Unit 4 The Introduction of Computer Network

Lesson 7 The Classification of Computer Networks

Computer networking is the practice of interfacing two or more computing devices with each other for the purpose of sharing data. Computer networks are built with a combination of hardware and software.Computer networks can be categorized in several different ways.

One approach defines the type of network according to the geographic area it spans. Local area networks (LANs), for example, typically span a single home, school, or small office building, whereas wide area networks (WANs), reach across cities, states, or even across the world. The Internet is the world's largest public WAN. The popularity of computer networks sharply increased with the creation of the World Wide Web (WWW) in the 1990s. Public Web sites, peer to peer (P2P) file sharing systems, and various other services run on Internet servers across the world.

Computer networks also differ in their design approach. The two basic forms of network design are called client/server and peer-to-peer. Client-server networks feature centralized server computers that store email, Web pages, files and or applications accessed by client computers and other client devices. On a peer-to-peer network, conversely, all devices tend to support the same functions.

Client-server networks are much more common in business and peer-to-peer networks more common in homes.

Communication languages used by computer devices are called network protocols.Yet another way to classify computer networks is the set of protocols they support. Networks often implement multiple protocols with each supporting specific applications. Popular protocols include TCP/IP - the one most commonly found on the Internet and in home networks.

Many of the same protocols like TCP/IP work in both wired and wireless networks. Networks with Ethernet cables predominated in businesses, schools, and homes for several decades. More recently, however, wireless technologies like Wi-Fi have emerged as the preferred option for building new computer networks, in part to support smartphones and the other new kinds of wireless gadgets that have triggered the rise of mobile networking.

Lesson 8 Network Topology

Network topology is the arrangement of the various elements (links, nodes and so on.) of a communication network.

Network topology is the topological structure of a network and may be depicted physically or logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

An example is a local area network (LAN). Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection. Network Topology can be classificed in several different ways.

1. BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

2.RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

3.STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

4.TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

5.HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

参考译文：

第 7 课 计算机网络的分类

计算机联网是为了共享数据而将两个或更多计算设备连接在一起的实践。计算机网络是由硬件和软件结合而成的，计算机网络可以分为几种不同的方式。

一种方法根据其跨越的地理区域定义网络类型。局域网（LAN），例如，通常跨越一个家庭，学校，或小型办公楼，而广域网（WAN），跨越城市、国家，乃至整个世界。互联网是世界上最大的公共广域网。随着 20 世纪 90 年代万维网（WWW）的出现，计算机网络的普及迅速增加，世界各地的因特网服务器上都有公共网站、对等（P2P）文件共享系统和各种其他服务。

计算机网络的设计方法也各不相同。网络设计的两种基本形式称为客户机/服务器网络和对等网络。客户机-服务器网络具有集中服务器计算机，用于存储客户端计算机和其他客户端设备访问的电子邮件、网页、文件和应用程序。相反，在对等网络上，所有设备都倾向于支持相同的功能。客户机-服务器网络在商业业务中常见而对等网络在家庭中更为普遍。

计算机设备使用的通信语言称为网络协议，而对计算机网络进行分类的另一种方法是它们支持的一组协议。网络通常实现多个协议，每个协议都支持特定的应用程序。流行的协议包括 TCP/IP，这是互联网上和家庭网络中最常见的协议之一。

许多相同的协议，如 TCP/IP，都在有线和无线网络中工作。几十年来，以太网电缆网络在商业、学校和家庭中占据了主导地位。然而，最近，Wi-Fi 等无线技术已经成为建立新计算机网络的首选方案，部分是为了支持智能手机和其他引发移动网络兴起的新型无线设备。

第 8 课 网络拓扑结构

网络拓扑是通信网络中各种元素（链路、节点等）的排列。

网络拓扑是网络的拓扑结构，可以在物理上或逻辑上加以描述。物理拓扑是网络各个组成部分的位置，包括设备位置和电缆安装，逻辑拓扑说明数据如何在网络中流动。节点间的距离、物理互连、传输速率或信号类型可能在两个网络之间有所不同，但它们的拓扑结构可能是相同的。

一个例子是局域网（LAN）。局域网中的任何给定节点都有一个或多个与网络中其他设备的物理链路；图形化地绘制这些链接，形成一个可以用来描述网络物理拓扑的几何图形。相反，映射组件之间的数据流决定了网络的逻辑拓扑。

