



# CompTIA Network+

## N10-006

### Official Study Guide

# INSTRUCTOR EDITION



**OFFICIAL**

MULTI-LAYERED LEARNING  
TOOLS INCLUDED



**CompTIA Network+ Certification  
Support Skills (Exam N10-006)**  
Instructor Edition  
Study Notes

G524Teng ver025 (PREVIEW)

## Acknowledgements

Course Developers ..... James Pengelly and Mark Waldron



[www.gtslearning.com](http://www.gtslearning.com)

This courseware is owned, published, and distributed by **gtslearning**, the world's only specialist supplier of CompTIA learning solutions.

✉ [sales@gtslearning.com](mailto:sales@gtslearning.com)

☎ +44 (0)20 7887 7999 📠 +44 (0)20 7887 7988

📄 Unit 127, Hill House, 210 Upper Richmond Road,  
London SW15 6NP, UK

### COPYRIGHT

This courseware is copyrighted ©2015 *gtslearning*. Product images are the copyright of the vendor or manufacturer named in the caption and used by permission. No part of this courseware or any training material supplied by the publisher to accompany the courseware may be copied, photocopied, reproduced, or re-used in any form or by any means without permission in writing from the publisher. Violation of these laws will lead to prosecution.

All trademarks, service marks, products, or services are trademarks or registered trademarks of their respective holders and are acknowledged by the publisher.

### LIMITATION OF LIABILITY

Every effort has been made to ensure complete and accurate information concerning the material presented in this course. Neither the publisher nor its agents can be held legally responsible for any mistakes in printing or for faulty instructions contained within this course. The publisher appreciates receiving notice of any errors or misprints.

Information in this course is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Where the course and all materials supplied for training are designed to familiarize the user with the operation of software programs and computer devices, the publisher urges the user to review the manuals provided by the product vendor regarding specific questions as to operation.

There are no warranties, expressed or implied, including warranties of merchantability or fitness for a particular purpose, made with respect to the materials or any information provided herein. Neither the author nor publisher shall be liable for any direct, indirect, special, incidental, or consequential damages arising out of the use or the inability to use the contents of this course.

**Warning** All gtslearning products are supplied on the basis of a single copy of a course per student. Additional resources that may be made available from gtslearning may only be used in conjunction with courses sold by gtslearning. No material changes to these resources are permitted without express written permission from gtslearning. These resources may not be used in conjunction with content from any other supplier.

**If you suspect that this course has been copied or distributed illegally,  
please telephone or email gtslearning.**

# Table of Contents

<b>Course Introduction</b>	<b>i</b>
Table of Contents .....	iii
About This Course .....	ix
<b>Module 1 / Topologies and Infrastructure</b>	<b>1</b>
<b>Module 1 / Unit 1</b>	
<i>Topologies and the OSI Model</i>	3
Key Features of Networks .....	3
Clients and Servers .....	6
Network Topologies .....	8
The OSI Model .....	14
Physical Layer .....	17
Data Link Layer .....	17
Network Layer .....	20
Upper Layers .....	21
OSI Model Summary .....	23
<b>Module 1 / Unit 2</b>	
<i>Ethernet</i>	25
Media Types and Modulation .....	25
Signaling .....	27
Media Access Control .....	29
Ethernet Frames .....	32
Legacy Ethernet Standards .....	34
Modern Ethernet Standards .....	36
MAC Addressing .....	38
Address Resolution Protocol (ARP) .....	40
Protocol Analyzers .....	43
<b>Module 1 / Unit 3</b>	
<i>Hubs, Bridges, and Switches</i>	46
Hubs and Bridges .....	46
Switches .....	49
Managing a Switch .....	51
Switch Interface Configuration .....	53
Virtual LANs (VLAN) .....	56
Spanning Tree Protocol (STP) .....	59
Power over Ethernet (PoE) .....	61
<b>Module 1 / Unit 4</b>	
<i>Infrastructure and Design</i>	63
Network Infrastructure Implementations .....	63
Planning an Enterprise Campus Network .....	65
Planning a SOHO Network Installation .....	68

Planning an Industrial Control System .....	72
TCP/IP Protocol Suite.....	73

<b>Module 1 / Summary</b>	
<i>Topologies and Infrastructure</i>	79

<b>Module 2 / Addressing and Routing</b>	<b>81</b>
--	-----------

<b>Module 2 / Unit 1</b>	
<i>Internet Protocol</i>	83

Internet Protocol Basics .....	83
Subnet Masks .....	86
ipconfig / ifconfig .....	87
IP Routing Basics .....	89
ICMP and ping .....	90

<b>Module 2 / Unit 2</b>	
<i>IPv4 Addressing</i>	95

IP Addressing Schemes .....	95
Subnetting and Classless Addressing.....	98
Planning an IP Addressing Scheme.....	100
Public Internet Addressing .....	102
Multicast and IGMP .....	104

<b>Module 2 / Unit 3</b>	
<i>DHCP and APIPA</i>	106

Static versus Dynamic IP Addressing .....	106
Configuring DHCP .....	109

<b>Module 2 / Unit 4</b>	
<i>IPv6 Addressing</i>	114

IPv6 Address Format .....	114
IPv6 Addressing Schemes.....	117
Configuring IPv6 Addresses .....	121
Migrating to IPv6.....	122

<b>Module 2 / Unit 5</b>	
<i>Routing</i>	125

Routing Basics .....	125
Routing Algorithms and Metrics .....	128
Routing Protocols .....	130
Administrative Distance and Route Redistribution .....	134
IPv4 and IPv6 Internet Routing .....	135
High Availability Routing .....	136
Installing and Configuring Routers .....	137
Routing Troubleshooting Tools .....	139

<b>Module 2 / Summary</b>	
<i>Addressing and Routing</i>	145

<b>Module 3 / Unit 1</b>	
<i>Transport Protocols</i>	149
Transmission Control Protocol (TCP) .....	149
User Datagram Protocol (UDP) .....	152
TCP/IP Ports .....	153
netstat .....	154
<b>Module 3 / Unit 2</b>	
<i>Name Resolution</i>	156
Host Names and FQDNs .....	156
Domain Name System (DNS) .....	157
Configuring DNS Servers .....	160
nslookup and nbtstat .....	163
<b>Module 3 / Unit 3</b>	
<i>Troubleshooting</i>	166
Troubleshooting Procedures .....	166
Identifying the Problem .....	167
Establishing a Probable Cause .....	169
Establishing a Plan of Action .....	172
Troubleshooting Connectivity Issues .....	174
Troubleshooting Configuration Issues .....	177
Troubleshooting Internetworking .....	180
Troubleshooting Services .....	183
<b>Module 3 / Unit 4</b>	
<i>Applications and Services</i>	186
TCP/IP Services .....	186
HTTP and HTTPS .....	186
FTP, TFTP, and SMB .....	188
Email (SMTP / POP / IMAP) .....	190
VoIP and VTC .....	192
Real-time Services Protocols .....	194
Quality of Service .....	197
Packet Shapers .....	199
Load Balancers .....	201
Multilayer Switches .....	203
<b>Module 3 / Unit 5</b>	
<i>Management and Monitoring</i>	206
Performance Monitoring .....	206
Network Monitoring Utilities .....	207
Logs .....	211
Analyzing Performance Metrics .....	214
Simple Network Management Protocol .....	216
Remote Administration Tools .....	219
<b>Module 3 / Unit 6</b>	
<i>Cloud and Virtualization</i>	223
Virtualization Technologies .....	223

Storage Area Networks.....	227
Cloud Computing.....	231

<b>Module 3 / Summary</b>	
<i>Troubleshooting and Management</i>	235

<b>Module 4 / Installation</b>	<b>237</b>
--------------------------------	------------

<b>Module 4 / Unit 1</b>	
<i>Network Sites</i>	240

Wiring Distribution .....	240
Rack Systems .....	245
Safety and ESD .....	247
Power Management .....	249
HVAC (Heating, Ventilation, Air Conditioning) .....	252
Physical Security Controls .....	255
Fire Prevention and Suppression.....	259

<b>Module 4 / Unit 2</b>	
<i>Installing Cable</i>	263

Twisted Pair Cable (UTP / STP / ScTP).....	263
Twisted Pair Connectors.....	266
Wiring Tools and Techniques .....	268
Cable Testing and Troubleshooting .....	270
Other Copper Cable Types .....	274
Fiber Optic Cable and Connectors.....	276
Media Converters .....	279
Troubleshooting Fiber Cable Issues .....	280

<b>Module 4 / Unit 3</b>	
<i>Installing Wireless Networks</i>	284

Wireless Standards (IEEE 802.11) .....	284
Wireless Network Topologies .....	287
Wireless Site Design .....	289
Site Surveys and Antenna Placement.....	293
Troubleshooting Wireless Links .....	295

<b>Module 4 / Unit 4</b>	
<i>WAN Technologies</i>	301

WAN Basics .....	301
Telecommunications Networks .....	303
Modern Telecommunications Networks .....	306
Packet-switched WAN Services.....	308
Local Loop Services .....	311
Wireless WANs .....	316

<b>Module 4 / Unit 5</b>	
<i>Remote Access</i>	320

Remote Access Services (RAS) .....	320
Virtual Private Networks (VPN).....	323
PPTP and SSL VPNs .....	324

IP Security (IPsec).....	326
Remote Access Servers .....	328
Installing Remote Access Links .....	330
Troubleshooting WAN Issues .....	334
<b>Module 4 / Summary</b>	
<i>Installation</i>	339
<b>Module 5 / Security</b>	<b>341</b>
<b>Module 5 / Unit 1</b>	
<i>Vulnerabilities and Threats</i>	343
Security Basics .....	343
Social Engineering.....	345
Network Reconnaissance .....	346
Wireless Security.....	352
Network Attack Strategies .....	355
Denial of Service .....	361
<b>Module 5 / Unit 2</b>	
<i>Security Appliances</i>	365
Network Segmentation .....	365
Demilitarized Zones (DMZ).....	368
Network Address Translation.....	370
Firewalls .....	373
Configuring a Firewall.....	376
Proxies and Gateways.....	380
Anti-malware Software .....	383
Intrusion Detection Systems (IDS).....	385
<b>Module 5 / Unit 3</b>	
<i>Authentication</i>	390
Authentication Technologies.....	390
Cryptographic Hash Functions .....	392
NTLM and Kerberos .....	393
RADIUS and TACACS+ .....	395
PAP, CHAP, and EAP .....	396
Wi-Fi Authentication .....	399
Endpoint Security .....	401
Network Access Control .....	403
Mobile Device Management .....	405
Troubleshooting Authentication and ACLs.....	407
<b>Module 5 / Unit 4</b>	
<i>Incident Response</i>	411
Business Continuity Concepts .....	411
Disaster Recovery Planning .....	414
IT Contingency Planning .....	415
Training .....	417
Incident Response Procedures.....	419
Forensic Procedures .....	422
Collection of Evidence .....	423



**Module 5 / Unit 5**

*Change and Configuration Management* 427

---

Change and Configuration Management ..... 427

Documentation ..... 429

Procedures and Standards ..... 434

Employee Policies ..... 437

Patch Management ..... 439

Backup Plans and Policies ..... 442

**Module 5 / Summary**

*Security* 445

---

**Taking the Exams** 447

**Glossary** 459

**Index** 483

---

# About This Course

This course is intended for those wishing to qualify with CompTIA Network+ Certification. Network+ is foundation-level certification designed for IT professionals with 1 year's experience whose job role is focused on network administration.

*The CompTIA Network+ certification will certify that the successful candidate has the knowledge and skills required to troubleshoot, configure, and manage common network wireless and wired devices, establish basic network design and connectivity, understand and maintain network documentation, identify network limitations and weaknesses, and implement network security, standards, and protocols. The candidate will have a basic understanding of emerging technologies including unified communications, mobile, cloud, and virtualization technologies.*

*CompTIA Network+ Exam Objectives Blueprint*

## Target Audience and Course Prerequisites

CompTIA Network+ is aimed at IT professionals with job roles such as network administrator, network technician, network installer, help desk technician and IT cable installer. Ideally, you should have successfully completed the "CompTIA A+ Support Skills" course, achieved CompTIA A+ certification, and have around 9-12 months' experience of networking support or IT administration. It is not *necessary* that you pass the A+ exams before completing Network+ certification, but it is *recommended*

Regardless of whether you have passed A+, it is recommended that you have the following skills and knowledge before starting this course:

- Configure and support PC, laptop, mobile (smartphone/tablet), and print devices.
- Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers).
- Configure and manage users, groups, and shared resources in a simple SOHO network.
- Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls.

Optionally, you can take a prerequisites test to check that you have the knowledge required to study this course at the gtslearning Freestyle site ([gtsgo.to/4mywk](https://gtsgo.to/4mywk)) accompanying this study guide (see below for details on registering).

## Course Outcomes

This course will teach you the fundamental principles of installing, configuring, and troubleshooting network technologies and help you to progress a career in network administration. It will prepare you to take the CompTIA Network+ exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can act as groundwork for more advanced training. On course completion, you will be able to:

- Describe the features of different network protocols and products for LANs, WANs, and wireless networks.
- Understand the functions and features of TCP/IP addressing and protocols.
- Identify threats to network security and appropriate countermeasures and controls.
- Install and configure network cabling and appliances.
- Manage, monitor, and troubleshoot networks.

### How Certification Helps Your Career

Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.



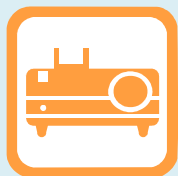
*Benefits of certification*

The CompTIA Network+ credential proves knowledge of networking features and functions and is the leading vendor-neutral certification for networking professionals. Worldwide nearly 500,000 individuals are CompTIA Network+ certified and 91% of hiring managers indicate CompTIA certifications are valuable in validating IT employee skills and expertise. Dell, HP, Sharp, Xerox and Ricoh are among the companies that employ Network+ certified staff and it is supported by top organizations, such as Apple, Best Buy, Canon, Cisco, Intel and U.S. Navy.



Your instructor edition is identical to the student edition, except that there are notes to help you deliver the course in the margins.

Note that answers to the review questions are also located in the "Notes" area of the "Review" slide for each unit.



This icon denotes a slide to accompany the text.

## About the Course Material

The CompTIA Network+ exam contains questions based on objectives and example content listed in the exam blueprint, published by CompTIA. The objectives are divided into five **domains**, as listed below:

CompTIA Network+ Certification Domain Areas	Weighting
1.0 Network Architecture	22%
2.0 Network Operations	20%
3.0 Network Security	18%
4.0 Troubleshooting	24%
5.0 Industry Standards, Practice, and Network Theory	16%

This course is divided into five **modules**, each covering a different subject area. Each module is organized into several **units**, containing related topics for study.

- Module 1 / Topologies and Infrastructure
- Module 2 / Addressing and Routing
- Module 3 / Troubleshooting and Management
- Module 4 / Installation
- Module 5 / Security

The modules in the course do not correspond directly to domains in the exam. Doing so would involve quite a lot of jumping around between different technologies. Instead, we try to cover topics in the most straightforward order for candidates at a foundation level to understand, starting with an overview of threats and attacks and proceeding to examine vulnerabilities and controls in different environments. Each module starts with a list of the CompTIA domain objectives and content examples that will be covered in each unit.

On the Freestyle course support website, you can find **Pre- and Post-assessment tests** for each unit. These are designed to identify how much you know about the topics covered in a unit before you study it and how much knowledge you have retained after completing a unit. You can use these tests in conjunction with your training provider to identify which units to focus on or to help you plan a self-study program.



*There are notes on registering for the course support site and planning a self-study program later in this section.*

Each unit in a module is focused on explaining the exam objectives and content examples. Each unit has a set of **review questions** designed to test your knowledge of the topics covered in the unit. Answers to the review questions are provided on the Freestyle course support website.






At the back of the book there is an **index** to help you look up key terms and concepts from the course and a **glossary** of terms and concepts used.

If you are studying with a training provider, you may also receive a "Labs" book containing the practical labs for you to complete in class.



*If you are viewing this course as an ebook, the "Labs" volume is located after the index - use the bookmarks panel to navigate between sections.*

The following symbols are used to indicate different features in the course book:

Icon	Meaning
	A tip or warning about a feature or topic.
	A reference to another unit, where more information on a topic can be found.
	A link to a Professor Messer video presentation. Click or use a QR scanner to open the link or enter <code>gtsgo.to/</code> followed by the code printed under the QR graphic into your browser.
	Review questions to help test what you have learned.
	A hands-on exercise for you to practice skills learned during the lesson.

