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	**1.6 Differentiate between common network topologies** *Mesh (Partial, Full) • Bus • Ring • Star • Hybrid • Point-to-point • Point-to-multipoint • Client-server • Peer-to-peer* **5.1 Analyze a scenario and determine the corresponding OSI layer** *Layer 1 – Physical • Layer 2 – Data link • Layer 3 – Network • Layer 4 – Transport • Layer 5 – Session • Layer 6 – Presentation • Layer 7 – Application* **5.2 Explain the basics of network theory and concepts** *Encapsulation / de-encapsulation*
Unit 1.2 / Ethernet	**1.8 Given a scenario, implement and configure the appropriate addressing schema** *MAC addressing • Broadcast domains vs collision domains* **4.2 Given a scenario, analyze and interpret the output of troubleshooting tools** *Command line tools (arp, MAC address lookup table) • Protocol analyzer* **5.2 Explain the basics of network theory and concepts** *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* **5.4 Given a scenario, deploy the appropriate wired connectivity standard** *Ethernet standards (10BASE-T, 100BASE-T, 1000BASE-T, 1000BASE-TX, 10GBASE-T, 100BASE-FX, 10BASE-2, 10GBASE-SR, 10GBASE-ER)*

Refer To	Domain Objectives/Examples
Unit 1.3 / Hubs, Bridges, and Switches	**1.1 Explain the functions and applications of various network devices** *Switch • Hub* **2.6 Given a scenario, configure a switch using proper features** *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*
Unit 1.4 / Infrastructure and Segmentation	**1.7 Differentiate between network infrastructure implementations** *WAN • MAN • LAN • WLAN (Hotspot) • PAN (Bluetooth, IR, NFC) • SCADA / ICS (ICS server, DCS / closed network, Remote terminal unit, Programmable logic controller)* **1.12 Given a set of requirements, implement a basic network** *List of requirements • Device types / requirements • Environment limitations • Equipment limitations • Compatibility requirements • Wired / wireless considerations • Security considerations* **5.4 Given a scenario, deploy the appropriate wired connectivity standard** *Ethernet standards (IEEE 1905.1-2013 [Ethernet over HDMI, Ethernet over Powerline])*

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**.

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.
- 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.
- 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 and Distance

One definition of **bandwidth** is the range of frequencies available in a modulated carrier wave. This can be measured in different units, from signals propagating once per second (1 Hz) to those propagating thousands (KHz), millions (MHz), billions (GHz), or trillions of times per second (THz). If the signaling method supports a range of frequencies from 0 to 100 MHz, it has 100 MHz bandwidth. Having a greater range of frequencies available allows the wave to carry more information.

The term "bandwidth" is also often used in computing just to mean the amount of information that can be transferred per second.

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).
- **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.

Copper Cable

Copper cable is used to carry signals over electrical conductors at KHz and MHz frequencies. The drawback is that the signals are susceptible to interference and dispersion. There is some degree of impedance in the copper conductor, signals can "leak" easily from the wire, and noise can also leak into the wire. This means that copper cable suffers from high attenuation, meaning that the signal loses strength over long links.

Fiber Optic Cable

Fiber optic cable carries very high frequency radiation in the infrared light part of the electromagnetic spectrum. Even though high frequencies are used they are very closely contained within the optical media and can propagate more easily. The light signals are also not susceptible to interference or noise from other sources. Consequently fiber optic cable supports higher bandwidth over longer links than copper cable.

Wireless Radio

Radio Frequencies (RF) can propagate through the air between sending and receiving antennas. This requires much more power than with electrical signals passing over copper conductors however. The use of the radio part of the electromagnetic 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.