网络拓扑是网络安排的示意性描述，通过连接线连接各种节点（发送方和接收方）。网络拓扑结构可分几种不同的方式。

1.总线拓扑

总线拓扑是一种网络类型，每一台计算机和网络设备都连接到一根电缆上。当它恰好有两个端点时，就称为线性总线拓扑。

2.环形拓扑

它被称为环形拓扑，因为当每个计算机连接到另一台计算机时，它形成一个环，最后一个连接到第一个计算机。每个设备正好有两个邻居。

3.星形拓扑

在这种拓扑结构中，所有的计算机都通过电缆连接到一个集线器。这个集线器是中央节点，所有其他节点都连接到中心节点。

4.树形拓扑

它有根节点，所有其他节点都连接到它，形成一个层次结构。它也被称为层次拓扑。它至少应该有三级层次结构。

5.混合拓扑

这是两种不同类型的拓扑，它们是两个或多个拓扑的混合体。例如，如果在一个部门使用环形拓扑，另一个使用星形拓扑，那么连接这些拓扑将产生混合拓扑（环形拓扑和星形拓扑）。

1. New Words

interface[ˈɪntəfeɪs] 接口

categorize[ˈkætəgəraɪz]把……分类

geographic [ˌdʒi:ə'græfɪk]地理的

span [spæn]测量，跨度

sharp [ʃɑ:p] 锋利的，尖锐的

centralize [ˈsentrəlaɪz]集中

cable[ˈkeɪbl]电缆

predominate [prɪˈdɒmɪneɪt] 占支配地位

gadget[ˈgædʒɪt]小配件

trigger[ˈtrɪgə(r)] 触发器

depict[dɪˈpɪkt] 描述，描绘

topology [tə'pɒlədʒɪ]拓扑结构

illustrate[ˈɪləstreɪt] 说明

identical [aɪˈdentɪkl]同一的，相同的

endpoint ['endpɔɪt]端点，结点

ring [rɪŋ]环形，戒指

neighbour['neɪbə(r)] 邻居

hub [hʌb]中心，集线器

hierarchy [ˈhaɪərɑ:ki]层次

hybrid [ˈhaɪbrɪd]混合的

2.Techmical Terms

Local area network (LAN)局域网

Wide area network (WAN)广域网

World Wide Web (WWW)万维网

Client-server network 客户服务器网络

peer to peer network 点对点网络

BUS Topology 总线拓扑

RING Topology 环形拓扑

TREE Topology 树形拓扑

STAR Topology 星形拓扑

3. Self-study Space

① TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

②The basic structure of all networks consists of a main computer or *server*, along with connected machines known as *clients*. The server typically has two Ethernet network interface cards (NICs) installed and software that can support the network. In the case of a simple home wireless LAN, a desktop might be the server while a laptop could be the client.

③Once the wireless LAN has been set up on the server and client, the machines can communicate by sending and receiving data via radio waves. This makes a wireless LAN very convenient because the client can remain mobile anywhere within the broadcasting range of the network. One can work on a laptop in any room in the house -- even the backyard in most cases -- and still share the network connection from the server.

4.Disscussion

(1) What is the difference of LAN and WAN?

(2)How does TCP/IP work?

(3)What are the advantages of a star topology?

(4)What is the difference of bus topology and ring topology?

5. Exercises

(1)Please translate the following words into Chinese.

①Once the wireless LAN has been set up on the server and client, the machines can communicate by sending and receiving data via radio waves. This makes a wireless LAN very convenient because the client can remain mobile anywhere within the broadcasting range of the network. One can work on a laptop in any room in the house -- even the backyard in most cases -- and still share the network connection from the server.

②Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central hub which acts as a conduit to transmit messages. In star topology, every host is connected to a central hub.[1] A star network is an implementation of a spoke–hub distribution paradigm in computer networks.

(2)Please translate the following sentences into English.

①广域网(简称 WAN)是一种跨地区的数据通讯网络,通常包含一个国家或地区。广域网通常由两个或多个局域网组成。广域网等于是把局域网连接起来成为更大的网络。一个国家应该算是一个广域网，而超过这个范围，将许多国家级的广域网结合在一起，就形成了全球互联的“因特网”。

②环形拓扑结构是一个像环一样的闭合链路，它是由许多中继器和通过中继器连接到链路上的节点连接而成。环形网络的一个典型代表是令牌环局域网，它的传输速率为4Mb/s或16 Mb/s。这种网络结构最早由IBM推出，但已被众多厂商所采用。

6. Reading Materials

Reading Material 7 Network Security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

Reading Material 8 Common Types of Network Attacks

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

1.Eavesdropping

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

2.Data Modification

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

3.Identity Spoofing (IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

4.Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

①Obtain lists of valid user and computer names and network information.

②Modify server and network configurations, including access controls and routing tables.

③Modify, reroute, or delete your data.

5.Denial-of-Service Attack

Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

①Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.

②Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.

③Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.

④Block traffic, which results in a loss of access to network resources by authorized users.

6.Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

7.Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

8.Sniffer Attack

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

① Analyze your network and gain information to eventually cause your network to crash or to become corrupted.

②Read your communications.

9.Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

①Read, add, delete, or modify your data or operating system.

②Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.

③Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.

④ Abnormally terminate your data applications or operating systems.

⑤Disable other security controls to enable future attacks.