## Integrated Learning with Professor Messer Video Tutorials



Professor Messer has long been a web hero for CompTIA certification students. With professionally-produced lessons covering the full exam objectives plus online forums, Professor Messer is a trusted online source for exam information. Professor Messer uses gtslearning's CompTIA certification courseware to develop and record his popular video training sessions. Now you can easily follow along with his video presentations using the links provided in this course book.

Each of the "TV static" icons above and in the rest of the book represents a Professor Messer video. The icons are called QR codes. They enable you to scan the link using a smartphone or tablet equipped with a camera. You can use the links in three ways:

- 1) If you have an ebook, just click the link to open the video in your browser.
- 2) If you have a QR code reader, open the app and point your camera at the icon to open the video in your phone or tablet's browser.



- 3) If you have a printed book but no reader, enter `gtsgo.to/` followed by the code printed under the QR graphic into your browser. For example, to access the code shown above, enter `gtsgo.to/dlbrs`) in your browser.



*We do endeavor to keep the video links up-to-date, but if you come across a broken link, please email the link code (for example "dlbrs") to [support@gtslearning.com](mailto:support@gtslearning.com) and we will update it.*



*If you have trouble scanning an icon, make sure the page is laid flat and try moving the camera closer to or farther from the image. Some topics feature more than one video link; you may have to cover the other link with your hand or a post-it to scan the one next to it.*



*As Professor Messer covers the objectives in domain order, some links are to segments of a longer video so do not be surprised if some video links do not play from the start.*



*The Professor Messer video series for the N10-006 exam is in production at the time of writing. The links in the course book will be updated from N10-005 versions to N10-006 versions as they become available. Also check for new videos at [gtsgo.to/zij4k](https://gtsgo.to/zij4k).*

## Getting Started and Making a Study Plan

If you are completing this course as self-study, you need to plan your study habits. The best way to approach the course initially is to *read through* the whole thing quite quickly. On this first reading, do not worry if you cannot recall facts, get two similar technologies mixed up, or do not completely understand some of the topics. The idea is to get an overview of everything you are going to need to know. The first reading shouldn't take you too long - a few hours is plenty of time. You don't have to do it at one sitting, but try to complete the read through within about a week.

When you have completed your first read through, you should make a **study plan**. We've put a sample study plan on the course website, but you'll need to adjust it to account for:

- How much you know about network technologies *already*.
- How much *time* you have to study each day or each week.
- *When* you want to (or have to) become Network+ Certified.

In your study plan, you'll identify how much time you want to spend on each unit and when you're going to sit down and do that study. We recommend that you study no more than one or two units per day. Studying a unit means reading it closely, making notes about things that come to mind as you read, using the glossary to look up terms you do not understand, then using the review questions on the course website to test and reinforce what you have learned.

Only you can decide how long you need to study for in total. Network+ Certification is supposed to represent the knowledge and skills of someone with 9-12 months of practical network administrative experience. If you cannot get that experience, you will need to do a corresponding amount of study to make up. We have included practice tests for the course; these should give you a good idea of whether you are ready to attempt the exams.

You also need to think about *where* you are going to study. You need to find somewhere comfortable and where you are not subject to interruptions or distractions. You will also need a computer or tablet with an internet connection for the review and practical activities.

## Freestyle Support Site

Purchasing this book gives you free access to the course support website. The website contains **practice tests** to help you in your final preparations to take the CompTIA exam. You can find the **answers** to the end-of-unit review questions on the support site. There is also a **glossary** of terms that you can use while reading the book or as a revision aid.

To register for the website, visit the Freestyle site ([gtsgo.to/oup4x](http://gtsgo.to/oup4x)) and complete the sign-up process.

Creating an account on Freestyle

You will need to validate the account using your email address. When you have validated your account, open [gtsgo.to/u7tlw](http://gtsgo.to/u7tlw) and log in if necessary.

*Students can self-register on the site using these instructions. When they enroll they will be placed in a pool with other retail customers.*

*If you want to track your students' performance in the practice exams, email [support@gtlearning.com](mailto:support@gtlearning.com) to obtain an alternative enrollment code and a teacher account with reporting rights.*

*Note that you will only be able to manage your students if they enroll using your personalized enrollment code.*



## Preparing for the Exams

When you've completed reading the units in detail, you can start to prepare for the exam. The "Taking the Exams" chapter and the support website contain tips on booking the test, the format of the exam, and what to expect.

Get tests and practice exams to accompany the course at [gtslearning's Freestyle site](https://gtslearning.com)



When it comes to booking your test, you might be able to save money by using a voucher code from [gtslearning](https://gtslearning.com). Check [gtslearning's website](https://gtslearning.com) ([gtslearning.com](https://gtslearning.com)) for any available offers.

## Content Seal of Quality

This course has been approved under CompTIA's **Authorized Quality Curriculum Program (CAQC)**. The following text is provided by CompTIA in acknowledgment of this. This courseware bears the seal of **CompTIA Official Approved Quality Content**. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

The contents of this training material were created for the CompTIA **Network+ Certification N10-006** exam covering the **2015 Edition** exam objectives and content examples. CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such "Authorized" or other training material in order to prepare for any CompTIA certification exam.

**OFFICIAL**MULTI-LAYERED LEARNING  
TOOLS INCLUDED

CAQC logo



*It is CompTIA's policy to update the exam regularly with new test items to deter fraud and for compliance with ISO standards. The exam objectives may therefore describe the current "Edition" of the exam with a date different to that above. Please note that this training material remains valid for the stated exam code, regardless of the exam edition. For more information, please check the FAQs on CompTIA's website ([support.comptia.org](http://support.comptia.org)).*

## Four Steps to Getting Certified

This training material can help you prepare for and pass a related CompTIA certification exam or exams. In order to achieve CompTIA certification, you must register for and pass a CompTIA certification exam or exams. In order to become CompTIA certified, you must:

- 1) Review the certification objectives at [gtsgo.to/yd4ou](https://gtsgo.to/yd4ou) to make sure you know what is covered in the exam.
- 2) After you have studied for the certification, take a free assessment and sample test from CompTIA at [gtsgo.to/mmbfu](https://gtsgo.to/mmbfu) to get an idea what type of questions might be on the exam. You can also use gtslearning's free practice tests on Freestyle ([gtsgo.to/u7tlw](https://gtsgo.to/u7tlw)).
- 3) Purchase an exam voucher on the CompTIA Marketplace, which is located at [www.comptiastore.com](https://www.comptiastore.com). When it comes to booking your test, you might be able to save money by using a voucher code from gtslearning. Check gtslearning's website ([gtsgo.to/lbjob](https://gtsgo.to/lbjob)) for any available offers.
- 4) Select a certification exam provider and schedule a time to take your exam. You can find exam providers at [gtsgo.to/4tij2](https://gtsgo.to/4tij2).

Visit CompTIA online - [www.comptia.org](https://www.comptia.org) - to learn more about getting CompTIA certified. Contact CompTIA - call 866-835-8020 ext. 5 or email [questions@comptia.org](mailto:questions@comptia.org).

# Module 1 / Topologies and Infrastructure

The following CompTIA Network+ domain objectives and examples are covered in this module:

CompTIA Network+ Certification Domain Areas	Weighting
1.0 Network Architecture	22%
2.0 Network Operations	20%
3.0 Network Security	18%
4.0 Troubleshooting	24%
5.0 Industry Standards, Practices, and Network Theory	16%

Refer To	Domain Objectives/Examples
Unit 1.1 / Topologies and the OSI Model	<b>1.6 Differentiate between common network topologies</b> <i>Mesh (Partial, Full) • Bus • Ring • Star • Hybrid • Point-to-point • Point-to-multipoint • Client-server • Peer-to-peer</i> <b>1.7 Differentiate between network infrastructure implementations</b> <i>WAN • MAN • LAN • WLAN (Hotspot) • PAN (Bluetooth, IR, NFC)</i> <b>5.1 Analyze a scenario and determine the corresponding OSI layer</b> <i>Layer 1 – Physical • Layer 2 – Data link • Layer 3 – Network • Layer 4 – Transport • Layer 5 – Session • Layer 6 – Presentation • Layer 7 – Application</i> <b>5.2 Explain the basics of network theory and concepts</b> <i>Encapsulation / de-encapsulation</i>
Unit 1.2 / Ethernet	<b>1.8 Given a scenario, implement and configure the appropriate addressing schema</b> <i>MAC addressing • Broadcast domains vs collision domains</i> <b>4.2 Given a scenario, analyze and interpret the output of troubleshooting tools</b> <i>Command line tools (arp, mac address lookup table) • Protocol analyzer</i> <b>5.2 Explain the basics of network theory and concepts</b> <i>Modulation techniques (Multiplexing, De-multiplexing, Analog and digital techniques, TDM) • Broadband / baseband • Bit rates vs baud rate • Sampling size • CDMA/CD and CSMA/CA • Carrier detect/sense • Wavelength • Collision</i> <b>5.4 Given a scenario, deploy the appropriate wired connectivity standard</b> <i>Ethernet standards (10BASE-T, 100BASE-T, 1000BASE-T, 1000BASE-TX, 10GBASE-T, 100BASE-FX, 10BASE-2, 10GBASE-SR, 10GBASE-ER)</i>

## Delivery Tips

Use the Freestyle course website to download resources to help to setup and run this course. Refer to the sign-up instructions in the prelims section.

The first three modules follow the OSI model while modules 4 and 5 focus on installation then security.

Consequently, each module in the course covers objectives from a range of domains.

As mentioned in the prerequisites, it is assumed that the students have A+ or equivalent knowledge and therefore will be aware of basic parameters for TCP/IP, understand the concept of clients and servers, and so on.

The labs also assume a working knowledge of the main configuration tools for Windows.

Refer To	Domain Objectives/Examples
Unit 1.3 / Hubs, Bridges, and Switches	<p><b>1.1 Explain the functions and applications of various network devices</b>  <i>Switch • Hub</i></p> <p><b>2.6 Given a scenario, configure a switch using proper features</b>  <i>VLAN (Native VLAN / Default VLAN, VTP) • Spanning tree [802.1D] / Rapid spanning tree [802.1w] (Flooding, Forwarding / blocking, Filtering) • Interface configuration (Trunking / 802.1Q, Tag vs untag VLANs, Port bonding [LACP], Port mirroring [local vs remote], Speed and duplexing, IP address assignment, VLAN assignment) • Default gateway • PoE and PoE+ (802.3af, 802.3at) • Switch management (User / passwords, AAA configuration, Console, Virtual terminals, In-band / Out-of-band management) • Managed vs unmanaged</i></p>
Unit 1.4 / Infrastructure and Segmentation	<p><b>1.7 Differentiate between network infrastructure implementations</b>  <i>SCADA / ICS (ICS server, DCS / closed network, Remote terminal unit, Programmable logic controller)</i></p> <p><b>1.12 Given a set of requirements, implement a basic network</b>  <i>List of requirements • Device types / requirements • Environment limitations • Equipment limitations • Compatibility requirements • Wired / wireless considerations • Security considerations</i></p> <p><b>5.4 Given a scenario, deploy the appropriate wired connectivity standard</b>  <i>Ethernet standards (IEEE 1905.1-2013 [Ethernet over HDMI, Ethernet over Powerline])</i></p>

# Module 1 / Unit 2

## Ethernet

### Objectives

On completion of this unit, you will be able to:

- Understand the properties of transmission media, data signaling, and media access control.
- Describe the features of IEEE 802.3 (Ethernet).
- Describe the properties of MAC addressing and ARP.
- Understand the use of packet sniffers / protocol analyzers to capture and examine network traffic.

### Media Types and Modulation

A transmission medium is the physical path (or **circuit**) through which **signals** travel to allow nodes to communicate with one another. The transmission media used for a network can be classified as cabled or wireless:

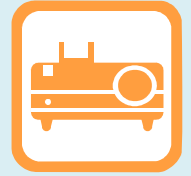
- **Cable** - a physical signal conductor is provided between two networked devices. Examples include cable types such as **twisted pair** or **fiber optic**. Cabled media can also be described as **bounded** media.
- **Wireless** - uses free space between networked devices (no signal conductor), such as **microwave** or **radio links**. Wireless media can also be described as **unbounded**.

Both categories of media may be used in local or wide area networks

### Modulation

All network signaling uses electromagnetic radiation. This refers to the wave-like movement of electrons as they move through media. An electromagnetic wave has the following properties:

- Wavelength - the distance between two peaks or troughs in the wave.
- Frequency - the oscillations per second of the wave, measured in Hertz. An oscillation or cycle is one complete transition (from crest-to-crest or trough-to-trough for instance). Frequency is inversely proportional to wavelength; so high frequency waves have shorter wavelengths compared to low frequency waves.



#### Delivery Tips

*Students need to be comfortable describing the features and performance of the various Ethernet standards.*

#### Timings

*Theory & Review Questions - 60 minutes*

*Labs - 60 minutes*



*These network theory basics are now topics on the exam so ensure that students understand how signaling works (in brief)...*

- Amplitude - the height or power of the wave. As a wave travels, its energy dissipates and the amplitude of the wave attenuates. As the amplitude diminishes, it becomes more susceptible to noise and reception problems (interference).
- Phase - the angle of the wave at a particular moment.

Signaling uses properties of electromagnetic waves to carry digital information by a process called **modulation**. Modulation means a property of the wave is varied by the sender and then measured (**de-modulated**) by the receiver. For example, high and low amplitude could be used to represent the 1s and 0s of digital data. Phase and frequency can similarly be used to encode digital data in the wave as a signal. A modulated wave carrying information is also referred to as a **carrier wave**.

## Bandwidth

**Bandwidth** is the range of frequencies available in a modulated carrier wave. The range of electromagnetic radiation frequencies is referred to as the electromagnetic spectrum. This ranges from waves propagating once per second (1 Hz) to those propagating thousands (KHz), millions (MHz), billions (GHz), or trillions of times per second (THz). At a given power level, high frequency waves have greater bandwidth but less range.

## Copper Cable

Copper cable is used to carry electromagnetic radiation in the MHz frequency ranges over electrical conductors. As the waves are low frequency, they require relatively little power to propagate. The drawback is that relatively little bandwidth is available in this part of the spectrum.

## Fiber Optic Cable

Fiber optic cable carries very high frequency radiation (THz) in the visible light part of the spectrum. Much higher bandwidths are available but more power is required to transmit signals over long distances.

## Wireless Radio

Radio Frequencies (RF) can propagate through the air between sending and receiving antennas. The use of the radio spectrum is regulated by national governments and (to some extent) standardized internationally by the **International Telecommunications Union (ITU)**. Use of many frequency bands requires a license from the relevant government agency.

Wireless radio networking products operate in unregulated bands (2.4 and 5 GHz) but there is a limit on power output, which means range is limited. They are often referred to as the Industrial, Scientific, and Medical (ISM) bands.



## Distance

Each type of media can consistently support a given data rate only over a defined distance. Some media support higher data rates over longer distances than others. **Attenuation** and **noise** affect the maximum supported distance of a particular media type.

- **Attenuation** is the progressive loss of signal strength, measured in decibels (dB). It has different causes depending on the type of media but generally speaking attenuation is increased by using faster signaling and by poor quality media.
- **Noise** is anything that gets transmitted within or close to the media that isn't the intended signal. This serves to make the signal itself difficult to distinguish. This causes errors in data, forcing it to be retransmitted.

*This is best explained by the "party" metaphor.*

*If you want to tell someone something and they are across the room from you, you have to speak more loudly to make them hear you than you would if they were nearby (attenuation).*

*If there are other people in the room and they are talking too, you have to speak even louder to make yourself heard (noise).*

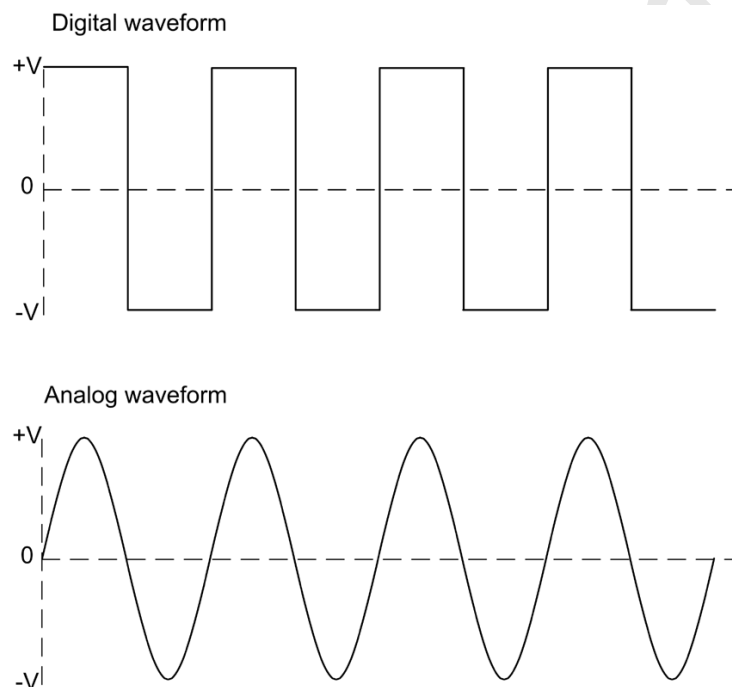
*You will find that you frequently have to repeat what you say to make yourself understood (data loss).*

## Signaling

**Analog** and **digital** are two formats for both circuits and signals. For example, it is possible that a digital signal could be carried over an analog circuit or a digital circuit could carry an analog signal. That said, modern networks now predominantly use digital circuits and signaling.

