TECHNICAL WHITE PAPER

SatSafe is a fully auditable satellite technology that automates patch management and broadcasts critical security updates and data content

Are your Systems secured?

“The need to deploy faster patch management solutions, and other technologies comes from the incredible shrinking window between vulnerability and exploit. The window is getting tighter, and as it does, that forces users to be more aggressive in how they deploy a patch.” - *Mark Nicolette, Gartner*

Why Patching is so critical

It is essential to update the operating system, security software, and all other programs on computers on a regular basis. Patching systems and programs is crucial to preventing malware from infiltrating computers. Unpatched programs are an ideal entry point for an attack.

How to effectively control and sustain Patch Management

To combat the threat of new and existing malicious code, multiple security products are deployed at different points in an organization. This is performed to ensure that malicious content is stopped before it can cause harm to the network. However, in order to sustain an effective and healthy environment, the products deployed need to be constantly updated. ***This applies specifically to updates from multiple vendors across different product versions and platforms.***

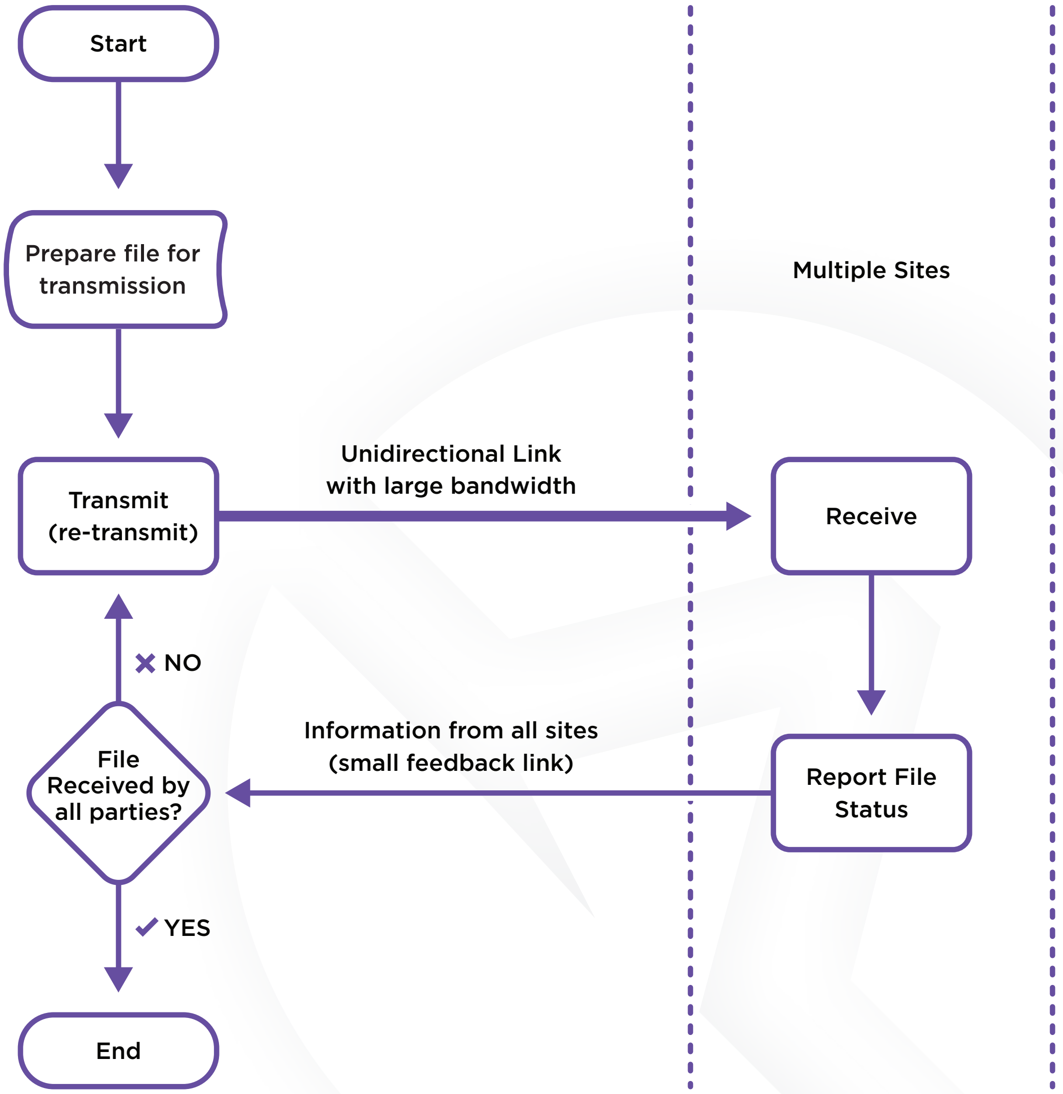
Current security update deployment mechanisms utilise **Pull Technologies**, a reactive measure to combat security system and network threats. These technologies are not capable of addressing new threats timeously, this is especially evident in respect of the size and frequency of today's Anti-Virus and Microsoft Operating System updates.

The only way to safely control the threat of malicious attacks on today's complex networks is through the use of **Push Technology**, a proactive, automated technology that updates security systems in real-time, as utilised by the Internationally Patented **SatSafe** system. (International Patent No. PCT/IB2004/0027b2.)

How SatSafe works

SatSafe provides the ultimate protection from computer malicious code through the use of "state-of-the-art" satellite communications technologies. Once a threat or vulnerability is identified, products deployed on a network to combat malicious code are automatically updated faster than ever previously possible. Security systems are updated as the patches are released, ensuring that systems are protected as soon as a new threat or vulnerability emerges.

How Satsafe Works


Start
Prepare file for transmission
Multiple Sites
Transmit (re-transmit)
Unidirectional Link with large bandwidth
Receive
✗ NO
File Received by all parties?
Information from all sites (small feedback link)
Report File Status
✓ YES
End

SATSAFE

Intrusion Detection:

Host based vulnerability scanning

There are various automated host scanning tools available to assist organisations in ensuring that their systems are protected, in the on-going cyber war.

These tools automatically scan systems and services on the network and safely simulate common intrusion or attack scenarios exposing vulnerabilities before intruders can exploit them and attack.

These systems help to secure an organization's networks by ensuring that they are protected against the latest exploits and vulnerabilities that a potential hacker would have available.

New system vulnerabilities are discovered in Internet time. It is essential to act proactively and protect the information infrastructure timeously against destructive malware.

SatSafe delivers and installs updates for existing Host based vulnerability scanning systems. This ensures that network security specialists are able to protect their systems in the shortest time possible.

