WHITE PAPER

Digital Banking and Financial Network Solutions

Strategies to overcome today's challenges in the financial industry

KEYSIGHT

Introduction

The financial industry is at the forefront of network technology. The reality is that the financial sector — from retail banking to high-speed trading — is at the cutting edge of network innovation. Network and IT leaders are always looking for the latest technologies to help them with the following challenges:

- faster technological changes
- changing consumer preferences
- cyberthreats

Bank fraud is now an ultra-sophisticated cybercrime. Highly organized syndicates leverage their technology and the ever-growing complexity of networks to their advantage. Sophisticated network equipment and topologies can lead to complex and slow fault diagnosis processes and periods.

Informed Decisions Require Accurate Data

The following technical factors impact the network and IT groups:

- increasing technical complexity
- accelerating rates of technology change and adoption
- escalating frequency and sophistication of cyberattacks
- performance, stability, and security issues that are not always visible

You can mitigate the risk by having the latest information needed to make informed decisions. With accurate data, you can:

- Legitimize vendor claims so you can make the right technology decisions.
- Optimize your technology roll outs, application performance, and network availability
- Remove the guesswork from your network security performance and resilience.
- Eliminate blind spots in the network by implementing end-to-end visibility.
- Provide your operators with actionable insight by maximizing the use of network tools.

The combination of Keysight's network testing and network visibility solutions provides a unique network partner that can ensure your financial network at all stages — from design to deployment and production.

Maximizing Trading Efficiency

The race to deliver low-latency trading and banking transactions continues to evolve. Financial organizations are vying for unrivaled speed, accuracy, and security within the network. Though the focus is often on the search for nanosecond latency savings, the reality is that dropping packets can have a significant impact on trading performance. Dropped packets lead to increased latencies and incorrect trades — or even compliance issues. These challenges impact, not just low latency trading, but also many other types of electronic trading.

Companies are adopting comprehensive strategies for measuring and minimizing latency and infrastructure quality after deployment. Customers are turning to Keysight for the broadest, most accurate array of testing solutions and services needed in vendor selection, design, and deployment of trading networks.

The goal is to minimize latency and packet losses — from quote reception and order entry — to the completion and settlement of trades. To achieve this, your engineering and operations teams need to understand how the performance of networks, links, devices, and applications affects users. This means modeling and measuring performance using simulated and real traffic — in both live environments and stress test lab scenarios.

Data Feeds

Rapidly detecting degradation in the quality of data feeds is a considerable challenge for any market participant who uses market feeds. The primary basis for market data transport technology is around the use of multi-cast, which does not have any error-correcting mechanisms at the network layer. Any packets that contain lost critical trade data are not detectable until they pass through a feed handler system at the end-user site.

Detecting a problem at the feed handler does not tell you where the problem occurred. For example, was it a problem with the exchange or market data vendor's ticker plant or in their internal network? Was there a problem in the third-party network carrier or extranet provider used to transfer the market data? Was the problem in the end user's internal network or firewall? These questions lead to prolonged decision-making and long fault repair times that are measurable in days and not minutes. So, how does IT overcome these challenges? Regardless of whether the financial institution is a bank, credit union, brokerage firm, investment or insurance company, it begins with a visibility architecture.

The following are several key market feed challenges that can impact your business:

- Application teams may be aware of the problem, but their tools may not be available to the network operations teams who are responsible for diagnosing and resolving the issue.
- Feed handlers use feed arbitration between A and B feeds to auto-correct message drops. Application teams may not be aware of problems and are unable to share the details with their network operations teams quickly.

Case study: Monitoring inbound market data feeds globally

A global trading company with operations in Asia, North America, and Europe has trading infrastructure in 20 co-location hosting facilities around the world. With its sophisticated trading algorithms, it is a leading player on many of the equities and derivatives exchanges worldwide. Having access to low latency market data is key to their trading – any faults in the inbound market data must be rapidly identified and fixed.

Deploying in-house tools to monitor feed performance takes technical time to maintain. This time reduces your deployment of the new and more effective trading infrastructure. They needed a tool that could monitor their inbound market data feeds and support their wide variety of active exchanges. This time takes away from deploying new and more effective trading infrastructure. They needed a tool that could monitor their inbound market data feeds and support their wide variety of active exchanges.