## Analog Modulation

**Analog modulation** is characterized by a continually changing wave. When used to convey digital signals, the wave is sampled to identify the signal but this sampling process is easily subject to interference. It is also difficult to boost an analog signal, as amplifying it will also amplify any interference affecting it.



View of digital and analog signals



## Digital Modulation

**Digital modulation** uses a series of discrete pulses. This makes the transmission less susceptible to interference and it makes it easier to regenerate the transmission over longer distances.

When an analog input (such as voice) needs to be converted to digital (1s and 0s), the input is **sampled** to derive a discrete value. When sampling like this, you have to balance quality with available bandwidth. For example, telecommunications links are based on 64 Kbps channels because that is the bandwidth requirement for carrying digitized voice calls. This is worked out as a result of the following calculation, derived from the Nyquist theorem that the sampling rate must be twice the signal bandwidth.

- 1) The voice frequency range is (or assumed to be) 4000 Hz.
- 2) This must be sampled at twice the rate (8000 Hz) to ensure an accurate representation of the original analog waveform.
- 3) The sample size is 1 byte (or 8 bits).
- 4) Therefore,  $8000 \text{ Hz} \times 8 \text{ bits} = 64 \text{ Kbps}$ .

## Baseband, Broadband, and Multiplexing

There are two ways of allocating the bandwidth of a carrier wave:

- **Baseband transmission** uses the complete bandwidth of the carrier wave as a single transmission path; that is a single circuit is used for a single channel.
- **Broadband transmission** can divide the available bandwidth of the carrier wave in a single circuit into a number of transmission paths (or channels).

The technique by which division of a carrier wave into multiple discrete channels is accomplished is called **multiplexing**. Conversely, **de-multiplexing** is the means by which each channel is extracted and processed from the carrier wave. The devices that put data into separate channels for transmission over a circuit are called **multiplexers (muxes)**. **De-multiplexers** perform the reverse process.

In multiplexing, the channels can be identified by a variety of methods. Two common ones are time division and frequency division.

- **Time Division Multiplexing (TDM)** - this means allocating each channel a window or slot during which it can add data to the circuit. TDM is typical of digital circuits. TDM can be used to multiplex baseband transmissions.
- **Frequency Division Multiplexing (FDM)** - this means dividing up the available frequency into channels and is typical of analog circuits and broadband transmission. If the overall frequency range of the circuit is 100 MHz, you could create 5 channels each with 20 MHz bandwidth.



There are many other types of multiplexing, some of which will be discussed elsewhere in this course.

## Baud Rate and Bit Rate

In a modulated carrier wave, each property of the wave can be referred to as a **symbol**. For example, in an amplitude modulated wave, each transition between a peak and a trough could be a single symbol. The number of transitions (or symbols) per second is called the **baud rate**. The baud rate is measured in **Hertz** (or MHz or GHz).

The bit rate is the amount of information that can be transmitted over the wave, measured in **bits per second (bps)**, or some multiple thereof.



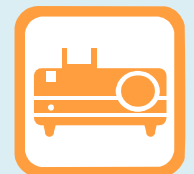
*The term "bandwidth" is also often used in networking to mean the bit rate.*

In order to transmit information more efficiently, a modulation scheme might be capable of representing more than one bit per symbol. In this case, the bit rate will be *higher* than the baud rate. For example, a 600 MHz carrier wave might be capable of a bit rate of 1 Gbps. Some examples of modulation and encoding schemes include Manchester Encoding, Pulse Amplitude Modulation (PAM), Quadrature Amplitude Modulation (QAM), and Orthogonal Frequency Division Multiplexing (OFDM).

## Media Access Control



mbqop



A network has to be able to share the available communications capacity between the various devices that use it. This means that networks need ways of determining when devices are allowed to communicate and to deal with possible problems, such as two devices attempting to communicate simultaneously. **Media Access Control (MAC)** is the methodology used to determine when devices are allowed to communicate using the network.

*While CSMA/CD is a bit redundant, students should still understand how it works and questions on it will probably feature in the exam.*

## 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. When two devices transmit at the same time, the signals are said to collide and neither signal can reach its destination. This means that they must be re-sent, reducing available bandwidth. The collisions become more frequent (geometrically) as more devices are added to the network and consequently the effective data rate (or throughput) reduces too.

To reduce collisions, protocols ensure devices listen to the media before transmitting and only transmit if the media is clear. A device wanting to transmit, but detecting activity, must wait and try later.

*Make sure they grasp the overall principle of media access and contention.*

*You might want to mention other media access methods, such as token passing. Also note that multiplexing is another media access method.*



*Although much less frequent, collisions still occur as multiple devices can simultaneously detect a clear media and transmit a signal.*

These contention protocols are called **Carrier Sense Multiple Access (CSMA)** protocols:

- **Carrier sense** - detect activity on the media.
- **Multiple access** - multiple devices using the same media.

Use of these protocols enforces limitations on the minimum and maximum lengths of cable that can be used and the size of packets transmitted. Each packet must fill the cable segment before the end of transmission is reached or a packet could be sent and involved in a collision and lost without the sending node being aware of it. There are two types of CSMA protocols: **CSMA/CD** - with collision **detection** - and **CSMA/CA** - with collision **avoidance**.



## CSMA/CD (with Collision Detection)

Ethernet's CSMA/CD protocol defines methods for detecting a collision on different types of media. In most cases this is when a signal is present on the adapter's transmit and receive lines simultaneously. On detecting a collision, the adapter broadcasts a jam signal. Each node that was attempting to use the media then waits for a "random" period (**backoff**) before attempting to transmit again.

## CSMA/CA (with Collision Avoidance)

The CSMA/CA protocols use schemes such as time-sliced accessing or requests to send data to gain access to the media. This reduces the number of collisions but adds overhead in terms of extra control signaling. The IEEE 802.11 Wi-Fi standard uses CSMA/CA.



See [Unit 4.3](#) for more information about CSMA/CA and wireless technologies.

## 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. A switch establishes a "temporary circuit" between two nodes that are exchanging messages. Using a switch means that each switch port is in a separate collision domain. This means that collisions can only occur if the device attached to the port is operating in half duplex mode and that the collisions affect only that port.

## Half Duplex and Full Duplex

Older hub-based networks operate **half duplex** transmissions. This means that a device (node) can transmit *or* receive, but cannot do both at the same time. Newer network devices, such as switches, allow for **full duplex** transmissions, where a device can transmit and receive simultaneously.

*Note that a full duplex link is a point-to-point link and so collisions cannot occur.*

## Broadcast Domains

Within a collision domain on a shared medium, any given node will see all the traffic transmitted within that domain. It will only normally choose to process traffic that is specifically addressed to it though. This is referred to as **unicast** traffic; traffic that is addressed by the sender to a single recipient.

*Make sure that students can distinguish broadcast domains and collision domains.*

It is useful to have a mechanism to transmit the same traffic to multiple nodes. This is referred to as **broadcast** traffic. This is accomplished using a special type of destination address. Nodes that share the same broadcast address are said to be within the same **broadcast domain**.

*Collision domains are about physically shared media and collision domain borders are established by bridges and switches (the latter puts each port in its own collision domain making the concept redundant!).*

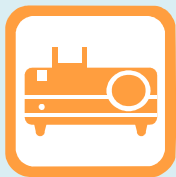
Broadcast traffic introduces efficiencies in some circumstances but inefficiencies in others. If the broadcast domain is very large, the amount of broadcast traffic will be correspondingly great and consume a disproportionate amount of bandwidth. This becomes an important factor in designing a network that works efficiently.

*Broadcast domains are established by layer 3 "logical" network devices and protocols (routers) but do note that this requires the concept of a layer 2 broadcast address.*

A collision domain is established by a devices operating at layer 1 or layer 2 of the OSI model, such as a hub, bridge, or switch. All devices attached to a hub will be part of the same collision domain; devices on either side of a bridge are in separate collision domains. Using switches effectively eliminates the concept of a collision domain entirely. Broadcast domains are normally established by routers, operating at layer 3 of the OSI model. A broadcast domain could contain multiple collision domains but the reverse is not true. A single collision domain can only be associated with one broadcast domain.



See [Unit 2.2](#) and [Unit 2.5](#) for more information on IP and routing and [Unit 1.3](#) for topics on bridges and switches.



Make sure students are familiar with framing and know the capabilities, media, and installation practices of the various standards.

Get students comfortable with the idea that addressing takes place at multiple levels of the OSI model, with Data Link (MAC) and Network (IP) being the most important.

Students must understand the concepts of an MTU and of fragmentation and reassembly.

# Ethernet Frames

Many technologies have been developed to enable LANs using different media and media access methods and subsequently fallen by the wayside. Ethernet is the "last man standing". Ethernet supports a variety of media options and is based upon inexpensive equipment. It was created in the 1960s at the University of Hawaii for its ALOHA network and was first used commercially by **DEC, Intel, and Xerox (DIX)** in the late 1970s. It was standardized by IEEE as 802.3 ([gtsgo.to/cto60](http://gtsgo.to/cto60)) in 1983.

Ethernet has a logical bus topology but is usually wired in a physical star topology, baseband signaling, and the CSMA/CD method for media access control.

The basic format of an Ethernet frame is as follows:

Pre- amble	Destination MAC	Source MAC	Length / Type	Payload	CRC
---------------	-----------------	------------	------------------	---------	-----

Construction of an Ethernet frame

## Preamble

The preamble is used for clock synchronization. It consists of 8 bytes of alternating 1s and 0s with two consecutive 1s at the end. This is not technically considered to be part of the frame.

## Addressing

The destination and source address fields contain the MAC addresses of the receiving and sending nodes. Ethernet network adapters have a unique hardware or physical address known as the **Media Access Control (MAC)** address. A MAC address consists of 48 binary digits (6 bytes).

## Frame Length and Payload

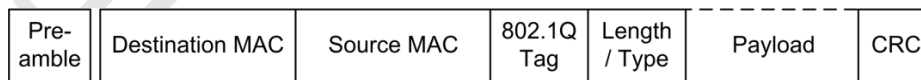
The official 802.3 standard defines a 2-byte *length* field to specify the size of the data field (also called the **payload**). This payload can normally be between 46 and 1500 bytes. The upper limit of the payload is also referred to as the **Maximum Transmission Unit (MTU)**.

However, most Ethernet products follow the original DIX specification (referred to as **Type II** frames) and use the field to indicate the *type* of network layer protocol contained in the frame (IP or IPX for instance). These Ethertypes are values of 1536 or greater (anything less than that is interpreted as the data length). For example, IPv4 is coded as the hex value 0800 (or 2048 in decimal) while IPv6 is 86DD.

**802.3 Ethernet** frames use a **Logical Link Control (LLC)** header to identify the protocol type. It can be further extended with a **Subnetwork Access Protocol (SNAP)** field to specify proprietary protocols. These headers take up part of the space normally reserved for data (reducing it to up to 1492 bytes). Consequently these frame types are not widely used.

To comply with CSMA/CD, the *minimum* length of an Ethernet frame is 64 bytes so the payload must be at least 46 bytes. If this is not the case it is automatically padded with redundant data.

The *maximum* size of any type of Ethernet frame is normally 1518 bytes (excluding the preamble). However, the 802.3ac standard specifies use of a 4-byte tag inserted between the source address and length fields designed to identify the VLAN to which the frame belongs, making the maximum allowable frame size 1522 bytes.



*Construction of an 802.1ac (VLAN) Ethernet frame*



*VLANs are a means of dividing a single physical network into multiple logically distinct networks. See [Unit 1.3](#) for details.*

Some Gigabit Ethernet products support **jumbo frames** with much larger MTUs. Such products are not standardized however making interoperability between different vendors problematic.



*Jumbo frames are discussed in some more detail in the topic on Storage Area Networks. See [Unit 3.6](#) for details.*

## Error Checking

The error checking field contains a 4-byte (32-bit) checksum called a **Cyclic Redundancy Check (CRC)** or **Frame Check Sequence (FCS)**. The CRC is calculated based on the contents of the frame; the receiving node performs the same calculation and, if it matches, accepts the frame. There is no mechanism for retransmission if damage is detected nor is the CRC completely accurate at detecting damage; these are functions of error checking in protocols operating at higher layers.



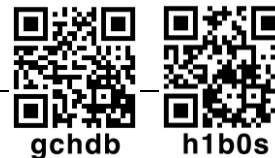


*The exam tends not to focus too heavily on specific distance limitations but students will probably want to learn them just in case.*

*Make sure students know which standard is applicable to a particular scenario - 10BASE-2 on a legacy network, 10G in a data center, and so on.*

*10BASE-2 has been restored to the objectives in the 2015 edition.*

# Legacy Ethernet Standards



Ethernet media specifications are named using a three-part convention. This describes:

- The bit rate (Mbps).
- The signal mode (baseband or broadband).
- A designator for the media type.

For example, 10BASE-T denotes an implementation that works at 10 Mbps, uses a baseband signal, and uses twisted-pair cabling.



*All types of Ethernet actually use baseband transmissions, so you will only see specifications of the form xBASE-y.*



*The cable types and specifications mentioned for each standard are covered in more detail in [Unit 4.2](#).*

## 10BASE-2

10BASE-2 (or Thinnet) is one of the earliest Ethernet standards. Unlike subsequent standards, it uses a physical bus topology. 10BASE-2 uses coaxial cabling and BNC connectors. In a single segment, each node is attached to the same run of cable using a T-connector. The cable must be terminated by resistors at each end and one end must be grounded.

10BASE-2 Specification	
Maximum segment cable length	185m (607 feet)
Minimum cable length	0.5m (1.5 feet)
Maximum nodes per segment	30
Maximum segments	5
Maximum repeaters	4
Maximum mixing segments (with nodes)	3

Thinnet was often used with 10BASE-5 (Thicknet). Thicknet uses a different grade of coax and supports longer segment lengths (up to 500m) and more nodes per segment. Consequently, in a typical installation, up to 3 Thinnet segments (with computers attached as nodes) could be linked (via devices called repeaters) using up to 2 Thicknet segments. These limitations were described as the 5-4-3 rule. The overall cable length for all segments cannot exceed 925m.

10BASE-2 would not be deployed on new networks but you may be called upon to maintain it in legacy installations.

## 10BASE-T

10BASE-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 (Tx), one pair to receive (Rx), while the other two pairs reduce crosstalk and interference. 10BASE-T networks are physically wired as a star. The link between the port on the host and the port on the hub or switch is a single segment. The logical topology is a bus:

- When a hub is used the transmission media are shared between all nodes as all communications are repeated to each port on the hub (point-to-multipoint).
- When a switch is used, a temporary virtual circuit is created between each host utilizing the full bandwidth available (point-to-point).

With compatible network adapters and switches, 10BASE-T also supports full duplex operation. Hub-based Ethernet supports half-duplex only.

The Ethernet specification imposes certain restrictions regarding the network design:

10BASE-T Specification	
Maximum segment cable length	100m (328 feet)
Minimum cable length	0.5m (1.5 feet)
Maximum segments	1024
Maximum hubs between nodes	4

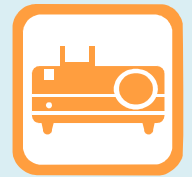
10BASE-T would not be deployed on new networks but you may be called upon to maintain it in legacy installations.

## Fast Ethernet

When it came to update the original Ethernet standard, the IEEE 802.3 committee decided on an approach that ensured backward compatibility. Its discussions resulted in the **IEEE 802.3u** specification, which is known as **Fast Ethernet**. Fast Ethernet is based on the same CSMA/CD protocols that define traditional Ethernet but reduces the duration of time each bit is transmitted by a factor of ten by using higher frequency signaling and improved encoding methods. This raises the bit rate from 10 Mbps to 100 Mbps. Data can move between Ethernet and Fast Ethernet devices without requiring protocol translation, as Fast Ethernet maintains the old error control functions, frame format, and length. Fast Ethernet can use twisted pair or fiber optic cable.