The SatSafe Process

1. The Security vendors' private Internet sites are monitored 24 hours a day, 365 days a year for new security updates. On availability, SatSafe immediately downloads and packages the data for distribution via satellite.

2. The packaged updates are uploaded for broadcast at a satellite uplink centre in the UK.

3. New updates are broadcast via satellite around the clock, as a one way UDP multicast.

4. New updates are received simultaneously by all Decoders within seconds of being broadcast.

5. SatSafe utilizes asymmetric encryption to ensure the highest level of security is maintained. All data received by the Security Decoder are validated with digital signatures.

6. The Security Decoder automatically demodulates new updates, publishes them, and sends delivery confirmation.

7. The Security Decoder can be configured within various firewall architectures.

8. Servers that require updates, communicate with the Security Decoder via passive mode SMTP. When new updates are detected, the SatSafe Communications Agent, which runs as a Windows service, requests the files. The appropriate SatSafe update agent is then installed and successful installations are logged.

9. Each Security Decoder has a web based management interface, allowing easy access to configuration, settings and a log of the successful installation of updates. All nodes on the network are continually monitored via their connection status for rapid troubleshooting and remediation.

Powerful Integration and Efficient Performance Functionality

SatSafe in partnership with ***Microsoft and Symantec*** provides the most comprehensive set of administrator tools that ensure 'peace of mind through simplicity', in the market today.

The Configuration Manager continues to simplify the complex task of delivering and managing updates to IT systems across an enterprise.

In addition, the Configuration Manager **monitors and evaluates** clients' health status across client environments. It displays client health evaluation results and the client activities directly in the Configuration Manager Console, providing alerting and remediation capabilities in the event that health statistics fall below established thresholds.

SatSafe in conjunction with the Microsoft System Centre Configuration Manager facilitates and accelerates administration of client systems and provides improved visibility and enforcement options for maintaining system compliance.

The following features highlight SatSafe's functionality:

- ***SatSafe*** delivers 'world-class': data inventory; operating system deployment; update management assessments; and settings enforcement—with exceptional support for Windows
- ***SatSafe*** facilitates the organization of 'day-to-day', administrative tasks, making it possible for administrators to define one application for delivery across multiple devices
- ***SatSafe*** provides continuous settings enforcement to automatically identify and remediate non-compliant machines

High-level System Overview

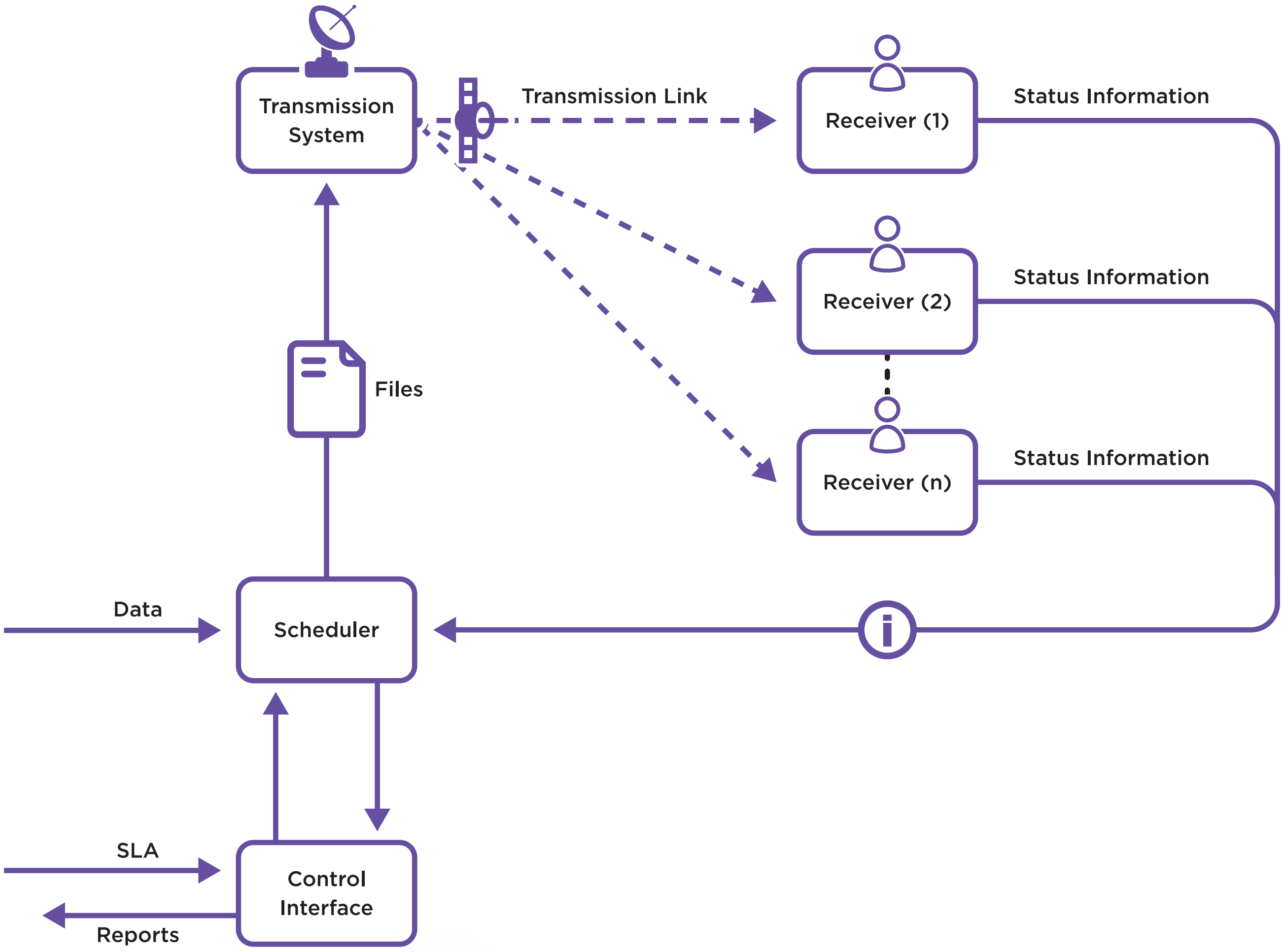


***Figure 1**: High-level System Diagram of the SatSafe Delivery System*

The High-level System Diagram for SatSafe is illustrated in ***Figure 1***. The dominant components of the system are detailed hereunder:

