HP Velocity Technology Overview

Third Edition: May 2013

First Edition: June 2012

Document Part Number: 689165-003

Contents

HP Velocity technology overview

Quality of Experience with HP Velocity

HP Velocity is a Quality of Service (QoS) software engine that improves the overall Quality of Experience (QoE) for real-time network applications.

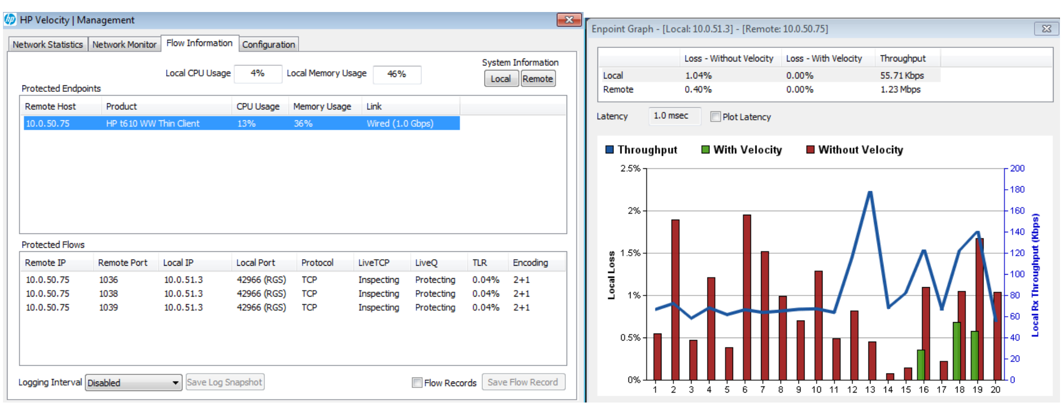
Real-time streaming applications delivered over data networks can be compromised by packet loss and transmission latency; this results in stop-and-go behavior, loss of interactivity, and an overall reduction in the throughput of an application.The experience dissatisfies application users.

Available on HP thin clients, HP Velocity easily integrates with existing systems to improve the QoE of a streaming application by tackling the underlying problems found in today's networks: packet loss, latency, and jitter.

HP Velocity automatically ensures the best end-user QoE by optimizing the underlying network to meet the requirements of bandwidth-intensive applications over wired and wireless, managed and unmanaged networks. By managing packet loss, WiFi congestion, and the impact of network latency, HP Velocity improves QoS, providing a better experience for the end user.

HP Velocity continuously monitors end-to-end network conditions to select the most appropriate data delivery mechanism. Rich reporting capabilities enable HP Velocity to provide end-to-end visibility to key flow information (Figure 1). The system's network monitoring and reporting tools capture in-depth statistics to log files, and displays them in the Management GUI for further analysis and problem detection to resolve network issues.

Figure 1. View of flow information for a local endpoint



NOTE: HP Velocity protects flows between HP thin clients and HP Velocity-enabled virtual desktops or terminal services servers.

