计算机网络课程辅助阅读材料（1）

厦门大学软件学院 黄炜

1. Socket types

- Datagram sockets, also known as connectionless sockets, which use User Datagram Protocol (UDP)
- Stream sockets, also known as connection-oriented sockets, which use Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP).
- Raw sockets (or Raw IP sockets), typically available in routers and other network equipment. Here the transport layer is bypassed, and the packet headers are made accessible to the application.

There are also non-Internet sockets, implemented over other transport protocols, such as Systems Network Architecture (SNA). See also Unix domain sockets (UDS), for internal inter-process communication.

2. Addresses

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

In network addressing, the host address, or the host ID portion of an IP address, is the portion of the address used to identify hosts (any device requiring a Network Interface Card, such as a PC or networked printer) on the network. The network ID, by contrast, is the portion of the address that refers to the network itself.

A socket address is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number

and a particular extension. Based on this address, internet sockets deliver incoming data packets to the appropriate application process or thread.

References:

http://en.wikipedia.org/wiki/MAC_address

http://en.wikipedia.org/wiki/Host_address

http://en.wikipedia.org/wiki/IP_address

http://en.wikipedia.org/wiki/Network_socket

3. Hop

In computer networking, a hop is one portion of the path between source and destination. Data packets pass through routers and gateways on the way. Each time packets are passed to the next device, a hop occurs. To see how many hops it takes to get from one host to another ping or traceroute/tracepath commands can be used.

(1) Hop count

The hop count refers to the intermediate devices (like routers) through which data must pass between source and destination, rather than flowing directly over a single wire.[1] Each router along the data path constitutes a hop, as the data is moved from one Layer 3 network to another. Hop count is therefore a basic measurement of distance in a network.

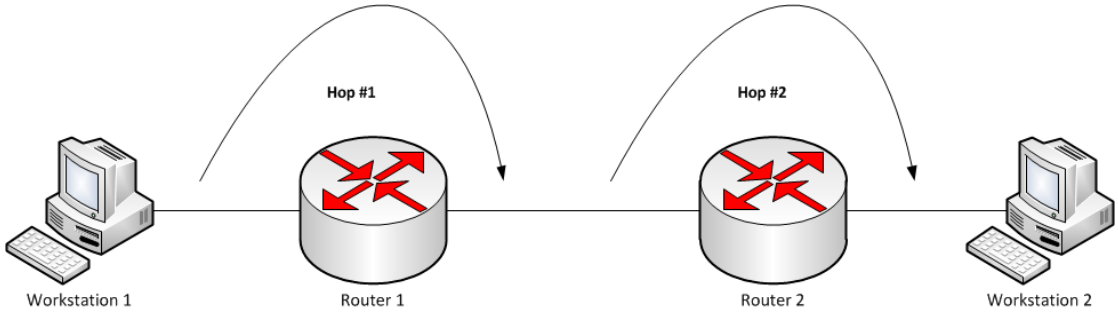

Fig. 3.1 An illustration of hops in a network. The hop count between the computers in this case is 2.

Hop count is a rough measure of distance between two hosts. A hop count of n means that n gateways separate the source host from the destination host. By itself, this metric is, however, not useful for determining the optimum network path, as it does not take into consideration the speed, load, reliability, or latency of any particular hop, but merely the total count. Nevertheless, some routing protocols such as RIP use hop count as their sole metric.[2]

Hop counts are often useful to find faults in a network, or to discover if routing is indeed correct. Network utilities like Ping can be used to determine the hop count to a specific destination. Ping generates packets that include a field reserved for the hop count. Each time a capable device receives these packets, that device modifies the packet, incrementing the hop count by one. In addition, the device compares the hop count against a predetermined limit and discards the packet if its hop count is too high. This prevents packets from endlessly bouncing around the network due to routing errors. Both routers and bridges are capable of managing hop counts, but other types of intermediate devices (like hubs) are not.

(2) Hop limit

In IPv4 known as "time to live", and "Hop Limit" in IPv6, this field specifies a limit on the number of hops a packet is allowed before it should be discarded. This prevents packets from following a loop forever.

(3) Next hop

Routing term used for the next gateway to which packets should be forwarded along the path to their final destination. One technique to make content of a routing table smaller is called next-hop routing.

(4) Next hop forwarding

A routing table usually contains the IP address of a destination network and the IP address of the next gateway (next hop) along the path to the final network destination. Using a routing table to store a next hop for each 'known' destination is called next-hop forwarding. Therefore a given gateway only knows one step along the path, not the complete path to a destination. It is also key to know that the next hops listed in a routing table are on networks to which the gateway is directly connected to.

References:

http://en.wikipedia.org/wiki/Hop_(networking)

4. 几个遗留问题

注：题末答案仅供参考，欢迎讨论。

（1）服务器端一个 Socket 是否能绑定多个 IP？不可以，IPAddress.Any 不是所有 IP，而是等效于 IP 地址 0.0.0.0。

（2）服务器端一个网络应用是否能绑定多个 IP？可以，多个线程，每个线程监听一个 Socket，各自绑定不同的 IP，但调用同样的处理函数。

（3）服务器端一个 Socket 是否能绑定多个端口？不可以。

（4）服务器端一个网络应用是否能绑定多个端口？可以，原理同上，多次调用 bind 会返回错误。

（5）服务器端的网络应用是否能自选 IP 和端口？可以，IP 要真实（除了多播或广播），端口号要合乎 IANA registration 规范。

（6）客户端的网络应用是否能自选 IP 和端口？不可以，默认找最短路径的 IP 以及空闲端口。

5. OSI & TCP/IP Models

	Data unit	OSI Layer	Function	TCP/IP Layer
Host layers	Data	7. Application	Network process to application	4. Application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data	
		5. Session	Interhost communication, managing sessions between applications	
	Segments	4. Transport	End-to-end connections, reliability and flow control	3. Transport
Media layers	Packet / Datagram	3. Network	Path determination and logical addressing	2. Internet
	Frame	2. Data link	Physical addressing	1. Link
	Bit	1. Physical	Media, signal and binary transmission	

References:

http://en.wikipedia.org/wiki/OSI_model