Module 1

TCP/IP internet

TCP/IP it can be used to communicate across any set of interconnected networks. For example, TCP/IP can be used to interconnect a set of networks within a single building, within a physical campus, or among a set of campuses.

Internet Services

Application Level Internet Services

- World Wide Web
- Cloud Access And Remote Desktop
- File Transfer
- Electronic Mail (email)
- Voice And Video Services

Network-Level Internet Services

- Connectionless Packet Delivery Service
- Reliable Stream Transport Service

Internetworking Concept and Architectural Model

Internetworking is the technology that makes it possible to interconnect many disparate physical networks with diverse underlying hardware technologies and make them function as a coordinated unit. The internetworking / Internet technology hides the details of network hardware and permits computers to communicate independent of their physical network connections. When we speak of interworking technology, we speak of the internet technology in particular.

There are two methods for providing interconnectivity for between communication application programs on different machines. One method is ***Application level interconnection*** in which we use application level programs running on each machine that could understand the details of the network connections for the machines and interoperates with the application programs across those connections. Eventhough this method hides the hardware details between source and destination, such an approach to network interconnection has various drawbacks since it requires to change the application software every time when the network functionalities are changes. Also as the network grows larger, it is impossible to code the application program for each interconnected applications.

The alternative approach to this is the ***Network-level interconnection*** that provides a mechanism that delivers packets from their original source to their ultimate destination in real time. Such an approach of universal network-level interconnection called the internetworking has the following features. It carries the data as small packets of data that could be easily mapped on the underlying network hardware. It separates the data communication activities from application programs, permitting machines to handle network traffic without understanding the application that use it. It keeps the system flexible making it possible to build general purpose network protocols. It allows network administrators to add new network technologies by modifying or adding a single piece of new network level software, while application programs remain unchanged. It detaches the notions of communication from the details of network technology and hides low level details from the user. It enables to build unified cooperative interconnection of computer networks that supports a universal communication service and interconnection scheme called the internetwork or the Internet with each machine on the internet having a specific address.

Internet Architecture

Computers that interconnect two networks and pass packets from one to the other are called internet routers or IP routers.

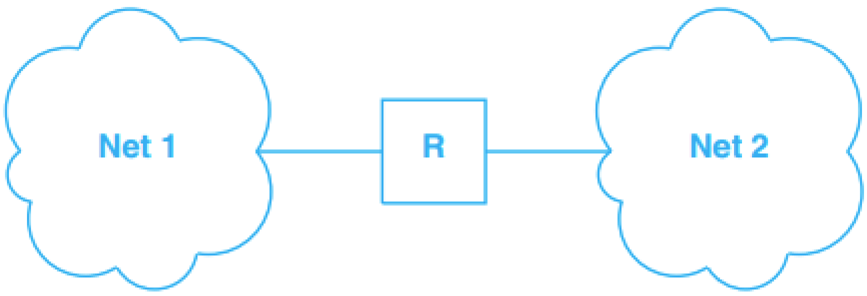


Figure 3.2 Two physical networks interconnected by an IP router, *R*.

Router R connects to both ***network 1*** *and* ***network 2***. For R to act as a router, it must capture packets on network 1 that are bound for machines on network 2 and transfer them. Similarly, R must capture packets on network 2 that are destined for machines on network 1 and transfer them.

Interconnection Of Multiple Networks With IP Routers.

A realistic internet will include multiple networks and routers. In such a case, each router needs to know about networks beyond the networks to which it connects directly.

Figure 3.3 Three networks interconnected by two routers.

Router R1 must transfer from network 1 to network 2 all packets destined for computers on either network 2 or network 3. Similarly, router R2 must transfer packets from network 3 that are destined for either network 2 or network 1.

The important point is that a router must handle packets for networks to which the router does not attach.

In a TCP/IP internet, special computer systems called IP routers provide interconnections among physical networks.

Routers use the destination network, not the destination computer, when forwarding a packet.

Protocol Layering

The structure of the software found in hosts and routers that carries out network communication.

The Need For Multiple Protocols

Problems that can arise when computers communicate over a data network

- Hardware Failure
- Network Congestion
- Packet Delay Or Packet Loss
- Data Corruption

- Data Duplication Or Inverted Arrivals

The problems seem overwhelming. It is impossible to write a single protocol specification that will handle them all.

The Conceptual Layers Of Protocol Software

Each layer takes responsibility for handling one part of the problem.