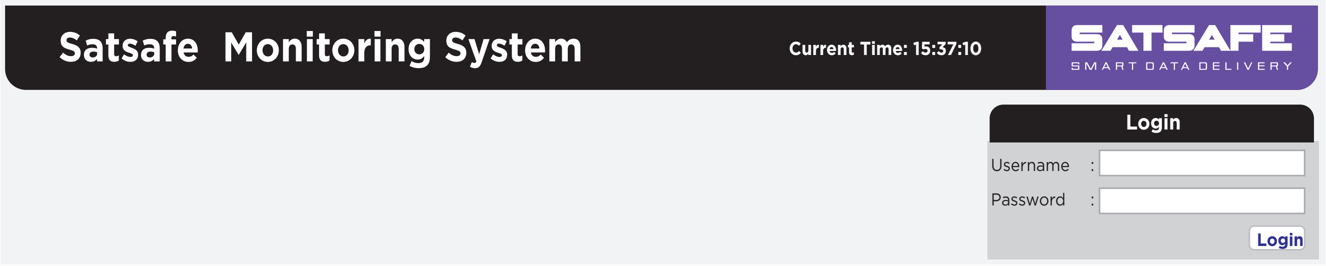
1. the Transmission System
2. the Transmission Link (**Link A**),
3. the Receiver Components (duplicated at each client)
4. the Status Links (**Link B**)
5. the Scheduler
6. the Control Interface

The SatSafe client interface comprises of information that is gathered from the following criteria:

1. the Service Level Agreement (SLA)

2. the client's data (for distribution to all the client's sites)

3. the corresponding System Status and Audit Reports



Satsafe Monitoring System

Current Time: 15:37:10

Login

Username :

Password :

Figure 2: SatSafe Client Monitoring Interface

The SatSafe system is designed to function over “one-way multicast stream technology” to allow the system to transmit files via one-way satellite systems. Satellite technology allows Link A, the transmission link, to broadcast substantial amounts of data to a wide variety of clients over a large geographical area, reliably and expediently.

Link A is one-directional utilizing the UDP protocol. There are two primary security benefits associated with the UDP protocol:

A) UDP does not require "Hand-shaking" or the ability to have two-way communication, thereby securely expediting critical updates without requiring acknowledgment from the network, a process that would severely delay update installation.

B) UDP is a one-way transmission protocol that eliminates the possibility of interception, masquerading and man-in-the-middle-attacks commonly perpetrated via the TCP/IP protocol.

Monitoring and Control Status Information is relayed back to the Scheduler and Control Modules via a second independent one-directional link **Link B, the status link.** As the amount of status information that is returned via Link B, is substantially smaller than the transmission data sent via Link A, the system is considered asymmetrical. Security requirements necessitate that Link B is half-duplex, only returning status information back to the monitoring system, as a full-duplex link could pose a possible security threat to the clients' environment.

The status information received via Link B completes the feedback loop. This information allows the broadcast system to monitor the status and compliance of all of the clients in the system. This is necessary for the service provider operating the service to comply with specific Service Level Agreements (SLA).

Transmission System & Receiver Components

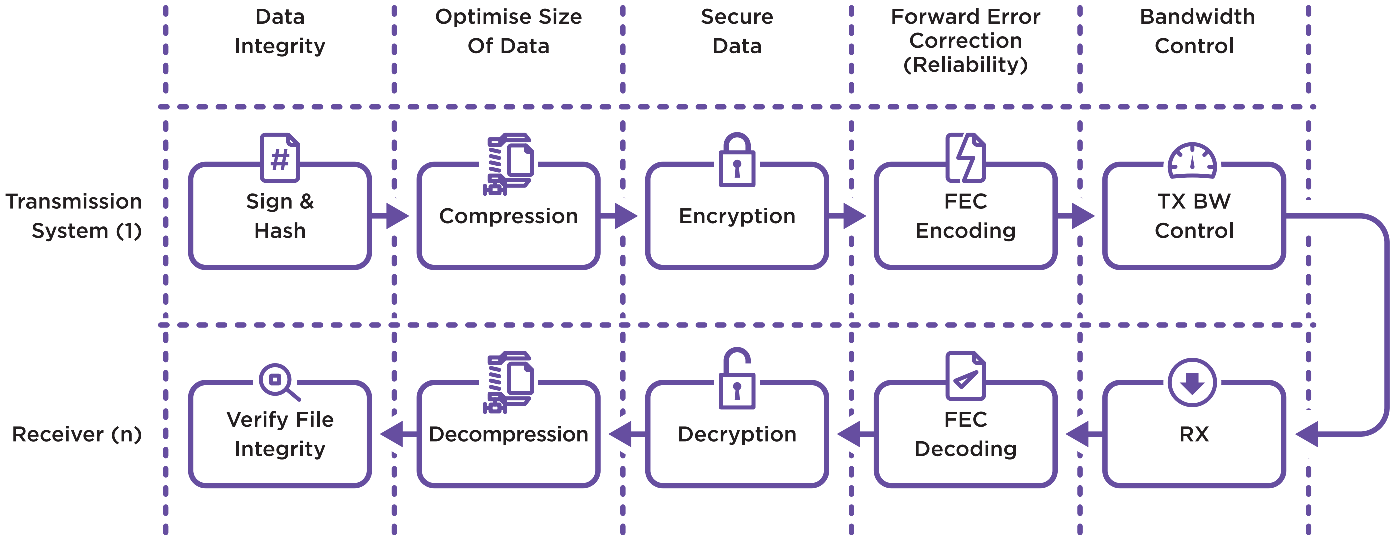


Figure 3: Overview of unidirectional information feedback system

The Transmission System is responsible for modifying and broadcasting transmission files so that they are received by the selected receivers within the client's environment(s). The Scheduler then determines the files that are required to be sent.

Before data is transmitted over Link A, it is modified by the system to ensure that it can maximize the manner in which it utilizes the bandwidth available over Link A. The sequence in which SatSafe performs the relevant data manipulation is illustrated in '***Figure 3: Overview of unidirectional information feedback system***'.

The process consists of 5 defined steps, namely:

1. **Signing and Verification (Data Integrity)**

2. **Data Optimization (Compression and Decompression)**

3. **Data Security and Privacy (Encryption and Decryption)**

4. **Forward Error Correction (Reliability)**

5. **Bandwidth Control and Optimization**

File Verification and Data Integrity:

Data integrity is the assurance that all the data in the system is consistent, certified and can be reconciled. In compliance with the discipline of data architecture, when functions are performed on the data, the functions ***must ensure integrity***.

