wireless 11g Firewall Router Wireless Settings](image)

**Figure 94: Configuring wireless authentication and encryption settings**

Source: GTSLearning (2014)

Other wireless security issues:

- Firewalling wireless links:
  - MAC address filtering
  - Firewall behind AP
- Disabling unused connections:
  - Backdoors and Rogue APs (wiphishing)
- Jamming, interference and signal strength

(GTSLearning, 2014)
13.4 Wireless WANs

Wireless technologies are now well established in terms of local and ‘personal’ area networking. There are three main technologies involved in providing Wireless WANs (WWAN) (GTSLearning, 2014). These are:

- Cellular radio:
  - GSM/IS-95 (2G)

- Packet radio:
  - WiMax:
    - Fixed and mobile deployments
    - WiMax 2 for 4G (up to 1Gbps for fixed sites)
  - 3rd Generation Partnership Project (3GPP):
    - Evolved High Speed Packet Access (HSPA+) for 3G
    - Long Term Evolution-Advanced (LTE-Advanced) for 4G

- Microwave satellite

(GTSLearning, 2014)

Concluding remarks

Wi-Fi includes specifications for transmission using a range of radio wave modulation techniques and frequencies, supporting different speeds and ranges. WLANs can be configured in a point-to-point (ad hoc) or infrastructure (access point) topology. A site survey determines the optimum positioning and tuning of access points. WLANs should be configured with the appropriate SSID, channel/frequency, security protocol (WPA) and authentication mechanism (PSK or RADIUS). Wireless security should be enforced by enabling WPA. WEP should only be used if there is no other choice. Wireless WANs are implemented using cellular and packet radio and satellite links. WiMAX and LTE offer the promise of high bandwidth, non-line-of-sight services covering several miles.

Self-assessment

Test your knowledge

1. Which IEEE WLAN standards specify a data transfer rate of up to 54 Mbps?

2. What is a BSSID?

3. What options may be available for an 802.11n network that are not supported under 802.11g?

4. What is a pre-shared key?
5. What is the main difference between WPA and WPA2?

6. What standard supports packet radio WWANs?
Unit 14: Network troubleshooting

Unit 14 is aligned with the following learning outcome and assessment criteria:

**Learning outcome**
LO5: Demonstrate the ability to implement and support networked systems.

**Assessment criteria**
AC5.4: Describe effective troubleshooting procedures.
AC5.5: Troubleshoot common connectivity scenarios.

**Learning objectives**
After studying this unit, you should be able to:
- Use effective troubleshooting procedures
- Troubleshoot common connectivity scenarios

**Supplementary reading**
Unit 14 adapted from:

**Introduction**
In this final unit of the guide, we will be exploring some effective troubleshooting procedures and how to troubleshoot common connectivity scenarios.
14.1 Troubleshooting procedures

1. Identify the problem:
   - Gather information
   - Identify symptoms
   - Question users
   - Determine if anything has changed
2. Establish a theory of probable cause (question the obvious)
3. Test the theory to determine cause:
   - Once the theory is confirmed, determine the next steps to resolve the problem.
   - If the theory is not confirmed, re-establish a new theory or escalate the problem.
   - Escalation means referring the problem to a senior technician, manager or third-party.
4. Establish a plan of action to resolve the problem and identify potential effects.
5. Implement the solution or escalate as necessary.
6. Verify full system functionality and, if applicable, implement preventive measures.
7. Document findings, actions and outcomes.

(GTSLearning, 2014)

14.2 Troubleshooting common connectivity scenarios

The following section explains how you would set about determining the cause and scope of the problem, faced with different connectivity or performance troubleshooting scenarios.

14.2.1 Troubleshooting specific topologies

- Star-wired topologies:
  - If one system is affected, then check the link from switch to host for that system
  - If more than one system is affected, check the backbone wiring between switches or the switch itself
- Backbones:
  - This is a question of determining which hosts can see which other hosts
- Mesh topologies:
  - Difficult to troubleshoot because all hosts have connections to all others
  - If Host A and B can communicate using three routes and they used to have four routes, then troubleshoot the fourth route; there may be a wiring problem there.

