Ground segment protocol

Communications department

November 3, 2016

1   Protocol model/suit

In order to find the protocols that will rule the ground communications of the network, it has been studied 4 protocol models and suits. It has to be found the advantages and disadvantages of each one and then, assess which suits better to the porpouse. The models and suits are:

- OSI
- TCP/IP
- NetBEUI
- IPX/SPX

OSI and TCP/IP have a complex structure which it is ideal for large networks. Althoght, this complexity makes the protocols inefficient in small networks. On the other hand NetBEUI and IPX/SPX protocols are simpler and optimum in simple comunications. They cannot work in a large network unless adding extensions.

In the begining of the network workint, the ground segment would not be so large as could be the space segment. Since there wont be lots of Ground Stations (3 at the begining, but it cuould increase) the big part of nodes will be the clients. If it is want to be versatile and adapt to the demand it has to be implemented protocols of the TCP/IP suit or based in the OSI model. Although these 2 will be more dificult to implement and configuate, it will be the better option to ensure a good coverege for the demand and a friendly use to the costumers.

The main diference between OSI and TCP/IP is that the first is a model and the second is a suit of potocols. OSI is structured in 7 layers, and it descives how these layers should work. It is a theorical guide for build a protocol but nobody had never implemented a complet OSI protocol. TCP/IP is structured in 4 layers and it is formed by a family of protocols which can be used in this layers. In the practice almost every network is ruled by TCP/IP protocols.

The decicison between OSI model and TCP/IP suit could be resumed as making a protocol or use existing ones. The work of the ground segment is not really diferent of many existing systems, so the better option is to use the existing TCP/IP protocols. It has to be found which fits better to the system in every layer and adapt it if it is need.

2 TCP/IP

The TCP/IP protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed and received. This functionality is organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved. From lowest to highest:

1. Link layer

2. Internet layer

3. Transport layer

4. Application layer

2.1 Link layer

The link layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer includes the protocols used to describe the local network topology and the interfaces needed to effect transmission of Internet layer datagrams to next-neighbor hosts.

The most used prtocols in this layer are stuied and presented in order to find the better option for the ground segment communications.

Ethernet

Over the years, Ethernet, which is technically IEEE 802.3 CSMA/CD LANs, has become the most commonly used standard for enterprise networks. These networks carry voice, graphics, and video traffic. Today's Ethernet networks run considerably faster than the original Ethernet. The most common top speed, for example, is a full thousand times faster than the original Ethernet — 10 gigabits per second (Gbps) versus 10 megabits per second (Mbps). With so much data being carried, the potential increases for more and more packet collisions in the collision domain. When a collision occurs, both data frames must be re-sent and this cuts down drastically

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames. As per the OSI model, Ethernet provides services up to and including the data link layer.

IEEE 802.11

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

With this connection the client would have a range of arround 60 m and a data rate that can arriive to 5 Gbit/s.

Frame Relay

Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.

This system requires an economical hardware, but it provides to the user a data rate in the order of 500 Mbit/s.

ATM

Asynchronous Transfer Mode (ATM) is a telecommunications concept for carriage of a complete range of user traffic, including voice, data, and video signals. It was designed for a network that must handle both traditional high-throughput data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video.

The reference model for ATM approximately maps to the three lowest layers of the ISO-OSI reference model: network layer, data link layer, and physical layer.

ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

The ATM system can work i data ates between 1 and 50 Mbit/s

Conclusion

The better option for the Astrea system will be that the clients could enter the wide with their own internet local network. It will be easy and frendly for the client since it can access the service with any especial hardware. He/she would only need a computer and its own connection to internet. The client will be free for using a LAN (Ethernet) a WAN (IEE 802.11), or other variants. This systems are able to work at 25 Mbit/s, which is the minimum data rate that it has to be ensured. Despite this, for avoiding conflicts, it has to be informed to the client that is required a local connection of at least 25 Mbit/s.

2.2 Internet Layer

The internet layer is a group of internetworking methods, protocols, and specifications in the Internet protocol suite that are used to transport datagrams (packets) from the originating host across network boundaries, if necessary, to the destination host specified by a network address (IP address) which is defined for this purpose by the Internet Protocol (IP). The internet layer derives its name from its function of forming an internet (uncapitalized), or facilitating internetworking, which is the concept of connecting multiple networks with each other through gateways.

The internet layer has three basic functions:

- For outgoing packets, select the next-hop host (gateway) and transmit the packet to this host by passing it to the appropriate link layer implementation.

- For incoming packets, capture packets and pass the packet payload up to the appropriate transport layer protocol, if appropriate.

- Provide error detection and diagnostic capability.

IPv4

IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^{32} addresses (just over 4 billion addresses). With the growth of the Internet it is expected that the number of unused IPv4 addresses will eventually run out because every device -including computers, smartphones and game consoles- that connects to the Internet requires an address.

IPv6

IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

While increasing the pool of addresses is one of the most often-talked about benefit of IPv6, there are other important technological changes in IPv6 that will improve the IP protocol:

- Auto-configuration

- No more private address collisions

- Better multicast routing

- Simpler header format

- Simplified, more efficient routing

- True quality of service (QoS), also called "flow labeling"

- Built-in authentication and privacy support

- Flexible options and extensions

- Easier administration

For this layer will be used IPv6. With the same porpoue it is clear that IPv6 is more efficient than IPv4. Astrea system would be operational for years, and it does not take sense to use a protoccol which would be obsolete in the future. Even so, it could be added some extension protocols that will make the system more robust.

IPsec

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

ICMPv6

ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions and has a framework for extensions to implement future changes. ICMPv6 messages may be classified into two categories: error messages and information messages. ICMPv6 messages are transported by IPv6 packets in which the IPv6 Next Header value for ICMPv6 is set to 58.

NDP

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6). It operates in the Link Layer of the Internet model, and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information of other active neighbor nodes.

SEND

The Secure Neighbor Discovery (SEND) protocol is a security extension of the Neighbor Discovery Protocol (NDP) in IPv6. NDP is insecure and susceptible to malicious interference. It is the intent of SEND to provide an alternate mechanism for securing NDP with a cryptographic method that is independent of IPsec, the original and inherent method of securing IPv6 communications.

MLD

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that makes decisions on the flow of multicast data packets.

Conclusion

ICMPv6 will be imlemented in order to ensure that the data arrives where it has to. For the adecuate work of the sistem it has to be also included NDP, in order to make easy the connection of the client to the network.

The security is a very imortant criteria for designing the protocols. It has to be considered that the ground segment is the most susceptible to be attacked. The privacy of the information that it will be managed has to be ensured. For this reason IPsec and SEND will be impemented.

Finally it is descarted to use MLD. It does not report any significant benefit to the system and it would be useless.