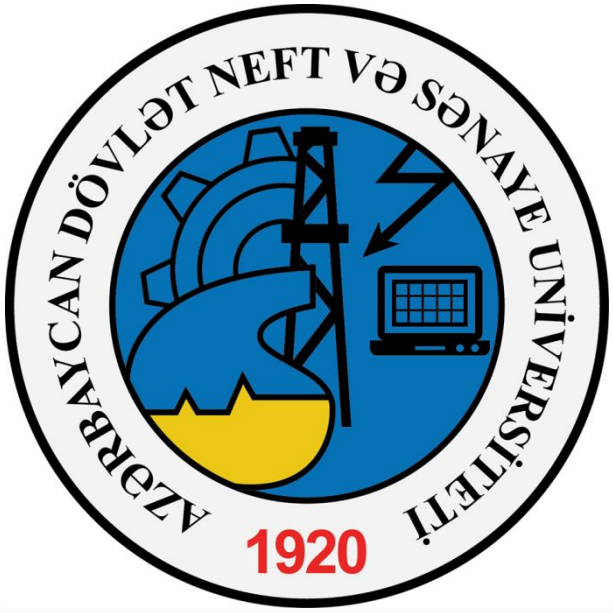
Network Programming



Network Programming is one of the central tasks when developing business applications.

The necessity in efficient and secure interaction between computers, which are in the same building or scattered all over the world, remains a basis for the success of many computer-based systems.

Introduction

Why network programming in .NET Framework?

One of the first technical decisions to be made whenever a new project is undertaken is what language to use. .NET Framework is a capable platform on which to develop almost any solution, and it offers substantial support for network programming.

.NET Framework comes with a new set of classes that facilitate solving networking problems.

Introduction

Why network programming in .NET Framework?

In fact, .NET Framework has more intrinsic support for networking than any other platform developed by Microsoft.

But .NET is not the be-all and end-all of network-programming applications. If your application runs over a UNIX-only infrastructure communicating via Java remote method invocation (RMI), then .NET is not the way to go.

Introduction

What can a network program do?

A network program is any application that uses a computer network to transfer information to and from other applications. Examples range from the ubiquitous Web browser such as Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc., or the program you use to receive your email, to the software that controls spacecraft at NASA.

Introduction

What can a network program do?

In case of a browser, every Web site you visit is actually files stored on a computer somewhere else on the Internet.

With your email program, you are communicating with a computer at your Internet Service Provider (ISP) or company email exchange, which is holding your email for you.

Introduction

What can a network program do?

Our course is largely concerned with creating network programs, not Web sites.

Although the capabilities of Web sites and network programs are quickly converging, it is important to understand the arguments for and against each system.

What can a network program do?

Users generally trust network applications, and as such these programs have much greater control over the computers on which they are running than a Web site has over the computers viewing it.

This makes it possible for a network application to manage files on the local computer, whereas a Web site, for all practical purposes, cannot do this.

Introduction

What can a network program do?

More importantly, from a networking perspective, an application has much greater control over how it can communicate with other computers on the Internet.

To give a simple example, a Web site cannot make the computer that is viewing it open a persistent network connection to another computer (except the computer from which the Web site was served).

What can a network program do?

This applies even when the Web site contains embedded content such as a Java applet or Flash movie.

There is one exception to this rule, when executable content (such as an ActiveX object) is included in a page. In this case, the page is capable of everything a network program could do, but most browsers and antivirus software will warn against or deny such executable content.

Let's introduce some of the basic networking concepts and protocols.

We start with an introduction to the hardware used in Local Area Networks (LANs), such as

- Hubs;
- Switches;
- Bridges;
- Routers.

Networking Concepts and Protocols

Then we take a look at the seven layers of the OSI model and their functionality.

Then we take a look at Transmission Control Protocol/Internet Protocol (TCP/IP) suite fits into the OSI layers.

After that, we cover the functionality of various network protocols.

Networking Concepts and Protocols

Outline

- The physical network
- The OSI seven-layer model
- Network protocols (including basic protocols, Internet protocols, and e-mail protocols)
- Sockets
- Domain name lookups
- The Internet
- .NET Remoting
- Messaging

Networking Concepts and Protocols

In essence, a network is a **group of computers or devices** connected by **communication links**.

In networking terms, every computer or device (printer, router, switch, and so on) connected to the network is called a **node**.

The Physical Network

Nodes are connected by links, which could be cables or wireless links (such as infrared or radio signals), and they can interact with any other node by transmitting messages over the network.

The Physical Network

We can differentiate networks according to their size:

- Local Area Network
- Wide Area Network
- Metropolitan Area Network

A **Local Area Network** (LAN), connects nodes over a limited area. The most commonly used LAN technology is the **Ethernet** network.

The Physical Network

A **Wide Area Network** (WAN) connects multiple LAN sites.

WAN technologies include

- Frame Relay
- Digital Data Service (DDT)
- Plain Old Telephony Service
- (Asymmetric) Digital Subscriber Line
- T1 line
- T3 line
- Integrated Services Digital Network
- X.25
- Asynchronous Transfer Mode (ATM)

The Physical Network

A **Metropolitan Area Network** (MAN) is very similar to a WAN insofar as it connects multiple LANs.

MANs use high-speed networks to connect the LANs of schools, governments, companies, and so on, by using fast connections to each site, such as fiber optics.

The Physical Network

Backbone

In discussions about networks, the term "backbone" is often used. A **backbone** is a high-speed network that connects slower networks. A company can use a backbone to connect slower LAN segments.

The Internet backbone is built of high-speed networks that carry WAN traffic. Your **Internet Service Provider (ISP)** connects either directly to the Internet backbone or to a larger provider that in turn connects directly to the Internet backbone.

The Physical Network

Ethernet

Let's look at the most common LAN network architecture – **Ethernet**.
Approximately 90% of devices attached to a LAN use Ethernet, which was initially developed by Xerox, Digital Equipment Corporation (DEC), and Intel.

Nowadays, Ethernet can support 100 Mbps and 1 Gbps lines. Many cabling technologies can be employed with Ethernet.

There is a standard naming convention that indicates the speed of the Ethernet network and the properties of the cable technology in use.

Such names start with a number indicating the maximum data transfer speed, followed by a word indicating the transmission technology supported, followed by a number indicating the maximum distance between nodes.