Ensuring that the data received at all of the selected receiver sites is correct is essential in terms of the **four required core attributes for data integrity namely**:

1. **Completeness**
2. **Currency / Timeliness**
3. **Accuracy / Correctness**
4. **Validity / Authorization**

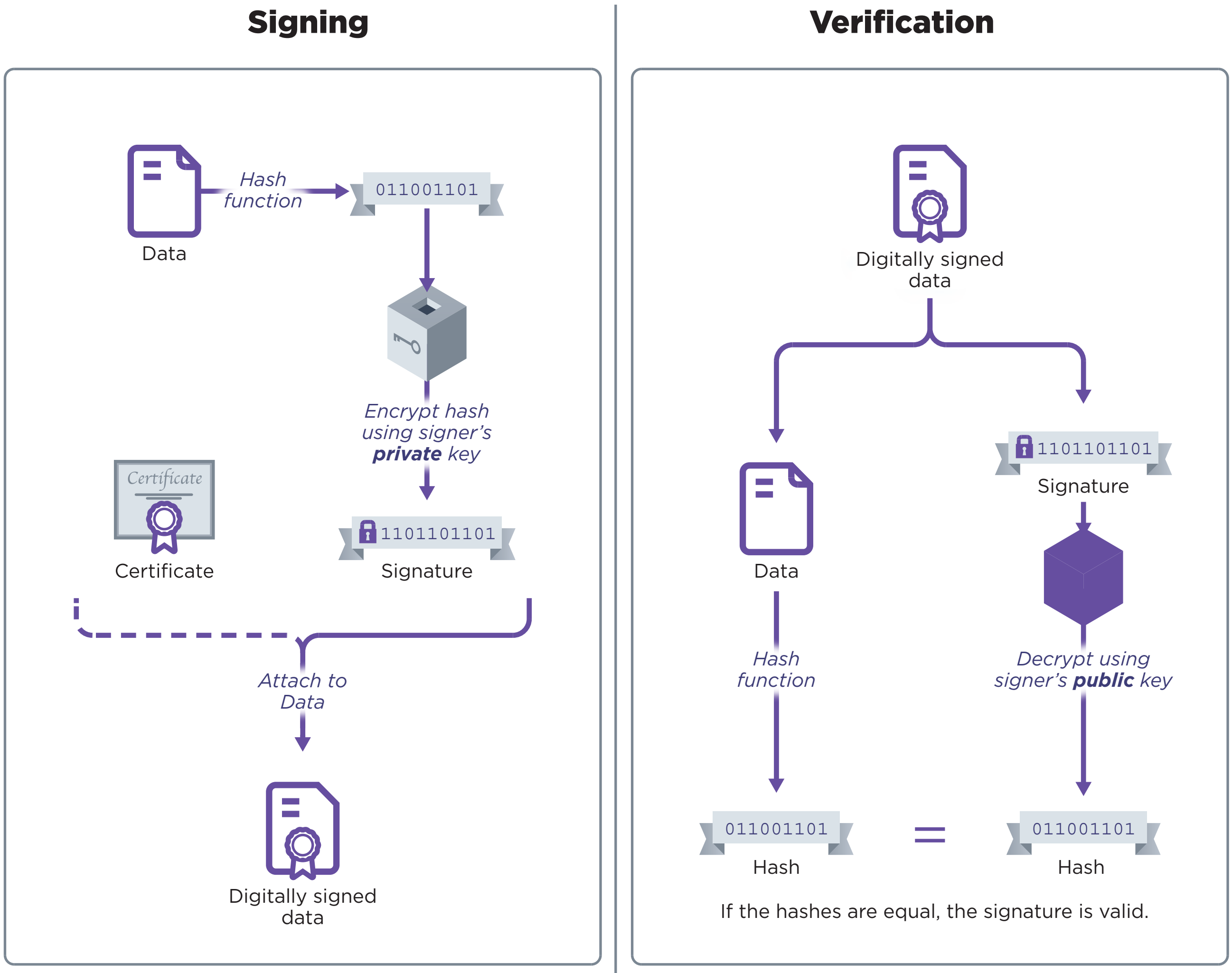


Figure 4: Digital Signing Procedure [1]

SatSafe verifies the integrity of the data during transmission via hash values and digital signatures.

A file-hash is calculated together with the digital signature. The digital signature scheme is to ensure authenticity of the received files. A valid digital signature provides confirmation to the receiver that the message/file conforms to the following instructions:

1. Created by a known sender
2. Not altered in transit
3. Not corrupted during the transmission process

The process by which the digital-signature is created is illustrated in '***Figure 4: Digital Signing Procedure***'.

- It is utilized for the file distribution system to ensure that the platform can detect forgery or tampering of the data

- A file-hash system is integrated into the transmission system as an assurance that the final file that is received at each of the clients, ***has arrived complete***.

The check-sum of the received files from each receiver is sent back to the transmission server, which in turn compares it to the original check-sum. If the sums differ, this information is used by the scheduler to re-transmit the data to the relevant parties ***as many times as is required for the receivers to receive the correct information and to ensure data integrity across the entire platform.***

