White paper

Verizon's Satellite Access: TCP Acceleration, Data Encryption, and Availability

TCP Acceleration

Verizon's Satellite Access Service uses Geostationary (GEO) satellites to deliver private, secure connectivity to Private IP (MPLS), the Public Internet, and Private Dedicated Point-to-Point circuits (Such as Ethernet – Dedicated E-Line).

GEO satellite service (the most commonly used type of satellite service at the moment), consists of satellites which are positioned approximately 22,000 miles away from Earth in a fixed equatorial plane relative to the Earth. While this design has the benefit of enabling a one-time alignment of a customer's VSAT (Very Small Aperture Terminal) antenna to the satellite, the extreme distance to the satellite results in approximately 600 milliseconds of round-trip latency. **To help minimize the effects of this latency, Verizon employs TCP Acceleration over the satellite link.**

TCP is a layer 4 connection-based protocol in which an initial handshake is used to establish a connection between a client and server before data can be exchanged. TCP employs techniques (such as retransmissions) to help mitigate packet loss and enable successful data delivery. TCP is designed to deliver error-free data, end-to-end, regardless of the underlying network architecture.

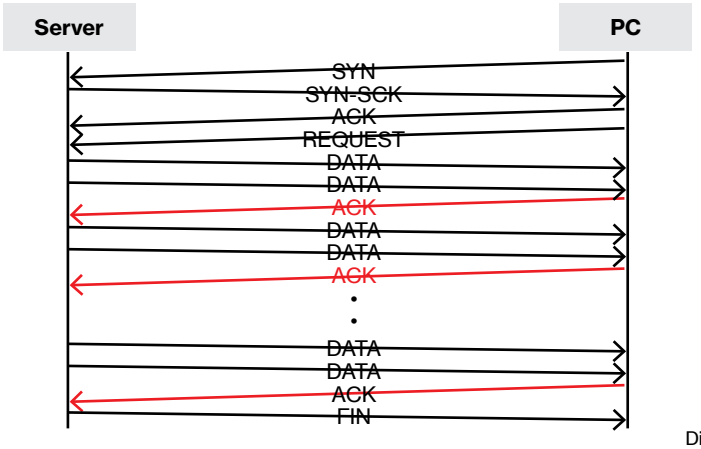
TCP Slow Start is part of a TCP congestion control strategy (used in conjunction with other algorithms) to avoid sending more data than the network can forward with the goal of reducing network congestion.

The higher the latency, the longer it takes for a TCP session to ramp up and use the available network capacity. To address this issue, TCP Acceleration 'accelerates' the TCP Slow Start to reach maximum speeds faster, and to sustain these speeds longer.

Under normal circumstances, when a data packet is sent across the network, a local copy of the information must be maintained until you get an acknowledgement that the information was received at the other end. If an acknowledgement is delayed, then the transmitting side must wait until the transmit window opens again. In order to avoid this delay, TCP Acceleration 'spoofs' the acknowledgement message (ACK) to trick the device to start sending the next data packet while the original packet is still in transit (Diagram 1).

Although TCP Acceleration cannot increase the maximum available bandwidth, it will improve efficiency over the satellite link, thereby making better use of network time to transfer more data.

Without TCP Acceleration



With TCP Acceleration

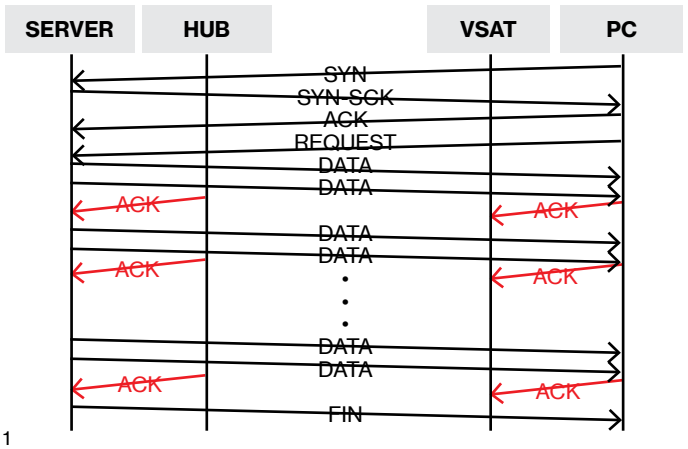


Diagram 1

verizon

AES 256-bit Encryption

TCP acceleration occurs prior to encryption within Verizon's satellite network, so TCP Acceleration is not impacted by the encryption process. All customer satellite modems purchased through Verizon come with an encryption license, and, therefore, all of them support 256-bit AES encryption across the satellite link.

AES stands for 'Advanced Encryption Standard' – a National Institute for Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) - and it is the only publicly available block cipher approved by the National Security Agency (NSA) for transmission and encryption of secret and top-secret information and intelligence. The specific AES encryption standard governing the 256-bit symmetric encryption algorithm is known as FIPS 197.

The AES algorithm utilizes a 128, 192, or 256-bit length symmetric key block cipher to encrypt and decrypt the information. This unique AES secret key is provided to both the Sender and Receiver to enable them to both encrypt and decrypt the data being sent and received.