Ethernet

Ethernet Cables

Ethernet Standard	Speed	Typical Cable Type	Description
10Base5	10 Mbps	Coaxial copper	This was the original standard for Ethernet, a so-called thick-net cabling technology.
10BaseT	10 Mbps	Copper	10BaseT is a 10 Mbps network with twisted-pair cabling. A *twisted pair* is simply that—a pair of wires twisted around each other.
100BaseTX	100 Mbps	Copper	This is a 100 Mbps network with twisted pair cabling and full-duplex (X) capability. *Full duplex* means that data can pass in both directions simultaneously.
1000 BaseSX	1,000 Mbps	Multimode fiber	This is a 1,000 Mbps network with fiber optic cables. The "S" indicates the short wavelength (850 nm) of the laser.

Ethernet

Ethernet is a Carrier Sense Multiple Access/Collision Detect (CSMA/CD) network.

Multiple devices are connected to the same network, and all have simultaneous access.

When a message is sent, it is transported across the complete network as shown in Figure 1. The receiver is identified by its unique address, and only this node reads the message; all other nodes ignore it.

Ethernet (CSMA/CD)

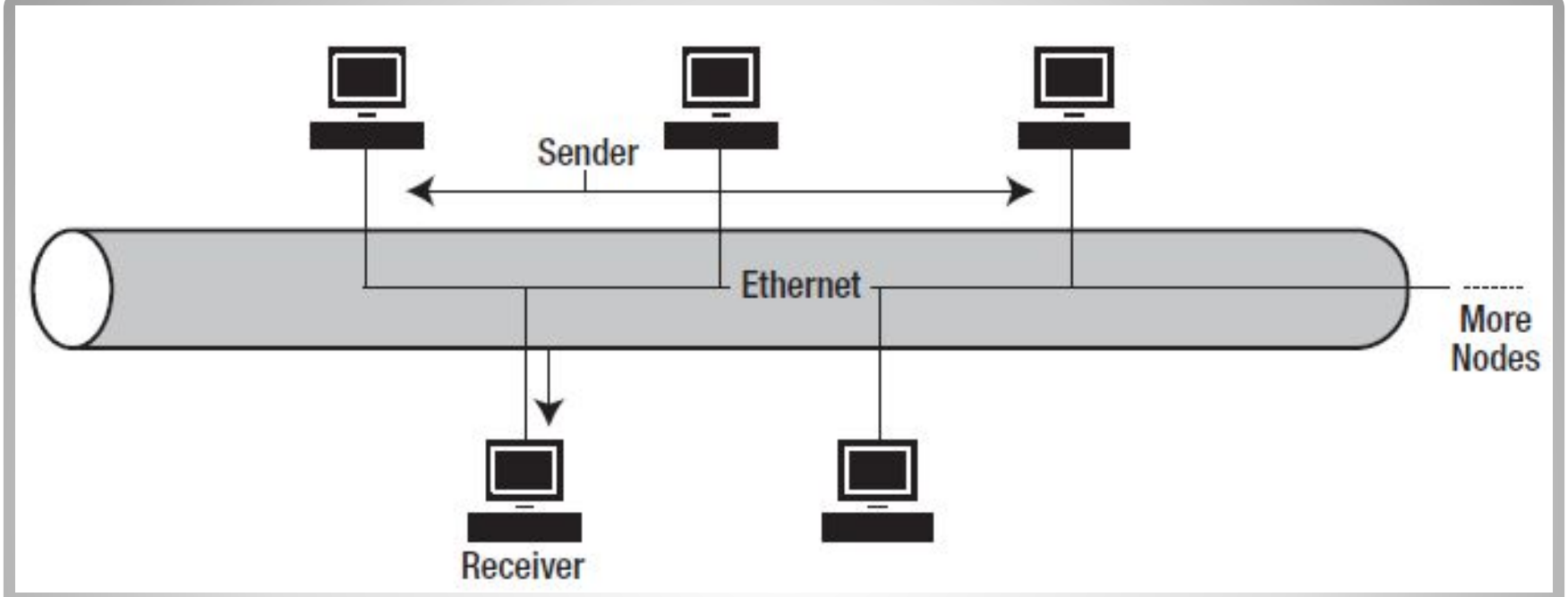


Figure 1.

Ethernet (CSMA/CD)

Ethernet (CSMA/CD)

There is a potential problem: more than one node could attempt to send a message at the same time, which could result in the packets becoming corrupted.

The solution used by Ethernet is that every node monitors the network and is thus aware of traffic. A node can start sending data only if no data is already being sent over the network. In short, this is the CSMA part of CSMA/CD.

There is still, however, the possibility that two nodes, after checking that the network is not already in use, start sending a packet at exactly the same time on the same network cable. This would cause a collision between the two packets, resulting in corrupted data. Both senders are aware of the corrupted packet because they still listen to the network while sending data and thus detect the collision.
This is the CD in CSMA/CD.

Ethernet (CSMA/CD)

Both nodes then halt their transmissions immediately and wait a random time interval before checking the network again to see if it is free to resend the packet.

Ethernet (CSMA/CD)

Every node on the local network uses a **Media Access Control** (MAC) address for unique identification.
This address is defined by the **Network Interface Card** (NIC). A network packet is sent across the network, but if the NIC does not identify its host as a receiver, it ignores the packet. Incidentally, if the packet has the same destination address as the node that is listening, the message is dealt with.

Ethernet (CSMA/CD)

Token Ring (IEEE 802.5) is a network architecture developed by IBM. The nodes are connected in a ring, as shown in Figure 2.

Every node has guaranteed access to the network in a predefined order. A token circulates around the network ring, and only the node that holds the token can send a message.

Token Ring is more expensive and more difficult to implement than Ethernet.