(GTSLearning, 2014)
14.2.2 Troubleshooting power problems
- Power problems:
  - Surge/spike
  - Brownout/blackout
- Uninterruptible Power Supply (UPS) can keep servers, switches and routers running for a few minutes. This provides time to either switch in a secondary power source (a generator) or shut down the system gracefully (to avoid data loss)
  (GTSLearning, 2014)

14.2.3 Troubleshooting cabled links
- Ping
- Verify patch cord
- Loopback on host and switch port
- Test permanent link
  (GTSLearning, 2014)

14.2.4 Cabling issues
- Opens, shorts and transpositions attenuation (distance)
- Crosstalk
- Impedance/echo/return loss
- Propagation delay/delay skew
- ElectroMagnetic Interference (EMI)
- Collisions
  (GTSLearning, 2014)

14.3 Troubleshooting intranetworking infrastructure
If the cabling is not the cause of the problem, you should check intranetwork infrastructure next. Network adapters, switches and access points operate at layers 1 and 2 in the OSI model (GTSLearning, 2014).

14.3.1 Troubleshooting network adapters
- Network adapters:
  - Loopback
  - Verify the driver
  - Speed/duplex autonegotiation
  (GTSLearning, 2014)
14.3.2 Troubleshooting hubs, bridges and switches

- Hubs, bridges and switches:
  - Check installation
  - Reboot
  - Swap out

(GTSLearning, 2014)

14.3.3 Troubleshooting fibre module

When troubleshooting a switch or router, also check that any plug-in modules (SFPs/GBICs) installed in the appliance are correctly seated and appropriate for the type of fibre being terminated (MMF or SMF). If the modules are hot-swappable, you can perform this check with the switch powered-up; otherwise, turn off the switch and reseat all modules. If available, swap out any such modules for known good ones (GTSLearning, 2014).
14.3.4 Troubleshooting wireless links

There are several sources of interference to consider:

- Bleed
- Bounce
- ElectroMagnetic Interference (EMI)
- Environmental factors, such as obstructions, standards mismatch and firmware/driver

(GTSLearning, 2014)

![Figure 96: Surveying Wi-Fi networks using inSSIDer](source)

14.4 Troubleshooting configuration issues

If you can rule out a problem at the physical layer, the next thing to check is basic addressing and protocol configuration at the data link (MAC addressing) and network (IP addressing) layers (GTSLearning, 2014).

14.4.1 Troubleshooting IP configuration and routing

Use `ipconfig/ifconfig` and `route` to check:

- IP address
- Subnet Mask (IPv4)/Network Prefix (IPv6)
- Default Gateway
- Any routes in the routing table of a host
- DNS server IP addresses

(GTSLearning, 2014)
14.4.2 Troubleshooting duplicate IP address issues

Two systems could end up with the same IP address because of a configuration error; perhaps both addresses were statically assigned or one was assigned an address that was part of a DHCP scope, by mistake. If Windows detects a duplicate IP address, it will display a warning and disable IP. Linux does not typically check for duplicate IP addresses (GTSLearning, 2014).
If there are two systems with duplicate IPs, a sort of ‘race condition’ will determine which receives traffic and set them to use unique addresses (GTSLearning, 2014).

### 14.4.3 Troubleshooting VLANs

VLANs:
- Check configuration on switch
- Check VLAN membership
- Check services available to VLAN

(GTSLearning, 2014)

### 14.4.4 Wireless configuration

- Check that the clients are configured with the correct SSID/ESSID
- Check that the client is configured to use the correct channel
- Check that the client can support the encryption and authentication standards configured on the access point – a driver update or OS patch may be needed
- Check that the authentication settings are the same on all devices. If a Preshared Key (PSK) is used, make sure it is entered correctly

(GTSLearning, 2014)

### 14.4.5 Troubleshooting wrong DNS/name resolution

- Verify name resolution sequence
- Test services with HOSTS
- Check client’s DNS server configuration
- Check server availability
14.5 Troubleshooting internetworking infrastructure

When you start to approach problems that require changes to major infrastructure, it may be appropriate to simply identify the problem and escalate it (GTSLearning, 2014).
14.5.1 Route problems
If you can Ping a host’s default gateway and additionally Ping some hosts on remote networks, but not all hosts, then there is a route problem. This will be because a router has gone offline and there is no alternative path to that network. Another common possibility is that a security appliance such as a firewall is blocking communications. Alternatively, some routing tables may have missing routes, or contain incorrect routing information (GTSLearning, 2014).

14.5.2 Routing loops
Routing loops happen when errors occur in a routing algorithm, resulting in packets looping endlessly around an internetwork. Most modern routing protocols, such as EIGRP, OSPF and IS-IS, avoid routing loops with built-in prevention protocols. Older routing protocols, such as RIP and IGRP, are prone to routing loops (GTSLearning, 2014).