Specification	Cable	Maximum Distance
100BASE-TX	Cat 5 UTP (using 2 pairs) or STP	100m (328 feet)
100BASE-FX	MMF (62.5/125) / 1300nm	400m (1312 feet) / half-duplex 2000m (6562 feet) / full duplex

*In fact, 10BASE-T is pretty much obsolete but it is still present in the objectives.*



*Most of the LANs the students will encounter will be Fast Ethernet or Gigabit Ethernet (or possibly 10G if they stay in the profession long enough).*

*Most LANs will be a mix of UTP-based horizontal links and fiber optic backbones.*

*Stress that no one is going to be building a network based on hubs anymore but that they do remain a popular topic for exam questions.*





There are a couple of defunct standards defining use over Cat 3 cable (100BASE-T4 and 100BASE-T2). The set of copper standards can collectively be referred to as 100BASE-T.

Fast Ethernet allows only one or two hubs, though this does not apply if the hubs are stacked using a proprietary backplane (the stack counts as one device). The standards documentation also defines two classes of hubs; Class I hubs are used to connect different media (twisted-pair and fiber optic for instance) and only one device per network is allowed if this type of hub is used. In most modern networks however the restriction is overcome by using switches in place of hubs.

Fast Ethernet also introduced an **autonegotiation** protocol to allow devices to choose the highest supported connection parameters (10 or 100 Mbps and half- or full-duplex). 10BASE-T Ethernet specifies that a node should transmit regular electrical pulses when it is not transmitting data to confirm the viability of the link (**Link Integrity Test**). Fast Ethernet codes a 16-bit data packet into this signal advertising its service capabilities (speed and half- or full-duplex). This is called a **Fast Link Pulse**. Fast Link Pulse is backwards-compatible with 10BASE-T but not mandatory, as it is under Gigabit Ethernet and later. A node that does not support autonegotiation can be detected by one that does and sent ordinary link integrity test signals (or **Normal Link Pulses**).

Fast Ethernet would not be deployed on new networks but you may be called upon to maintain it in legacy installations.



## Modern Ethernet Standards

While the standards listed previously are obsolete, the subsequent versions of Ethernet remain very much in use.

### Gigabit Ethernet

**Gigabit Ethernet** builds on the standards defined for Ethernet and Fast Ethernet. The bit rate is 10 times faster than with Fast Ethernet. The Gigabit Ethernet standard over fiber (LX and SX) is documented in IEEE 802.3z. The various fiber standards are collectively known as **1000BASE-X**. The IEEE also approved 1000BASE-T, a standard utilizing Cat 5e or Cat 6 copper wiring. This is defined in IEEE 802.3ab.

Specification	Cable	Maximum Distance
1000BASE-T	UTP (Cat 5e or Cat 6)	100m (328 feet)
1000BASE-SX	MMF (62.5/125) / 850nm	220m (721 feet)
	MMF (50/125) / 850nm	550m (1640 feet)
1000BASE-LX	SMF (9/125) / 1300nm	5km (3 miles)
	MMF (62.5/125 or 50/125) / 1300nm	550m (1800 feet)

Note that 1000BASE-X is not a standard itself but a reference to CX, SX, and LX collectively.



*For 1000BASE-T, Cat 5 is also acceptable (if properly installed) but Cat 5 cable is no longer available commercially. Unlike Ethernet and Fast Ethernet, Gigabit Ethernet uses all four pairs for transmission and so is much more sensitive to crosstalk. A standard was created using only two pairs (1000BASE-TX) but was not successful commercially.*

In terms of network design, Gigabit Ethernet is implemented using switches, so only the restrictions on cable length apply. Gigabit Ethernet would be the mainstream choice for most new network installations. The main decision would be whether to use copper or fiber cable. Fiber cable would give better upgrade potential in the future while copper cable would be cheaper to install.

## 10G(igabit) Ethernet

**10G Ethernet** multiplies the nominal speed of Gigabit Ethernet by a factor of 10. 10G is not deployed in many office networks however as the cost of equipment (10G network adapters and switches) is high. The major applications of 10G Ethernet are:

- Increasing bandwidth for server interconnections and network backbones, especially in data centers and for Storage Area Networks (SAN).
- Replacing existing switched public data networks based on proprietary technologies with simpler Ethernet switches (Metro Ethernet).

10G Ethernet is standardized under a number of publications with letter designations (starting with 802.3ae), which are periodically collated (the current one being IEEE 802.3-2008).

Specification	Cable	Maximum Distance
10GBASE-T	UTP (Cat 5e/6/6a) and STP	20-100m
10GBASE-SR	MMF / 850nm	26-400m
10GBASE-LR	SMF (9/125) / 1310nm	10km (6.2 miles)
10GBASE-ER	SMF (9/125) / 1550nm	40km (25 miles)

10G works only with switches in full duplex mode.

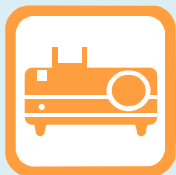


HP transceivers (network ports) for 10GBASE-SR / ER / LR (fiber optic) links

The 10GBASE-"R" standards all have WAN specifications (10GBASE-SW, 10GBASE-LW, and 10GBASE-EW) that allow interoperability with existing SONET infrastructure.



See [Unit 4.4](#) for more information on WAN technologies.



*This is addressing at the data link layer.*

*Make sure students are familiar with the format of MACs and the process of ARP.*

*Don't worry too much about exactly what layer in OSI ARP counts as - it's unlikely to be tested as an exam question in the same way something like a switch, IP, or TCP are.*

*You might want to explain the notation of MAC addresses and the term "least significant bit", though it shouldn't be necessary for the exam.*

*The I/G bit is the least significant bit of the most significant byte. In Ethernet transmission and related notation (canonical format), the bits are sent over the wire least significant bit first, as is shown in the screen capture.*

*The U/L bit is the second least significant bit of the most significant byte.*

# MAC Addressing



v6bqq

The component responsible for physically connecting the node to the transmission medium is called a **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.

Each Ethernet network interface has a unique hardware address known as the **Media Access Control (MAC)** address. This may also be referred to as the Ethernet Address (EA) or (in IEEE terminology) the Extended Unique Identifier (EUI). The IEEE deprecates use of the term "MAC address" as interfaces are increasingly likely not to be tied to a particular hardware adapter

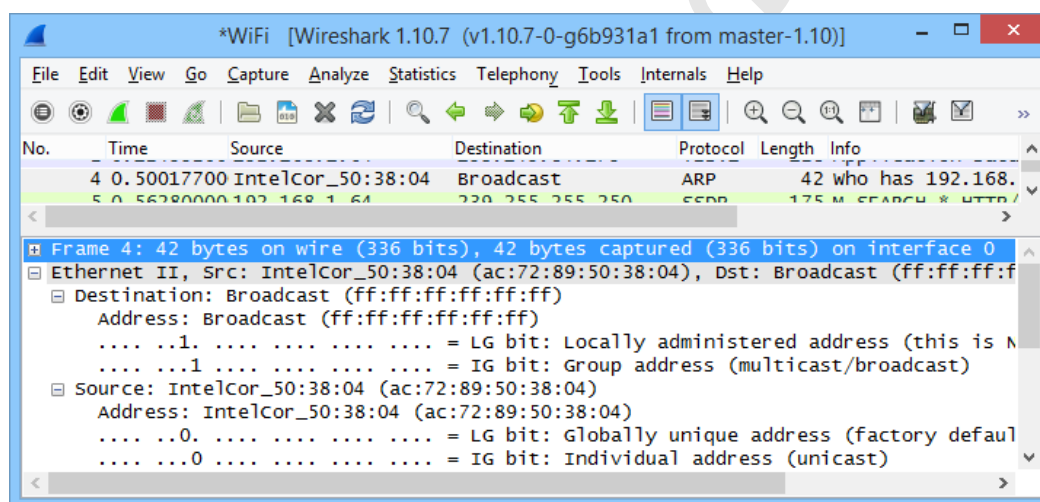
## MAC Address Format

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).



Hexadecimal uses digits 0-9 and letters A, B, C, D, E, and F to represent the 16 possible values of each hex digit See [Unit 2.4](#) for more information on the hex numbering system.

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". The first six hex digits (3 bytes or octets) represent the manufacturer (the **Organizationally Unique Identifier [OUI]**); the last six digits are a serial number.



*Captured Ethernet frame showing the resolved OUI and I/G and U/L bits in the destination (broadcast) and source addresses*

An organization can decide to use **locally administered** addresses in place of the manufacturers' universal coding systems. This can be used to make MACs meaningful in terms of location on the network but adds a significant administrative overhead. A locally administered address is defined by changing the U/L bit from 0 to 1. The rest of the address is configured using the card driver or network management software. It becomes the network administrator's responsibility to ensure that all devices are configured with a unique MAC.

The I/G bit of an Ethernet MAC address determines whether the frame is addressed to an individual node (0) or a group (1). The latter is used for multicast transmissions. A MAC address consisting entirely of 1s is the broadcast address and received by all nodes within the same broadcast domain.

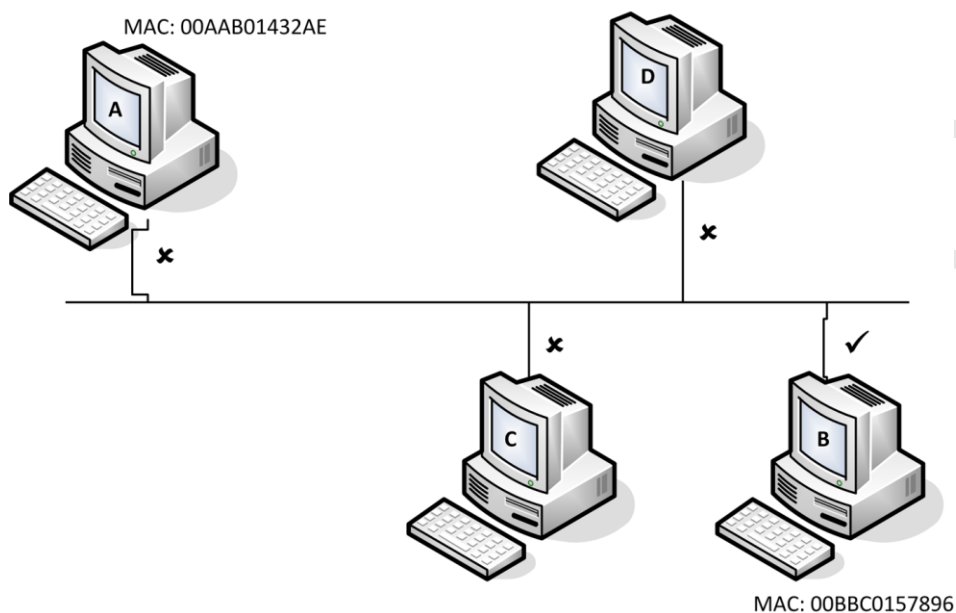


An EUI-64 is a 64-bit hardware address. A translation mechanism allows a 48-bit MAC address to be converted to an EUI-64. See the topic on IPv6 in [Unit 2.4](#) for more information.

## Unicast and Broadcast

When a sending interface addresses a single receiving interface, this is referred to as a **unicast** transmission. In the figure following, computer A sends a frame of data to computer B. Computer B recognizes 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.

	Destination Address	Source Address			
Start	00BBC0157896	00AAB01432AE	Type	Data	CRC

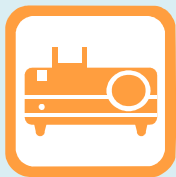


Checking the destination address of a frame

Under certain circumstances, it is necessary for a computer to **broadcast** data to all computers on the network. The computer broadcasting the data uses a broadcast "hardware" address of ff:ff:ff:ff:ff:ff.



It is important students be able to distinguish unicast and broadcast.



Make sure you cover this section in detail.

# Address Resolution Protocol (ARP)

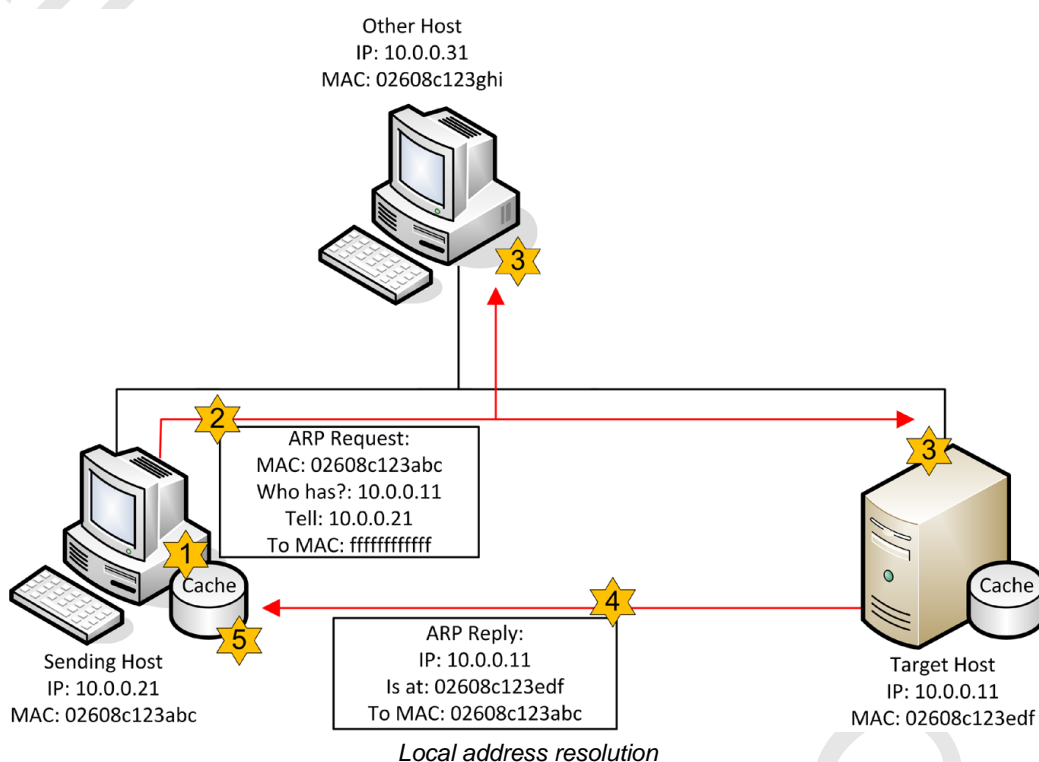


mbr2p

When two machines communicate using TCP/IP, an **IP address** is used at the network layer to identify each machine. However, transmission of data must take place at the physical and data link level using the hardware / MAC address of the interface. The TCP/IP suite includes the **Address Resolution Protocol (ARP)** to perform the task of resolving an IP address to a hardware address.

## Local Address Resolution

When both sending and receiving hosts are on the same local network (connected to the same switch for instance), local address resolution takes place as follows:



- 1) When the IP address has been determined to be a local address, the source host checks its ARP cache for the required hardware address (MAC address) of the destination host.
- 2) If not present in cache, ARP builds a request, which is then broadcast onto the network.
- 3) The broadcast is processed by all the hosts on the local network but unless the request contains its own IP address, most hosts ignore the request.
- 4) If the target host recognizes 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.

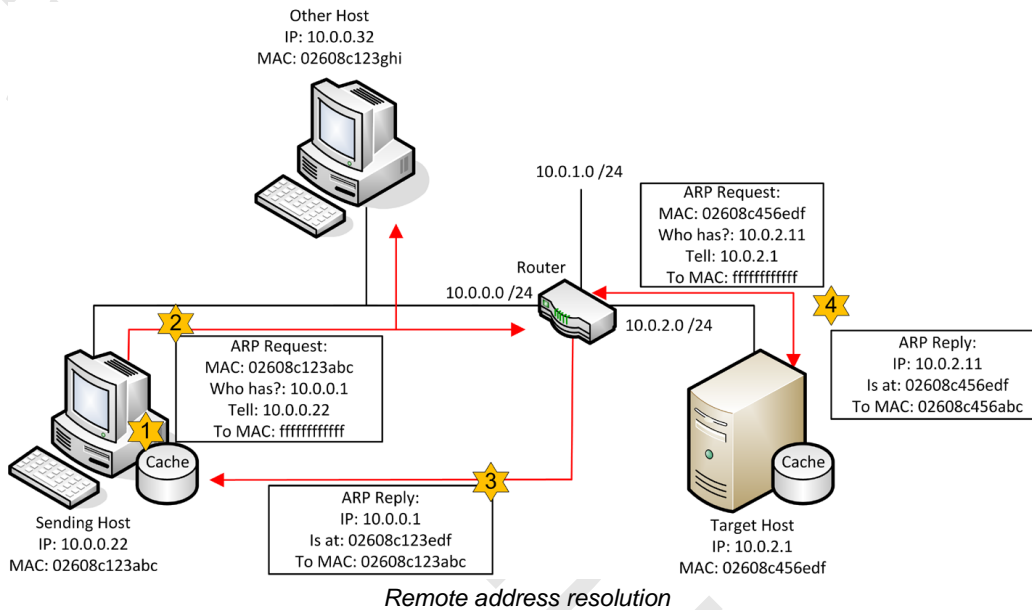




A subnet is the region of the network that receives broadcasts. This is explained in more detail in [Unit 2.1](#) and [Unit 2.2](#).

