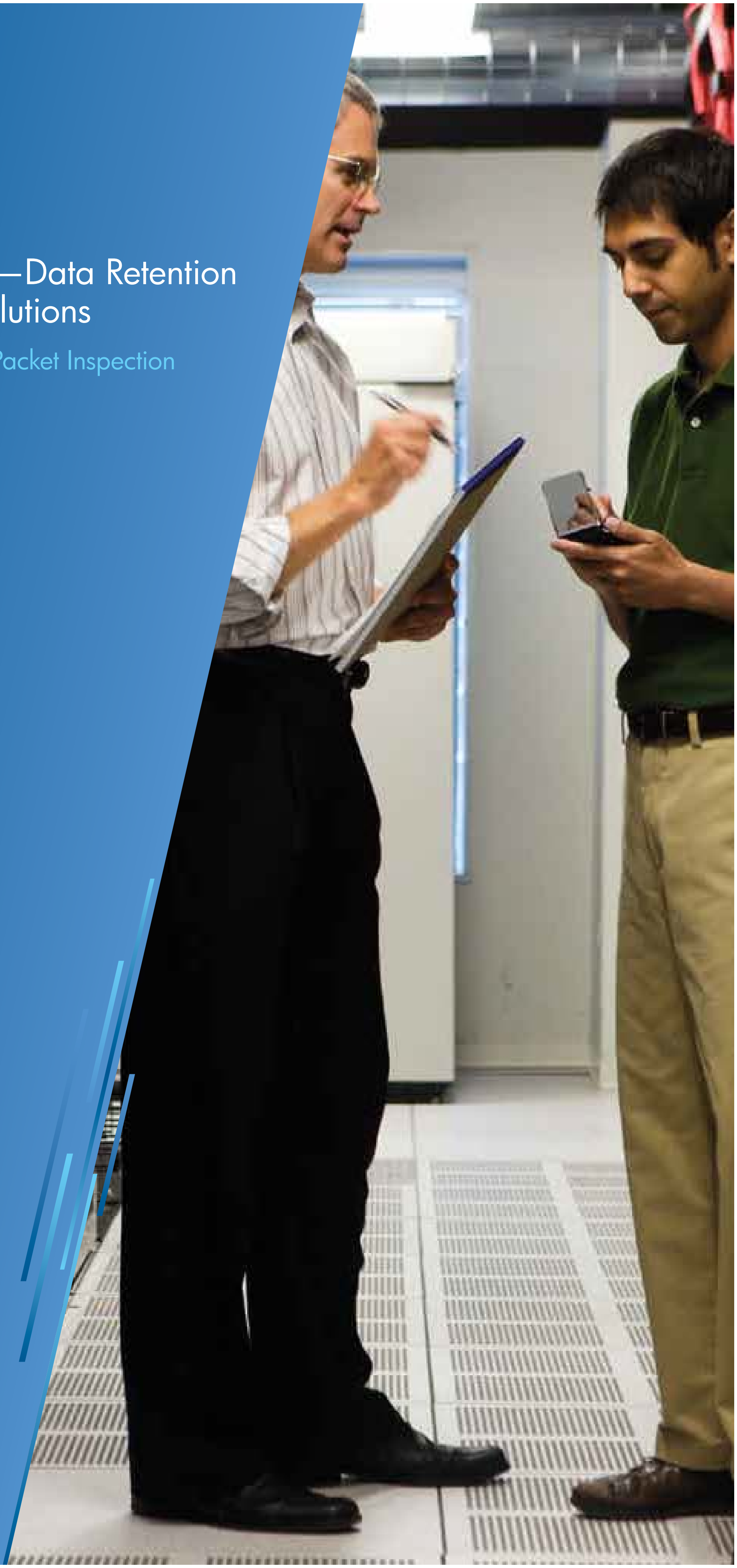
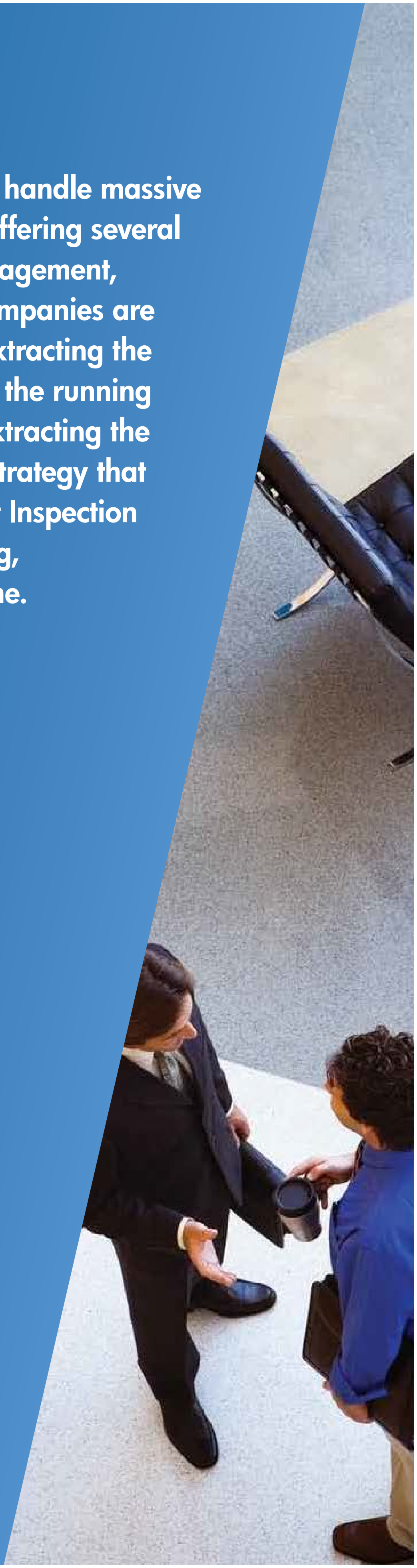
HP Investigation (Dragon—Data Retention and Guardian Online) solutions