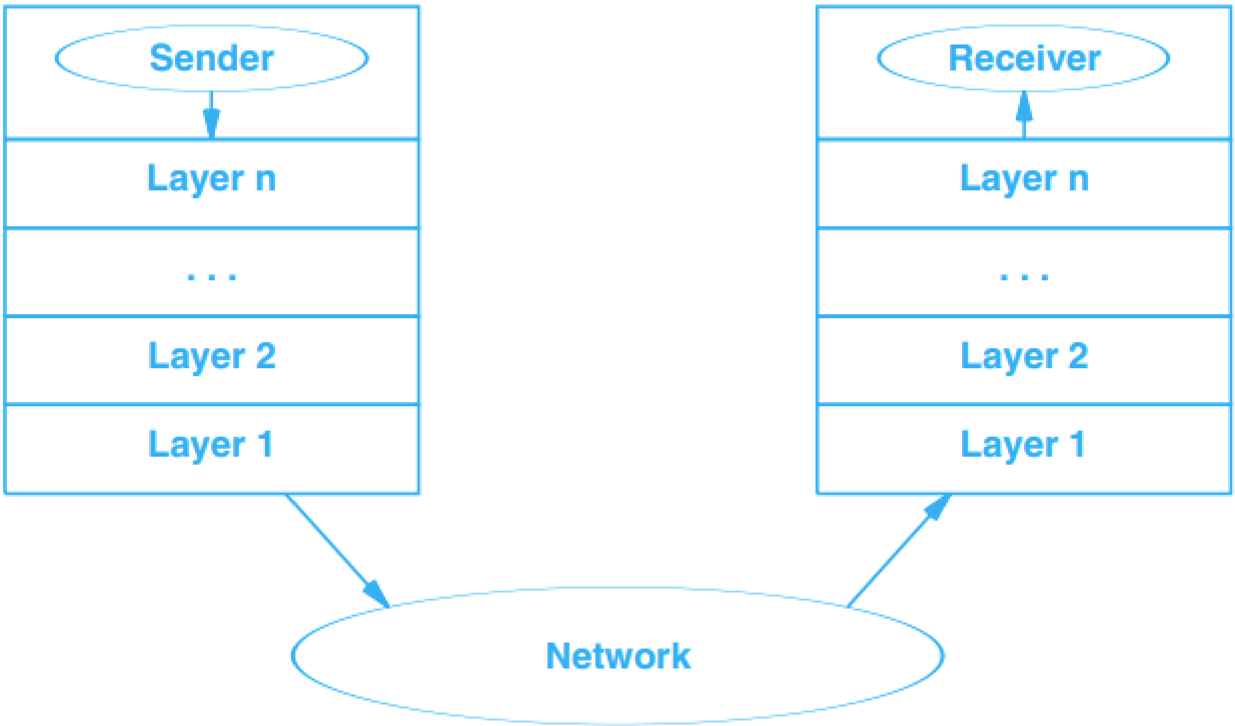


Figure 4.1 The conceptual organization of protocol software in layers.

Sending a message from an application on one computer to an application on another means transferring the message down through successive layers of protocol software on the sender's machine, forwarding the message across the network, and transferring the message up through successive layers of protocol software on the receiver's machine.

Functionality Of The Layers

Two interrelated questions arise:

how many layers should be created, and what functionality should reside in each layer?

The questions are not easy to answer for several reasons.

First, given a set of goals and constraints governing a particular communication problem, it is possible to choose an organization that will optimize protocol software for that problem.

Second, even when considering general network-level services such as reliable transport, it is possible to choose from among fundamentally distinct approaches to solving the problem.

Third, the design of network (or internet) architecture and the organization 50 Protocol Layering Chap. 4 of the protocol software are interrelated; one cannot be designed without the other

