**CS635: Computer Networking**

**Individual Project 5: iSpace**

**Ajitpal Grewal**

**6/2/2024**

**Colorado Technical University**

Contents

[ Project Outline 3](#_Toc168261338)

[ Distributed Network Requirements Analysis 5](#_Toc168261339)

[ Communication Protocols Analysis and Recommendations 7](#_Toc168261340)

[ Network Traffic Analysis and Recommendations 11](#_Toc168261341)

[ Network Design and Architecture 15](#_Toc168261342)

[ Future Needs Analysis and Recommendations 21](#_Toc168261343)

[ References………. 24](#_Toc168261344)

## Project Outline

iSpace aims to be the global leader of space exploration. The organization utilizes a network of spacecraft, satellites, and rovers to observe movements of celestial bodies and gather samples from distant planets and moons. iSpace employs over 2,500 engineers and researchers with its headquarters located in Silicon Valley, California. With an increasing number of deployed functional units, iSpace requires scaling networkability within its infrastructure. Each of these functional units is specialized for their individual objectives. Examples are the rovers embedded with real-time operating systems that direct processes such as movement and data collection (Stallings, 2017). These rovers and their associated basecamps will be dispatched to the surface of Mars. The basecamps will serve as checkpoints for future missions involving deeper space travel. Once trained astronauts have safely established these basecamps, they will be the foundations for space tourism for humans. This will inevitably lead to the successive exploration of further planets outside of our solar system.

iSpace features a strategic server distribution across the Earth. Locations of these servers include Texas, Florida, Australia, and China. The company also disperses its launch sites across those same locations to ensure low latency environments and effective communication. It is imperative for iSpace servers to be able to swiftly communicate with its functional units. This is relevant in cases where a ground server must correct the course of a satellite in accordance with the changing trajectory of a celestial body (Comins, 2017). Having multiple servers, or nodes, ensures resilience of iSpace’s distributed networking system (Tanenbaum, 2020). This is also relevant in cases where launch windows are small with severe time constraints. Having multiple launch sites allows for flexibility during natural disaster considerations.

Distributed networking in iSpace allows the company to see upheld redundancy and fault tolerance (Stallings, 2017). Minimizing the amount of data loss and corruption is crucial for company success. If data collected by a satellite is communicated between multiple servers through a network before one of those servers goes down, it may mean the difference between a failed or successful mission. This type of infrastructure communication will also lead to exponential scalability of iSpace functional units. The expansion of the iSpace armada requires intense and deliberate work. Having a distributed network allows engineers to make constant adjustments as mission objectives change. Flow of data within the organization is efficient across iSpace’s multiple locations due to its reliable distributed networking system.

## Distributed Network Requirements Analysis

* **Data Collection & Management:** Without distributed networking, it would be impossible for the company to collect and manage data over vast distances. iSpace’s distributed network must be able to provide high speed communications between its Linux-based real-time operating systems and ground servers. The network must also be able to transfer large volumes of data in the form of images obtained from satellites. iSpace must be able to accommodate for zettabytes of incoming data. Each satellite is equipped with transponders that function as antennas acquiring radio frequencies. To ensure confidentiality, iSpace utilizes the public key infrastructure. The PKI structures users and directories by defining standards for protocols (Tanenbaum, 2020).
* **Disaster Recovery:** In the extremes of an aerospace environment, it is crucial for engineers to consider the potential of disaster and data loss. Since safety is of the utmost importance for iSpace, single point failure cannot be allowed to cascade and jeopardize the remainder of a mission. To mitigate this risk, the iSpace network utilizes routing algorithms to ensure quick and efficient data flow between its functional units. To reduce network congestion, the routing algorithm directs packets to the output lines they are to be transmitted on (Tanenbaum, 2020). Quick, synchronized transmission of incoming data from server to server can reduce data corruption in the case of server failure.
* **Spacecraft Communication:** A distributed network allows iSpace to deploy multiple spacecraft of different variations across the galaxy. It is essential that the network supports high-bandwidth and low-latency interactions between units to ensure spacecraft integrity. This is relevant in cases of debris avoidance. One spacecraft must be able to communicate a dangerous occurrence to another spacecraft in sufficient time. Engineers utilize the frequency hopping spread spectrum technique to make it difficult for outsiders to detect transmissions and making them almost impossible to jam (Tanenbaum, 2020). Hopping up and down frequencies will also allow different subsets of iSpace functional units to cooperate with one another at the same time, without interference.
* **Dispersed Simulation Training:** Distributed networking plays a significant role in simulation training for astronauts and mission planners across separate locations of the globe. The network must support video streaming of at least 50 Mbps for proper immersive experiences. iSpace utilizes a company firewall, a virtual private network, and tunnels to ensure packets are properly encapsulated and decapsulated before they enter the network. Minimizing jitter and packet loss are defining parameters to uphold quality of service and quality of experience (Tanenbaum, 2020). In cases of astronaut training, real-time response can be a matter of life and death. Therefore, the simulations provided to them must be as realistic as possible for proper training purposes.
* **Research & Innovation Team Collaborations:** iSpace’s distributed network enables secure communication between development teams within the organization, or third-party development teams and vendors. Secure, high-speed, and high-bandwidth capabilities are necessary characteristics of the network to solidify the uninterrupted sharing of ideas and resources between parties. iSpace utilizes the secure hypertext transfer protocol to ensure these ideas remain private. By encrypting transmitted data and requiring user authentications/privileges, the company and its partners can keep new findings discrete (Tanenbaum, 2020).
* **Conclusion:** iSpace allocates hundreds of millions of dollars per year to mission planning, research and development, and training purposes. The network and security regulations imposed by iSpace must also follow the FAA guidelines (McKenna, 2013). iSpace engineers must consider the software-defined networking intricacies of the Linux kernel in conjunction with the distributed network. This open-source environment allows for customization of forwarding in data centers across the globe (Tanenbaum, 2020).