Digital File Verification Process

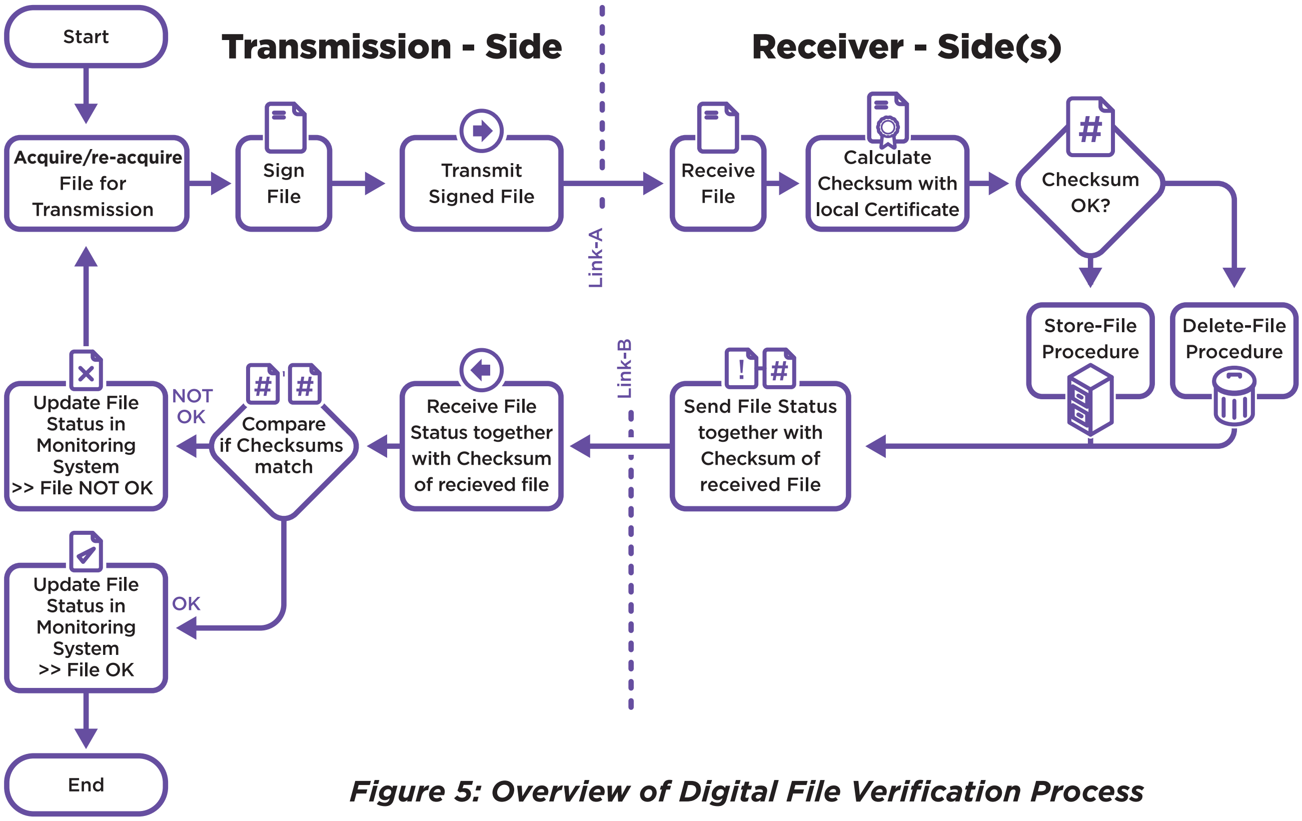

Start
Transmission - Side
Receiver - Side(s)
Acquire/re-acquire File for Transmission
Sign File
Transmit Signed File
Link-A
Receive File
Calculate Checksum with local Certificate
Checksum OK?
Store-File Procedure
Delete-File Procedure
Send File Status together with Checksum of received File
Link-B
Receive File Status together with Checksum of recieved file
Compare if Checksums match
NOT OK
Update File Status in Monitoring System >> File NOT OK
OK
Update File Status in Monitoring System >> File OK
End

Figure 5: Overview of Digital File Verification Process

Compression

Compression assists in reducing the transmission bandwidth requirements for Link A. At the receiver's end, the compressed data is decompressed for use. The design of data compression schemes involves trade-offs among various factors, including the degree of compression and the amount of the computational resources that are required to compress and decompress the data. SatSafe Forward Error Correction technology ensures the integrity of data while gaining efficient bandwidth utilization through compression.

Most of the data transmitted over the SatSafe system has already been compressed. Any increase to the file size is minimal. At this stage, the compression scheme is included in order to provide a means of easily attaching file names and data as headers for data transmission.

Forward Error Correction

As the satellite transmission system is required to perform reliably under unfavorable weather conditions, the SatSafe system implements the following pre-requisites:

1. Hybrid Automated Request (HARQ) System
2. Forward Error Correction (FEC) codes (erasure codes)

The SatSafe transmission occurs over a satellite link, provisioning for Forward Error Correction (FEC) or channel coding is therefore required. FEC is used to correct and control errors in data transmission over unreliable or noisy communication channels, t***o ensure that the satellite system remains reliable and resistant to transmission error***.

A carefully designed redundancy allows the receiver to detect a number of errors that may occur anywhere in the message. ***The receiver can correct these errors by using redundant information without requesting re-transmission***. FEC gives the receiver the ability to correct errors without needing a reverse channel to request re-transmission of data. ***FEC is therefore applied in situations such as stormy weather conditions where re-transmission to multiple receivers can be challenging.***

Forward Error Correction

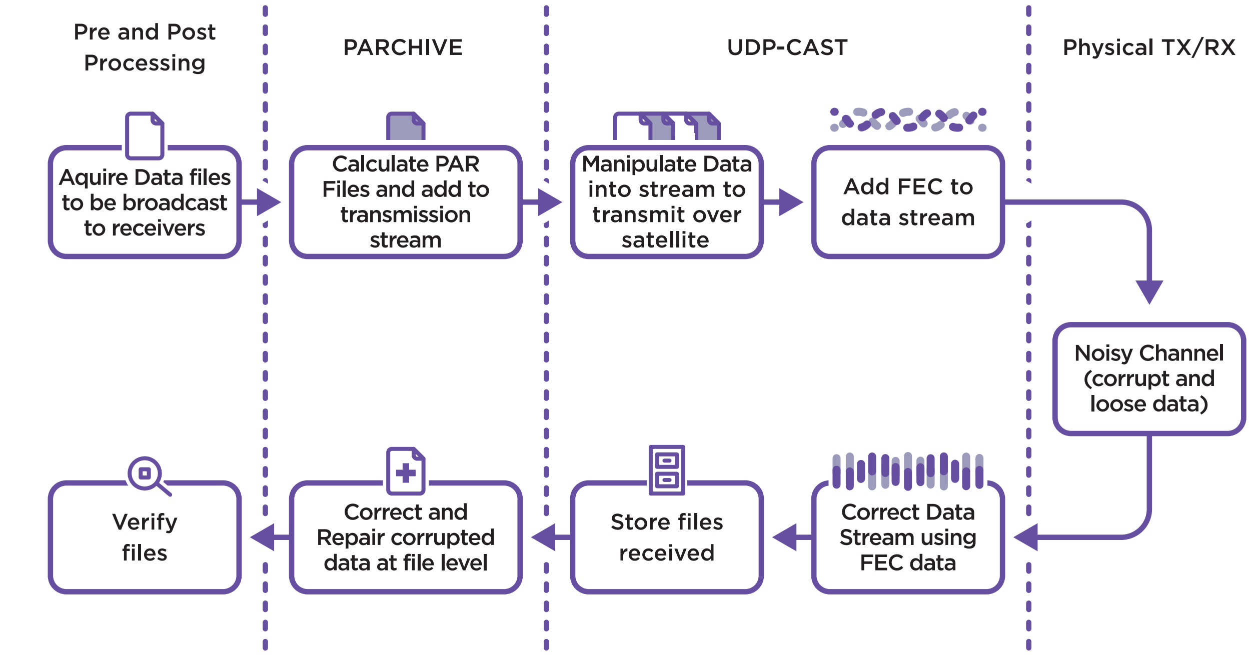

Pre and Post Processing
PARCHIVE
UDP-CAST
Physical TX/RX
Aquire Data files to be broadcast to receivers
Calculate PAR Files and add to transmission stream
Manipulate Data into stream to transmit over satellite
Add FEC to data stream
Noisy Channel (corrupt and loose data)
Correct Data Stream using FEC data
Store files received
Correct and Repair corrupted data at file level
Verify files