The following methods are implemented by routers to avoid looping:
• Defining infinity
• Split horizon
• Holddown timer

(GTSLearning, 2014)

14.5.3 Maximum Transmission Unit (MTU) black hole
When packets move across routers from one segment to another, it is possible that the Maximum Transmission Unit (MTU) may be different from one segment to another. In cases where the receiving segment has a lower MTU, it may not be possible for some packets to be forwarded. In such cases, depending on the IP header, the packet may be fragmented, or it may be dropped and an ICMP message sent to the source. If the ICMP response cannot reach the source, the original packets are never re-sent, and so disappear from the network. A router that creates such a situation is called MTU black hole. This can be diagnosed and located by a combination of Ping and tracert/traceroute commands (GTSLearning, 2014).

14.5.4 Proxy ARP
Proxy ARP is a feature whereby a router responds to an ARP request for an IP address on a different subnet but the same physical segment (GTSLearning, 2014).
14.5.5 Switching loops (broadcast storms)

Switching loops cause broadcast frames to circulate the network permanently. Such loops at the data link layer can cause broadcast storms. A broadcast storm may quickly consume all link bandwidth and crash network appliances. The Spanning Tree Protocol is supposed to prevent such loops, but this can fail if STP communications between switches do not work correctly (GTSLearning, 2014).

Figure 101: Configuring broadcast storm control settings on a Dell switch

Source: GTSLearning (2014)

14.6 Troubleshooting services

Troubleshooting issues farther up the network stack become more and more product-specific; but consider some of the following scenarios:

- Security appliances/software:
  - Technologies such as firewall, NAT and IPS
- Establishing a session:
  - Troubleshooting Windows
  - Troubleshooting non-Windows networks
- DHCP:
  - Server offline
  - Address pool exhausted
  - Scopes misconfigured
  - Duplicate services
• DNS:
  o No DNS server address or wrong DNS server address
  o Incorrect DNS suffix
  o DNS server offline
  o Check DNS service configuration
• User problems:
  o Forgotten passwords
  o CAPS lock left on
  o Locked accounts
  o Printers off

(GTSLearning, 2014)

Concluding remarks
Troubleshooting should be completed against a checklist of best practice actions (gather information, establish scope, establish cause, establish authority, define an action plan, implement the plan, test the solution and document the solution). Taking a layered approach can help to troubleshoot specific connectivity scenarios.