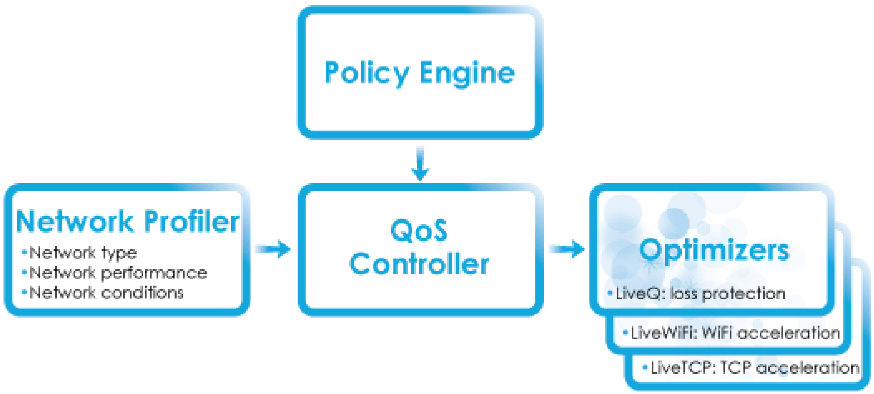
Benefits of HP Velocity

Adaptive network analysis	HP Velocity continuously monitors end-to-end network conditions for individual data flows, providing adaptive optimizations and data flow protection.
Monitoring	HP Velocity collects and reports an extensive set of statistics: • System Information: Operating system, network adapter, CPU, and memory usage. • Endpoint network statistics: Network loss rates, corrected loss rates, throughput, and latency. • Per flow network statistics: Network loss rates, corrected loss rates, throughput, and latency.
Packet loss protection	HP Velocity protects against packet loss, which is key to improving an application's QoE. Packet loss reduces application throughput, degrades or halts streaming applications, and introduces lag for interactive applications.
Latency mitigation	HP Velocity boosts application QoE in a high-latency environment. By actively adapting TCP, HP Velocity automatically calibrates congestion control parameters for each TCP flow, based on the conditions present in the network.
Congestion detection	HP Velocity automatically detects network congestion and adapts accordingly to maximize QoE.
WiFi acceleration	HP Velocity automatically reduces latency and transmission times for wireless networks and minimizes protocol overhead, resulting in improved QoE for WiFi applications.
Seamless integration	HP Velocity is a transparent, plug-and-play solution, which provides QoE benefits to all applications and users.
Lightweight	HP Velocity is delivered as a lightweight implementation, which achieves QoE benefits while keeping system resource utilization to a minimum.

HP Velocity components

The HP Velocity solution consists of three key components (Figure 2), which form an integrated system dedicated to improving the overall QoE.

Figure 2. HP Velocity components



Network Profiler

The Network Profiler profiles the network path between HP Velocity-enabled endpoints. It identifies the type of network connectivity (wired or wireless) and measures key network metrics (packet loss, latency, bandwidth constraints) independently for each flow. The Network Profiler continually updates the QoS Controller on current network conditions.

QoS Controller

The QoS Controller uses the current and trending network conditions provided by the Network Profiler to intelligently activate and adjust the optimizers.

Optimizers

HP Velocity's optimizers work together to deliver maximum QoE:

1. LiveQ: Provides zero latency loss protection from end-to-end packet loss. HP Velocity protects application flows from packet loss by automatically adapting the amount of added redundancy. For more information, see "LiveQ" on page 7.
2. LiveWiFi: Improves performance for congested WiFi networks and increases the efficiency of TCP over WiFi. HP Velocity protects application flows by leveraging WiFi standards to minimize latency, resulting in the prioritization of HP Velocity protected flows. For more information, see "LiveWiFi" on page 10.

3. LiveTCP: Optimizes TCP throughput over all networks and provides latency mitigation for RDP, RGS, and ICA protocols. HP Velocity improves the throughput of streaming and remote desktop applications by modifying TCP flow control mechanisms to perform better in high-latency environments. For more information, see “LiveTCP” on page 13.

LiveQ

Packet loss occurs when one or more data packets traversing a network do not reach their destination. A number of factors contribute to packet loss, including signal degradation over the network, network congestion, corrupted packets, and hardware issues.

Packet loss caused by network impediments can result in QoE issues with streaming applications, Voice over IP (VOIP), video conferencing, and virtualized environments.

TCP QoE and packet loss

TCP, a network transport protocol, guarantees the reliable delivery of packets. When packet loss occurs, TCP stops delivering packets to ensure that packet order is preserved. The receiver will request retransmission, or the sender will automatically resend any unacknowledged segments. At this point, TCP slows down and connection throughput is decreased. As an example, in a GbE network, 1% packet loss with 100 ms of latency throttles TCP throughput to 1 Mbps.

