



2009 was truly remarkable from an economic, political, and financial stand-point. It seemed each passing day brought a new challenge for ASK, our vendors and most importantly our clients to navigate. We came to find, as no surprise, that specific knowledge, experience and operational efficiencies are required for survival. Improved operational efficiencies and increased employee productivity both achieved through various technology implementations must be front and foremost in FY2010.



Inside this issue:

How Much Longer Are You Going to Hold Onto That Ethernet Cable? 2

Why XP Will Never Die 3

Stephen Pirolli, ASK Technologies, Inc.

Another Cost Savings Program for ASK Clients

by Curt Schappell, Tech Staff

The ACH (Automated Clearing House) Network is a highly reliable and efficient nationwide batch-oriented electronic funds transfer system governed by the NACHA-The Electronic Payments Association, which provide for the inter-bank clearing of electronic payments for participating depository financial institutions. The Federal Reserve and Electronic Payments Network act as ACH Operators, central clearing facilities through which financial institutions transmit or receive ACH entries.

ACH payments include:

- Direct Deposit of payroll, Social Security and other government benefits, and tax refunds
•Direct Payment of consumer bills such as mortgages, loans, utility bills and insurance premiums
•Business-to-business payments
•E-checks
•E-commerce payments
•Federal, state and local tax payments

vendor checks and to mail them, and thus reduce the costs of these weekly functions. Assuming that your bank is a qualified and participating ACH institution, all that is required is that each of your employees or vendors provide you with the ABA Routing Number of their Bank and the checking or savings account at that bank into which the payment is to be deposited and an email address to send the payment notification with the information

The basic concept behind ACH is to eliminate the need to print payroll or

continued on pg. 2

WELCOME NEW CLIENTS



Firewall Security: The Next Generation

featuring Palo Alto by Geoff Smith, Tech Staff

Over the past two years there has been a steady increase in Web 2.0 type applications used both on the Internet and within an organizations perimeter, which

has created a number of challenges for IT organizations using traditional legacy port-based firewalls. These challenges are isolated into three distinct areas of

security policy and compliance. The three main areas are Content, Application and User Identity.

continued on pg. 3

# Another Cost Savings Program for ASK Clients

*continued from pg. 1*

pertaining the sender of the payment, the payment amount deposited, the date of deposit, the bank account, and the reasons for the payment deposited.

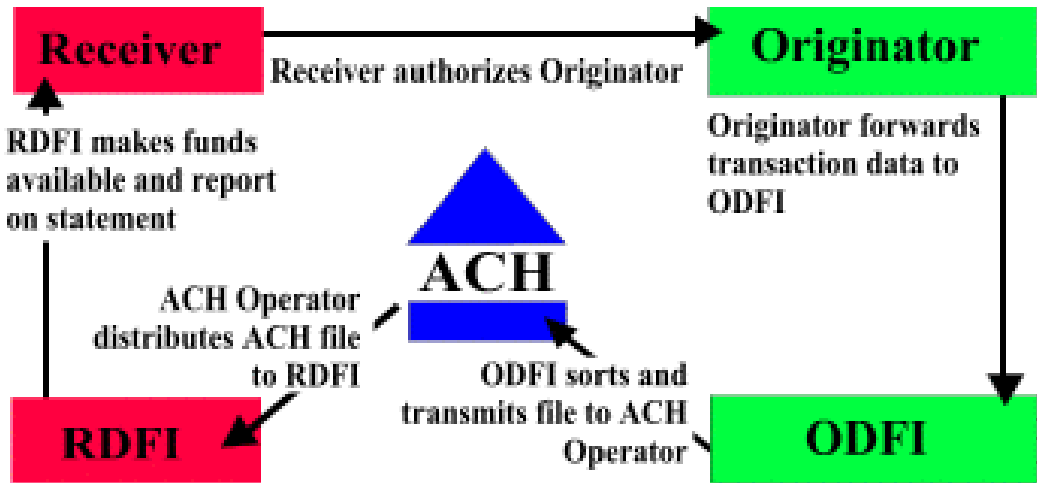
Once employees or vendors are updated with this information, your payroll and accounts payable systems can be easily enhanced to no longer print paychecks or vendor checks, and instead electronically transfer the funds owed

directly into their bank account via the ACH process. Instead of receiving a check in the mail, an email is sent to notify the recipient of the payment and the payment is automatically posted to the recipient's bank account.

As we all know, more and more companies are cutting their operational costs by utilizing ACH to make their payments to their employees and vendors. If you are still

paying all of your bills with checks, you might want to take a serious look at the ACH payment process being made part of your current payroll and payables software applications.

Please contact your local **ASK** sales rep at (610) 617-0300 for more information regarding the installation of the ACH software enhancements for your current payroll & payables software applications.



