International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 7759-7764

Protocols

Ritika Maini

Assistant Professor, Govt. Bikram College of Commerce, Patiala, Patiala-147001, India.

Abstract

When two humans converse, they may have to use the same language but they generally understand each other without having to adhere to rigid rules of grammar or formal language frameworks. Computers, on the other hand, have to have everything explicitly defined and structured. If computers wish to communicate with one another, they have to know in advance exactly how information is to be exchanged and precisely what the format will be. Therefore, standard methods of transmitting and processing various kinds of information are used and these methods are called "protocols". Protocols are established by international agreement and ensure that computers everywhere can talk to one another. There are a variety of protocols for different kinds of information and functions. This article will discuss some of the common protocols that the average PC user is likely to encounter.

The official procedure or system of rules governing affairs of state or diplomatic occasions: protocol forbids the prince from making any public statement in his defense.

Keywords: Protocol, TCP, IP, Networking, IEEE, XML, HTTP, FTP, Cryptography, Mallicious

Protocol

Protocol is a set of rules that govern all aspect of data communication between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer. A protocol defines what, how, when it communicated. The key elements of a protocol are syntax, semantics and timing. Protocols are to computers what language is to humans. Since this article is in English, to understand it you must be able to read English. Similarly, for two devices on a network to successfully communicate, they must both understand the same protocols. The accepted or established code of procedure or behavior in any group, organization, or situation:

Standards are developed by cooperation among standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

a) International Standards Organization (ISO)
b) International Telecommunications Union (ITU)
c) American National Standards Institute (ANSI)
d) Institute of Electrical and Electronics Engineers (IEEE)
e) Electronic Industries Association (EIA)
f) Internet Engineering Task Force (IETF)

What is the protocol at a smart lunch if one's neighbor dozes off during the speeches?

More example sentences

- At the end of the day, everyone knows that this is still a diplomatic affair, where protocol and ethics must be observed, and cordiality must always be extended.
- So how could he make a preference known without breaching diplomatic protocol?
- It seems that besides teaching new government leaders protocol, they certainly need lessons in public speaking.
- In this particular instance, a temp employee made a mistake and did not follow our established protocol, and we regret any inconvenience this may have caused.
- But museum bosses have now decided to eschew accepted protocol because they believe museum visitors should have the opportunity to join the discussion about whether mummies should be shown.
- He said he obviously went against established protocol.
- Why did New Zealand sign and ratify a protocol that has already agreed to set rules for liability and redress for damage, if it now intends to undermine the treaty by suggesting that rules on liability may not be necessary?
- According to the report, the ministries of external affairs, finance, labour and commerce have already agreed on the draft agreement on the protocol to be signed with the US.
- The Netherlands is very serious, as is Europe, about this issue, and I believe that the Russians will sign the protocol - but let us wait and see
- In addition there were various protocols to the Treaty and declarations adopted by the Member States.
- Moreover, new treaties, protocols, or amendments thereto will normally require positive ratification to enter into force.
- Essentially every country in the world has ratified these treaties, bar three; also Australia has ratified the two additional protocols to the Geneva Conventions.

A procedure for carrying out a scientific experiment or a course of medical treatment: a study protocol approved by the ethics committee of the hospital the low doses of morphine recommended in the protocol Computing A set of rules governing the exchange or transmission of data between devices

- The study protocol was approved by the University Hospital Medical Ethics Committee, and written informed consent was obtained from all participants.
- In one study there was no indication as to the protocol for intubation and treatment failure.
- The medical center's institutional review board approved the study protocol.
- Internet mail protocols - the technical rules that govern how messages are transmitted - need revamping.
- Typically, a firewall lets HTTP requests pass through - HTTP being the standard protocol for transmitting WebPages.
- Using ubiquitous internet protocols like XML and HTTP, web services allow the sharing of data or logic over the network and even through firewalls.

Origin

Late Middle English (denoting the original minute of an agreement, forming the legal authority for future dealings relating to it): from Old French protocol, via medieval Latin from Greek prōtokollon 'first page, flyleaf', from prōtos 'first' + kolla 'glue'. Sense 1 derives from French protocol, the collection of set forms of etiquette to be observed by the French head of state, and the name of the government department responsible for this (in the 19th century).

An agreed-upon format for transmitting data between two devices. The protocol determines the following:

the type of error checking to be used data compression method, if any

how the sending device will indicate that it has finished sending a message

- how the receiving device will indicate that it has received a message

There are a variety of standard protocols from which can choose. Each has particular advantages and disadvantages; for example, some are simpler than others, some are more reliable, and some are faster.From a user's point of view, the only interesting aspect about protocols is that your computer or device must support the right ones if you want to communicate with other computers. The protocol can be implemented either in hardware or in software.