## Remote Address Resolution

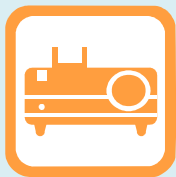
If the host is on a remote network, then the local host must use a router (or default gateway) to forward the packet. Therefore, it must determine the MAC address of the *gateway* using ARP.



- 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 (but NOT the IP address of the remote destination host).
- 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.
- 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.



*Stress the point that the sending host does not use ARP to determine the hardware addresses of hosts on remote networks. All communications are facilitated by the router (default gateway).*



Demonstrate each utility in turn. Explain the output from each and be sure that the students understand which program to use when.

ARP itself is also an exam content example. Ensure students can distinguish the protocol from the utility and the arp utility from the arp ping utility.

## ARP Cache

ARP broadcasts can generate considerable traffic on a network, which can reduce performance. To optimize this process, the results of an ARP broadcast are held in a cache initially. 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 timeout for the ARP cache varies by operating system and version and can often be configured manually.*

Entries in the ARP cache are automatically timed out in case a hardware address changes (for example, if a network card is replaced).

The cache is an area reserved in memory that contains the IP address and the associated hardware address. Before an ARP broadcast is performed, the cache is always checked for the correct MAC address. Broadcasting is reduced further as the host receiving an ARP request always extracts the IP address and hardware address of the source host and places this information in its ARP cache before transmitting an ARP reply.



### arp

The **arp** utility can be used to perform a number of functions related to the ARP cache.

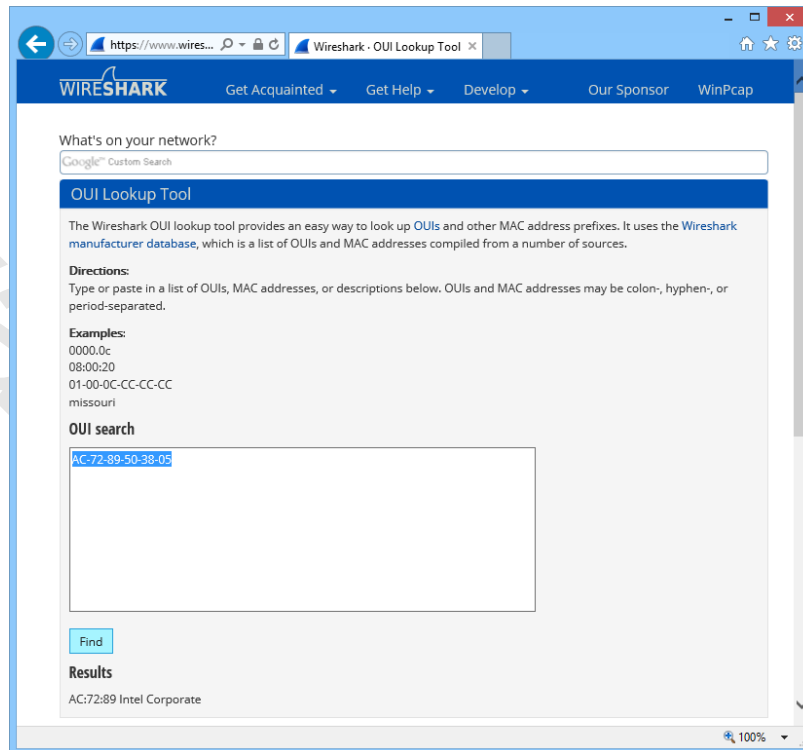
- **arp -a** (or **arp -g**) views the ARP cache contents; use with *IPAddress* to view the ARP cache for the specified interface only.
- **arp -s *IPAddress* *MACAddress*** adds an entry to the ARP cache. Under Windows, *MACAddress* needs to be entered using *hyphens* between each hex byte.
- **arp -d \*** deletes all entries in the ARP cache; can also be used with *IPAddress* to delete one entry only.



*The above illustrates some uses of the command under Windows. Syntax for Linux and UNIX is often different. Check the help for the utility on the system you are using to learn about switches and arguments available.*

## MAC Address Lookup Table

A **MAC Address Lookup Table** (or **OUI Lookup Table**) enables you to identify the manufacturer or a network adapter from the OUI value coded in its MAC address.



*Finding the network adapter vendor from a MAC address using Wireshark's OUI Lookup Tool*

## Protocol Analyzers



60wqy



7nvub



9rfjc



*Students will use Wireshark during the labs.*

A **protocol analyzer** (or **packet sniffer** or **network analyzer**) performs frame capture and analysis. The analyzer can be implemented on special hardware (as part of a cable tester for instance) or installed as software on a PC host. There isn't really much of a distinction between a packet sniffer and protocol analyzer. You can think of a packet sniffer as something that only captures frames (without doing any decoding, filtering, or analysis) but almost all the tools available have some sort of analysis functionality built-in, making the terms pretty much interchangeable.

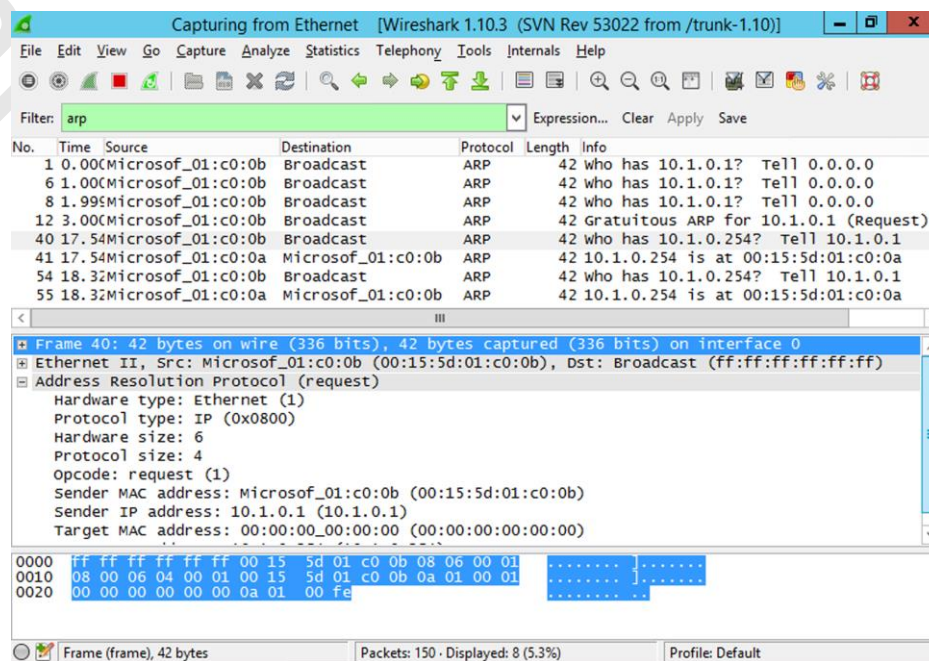
Protocol analyzers can decode a captured frame to reveal its contents in a readable format. You can choose to view a summary of the frame or choose a more detailed view that provides information on the OSI layer, protocol, function, and data.

The capabilities of different products vary widely, but in general terms protocol analyzers can perform the following functions:

- Identify the most active computers on the network, which aids in balancing traffic on networks.
- Isolate computers producing erroneous packets and rectify the problem.



- Filter traffic and capture packets meeting certain criteria (capturing traffic to and from a particular device for instance).
- Baselining - the activity on a network is sampled periodically to establish normal levels of activity. The baseline is then used to compare against activity when a problem is suspected or as a basis for network expansion plans.
- Generate frames and transmit them onto the network to test network devices and cabling.
- Monitor bandwidth utilization by hosts, applications, and protocols.
- Trigger alarms when certain network conditions fall outside "normal levels".



Wireshark protocol analyzer

## Promiscuous Mode and Sniffing Switched Ethernet

By default, a network interface only processes packets that are directed to that card (unicast or multicast traffic) or broadcast messages. Most packet sniffers can make a network adapter work in **promiscuous mode**, so that it processes all traffic within the Ethernet broadcast domain, whether it is intended for the host machine or not.

While this approach works for a hub, where all traffic is repeated on every port, on a switched network, the switch makes decisions about which port to forward traffic to, based on the destination address and what it knows about the machines connected to each port. This means that to capture unicast traffic intended for other hosts, the sniffer needs to be connected to a suitably configured spanning port (mirrored port).



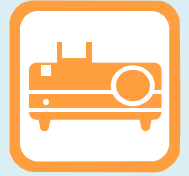
*There are various, less legitimate techniques available to sniff switched traffic, such as arp spoofing. See [Unit 5.1](#) for more details. Switches and mirrored ports are discussed in [Unit 1.3](#).*



### ***Review Questions / Module 1 / Unit 2 / Ethernet***

Answer these questions to test what you have learned in this unit. You can submit your answers and review the model answers on the [course website](#).

- 1) What is attenuation?
- 2) Is Pulse Amplitude Modulation a digital or analog signaling technique?
- 3) What are multiplexing and de-multiplexing?
- 4) Why might the baud rate be different from the bit rate?
- 5) With CSMA/CD, what will happen if a computer has data to transmit and there is already data on the cable?
- 6) What is an MTU?
- 7) True or false? The CRC mechanism in Ethernet allows for the retransmission of damaged frames.
- 8) Which Ethernet standard uses coaxial cabling?
- 9) True or false? A computer with a 10BASE-T Ethernet adapter cannot be joined to a 100BASE-T network.
- 10) What is an I/G bit?
- 11) If a mapping for a local host is not found in a source host ARP cache, how does the source host send an ARP request?
- 12) If a packet is addressed to a remote network, what destination MAC address will the sending node use?
- 13) True or false? The arp utility allows you to discover another host's MAC address.
- 14) On a switched network, what configuration changes must be made to allow a host to sniff unicast traffic from all hosts connected to a switch?



*Run labs 1-3 after completing the review questions with the students.*

# Module 1 / Summary

## *Topologies and Infrastructure*

---

In this module, you learned about the basic components that make up Local Area Networks.

*Try to include some time at the end of each module to check students' understanding and answer questions.*

### **Module 1 / Unit 1 / Topologies and the OSI Model**

- Networks comprise nodes, transmission media, intra- and internetwork devices, and protocols.
- Physical and logical topologies used include client/server, peer-to-peer, point-to-point, point-to-multipoint, star, bus, ring, mesh, and hybrid.
- The OSI model is used to analyze 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.

### **Module 1 / Unit 2 / Ethernet**

- Most LAN products are based on IEEE 802.3 (Ethernet).
- Transmission media and network physical and data link technologies can be distinguished by a number of factors, including modulation scheme, bandwidth, media type, and access control method.
- Ethernet includes specifications for a range of speeds (10/100 Mbps and 1/10 Gbps) using different media (principally copper twisted-pair and fiber optic).
- Addressing schemes apply at layer 2 (MAC) and layer 3 (Network / IP). Layer 2 MAC addresses (48-bit) are mapped to Layer 3 IPv4 addresses (32-bit) by ARP.
- Protocol analyzers (packet sniffers) such as Wireshark or Network Monitor allow for the capture and analysis of frames sent to and received by a network node.

# Taking the Exams

When you think you have learned and practiced the material sufficiently, you can book a time to take the test.

*Students should use these tables to help to revise for the exam.*

## Preparing for the Exam

We've tried to balance this course to reflect the percentages in the exam so that you have learned the correct level of detail about each topic to comfortably answer the exam questions. Read the following notes to find out what you need to do to register for the exam and get some tips on what to expect during the exam and how to prepare for it.

*Stress that the training material remains current for the stated exam code, regardless of the date or edition appearing on the exam.*

Questions in the exam are weighted by domain area as follows:

CompTIA Network+ Certification Domain Areas	Weighting
1.0 Network Architecture	22%
2.0 Network Operations	20%
3.0 Network Security	18%
4.0 Troubleshooting	24%
5.0 Industry Standards, Practice, and Network Theory	16%

The objectives and content examples are covered in units in the course as listed in the table below. You can also use the index at the back of the book to look up specific content examples:

Domain Objectives/Examples	Refer To
<b>1.1 Explain the functions and applications of various network devices</b> <i>Switch • Hub</i>	Unit 1.3 / Hubs, Bridges, and Switches
<i>Router</i>	Unit 2.5 / Routing
<i>Multilayer switch • Load balancer • Packet shaper</i>	Unit 3.4 / Applications and Services
<i>Access point (wireless / wired)</i>	Unit 4.3 / Installing Wireless Networks
<i>Analog modem • VPN concentrator</i>	Unit 4.5 / Remote Access
<i>Firewall • HIDS • IDS/IPS • Content filter</i>	Unit 5.2 / Security Appliances
<b>1.2 Compare and contrast the use of networking services and applications</b> <i>Web services • Unified voice services</i>	Unit 3.4 / Applications and Services
<i>Network controllers</i>	Unit 3.6 / Cloud and Virtualization
<i>VPN • Site to site / host to site / host to host • Protocols (IPsec, GRE, SSL VPN, PPP/PPTP) • RAS</i>	Unit 4.5 / Remote Access
<i>TACACS / RADIUS</i>	Unit 5.3 / Authentication

Domain Objectives/Examples	Refer To
<b>1.3 Install and configure the following networking services / applications</b> <i>DHCP (Static vs dynamic IP addressing, Reservations, Scopes, Leases, Options [DNS servers, suffixes], IP helper / DHCP relay)</i>	Unit 2.3 / DHCP and APIPA
<i>DNS (DNS servers, DNS records [A, MX, AAAA, CNAME, PTR], Dynamic DNS)</i>	Unit 3.2 / Name Resolution
<i>Proxy / reverse proxy • NAT (PAT, SNAT, DNAT) • Port forwarding</i>	Unit 5.2 / Security Appliances
<b>1.4 Explain the characteristics and benefits of various WAN technologies</b> <i>Fiber (SONET, DWDM, CWDM) • Frame relay • Satellite • Broadband cable • DSL/ADSL • ISDN • ATM • MPLS • GSM/CDMA (LTE/4G, HSPA+, 3G, EDGE) • Dial-up • WiMAX • Metro-Ethernet • Leased lines (T1, T3, E1, E3, OC-3, OC-12) • Circuit switch vs packet switch</i>	Unit 4.4 / WAN Technologies
<i>PPP / Multilink PPP</i>	Unit 4.5 / Remote Access
<b>1.5 Install and properly terminate various cable types and connectors using appropriate tools</b> <i>Copper connectors (RJ-11, RJ-45, RJ-48C, DB9 / RS-232, DB25, UTP coupler, BNC coupler, BNC, F-connector, 110 block, 66 block) • Copper cables (Shielded vs unshielded, CAT3, CAT5, CAT5e, CAT6, CAT6a, PVC vs plenum, RG-59, RG-6, Straight-through vs crossover vs rollover) • Fiber connectors (ST, SC, LC, MTRJ, FC, Fiber coupler) • Fiber cables (Single mode, Multimode, APC vs UPC) • Media converters (Single mode fiber to Ethernet, Multimode fiber to Ethernet, Fiber to coaxial, Single mode to multimode fiber) • Tools (Cable crimpers, Punch down tool, Wire strippers, Snips, OTDR, Cable certifier)</i>	Unit 4.2 / Installing Cable
<b>1.6 Differentiate between common network topologies</b> <i>Mesh (Partial, Full) • Bus • Ring • Star • Hybrid • Point-to-point • Point-to-multipoint • Client-server • Peer-to-peer</i>	Unit 1.1 / Topologies and the OSI Model
<b>1.7 Differentiate between network infrastructure implementations</b> <i>WAN • MAN • LAN • WLAN (Hotspot) • PAN (Bluetooth, IR, NFC)</i>	Unit 1.1 / Topologies and the OSI Model
<i>SCADA / ICS (ICS server, DCS / closed network, Remote terminal unit, Programmable logic controller)</i>	Unit 1.4 / Infrastructure and Segmentation
<i>Medianets (VTC, ISDN, IP/SIP)</i>	Unit 3.4 / Applications and Services
<b>1.8 Given a scenario, implement and configure the appropriate addressing schema</b> <i>MAC addressing • Broadcast domains vs collision domains</i>	Unit 1.2 / Ethernet
<i>IPv4 (Address structure)</i>	Unit 2.1 / Internet Protocol
<i>IPv4 (Subnetting, Classful A, B, C, D, Classless) • Private vs public • Multicast • Unicast • Broadcast</i>	Unit 2.2 / IPv4 Addressing
<i>IPv4 (APIPA)</i>	Unit 2.3 / DHCP and APIPA
<i>IPv6 (Autoconfiguration, EUI 64, DHCP6, Link-local, Address structure, Address compression, Tunneling 6to4, 4to6, Teredo, Miredo)</i>	Unit 2.4 / IPv6 Addressing
<i>NAT/PAT</i>	Unit 5.2 / Security Appliances

# Glossary

## 10xBASE

The Ethernet-type networks can be subdivided into several types of network. The IEEE 802.3 standard uses the following notation to indicate Ethernet type: x-BASE-y, where "x" indicates the data rate (in Mbps), "BASE" denotes that baseband transmission is used and "y" either describes the maximum media distance or the cable type. More recent standards define gigabit (1000BASE-Y) and 10 Gigabit (10GBASE-Y) speeds.