Applications typically affected when TCP flows are interrupted by packet loss include RDP, RemoteFX, RGS, ICA, video, and audio streaming. The QoE impact of packet loss on TCP includes:

- Low frame rates
- Slow file transfers
- High lag
- Unresponsive user interfaces

UDP QoE and packet loss

UDP does not provide a recovery strategy for packet loss, and applications that use UDP are directly impacted by even small amounts of packet loss. UDP-based applications typically react to packet loss by slowing down or reducing bitrate.

When packet loss occurs, the QoE for UDP applications, including PCoIP, RDP, VP8, SIP, VoIP, and video is reduced, resulting in:

- Digital artifacts, smeared video
- Broken, choppy audio
- Low frame rate

Packet loss protection

HP Velocity protects against network loss by applying mathematical transformations to IP packets.

Given a single packet as an input, the HP Velocity transformation will output one or more segments. Each segment will logically represent a portion of the input packet and might carry additional information, such as redundancy data.

The number of logical segments used to represent the original packet will vary based on current network loss conditions. Figure 3 shows a packet being transformed and sent over the network as three distinct segments.

Figure 3. HP Velocity transformation of a packet

Target Loss Rate

Different applications are tolerant to different levels of packet loss. Some applications perform poorly with a small amount of packet loss while other applications perform satisfactorily even with significant amounts of packet loss. HP Velocity adjusts its operation to ensure that each application is protected from experiencing too much packet loss.

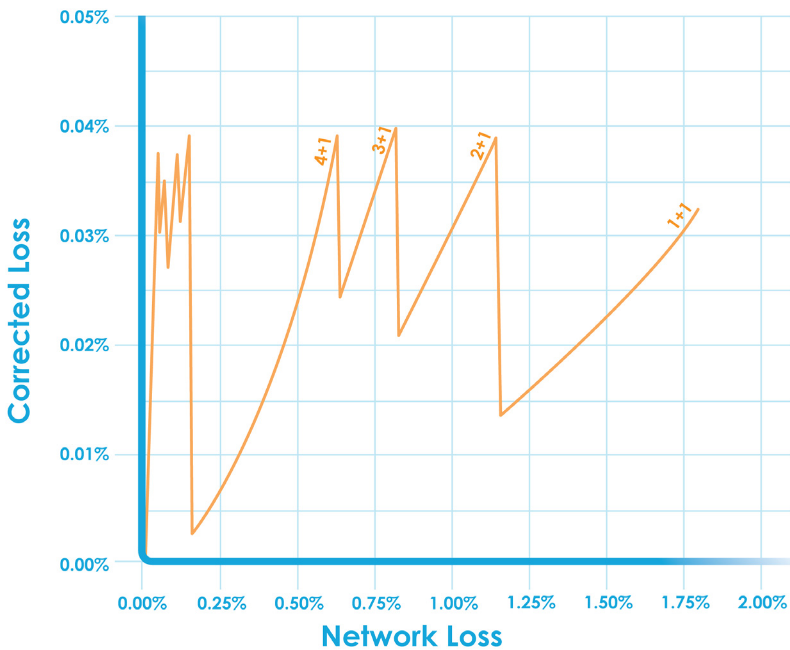
The Target Loss Rate (TLR) is the amount of loss that an application can tolerate while still delivering an acceptable QoE. The default and recommended TLR for thin client applications is 0.04%.

Encoding modes

The encoding mode determines the number of logical data segments that are generated based on the original packet. HP Velocity automatically adapts a flow's encoding mode according to the configured TLR and to the flow's current network conditions.

Figure 4 demonstrates how HP Velocity selects the appropriate encoding mode based on measured network loss and TLR. In this case, HP Velocity changes encoding modes to keep the correct loss level below a TLR of 0.04%.