Self-assessment

Test your knowledge

1. What are the two basic principles of identifying the cause of a problem?

2. In what sort of circumstances should you escalate a problem?

3. Network monitoring software can detect ‘broadcast storms’. What is usually the cause of broadcast storms?

4. How would you test for excessive attenuation in a network link?

5. Your network manager has told you to fix a problem with WLAN bleed. What are you going to do?

6. Users on a floor served by a single switch cannot get a network connection. What is the best first step?
## Glossary

<table>
<thead>
<tr>
<th>Access Control Lists (ACL)</th>
<th>A list configured on a resource or appliance that determines access/deny access rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Point (AP)</td>
<td>See: Wireless Access Point (WAP)</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>Used by IP to find the hardware address of a computer network card based on the IP address.</td>
</tr>
<tr>
<td>ADSL</td>
<td>See: DSL</td>
</tr>
<tr>
<td>Antenna</td>
<td>Used to focus a signal to a particular point or more widely</td>
</tr>
<tr>
<td>Application layer</td>
<td>OSI model layer providing support to applications requiring network services</td>
</tr>
<tr>
<td>Application Programming Interface (API)</td>
<td>A library of programming utilities</td>
</tr>
<tr>
<td>Asynchronous Transfer Mode (ATM)</td>
<td>A network technology based on sending data in cells or packets of a fixed size.</td>
</tr>
<tr>
<td>Attenuation</td>
<td>Degradation of a signal as it travels over media</td>
</tr>
<tr>
<td>Authentication</td>
<td>Identifies a user on a network</td>
</tr>
<tr>
<td>Automatic Private IP Addressing (APIPA)</td>
<td>Developed as a means for clients configured to obtain an address automatically that could not contact a DHCP server to communicate on the local subnet</td>
</tr>
<tr>
<td>Backbone</td>
<td>A backbone is a fast link that connects the various segments of a network</td>
</tr>
<tr>
<td>Backup</td>
<td>Recovery of data can be provided through the use of backup system</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The range of frequencies supported by a particular media type and more generally the maximum data rate supported by a link</td>
</tr>
<tr>
<td>Baseband</td>
<td>Baseband transmission uses the complete bandwidth of the media as a single transmission path</td>
</tr>
<tr>
<td>Baseline</td>
<td>The point from which something varies</td>
</tr>
<tr>
<td>Beacon</td>
<td>A special management frame broadcast by the AP to advertise the WLAN</td>
</tr>
<tr>
<td>Bonding</td>
<td>Using multiple network adapters for a single link for fault tolerance and load balancing</td>
</tr>
<tr>
<td>Border Gateway Protocol (BGP)</td>
<td>A routing protocol exchanges routing information between autonomous systems while guaranteeing loop free path selection. BGP is the principal route advertising protocol used by major companies and ISPs on the Internet</td>
</tr>
<tr>
<td>Bridge</td>
<td>A bridge can be used to divide an overloaded segments</td>
</tr>
<tr>
<td>Broadband</td>
<td>Broadband transmission divides the available media bandwidth into a number of transmission paths or channel</td>
</tr>
<tr>
<td>Broadcast</td>
<td>A packet sent to all hosts on the local network or subnet</td>
</tr>
<tr>
<td>Buffer overflow</td>
<td>One of a number of techniques used by malware attempting to exploit vulnerabilities in software</td>
</tr>
<tr>
<td>Bus topology</td>
<td>A linear network with all nodes attached directly to the main cable</td>
</tr>
<tr>
<td>Butt set</td>
<td>A telephone handset that connects to telephone wires using crocodile clips rather than a modular jack</td>
</tr>
<tr>
<td>Cable modem</td>
<td>A cable Internet connection is usually available along with a cable telephone</td>
</tr>
<tr>
<td>Cable stripper</td>
<td>Tool for stripping the cable jacket</td>
</tr>
<tr>
<td>Cable tester</td>
<td>Troubleshooting devices designed to locate breaks in cable runs</td>
</tr>
<tr>
<td>Campus Area Network (CAN)</td>
<td>It is limited in scope to a single geographical location, but this may exceed the size normally defined for a LAN</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Carrier Sense Multiple Access (CSMA) protocols</strong></td>
<td>The CSMA protocols allow contention-based networks to successfully communicate by detecting activity on the network media and reacting to this.</td>
</tr>
<tr>
<td><strong>Certificate Authority (CA)</strong></td>
<td>A server responsible for issuing and managing digital certificates.</td>
</tr>
<tr>
<td><strong>Challenge Handshake Authentication Protocol (CHAP)</strong></td>
<td>Authentication scheme developed for dial-up networks that uses an encrypted three-way handshake to authenticate the client to the server.</td>
</tr>
<tr>
<td><strong>Channel Service Unit/Data Service Unit (CSU/DSU)</strong></td>
<td>The DSU encodes the signal from Data Terminal Equipment (DTE). The CSU is used to perform diagnostic tests on the line.</td>
</tr>
<tr>
<td><strong>Circuit switching</strong></td>
<td>Form of switching that establishes a temporary dedicated path between nodes.</td>
</tr>
<tr>
