Tap Technology Enables Healthcare’s Digital Future
Table of Contents

Executive Overview ................................................................. 4
Introduction ......................................................................................... 4
HIT’s foundation .................................................................................. 5
Keeping your network healthy ......................................................... 5
Use cases ............................................................................................... 6
Information at the bedside.............................................................. 6
Health insurer balances the demand .............................................. 7
HIPAA compliance without risking downtime ............................... 8
Summary ................................................................................................. 9
Executive Overview

A revolution is taking place in the practice and business of healthcare. Digital information technology is enabling instant access to patient records and imaging data; collaboration between local doctors and remote specialists; mobile voice and data connectivity; and more convenient billing and payments. The benefits of deploying these new technologies are more efficient operations, lower costs, and, ultimately, improved quality of care and better medical outcomes.

A critical enabler of digital healthcare initiatives is a network that connects systems and people so quickly, securely, and reliably that it is invisible to users; it just works. Underneath the hood, systems and professionals constantly monitor and tune the network, dealing with issues before they impact users. For these monitoring systems and professionals to succeed in this mission, they need 100% visibility of all of the network traffic, all of the time. This paper examines how Tap technology provides this key capability of traffic visibility to enable healthcare’s digital future.

Introduction

Healthcare reform legislation is in the headlines, and more than US$30 billion in the American Recovery and Reinvestment Act of 2009 (ARRA, also known as the economic stimulus plan) is allocated for Health Information Technology (HIT) investments. This activity has focused attention on information and communications technology (ICT) as a means to drive down healthcare costs and increase the quality of patient care. Much of the ARRA money is in the form of incentives to encourage adoption of electronic health records, but ICT offers many more opportunities for modernization within the healthcare industry. A few of the benefits ICT can bring to healthcare organizations include:

- Better sharing of diagnostic data with picture archiving and communications systems (PACS) to store and access data-rich images generated by computed tomography (CT or CAT scans), magnetic resonance imagery (MRI), and other methods
- Improved communication, collaboration, and mobility for caregivers by leveraging IP telephony technology
- Prevention of medical errors, such as administering the wrong medicine, by making accurate information available at the point of care using wireless, handheld devices
- A higher level of medical team collaboration and remote care delivery enabled by videoconferencing, telepresence, and telemedicine
- Energy savings and compliance with environmental regulations through improved management of heating, ventilation, air conditioning, and lighting systems in hospitals, clinics, and medical office buildings
- Better physical security and access control in hospitals and medical buildings using electronic authentication and surveillance systems
- Capital and operating expense savings by tagging and tracking equipment electronically
- Efficiency and cost savings from centralizing and consolidating services such as security and building management
**HIT’s foundation**

The common foundation of all of these HIT initiatives is a secure, reliable, high performance network to carry all of the electronic data and audio/video communications. In fact, the trend is to converge as many of these services as possible—and preferably all of them—onto a single IP network for maximum efficiency and integration. To meet this challenge, the network must possess these key attributes:

- High performance, to provide quick response times and handle a wide variety of protocols and data types
- Secure, to protect confidential patient data and to comply with the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) requirements
- Reliable, so services are always available
- Interoperable (standards based), to integrate many different types of systems
- Scalable, to grow with the organization

Today’s IP network technology meets all of these requirements, and many vendors including IBM, HP, and Cisco are delivering HIT solutions based on converged IP networks.

**Keeping your network healthy**

With services depending more and more heavily on the network, it is critical to a healthcare organization’s success to constantly monitor the health of the network, much like a patient’s health is monitored. Most networking equipment such as enterprise-class switches and routers have monitoring facilities integrated within their software, but sometimes it is necessary to apply specialized monitoring tools such as protocol analyzers, intrusion detection systems, and forensic recorders. These tools need to be able to listen to the network traffic without disturbing it in any way, and for that job they need Traffic Access Ports or Taps. Like a doctor uses a stethoscope to listen to a patient’s heartbeat, a Tap enables a monitoring tool to listen to the data passing through a network link.

Tap technology includes a variety of Tap types with different capabilities that make it possible for monitoring tools to see all of the traffic anywhere and at any time on a medical organization’s network. The main categories of Taps are:

- **Network Taps**, which connect one monitoring tool to one fiber or copper network link, enabling the tool to listen to all of the traffic on the link—without any impact on the traffic, and without introducing a potential point of failure
- **Regeneration Taps**, which connect several monitoring tools to a single network link, enabling network managers, security specialists, and compliance officers to access the same traffic simultaneously, without conflicts
- **Aggregation Taps**, which combine the traffic passing through as many as 10 network links or switch Span ports and send all of the data to one or more tools, enabling fewer tools to monitor larger sections of the network

With services depending more and more heavily on the network, it is critical to a healthcare organization’s success to constantly monitor the health of the network.
• Data Monitoring Switches, which are high port density devices that incorporate tapping, regeneration, and aggregation functions; they also do switching and filtering to direct only traffic of interest to specific tools, increasing the efficiency of the tools; Data Monitoring Switches are ideal for sharing a pool of tools across an entire network.

• Bypass Switches, which are fail-safe access ports for in-line devices such as intrusion prevention systems (IPSs), firewalls, and Web application firewalls; they keep the network traffic flowing when the in-line device fails or is removed for maintenance or upgrade.

Some typical use cases of the various types of Taps in healthcare environments are presented in the following sections.

Use cases

Information at the bedside

A hospital is deploying wireless handheld devices so doctors and nurses can access digital health records and prescription information at the patient’s bedside. The network administrator deploys network Taps at each wireless access point so that if issues arise with wireless connectivity, a protocol analyzer can be attached to examine wireless traffic immediately, without waiting for a maintenance window or reconfiguring switches to access traffic through Span ports. The time saved by having the Taps ready and waiting at the access points can increase the quality of patient care and even save lives.