## Communication Protocols Analysis and Recommendations

**- Data Collection & Management –** Inefficient data collection and improper management of that data can lead to failure of a mission. This implies the waste of valuable resources such as fuel. Therefore, it is imperative that iSpace implements appropriate communication protocols to strengthen routine data collection and storage. Operating heavily at the transport and internet layers, the Transmission Control Protocol/Internet Protocolis a reliable communication protocol architecture that dates to the days of ARPANET. The TCP is connection-oriented and allows error checked byte stream communication between two machines across the internet. Upon reception of the byte stream, the host protocol breaks it up into separate messages which are passed onto the internet layer. After they are passed on, the messages are reassembled into the output stream. The transmission control protocol also regulates flow control to ensure that the sender is not delivering too many messages for the receiver to handle. The IP allows seamless identification of machines on a network due to their assigned addresses which can be IPv4 or IPv6. The IP routes packets of data to their appropriate destinations. Each of these packets contains headers with important information pertaining to the packet length and IP address destination.

The Secure Hypertext Transfer Protocol suite regulates web-based services and ensures secrecy during communications across a network. This protocol can be used to safely access dashboards. HTTPS uses Transport Layer Security (TLS) to execute its request-response mechanism. Some of these request methods can read a Web page (GET), store a Web page (PUT), or remove a Web page (Delete). This protocol determines the messages a client may send to a server, and responses the server may send back to the client.

The TCP/IP method in conjunction with the HTTPS architecture allows iSpace to ensure its samples collected by rovers and images captured by satellites are safely processed and stored in distributed iSpace ground servers. Once data is transmitted from iSpace functional units into its ground servers, it can be accessed securely only by those with permission. The data can be sent between servers and other appropriate destinations reliably. Successful inter-device communication results in data integrity.

The TCP/IP architecture is widely used across the globe, making it simple to implement across different types of machines. The HTTPS architecture is also standardized, allowing for effective web communication (Tanenbaum, 2020). Some drawbacks of the TCP/IP suite are due to its connection orientation. The management of this connection can cause high, unmanageable overhead. The enterprise cannot afford to account for extra allocation of resources. The HTTPS methodology can bring latency to its environment due to its encrypting and decrypting capabilities. In a stringent real-time environment this may be detrimental to the success of a mission depending on how quickly information can be processed.

**- Disaster Recovery –** iSpace must assume failures will occur during any given space mission and respond to those failures accordingly. The incorporation of the Trivial File Transfer Protocol (TFTP) and Internet Protocol Security Virtual Private Network (IPSec VPN) will assist iSpace in recovery from disasters such as satellite or rover collisions. TFTP is connectionless and uses no handshakes before sending packets. As with HTTPS, TFTP also uses a request-response mechanism where the client requests a response (READ), and the server provides the requested file (WRITE) or an error message. The files are broken up into smaller files that contain information on where they are to be sent. The underlying mechanism of TFTP is User Datagram Protocol (UDP), which regulates the sending of messages between applications on different hosts (Mohamed, 2018). TFTP efficiently moves files between iSpace satellites, rovers, and ground servers.

IPSec VPN provides iSpace with confidentiality during communication between parties and encryption of data when faced with disaster. IPSec VPN in tunnel mode enhances security features of all transmitted IP packets (Nam, 2022). Tunnel mode allows iSpace to utilize public networks such as the internet while retaining secrecy throughout the entirety of its network infrastructure. This enables protected signaling between satellites and related ground units.