<td><strong>Classless Inter-Domain Routing (CIDR)</strong></td>
<td>An addressing scheme for IP addresses, providing greater flexibility in defining the domain than was possible with simple class A, B and C addressing.</td>
</tr>
<tr>
<td><strong>Class (IP addressing)</strong></td>
<td>IP addressing divides ranges of addresses into classes to allow for public networks of different sizes.</td>
</tr>
<tr>
<td><strong>Client</strong></td>
<td>A network client provides connectivity to servers.</td>
</tr>
<tr>
<td><strong>Contention</strong></td>
<td>In a contention-based system, each network device competes with the other connected devices for use of the transmission media.</td>
</tr>
<tr>
<td><strong>Cross-connect</strong></td>
<td>A distribution frame providing a central termination point for cabling.</td>
</tr>
<tr>
<td><strong>Crossover cable</strong></td>
<td>Cabling where the transmit pair at one end is connected to the receive pair at the other.</td>
</tr>
<tr>
<td><strong>Crosstalk</strong></td>
<td>A phenomenon whereby one wire causes interference in another as a result of their close proximity.</td>
</tr>
<tr>
<td><strong>Data link layer</strong></td>
<td>OSI model layer responsible for transferring data between nodes.</td>
</tr>
<tr>
<td><strong>Default gateway</strong></td>
<td>The term used in TCP/IP networking for a router.</td>
</tr>
<tr>
<td><strong>Demarc</strong></td>
<td>It represents the end of the access provider’s network.</td>
</tr>
<tr>
<td><strong>Demilitarised Zone (DMZ)</strong></td>
<td>A private network connected to the Internet must be protected against intrusion from the Internet.</td>
</tr>
<tr>
<td><strong>Dense Wave Division Multiplexing (DWDM)</strong></td>
<td>A technology for multiplexing multiple signals on a single fibre using different wavelengths.</td>
</tr>
<tr>
<td><strong>Digital certificate</strong></td>
<td>An encrypted certificate that can be attached to a file to confirm who created the file and that the file has not been tampered with.</td>
</tr>
<tr>
<td><strong>Digital Subscriber Line (DSL)</strong></td>
<td>A technology for transferring data over voice-grade telephone lines.</td>
</tr>
<tr>
<td><strong>Disaster recovery</strong></td>
<td>Contingency planning to provide for speedy resumption of services and data after a critical event.</td>
</tr>
<tr>
<td><strong>Domain Information Gopher (Dig)</strong></td>
<td>Utility to query a DNS and return information about a particular domain name.</td>
</tr>
<tr>
<td><strong>Domain Name System (DNS)</strong></td>
<td>A system used on the Internet for translating names of domains and their publicly advertised network nodes into IP addresses.</td>
</tr>
<tr>
<td><strong>Duplex</strong></td>
<td>It refers to the ability of connectivity media and hardware to support the simultaneous reception and transmission of data.</td>
</tr>
<tr>
<td><strong>Dynamic Host Configuration Protocol (DHCP)</strong></td>
<td>A protocol used to automatically assign IP address and configure TCP/IP for network clients.</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>Scrambling the characters used in a message so that the message can be seen but not understood unless it can be deciphered.</td>
</tr>
<tr>
<td>Glossary Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Ethernet (802.3)</strong></td>
<td>The most popular type of LAN technology</td>
</tr>
<tr>
<td><strong>Ethernet Distribution Frame (EDF)</strong></td>
<td>Cross-connect for Metro Ethernet networks to connect the fibre link from the access provider to premises wiring</td>
</tr>
<tr>
<td><strong>Extensible Authentication Protocol (EAP)</strong></td>
<td>Defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves</td>
</tr>
<tr>
<td><strong>Extranet</strong></td>
<td>A TCP/IP-based network that provides distributed, authenticated access to resources</td>
</tr>
<tr>
<td><strong>Fault tolerance (redundancy)</strong></td>
<td>Protection against system failure by providing extra capacity</td>
</tr>
<tr>
<td><strong>Fibre Distributed Data Interface (FDDI)</strong></td>
<td>It is a 100 Mbps token passing network developed for use in MAN-like networks</td>
</tr>
<tr>
<td><strong>Fibre-optic cable</strong></td>
<td>Cable type that uses light as the signalling medium</td>
</tr>
<tr>
<td><strong>File Transfer Protocol (FTP)</strong></td>
<td>A method of transferring files from one computer across the network</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>A range of devices and software products designed to restrict access from one network zone to another to defined IP address ranges or TCP/UDP application ports</td>
</tr>
<tr>
<td><strong>Frame</strong></td>
<td>The basic unit of data that is transmitted on a network</td>
</tr>
<tr>
<td><strong>Frame relay</strong></td>
<td>Packet-Switched WAN protocol running over T-carrier or ISDN</td>
</tr>
<tr>
<td><strong>Frequency Division Multiplexing (FDM)</strong></td>
<td>Splitting a channel into multiple sub-carriers based on frequency bands</td>
</tr>
<tr>
<td><strong>Frequency Hopping Spread Spectrum (FHSS)</strong></td>
<td>A mechanism for transmitting data over traffic</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>A device used to connect networks using dissimilar protocols so that information can be passed from one to another</td>