## 110 Block

Punch-down cross-connect format offering high density (supporting up to 300 pairs). 110 wiring blocks are used for various applications. The 110 IDC format is used in most patch panels and wall jacks.

## 25-pair / 100-pair

Data cabling has four pairs within a single jacket. Telephone cabling often uses bundles of color-coded 25-pair cables. These are generally unsuitable for data applications because of excessive crosstalk.

## 568A / 568B

Termination standards defined in the ANSI / TIA / EIA 568 Commercial Building Telecommunications Standards. 568A is mandated by the US government and for US residential wiring but the only commercial rule is not to mix the two on the same network. Wiring a cable with both 568A and 568B termination creates a crossover cable.

## 66 Block

Punch-down cross-connect used to terminate telephone wiring. Each 66 block can terminate a single 25-pair cable.

## 802 Protocols

The 802 standards, published by the LAN / MAN Standards Committee of the Institute of Electrical and Electronics Engineers (IEEE), define technologies working at the physical and data link layers of the OSI model. These layers are subdivided into two sub-layers. The Logical Link Control (LLC) sub-layer is used with other 802 protocols, such as 802.3 and 802.11, which are conceived as operating at a Media Access Control (MAC) sub-layer and the physical (PHY) layer.

## 802.1X

Port authentication framework that requires the device to authenticate before it is granted access to the network. 802.1X defines how devices should provide support for Extensible Authentication Protocol (EAP).

## Access Point

See: *Wireless Access Point*.

## ACL (Access Control List)

A list configured on a resource (such as file system object) or appliance (firewall or switch) that determines access / deny access rules. Filtering is often performed on the basis of MAC or IP address.

## ADSL

See: *DSL*.

## Antenna

Different types of antenna can be used to focus a signal to a particular point or more widely (omnidirectional). Many wireless devices use a simple rod-type antenna.

## API (Application Programming Interface)

A library of programming utilities used, for example, to enable software developers to access functions of the TCP/IP network stack under a particular operating system.

## APIPA (Automatic Private IP Addressing)

APIPA was 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. The host randomly selects an address from the range 169.254.1.0 - 169.254.254.255. This is also called a link-local address.

## Application Layer

OSI model layer providing support to applications requiring network services (file transfer, printing, email, databases, and so on).

## ARP (Address Resolution Protocol)

When two systems communicate using TCP/IP, an IP address is used to identify the destination machine. The IP address must be mapped to an interface (the NIC's MAC address). ARP performs the task of resolving an IP address to a hardware address. arp is also a utility used to manage the ARP cache.

*The glossary references almost all the terms used in the exam syllabus and acronyms list and the study notes.*

*Students should find it a useful revision tool when they are preparing for the exam.*



**arp ping / arping**

This is a version of ping used to test connectivity to a host. It uses ARP rather than ICMP and so cannot be blocked.

**ATM (Asynchronous Transfer Mode)**

ATM is an advanced implementation of packet switching that provides a high-speed transport mechanism for all types of data including voice and video. ATM divides information into 53-byte cells containing 48 bytes of data and 5 bytes of header data. The small size of the cells and their fixed length mean delays can be predictable so that time-sensitive data is readily accommodated.

**Attenuation**

Degradation of a signal as it travels over media. This determines the maximum distance for a particular media type at a given bit rate.

**Authentication**

Identifying a user on a network. Authentication allows the network administrator to control access to the network and (with some sort of rights system [authorization]) to particular resources on the network (directories, printers, configuration, and so on). Standard authentication consists of a user name and password (a logon). Secure authentication requires that transmission of the logon be encrypted.

**Autonomous System (AS)**

See: *BGP*.

**Backbone**

A backbone is a fast link that connects the various segments of a network.

**Backup**

Recovery of data can be provided through the use of a backup system. Most backup systems provide support for tape devices. This provides a reasonably reliable and quick mechanism for copying critical data. Backups take place under a schedule of tape rotation, which allows for optimum efficiency of backup and restore operations and for storage of media offsite.

**Bandwidth**

Bandwidth is the range of frequencies supported by a particular media type and more generally the maximum data rate supported by a link.

**Bandwidth Shaper**

See: *Traffic Shaping*.

**Baseband**

Baseband transmission uses the complete bandwidth of the media as a single transmission path. LAN signaling normally uses this transmission method and it is also more reliable than the broadband method.

**Baseline**

The point from which something varies. A configuration baseline is the original or recommended settings for a device while a performance baseline is the originally measured throughput.

**Beacon**

A special management frame broadcast by the AP to advertise the WLAN.

**BGP (Border Gateway Protocol)**

BGP is designed to be used between routing domains, or Autonomous Systems (AS), and as such is used as the routing protocol on the Internet, primarily between ISPs. Autonomous systems are designed to hide the complexity of private networks from the public Internet. Border (or edge) routers for each AS exchange only as much route information as is required to access other autonomous systems, rather than hosts within each AS. Autonomous System Numbers (ASN) are allocated to ISPs by IANA via the various regional registries.

**Bluetooth**

Short range (up to 32 feet or 10m) radio technology providing connectivity for mobile devices such as PDAs or XDAs (generally to synchronize email and contact data with a PC). It also provides connectivity for wireless devices generally (printer, mouse, keyboard, and so on).

**BNC (British Naval Connector/Bayonet-Neill-Concelman) Connectors**

These are twist and lock connectors that are used with coax cabling.

**Bonding**

Using multiple network adapters for a single link for fault tolerance and load balancing. For Ethernet, this type of "adapter teaming" is defined in 802.3ad. 802.11n and 802.11g Wi-Fi channels can also be bonded to improve bandwidth.

**BOOTP (Bootstrap Protocol)**

TCP/IP protocol enabling a host to acquire IP configuration information from a server or download a configuration program using TFTP. BOOTP is an earlier, simpler form of DHCP and also works over UDP port 67. Unlike DHCP, the configuration settings for each host must be manually configured on the server.



# Index

Where a term or phrase is abbreviated, the acronym is the form listed in the index. Note that index references are made to the nearest main heading for the topic in which the term appears.

<b>1</b>		Adherence to Standards417	Attacker .....344
1000BASE ..... 36		Administration..... 244	Attacks/Threats.....343
100BASE ..... 35		Administrative Distance134	Attenuation ...27, 273, 280
10BASE ..... 34, 35		Admission Control ..... 403	Authentication .....390
10GBASE..... 37, 308		ADSL ..... 314	Authorized Downtime..428
110 Block ..... 269		AES ..... 399	Autoconfiguration 118, 121
<b>2</b>		Agent..... 217	Autonegotiation.....35, 53
2.4 GHz..... 285		Air Conditioning ..... 252	Autonomous System
<b>3</b>		Air Flow ..... 246, 254	Number..... 133
3G ..... 317		Air Gap ..... 365	Awareness.....417
<b>4</b>		Alarms ..... 213	AWG.....263
4G ..... 317		Alert..... 213	
4to6 ..... 123		All-in-One Security	<b>B</b>
<b>5</b>		Appliance..... 386	Backbone.....4, 9
5 GHz..... 285		Amplification Attack .... 362	Backdoor .....358
568A / 568B ..... 267		Analog ..... 27	Backout Contingency Plan
<b>6</b>		Analog Modem ..... 332	.....443
66 Block ..... 269		Analysis Engine..... 387	Backup.....442
6to4 ..... 123		Anomaly-based Detection	Bad Connector.....273
<b>8</b>		..... 388	Bad Fiber Cable.....282
802 Standards... See IEEE		ANSI/TIA/EIA 568241, 264	Bad SFP/GBIC .....281
802.1X..... 402		Antenna Placement .... 293	Bad Wiring .....273
<b>A</b>		Antenna Types ..... 291	Bandwidth.....26, 129, 214
A / AAAA Record..... 161		Anti-malware Software383	Bandwidth Saturation..298
AAA Configuration..... 52		Anti-spam ..... 384	Bandwidth Shaper ..... 199
AAA Server ..... 395		Anycast ..... 120	Banner Grabbing .....348
Acceptable Use Policy 437		AP ..... 287, 288	Base64 .....360
Access Point ..... See AP		AP Configurations ..... 288	Baseband .....28
ACL ..... 367, 374, 376		AP Placement..... 293	Baseline.....206, 427
ACR ..... 273		APC ..... 278	Battery Backup .....415
Ad hoc Topology ..... 287		APIPA..... 109	Baud Rate.....29
Adaptability ..... 67		Application Control ..... 405	Beacon Frame .....290
Address Class..... 86		Application Layer .... 22, 74	Behavior-based Detection
Address Compression 116		Application Layer Gateway376	.....388
Address Structure 84, 117		Approaching Multiple	Bend Radius Limitations282
Addressing40, 100, 102, 114		Problems ..... 169	BGP ..... 133
		Approval Process ..... 428	BIA.....411
		Archiving..... 442	Binary ..... 114
		ARIN..... 76	Binary/Decimal Conversion85
		ARP (Protocol) ..... 40	Biometrics.....256
		arp (tool)..... 42	Bit Rate.....29
		ARP Cache Poisoning 356	Block/Allow .....374
		ARP Inspection... 349, 402	Blocking.....337
		Asset Management411, 429	Bluejacking / Bluesnarfing
		ATM..... 309	.....355
		Attack Surface ..... 358	Bluetooth .....64

BNC .....274  
 Bonding .....54  
 BOOTP .....106  
 Botnet .....361  
 Bottleneck .....207  
 Bottom-to-Top.....170  
 Bounce .....296  
 BPDU.....59  
 Bridge .....48  
 Broadband .....28  
 Broadband Cable.....315  
 Broadcast .....31, 95  
 Broadcast Domain ..56, 98  
 Broadcast Domain versus  
 Collision Domain.....95  
 Broadcast Storm .....181  
 Brute Force Attack .....360  
 BTU .....252  
 Building Layout .....259  
 Bus Topology.....9  
 Business Continuity ....411  
 Butt Set.....272  
 BYOD .....405

## C

Cable Certifier.....272  
 Cable Mismatch.....281  
 Cable Modem .....334  
 Cable Placement 175, 268  
 Cable Tester .....270, 272  
 Cable Tray .....246  
 Cabling .....17  
 Caching Engine .....380  
 Callback.....328  
 CAM.....50  
 Camera vs. Guard .....258  
 CAN .....63  
 Captive Portal .....404  
 CARP.....202  
 Carrier Wave .....25  
 Cat 3/5/5e/6/6A.....264  
 CATV .....315  
 CCTV .....258  
 CDMA .....316  
 Cellular Radio .....316  
 CENELEC.....241  
 Central Office.....303  
 CERT .....343  
 Chain of Custody .....424  
 Change Request.....428  
 Channel .....285, 298  
 Channel Bonding .....286  
 CHAP.....396

CIDR ..... 102, 135  
 Circuit..... 25  
 Circuit Switching 301, 305  
 Circuit-Level Firewall.. 375  
 Class (IP Addressing) .. 86  
 Classful Addressing ..... 96  
 Classless Addressing... 99  
 Cleartext Credentials 351,  
 360  
 Client..... 6  
 Closed Network..... 72, 73  
 Cloud Computing ..... 231  
 CNAME Record ..... 161  
 Coax Cable ..... 274  
 Collection of Evidence 423  
 Collision ..... 392  
 Collision Domain .... 29, 30  
 Company Security Policy337  
 Compatibility Requirements66, 71  
 Compliance ..... 365  
 Compromised System359,  
 361  
 Configuration Backup. 442  
 Configuration Management427  
 Configuration Procedures  
 ..... 428  
 Connectivity Software 219  
 Connector ..266, 274, 275,  
 278  
 Connector Mismatch.. 281  
 Consent to Monitoring 438  
 Console..... 51  
 Console Cable ..... 275  
 Content Inspection ..... 382  
 Content Switch..... 203  
 Contention..... 29  
 Convergence..... 128  
 Copper Line Driver /  
 Repeater ..... 331  
 CoS..... 199  
 Costs..... 129  
 Coverage ..... 293  
 CP ..... 415  
 CPE ..... 303  
 CRC ..... 17, 33  
 Crossover Cable ..... 268  
 Crosstalk ..... 263, 273  
 CSIRT ..... 420  
 CSMA/CA..... 30, 284  
 CSMA/CD ..... 30  
 CSU/DSU..... 331  
 Customer Premises  
 Equipment..... 330, 336  
 CWDM ..... 307

## D

Data Breach ..... 421  
 Data De-duplication.... 226  
 Data Link Layer ..... 17  
 Data Ownership ..... 405  
 Datagram ..... 83  
 dB Loss ..... 273  
 DB9 / DB25 ..... 275  
 DCS..... 73  
 DDoS..... 361  
 De-encapsulation ..... 15  
 Deep Packet Inspection386  
 Default Gateway..... 54, 89  
 Default Passwords / Settings358  
 Default Ports ..... 153  
 Default Route ..... 126  
 Default VLAN ..... 57  
 Demarc..... 330  
 De-multiplexing ..... 28  
 Determine If Anything Has  
 Changed..... 168  
 Device Antenna..... 291  
 Device Density ..... 290  
 Device Placement246, 254,  
 354  
 Device Saturation..... 298  
 Device Types /  
 Requirements..... 66, 70  
 DHCP ..... 107, 109, 183  
 DHCP Relay..... 112  
 DHCP Snooping ..... 402  
 DHCPv6 ..... 122  
 Diagram..... 429  
 Dial-up..... 311  
 DiffServ ..... 198  
 Digital ..... 28  
 Dirty Connectors ..... 282  
 Disabling Unused Features405  
 Disabling Unused Interfaces  
 / Service Ports..... 402  
 Disaster Recovery ..... 414  
 Discards ..... 215  
 Distance ..... 27, 273, 291  
 Distance Limitations ... 281  
 Distance Vector..... 128  
 Distribution Frame..... 243  
 Divide and Conquer ... 171  
 DLP ..... 406  
 DMZ ..... 368  
 DNAT ..... 373  
 DNS..... 158, 160, 184  
 DNS Issues ..... 337  
 DNS Record ..... 161



**CompTIA Network+ Certification  
Support Skills (Exam N10-006)**  
Instructor Edition  
Labs

G524Teng ver025 (PREVIEW)

## Acknowledgements

Course Developer .....gtslearning

Editor ..... James Pengelly



[www.gtslearning.com](http://www.gtslearning.com)

This courseware is owned, published, and distributed by **gtslearning**, the world's only specialist supplier of CompTIA learning solutions.

✉ [sales@gtslearning.com](mailto:sales@gtslearning.com)

☎ +44 (0)20 7887 7999 📠 +44 (0)20 7887 7988

📍 Unit 127, Hill House, 210 Upper Richmond Road,  
London SW15 6NP, UK

### COPYRIGHT

This courseware is copyrighted ©2015 *gtslearning*. Product images are the copyright of the vendor or manufacturer named in the caption and used by permission. No part of this courseware or any training material supplied by the publisher to accompany the courseware may be copied, photocopied, reproduced, or re-used in any form or by any means without permission in writing from the publisher. Violation of these laws will lead to prosecution.

All trademarks, service marks, products, or services are trademarks or registered trademarks of their respective holders and are acknowledged by the publisher.