**ORIGINATOR**  
Your Business

**ODFI :Originating Depository Institution**  
Your Bank

**RDFI: Receiving Depository Financial Institution**  
Your Employee or Vendor's Bank

**RECEIVER**  
Your Employee or Vendor & their Bank

# How Much Longer Are You Going to Hang Onto That Ethernet Cable? *as featured in Network World*

As more enterprises deploy wall-to-wall Wi-Fi, they're finding end users voting with their network interface cards: given a choice, they go with wireless rather than wired access.

In pervasive wireless LANs (WLAN), depending on the industry segment, ever-more IT departments are finding 50% to as much as 90% of edge switch ports sitting idle.

One well-known North-east college is starting to evaluate 802.11n as an upgrade to its campus-wide 802.11abg WLAN, based on Cisco gear.

*continued on pg. 5*



## Why XP Will Never Die

*as featured in CRN*

So how much do businesses love Windows XP? Enough to pay up front for license packs and have them stored away by their solution provider partners, that's how much. Businesses want to be sure they can get their hands on the operating system well into the future, even after the arrival of Windows 7. The fact that many businesses want to stick with XP flies in the face of Microsoft's efforts to let XP fade into the rearview mirror.

With Windows 7, Microsoft is offering XP Mode, which uses virtualization to run legacy XP apps within Windows 7. But the shaky performance of XP Mode test builds, combined with the security and management implications, are giving customers even more reason to stay on XP. What's more, Microsoft is going to have to grapple

with lingering anti-Vista sentiment, even though Windows 7 is being 'praised' within the Microsoft channel as a back-to-basics OS that is everything Vista should have been.

"Corporate America and the general public got burnt and screwed with Vista," said one solution provider. "And they are not going to let that happen again." Microsoft is trying to counteract the Vista loathing by portraying Windows 7 as a kinder, gentler OS that offer a simpler and more pleasing experience, claiming it requires "less waiting, less clicks, less hassles connecting to things...just less complex."

With that in mind, it is important to remember that Windows 7's biggest competition is not Vista or the Mac OS X. It's Windows XP, an 8 year old OS that remains the

de facto standard for a large swath of the IT industry. XP works just fine for vertical market customers like nursing homes and police departments that run specialized, custom-built applications, and these organizations don't even have Windows 7 on their radar as yet.

Microsoft insists that Windows 7 will run well on smaller devices, which wasn't the case with Vista. But Microsoft isn't offering an upgrade path from XP to Windows 7, and its expectation is that customers will migrate to the new OS on new hardware. Given the continued economic uncertainty, companies aren't exactly champing at the bit to make that type of capital expenditure.

What do you think of the Windows 7 vs. XP battle?



*"...Windows 7's biggest competition is not Vista or the Mac OS X. It's Windows XP..."*



## Firewall Security: The Next Generation

*continued from pg. 1*

The days of a one size fits all policy for IT security and compliance are long gone, this approach commonly referred to as a Least Common De-

nominator (LCD), which results in a policy that is not comprehensive enough to meet the requirements of the production business require-

ments. Most companies have excellent perimeter security policies that

*continued pg. 4*



# Firewall Security: The Next Generation

*continued from pg. 3*

block 99% of unwanted attacks from ever reaching the inside of the network from the Internet. Unfortunately, the internal network policy is not as simplistic, because the internal users are considered "trusted users" and therefore they require a more relaxed security policy outbound to conduct day to day business.

Most port-based firewalls are ineffective at identifying and controlling Internet bound applications because of their reliance on port and protocol as a means of traffic classification. As a result, both users and applications are capable of bypassing most infrastructure and security policies using a variety of techniques such as tunneling another application, sneaking across port 80, hopping ports or using SSL. The lack of visibility and control means that port-based firewalls are no longer the central control point of the security policy within the network infrastructure.

In order to restore the firewall as the strategic center of the security infrastructure, Palo Alto Networks developed a traffic classification tech-

nology that accurately identifies the applications, irrespective of port, protocol, SSL, or evasive tactic. The result is App-ID™, which is a traffic classification technology that enables administrators to determine exactly which applications are running on their network.

Whereas port-based firewalls use only one mechanism of traffic classification, App-ID goes well beyond any other network security technology available, inspecting all of the traffic passing through the firewall, with one or more of identification techniques – including application protocol detection and decryption, application protocol decoding, application signatures, and heuristic analysis. The application identity is then used as the basis of the security policy for outbound traffic.

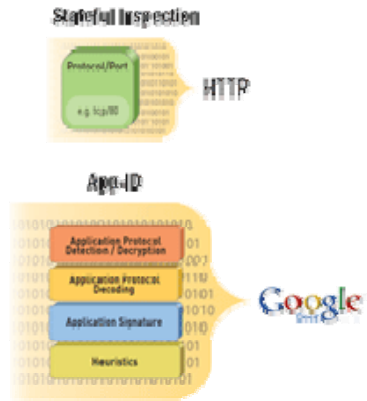
Now, rather than react to the discovery of a strange application by summarily blocking it, the administrator can take a more balanced and informed approach by learning more about the application and then safely enabling its usage or blocking it based on

the security risks. With App-ID, Security administrators can now:

- Improve network visibility by accurately identifying application traffic irrespective of port and protocol.
- Enhance security by dictating access rights based upon the actual application traffic as opposed to simply the port and protocol.
- Increase malware prevention effectiveness by narrowing down the number of unauthorized applications traversing the network.