HP Dragon Blue—IP Probe Deep Packet Inspection

Solution brief



HP Investigation is committed to help organizations to handle massive data in an efficient, secure, cost-effective manner by offering several state-of-the-art solutions for data archiving, data management, and transferring data into information. Nowadays, companies are struggling to turn data into an actionable format by extracting the relevant information that would help them to enhance the running of their business. Understanding the information by extracting the data from traffic flows at protocol level is the winner strategy that can be powered by Dragon Blue IP Probe Deep Packet Inspection solution, providing the capability of extracting, filtering, analyzing data directly from network traffic in real time.



According to a recent Yankee Group report: "Mobile network operators (MNOs) must introduce customized price plans to sustain mobile broadband (MBB) revenue growth and ensure long-term business model sustainability. Tiered pricing should be only the first step toward a more personalized approach. MNOs' end goal must be to ensure consumers are offered MBB services that meet their specific needs in terms of preferred devices, consumption behavior, and price-sensitivity." The most important message of this statement is that mass consumption is becoming individualized where the service providers need to cope with the challenge of managing a huge number of clients while handling them individually by offering customized services for their needs. The first step is to understand the clients' needs by employing a mechanism that collects the necessary data, that is, data that can be easily analyzed to be evaluated correctly and making the right decision by company senior management. Data capture directly from data flows is the perfect solution, resulting in the correct understanding of the data and making the correct conclusions. Using obsolete technologies for data extraction is one of the reasons for data misinterpretation, which result in negative consequences on the business.

Network-based vs. log-based monitoring

For data capture in general, there are network-based and log-based data collection approaches. When data is captured from log databases and log servers, then we have to count with latency any obstacles that arise from the database model, and no guarantees for up-to-date data. Finally, there are restrictions because we can access the data stored in database but not the data transferred via network.

In the new era in data monitoring, network-based monitoring has to be considered. The main advantages are that the data collected directly from traffic flows goes through the network; the relevant information can be extracted from data flows by going down to protocol levels; and all the data is collected and can be analyzed in real time. The technology behind this network-based approach is called IP Probe.