Other Network Architectures

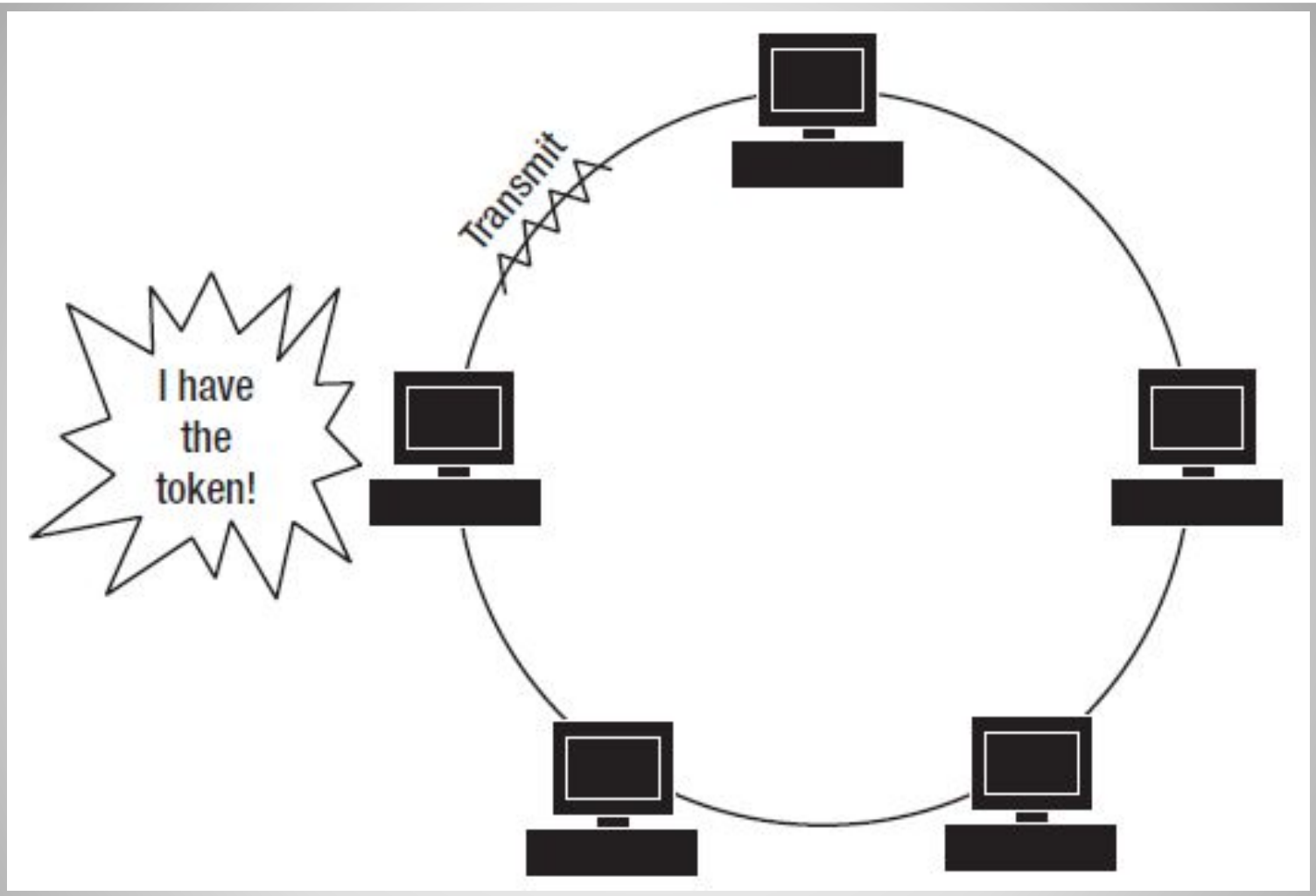


Figure 2

Other Network Architectures

AppleTalk is a LAN protocol developed by Apple for Apple Macintosh networks that has been quite popular in schools, factories, and so on.

Asynchronous Transfer Mode (ATM) is another protocol that can be found in LANs. It supports fast network-switching and has a guaranteed Quality of Service (QOS), but because the cost of ATM network cards is considerably high, ATM is a niche player in the LAN market.

Other Network Architectures

Physical Components

An important aspect of understanding the network is knowing the hardware components.

The major components of a LAN are:

- **NIC**
- **Hub**
- **Switch**
- **Router**

A **NIC** is the adapter card used to connect a device to the LAN. It allows you to send messages to and receive messages from the network. A NIC has a unique MAC address that provides a unique identification of each device.

The MAC address is a 12-byte hexadecimal number uniquely assigned to an Ethernet network card. Usually the MAC address is not changed.

Network Interface Card (NIC)

You can find the MAC address of a Windows machine using the command-line utility **ipconfig** in a DOS/CMD prompt with the **/all** switch. Figure 3 shows the output produced on a machine where the MAC address is A8-20-66-2C-8F-8C.

The first part of this number, A8-20-66, is assigned to the manufacturer of the network card; the manufacturer uses the remainder to create a unique MAC address.

Network Interface Card (NIC)