Validate Vendor Claims

The vendor's goal is to get you to buy their solutions rather than those of their competitors, accentuating the positive and presenting the best-case scenario for a product's functionality, performance, and stability.

Most IT departments evaluating solutions perform due diligence through live demonstrations and proof of concept tests. However, these evaluations are often limited in scope and do not provide a real-world assessment. The demonstrations are usually performed in isolation and under the vendor's control. The testing often does not accurately emulate the complex interactions with other devices, systems, and users that you find in a live network.

These evaluations rarely provide an accurate comparison across multiple vendors. It is challenging to get a vendor to relinquish the necessary control so you can thoroughly test their product in unpredictable conditions, with unforeseen traffic patterns and types, and while under attack from malicious software.

The data available for making networking decisions is often suboptimal — a risky proposition for such a high-stakes decision.

Resiliency Score

Keysight's BreakingPoint resiliency score provides a repeatable and comparable measurement for the performance, security, and stability of physical network devices.

The resiliency score tests for performance and security with real-world traffic mixes. It gives you a numeric grade from 1 to 100 to give you a common basis for comparison between vendors. This process gives you a comparison based on your network's actual traffic profiles and loads instead of using an artificial and limited mix. The resiliency score also works when comparing physical appliances to virtualized network functions to help ensure that network functions virtualized (NFV) rollouts are properly resourced and fine-tuned.

Case study: Optimized vendor selection

A major credit card company needed to scale and redesign its access network infrastructure to cope with an ever-increasing volume of mobile users. The company's goal was to determine whether they could replace incumbent IPS devices with next-generation firewalls. They had firsthand experience with vendors not meeting their scalability claims, providing only best-case performance numbers, and not providing scalability numbers for the specific application mix and network design that would be deployed.

With BreakingPoint, they validated the new network and security architectures to support their future strategic initiatives.

BreakingPoint validated design options by:

- Comparing device features and performance.
- Ensuring security devices were tuned correctly to detect the latest attacks (and DDoS) under a variety of loads.
- Quickly recreating production traffic with real stateful applications and adverse conditions.

The result was a highly optimized vendor selection process that eliminated uncertainty. They can now be confident in their network selections by using Keysight's resiliency score.

The High Price of Outages

U.S. options trading was halted In September of 2013, due to a problem with a data feed that supplied prices to traders. According to the Wall Street Journal, the outage affected the trading of options based on stocks, exchange-traded funds, currencies, and other asset classes. In addition to preventing trading, a small number of trades were canceled as a result of the issue.

This brief episode impacted or prevented billions of dollars in trades in a matter of minutes. In this case, the outage affected the market equally — positively or negatively. When a bank or trading firm experiences a network issue or outage, their customers are impacted — this also impacts the company's reputation and bottom line.

Optimizing Network Performance

Operating and optimizing the network used to require training and specialized skills. Today's networks, however, take a team of trained specialists to maintain. The simple adjustments that control direction are now complex, interwoven systems. A myriad of calculations and interactions take place because of simple surface changes.

Keysight helps companies refine their networks with a suite of solutions that can test, emulate, monitor, and optimize modern networks and ultra-complex data centers.

Case study: Stress testing trading infrastructure

A major global investment bank was concerned with how their trading infrastructure could cope with sudden changes in trading volumes and market data. They were concerned that unexpected market events might lead to trading infrastructure saturation — resulting in delayed orders.

Keysight provided a solution that allowed the bank to generate test traffic at varying data rates to simulate varying traffic profiles. Keysight's Application and Threat Intelligence (ATI) solution has built-in signatures that support a variety of order entry protocols such as FIX and ITCH, as well as market data feeds. Using ATI data, the bank was able to successfully test the capabilities of critical networking and system components without having to deploy expensive and difficult-to-support real trading servers and applications.

The bank can now test against changes in market conditions, tools, applications, or global events to ensure their network meets the needs of the business regardless of changing external or internal conditions.

How to Know if Your Network Security Is Working

If your CTO asks how you if the network is secure, how will you answer?

- breach did not occur
- passed our IT audit
- applied the most recent updates and signatures
- performed regular vulnerability scans or assessments
- executed annual penetration testing
- network has not gone down

Several companies who suffered devastating security breaches over the past two years gave the above answers. In today's world of hyper-complex systems and ever-changing arrays of attacks and defenses, the only way to answer this question is in the affirmative — because we tested it.