Figure 6*: *Overview of Forward Error Correction

Two types of FEC are implemented at different data levels, ***to ensure that minimal re-transmission of data is required over Link-A***. The process is illustrated in ***Figure 6: 'Overview of Forward Error Correction'.***

- At a lower level, FEC is added to the bit-stream that is broadcast over Link-A. This permits the system to compensate for errors introduced during the transmission over the satellite link. This is achieved using UDP-Cast.
- At file-level, the system adds “File-Level” FEC. This is performed using Parchive. It uses parity files which also use a forward error correction-style system that can be used to perform data verification, and allow recovery when data is lost or corrupted.

UDP-Cast allows the user to configure the forward error correction according to requirements. The software allows the user to add FEC to each data segment as well as interleave and increase performance of the FEC-Data in the stream. A variable "Interleave" is configured in order to offer better protection against burst packet loss, when many consecutive packets are lost. Higher interleave spreads the FEC data over a longer period of time and introduces latency to the system.

With the introduction of Parchive, parity files are created and uploaded along with the original data files. If any of the data files are damaged or lost during the broadcast to the receivers, the parity files are used to reconstruct the damaged or missing files. In the event that the reconstruction of files is not possible, packets are re-transmitted from the uplink.

These files are then decompressed and verified by the system according to the digital signature processes described in the previous sections.

Bandwidth Control

The transmission bandwidth is implemented and controlled using UDP-Cast. To improve the default functionality that is housed within the UDP-Cast software, a UDP Block has been implemented for additional functionality to enable file-monitoring, multiple instances, additional logging including statistics and errors.

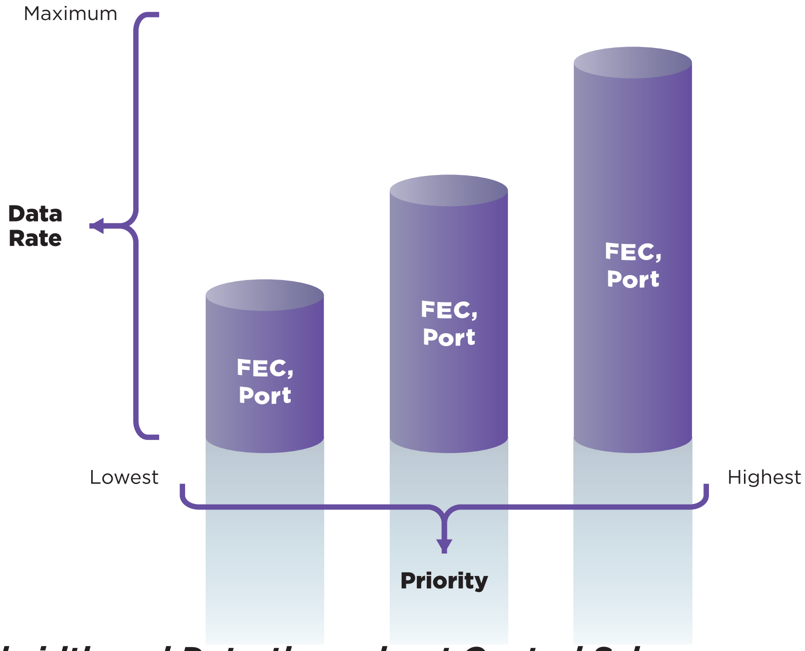


Figure 7: Bandwidth and Data-throughput Control Scheme

Multiple connection instances are required for the system to be able to send multiple files simultaneously. This allows different data sources to be transferred over Link-A at the same time with different bandwidth restrictions. These requirements are controlled by the Scheduler as per the relevant Service Level Agreements, allowing each data-set to be throttled. The effect is illustrated in '**Figure 7: Bandwidth and Data-throughput Control Scheme' above**.

Each connection transmission stream therefore has an associated data rate and FEC –setting (Data Stream Level). A variable FEC-setting enables low priority “running in the background” data to have optimized error correction if the broadcast times are longer.

An alternating port number scheme also enables more data to be compressed into the same amount of time. This is illustrated in '**Figure 8: “A short delay between consecutive UDP-Cast calls waists Bandwidth**” and ‘**Figure 9:** ‘**Figure 9:** “**Multithreading Bandwidth Scheme**”. Using the existing UDP-Cast software on a single port does not allow consecutive connections to be established immediately.

This produces a small time delay for files that are sent to each other. The effect is exaggerated when sending many small files, where the delay can be longer than the time it takes to send the file.

By implementing an alternating port scheme, a second connection is opened immediately after the first connection is closed by the transmission system, ***without any risk of losing data packages***. This allows the system to use all of the available Bandwidth.

