WIKIPEDIA

Networking hardware

Networking hardware, also known as **network equipment** or **computer networking devices**, are electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.[1] Units which are the last receiver or generate data are called hosts, end systems or data terminal equipment.

Contents

Range

Networking devices includes a broad range of equipment which can be classified as core network components which interconnect other network components, hybrid components which can be found in the core or border of a network and hardware or software components which typically sit on the connection point of different networks.

The most common kind of networking hardware today is a copper-based Ethernet adapter which is a standard inclusion on most modern computer systems. Wireless networking has become increasingly popular, especially for portable and handheld devices.

Other networking hardware used in computers includes data center equipment (such as file servers, database servers and storage areas), network services (such as DNS, DHCP, email, etc.) as well as devices which assure content delivery.

Taking a wider view, mobile phones, tablet computers and devices associated with the internet of things may also be considered networking hardware. As technology advances and IP-based networks are integrated into building infrastructure and household utilities, network hardware will become an ambiguous term owing to the vastly increasing number of network capable endpoints.

Specific devices

Network hardware can be classified by its location and role in the network.

Core

Core network components interconnect other network components.

- Gateway: an interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures.[2]
- Router: a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.[3] It works on OSI layer 3.[4]
- Switch: a device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.[5] It works on OSI layer 2.
- Bridge: a device that connects multiple network segments. It works on OSI layers 1 and 2.[6]
- Repeater: an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances.[7]
- Repeater hub: for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming.[1] A hub works at the physical layer (layer 1) of the OSI model.[8] Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision. Hubs are now largely obsolete, having been replaced by network switches except in very old installations or specialized applications.
- Wireless access point
- Structured cabling

Hybrid

Hybrid components can be found in the core or border of a network.

- Multilayer switch: a switch that, in addition to switching on OSI layer 2, provides functionality at higher protocol layers.
- Protocol converter: a hardware device that converts between two different types of transmission, for interoperation.[9]
- Bridge router (brouter): a device that works as a bridge and as a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would.[10]

Border

Hardware or software components which typically sit on the connection point of different networks (for example, between an internal network and an external network) include:

- Proxy server: computer network service which allows clients to make indirect network connections to other network services.[11]
- Firewall: a piece of hardware or software put on the network to prevent some communications forbidden by the network policy.[12] A firewall typically establishes a barrier between a trusted,

secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.[13]

- **Network address translator** (NAT): network service (provided as hardware or as software) that converts internal to external network addresses and vice versa.[14]
- **Residential gateway**: interface between a WAN connection to an internet service provider and the home network.

End stations

Other hardware devices used for establishing networks or dial-up connections include:

- **Network interface controller** (NIC): a device connecting a computer to a wire-based computer network.
- **Wireless network interface controller**: a device connecting the attached computer to a radio-based computer network.
- **Modem**: device that modulates an analog "carrier" signal (such as sound) to encode digital information, and that also demodulates such a carrier signal to decode the transmitted information. Used (for example) when a computer communicates with another computer over a telephone network.
- **ISDN terminal adapter** (TA): a specialized gateway for ISDN.
- **Line driver**: a device to increase transmission distance by amplifying the signal; used in base-band networks only.

See also

- Computer hardware
- Data circuit-terminating equipment
- List of networking hardware vendors
- Network simulation
- Node (networking)
- Telecommunications equipment

References

1. IEEE 802.3-2012 Clause 9.1
2. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=4990). *www.atis.org*. Retrieved 2016-02-12.
3. "The TCP/IP Guide - Overview Of Key Routing Protocol Concepts: Architectures, Protocol Types, Algorithms and Metrics" (http://www.tcpipguide.com/free/t_OverviewOfKeyRoutingProtocolConceptsArchitecturesP.htm). *www.tcpipguide.com*. Retrieved 2016-02-12.
4. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=1685). *www.atis.org*. Retrieved 2016-02-12.
5. "Hubs Versus Switches – Understand the tradeoffs" (http://www.ccontrols.com/pdf/Extv3n3.pdf) (PDF). *ccontrols.com*. 2002. Retrieved 2013-12-10.
6. E., Decker; A., Rijsinghani; K., McCloghrie; P., Langille. "Definitions of Managed Objects for Bridges" (https://tools.ietf.org/html/rfc1286). *tools.ietf.org*. Retrieved 2016-02-12.
7. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=1966). *www.atis.org*. Retrieved 2016-02-12.
8. Dean, Tamara (2010). *Network+ Guide to Networks*. Delmar. pp. 256–257.
9. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=2412). *www.atis.org*. Retrieved 2016-02-12.

10. "bridge router Definition from PC Magazine Encyclopedia" (https://www.pcmag.com/encyclopedia/term/38924/bridge-router). *www.pcmag.com*. Retrieved 2016-02-12.
11. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=8233). *www.atis.org*. Retrieved 2016-02-12.
12. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=5107). *www.atis.org*. Retrieved 2016-02-12.
13. Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND" (https://www.semanticscholar.org/paper/c56e4f9624a325b239fc5ac6a0f6c0911034aaf5). *Communications of the ACM*. **40** (5): 94. doi:10.1145/253769.253802 (https://doi.org/10.1145%2F253769.253802).
14. "ATIS Telecom Glossary" (http://www.atis.org/glossary/definition.aspx?id=9232). *www.atis.org*. Retrieved 2016-02-12.

External links

- USF Explanation of network hardware (http://fcit.usf.edu/network/chap3/chap3.htm)