http://www.adminsub.net/mac-address-finder

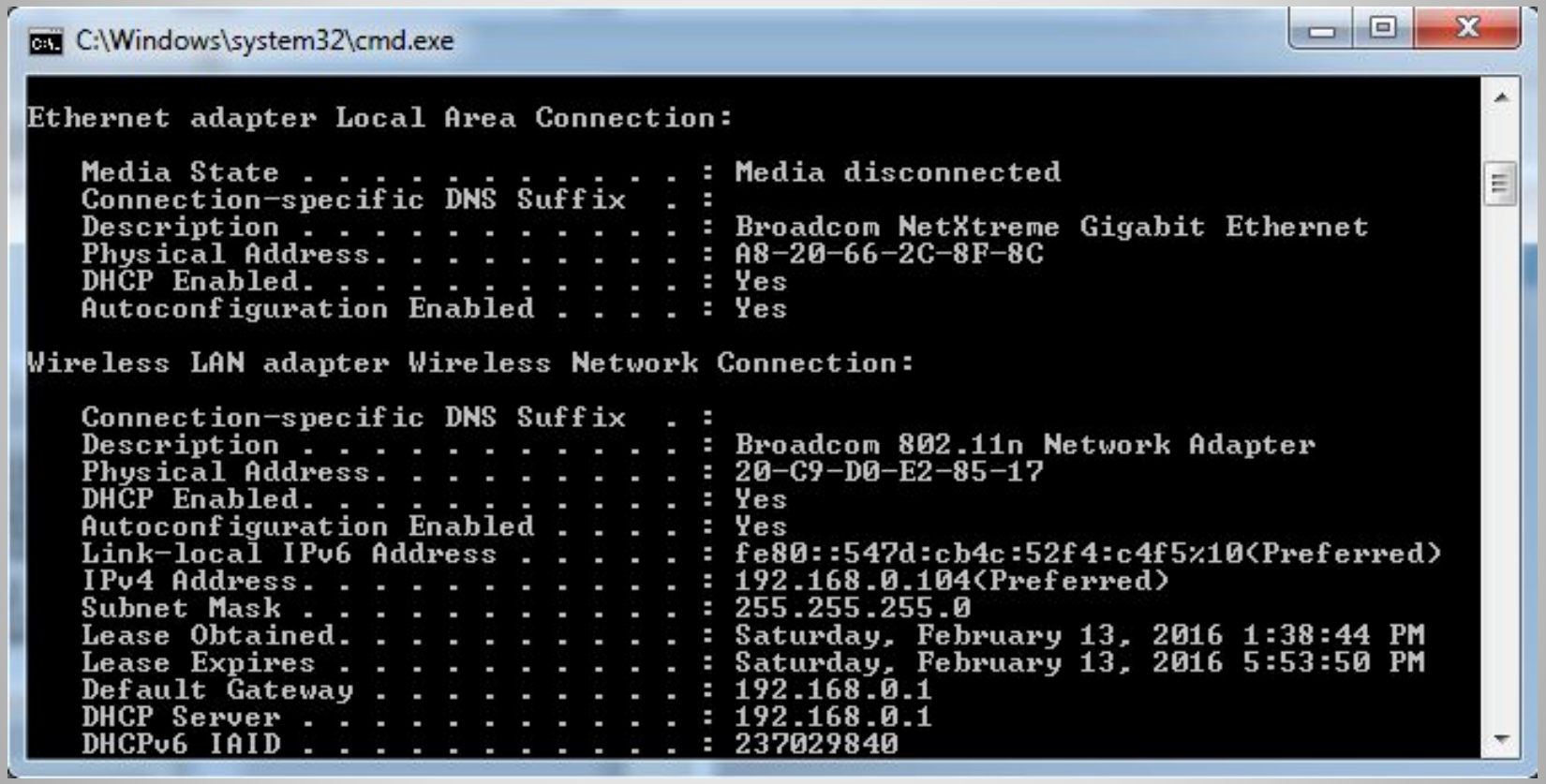


Figure 3

Network Interface Card (NIC)

Multiple devices can easily be connected with the help of a **hub** (see Figure 4).
A hub is a connectivity device that attaches multiple devices to a LAN.

Each device typically connects via an **Unshielded Twisted Pair** (UTP) cable to a port on the hub.

You may have already heard about the **Registered Jack-45** (RJ-45) connector.

Hub

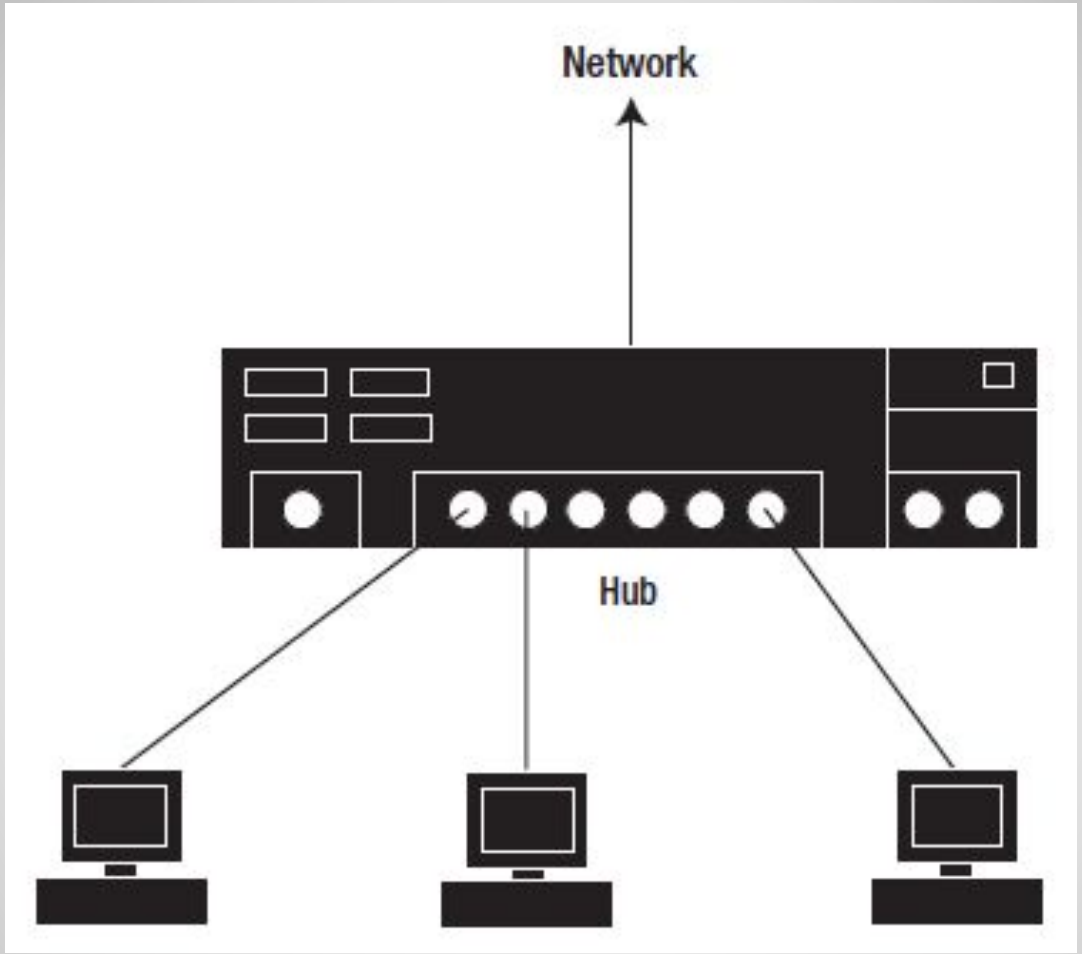


Figure 4

Hub

The hub acts as a repeater as it forwards every message from each port to every other port, and to the network.

A hub is a fairly simple element of a network, operating at the physical network layer to retransmit data without any processing.

This makes a hub easy to install and manage, as it doesn't require any special configuration.

Hub

Switches separate networks into segments. Compared to a hub, a switch is a more intelligent device. A switch stores the MAC addresses of devices that are connected to its ports in lookup tables. These lookup tables allow the switch to filter network messages and, unlike the hub, avoid forwarding messages to every port. This eliminates possible collisions, and a better performing network can be achieved.