### LIMITATION OF LIABILITY

Every effort has been made to ensure complete and accurate information concerning the material presented in this course. Neither the publisher nor its agents can be held legally responsible for any mistakes in printing or for faulty instructions contained within this course. The publisher appreciates receiving notice of any errors or misprints.

Information in this course is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Where the course and all materials supplied for training are designed to familiarize the user with the operation of software programs and computer devices, the publisher urges the user to review the manuals provided by the product vendor regarding specific questions as to operation.

There are no warranties, expressed or implied, including warranties of merchantability or fitness for a particular purpose, made with respect to the materials or any information provided herein. Neither the author nor publisher shall be liable for any direct, indirect, special, incidental, or consequential damages arising out of the use or the inability to use the contents of this course.

**Warning** All gtslearning products are supplied on the basis of a single copy of a course per student. Additional resources that may be made available from gtslearning may only be used in conjunction with courses sold by gtslearning. No material changes to these resources are permitted without express written permission from gtslearning. These resources may not be used in conjunction with content from any other supplier.

**If you suspect that this course has been copied or distributed illegally,  
please telephone or email gtslearning.**

# Table of Contents

---

Introduction .....	1
Lab 1 / Configuring a Network Adapter .....	2
Lab 2 / Using Hyper-V .....	3
Lab 3 / ARP and Packet Analysis .....	7
Lab 4 / IP Address Configuration .....	13
Lab 5 / IP Addressing Schemes .....	18
Lab 6 / Configuring DHCP in Windows .....	20
Lab 7 / Configuring DHCP in Linux .....	23
Lab 8 / IPv6 Addressing .....	26
Lab 9 / Configuring Routing .....	29
Lab 10 / TCP and Port Scanning .....	39
Lab 11 / Name Resolution .....	43
Lab 12 / Configuring DNS .....	49
Lab 13 / Configuring Email Services .....	52
Lab 14 / Performance Testing and Monitoring .....	58
Lab 15 / Monitoring and Management Tools .....	61
Lab 16 / Configuring Certificate Services, HTTPS, and FTPS .....	66
Lab 17 / Configuring a NAT Firewall .....	76
Lab 18 / Authentication Methods and VPNs .....	86

Evaluation Use Only



## **Introduction**

---

The following conventions have been used in the course practical lab exercises.

- Bullet and number lists - steps for you to follow in the course of completing a task or hands-on exercise.
- File and command selection - files, applets, dialogs and other information that is displayed on the screen by the computer is shown in sans serif bold. For example: Click **OK**, Select **Control Panel**, and so on.
- Sequences of commands - a sequence of steps to follow to open a file or activate a command are shown in bold with arrows. For example, if you need to access the system properties in Windows, this would be shown in the text by: **Start > Control Panel > System**.
- Commands - commands or information that you must enter using the keyboard are shown in Courier New Bold. For example: Type **webadmin@somewhere.com**. Courier New Bold-Italic represents some sort of variable, such as your student number. For example, if your student number is "5", you would follow the instruction **ping 10.0.0.x** by entering **ping 10.0.0.5**.
- Using the mouse - when instructed to click, use the main mouse button; when instructed to alt-click, use the secondary button (that is, the button on the right-hand side of the mouse, assuming right-handed use). Sometimes you need to use both the keyboard and the mouse - for example, **Ctrl+click** means hold down the **Ctrl** key and click the main mouse button.





Duration - 15 minutes.

*This lab is performed on the HOST PC. If the OS is other than Windows 8, steps may vary slightly. The options available may also depend on the network adapter driver.*

### **Lab 1 / Configuring a Network Adapter**

In this lab you will use Device Manager to discover what properties and configurable settings your network adapter has.

- 1) On the **HOST** PC, alt-click the **Start** button and select **Device Manager**.

The list of installed devices appears.

- 2) Click the arrow symbol beside **Network adapters** to expand the **Network Adapter Subtree**.

- 3) What is the name of your network card?

\_\_\_\_\_

- 4) Alt-click your network card and select **Properties**.

- 5) Click the **Driver** tab and record the following information (you may need to use the **Driver Details** button too):

- Provider: \_\_\_\_\_
- Version: \_\_\_\_\_
- Date: \_\_\_\_\_
- File path: \_\_\_\_\_

- 6) Look at the configuration options on the **Advanced** tab. Is there an option to define a locally administered address?

\_\_\_\_\_

- 7) Look for the link speed and duplex configuration option - what is it set to?

\_\_\_\_\_

- 8) Does the adapter support advanced features, such as WoL ("wake up") or ToE (offload)?

\_\_\_\_\_

- 9) Click **Cancel** to the **Properties** dialog.

- 10) Select **View > Show hidden devices**.

The adapter list should refresh to show a number of other adapters, mostly used for remote tunneling protocols (WAN Miniport) or IPv6 tunneling (ISATAP).

- 11) Close **Device Manager**.



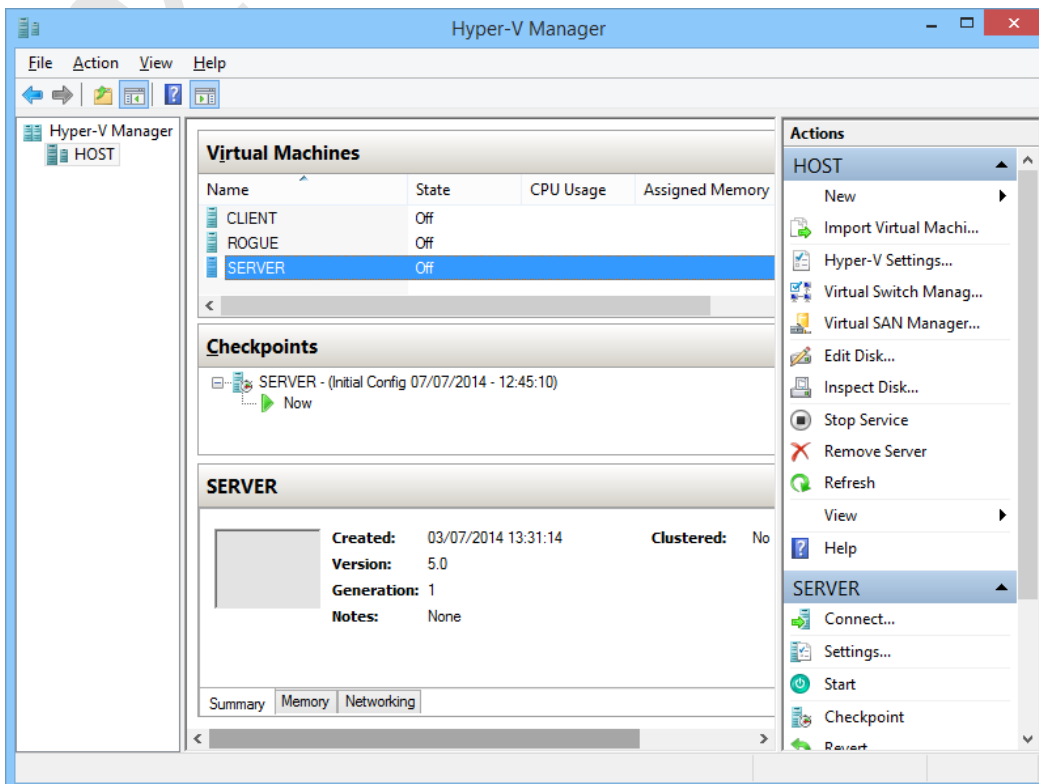
## Lab 2 / Using Hyper-V

Duration - 15 minutes.

Many of the practical labs in this course use Microsoft's host virtualization product Hyper-V. In this lab, you will learn how to configure the Virtual Machines (VM) and about the VMs that you will use.

- 1) On the **HOST** PC, press **Start** then type **Hyper-V Manager** then press **Enter**.

The Hyper-V Manager console is loaded. This shows the VMs available to you. Selecting a VM displays more information about it.



Hyper-V console

You have 6 VMs:

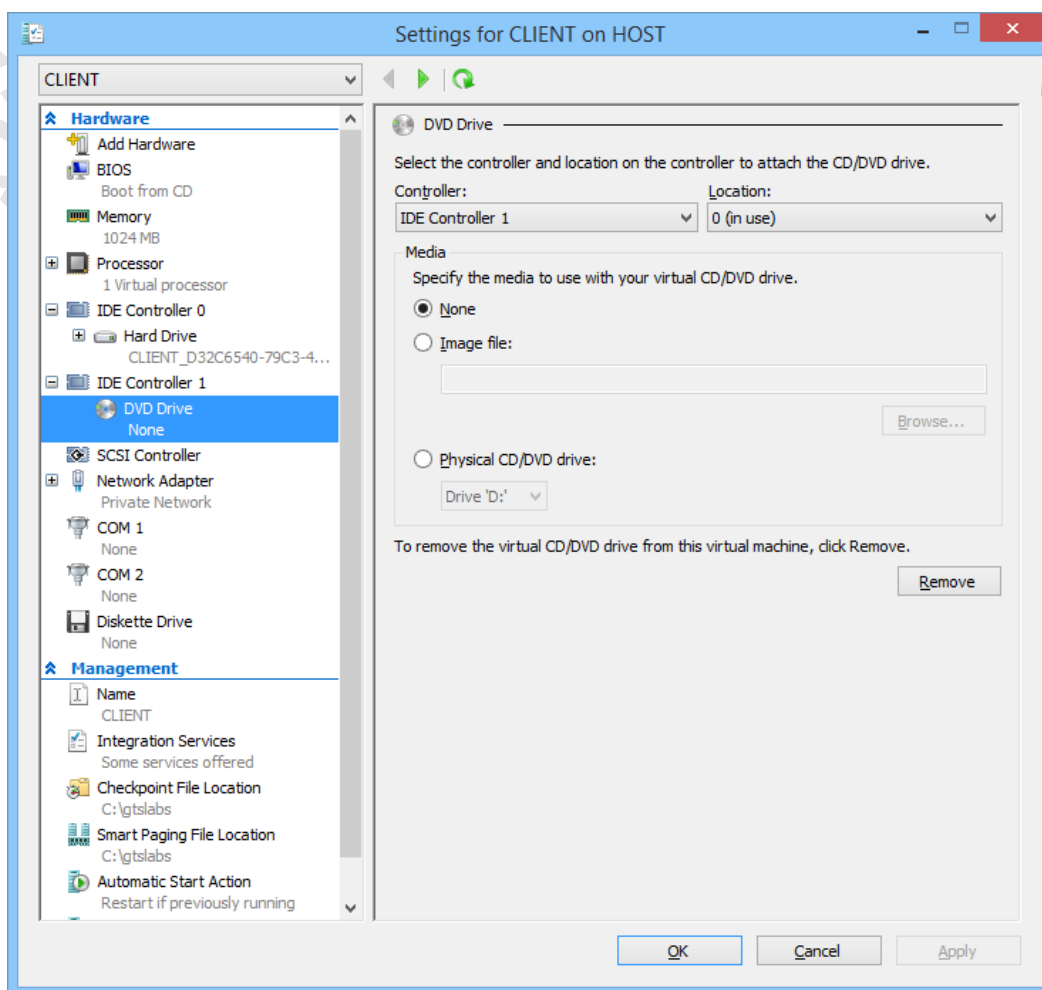
- CLIENT and ROGUE are Windows 8.1 Enterprise workstations. CLIENT will be connected to the Windows domain network. ROGUE will be used (mostly) to make remote connections to the Windows network.
- SERVER is a Windows Server 2012 R2 Enterprise server that will host resources on the Windows domain network.
- GATEWAY is a Windows Server 2012 R2 Enterprise server that you will configure as a router for the Windows network.
- ROUTER is a Linux server (running the Ubuntu distribution of Linux).

- LAMP is also an Ubuntu Linux server, configured as a web server (installed with the OS and applications Linux, Apache [web server], MySQL [database], and PHP [programming]).

2) Alt-click the **CLIENT** VM then select **Settings**.

This dialog allows you to configure the VM's hardware. Some settings can only be changed when the VM is powered off; others you can change from the VM's window menu when it is running.

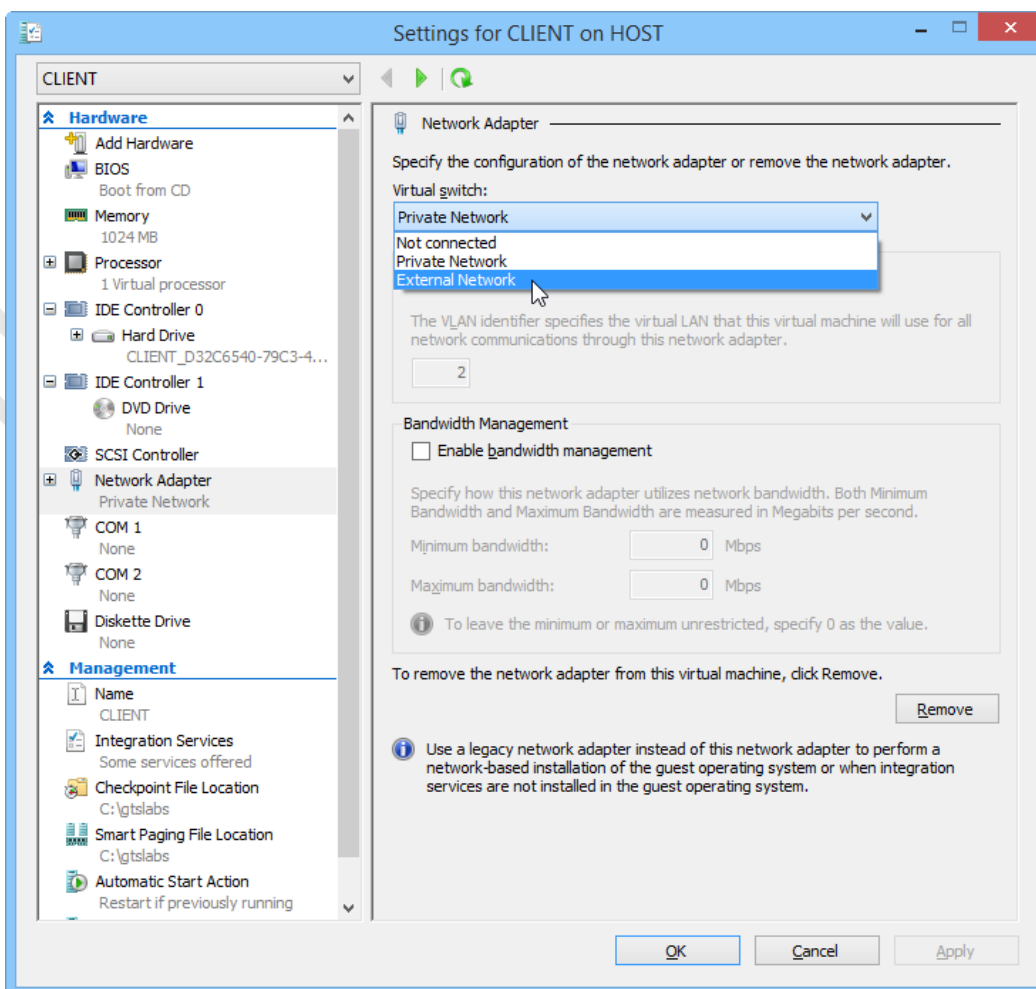
3) Observe the IDE and SCSI controller nodes.



Configuring VM storage options

These nodes allow you to add hard drives to the VM and to use disc images (ISOs) in the optical drive (or share the HOST's drive).

- 4) Click the **DVD Drive** node, then on the opposite pane select **Image file** and click **Browse**. Locate the Windows 8 ISO image in **c:\GTSLABS** and click **Open**.
- 5) Click the **Network Adapter** node.



Configuring network options


This page allows you to choose which network switch the adapter is connected to. In these labs, the switches will be configured so that each VM can "see" only other VMs installed on the host but not the host itself or the physical network. The VMs can be put on separate internal networks by giving the networks names, much like a Virtual LAN (VLAN). The CLIENT VM is on a network named "Private Network".

You can also "install" additional adapters in a VM. This is an option we will use later in the labs.

- 6) Click **OK**.
- 7) With the **CLIENT** VM still selected, observe the **Checkpoints** pane.

A checkpoint is an image of the VM's disk at a particular point. You can use checkpoints to discard the changes in a particular lab or reset the lab if you need to attempt it again from the start.

These checkpoints can be used to revert any VM easily to its initial configuration if necessary.

- 8) Double-click the CLIENT VM to connect to it. A new window will open. Click the **Start** button  to boot the VM.

When the VM has booted, you may be asked to choose a desktop size. If so, choose a setting that is smaller than your host desktop resolution, so that the entire VM desktop will be easily visible.