In the event of disaster, TFTP allows for quick transmission of data due to its low security features. In cases of emergency where speed of file transfer is of the essence, TFTP provides minimal overhead and allows for maximum movement of data before the affected server or functional unit is disabled. On the other hand, the lack of security features implemented within this mechanism gives rise to the possibility of information being stolen during the transfer process. In the case of IPSec VPN, the security features it provides may be a detriment to the operation if those encryption processes result in overhead and latency. A few milliseconds can be the difference between information being saved or lost.

**- Spacecraft Communication** **–** Spacecraft communication is an integral part of iSpace missions’ success. SpaceWire (SpW) and Proximity-1 are two communication protocols used in iSpace vehicles. SpW is a high-speed serial communication protocol where data is sent in well-formed packets, sequentially, one bit after another within subsystems of a spacecraft. An example of this can be seen in point-to-point linked communication between debris sensors and the central processing unit. This type of direct communication allows quick and reliable data transfers with low latency in cases of real-time emergencies such as collision avoidance (Ciardi, 2023). A few limitations of this communication protocol are due to the specialized hardware requirements of the serial connection between two points and their wiring. The integrity of this protocol can be disrupted if the hardware is damaged, and the protocol has a limited distance it can efficiently work through.

Proximity-1 is a communication protocol that is used during close-contact maneuvers or docking formations by satellites, spacecraft, and rovers. Proximity-1 involves a process called hailing, like a handshake, between two terminals. This protocol operates heavily on the application/data link layers and is flexible in that it allows full user control in case of emergency, improving reliability. Another implementation of this protocol is used between a rover and a nearby orbiter to send information about collected samples. The protocol offers different modes such as simplex and full-duplex mode to allow customization of data transfer rates based on mission needs (Sharma, 2014). The limitations of this protocol are like those of SpW in that it has a limited range of communication. Proximity-1 also requires monitoring to ensure the correct modes of communication are upheld.

- **Dispersed Simulation Training** **–** iSpace provides opportunities for astronauts and relevant operators to simulate real-time scenarios across different facilities. Engineers utilize the connection-less transport protocol called User Datagram Protocol within the Internet protocol architecture to send packets between applications. With UDP, applications can send encapsulated IP datagrams without handshakes (Tanenbaum, 2020). This enhances the real-time processing and transfer of bits across different applications, enabling the simulation of real-time scenarios. The downside to this technique is the lack of reliability because this protocol does not account for errors, and does not retransmit packets, leading to possible simulation inaccuracies. UDP’s connection-less quality can also lead to improper timing of packet delivery.

iSpace also uses the Real-Time Transport Protocol to support its multimedia applications. RTP sends audio and video across multiple points in packets and provides timestamps. Timestamps allow packets to be processed in the correct order and improve the chances that received audio and video are played at the correct times. RTP integrates multiple streams of data into one stream of packets. RTP supports multiple formats such as MP3 and GSM (Tanenbaum, 2020). One drawback of this technique is that it does not prioritize reliability of data transfer because it does not have built-in acknowledgement mechanisms for reception of the sent message. This can cause the simulation to be inaccurate due to frame skipping.

- **Research & Innovation Team Collaborations –** iSpace utilizes Network File System (NFS) protocols to improve collaborations between research teams and relevant implementation parties. The data gathered by these teams is held within central servers of iSpace basecamps, and authorized employees can share information regarding their specific objectives. The servers can communicate with multiple clients, allowing the clients to communicate with each other and modify existing files in coordination. NFS allows for up-to-date content daily (Flynn, 2024). An example can be seen in the case of updating existing software integrated with new hardware. Some drawbacks of NFS can be seen in cases of high overhead due to the large masses of incoming data from multiple sources. Another imperfection in this protocol is due to its centralization of data. If servers are infiltrated, attackers may have access to several pieces of information if security measures are insufficient.

iSpace network architecture implements the Session Initiation Protocol (SIP) to establish connections between multiple parties in the forms of Internet phone calls and video meetings. This can allow for efficient communication between a team lead and their associates. SIP operates on the application layer and has features such as the ability to locate callers and end the call itself. This protocol portrays phone numbers as URLs so that they can be clicked on as links within a Web page. Some messages that are sent over this protocol are ‘INVITE’ and ‘BYE’ to start and end a connection between clients. SIP is flexible because it works well with different types of applications. This flexibility can also be considered a disadvantage because different parties can set up their SIPs based on their own preferences, making it difficult to coordinate (Tanenbaum, 2020).

