3.1.2 Network Adapter Facts

A network adapter (also called a network interface card, or NIC) connects a host to the network medium. It is responsible for converting binary data into a format that can be sent on the network medium.

- The network adapter is responsible for converting binary data into a format that can be sent on the network medium.
  - A transceiver is responsible for converting digital data into digital signals to be sent on the medium. The type of signal the transceiver sends depends on the type of network. A fiber optic NIC sends light signals, a wired NIC sends electronic signals on a wire, and a wireless NIC sends radio signals. To receive signals, the transceiver converts digital signals from the network to digital data for the PC.
  - A modem converts binary data to analog waves on the sending end (modulation) and then converts the analog waves back to binary data on the receiving end (demodulation).
- Some computers, like laptops, come with built-in network adapters. Other computers use NICs that plug in to the system's expansion slots or are external to the computer and connect through an existing computer port.
- Network adapters are Layer 1 devices because they send and receive signals on the network medium. They are also Layer 2 devices because they must follow the rules for media access and because they read the physical address in a frame.
- The type of network adapter you choose must match the network architecture you are connecting to.
- Older network adapters used an external transceiver to connect to the network media. However, all modern network adapters use a built-in transceiver.

Network Adapter Components

The following table describes various components used by a network adapter.

Component	Description
Transceiver Module	A transceiver module is used to change the media type of a port on a network device, such as a switch or a router. The following are the most common types of transceiver modules: - A GBIC (gigabit interface converter) is a large transceiver that fits in a port slot and is used for Gigabit media, including copper and fiber optic. - An SFP (small form-factor pluggable) is similar to a GBIC, but is a smaller size. An SFP is sometimes called a mini-GBIC. - SFP+ is a newer version of the SFP. SFP+ supports data rates as high as 10 Gbit/s, 8 Gbit/s Fibre Channel, 10-gigabit Ethernet, and the Optical Transport Network standard OTU2. - An XFP transceiver is similar to an SFP in size, but is used for 10-Gigabit networking. - QSFP (quad, or 4-channel, small form-factor pluggable) is a compact hot-pluggable transceiver that is also used for data communication applications.
Media Converter	A media converter is used to connect network adapters that are using different media types. For example, a media converter could be used to connect a server with a fiber optic Ethernet NIC to a copper Ethernet cable. - Media converters work at the Physical layer (Layer 1). Media converters do not read or modify the MAC address in any way. - Media converters only convert from one media type to another within the same architecture (such as Ethernet). A media converter cannot translate between two different architectures. This must be done using a bridge or a router. Converting from one architecture to another would require modifying the frame contents to modify the Data Link layer address.
MAC Address	A MAC address is a unique identifier burned into the ROM of every Ethernet NIC. - The MAC address is a 12-digit (48-bit) hexadecimal number (each number ranges from 0–9 or A–F). - The address is often written as 00-B0-D0-06-BC-AC or 00B0.D006.BCAC (dashes, periods, and colons can be used to divide the MAC address parts). - The MAC address is globally unique by design. The first half of the MAC address, the first six digits, is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value that identifies the host address. A manufacturer that uses all the addresses in the original assignment can apply for a new MAC address assignment. - Devices use the MAC address to send frames to other devices on the same subnet. Some network cards allow you to change the MAC address through jumpers, switches, or software, but there are few legitimate reasons for doing so.
Address Resolution Protocol (ARP)	Hosts use ARP to discover the MAC address of a device from its IP address. Before two devices can communicate, they must know the MAC address of the receiving device. If the MAC address isn't known, ARP does the following to find it: 1. The sending device sends out a broadcast frame. - The destination MAC address is all Fs (FFFF:FFFF:FFFF). - The sending MAC address is its own MAC address. - The destination IP address is the known IP address of the destination host. - The sending IP address is its own IP address. 2. All hosts on the subnet process the broadcast frame, looking at the destination IP address. 3. If the destination IP address matches its own address, the host responds with a frame that includes its own MAC address as the sending MAC address. 4. The original sender reads the MAC address from the frame and associates the IP address with the MAC address, saving it in its cache. Once the sender knows the MAC address of the receiver, it sends data in frames addressed to the destination device. These frames include a cyclic redundancy check (CRC), which is used to detect frames that have been corrupted during transmission. Hosts use the reverse address resolution protocol (RARP) to find the IP address of a host with a known MAC address.