ISO 7-Layer Reference Model

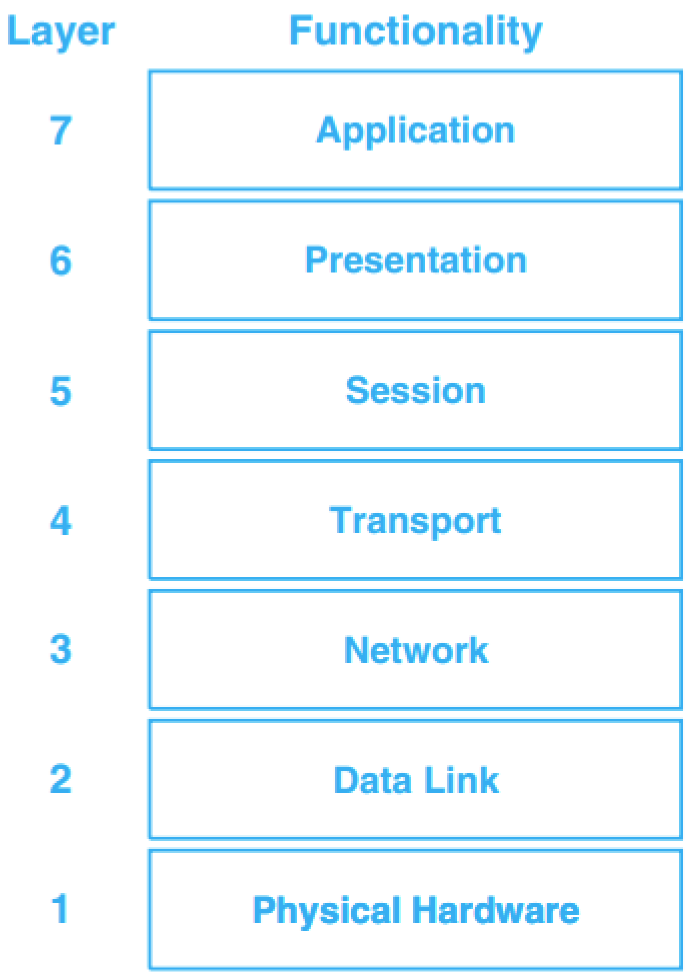


Figure 4.2 The ISO 7-layer reference model. Because it was designed to describe protocols in a single network, the model does not describe the organization of TCP/IP protocols well.

The TCP/IP 5-Layer Reference Model

Unlike the ISO model, which was defined by committees before protocols were implemented, the Internet 5-layer reference model was formalized after protocols had been designed and tested.

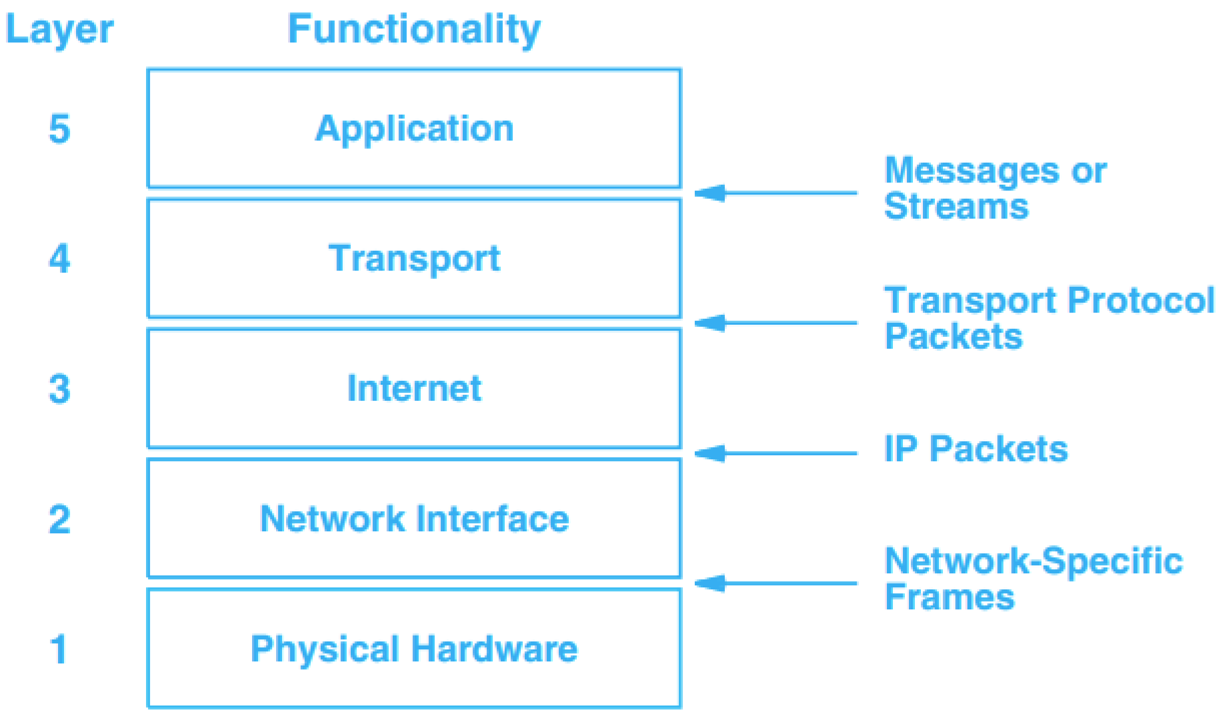


Figure 4.3 The 5-layer TCP/IP reference model showing the form of objects passed between layers.