Performance, security, and compliance without competition

To keep their network-based health and business applications running smoothly, a healthcare organization employs a network administrator to maintain and tune the system; a security specialist to prevent spam, malware, and attackers from entering the network; and a compliance officer to ensure that HIPPA and PCI requirements are met. The administrator had installed Taps on critical network links to provide 100 percent visibility of the traffic, but scheduling use of the Taps between the administrator’s own...
needs and those of the security specialist and compliance officer was a problem – often someone could not get use of the Tap when it was necessary. The solution was to replace the Taps with Regeneration Taps that provide simultaneous access to the same traffic through four ports. Each of the three professionals was given ownership of one port on each Regeneration Tap, so they all had continuous access to all of the traffic at any time. They also found that they could attach a forensic recorder to the fourth port when it was necessary to capture all of the traffic for an extended period of time to investigate a security breach or data leakage problem, and the presence of the extra tool did not limit their normal traffic access.

Health insurer balances the demand

A health insurer achieved huge cost savings by implementing a customer self-help application on the Internet. Customers could connect through a Web browser to check claims status, pay bills, and receive quotes, all without human intervention – and without the costs of having humans answer the phone. The Web site is so popular that a farm of eight Web servers is needed to service all of the requests in a timely manner, and a load balancer distributes incoming requests to the different servers. They use an Aggregation Tap to combine the traffic going to each of the eight servers, and send it as a single stream to a Web application monitoring system that verifies that no packets were dropped by the load balancer. Without the Aggregation Tap, more NICs would have to be added to the monitoring system – but the system only supports four NICs, so two systems would have to be applied to see all of the traffic.

The digital hospital of the future – now!

A new hospital is being built and digital HIT systems are a focus of the planned operations. The network is, of course, a fundamental part of the building plan. The network architect knows that the network will have to carry large amounts of data, image, voice, video, e-mail, and Internet traffic, reliably and securely. Therefore traffic monitoring is essential, and a Monitoring Access Platform (MAP) is integrated within the network architecture.

At the core of the MAP are ten Data Monitoring Switches that will be deployed at key locations throughout the hospital. The Data Monitoring Switches will gather copies of
traffic from network links, Taps, and switch Span ports throughout the network, and direct them to a central network operations center (NOC) for monitoring. Through the Data Monitoring Switches, professionals in the NOC will be able to direct traffic from anywhere in the hospital’s network to any of the tools in the NOC, to quickly track down issues before they impact doctors, nurses, and patients. The Data Monitoring Switches will enable traffic from multiple links to be aggregated and sent to particular tools, and for traffic to be regenerated so multiple tools can be applied to the same traffic at the same time. They also enable the NOC personnel to select particular traffic of interest, such as specific protocol types or VLANs, to narrow down issues quickly and prevent tools from being overloaded. For instance, they can focus just on voice traffic or e-mail. Furthermore, the system is easy to operate because all ten Data Monitoring Switches, even though they are scattered around the hospital, are linked by high-speed fiber optic cables so they appear as a single logical device to the users. The network architect believes this MAP architecture is essential to enable the NOC to keep the wide variety of health and business applications on which the hospital will depend running at peak performance, with security and reliability worthy of the digital age.

The Data Monitoring Switches will enable traffic from multiple links to be aggregated and sent to particular tools, and for traffic to be regenerated so multiple tools can be applied to the same traffic at the same time.

**Director - Data Monitoring Switch Implementation**

**HIPAA compliance without risking downtime**

As part of a data security initiative for achieving HIPAA compliance in a large medical clinic, the clinic’s network architect specifies in-line data loss-prevention (DLP) appliances to confine confidential patient information to departments that have a legitimate need for it. For example, financial information will be restricted to the Finance Department, and will not be accessible in Human Resources or the medical labs. The DLP appliance examines all traffic leaving the department’s VLAN; when it detects a document with Protected Health Information (PHI) that is not allowed outside of the department, it drops the packet so the PHI is not transferred and sends a compliance warning message to the originator.

However, interdepartmental network access is critical to the clinic’s functioning, so the network architect wants to ensure that network traffic keeps flowing even if a DLP appliance loses power, fails, or is removed for maintenance or another reason. The architect satisfies this requirement by attaching each DLP appliance to the network through a Bypass Switch, which is a device specifically designed to keep traffic flowing in all of these conditions.
Bypass Switches are also installed at departmental gateways that are not receiving DLP appliances at this time; the Bypass Switch enables a DLP appliance to be added at a later date without incurring any downtime or disturbing the network traffic in any way. In addition, the Bypass Switch adds value even without a DLP appliance attached, because its remote management interface allows operators to monitor network traffic through the link continuously, and to attach specialized monitoring tools if issues demand deeper investigation.

**Summary**

Information and communications technologies are changing the way medicine is practiced, driving down costs and increasing the quality of patient care across the board. All of the new digital health initiatives depend on the foundation of a rock-solid, high-performance network. To ensure the necessary performance, security, and reliability, the network must be on a wellness program, and not depend on trips to the emergency room when something goes wrong. The network wellness program means that systems and operators must be able to monitor all of the network traffic at all times, being alert to performance bottlenecks, security breaches, data leakage, and regulatory compliance. Tap technology gives monitoring systems 100 percent visibility of network traffic without interfering with that traffic or introducing a potential point of failure. It also enables multiple users to access traffic simultaneously, for traffic from multiple links to be aggregated into a single view, and for monitoring functions to be centralized in the NOC of large hospitals, medical office buildings, and clinics. HIT investments are protected and their ROI is increased when a Monitoring Access Platform built with Tap technology is an integral part of the medical information network.