**- Protocol Recommendations –** The combined integration of the described protocols with relevant network firewalls can propel iSpace success by ensuring quick and efficient flow of information between different sectors of the enterprise. TCP/IP architecture enables error checked communication between iSpace functional units and its ground servers. HTTPS allows a secure connection during information exchange over the web, creating an environment where secret information can be viewed. TFTP is a reliable protocol to implement into the iSpace network because of its quick processing ability in cases of urgency. In conjunction with IPSec VPN, the two methodologies provide encryption of information during disaster recovery. In terms of spacecraft communication, SpaceWire and Proximity-1 are state of the art techniques that allow for effective data transfers between systems within a spacecraft and between satellites and rovers. To provide the best simulation tactics, the iSpace network should utilize UDP and RTP protocols. The real-time processing of data bits and synchronized packet transport allows for accurate depictions of real-world events. Collaborators within iSpace can benefit from the Network File System and SIP protocols by sharing information with each other and discussing the pros and cons of existing technologies. The overarching firewall can enhance security by directing passage of information within these protocols (Tanenbaum, 2020).

## Network Traffic Analysis and Recommendations

* **Analysis:**
  + **Data Management & Transfer –** Mission success is determined by capabilities of the iSpace distributed network to store collected information, such as information from samples gathered by a rover, and transfer that data to central ground servers for preservation. The network is used to reliably transmit analyzed data from functional units to relevant scientists and data analysts.

*Traffic Estimates:* A rover may gather 10-20 GB of sample data daily. With no delays, this data can be transmitted from the rover to a ground server within 20 seconds. Peak traffic times and levels occur after rovers have collected their terrain samples and are ready to transmit that data up to twice daily. This may include instances where multiple rovers are deployed on the same terrain concurrently and can occur at any hour of the day. Multiple transmissions of rover data can cause congestion on the network, causing limited bandwidth issues.

*Latency Requirements: <1 hour:* Bits of sample data are of high priority and require careful transmission. This category falls under bulk science data where data is accumulated and transmitted in divisions. Integrity of data is prioritized over transmission speed (Cheung, 2013).

* + **Training & Simulation -** iSpace astronauts should be prepared to execute precise evasive maneuvers in the face of disaster. The distributed network allows astronauts to be presented with accurate real-time scenarios prior to launch for human error mitigations by using real-world simulations.

*Traffic Estimates:* A 1 hour simulated training scenario requires approximately 5 GB of data transfer. At peak times where multiple teams are training simultaneously, this number may reach 10-15 GB. Congestion may occur during any scheduled training session during the workday (9 A.M. – 5 P.M.). It can also occur on the network at times where astronauts are training while research and development teams are collaborating.

*Latency Requirements: <1 second:* An accurate simulation of real-world characteristics requires latency delays of less than a second to provide astronauts with realistic scenarios (Cheung, 2013).

* + **Research & Development –** Innovation and research teams within iSpace along with third-party vendors can accumulate their ideas on dashboards and coordinate those ideas into practical implementations through a distributed network. The collaboration of multiple sectors within a network allows exponential expansion of the enterprise.

*Traffic Estimates:* Development teams may transmit an average of 2 GB of shared data between each other every hour. Peak levels range from 5-6 GB every hour during innovation intensive periods of the iSpace yearly schedule, especially during business hours (9 A.M. – 5 P.M.). The cooperation of vast datasets from multiple sources can cause high levels of congestion on the network.

*Latency Requirements:* *<5 minutes:* Effective coordination between collaborative parties requires communication and analyzation methods to be delayed no longer than 5 minutes (Cheung, 2013).

* + **Functional Unit Communication –** Rovers, satellites, and spacecraft must be able to communicate with one another with minimal delays to ensure functional unit integrity. Proper data transfer between these units is crucial in conserving important resources, and ensuring no time is wasted between critical transmissions.

*Traffic Estimates:* iSpace currently operates a fleet of 10 functional units, leading to approximately 50 GB of data transfer between them each day. Peak traffic times and levels occur in cases of collision avoidance, and other formation critical operations. This can occur any time of the day within instances such as docking formations, landing, or launching. Congestion may occur during circumstances where multiple functional units must execute evasive maneuvers concurrently to avoid hazards such as debris.

*Latency Requirements:* *<1 second:* Units must be able to coordinate movements within milliseconds to mitigate potential collisions and other related risks (Cheung, 2013).

* + **Threat Detection –** The network must be able to detect and eliminate potential threats that may attempt to steal or corrupt sensitive information collected by functional units of iSpace.