</tr>
<tr>
<td><strong>Honeypot/honeynet</strong></td>
<td>A server set up to entice attacks</td>
</tr>
<tr>
<td><strong>Hop</strong></td>
<td>A path from a host to a router or from router to router</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>A device that can directly communicate on a network</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>This command returns the hostname</td>
</tr>
<tr>
<td><strong>Hybrid topology</strong></td>
<td>A network that uses a combination of physical or logical topologies</td>
</tr>
<tr>
<td><strong>Hyper Text Transfer Protocol (HTTP)</strong></td>
<td>A network protocol for the transfer of Web or intranet pages</td>
</tr>
<tr>
<td><strong>Industry of Electronic and Electrical Engineers (IEEE)</strong></td>
<td>A professional body to oversee the development and registration of electronic standards</td>
</tr>
<tr>
<td><strong>Insulation Displacement Connector (IDC)</strong></td>
<td>Block used to terminate twisted-pair cabling</td>
</tr>
<tr>
<td><strong>Integrated Services Digital Network (ISDN)</strong></td>
<td>A digital circuit-switched technology for voice, video and data</td>
</tr>
<tr>
<td><strong>Intermediate System-Intermediate System (IS-IS)</strong></td>
<td>A link state interior gateway routing protocol intended for routing operations between devices that are part of the same autonomous system</td>
</tr>
<tr>
<td><strong>Internet</strong></td>
<td>A worldwide network of networks that is based on the TCP/IP protocol</td>
</tr>
<tr>
<td><strong>Internet Control Message Protocol (ICMP)</strong></td>
<td>Protocols used for error reporting during transmission of data</td>
</tr>
<tr>
<td><strong>Internet Group Management Protocol (IGMP)</strong></td>
<td>TCP/IP suite network protocol supporting multicast operations</td>
</tr>
<tr>
<td><strong>Internet Message Access Protocol (IMAP4)</strong></td>
<td>TCP/IP application protocol providing a means for a client to access email messages stored in a mailbox on a remote server</td>
</tr>
<tr>
<td><strong>Internet Protocol (IP)</strong></td>
<td>The protocols responsible for routing on the Internet</td>
</tr>
<tr>
<td><strong>Intranet</strong></td>
<td>A network designed for information processing within a company or organisation</td>
</tr>
<tr>
<td>Term</td>
<td>Definition/Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intrusion Detection System (IDS)</td>
<td>Software or security appliance designed to monitor network traffic (NIDS) or configuration files and logs on a host (HIDS) to record and detect unusual activity</td>
</tr>
<tr>
<td>ipconfig/ifconfig</td>
<td>A utility providing information about the IP configuration of a workstation</td>
</tr>
<tr>
<td>IPsec</td>
<td>Layer 3 protocol suite providing security for TCP/IP</td>
</tr>
<tr>
<td>Jitter</td>
<td>A variation in the time it takes for a signal to reach the recipient</td>
</tr>
<tr>
<td>Load balancer</td>
<td>A type of switch or router that distributes client requests between different resources</td>
</tr>
<tr>
<td>Local Area Network (LAN)</td>
<td>Defined as a network that does not exceed a distance of 2 km from end to end</td>
</tr>
<tr>
<td>Logical Link Control (LLC)</td>
<td>A division of the data link layer responsible for establishing and maintaining a link between communicating devices for the transmission of frames</td>
</tr>
<tr>
<td>Mailbox</td>
<td>Part of a message store designed to receive emails for a particular recipient</td>
</tr>
<tr>
<td>Main Distribution Frame (MDF)</td>
<td>A cross-connect distributing backbone wiring to horizontal cross-connects through a building and connecting to an external access provider network</td>
</tr>
<tr>
<td>Maximum Transmission Unit (MTU)</td>
<td>The maximum size in bytes of a packet’s payload</td>
</tr>
<tr>
<td>Media</td>
<td>The transmission medium used to establish network connectivity</td>
</tr>
<tr>
<td>Media Access Control (MAC)</td>
<td>A unique hardware address that is hard-coded into a network card by the manufacturer</td>
</tr>
<tr>
<td>Media converter</td>
<td>Device to convert one media type to another</td>
</tr>
<tr>
<td>Metropolitan Area Network (MAN)</td>
<td>Defined as a network that covers the area of a city</td>
</tr>
<tr>
<td>Multicast</td>
<td>A packet sent to selection of hosts</td>
</tr>
<tr>
<td>Multimeter</td>
<td>Used to check physical connectivity</td>
</tr>
<tr>
<td>Multiprotocol Label Switching (MPLS)</td>
<td>Provides traffic engineering (congestion control), class of service and Quality of Service within a packet-switched network</td>
</tr>
<tr>
<td>nbtstat</td>
<td>Utility to show NetBIOS information</td>
</tr>
<tr>
<td>NetBIOS Enhanced User Interface (NetBEUI)</td>
<td>A small and fast protocol that functions with little memory but can be routed by using token ring routing</td>
</tr>
<tr>
<td>Network Address Translation (NAT)</td>
<td>Allows companies to use private addressing on the LAN and still allow hosts to connect to the Internet</td>
</tr>
<tr>
<td>Network</td>