Verizon has chosen to use a 256-bit key to encrypt and decrypt data traffic over the satellite links in order to provide the highest level of security. During the encryption process, the initial plain text data transmitted by the Sender is converted into an indecipherable version known as ciphertext. Ciphertext is designed to be unreadable - the AES secret key is required to decrypt it.

Upon receipt of the ciphertext by the Receiver, an identical AES secret key is used to convert information back into readable plaintext. In the unlikely event that a hacker gains access to the data being transmitted, they would be unable to decipher the ciphertext without the AES secret key, and would be unable to read it as a result.

As mentioned above, the transmitted data from the Customer's satellite modem is converted into ciphertext before being sent to the satellite, and remains encrypted when sent from the satellite to Verizon's Satellite Earth Station (Teleport). Upon receipt of the traffic at the Teleport station, the shared AES secret key is used to convert the ciphertext back into readable plaintext which is sent to the Satellite Gateway for routing to either the Private IP Network or to the Public Internet via dedicated Gigabit Ethernet circuits.

Traffic sent from Verizon's Satellite Earth Station to the customer's satellite modem (via the satellite) follows the same encryption decryption process described.

The AES key used by the Verizon satellite access service resides solely within the application and is not stored on the satellite modem or on any other device. An RSA-based key management algorithm rolls the symmetric keys by default every 2 hours. The primary difference between link encryption and multicast encryption is the default key roll time.

However, the keys are generated and stored in the same fashion. The Protocol Processor (PP) at the Teleport station contains an RSA public/private key pair. The public RSA key i s sent to the remote site (Customer satellite modem), which generates the symmetric key, encrypts it to the RSA public key, and sends it back to the Protocol Processor which can then decrypt it. At that point the encrypted session is established. The symmetric key generated is actually a set of the next 4 keys generated; this facilitates the key rolling mechanism. At no point are any of the symmetric keys visible or stored in any place other than the applications memory space. If any application dies, the keys are reset.

The following is an illustration of the Link Encryption Protocol process (Diagram 2):

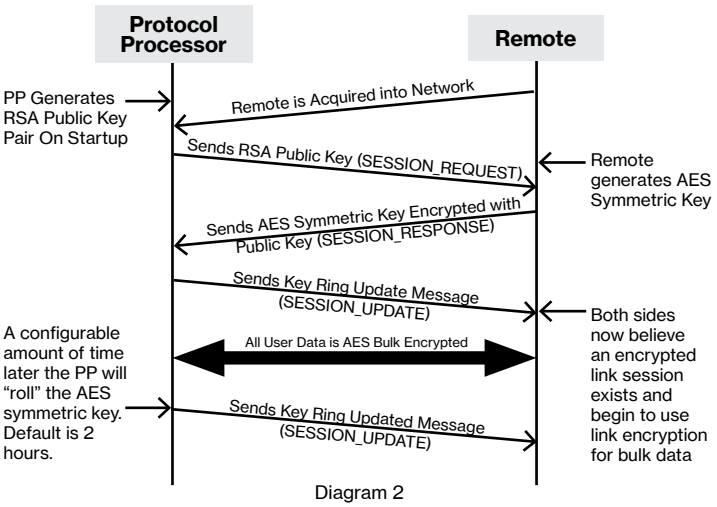


Diagram 2

Bit Error Rate (BER) Testing, Packet Loss, and Availability

Although Bit Error Rate (BER) testing worked well on older synchronous digital networks, a better indicator of modern IP-Based network performance is achieved by measuring packet loss rather than BER. Verizon's Link Budgets are therefore designed to offer an Availability SLA target of 99.5% or better, and a Packet Loss SLA of less than 1%.

The way Verizon achieves this is by designing in margin and multiple MODCODs (MODulation and CODing) based upon the rain zone of the site to reduce the impact of rain fade on the link. The higher the availability target, the more margin and higher power transmitters that are required.

When sending data across the satellite link, the digital data must be converted into an analog signal which is then used to 'modulate' the carrier frequency for transmission from the customer VSAT antenna to the satellite in space.

'Coding' refers to Forward Error Correction (FEC) overhead that is applied to the satellite signal. Additional bits of data are added to the data in order to ensure that the satellite traffic is reliably transported from one point to another. These FEC bits are used to detect and/or correct errors in the transmission. Very robust satellite links require fewer FEC bits in order to provide error correction. However, if the satellite link is marginal, more bits will be required.

Without FEC, transmission errors may occur, resulting in the need to retransmit additional packets. This in turn will negatively impact performance. Although the FEC bits can be used to reconstruct the original data and help reduce retransmissions, the more bits that are required for error correction, the less actual data ends up being transmitted during the same period. Therefore, care must be taken to ensure that the additional MODCODs don't cause more harm than good.