Testing use to be a daunting task, but now there are easy, affordable, and highly repeatable methods of testing products, solutions, and production networks. These methods have fully loaded application traffic that is customizable to your environment.

This traffic can be injected with DDoS, malware, and other exploits so that you know for sure how your actual network defenses will respond. These applications and attack scripts are updated on a bi-weekly basis to ensure you are ready for the latest attacks.

Case study: Real-world DDoS validation and response

A progressive trading group was particularly concerned about DDoS attacks after observing real service delivery and impact during a volumetric distributed denial-of-service (DDoS) attack. Since the company was paying a DDoS cloud mitigation service provider $250,000 per month for this service, the level of confidence they had with their effectiveness at stopping DDoS attacks while not denying legitimate user transactions was quickly deteriorating. They needed a real method of understanding the resiliency of their DDoS mitigation service provider.

Keysight's BreakingPoint was able to uncover a flaw in the data center workflow of their defenses, showing that the DDoS attack mitigation initiated by the DDoS service provider was blocking legitimate user traffic. By simulating a DDoS attack under loaded conditions, the Keysight attack revealed a core router failure in the service provider network within an hour of launching the attack. Sixty-one percent of CIOs and CISOs believe the scope and complexity of IT security makes it difficult for their organizations to assess their security capability.*

Meeting the Needs of Mobile Clientele

There was a time when users who adopted new technologies would accept compromises in quality of experience or performance, and even security for the added convenience that those new technologies offer for online banking or mobility.

In the world of credit cards and retail banking, having a resilient and high-performance mobile access product is a critical aspect of an overall growth strategy. A poorly-executed mobile app can lead to customer frustration, dissatisfaction, and loss of market share.

Despite the explosive growth in mobile data usage over the past five years, the requirements for mobility are increasing. According to a 2014 study from Cisco Systems, "Traffic from wireless and mobile devices will exceed traffic from wired devices by 2016. Business IP traffic will grow at a CAGR of 18% from 2013 to 2018."

The increased usage identifies a need to understand how the network will respond to a variety of mobile users, devices, and applications. Network operators must account for the impact of growth in terms of the mobility of applications, servers, and data within and among data centers. They also need to consider the impact of network advancements — such as the virtualization of firewalls, load balancers, core routing, and switching. The importance of user quality and security, and its impact on customer retention, are too critical to be left to ad hoc testing and optimization.

Case study: Leading global credit card company – mobile access testing

A leading global credit card company needed to test new applications and enhancements thoroughly before release. Historically, their applications underwent testing in an ad hoc manner, but the increasing importance and wide variety of customer devices meant that this was no longer possible. A more rigorous approach was necessary. The company needed visibility into how new application rollouts would affect their mobile network to ensure their customers did not experience a negative impact.

Keysight IxVeriWave, a comprehensive Wi-Fi test platform, helped the company solve their test needs. IxVeriWave allowed the credit card company to automate testing processes to ensure that testing is repeatable and consistent. This process facilitates a smooth rollout of new capabilities and applications that are accessible over wireless and Wi-Fi networks.

IxVeriWave reduces the test times from months to weeks or days — reducing time to

market. The credit card company can now offer improved services to its customers regularly, without degrading their quality of experience (QoE).

IxVeriWave helped the credit card company:

- validate various design options
- compare device features and performance
- accurately recreate production traffic with real stateful applications and inject adverse conditions

How to Control Blind Spots

Most problems catch teams by surprise because they emerge from blind spots — the areas within the network that are not visible. Blind spots are a result of increased network complexity, increasing the possibility of a cybersecurity breach.

Keysight can help you to eliminate blind spots in the network by getting the right information to the right tools at the right time to improve performance, QoE, and security. Keysight's Visibility Architecture solution includes physical and virtual taps, bypass switches, and full-featured network packet brokers. These tools enable network visibility requirements — from single-point solutions to large-scale enterprise and service provider network deployments.

A well-implemented Visibility Architecture extends the life of your existing tool investments and maximizes current tool capacity. Our Visibility Architecture provides network visibility that is scalable to help you with end-to-end testing — from a product, portfolio, design, management, and support.

Case study: Global investment bank standardizes monitoring infrastructure

A major global investment bank needed to monitor its trading infrastructure in over 30 worldwide locations. The bank required access to order entry and market data at varying points in each location.