Protocols used in day to day life

BASIC PRINCIPLE: It should not be possible to do more or learn more than

is specified by the protocol.

Lots of protocols in daily life:

Paying for goods at a store.

Playing poker.

Talking on the phone.

Voting in an election

The players

A: First participant (A) in protocols

B: Second participant (B) in protocols

C: Participant (C) in three and four party protocols

D: Participant (D) in four party protocols (or maybe Ted)

Eve: Evil Eavesdropper

Mallory: Malicious (Man-in-the-Middle) active attacker

Trent: Trusted arbitrator

W: Warden - guards A and B in some protocols

Peggy: Prover

Victor: Verifier

Characteristics of protocol

a) Direct / indirect

Communication between two entities maybe direct or indirect.

i) **Point-to-point** link connection provides a dedicated link between two devices the entities in these systems may communicate directly that is data and control information pass directly between entities with no intervening active agent.

ii) **Multipoint** link connection more than two devices can share a single link.

The entities must be concerned with the issue of access control and making the protocol more complex.

b) Monolithic / structured The task of communication between entities on different systems is too complex to be handled as a unit.

c) Symmetric / asymmetric Symmetric is the most use in protocol and involve communication between peer entities. Asymmetry may be dictated by the logic of an exchange (eg; client and a server process) the desire to keep one of the entities or systems as simple as possible.

d) Standard / nonstandard If ***K*** different kinds of information sources have to communicate with ***L*** types of information receivers, as many as ***K x L*** different protocols are needed without standards and a total of ***2 x K x L*** implementations are requiredIf all systems shared a common protocol, only ***K+L*** implementations would be needed.

Types of protocols

A. Arbitrated protocols: A disinterested party, known to and trusted by both A and B acts as intermediary to make it difficult for A and B to cheat each other. For example, in real life a lawyer might help B buy a car from A when B does not trust A to give him the title, and A does not trust B to give her a valid check, using the following protocol

1. A give the title to the lawyer (Trent)
2. B gives the check to A
3. Trent waits a specified time for the check to clear, and then gives the title to A.
4. If the check does not clear within the specified time, A presents proof of this to Trent, who returns the title.

A notary public is another sort of arbitrator - one who can attest to the validity of a signature, for example.

B. Adjudicated protocols

Basically a potentially arbitrated protocol, where the arbitrator, here called an adjudicator (or judge) is called in only in the case of a dispute.

What is needed here is a protocol that leaves enough of a paper (or electronic) trail to allow a judge to make a decision.

For example, A and B might draw up a contract agreeable to both of them, sign it, and maybe even get a couple of friends on each side to witness the signing. Both keep a copy.

Later, if there is a dispute, both can present their evidence, and call witnesses, before a judge.

C. Self-enforcing protocols

The idea is that the protocol itself guarantees fairness, prevents disputes, and detects any attempt to cheat in time to allow the protocol to be terminated without the cheater gaining an advantage.

This is the most desirable situation, but also more difficult to achieve, and such protocols are not known for all problems

PROTOCOL– Set of rules or language use by computer and networking devices to communicate with one another

SERVICE - A service use by computer and networking devices such as file and print services

Computer Protocols- TCP/IP, POP, SMTP, HTTP, FTP

Protocol	Acronym	Remarks
Point To Point	PPP	Used to manage network communication over a modem
Transfer/Transmission Control Protocol	TCP / IP	Backbone protocol. The most widely used protocol.
Internetwork package exchange	IPX	Standard protocol for Novell NOS
NetBIOS extended user interface	NetBEUI	Microsoft protocol that doesn't support routing to other network. Running only Windows-based clients.
File transfer Protocol	FTP	used to send and received file from a remote host
Simple mail Transfer protocol	SMTP	Used to send Email over a network
Hyper text transfer protocol	HTTP	Used for Internet to send document that encoded in HTML
Apple Talk	Apple Talk	Protocol suite to network Macintosh computer and a peer-to-peer network protocol
OSI Model	OSI Layers	A way of illustrating how information functions travels through network of its 7 layers.

Networking Protocols

UDP – User Datagram Protocol is a streamline economy class version of TCP which is connectionless but is very unreliable compared with TCP which is connection oriented

IPX/SPX – Internet Network Packet Exchange/Sequential Packet Exchange the Native protocol use by an older Novell Netware Networks

NetBEUI- Pronounced net-booey, NetBEUI is short for NetBios Enhanced User Interface. It is an enhanced version of the NetBIOS protocol used by network operating systems such as LAN Manager, LAN Server, and Windows for Workgroups, Windows 9 xs and Windows NT. NetBEUI does not support routing and thus cannot communicate in the Internet.

Apple Talk - Protocols use by older Apple computers

DLC Short for Data Link Control, an older protocol use to communicate with Mainframe computers and some older HP network laser printers.