Not so important

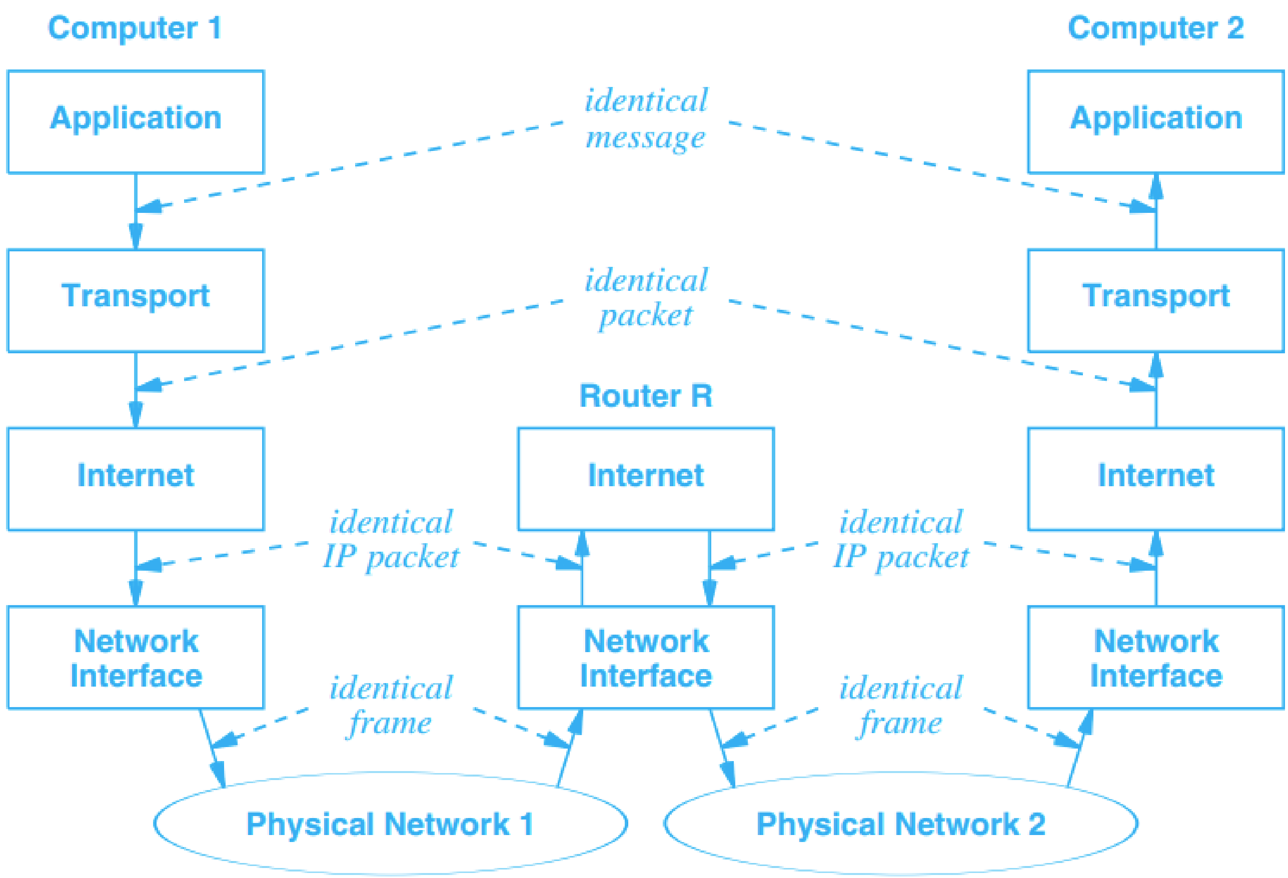
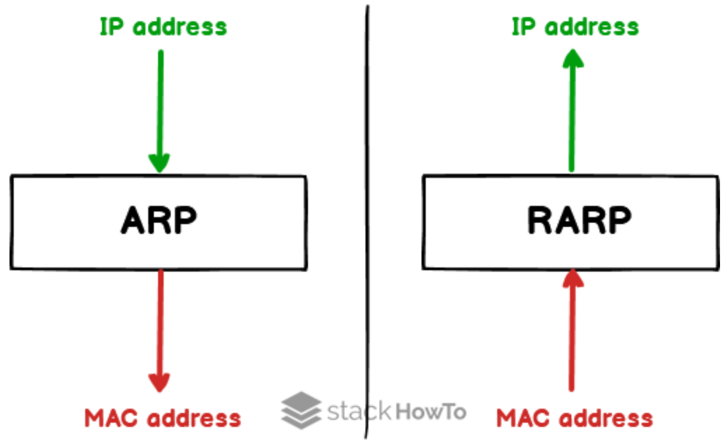


Figure 4.7 The layering principle when a message passes from an application on one computer, through a router, and is delivered to an application on another computer.