Alternating Port Scheme

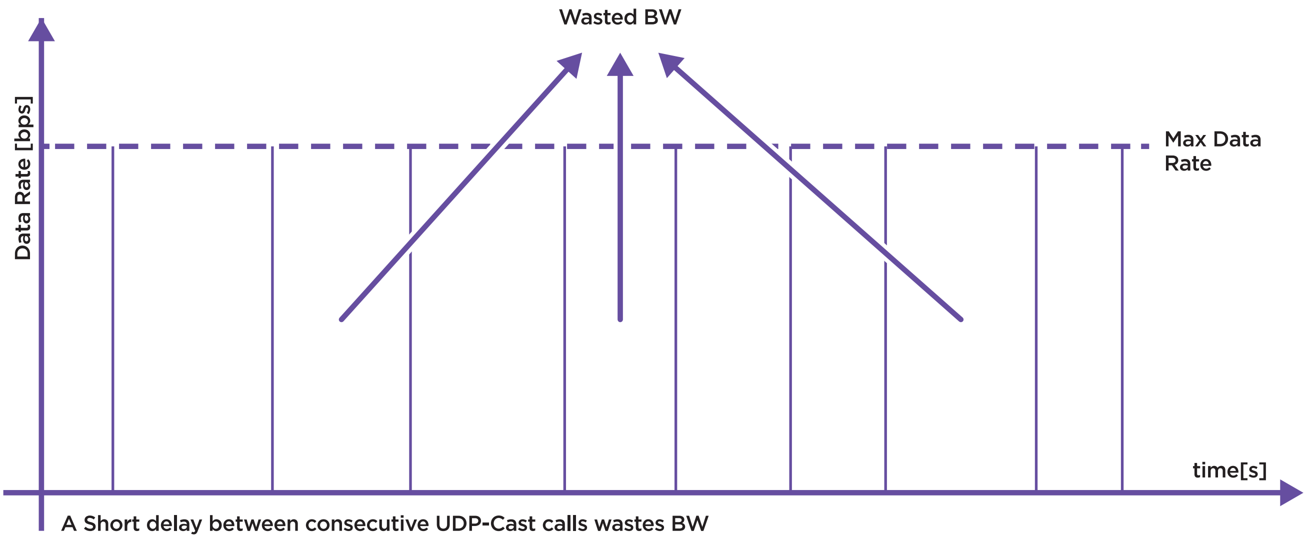


Figure 8: Short delay between consecutive UDP-Cast calls wastes BW

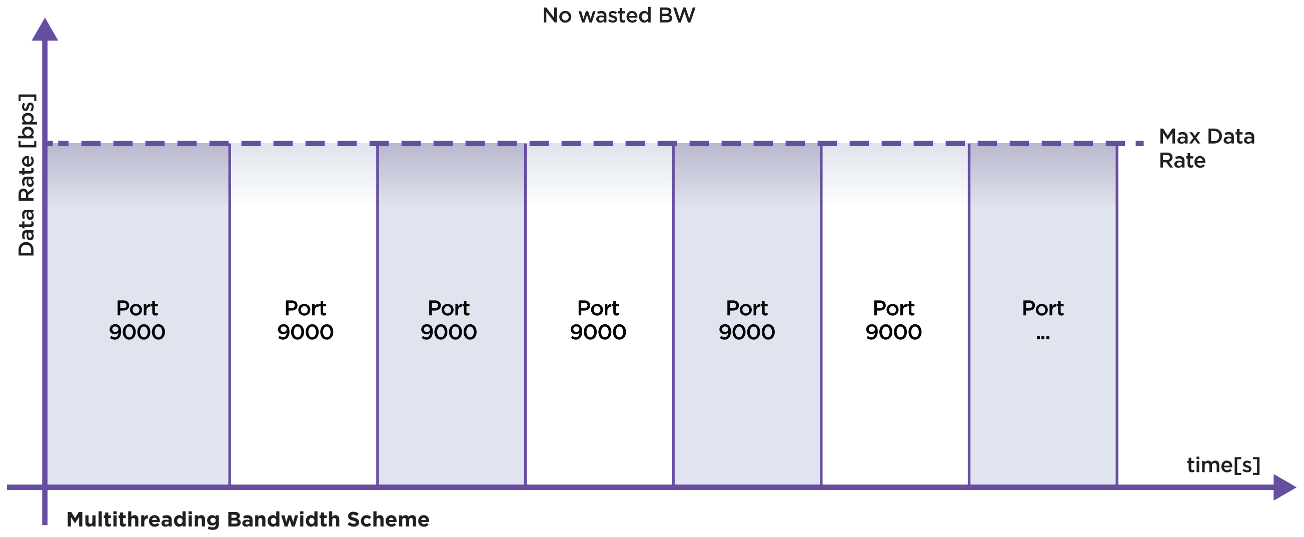


Figure 9: Multithreading Bandwidth Scheme

Transmission Link (Link-A)

The transmission link is initiated by the sender. This link is also known as the Electronic Program Guide (EPG). The Electronic Program Guide is a message that tells the receiver which files it expects to receive and how the files are handled. Some of the information incorporated in this link includes Queue ID, Validity, Timeout, and the Update type ID. The Sender notifies the web server of the files that have been queued for sending as well as the date and time they were queued.

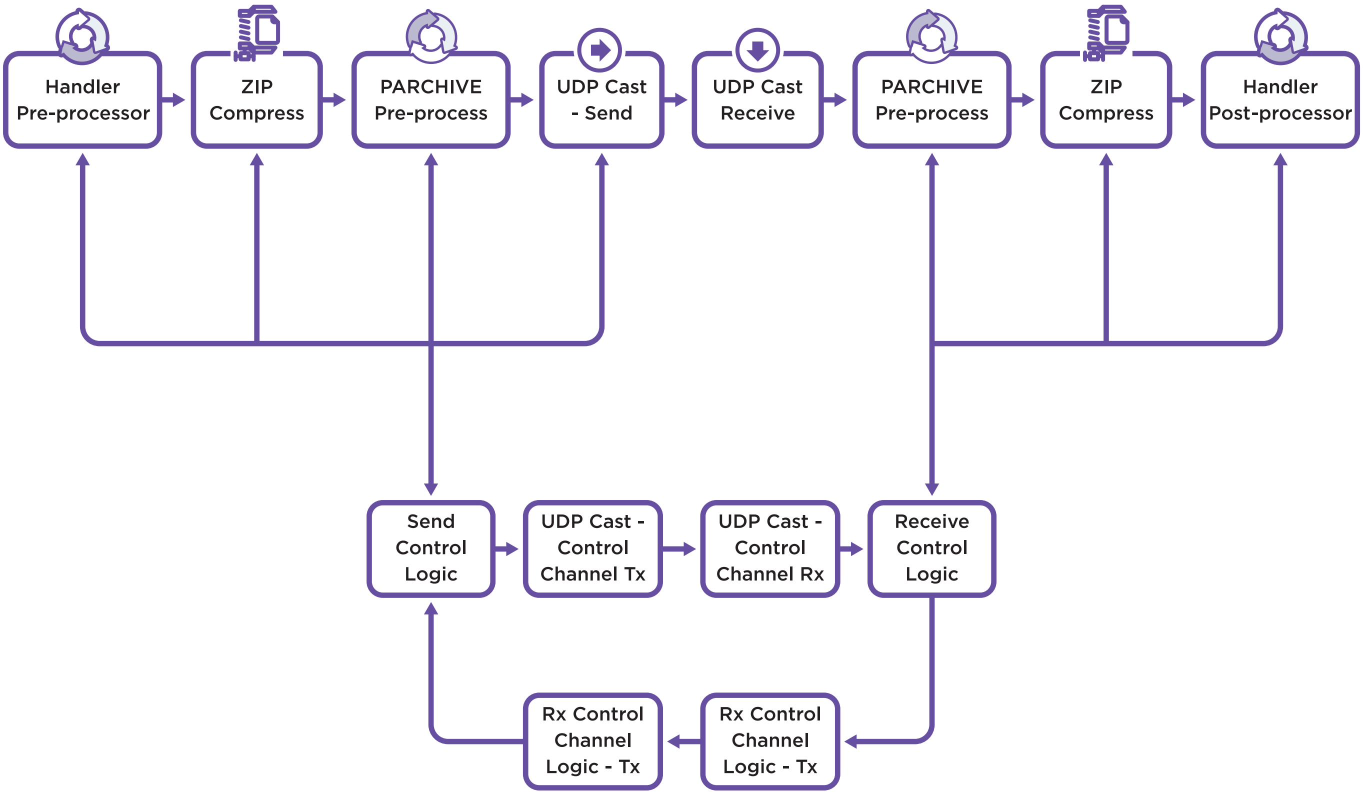
Status Information (Link-B)

The status information provides feedback on each of the receiver boxes. There are two different feedback mechanisms associated with Link-B: The File Information Status, and the Box Health Status, also known as 'the Heartbeat'. These can be used to analyse the boxes and easily identify any problems that the receivers are experiencing from any remote location.