NWLINK- Netware Link developed by Microsoft to communicate with Older Novell Netware networks

Dial Up and Remote Access Networking Protocols

PPP Short for Point-to-Point Protocol, a method of connecting to a computer to the Internet PPP is more stable than the older SLIP protocol and provides error-checking features.

SLIP-Short for Serial Line Internet Protocol, a method of connecting to the Internet another more common method is PPP (Point-to-Point Protocol). SLIP is an older and simpler protocol, but from a practical perspective, there's not much difference between connecting to the Internet via SLIP or PPP. In general, service providers offer only one protocol although some support both protocols.

RAS – Dial up Protocol service use for connecting to a Microsoft Remote Access Server

PPPoE- Point to Point Protocol over Ethernet used for connecting multiple network users on an Ethernet LAN to a remote site through a common device. Very popular with DSL and wireless

Transferring File Protocols

FTP - Abbreviation of File Transfer Protocol, the protocol used on the Internet for connection oriented transferring of files. Popular protocol for uploading and downloading pages

SFTP – Secure File Transfer Protocol use for transferring files in a secure manner

TFTP – Trivial File Transfer Protocol is a connectionless FTP as opposed to FTP which is connection oriented

World Wide Web Protocol

HTTP - Short for Hypertext Transfer Protocol, the underlying protocol used by the World Wide Web. It lets the browser communicate with the web server.

HTTPS – HTTP Secure with built in SSL (Encryption)

Newsgroup Protocols

NNTP - Short for Network News Transfer Protocol, the protocol used to post, distribute, and retrieve USENET, BBS or newsgroup materials

Directory protocols

LDAP - Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDA

TCP/IP

TCP (Transmission Control Protocol) and IP (Internet Protocol) are two different procedures that are often linked together. The linking of several protocols is common since the functions of different protocols can be complementary so that together they carry out some complete task. The combination of several protocols to carry out a particular task is often called a "stack" because it has layers of operations. In fact, the term "TCP/IP" is normally used to refer to a whole suite of protocols, each with different functions. This suite of protocols is what carries out the basic operations of the Web. TCP/IP is also used on many local area networks. The details of how the Web works are beyond the scope of this article but I will briefly describe some of the basics of this very important group of protocols. More details can be found in the references in the last section. When information is sent over the Internet, it is generally broken up into smaller pieces or "packets". The use of packets facilitates speedy transmission since different parts of a message can be sent by different routes and then reassembled at the destination. It is also a safety measure to minimize the chances of losing information in the transmission process. TCP is the means for creating the packets, putting them back together in the correct order at the end, and checking to make sure that no packets got lost in transmission. If necessary, TCP will request that a packet be resent.

Internet Protocol (IP)

IP is the method used to route information to the proper address. Every computer on the Internet has to have its own unique address known as the IP address. Every packet sent will contain an IP address showing where it is supposed to go. A packet may go through a number of computer routers before arriving at its final destination and IP controls the process of getting everything to the designated computer. Note that IP does not make physical connections between computers but relies on TCP for this function. IP is also used in conjunction with other protocols that create connections.

UDP and ICMP

Another member of the TCP/IP suite is User Datagram Protocol (UDP). (A datagram is almost the same as a packet except that sometimes a packet will contain more than one datagram.) This protocol is used together with IP when small amounts of information are involved. It is simpler than TCP and lacks the flow-control and error-recovery functions of TCP. Thus, it uses fewer system resources.A different type of protocol is Internet Control Message Protocol (ICMP) . It defines a small number of messages used for diagnostic and management purposes. It is also used by Ping and Traceroute.

Mail Protocols POP3 and SMTP

Email requires its own set of protocols and there are a variety, both for sending and for receiving mail. The most common protocol for sending mail is Simple Mail Transfer Protocol (SMTP). When configuring email clients, an Internet address for an SMTP server must be entered. The most common protocol used by PCs for receiving mail is Post Office Protocol(POP). It is now in version 3 so it is called POP3. Email clients require an address for a POP3 server before they

can read mail. The SMTP and POP3 servers may or may not be the same address. Both SMTP and POP3 use TCP for managing the transmission and delivery of mail across the Internet.A more powerful protocol for reading mail is Interactive Mail Access Protocol (IMAP). This protocol allows for the reading of individual mailboxes at a single account and is more common in business environments. IMAP also uses TCP to manage the actual transmission of mail.