Switch

As shown in Figure 5, a switch can be used to connect hubs at a site.
If node A sends a message to node B, the switch doesn't forward the message to segment 2 because the switch knows that node B is on the same portion of the network as node A. However, if node A sends a message to node C, the message is forwarded from segment 1 to segment 2.

Switch

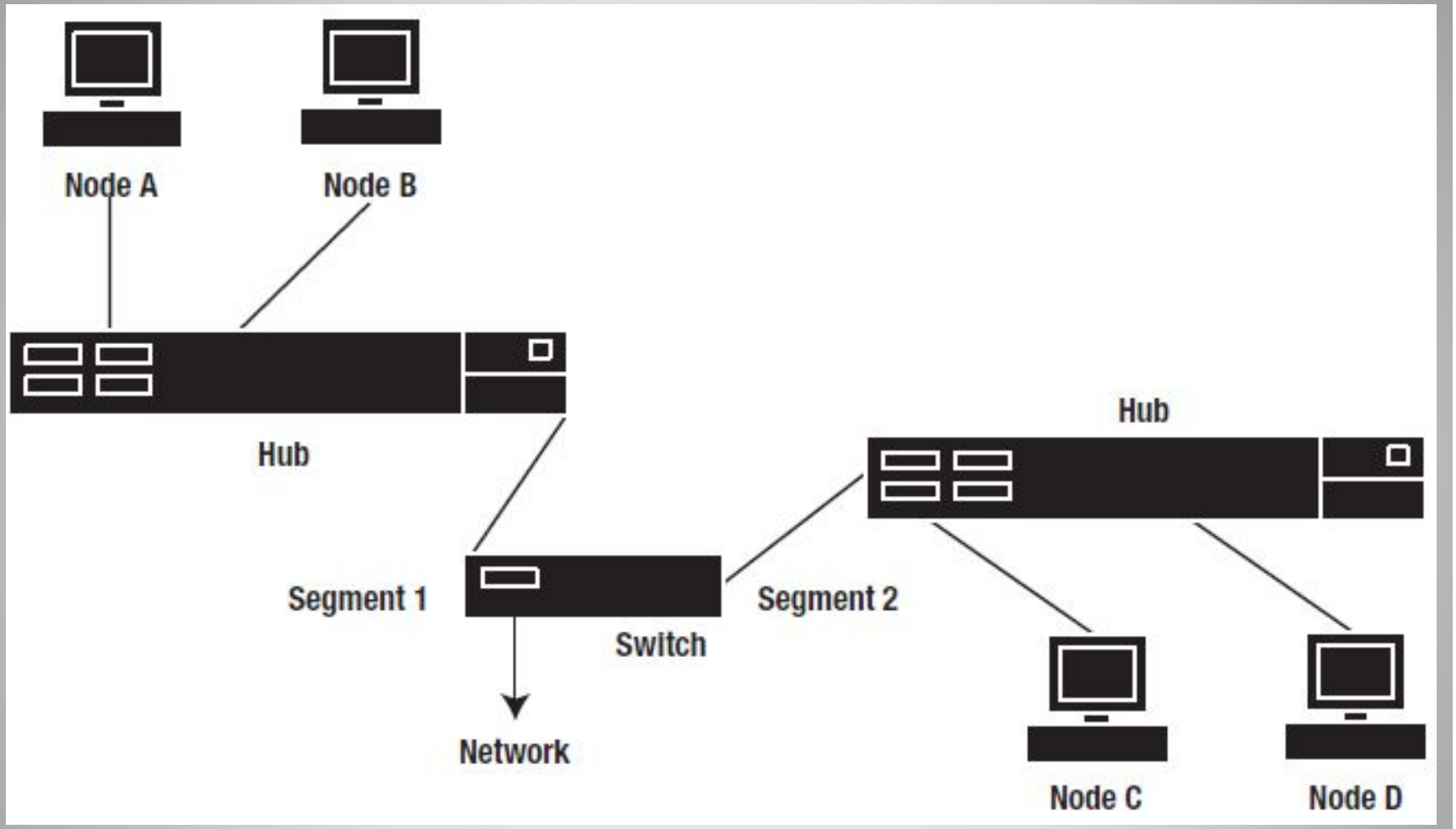


Figure 5

Switch

This sort of arrangement was popular in the early days, when hubs were much cheaper than switches.

But it is less common now, as the price of switches has dropped to pretty much the same as hubs.

Because of the enhanced network performance from collision reduction, new networks often use switches in place of hubs, and end users are connected directly to a switch.

Switch

A router is an intermediary network device that connects multiple physical networks. With many hosts, it can be useful to split a LAN into separate portions, or subnets.
The advantages of subnets are as follows:

- Performance is improved by reducing broadcasts, which is when a message is sent to all nodes in a network. With subnets, a message is sent only to the nodes in the appropriate subnet.

Router

- The capability of restricting users to particular subnets offers security benefits.
- Smaller subnets are easier to manage than one large network.
- Subnets allow a single network to span several locations.

Figure 6 shows how routers might connect several subnets.