Figure 1. DRAGON Data Retention: data capture approaches

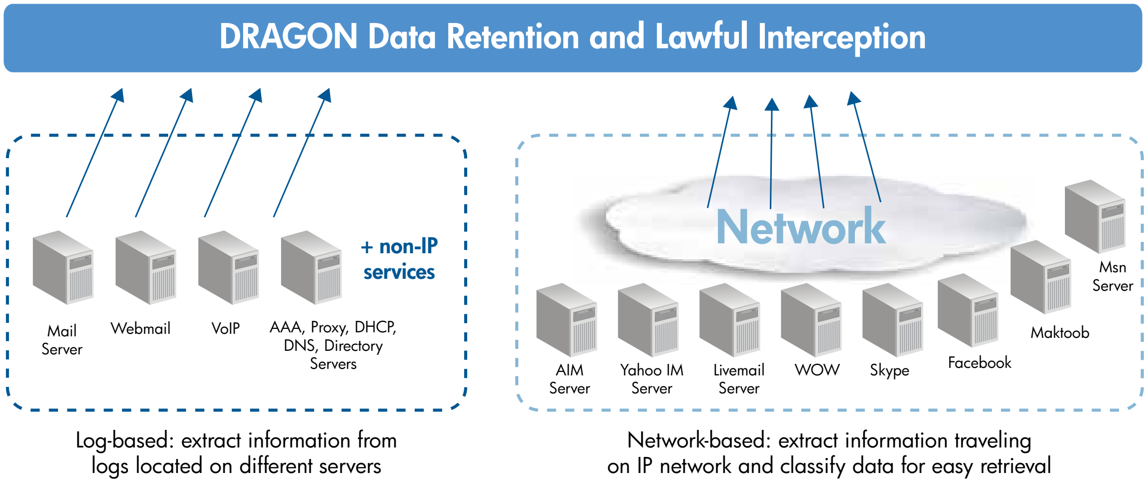

DRAGON Data Retention and Lawful Interception
+ non-IP services
Mail Server
Webmail
VoIP
AAA, Proxy, DHCP, DNS, Directory Servers
Network
Msn Server
Maktoob
Facebook
AIM Server
Yahoo IM Server
Livemail Server
WOW
Skype
Log-based: extract information from logs located on different servers
Network-based: extract information traveling on IP network and classify data for easy retrieval

Table 1. Advantages of network-based monitoring over log-based monitoring

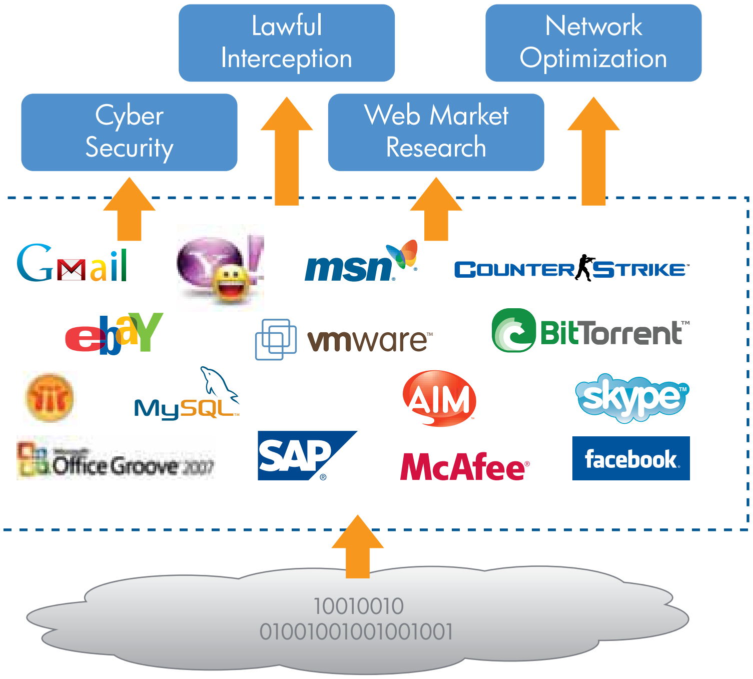
Server log based	Network based
Must handle various formats of stored information	Easy to interpret and retrieve, because of single data format on the IP network (for example, SMTP for email)
Could necessitate professional services and custom development to upgrade existing IT systems	Single point of capture directly from the network, independently of existing IT systems
Could be complicated to collect and correlate data if network is complex with many devices	Highly optimized information format: gain over 90% volume on logs data → only one line per event

The IP Probes

Network Probe is a technology that can decode protocols, extract information embedded in the traffic, or transmit information over the traffic and deliver this information in the form of metadata and content feeds to an application developed by the user that can leverage the information provided by the Network Probe.

The Network Probe can make an acquirement specifying what information is required. It can deliver this information in a tabular format, just like in a database. This technology can also deliver packets and packet contents. The process of extracting and delivering the information from the network is performed in real time and can scale up 20 Gb/s.

Figure 2. User identification and data extraction across multiple applications



HP Dragon Blue IP Probe (Deep Packet Inspection) solution

Due to the increasingly rapid pace of life, deep packet inspection (DPI) has become a relevant tool in telecommunications and Intelligence Support System sector for data collection during the last decade. DPI technology delivers the solution for real-time data collection directly from network data transmission and also brings the capability to filter unnecessary data. HP Investigation solutions are improved by the DPI data collection mechanism because the DPI solution can be integrated for data retention, lawful interception, warrant management solution; DPI can also be deployed in the Intelligent Support Solutions as service/cloud solution.