A single packet dropped out of millions of packets sent on high-speed data feeds can easily lead to multicast gaps occurring multiple times per second. The bank required a compact solution due to multiple fiber types in each location. They could not spare the space in the expensive colocation centers necessary for multiple fiber taps.

The bank chose the Keysight Flex Tap solution because of its flexibility. It allows up to 24 fiber taps in a 1 RU form factor. It gives the option to mix and match a wide variety of fiber taps (split ratios, fiber types, and speeds) to meet the specific requirements of the local data center and trading infrastructure.

Flex Tap provided the bank the ability to access critical markets on a global basis because of the tap's flexibility and small form factor. Their network visibility was enhanced further with the Keysight Vision Series packet broker. The Vision Series gave the bank a scalable, easy-to-configure, and manageable solution for their global network visibility. Not only does the solution eliminate blind spots, but it ensures that networking tools receive optimized and actionable information.

Retail Banking Moves into the 22nd Century

Retail banking is one of the fastest-changing areas of banking. No longer are retail bank branches seen as the core of the transactional banking business. Over the past several years, retail banking has continued to increase, with a focus on cost optimization and staff reduction. Critical functions of retail branches are less about transactions and more about non-traditional and modernized accessibility and the following offerings:

- positive customer experience
- advisory services
- digital banking from mobile devices
- community outreach
- wealth management development

At the core of the modern branch, the experience is technology-related. High quality and modern IT infrastructure will be key to market-leading customer experiences. High-performance infrastructure will address the following services:

- Wi-Fi access
- smart ATMs
- teller-less "robo-branch" kiosks and touch screens
- targeted advertising linked to social profiling of customers

Branch networks will evolve to provide access to the banking applications managed by the banks, including banking partners integrated into the core bank offerings.

The management of this branch "edge network" will be critical to the successful evolution of the retail branch experience. You need to manage risk and provide superior IT capabilities to ensure your bank's competitiveness.

Keysight has a range of edge network solutions that allow managers of widely dispersed branch networks to monitor the overall effectiveness of telecommunications and the customer's experience. Keysight's Hawkeye, in combination with a family of low-cost hardware and software endpoints including Keysight IxProbe, allows network managers to:

- directly monitor QoS and experience of mobile users
- receive alerts when QoS targets are breached
- schedule network KPI tests on a programmed basis
- monitor the performance of third-party applications
- demonstrate to business sponsors the overall ROI on IT infrastructure investments
- perform QoS tests specifically designed to test video and audio applications

A central software server manages these capabilities — either installed in a private data center or a public cloud environment. The Hawkeye central server has extensive API connectivity to allow easy interfacing into bank back-office systems. Hawkeye helps you to deploy wireless-enabled endpoints in different locations. You can find Hawkeye deployments in over 12 countries.

> "Powerful forces are reshaping the banking industry. Customer expectations, technological capabilities, regulatory requirements, demographics, and economics are together creating an imperative to change. Banks need to get ahead of these challenges and retool to win in the next era."[1]

1 PwC. *Retail Banking 2020 - Evolution or Revolution? 2014.*

Conclusion

Times are changing, and retail banking businesses and their customers are demanding more of their networks and applications, including services. And it goes beyond simply more and faster — the nature of the network is changing as well. The network counts — as does your ability to deliver guest access or when shaving nanoseconds off a brokerage's critical trades.

Today the network is critical to meet your business commitments. The key to making an informed decision is having accurate data and network visibility. For over two decades, Keysight has been providing solutions to financial services companies to help test and monitor their infrastructure.

Keysight can help you monitor and effectively manage your networks with the following solutions:

- **TradeVision** — delivers high-performance monitoring of market data feeds, enabling you to detect multicast sequence gaps or feed failures instantly.
- **Optical Taps** — provide cost effective copies of live network and trading data to monitoring tools
- **Vision Series Network Packet Brokers** — pass relevant traffic to just the security and application monitoring tools that need it, reducing tool cost and utilization
- **IxVeriWave** — enables accurate testing and validation WLAN infrastructure through comprehensive testing.
- **BreakingPoint** — an all-in-one application and network security system platform to help you validate network security and performance.
- **Hawkeye** — quickly and effectively validates network performance, isolate problems, and proactively detects issues by running scheduled verification tests on any site using wireline or Wi-Fi connections. Ensures high customer QOS and allows real time testing of BCP deployments