Router

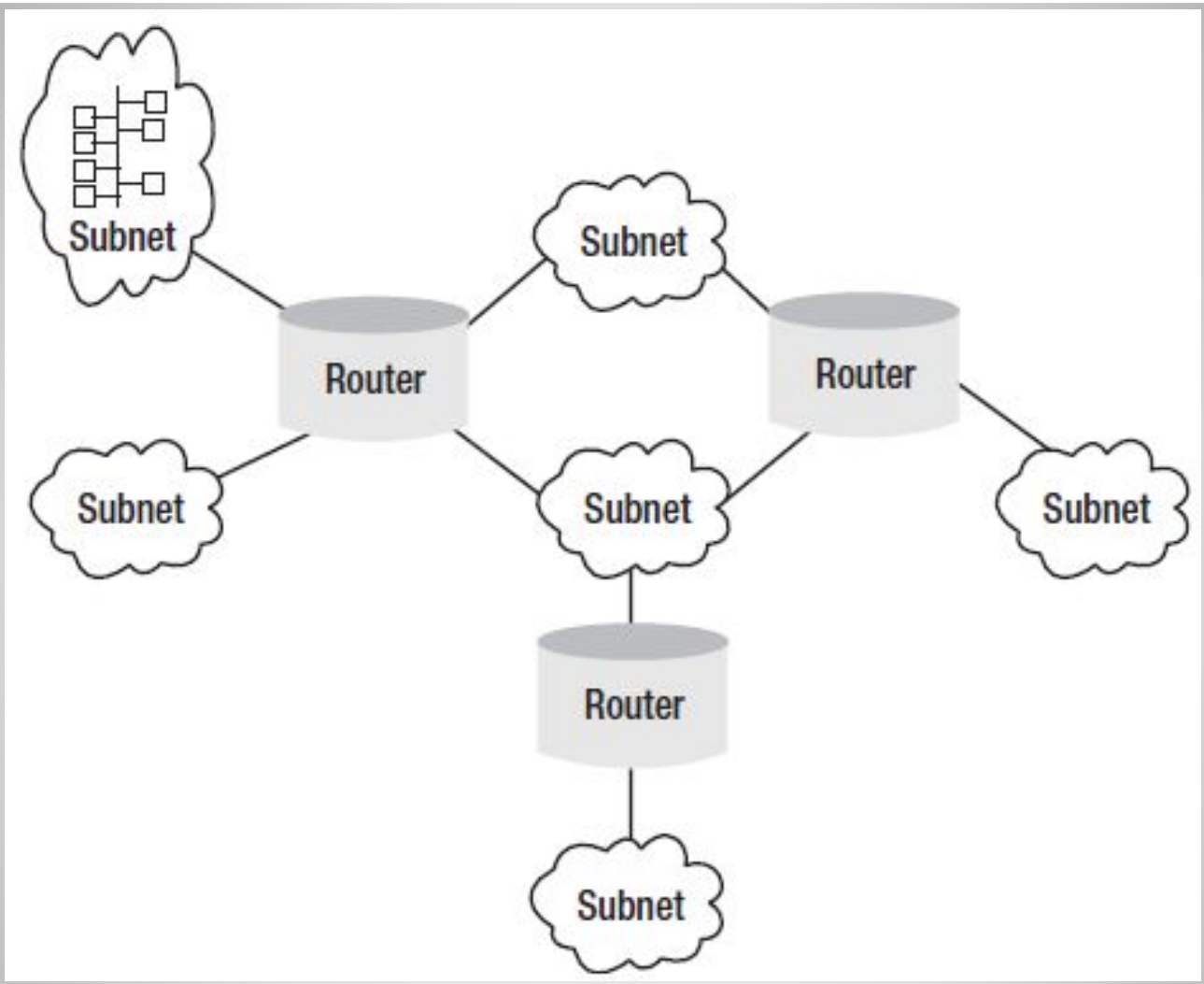


Figure 6

Router

Note

If you're using a router in a LAN, be aware that a router isn't as fast as a switch. The router must apply more processing to messages than a switch needs to, and consequently it takes a little more time before passing on packets.

Router

Routers are not only used within LANs, but also have an important place in WANs where they connect different network lines.

The router receives a message and forwards it to the destination using the last known best path to that destination, as illustrated in Figure 7.

Router

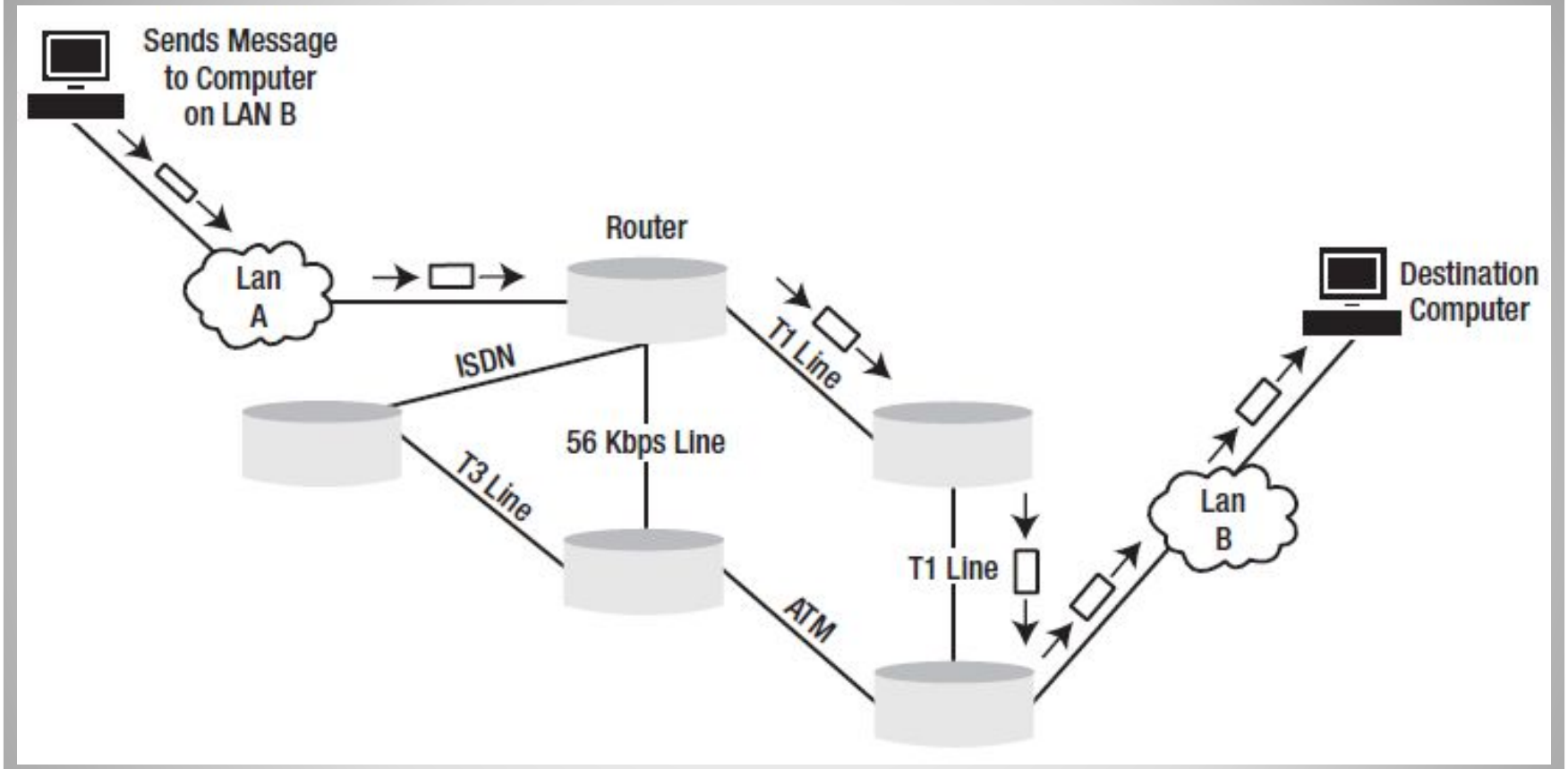


Figure 7

Router

A router holds a routing table that lists the ways particular networks can be reached. There will often be several different routes from one network to another, but one of these will be the best, and it is the best one that is described in the routing table. Routers communicate using routing protocols that discover other routers on the network and support the exchange of information about networks attached to each router.