<td>A network consists of two or more computers connected to each other by an appropriate transmission medium which allows them to share data</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>Allows a physical connection between the computer and the transmission media</td>
</tr>
<tr>
<td>Network layer</td>
<td>OSI model layer responsible for routing data between different networks</td>
</tr>
<tr>
<td>Network Time Protocol (NTP)</td>
<td>TCP/IP application protocol allowing machines to synchronise to the same time check</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>A hierarchical link-state interior gateway routing protocol</td>
</tr>
<tr>
<td>Open Systems Interconnect (OSI)</td>
<td>It aids the understanding of how a network system functions in terms of both hardware and software components</td>
</tr>
<tr>
<td>Optical Time Domain Reflectometer (OTDR)</td>
<td>Used to measure the length of a cable run and are able to locate faults</td>
</tr>
<tr>
<td>Term</td>
<td>Definition/Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Patch panel</td>
<td>A type of cross-connect with IDCs to terminate fixed cabling on one side and modular jacks to make cross-connections to other equipment on the other</td>
</tr>
<tr>
<td>Packet sniffer</td>
<td>Used to capture information about a network and data that is being transmitted</td>
</tr>
<tr>
<td>Packet switching</td>
<td>A way to make more efficient use of bandwidth by splitting data into small packets and routing them via any available path</td>
</tr>
<tr>
<td>Passive Optical Network (PON)</td>
<td>This technology underpins some ‘near’ fibre solutions</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Lowest layer of the OSI model providing for the transmission and receipt of data bits from node to node</td>
</tr>
<tr>
<td>Ping</td>
<td>Command-line utility for testing TCP/IP configuration</td>
</tr>
<tr>
<td>Plenum</td>
<td>Plenum cable is designed to be fire resistant and uses Teflon coatings for the jacket material so it produces a minimal amount of smoke</td>
</tr>
<tr>
<td>Post Office Protocol (POP3)</td>
<td>A protocol used to access mail over the Internet.</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>Specification allowing power to be supplied via switch ports and ordinary data cabling to devices</td>
</tr>
<tr>
<td>Presentation layer</td>
<td>Transforms data between the formats used by the network and applications</td>
</tr>
<tr>
<td>Protocol</td>
<td>Any set of rules</td>
</tr>
<tr>
<td>Protocol analyser</td>
<td>Software that intercepts network traffic and displays the captured packets for analysis, allowing inspection of the packet headers and payload</td>
</tr>
<tr>
<td>Proxy server</td>
<td>A server that mediates the communication between a client and another server</td>
</tr>
<tr>
<td>Public Switched Telephone Network (PSTN)</td>
<td>It is capable of carrying more than simply voice-call services</td>
</tr>
<tr>
<td>Punch down tool</td>
<td>Tool for terminating UTP cable to an IDC in a wall outlet or patch panel</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>Systems that differentiate data passing over the network that can reserve bandwidth for a particular applications</td>
</tr>
<tr>
<td>Repeater</td>
<td>It is used to amplify signal and extend the maximum allowable distance for a media type</td>
</tr>
<tr>
<td>Ring topology</td>
<td>All computers are connected in a circle</td>
</tr>
<tr>
<td>Route</td>
<td>Command utility to configure and manage the routing table on a Windows or Linux host</td>
</tr>
<tr>
<td>Routing Information Protocol (RIP)</td>
<td>A distance vector based routing protocol that uses a hop count to determine the distance to the destination network</td>
</tr>
<tr>
<td>Routing table</td>
<td>A host’s routing table contains information about routes to other hosts</td>
</tr>
<tr>
<td>Server</td>
<td>In a server-based networks, a central machine provides dedicated file, print, application and user management services to clients</td>
</tr>
<tr>
<td>Session layer</td>
<td>OSI model layer that provides services for applications that need to talk to one another</td>
</tr>
<tr>
<td>Service Set ID (SSID)</td>
<td>Identifies a particular WLAN</td>
</tr>
<tr>
<td>Simple Mail Transfer Protocol (SMTP)</td>
<td>An Internet protocol for sending and receiving email messages.</td>
</tr>
<tr>
<td>SONET</td>
<td>High-speed fibre-optic network used for the new generation of telecommunications backbones</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Protocol allowing multiple bridges/switches to arrange themselves in such a way as to avoid loop-free broadcast communications when redundant links are present between devices</td>
</tr>
<tr>
<td>Straight-through cable</td>
<td>Cabling where the transmit pair at one end is connected to the transmit pair at the other</td>
</tr>
<tr>
<td><strong>Straight Tip (ST) connector</strong></td>
<td>Uses a push-and-twist locking mechanism</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td><strong>Star topology</strong></td>
<td>All devices are connected to a central device</td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
<td>A portion of a network in which all devices share a common prefix on their IP address</td>
</tr>
<tr>
<td><strong>Subnet mask</strong></td>