*Traffic Estimates:* The network requires approximately 1 GB per hour to account for security analyses. In cases of breach or multiple packets’ dissection, the network may require anywhere from 5-10 GB of data transfer momentarily. Peak traffic times and levels occur randomly throughout the day, especially during suspected attacks. Congestion may occur during instances of breach or at times where additional monitoring is required in cases of sensitive information transfer.

*Latency Requirements: <1 second:* Threats must be detected within milliseconds to ensure integrity of stored data within the central servers of iSpace and its functional units (Cheung, 2013).

**- Recommendations for Projected Traffic:**

* **SCaN Network Infrastructure –** The Space Communication and Navigation (SCaN) network dedicates an estimated required bandwidth between two communication points. Data traffic flows are initiated by downlinks that operate over constant bit rates, and flow over predetermined time intervals. The network uses source nodes, intermediate nodes, and destination nodes to transmit data. The network also models different data types and their transmission rates to determine max latency requirements. Using the store-and-forward techniques, sensitive data can be moved from node-to-node securely. The source node transmits data to the intermediate network node where the data is temporarily stored and can then be sent to another intermediate or its destination node. SCaN selects a minimum “pipe” size that is most suitable for efficient traffic flow between two points, estimating bandwidth. An example of implementation is seen when a spacecraft RF signal travels within range of the SCaN Network and undergoes processing and transformations of the waveform. The incoming data is decoded, and the waveform is filtered. The transmitter may use frequency-shift keying (FSK) to modulate the incoming signal. The packets are then standardized and distributed to their appropriate nodes by using headers containing routing addresses. The data is then converted back into the original transmitted bits and processed by the receiver. The store-and-forward method of the SCaN Network ensures that data is transmitted between nodes without packet loss (Cheung, 2013). Bandwidth allocation, node customization, latency management, and packet routing are just some of the features the SCaN infrastructure can provide for iSpace to ensure proper data transfer and communication between units.
* **Cisco DNA Center Software –** Distributed Network Analytics (DNA) analyzes telemetry data within the collecting device upon retrieval of that data without transmission to a different destination for analyzation. The programs within the network devices are configured to collect and analyze relevant data. The DNA Controller allows users to configure the network holistically, rather than setting up each device individually. This technique leads to the conservation of bandwidth and reduces overhead. DNA also enables adaptation to real-time circumstances (Clemm, 2015).

**- Recommendations for Potential Congestion:**

* **SolarWinds Orion Network Performance Monitor –** In order to mange potential congestion, the SolarWinds Orion Network Performance Monitor is an efficient software that can optimize performance by continuous supervision of relevant network devices such as routers. This type of NPM allows customization of communication tools such as dashboards. SolarWinds can analyze patterns of traffic and assume potential points of congestion. This also allows proficiency for future bandwidth allocation. The NPM has built-in alert systems that notify users of high bandwidth congestion which enables timely response to that congestion. These attributes make the SolarWinds Orion Network Performance Monitor a reliable method of congestion management. An example can be seen in cases where multiple rovers are collecting data concurrently.The NPM can record this congestive period and notify users to make future adjustments (Dissmeyer, 2013).
* **Paessler PRTG Network Monitor –** The PRTG offers over 284 different types of sensors that cover a multitude of network devices and hardware components. PRTG’s organizational features make it a suitable software tool for iSpace. This software can provide large data visualizations by organizing them into hierarchical groups. Each group has its own set of preferential settings. The PRTG monitor also provides visual representations of network congestion points by marking them with appropriately assigned colors representing their congestion levels. This type of monitor records historical data for sensors and devices for longer than one year, making it an effective information tool for future predictions of congestion. The PRTG also has multiple methods of notifying administrators of high levels of congestion through e-mail, SMS, and more. This monitor can also be accessed by mobile phones. These traits make the Paessler PRTG Network Monitor an effective method of managing potential congestion (The Network Business Focus, 2023).

## Network Design and Architecture

* **Infrastructure:**
* iSpace embraces an architecture akin to the Space Communications and Navigation (SCaN) distributed network. This network serves as the blueprint for all aspects of data transmission throughout the company including communication between spacecraft, information exchange between satellites and central ground servers, and user access (Cheung, 2013).
* *Hybrid Topology:* iSpace architecture integrates multiple design templates into a single, efficient architecture. The store-and-forward method can be applied with ground servers acting as central servers and satellites acting as nodes (Cheung, 2013).
* *Network Flow:* Information collected by spacecraft can be stored temporarily in the data stores within the spacecraft and transmitted to intermediate satellites which then send that data to ground servers. Authorized users on the network can access this data.
* *Advantages:* This type of network architecture allows for efficient storage of information over vast aerospace distances. This network also enables data exchange between ground servers over large geographical distances using intermediary satellite transmissions. Information collected by iSpace functional units can be distributed across multiple servers, enabling redundancy and scalability with future addition of functional units.
* A diagram of a network