Router

The information that a router collates about the paths between networks is known as **router metrics**, and it may include information such as packet loss and transmission time.

The information used to produce the metrics depends on the routing protocol.

Router

Distance vector routing protocols:
Routing Information Protocol
and
Interior Gateway Routing Protocol
use a hop count, which indicates the number of routers that are passed through on the way to the target network.
These protocols prefer paths with fewer routers, regardless of their speed and reliability.

Router

Link state routing protocols:

The best path calculation of the Open Shortest Path First (OSPF) routing protocol

and

Border Gateway Protocol (BGP)

takes into account multiple factors such as the speed, reliability, and even cost of a path.

Hybrid routing protocols:

Hybrid routing protocols use a combination of distance vector and link state calculation.

With the TCP/IP configuration, you can set up a **default gateway**. This is the **Internet Protocol** (IP) address of the router port that the machine's subnet is connected to. This router is used when a host outside the subnet needs to be contacted.

You can see the local routing table on a Windows system by entering **route print** at the command line.

This command displays the gateways that will be used for each network connection.

Finding the Route

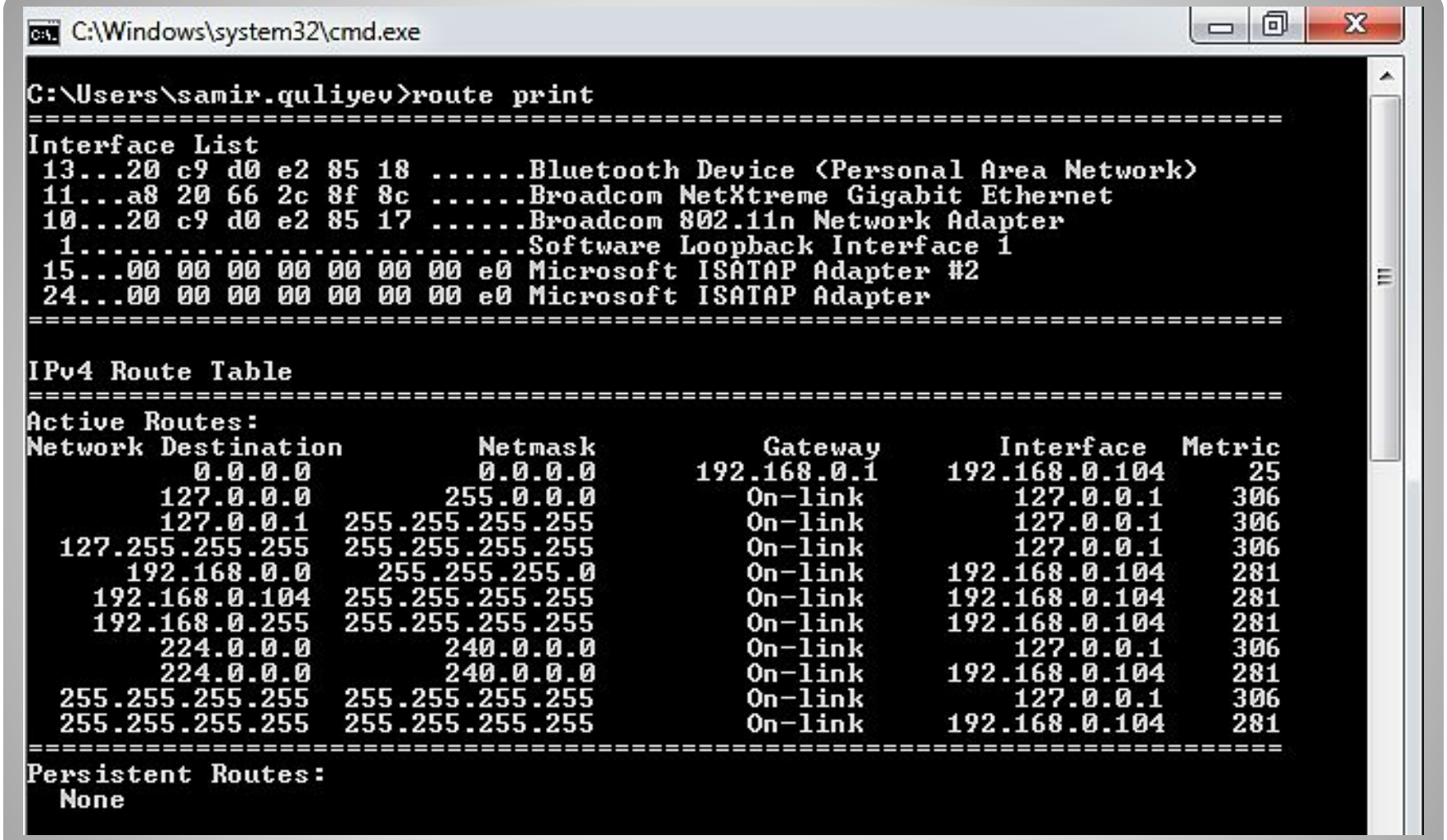


Figure 8. route print command

Finding the Route

Another useful command is **tracert**. It allows you to examine the path used to reach a destination.

'tracert www.w3.org' in Figure 9 shows all routers that were used to reach the specified host. The command also displays the time needed to reach the next hop.

This command is very helpful if a host cannot be reached, which could indicate that some network in between is down or not available.