Figure 4. Corrected loss for TLR of 0.04%

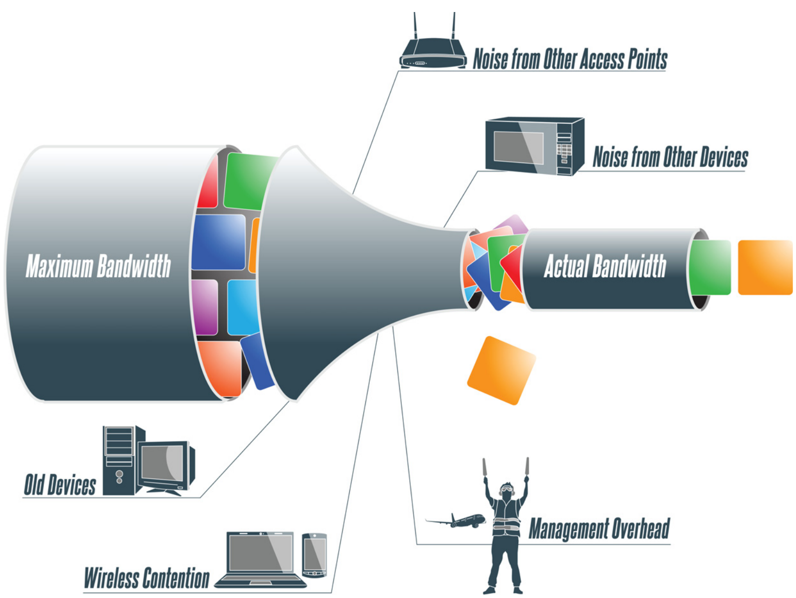


LiveWiFi

WiFi is constrained for a number of technical reasons and, as a result, delivers a much lower network performance experience. High-end, consumer-grade WiFi access points (APs) advertise that they are capable of speeds of 300 to 450 Mbps. In reality, WiFi capacity is much lower than advertised (Figure 5):

- **Distance** (signal strength): The further away a WiFi-enabled device is from the AP the lower the signal strength, which in turn lowers the effective available throughput.
- **Noise from other devices**: The most common frequency used for WiFi is the 2.4GHz band, which is also used for household devices, such as cordless phones, baby monitors, and microwave ovens. Throughput is degraded if any of these devices are used within range of a WiFi network.
- **Noise from other APs**: There are only three non-overlapping channels that can be used by 2.4GHz WiFi. In areas with a high density of APs, such as a city neighborhood or an office tower, it is likely that there will be several other networks using the same channel, leading to speed degradation.
- **Older devices**: If an 802.11n-enabled AP tries to connect to an older device that supports only 802.11b, then the AP is forced to drop the supported speeds for everyone while the 802.11b device is operating. This significantly reduces the throughput that 802.11n devices can achieve.

Figure 5. WiFi bandwidth constraints



- **Management overhead**: WiFi networks carry a significant amount of management overhead. APs advertise their presence and wireless clients must regularly probe the AP to notify it that they are still there. When there are a large number of WiFi devices present in a single location, the management overhead becomes excessive and the capacity of the WiFi network is reduced.
- **Acknowledgments**: All WiFi packets must be acknowledged by the receiver to ensure successful delivery. These acknowledgment packets are sent by a WiFi device every time it receives a packet. When combined with the overhead of protocols like TCP, this can result in 3 out of every 4 WiFi packets becoming overhead packets, with only 1 out of 4 packets containing “useful” data.
- **Retransmissions**: Not all WiFi packets are successfully received the first time they are sent. A client might not receive a packet because of collisions or insufficient signal strength. A single bit error in a packet will result in the retransmission of the entire WiFi packet. Retransmissions might happen repeatedly for the same WiFi packet.
- **WiFi is half duplex**: A wired Ethernet network is full duplex, meaning that a device can send and receive, or upload and download, simultaneously. WiFi is half duplex, so if a client sends data to the AP, the AP cannot send data to the same or any other client at the same time. For two-way communication, which includes most applications used over the Internet, such as video or voice chat, this essentially halves throughput when compared to a full-duplex technology, including a wired Ethernet connection.
- **Wireless contention**: When a client wants to send data and the channel is occupied, the client must wait, otherwise collisions will occur and the data will be corrupted. Once the channel clears, the client must wait even longer before it can attempt to send. Similar to trying to cross a single-lane bridge, if there are cars wanting to cross from both directions, everyone must wait their turn and there is uncertainty about whose turn is next. If a user on a wireless network is using large amounts of bandwidth through activities such as watching a video on YouTube or downloading a file, it will be more difficult and take longer for another device to send, even if it is trying to do a task that requires very little data, such as checking email.