  Description automatically generated**Network Diagram:**
* **System Design Justification**
* *Data Collection & Management:*
  + Central data servers (central nodes) across the globe containing massive data storage systems can hold terabytes of information collected by their respective functional units. This data is stored and accessed securely and efficiently.
  + Network switches active within distributed server facilities enable real-time processing and minimized latency during incoming traffic from satellites to servers, and during the process of multiple users accessing that information.
  + Satellites (intermediate nodes) act as the middleman during transmission of collected data by functional units. Using store-and-forward mechanisms, data is transferred from one store to another quickly and without packet loss (Cheung, 2013).
* *Disaster Recovery:*
* The storage of data across multiple nodes ensures redundancy of the overall system in the case of single-point failure. The data can be copied and moved to multiple locations.
* Satellites communicating with more than one server at a time allows alternative methods of data transmission in case of disaster. Protocols such as the trivial file transfer protocol allow for data replication in cases of emergency (Mohamed, 2018).
* *Spacecraft Communication:*
* Antennas of satellite dishes within ground stations of iSpace enable real-time communication with satellites while maintaining high-bandwidth information transfer.
* Orbital satellites are in constant contact with spacecraft and ground stations simultaneously, allowing a steady stream of data flow.
* RF Transceivers positioned strategically in facility grounds and on spacecraft enable continuous transfer of information using the store-and-forward technique (Cheung, 2013).
* *Dispersed Simulation Training:*
* Central ground servers can hold gigabytes of simulation-related data, and multiple users can train simultaneously using this information.
* Network switches supporting real-time data transfer ensure all simulations are provided to trainees with minimal latency, and that those simulations are accurately updated to current standards or objectives.
* *Research & Innovation Team Collaboration:*
* Massive storage centers containing research data can be accessed by users anywhere on Earth.
* State of the art orbital satellites and efficient network switches coordinate quick communication and sharing of ideas between collaborators.

(Continued)

***Estimated Cost***

|  |  |
| --- | --- |
| 3,000 User Terminals \* $1,500 | ~ $4,500,000 |
| 3 Ground Central Servers \* $300,000 | ~ $9,000,000 |
| 3 Network Switches \* $30,000 | ~ $90,000 |
| 3 RF Transceivers \* $25,000 | ~ $75,000 |
| 3 Satellite Dishes \* $80,000 | ~ $240,000 |
| 3 Satellites \* $55,000,000 | ~ $165,000,000 |
| 2 Spacecraft \* $600,000 | ~ $1,200,000 |
| Total | ~ $180,105,000 |

(*NASA Cost Estimating Handbook)*

* **Software:**
* User terminals operate on Windows 10. iSpace ground servers operate on Linux, and iSpace functional units are embedded with Linux-based real-time operating systems (LRTOS). The LRTOS enables real-time multiprocessing capabilities and enhances reliability through fault tolerant mechanisms. The operating system must be able to react swiftly to external events.
* SolarWinds Orion Network Performance Monitor: This NPM is a software tool designed to observe and mitigate potential congestion throughout the iSpace network. It includes features such as built-in alert systems to notify users of high traffic levels. SolarWinds can also help predict future instances of congestion points. It can manage large quantities of incoming data. SolarWinds reduces downtime by identifying problem areas efficiently. By supervising bandwidth usage, effective spacecraft and research team communication is stabilized. Simulations for trainees are rarely interrupted due to the monitor’s continuous observation (Dissmeyer, 2013).
* Microsoft 365 and Google Workspace are effective tools for collaboration amongst research and development teams.
* MySQL has open-source features that support distribution of information. MySQL is flexible in that it is compatible with several platforms.

***Estimated Cost***

|  |  |
| --- | --- |
| Windows 10 (3,000 users) | ~$600,000 |
| SolarWinds Orion NPM | ~$3,000 |
| Microsoft 365/Google Workspace | ~$500,000 annually |
| Linux Server Systems: 3 \* $3,500 | ~$10,500 annually |
| Total | ~$1,100,000 at startup |