*To change the console window size, when the VM is running, alt-click the icon in the Hyper-V Manager console and select **Edit Session Settings**.*

9) Click on **CLIENT\Admin** to log in.

10) Enter the password **Pa\$\$w0rd**.



*That's a zero between the "w" and the "r".*

11) On the VM window, click the **File > Settings** menu. You can configure some settings here (though you cannot change the installed hardware without shutting down the VM).

12) On the VM window, click the **Media > DVD Drive** menu. You can select a different ISO or choose the host drive here (or just eject the current image).

13) In the CLIENT VM, alt-click the Start button and select **Shut down or sign out > Shut down**.

During the labs you will use the Ubuntu Server Linux distribution. This is operated at a command prompt with no GUI.

14) Double-click the LAMP VM to open its console then click the **Start** button to boot it. When the computer has booted, a "lamp login" prompt will be displayed.

15) Type **administrator** and press **Enter**.



*Remember that all commands in Linux are case-sensitive.*

16) Type **Pa\$\$w0rd** and press **Enter**.

To run system-level commands in this distribution of Linux, you have to precede them with the **sudo** command to obtain elevated (root) privileges. Shutting down the machine is an example of a system-level command.

17) Type **sudo shutdown -h now** and press **Enter**.

18) Type **Pa\$\$w0rd** and press **Enter**.



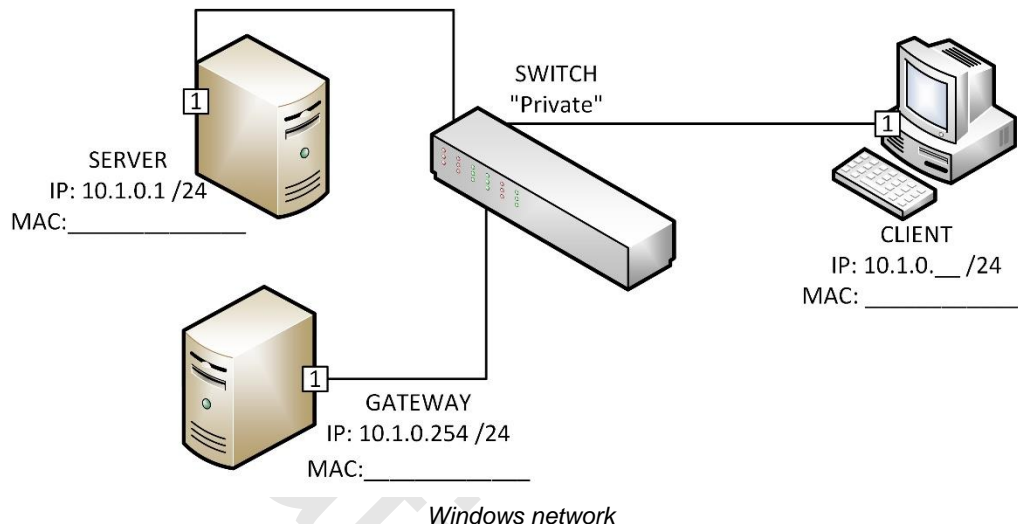
*You do not have to enter the password every time you use **sudo**. The password gets cached for a few minutes.*



### Lab 3 / ARP and Packet Analysis

Duration - 30 minutes.

In these exercises, you will investigate ARP and the use of the Wireshark protocol analyzer to capture and inspect network traffic.



#### Exercise 1: Investigating the ARP Cache Table

The ARP cache table contains entries for hosts that have been contacted recently (the cache is cleared every few minutes). This reduces the frequency of ARP broadcasts.

- 1) In the Hyper-V Manager console on the HOST, alt-click the **GATEWAY** VM icon and select **Start**. Double-click the icon to open a console window.
- 2) When the **GATEWAY** VM has booted, log on with the user name **Administrator** and the password **Pa\$\$w0rd**. At log on, Server Manager will be started. Wait for this to initialize before proceeding.
- 3) Press **start**, type **cmd**, then press **Enter** to load the **Command Prompt**.
- 4) Enter **arp -a**.

This displays the ARP cache table. The only entries should be for the network broadcast address (10.1.0.255) used to address every machine on the local network and multicast addresses (starting 224) used by Windows' network discovery protocols.


Remember that the VM is set to use the Windows VMs' local network and there are no other machines on that network yet so it is not surprising that there are no host addresses yet.

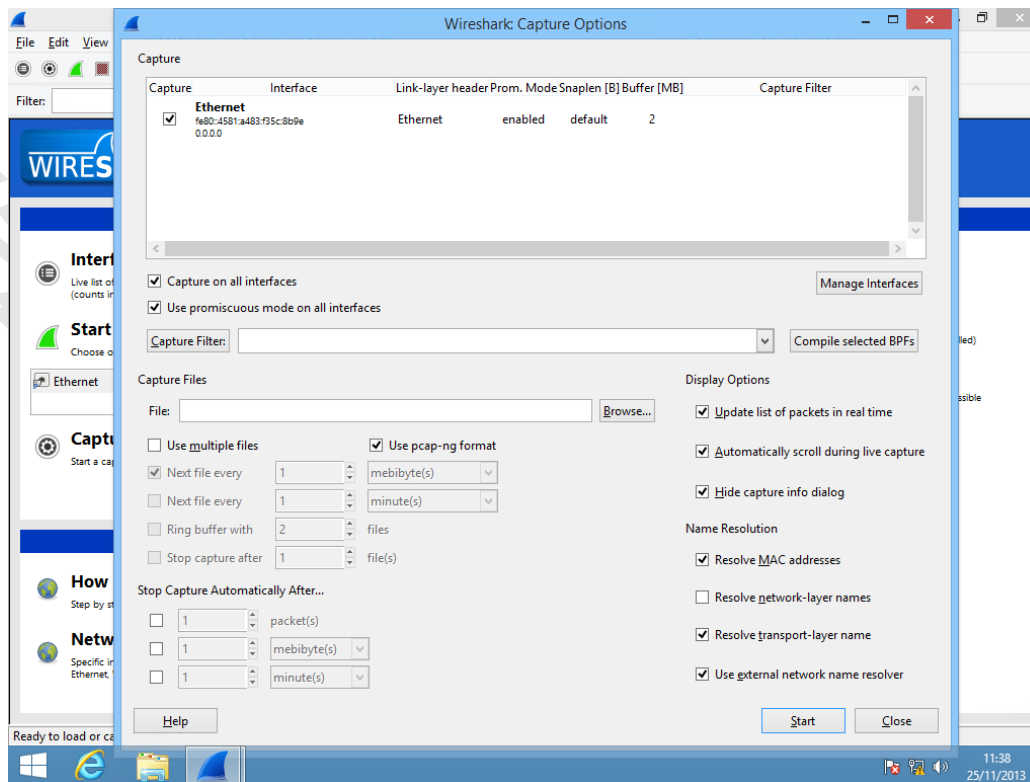
#### Exercise 2: Using Wireshark to Capture Packets

Wireshark is an example of a protocol analyzer. It allows you to view the contents of packets being sent to and from the local machine (and, in some circumstances, other machines).



1) Double-click the **Wireshark** icon on the Desktop.

2) When the program has loaded, click the **Capture Options** button  in the toolbar.




Wireshark capture options

3) Ensure that the adapter is set to "Ethernet" (this is the virtual adapter driver used by VM), that the "Capture filter" box is empty, and that **Use promiscuous mode on all interfaces** is checked.

4) Click **Start**.

5) Switch to the Hyper-V Manager console on the HOST, start the **SERVER** VM, then open a console for it.

6) Switch back to the GATEWAY VM console and watch the packet capture window while the SERVER VM boots. Maximize the window and adjust the size of the panes so that you can view the frames clearly.

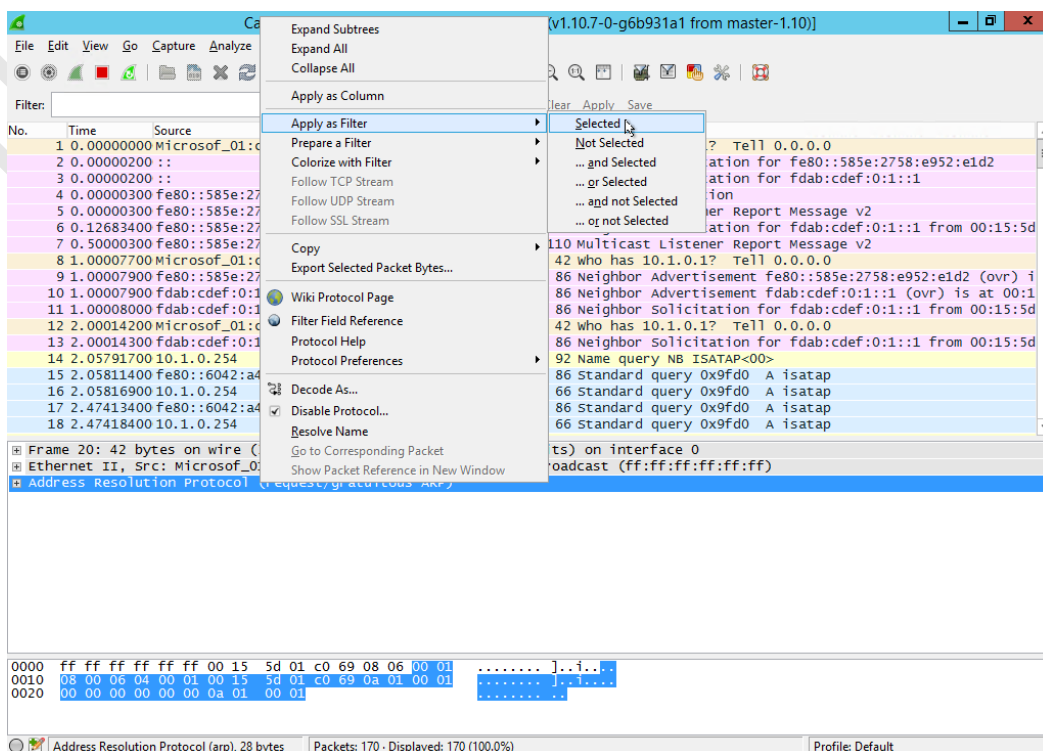
7) Click the **AutoScroll** button  to turn off autoscrolling then scroll to the top of the capture.

One of the most useful options in packet analysis software is the one to filter by different criteria. You may have noticed in the Capture Options dialog that there was a capture filter option (to only record packets that match the filter in the first place).



You can also apply filters to the captured data. You can construct complex filter criteria by building an expression or by alt-clicking in the frame analysis pane.

- 8) Select the first ARP frame in the top pane, then in the middle pane, alt-click **Address Resolution Protocol** and select **Apply as Filter > Selected**.



Applying a filter

The frames panel now shows only ARP traffic. Note the filter expression "arp" has been added to the filter panel and that the panel is highlighted green to show that a filter is in effect.

You should now be able to see the results of an ARP session. The SERVER machine is checking whether anyone owns its IP address (10.1.0.1); there is no reply to this broadcast, as SERVER owns the IP address 10.1.0.1




*If another machine did own 10.1.0.1, SERVER would detect a duplicate IP address and prompt the user to change the configuration.*

- 9) Click each ARP frame in the top pane and expand the frame analysis in the second pane.


Note that the frame (data link layer) simply contains source and destination MAC addresses (note that some frames use the broadcast address) and a protocol type field (ARP) plus a checksum (part of the trailer, which also ensures that the frame is at least the minimum length). Note that Wireshark decodes the OUI and that you can expand the MAC fields to decode the multicast/broadcast bit and locally administered bit.

The ARP headers (layer 2.5 or 3-ish) contain similar information plus the sender and target IP addresses. ARP is a very simple protocol. IP and higher level packets often contain many more headers.

Also note the bottom frame. This contains the raw data in hexadecimal format (the computers receive it as a series of 1s and 0s. When you select information in pane 2, the relevant hex digits are selected here (and vice versa).

- 10) In the filter bar, click the **Clear** button then turn autoscrolling back on.
- 11) When SERVER has finished booting, enter the password **Pa\$\$w0rd** to log on as **CLASSROOMAdministrator**.
- 12) Open File Explorer and enter `\\10.1.0.254\admin$` in the address bar.
- 13) When the server share has opened, switch back to the GATEWAY VM and click **Stop**  to halt packet capture.

The captured frames are displayed.

- 14) Look for a second ARP session as SERVER resolves the IP address 10.1.0.254 to a MAC address.
- 15) Click one of the SMB2 frames - note that additional layers of protocols are shown in the frame analysis pane. SMB (the protocol used for file sharing on Windows networks) makes more use of the upper network layers than ARP (IP for logical addressing at the network layer, TCP at the transport layer, NetBIOS at the session layer, and SMB (version 2) itself to exchange the application data).
- 16) Press the **Start** button  to start another packet capture with the current options set. When you are prompted to save the packet capture, click **Continue without Saving**.

- 17) Boot the CLIENT VM. What do you notice that is different about the packet capture?

---

---

---

- 18) Analyze the ARP traffic and fill in the MAC addresses for all the computers in the network diagram at the start of the lab.

- 19) Stop the packet capture.

*CLIENT uses DHCP so broadcasts to discover an address, which SERVER responds to (note that the DHCP used by CLIENT is different to the DHCPv6 protocol that VMs are using to autoconfigure their IPv6 link-local adapters).*

*Note that there are much easier ways to discover a workstation's MAC address but the point here is to ensure the students can decode the source and destination fields.*

**Exercise 3: ARP Problems**

In this exercise, you will investigate some of the problems that can be caused by an incorrect MAC address.

As a first step, you will disable IPv6 on the GATEWAY VM so that it can only contact SERVER using IPv4.

- 1) On the GATEWAY VM, alt-click the **Network Status** icon in the notification area and select **Open Network and Sharing Center**.

This page gives you an overview of the network and file sharing / firewall settings.

- 2) Click **Change adapter settings**.



A shorter route to the Network Connections page is to run `ncpa.cpl`.


- 3) Alt-click **Ethernet** and select **Properties**. Click the **Internet Protocol Version 6 (TCP/IPv6)** check box to *clear* the tick. Click **OK**.
- 4) Switch back to the command prompt and repeat the `arp -a` command (you can press the `Up` arrow key to select from previously issued commands).
- 5) Are there any entries? How do you explain this?

---



---

*There will either be an entry for 10.1.1 or 10.1.0.128 or both or no entry. Hopefully some students will see an empty cache.*

- 6) In Wireshark, press the **Capture Options** button . In the "Filter" box, enter `arp`.
- 7) Click the **Start** button. When you are prompted to save the packet capture, click **Continue without Saving**.
- 8) Open File Explorer and enter `\\SERVER\admin$` in the address bar. You should be able to see the folders in the administrative share.
- 9) Close the File Explorer window.
- 10) In the command prompt, check the ARP cache and note the result below:

---

*ARP entries are only cached for a couple of minutes. If no network activity has taken place, it could be that the cache will be empty but being on a domain means there is plenty of "chat".*

- 11) Enter the following command:

```
arp -s 10.1.0.1 aa-bb-cc-dd-ee-ff
```

Note the error. The latest versions of Windows prevent use of the `arp` tool to change hardware addresses on the local subnet. You can however use a `netsh` command to do the same thing.

*There will be an entry for 10.1.0.1 - SERVER - along with its MAC address.*

The server cannot be found.

GATEWAY is convinced it knows the MAC address of 10.1.0.1 and cannot figure out why it is not getting a response. Note that GATEWAY is still receiving ARP packets from 10.1.0.1, which is SERVER wondering why GATEWAY has "disappeared".

Using the IP address rather than the machine name has no effect because ARP is a more fundamental type of addressing than either.

The entry type is "Static".

ARP fires up again because the cache table has been cleared of the incorrect static mapping and normal to and fro communications are restored.

12) At the command prompt, run the following command (ignore the line break):

```
netsh interface ipv4 add neighbors Ethernet 10.1.0.1
aa-bb-cc-dd-ee-ff
```

13) Open Explorer and enter \\SERVER\admin\$ in the address bar. What happens?

---

14) Try \\10.1.0.1\admin\$ in the address bar - does this work?

---

15) What do you notice about the captured frames?

---

16) View the ARP cache again. What do you notice about the entry?


---

17) Enter the command `netsh interface ip delete arpcache` then try to connect to \\SERVER\admin\$ again. Observe the packet capture as you do so. What happens and why?

---

#### **Exercise 4: Closing the Lab**

At the end of this lab, we will discard any changes that might have been made to either VM.

- 1) On each VM's console window, click the **Revert** button  in the toolbar.
- 2) Confirm by clicking the **Revert** button in the dialog.