LiveWiFi addresses these issues using WiFi prioritization and TCP over WiFi.

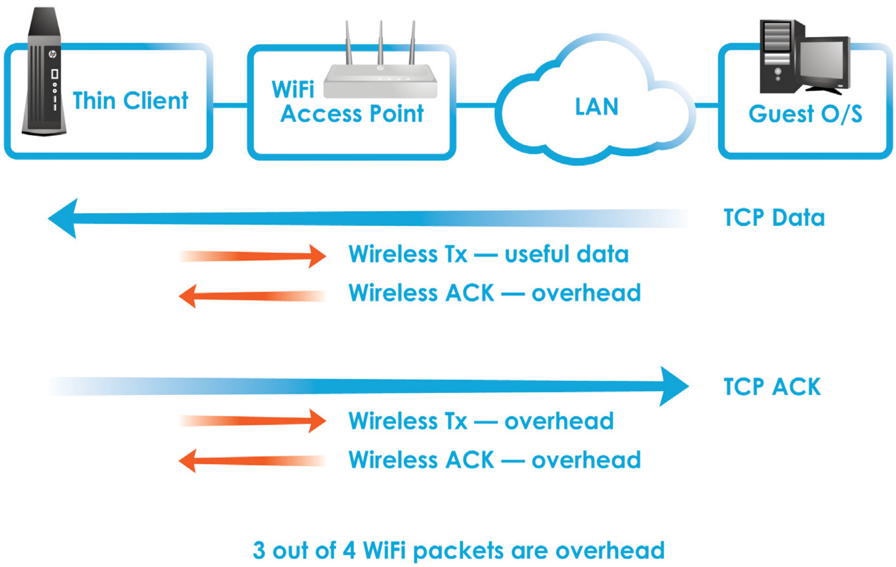
WiFi prioritization

LiveWiFi awards HP Velocity traffic a higher priority than other traffic on the network. Both endpoints mark HP Velocity traffic to prioritize packets moving in either direction. LiveWiFi leverages the WiFi Multimedia (WMM) Standard to reduce packet wait times compared to other traffic in the network. This results in lower latency, less jitter, and higher throughput.

TCP on WiFi

Standard TCP traffic acknowledgments interfere with the transmission of useful data on a WiFi network (Figure 6). With LiveWiFi enabled, HP Velocity modifies the rate of TCP acknowledgments to reduce protocol overhead and improve network performance. This can liberate up to 15% of additional usable WiFi bandwidth.

Figure 6. WiFi overhead in non-optimized flow



LiveTCP

Real-world IP networks introduce both latency and packet loss to application flows. A primary cause of these issues is network congestion. TCP retransmits lost packets, providing applications with guaranteed, correctly sequenced packet delivery. TCP also has built-in algorithms to avoid excessive congestion of the network.

Both latency and packet loss degrade the end user QoE, especially for applications that use TCP for reliable data transmission, such as video streaming, chat, remote desktop, and file transfers. This results in unresponsive user interfaces for remote desktop users, extended wait times for file transfers, and choppy video with reduced frame rates.