Hypertext Transfer Protocol

Web pages are constructed according to a standard method called Hypertext Markup Language (HTML). An HTML page is transmitted over the Web in a standard way and format known as Hypertext Transfer Protocol (HTTP). This protocol uses TCP/IP to manage the Web transmission.A related protocol is "Hypertext Transfer Protocol over Secure Socket Layer" (HTTPS), first introduced by Netscape. It provides for the transmission in encrypted form to provide security for sensitive data. A Web page using this protocol will have https: at the front of its

File Transfer Protocol

File Transfer Protocol (FTP) lives up to its name and provides a method for copying files over a network from one computer to another. More generally, it provides for some simple file management on the contents of a remote computer. It is an old protocol and is used less than it was before the World Wide Web came along. Today, Its primary use is uploading files to a Web site. It can also be used for downloading from the Web but, more often than not, downloading is done via HTTP. Sites that have a lot of downloading (software sites, for example) will often have an FTP server to handle the traffic. If FTP is involved, the URL will have ftp: at the front.

Attacks on protocols

* Passive attacks

A third party (Eve) eavesdrops on some or all of the protocol, and attempts to obtain information they are not intended to have Generally difficult to detect, (except in the case of certain quantum communication techniques), so generally protocols are designed to be as secure as possible against it.

Different levels of eavesdropping:

Does Eve see only communication sent between parties? or is she also watching keystrokes or reading decrypted messages?.

*** Active attacks**

A third party (Mallory) attempts to alter the protocol to his own advantage - pretending to be

someone else, intercepting and retransmitting messages, or retransmitting altered versions,

changing information stored in a computer, etc. Goals could be corrupting information, obtaining unauthorized information, disrupting service etc.Mallory might be anyone, up to and including the system administrator.

*** Cheaters**

One (or more) parties in the protocol might attempt to subvert the protocol to gain more

information or to accomplish something more than is specified by the protocol. There can be passive cheaters, who follow the protocol, but attempt to gain extra information, and active cheaters, who disrupt the protocol in an attempt accomplish their nefarious ends.

It is (unsurprisingly) hard to make a secure protocol if most participants are active cheaters.

Cryptographic tools employed in protocols

1. **Symmetric cryptosystems (DES etc.) We know a bit about these already.**

- Security should lie in the key
- Keys must be distributed in secret, and are as valuable
- as all the information they encrypt
- Having a key compromised (broken, stolen, extorted, bribed) permits all sorts of mayhem through messages read, and messages faked,
- N users need O(n^2) keys to communicate securely.

2. One-way functions

Functions that are easy to compute, but hard to invert.Lots of proposed one-way functions, many do seem hard to invert but there are lots of examples of ideas that looked good and were later broken. No proof that any actually exist.

3. Trap-door one-way functions

- Functions that are one-way, unless one knows the secret
- that allows them to be inverted.
- Such functions are at the heart of public key systems such as RSA
- Difficulty of factoring, discrete logs, various NP complete problems
- have been used as a basis for trapdoor functions.
- Again, no mathematical proof that such functions actually exist.

4. One-way hash functions

- One way functions that map plaintexts (preimages) of arbitrary size many-to-one to a fixed size output string or "fingerprint in a way that makes it difficult to find a preimage that matches any particular fingerprint.

Other names:

Compression function, contraction function, message digest, Fingerprint, cryptographic checksum, message integrity check (MIC), Manipulation detection code (MDC)...

Many uses in cryptographic protocols, some suggested by preceding names.

Basic utility is in verifying that someone has a particular object

without actually sending a full description of the object.

Fingerprint size must be long enough to prevent brute-force searches for messages that produce a given fingerprint.

Must not only prevent arbitrary inversion, but prevent generation of two (related) messages that generate the same fingerprint.

A Message Authentication Code (MAC) is a one-way hash function that can only be verified using a secret key.

5. Public-key cryptosystems (RSA etc.) We know a bit about these already as well. Summarizing the main points.

- Each person has a public key, and a private key.
- Standard use is that A encrypts a message for B using B's public key, and B decrypts it with his private key
- Often the public and private keys can both encrypt and decrypt, so that they can be used (e.g.) for digital signatures as well as message encryption. (more on this later)
- Easily extended to networks of many users with only
- O(n) keys needed for secure communication among n users.
- Public-key systems are slow compared to symmetric systems (by a factor of 1000 or more).
- They are also vulnerable to chosen plaintext attack if the number of possible messages is modest.

6. Hybrid cryptosystems (PGP etc.)

- Public key system is used to exchange a "session key" for a symmetric system, which is then used to encrypt and transmitthe bulk of the data.
- Reduces problems of key distribution, and amount of potential damage if symmetric key is compromised without incurring cost of using public key system for all encryption.

Simplest protocol

1. B sends A his public key (or she gets it from a database)
2. A generates a random session key, encrypts it with B's private Key, and sends it to B.
3. B decrypts A's message using his private key to recover the Session key
4. A and B encrypt further communication using the session key and a symmetric system.

REFERENCES

[1] TCP/IP

[2] Internet protocol

[3] TCP/IP

[4] http://www.escotal.com/protocol.html

[5] https://www.cs.rochester.edu/~nelson/courses/cryptology/notes/lecture_13.txt