NETWORK INTERFACE CARD

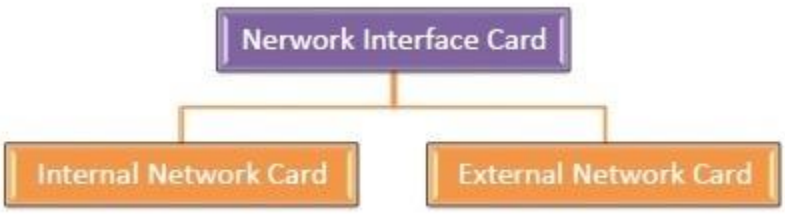
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called a network interface controller, network adapter, or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over the large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types –



Internal Network Cards

In internal network cards, the motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses the Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard; however, no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

ARCNET

ARCNET is a widely-installed local area network (LAN) technology that uses a token-bus scheme for managing line sharing among the workstations and other devices connected to the LAN. The LAN server continuously circulates empty message frames on a bus (a line in which every message goes through every device on the line and a device uses only those with its address). When a device wants to send a message, it inserts a "token" (this can be as simple as setting a token bit to 1) in an empty frame in which it also inserts the message. When the destination device or LAN server reads the message, it resets the token to 0 so that the frame can be reused by any other device. The scheme is very efficient when traffic increases since all devices are afforded the same opportunity to use the shared network.

- ARCNET is a widely-installed local area network (LAN) technology that uses a token-bus scheme for managing line sharing among the workstations and other devices connected on the LAN
- ARCNET can use coaxial cable or fiber-optic lines.
- ARCNET is one of four major LAN technologies

Ethernet

Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol — a set of rules or common network language. As a data-link layer protocol in the TCP/IP stack, Ethernet describes how network devices can format and transmit data packets so other devices on the same local or campus area network segment can recognize, receive and process them. An Ethernet cable is the physical, encased wiring over which the data travels. Any device accessing a geographically localized network using a cable — i.e., with a wired rather than wireless connection — likely uses Ethernet — whether in a home, school, or office setting. From businesses to gamers, diverse end users depend on the benefits of Ethernet connectivity, including reliability and security.

Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions — whether from radio wave interference, physical barriers, or bandwidth hogs. It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling — making it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

How Ethernet works

The Institute of Electrical and Electronics Engineers Inc. (IEEE) specifies in the family of standards called IEEE 802.3 that the Ethernet protocol touches both Layer 1 — the physical layer — and Layer 2 — the data link layer — on the OSI network protocol model. Ethernet defines two units of transmission: packet and frame. The frame includes not just the payload of data being transmitted, but also:

- the physical media access control (MAC) addresses of both the sender and receiver;
- VLAN tagging and quality of service information; and
- error correction information to detect transmission problems.

Each frame is wrapped in a packet that contains several bytes of information to establish the connection and mark where the frame starts.

Engineers at Xerox first developed Ethernet in the 1970s. Ethernet initially ran over coaxial cables, while a typical Ethernet LAN today uses special grades of twisted pair cables or fiber optic cabling. Early Ethernet connected multiple devices into network segments through hubs — Layer 1 devices responsible for transporting network data — using either a daisy chain or star topology.

If two devices that share a hub try to transmit data at the same time, however, the packets can collide and create connectivity problems. To alleviate these digital traffic jams, the IEEE developed the **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** protocol, which allows devices to check whether a given line is in use before initiating new transmissions.

Later, Ethernet hubs largely gave way to network switches, their more sophisticated and modern counterparts. Because a hub cannot discriminate between points on a network segment, it can't send data directly from point A to point B. Instead, whenever a network device sends a transmission via an input port, the hub copies the data and distributes it to all the available output ports.