TCP congestion avoidance mechanisms

TCP is designed to send data as rapidly as possible until it detects packet loss. Once packet loss is detected, TCP will guarantee delivery by retransmitting, halting delivery to preserve ordered packet transmission, and reducing transmission speed. When packet loss dissipates, TCP will again increase the speed of data delivery. The speed of data delivery might be impacted by standard TCP.

TCP algorithms

TCP can be controlled by different algorithms to accommodate different types of networks. However, only one network type at a time can be accommodated under native TCP. For example, LANs are characterized by low packet loss and high bandwidth. Remote office networks typically have high packet loss and high latency. WiFi networks have high jitter (the latency is highly variable) and variable throughput capacity.

TCP Tuning

Most operating systems allow only a single TCP algorithm to be active with a single set of settings. If a network is optimized for LAN traffic, WAN connections will be less efficient.

While the TCP stack can be tuned, the effort required by network administrators is a deterrent. LiveTCP provides tuning automatically, which boosts TCP throughput over all networks and provides latency mitigation for streaming applications.

LiveTCP congestion control

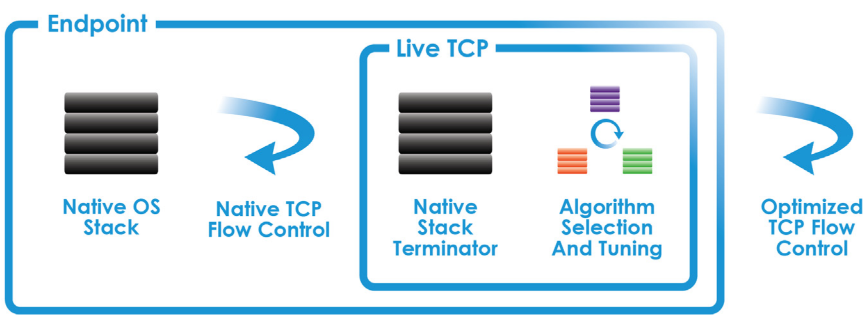
LiveTCP adapts its algorithm to automatically provide congestion control that is optimized independently for each TCP flow (LAN, remote network, WiFi) and the conditions in the network. LiveTCP achieves this without requiring any intervention from IT.

By improving on native TCP, LiveTCP accelerates the speed at which thin client protocols transmit data. For example, RDP, which is highly sensitive to latency, can benefit from LiveTCP by improving transmission speeds up to 10 times. RGS improvements are in the range of two to three times faster, whereas ICA is up to twice as fast with LiveTCP.

In public networks, including those at airports, hotels, and coffee shops, where congestion is often a problem, LiveTCP improves overall throughput by more effectively managing shared bandwidth.

Figure 7 illustrates the process by which LiveTCP independently adjusts the congestion avoidance algorithm for each flow. The optimized LiveTCP algorithm takes precedence over the native TCP algorithm.

Figure 7. LiveTCP algorithm in action



Summary

HP Velocity's patented technology is available exclusively on HP thin clients. It provides a seamless, integrated QoE solution for both managed and unmanaged networks. This allows organizations to gain valuable insight into their thin client data flows, offload more expensive infrastructures (such as MPLS networks) to lower cost networks, and achieve maximum performance regardless of network conditions.

The major benefits of HP Velocity include:

- End-to-end visibility of thin client data flows
- In-depth monitoring and reporting
- Packet loss protection
- Latency mitigation
- WiFi acceleration
- Support for all VDI protocols, including RGS, PCoIP, RDP, and ICA

HP Velocity protects data flows between HP thin clients and HP Velocity-enabled servers, including terminal services and virtual desktops hosted by VMware, Citrix, and Microsoft hypervisors. To obtain the HP Velocity server-side components and associated documentation, visit http://www.hp.com/support. Select the country/region from the map and then select ***Product Support & Troubleshooting***. Type the thin client model in the field (for example, t610, t510, or t410.) and select ***Search***. The server-side components can be downloaded.