## Future Needs Analysis and Recommendations

* + *Machine Learning*
    - Implementation of machine learning techniques in iSpace distributed systems enhances the ability of the corporation to monitor future securities, network scheduling, and traffic patterns with strict supervision. Pinpointing and controlling key points of congestion through use of artificial intelligence and appropriate machine learning algorithms allows iSpace to allocate its resources efficiently.
    - *ML Workflow:* The typical machine learning workflow in the iSpace network involves 6 steps: 1) Problem Formation – predicting and clustering important bits of information into related groups, such as rover samples and satellite imagery 2) Data Collection – using traffic tracers and collecting performance logs to gather historical references for future model input 3) Data Analysis – preprocessing and feature extraction to monitor patterns and remove unnecessary data or bits that have been corrupted during transmission 4) Model Construction – training and finetuning a model to find optimal parameters for resource allocation and prediction of future congestive points, especially during mission operations 5) Model Validation – the model is checked for errors and instances where more effective algorithms may be used 6) Deployment & Interference – speed tradeoffs and stability are supervised by engineers to ensure the system is functioning optimally.
    - *Design & Architecture Modifications:* The following are mechanisms to be inherited by iSpace architecture to enhance mission requirements: 1) CS2P – Cluster-based Session-level throughput Prediction is used to improve audio/video QoE with its dynamic features that adjust bitrates based on the current system state. 2) Cherrypick – the Cherrypick technique utilizes the Bayesian Optimization algorithm to decrease the number of test runs required to find an optimal model preference by adjusting model configurations to minimize latency and maximize throughput. Coordination of the iSpace Transmission Control Protocol with REMY, a reinforcement-based machine learning technique, optimizes congestion control by adjusting the congestion window size based on current transmission conditions. REMY congestion control supports satellite and spacecraft communication by predicting sufficient communication rates and windows.
    - *Advantages:* ML enhances iSpace distributed network architecture by reducing testing costs, offering continued autonomous adjustments based on the network state, and allocating resources such as bandwidth efficiently.
    - *Challenges:* In a dynamic aerospace environment, it may be difficult for artificial intelligence to predict the next most effective outcome if there is no historical data regarding the current state of the system. The design of ML techniques may not be feasible due to their high computational loads (Wang, 2017).
* *Quantum Computing*
* Quantum Computing throughout iSpace’s distributed network allows for parallel data processing, improved sensing capabilities, and optimization of mission plans through analysis of trajectories.
* *Quantum Internet:* The Quantum Internet applies the principles of quantum mechanics to iSpace computational abilities. Using qubits, satellites and ground servers can communicate with high levels of security and reliability. Qubits can process massive amounts of information compared to classical bits due to their superposition states. This allows enhanced real-time calculations done by spacecraft and satellites.
* *Design & Architecture Modifications:* Quantum Key Distribution (QKD) enables secure transmission of information between iSpace functional units at large distances. A third party attempting to access private information disrupts the quantum states of the transmitted qubits, alerting relevant authorities of intrusion. Quantum Teleportation involves encoding (destruction) of the qubit along with its entanglement-pair and reconstruction of the state of the qubit at the destination. The process utilizes an entanglement generator, two quantum nodes, two measurement devices, and two quantum memory nodes in coordination with a quantum link that uses a classical link as a template. The following layers of the iSpace network must be modified to accommodate quantum processing:1) The physical layer must be configured such that quantum generators and receptors are located on each of the iSpace functional units. Shorter transmissions suffice through free-space transmission, while large distance transmissions require antennas equipped with kilometer-long optical fibers 2) The link layer must be configured to accommodate multiplexing techniques for channel sharing through frequency and time parameters. The QKD mechanism is applied at this layer. 3) The network layer must be configured to route photons appropriately along the correct paths. This includes implementing alternate resource allocation algorithms and mechanisms that support quantum routing protocols
* *Advantages:* iSpace experiences nearly impenetrable communication through quantum communication channels. The superposition principle allows *n* qubits to encode all 2^n possible states simultaneously. Multiple satellites and ground servers contain equivalent information due to photon entanglement, enabling redundancy and multiplied parallel processing capabilities.
* *Challenges:* The integration of quantum mechanics into existing distributed systems is a recent development, and therefore its implementation in iSpace architecture poses risk of data corruption. The cost of resource input involving computational load may outweigh the benefits of speed and reliability (Cacciapuoti, 2019).
* *Network Virtualization*
* iSpace reduces the cost of multiple machines by utilizing Software-Defined Networking (SDN) and Software-Defined Wide Area Networking (SD-WAN). The local area network (local network switches and routers) is supported by network virtualization through means of centralized control. The wide area network is supported by network virtualization through means of bandwidth allocation amongst centralized servers across the globe.
* *Software-Defined Networking:* SDN implements network slicing which stacks multiple virtual networks on top of a physical machine network. Each of these slices can be configured with preferences depending on their performance requirements. For example, one slice can manage incoming phone call traffic while another slice is responsible for maintaining strong data transfers.
* *Software-Defined Wide Area Networking:* SD-WAN allows for quick adaptation to the current system state. Bandwidth allocation to crucial data transfers such as data collected by a satellite can be prioritized using software that dictates packet paths, ensuring minimized congestion throughout the distributed network.
* *Design & Architecture Modifications:* OpenFlow enables a centralized controller to act as the director of switch and router behavior. These specificities can be programmed into the controller to optimize traffic flow within software-defined networking. Traffic steering mechanisms within software-defined wide area networking ensure mission crucial information is passed on with high prioritization and low latency. Increased virtualization requires increased authentication controls and supervision of the system to mitigate errors and threats. Traffic shaping and other QoS mechanisms must be employed to balance the workload of multiple virtual machines acting on a single network, especially within the LAN of a centralized data server (Tanenbaum, 2020). Training of relevant employees involves constant updates on evolving technologies such as cloud computing.
* *Advantages:* Network resource management by a centralized control plane enables rapid switching and forwarding of packets depending on their importance and the current system traffic levels. The separation of the control plane from the data plane allows flexibility of virtual network function nodes by catering their settings to simplify network and control operations (Kim, 2020).
* *Challenges:* Compatibility between third-party vendors of applicable hardware must be carefully evaluated to ensure coordination between relevant software controllers. The integration of network virtualization with AI/ML expands the frontiers of the aerospace industry, leaving room for new errors.