The DPI solution features:

- Accurate identification of users across multiple applications, multiple physical locations, multiple terminals, and multiple identities
- Only relevant data is extracted to save storage space and speed up postprocessing
- Using probes, network-based real time monitoring can be implemented for data collection
- Real-time traffic analysis based on Layer 7 (deep packet inspection)

Protocol and application identification based on a portfolio of analyzers covering all types of applications, including social networks (Facebook, Twitter, etc.), streaming and progressive download (Flash video, YouTube, Netflix, etc.), peer-to-peer (BitTorrent, eMule, etc.), VoIP (SIP, RTP, etc.), messaging and chat (Skype, Windows® Live, Yahoo Messenger), and so on.

Extraction of traffic metadata for use in cases such as:

- Charging (e.g., codec settings used by video streaming applications provides level of quality by user and by application to enable differentiated VIP plans based on enhanced quality of experience for certain applications)
- Data retention (extraction of senders and receivers of messages and calls, websites visited, etc.)
- Real-time traffic analysis at 20 Gb/s in a single probe

The protocols supported are network protocols, application protocols such as webmail, email database, or any kind of network application. For each protocol, tens of metadata are delivered, which translates to thousands of metadata in your application. These protocols are regularly updated, and new protocols are added to protocol plug-in library.

Network Probe network intelligence is designed to be embedded into your application so that you can rely on the real-time visibility provided by Network Probe to develop the application, process the traffic information, or store this information for reporting or traffic shaping.

Business benefits

Dragon Blue Application aware IP probe provides real-time visibility on traffic per user and per application. Probes are used as an independent, trusted third-party source of data to feed customized systems used by telecom operators to perform various tasks such as charging, subscriber analytics, and data retention.

By providing full visibilities on what applications are used, when, by whom, and how, Dragon Blue probes enable telecom operators to:

1. Understand how subscribers use the network to propose personalized plans and services
2. Increase average revenue per user by developing tiered plans where billing is based on application usage and customized quality of service
3. Comply with either data retention or other national regulations

Benefits from probe technology

- No impact on network operations
  - Passive probes, generate no overhead on network devices
  - Not impacted by network devices upgrades, reconfiguration or changes
  - No operational risk due to Internet Protocol Data Record (IPDR) generation
- More actionable information
  - Probes have been designed for IPDR generation (network devices are not)
  - Standardized IPDR, whatever the brand and model of network device provides homogeneity in the network
  - IPDR generate smaller volume of data than servers logs, which results in lower total cost of ownership and better reactivity
- IPDR are richer than server logs
  - Information for over-the-top applications are not available on server logs (e.g., user action in Facebook such as login, chat, and file transfer)
  - Provides visibility on non-browser-based applications (e.g., Instant Messaging, Google™ Earth, mobile apps)
  - Correlation of subscriber information with application-level information

HP advantage

Dragon Blue is part of HP Investigation solution portfolio, with which HP offers end-to-end data retention, lawful interception, warrant management, data archiving solution featuring several options, flexibility, and cloud capability. Dragon Blue:

- Provides a higher granular level of visibility over application used on an IP network
- Offers more reactive updates when application change or new applications emerge
- Provides the lower cost per Gb/s for network analysis
- Helps maintain log accuracy and integrity under a heavy load of traffic

Dragon Blue provides better visibility in application usage at core network speed (20 Gb/s) in real time. The portfolio of protocols and applications analyzers covers nearly 100 percent of IP traffic, and provides faster updates as protocols change and new applications emerge. Dragon Blue probes are the only appliances built for multipurpose network intelligence, enabling telecom operators to leverage the most granular application-aware traffic analysis for building tailored solutions to fit their specific requirements.

HP in the telecommunications industry

HP helps the world's communications service providers (CSPs) transform the way they do business—to grow in a fast-changing market. CSPs must meet the huge demand for new services—and streamline internal operations. HP is a leader in helping CSPs drive transformation, with over 30 years of telecom experience, global IT leadership, expertise in entertainment, and leadership in consumer devices.

HP offers a truly end-to-end portfolio from core network to handheld devices—including a suite of convergent IT and telecom solutions, such as software (OSS/BSS, SDP, SDM, cloud); professional services, including business consulting, integration, and managed services/outsourcing; joint go-to-market programs; carrier-grade servers; storage; printers; and tablets and smartphones.