Mapping Internet addresses to physical addresses (ARP)



ARP

Two machines on a given physical network can communicate only if they know each other's physical network address.

Address Resolution Protocol (ARP) is a network-specific standard protocol. The Address Resolution Protocol is important for changing the higher-level protocol address (IP addresses) to physical network addresses.

When ARP messages travel from one computer to another, they must be carried in a network frame.

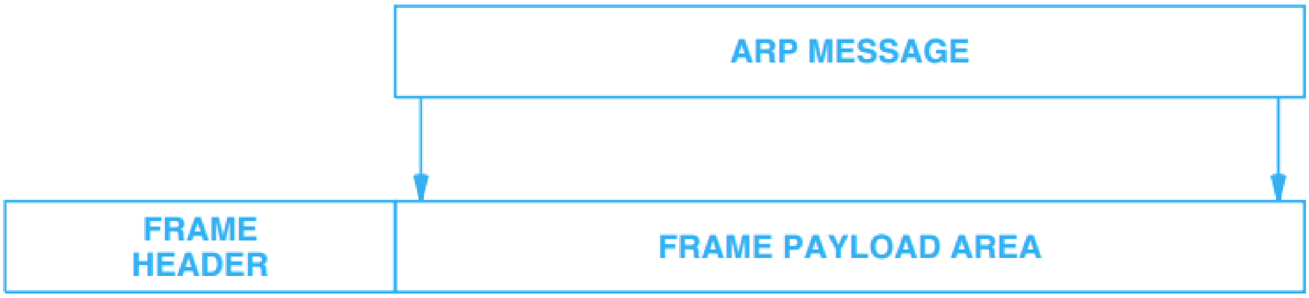


Figure 6.3 An ARP message encapsulated in a physical network frame.

ARP Message format

The design allows ARP to map an arbitrary high-level protocol address to an arbitrary network hardware address. In practice, ARP is only used to map 32-bit IPv4 addresses to 48-bit Ethernet addresses.

The example in Figure 6.4 shows the format of a 28-octet ARP message when used with an IPv4 protocol address and an Ethernet hardware address. The protocol address is 32 bits (4 octets) long, and the hardware address is 48-bits (6 octets) long.

0	8	16	24 31
HARDWARE TYPE		PROTOCOL TYPE	
HLEN	PLEN	OPERATION	
SENDER HARD (octets 0-3)			
SENDER HARD (octets 4-5)		SENDER IPv4 (octets 0-1)	
SENDER IPv4 (octets 2-3)		TARGET HARD (octets 0-1)	
TARGET HARD (octets 2-5)			
TARGET IPv4 (octets 0-3)			

Figure 6.4 The ARP message format when used to map an IPv4 address to an Ethernet address.

An ARP reply carries the IPv4 address and hardware address of the original requester as well as the IPv4 address and hardware address of the sender. In a request, the target hardware address is set to zero because it is unknown.

- **Hardware Type**: This is to specify the type of hardware used by the local network to transmit the Address Resolution Protocols message. Once common hardware under this category would be the 'Ethernet' with a value equal to 1, and field size would be 2.
- **Protocol Type**: To assign a fixed number in this field, IPV4 has a number 2048.
- **HLEN**: This is the length in bytes for the MAC address; generally, we see the ethernet has a MAC address of 6 bytes long.
- **PLEN**: It represents the length of the IPV4 logical address, IPV4 address re generally 4 bytes long.

- **Operation**: This is the length of the logical address in bytes; it specifies the nature of the ARP message. An ARP Request has an assigned value of 1, whereas the ARP reply holds the value of 2.
- **Sender hard address**: Layer 2 address for the device sending the message.
- **Sender IP address**: Protocol address in IPV4 for the device sending the message.
- **Target hard address**: Layer 2 of the intended receiver. This field does not hold any value during the request phase and works only during the reply phase.
- **Target IP address**: This address the protocol address for the intended receiver.

Reverse Address Resolution (RARP)

Reverse Address Resolution Protocol (RARP) is a protocol a physical machine in a local area network (LAN) can use to request its IP address. It does this by sending the device's physical address to a specialized RARP server that is on the same LAN and is actively listening for RARP requests.