<td>Used to distinguish between a network ID and host ID within a single IP address</td>
</tr>
<tr>
<td><strong>Subscriber Connector (SC)</strong></td>
<td>Push-pull fibre-optic connector available in simplex and duplex versions</td>
</tr>
<tr>
<td><strong>Supernetting</strong></td>
<td>A solution to the shortage of publicly addressable Class B network addresses on the Internet</td>
</tr>
<tr>
<td><strong>Switch</strong></td>
<td>Receives incoming data into a buffer then the destination MAC address is compared with an address table</td>
</tr>
<tr>
<td><strong>Telnet</strong></td>
<td>TCP/IP application protocol supporting remote command-line administration of a host</td>
</tr>
<tr>
<td><strong>Time Domain Reflectometer (TDR)</strong></td>
<td>Used to measure the length of a cable run and are able to locate open and short circuits, sharp bends and other imperfections in cable that could affect performance</td>
</tr>
<tr>
<td><strong>Toner probe</strong></td>
<td>A network tone generator and probe used to trace a cable from one end to the other</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>The shape or structure of a network</td>
</tr>
<tr>
<td><strong>Tracert/traceroute</strong></td>
<td>Utility used to trace the route taken by a packet as it hops to the destination host on a remote network</td>
</tr>
<tr>
<td><strong>Transmission Control Protocol (TCP)</strong></td>
<td>Provides connection-oriented and guaranteed delivery of packets</td>
</tr>
<tr>
<td><strong>Transmission Control Protocol/Internet Protocol (TCP/IP)</strong></td>
<td>Network protocol suite used by most operating systems and the Internet</td>
</tr>
<tr>
<td><strong>Transport layer</strong></td>
<td>OSI model layer responsible for ensuring reliable data delivery</td>
</tr>
<tr>
<td><strong>Trivial File Transfer Protocol (TFTP)</strong></td>
<td>A simplified form of FTP supporting only file copying</td>
</tr>
<tr>
<td><strong>Trunks</strong></td>
<td>Backbone links between switches and routers</td>
</tr>
<tr>
<td><strong>Twisted pair cable</strong></td>
<td>Common type of cable that has been extensively used for telephone and data systems</td>
</tr>
<tr>
<td><strong>Unicast</strong></td>
<td>A packet sent to a single host</td>
</tr>
<tr>
<td><strong>Uniform Resource Locator (URL)</strong></td>
<td>Provides a standard way to address any resource on the Internet</td>
</tr>
<tr>
<td><strong>Virtual LAN (VLAN)</strong></td>
<td>A virtual LAN is a separate network, created using switching technology</td>
</tr>
<tr>
<td><strong>Voice over IP (VoIP)</strong></td>
<td>Can be cost-effective way of providing telephony services to end users over corporate IP networks or even public IP networks</td>
</tr>
<tr>
<td><strong>War driving and war chalking</strong></td>
<td>War driving is the practice of using a Wi-Fi sniffer to detect WLANs and then either making use of them. War chalking is the activity of marking out WLAN locations for other war drivers</td>
</tr>
<tr>
<td><strong>Web</strong></td>
<td>The collection of servers providing HTTP based services on the Internet</td>
</tr>
<tr>
<td><strong>Web browser</strong></td>
<td>A software application which enables a user to display and interact with text, images, videos, music, games and other information typically located on a Web page at a website on the World Wide Web or a local area network</td>
</tr>
<tr>
<td><strong>Wide Area Network (WAN)</strong></td>
<td>A network that covers a larger area than campus or building</td>
</tr>
<tr>
<td><strong>Wi-Fi (IEEE 802.11)</strong></td>
<td>IEEE standard for wireless networking based on spread spectrum radio transmission in the 2.4 GHz and 5 GHz</td>
</tr>
<tr>
<td><strong>Wi-Fi Protected Access (WPA)</strong></td>
<td>Improved security mechanism for Wi-Fi and supports EAP</td>
</tr>
<tr>
<td><strong>Wire crimper</strong></td>
<td>Device for joining cable to connector</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>Wired Equivalent Privacy (WEP)</td>
<td>Uses an encryption technology that is simple to crack and only supports preshared keys for authentication</td>
</tr>
<tr>
<td>Wireless</td>
<td>Network connectivity that uses electromagnetic waves as the transmission medium</td>
</tr>
<tr>
<td>Wireless Access Point (AP)</td>
<td>A transceiver providing connectivity between wireless client devices and a wired network</td>
</tr>
<tr>
<td>X.25</td>
<td>Mature but low-bandwidth packet switching WAN technology</td>
</tr>
<tr>
<td>Zero Configuration Networks (ZEROCONF)</td>
<td>The Internet Engineering Task Force is working on ZEROCONF networking, which aims to provide IP level networking without requiring a network administrator</td>
</tr>
</tbody>
</table>
Bibliography

GTSLearning. 2014. *Network technologies study notes.*
CTI is part of Pearson, the world’s leading learning company. Pearson is the corporate owner, not a registered provider nor conferrer of qualifications in South Africa. CTI Education Group (Pty) Ltd. is registered with the Department of Higher Education and Training as a private higher education institution under the Higher Education Act, 101, of 1997. Registration Certificate number: 2004/HE07/004. www.cti.ac.za.