Unfortunately, today's port-based firewalls rely heavily on IP addresses as a means of identifying and controlling user activity.

Palo Alto Networks User-ID technology addresses the lack of visibility into user activity by seamlessly integrating with Active Directory to dynamically link an IP address to user and group information. In Citrix and terminal services environments, User-ID can associate the individual user with their network activity, enabling IT to



*App-ID™ is a traffic classification technology that enables administrators to determine exactly which applications are running on their network.*

*App-ID goes well beyond any other network security technology available, inspecting all of the traffic passing through the firewall, with one or more of identification techniques.*

*continued pg. 5*

## How Much Longer Are You Going to Hang Onto That Ethernet Cable? *continued from pg. 2*

Parts of the network are saturated with lots of users and heavy traffic because, despite plenty of Ethernet ports, students use wireless almost exclusively. "We think 11n will reduce but not totally eliminate wired ports," says the campus networking director.

Colleges and universities have been among the first to discover and tackle what is, for IT, an entirely novel development and an issue that touches a nerve.

"We haven't been rushing around looking to

pull out wired switches," said one networking director who had recently deployed a campus-wide 802.11n WLAN. "But as the existing wired infrastructure reaches 'end of life' and we look towards replacement, we're definitely going to be evaluating a scaled-back deployment of wired."

The California State University system of 23 institutions did a port-by-port analysis of Ethernet use in preparing a rollout of 802.11n (upgradeable to 802.11n) WLANs on all campuses. Not a single

campus had greater than 50% wired port use, and most had far less than that, says Michel Daviddoff, CalState's director of cyberinfrastructure services.

A careful analysis of the California State University system of 23 institutions concluded that by reducing Ethernet ports to reflect actual usage, they could eliminate 2,500 switches, and save about \$30 million over five years in capital costs, hardware staging

*continued pg. 6*



*"...despite plenty of Ethernet ports, students use wireless almost exclusively."*

## Firewall Security: The Next Generation

*continued from pg. 4*

deploy granular security policies. With visibility into user activity, enterprises can monitor and control applications and content traversing the network based on the user and group information stored within the user repository. User-ID enables IT to:

- Regain visibility into user activities relative to the applications in use and the content they may generate.
- Tighten security position

by implementing policies that ties application usage to specific users and groups, as opposed to simply the IP address.

User-ID gives an administrator complete visibility into the application activity at a user level, not just an IP address level and in so doing, addresses a key requirement in regaining control over the applications traversing the network. When used in conjunction with App-ID, and

Content-ID technologies, User-ID enables IT organizations to enjoy unmatched policy-based visibility and control over users, applications and content and the enterprise network infrastructure.

Accurately identifying the applications traversing the network is only part of the challenge IT departments face with today's Internet-centric environment. Inspecting permitted application

*continued pg. 6*



You can also click this link for a brief, product tutorial:

<http://www.paloaltonetworks.com/literature/video/firewall/>

**ASK Technologies, Inc.**

7 Bala Avenue  
Suite 201  
Bala Cynwyd, PA 19004

610-617-0300 Office  
610-617-0307 Fax  
[info@asktech.com](mailto:info@asktech.com)

*For operational excellence  
at predictable costs, turn  
to ASK.*

## How Much Longer Are You Going to Hang Onto That Ethernet Cable? *continued from pg. 5*

And that didn't include electricity and heating/cooling savings.

No one, repeat no one, is saying scrap the Ethernet cabling and edge switching infrastructure tomorrow. But plenty of IT professionals are starting to ask ex-

actly what the real bandwidth requirements of their users and applications are, and how these change in peaks and troughs during a day or week.

For industries, companies and locations where mobility is a primary en-

abler of productivity, the answers to these questions can be used to make realistic assessments of when and where to rely on the WLAN – a well-designed, well-managed, secure WLAN – and cut the cord for most if not all users.



## Firewall Security: The Next Generation

*continued from pg. 5*

traffic at performance levels that satisfy high speed network demands becomes the next significant challenge, and one that is addressed by an innovative technology

authorized file transfers, detect and block a wide range of threats and control non-work related web surfing.

If you organization is

ments and concerns to see how a Next Generation Firewall like Palo Alto Networks can streamline and enforce a comprehensive approach to IT security.



called Content-ID.

Content-ID melds a uniform threat signature format, stream-based scanning and a comprehensive URL database with elements of application visibility to limit un-

interested in learning more about the potential threats and mitigating data leakage and controlling Web 2.0 applications, **ASK** would like to discuss and review your Security policy require-

If you would like to learn more about how a Next Generation Firewall can eliminate and solve most security policy concerns, contact your local **ASK** sales rep at (610) 617-0300 to setup a meeting.