## References

Cacciapuoti, A. (2019, November 22). Quantum Internet: Networking Challenges in Distributed Quantum Computing. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/8910635

Cheung, K.-M. (5 C.E., Spring). Coarse-Grain Bandwidth Estimation Techniques for Large-Scale Network. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/6496881

Ciardi, R. (2023). SpaceART SpaceWire Sniffer for Link Monitoring: A Complete Communication Analysis in a Time-Constrained Test Scenario. Sensors, 23(3), 1580–1580. https://doi.org/10.3390/s23031580

Clemm, A. (2015, February 7). DNA: An SDN Framework for Distributed Network Analytics. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/7140450

Comins, N. F. (2017). The Traveler’s Guide to Space: for One-way Settlers and Round-Trip Tourists. Columbia University Press.

Dissmeyer, J. (2013). SolarWinds Orion Network Performance Monitor. Packt Publishing Ltd.

Flynn, D. (2024). Overcoming Performance Bottlenecks with a Network File System in Solid State Drives. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/10224581

Kim, Y. (2020). A Location‐Aware Network Virtualization and Reconfiguration for 5G Core Network Based on SDN and NFV. International Journal of Communication Systems, 34(2). https://doi.org/10.1002/dac.4160

Larsson, D. (2021, October 5). Cisco Learning Network. Learningnetwork.cisco.com. https://learningnetwork.cisco.com/s/article/Brief-Architecture-Overview-to-understand-Cisco-s-DNA-Architecture

McKenna, E. (2013, April 1). Real-Time Operating Systems. Aviation Today. https://www.aviationtoday.com/2013/04/01/real-time-operating-systems/

Mohamed, N. N. (2018). Extending Hybrid Approach to Secure Trivial File Transfer Protocol in M2M Communication: A Comparative Analysis. Telecommunication Systems, 70(4), 511–523. https://doi.org/10.1007/s11235-018-0522-5

Nam, T. S. (2022). A High-Throughput Hardware Implementation of NAT Traversal for IPSEC VPN. International Journal of Communication Networks and Information Security (IJCNIS), 14(1). https://doi.org/10.17762/ijcnis.v14i1.5260

NASA Cost Estimating Handbook (CEH) - NASA. (n.d.). https://www.nasa.gov/ocfo/nasa-cost-estimating-handbook-ceh/

Paessler PRTG Network Monitor 22.4. (2023, April). The Network Business Focus, 342, 89–90.

Ribeiro, L. (2014, May 19). A Framework for Dimensioning VDL-2 Air-Ground Networks. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/6820012

Sharma, A. (2014). Development of CCSDS Proximity-1 Protocol for ISRO’s Extraterrestrial Missions. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/6968319

Stallings, W. (2017). Operating Systems: Internals and Design Principles (9th ed.). Pearson Education (US). https://coloradotech.vitalsource.com/books/9780134700113

Tanenbaum, Andrew, S. et al. Computer Networks. Available from: Colorado Technical University (CTU), (6th Edition). Pearson Education (US), 2020.

Wang, M. (2017, November 28). Machine Learning for Networking: Workflow, Advances and Opportunities. Oclc.org. https://ieeexplore-ieee-org.coloradotech.idm.oclc.org/document/8121867