The File Information Status returned shows an acknowledgement that the file was received, as well as, the amount of PAR required for rebuilding the file (if necessary). The Scheduler uses this information in order to re-send the required file or missing PAR blocks. Also included in this feedback signal is the date and time the file was received and the hash code of the file.

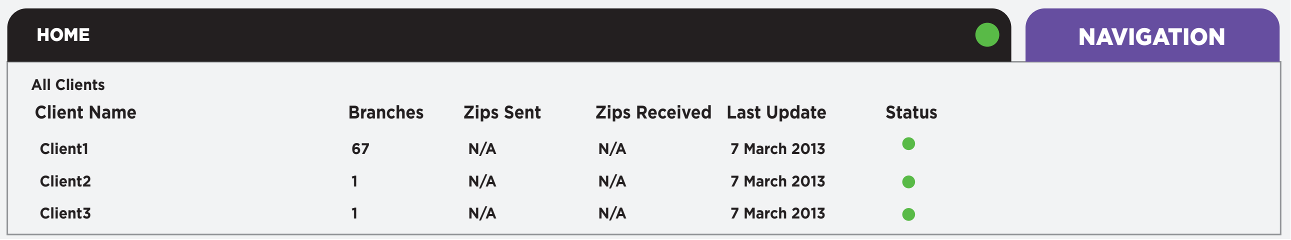
The decoder Health Status delivers details of vital information about each of the decoders such as: Client Name, Branch Name, Up-time, MAC addresses of various components, Available Memory, CPU Load and a List of hard drives and their available free disk space. ***The SatSafe Status feedback also serves as a monitoring service in order to identify whether the receiver node is online***. The status information is sent regularly on a predetermined time interval to the web server. The server displays a coloured status ranging from green to black depicting when last 'the Heartbeat' was received as well as the status data of updates including WSUS and Anti Virus definitions.

The Broadcast System



Monitoring and Control System

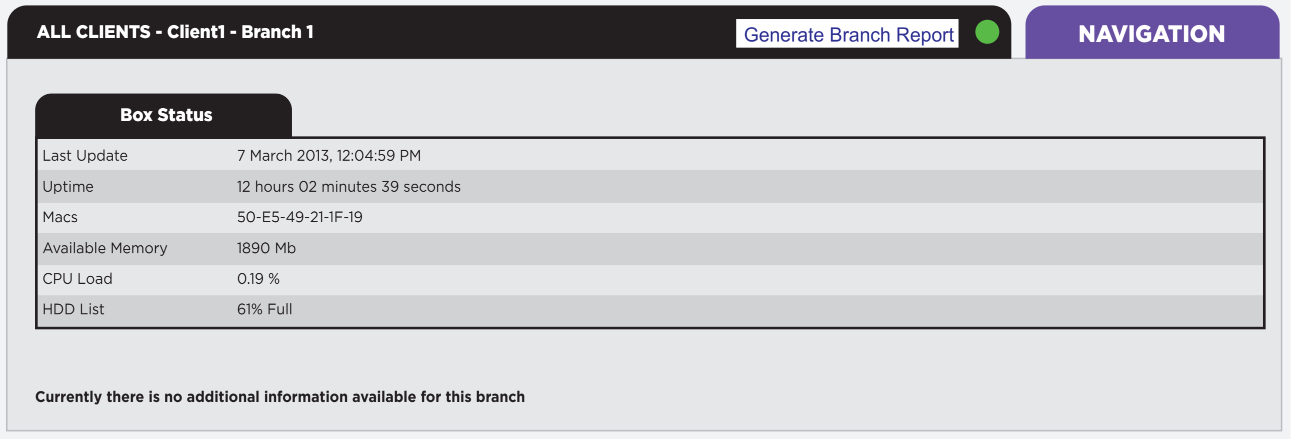
A screenshot depicting all client branches is detailed below displaying how many files have been sent and received to each client, with both ***a block indicating the status of each branch being 'up-to-date'***.



All Clients

Client Name	Branches	Zips Sent	Zips Received	Last Update	Status
Client1	67	N/A	N/A	7 March 2013	●
Client2	1	N/A	N/A	7 March 2013	●
Client3	1	N/A	N/A	7 March 2013	●

A screenshot is detailed below depicting the Branch for a Client, showing the names of the 3 files sent to the Branch, including the hash code for each file, as well as the confirmation that it has been received. The timestamp indicates the time that the files were sent.



Last Update	7 March 2013, 12:04:59 PM
Uptime	12 hours 02 minutes 39 seconds
Macs	50-E5-49-21-1F-19
Available Memory	1890 Mb
CPU Load	0.19 %
HDD List	61% Full

Currently there is no additional information available for this branch

As demonstrated, SatSafe is designed to ensure that malicious content is stopped before it can cause harm to a network. SatSafe seamlessly delivers these updates timeously, **guaranteed 24/7/365**.

Conclusion

*As demonstrated, **SatSafe** is specifically designed to ensure that malicious content is stopped before it can wreak havoc to a network. **SatSafe** guarantees that the allocation of bandwidth is dedicated to operational requirements while updates are seamlessly delivered and installed via **SatSafe**'s patented technology.*

Smart Data Delivery

1. Secure

SatSafe ensures the highest degree of resistance and protection against malicious software by utilizing a one way multicast that eliminates interception

2. Manageable

SatSafe offers a fully managed service, which enables higher productivity

3. Auditable

SatSafe provides comprehensive and timely audit reports detailing delivery confirmation

4. Reliable

SatSafe guarantees the automated delivery of data content, eliminating strain on network resources

5. Transmission

SatSafe's patented transmission technology instantaneously broadcasts and delivers data