Verizon's satellite hardware recommendations are required to meet the minimum Satellite Network Service Availability SLA. If a customer wants to achieve an even higher level of Satellite Network Service Availability, the following hardware upgrades can be implemented:

- Install a higher Wattage BUC (Block Up-Converter) to help boost the satellite transmit power
- Install a High Wind antenna & mount to protect against misalignment due to high wind conditions
- Install a de-ice antenna in areas that have the potential for freezing rain, sleet, and snow (if not already recommended); for sites that require a ½ de-ice antenna, customer can upgrade to a full de-ice antenna

An example of the maximum amount of acceptable disruption for two different availability targets is listed below:

99.5% Availability

- Daily: 7m 12s
- Weekly: 50m 24s
- Monthly: 3h 39m 0s
- Quarterly: 10h 57m 0s
- Yearly: 43h 48m 0s

99.9% Availability

- Daily: 1m 26.4s
- Weekly: 10m 4.8s
- Monthly: 43m 48s
- Quarterly: 2h 10m 48s
- Yearly: 8h 45m 36s

One of the reasons that Verizon focuses on availability rather than BER is that all the current modulation schemes include error correction. For instance, in the '16 APSK-3/4' modulation scheme (which is one of many that Verizon uses) 25% of the total bits transmitted are error correction bits. The 'APSK' in the '16 APSK-3/4' modulation scheme name stands for 'Amplitude and Phase-Shift Keying', and it refers to a digital modulation scheme that modulates both the amplitude and carrier wave phase by combining both amplitude-shift keying (ASK) and phase-shift keying (PSK).

In this example, the '16 APSK-3/4' modulation scheme results in reduced bit errors and contributes to a straight-line graph below (Diagram 3).

Verizon also sets a target 'Eb/No', where 'Eb' is the energy per information bit and 'No' (N-Zero) is the noise in 1 Hz bandwidth. This ratio is also referred to as 'Signal-to-Noise Ratio (SNR) Measurement per Bit' or 'energy per bit to noise power spectral density ratio', and is used to measure how strong a signal is. It provides the margin to achieve a desired error free performance in clear skies, and then adds additional margin or MODCODs to account for rain fade.

If you would like to discuss this further with Verizon, please contact us at tech-expert@verizon.com.

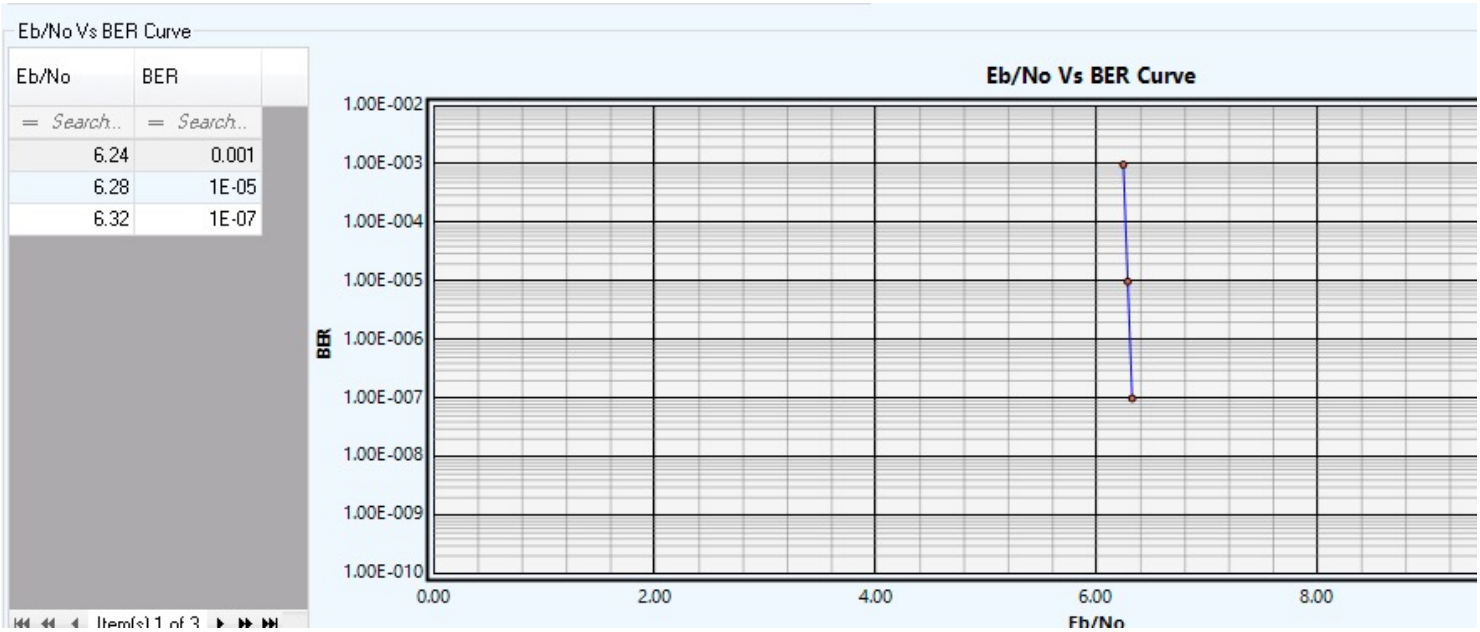


Diagram 3