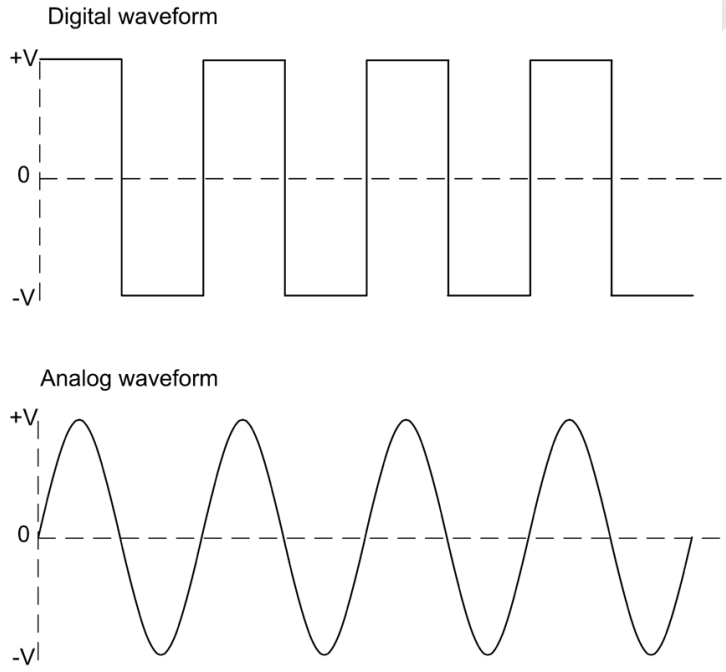
Wireless radio networking products operate in unregulated "Industrial, Scientific, and Medical (ISM)" bands (2.4 and 5 GHz) but there is a limit on power output and there is also often substantial interference, which means range is limited. Also, each product must work within a fairly narrow channel, allowing bandwidths in the MHz ranges only.

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 or 8 KHz) to ensure an accurate representation of the original analog waveform.
3) The sample size is 1 byte (or 8 bits).
4) Therefore, 8 KHz x 8 bits = 64 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 and 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 in the signal, measured in **bits per second (bps)**, or some multiple thereof.

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.

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 nodes that use it. This means that networks need ways of determining when nodes 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 nodes are allowed to communicate using the network.

Contention and Collision Domains

In a **contention**-based system, each network node within the same **collision domain** competes with the other connected nodes for use of the transmission media. When two nodes 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 nodes are added to the network and consequently the effective data rate (or throughput) reduces too.

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

Although much less frequent, collisions still occur as multiple nodes 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 nodes 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**.

yonl6

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 interface's transmit and receive lines simultaneously. On detecting a collision, the node 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 node can transmit *or* receive, but cannot do both at the same time. Modern intranetwork appliances, such as switches, allow for **full duplex** transmissions, where a device can transmit and receive simultaneously.

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.

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**.

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.

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.

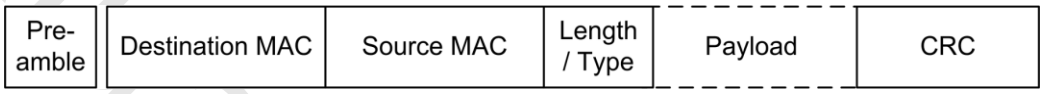
See Unit 2.2 and Unit 2.5 for more information on IP and routing and Unit 1.3 for topics on bridges and switches.

Ethernet Frames

Many technologies have been developed to enable local networks 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) 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:



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

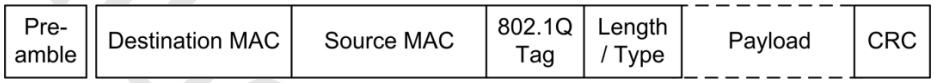
The official 802.3 standard defines a 2-byte *length* field to specify the size of the data field (also called the **payload**). This payload can normally be between 46 and 1500 bytes. The upper limit of the payload is also referred to as the **Maximum Transmission Unit (MTU)**.

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 **IEEE 802.1Q Virtual LAN (VLAN)** standard specifies use of a 32-bit (4-byte) tagging field inserted between the source address and length fields. This makes the maximum allowable frame size 1522 bytes. This increase in frame size is implemented by the 802.3ac amendment to the Ethernet standard.



Construction of an 802.1Q / 802.3ac (VLAN tagged) Ethernet frame

The tag field can be used to identify the VLAN to which the frame belongs and to assign an **IEEE 802.1p** frame priority level.

VLANs are a means of dividing a single physical network into multiple logically distinct networks. See Unit 1.3 for details. IEEE 802.1p is a means of prioritizing some types of traffic over others as part of a Quality of Service (QoS) mechanism. QoS and 802.1p are discussed in Unit 3.4.

Some Gigabit and 10G 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 32-bit (4-byte) 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.

Legacy Ethernet Standards

gchdb h1b0s

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 bus cable using a T-connector. The bus 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.