Tcp ip framework case study examples

Sociology, Communication

TCP/IP Framework

TCP/IP stack is a set of hierarchically ordered network protocols. The name of the stack represents a combination of two major protocols – TCP (Transmission Control Protocol) and IP (Internet Protocol). Apart from them, there are dozens of different protocols in the stack. Currently, TCP/IP protocols are the main ones allowing the Internet existence, as well as functioning of the majority of corporate and local area networks.

The history of TCP/IP started in 1967, when the Defense Advanced Research Projects Agency (DARPA) initiated development of computer network, which was to link a number of universities and research centers, performing orders for the Agency. The project was called ARPANET and by 1972 the network united thirty locations. In 1980-1981 within the framework of this project the main protocols of the TCP/IP stack were developed – IP, TCP and UDP. An important factor in the spread of TCP/IP stack was implementation of the operating system UNIX 4. 2 BSD, which happened in 1983.

In order to better understand the architecture of the model, it will be useful to compare it to the OSI model (Open Systems Interconnection) and to view them together. Multilevel models offer various advantages, as in them there are clearly described functions for each level, and direct relationship to adjacent levels. All network protocols are developed in accordance with a specific network model and pertain to a certain level. Thus, taking for example a particular protocol, you can say with confidence what function (global) is assigned to it, and what it cannot perform. Similarly, the network equipment can be attributed to a certain level model, given its function. What does it mean? It allows for distribution of collisions, broadcasting messages, the possibility of work of individual protocols and establishment of communication between two hosts in general, and so on, the list is quite extensive.

The network model helps to find errors and failures, as on the basis of symptoms it is possible to determine at what level the problem happened. As a result, the search scope narrows down considerably (protocols, equipment, etc.). If symptoms do not lead to a decision, you can systematically go through all the models from the lower to upper levels, paying attention to functioning of the network (Kleinrock, 2010). The lower level, at which the problem is identified requires attention (functions assigned to it are not executed or done with errors). Finally, the network model creates a standard that ensures interoperability of protocols and equipment from different manufacturers.

The network models that can be called basic and that are widely used and enhanced today are OSI and TCP/IP. They are both layered, which means that there is a clear division into separate levels. As mentioned above, each level has clearly attributed functions that are not repeated within the same model. The OSI model is divided into seven levels, and TCP/IP into 4:

Figure 1. Correlation between OSI and TCP/IP layers.

Protocols of each level are based on those that correspond to a lower level. Data passes down the protocol stack at the sending machine, then move to the physical network, and go up the protocol stack on a machine-destination. For example, an application that only seems to use the UDP protocol, actually activates the protocols UDP, IP, and the physical network (Farahmand & Rodrigues, 2009).

Under is the data link layer there is only physical level, which defines the electrical, mechanical, procedural, and functional characteristics of activation and deactivation of the maintenance of the physical link between end systems (voltage levels, timing changes in voltage, the transmission rate of physical information, the maximum distance of transmission, physical connectors, etc.).

Protocols that provide data link layer functions are closely related to physical (hardware) environment, in which they operate, for example, Ethernet, Token Ring, FDDI, PPP, ISDN, etc. In the TCP/IP protocol there are no protocols belonging to this level, due to which the hardware independence is achieved in the family of TCP/IP. However, the family includes ARP and RARP protocols, providing communication between the data link layer and the next – network layer of TCP/IP, namely, providing network address translation in the local network address.

IP protocol belongs to the network layer in TCP/IP model, which is the basic one in the structure of TCP/IP and delivers the package to its destination – routing, fragmentation and assembly of packages received in the host of recipient. ICMP protocol also belongs to this level, and its basic functions are error messages, and collection of information on the network operation. Optimal routes through a sequence of interconnected subnetworks are selected by routing protocols. They include protocols such as RIP, EGP BGP OSPF, etc.

The transport layer provides data transport services. They free the application-level data transport mechanisms from the need to delve into the details of data transport. In particular, the concern of the transport layer is safe and reliable transport of data over the network. The transport layer implements mechanisms for installing, maintaining and orderly closing of connections, mechanisms for tracking and troubleshooting transport, flow control.

The application layer identifies and establishes the presence of prospective partners for communication, synchronizes applications running together, establishes agreement on procedures for error recovery and data integrity management. In addition, application-level protocols define whether there are enough resources available for the intended communication. It is also responsible for ensuring that information sent from the application layer of one system is read by the application layer of another system (Chan, 2008). If necessary, it is used to translate between multiple formats of information through the use of a common format and data structures, as well as agree on the syntax of the data for the application layer. The application layer establishes and terminates sessions of interaction between applications, manages these sessions, synchronizes dialogues between objects and directs exchange of information between them. In addition, the application layer provides the means for sending information and notification of data transmittance in case of exceptions.

Although the actual architecture of TCP/IP allowed for fast and successful development of the internet, it has certain issues that are solved via development of new versions. Today IPv6 is in active use. Its history began in 1992 when it was designed to address the problems of address space, and a number of related tasks. The IPv6 address space will be distributed by the Internet Assigned Numbers Authority that will have regional representatives who will be engaged in issuing IP-addresses in their areas. Such a distribution will not be irreversible. IANA will be able to reallocate the address space at any time, in case of errors in their distribution. In other words, everything is done so as not to repeat the mistakes of IPv4.

As for the address space, it will be expanded from the previous 4 billion in IPv4 until 340 282 366 920 938 463 463 374 607 431 768 211 456 addresses (Sailan, Hassan & Patel, 2009). IP-space of IPv6 is 128 bits, which adds routing capabilities (especially it will be noticeable for the multicast broadcast). It defines a new type of address " anycast", which will lead to the nearest interface from the list of addresses. IPv6 addresses can also be configured automatically not depending on the context. Such addresses greatly simplify routing and routing tables will be four times shorter.

In addition to obvious advantages in extending the address space, there are the following advantages of IPv6 over IPv4:

Ability to auto-configure IP addresses.

Simplification of routing.

Simplification of the packet header.

Maintenance of Quality of Service (QoS).

Increased security of data transmission.

Actually, almost all the benefits of IPv6 stem from its packet format and addressing. Redesigned and improved standard allows for realization at the protocol level of strong cryptographic (encryption), and many services such as QoS. QoS in IPv6 is fully supported at the network level. This is very important for multimedia conferencing. Changes made in IPv6 show that it will not only solve the basic problem of lack of address space, but will also rebuild the entire structure of the Internet so that it becomes more logical and sound.

References

Bell, V. (2009). Taking an internet history. The British Journal of Psychiatry, 194, 561-562.

Chan, M. C. (2008). Improving TCP/IP Performance over Third-Generation Wireless Networks. IEEE Transactions on Mobile Computing, 7(4), 430-443.

Farahmand, F., Rodrigues, J. (2009). A layered architecture for Vehicular Delay-Tolerant Networks. IEEE Symposium on Computers and Communications. ISCC, 122-127.

Kleinrock, L. (2010). An early history of the internet [History of Communications]. IEEE Communications Magazine, 48(8), 26-36.

Sailan, M. K., Hassan, R., Patel, A. (2009). A comparative review of IPv4 and IPv6 for research test bed. International Conference on Electrical Engineering and Informatics, 2, 427-433.