Finding the Route

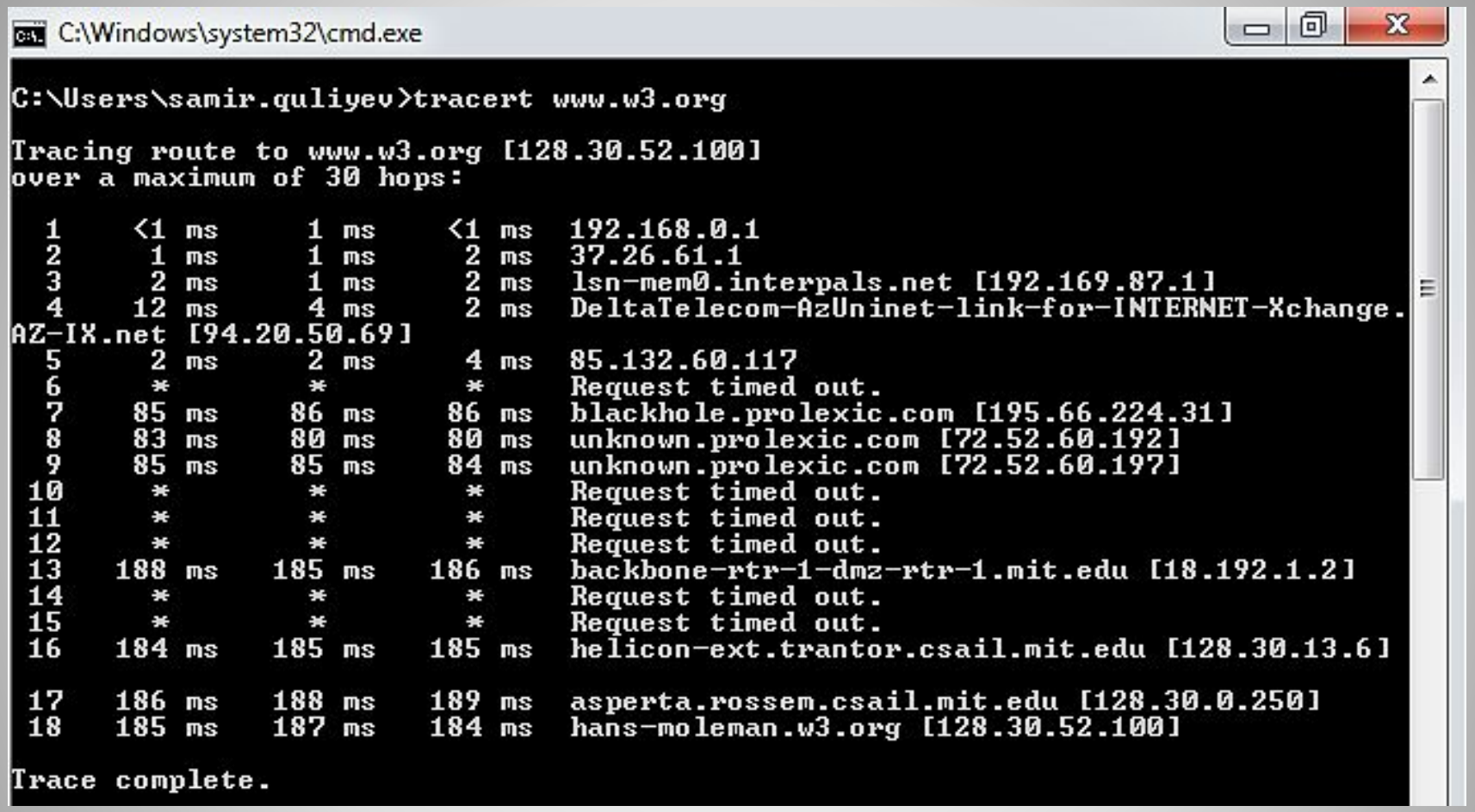
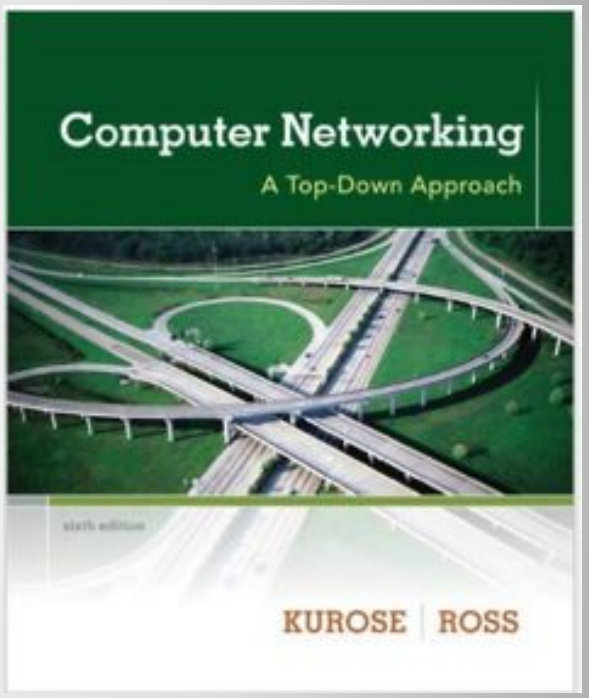


Figure 9. tracert command in action

Finding the Route

References

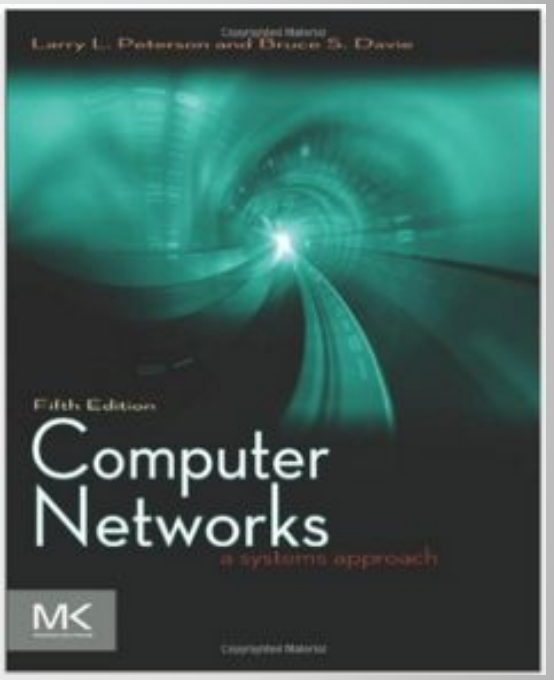
Computer Networking: A Top-Down Approach (6th Edition)
[James F. Kurose]
[Keith W. Ross]
2012



References

Computer Networks, Fifth Edition: A Systems Approach

[Larry L. Peterson]
[Bruce S. Davie]
2011



References

Компьютерные сети. Принципы, технологии, протоколы.
[Виктор Олифер]
[Наталия Олифер]
2016