HP Services

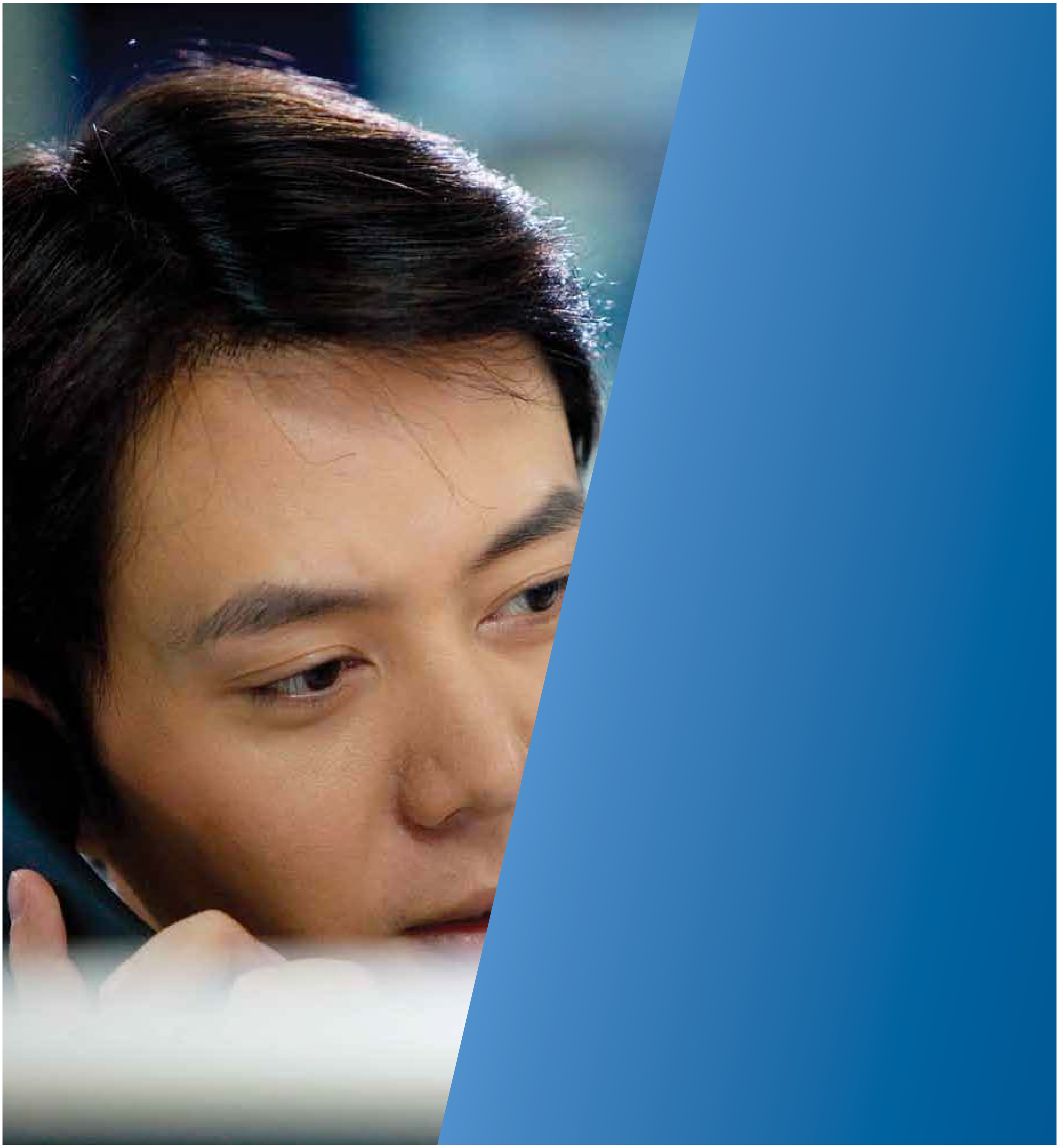
HP Solution Lifecycle Services

HP Solution Lifecycle Services for the communications and media industry help you realize the full value of your solutions, from planning and assessment through testing, deployment, operation, and nearly continuous improvement. Each service area leverages proven processes and best practices to balance capital and operating expenditure (OPEX) and reduce risk, while keeping your projects on time and your operations running smoothly.

HP Services offer a proven way for navigating through your transformational journey:

- **Consulting**—HP Solution Consulting Services help define business transformation and translate strategies into actionable solutions.
- **Implementation**—HP Solution Implementation Services offer a low risk project lifecycle across design, development, customization, and network and system integration.
- **Management**—HP Solutions Management Services increase the operational efficiency of your existing solutions, including reactive, proactive, operational, and enhancement services.
- **Outsourcing**—HP Services offer a variety of sourcing options designed to improve business agility while reducing your OPEX. The options include IT and infrastructure outsourcing, application management, and business process outsourcing.

Extract, filter, and analyze data directly from network traffic in real time. For more information, visit www.hp.com/go/investigation, or email investigation@hp.com.



4AA3-7404ENW, Created December 2011