Broadcom App-IQ Technology for Web 2.0 Application Intelligence in the Enterprise Edge Network

Sujal Das
Product Marketing Director
Network Switching

Joseph Tardo
Associate Technical Director
Network Switching

April 2012

Introduction

Usage patterns with respect to applications in the enterprise are changing, driven by the increasing use of social networking, browser-based file sharing, and peer-to-peer applications. Such applications, sometimes referred to as Web 2.0 applications, typically have both an upside and a downside in terms of impact on the business and on the network. The upside is that these applications enable business collaboration and improve productivity. The downside is the potential that these applications flood the network with unwanted traffic, harming employee productivity and risking legal and copyright exposure of enterprise's proprietary data. The use of such applications results in new traffic patterns in the network that are not straightforward to distinguish. Providing visibility of such traffic patterns to IT managers and implementing policy actions on them today is out of reach for many, since it requires sophisticated and expensive equipment. Broadcom's *StrataXGS*® architecture-based Ethernet switches support App-IQ (application intelligence) technology that enables unprecedented visibility into Web 2.0 traffic patterns in the enterprise network. App-IQ enables the necessary sophisticated traffic visualization technologies to be implemented directly in enterprise edge switches.

This white paper explores the use of Web 2.0 applications in the enterprise, their impact on the performance of the network, and the available solutions in the industry for traffic visualization. It introduces Broadcom's App-IQ technology, which is available as an integrated feature in its latest generation of Enterprise LAN Ethernet switch solutions. Together with integrated WLAN capabilities, these switch solutions form the cornerstone of leading switch OEM products, as they deliver on the promise of mobility and visibility required in current and next-generation networks. This paper also describes how this technology can help IT managers implement policies for Web 2.0 traffic patterns using cost-effective, power-efficient, network edge and aggregation switches.

Rising Use of Web 2.0 Applications in the Enterprise

Industry studies[1] indicate that there is increasing use of the following applications in the enterprise.

Social networking applications: Active usage of these applications (e.g., Facebook apps, games, social plug-ins, and posting) more than tripled in the 2010-2011 time frame.

Peer-to-peer (P2P) applications: P2P file sharing and video streaming are popular applications. In addition to being a common source of pirated music and movies, P2P applications have been at the heart of some high-profile examples of inadvertent sharing of proprietary or confidential data. However, many P2P applications can be used to deliver a service or improve productivity. About 10% of applications used in a typical enterprise are based on P2P technology. A study conducted in popular

[1] Examples: Applications Usage Risk Report 2011-2012, and Controlling P2P Applications at www.paloaltonetworks.com; Impact of Web 2.0 on the Enterprise, © 2010 IANS at partner@iansresearch.com.

German universities shows that more than 50% of the network bandwidth is consumed by P2P applications.[2]

Browser-based file-sharing applications: Some of these applications fall in the P2P category. Two clear use cases are emerging within the browser-based file-sharing market: work and entertainment. There are over 65 different browser-based file sharing variants, and about 20% of them are actively used in enterprises.

New Visibility Challenges in the Enterprise Network

The following table shows differences between past and present enterprise applications:

Yesterday's applications	Today's applications
Applications use well-known ports.	Web 2.0 applications ride over Hypertext Transfer Protocol (HTTP).
Can easily tell file transfer protocol (FTP) from Simple Mail Transfer Protocol (SMTP).	Can't tell images from videos, file downloads, or uploads from email or chat.
Homogeneous managed corporate desktops.	Personal devices, mobile devices, remote access.
Simple permit/deny policy goals.	Policies to access control information flow, QoS policies, acceptable use policies.
Outsider threat is the main concern.	Internal compliance is the main concern.
Data is maintained in isolated departmental servers.	Data is stored in many places, e.g., removable media, enterprise cloud.

Unlike the traditional enterprise applications of yesterday, the new Web 2.0 applications pose challenges to IT managers in two distinct ways:

- Most of these applications consume a lot of bandwidth in the network. Some help productivity, some (such as VoIP) are bound by requirements in terms of needed quality of service from the network, and others may have legal implications because content used violates copyright laws.
- Traditional network switches and firewalls lack full visibility into such applications. Sophisticated and expensive equipment is needed to enable effective policies for such applications.

[2] Ipoque Internet Study, www.ipoque.com.

As a result of these challenges, the level of sophistication required in network equipment is changing, especially in the ability to classify traffic. At a high level, there are three degrees of traffic classification:

1. Traditional classification: Traffic traversing through network equipment such as network switches is classified based on fields in the layer 2, layer 3, or layer 4 headers. Such features are available in most network switches and routers today.

2. Deep packet inspection: In this scenario, the network equipment can look deeper into the packet—beyond the layer 2, layer 3, or layer 4 headers—into the application headers and even the payload, as long as the fields of interest are at fixed locations in the packet. By doing so, such equipment can identify many applications but may only be able to take actions on a packet-by-packet basis. These features are available in some network switches today.

3. Stateful packet inspection: In this scenario, network equipment needs to maintain state of the packets it classifies. Fields can be matched at arbitrary offsets in payloads, and actions can be applied to entire flows. Some applications use dynamically assigned TCP and UDP port numbers. Classification of such applications requires the ability to discover the data connections to be classified by parsing the connections where the port assignments are made. In some cases, the application of signatures to the allowed traffic is used to identify the application based on its unique properties and related transaction characteristics. Many Web 2.0 applications fall in this category. Stateful packet inspection features are available only in specialized network switches or dedicated appliances today.

Intelligence Needed at the Enterprise Edge

Currently available solutions for classifying Web 2.0 traffic and enforcing policies are designed for the wide area network (WAN) and are typically deployed at the core of the network. They are sophisticated and dedicated appliances, sometimes implemented using software, and can cater to WAN access speeds only. Some of these centralized appliances can scale to a very large number of flows and applications, classify encrypted packets, and apply intelligent heuristics when applications cannot be identified. These solutions solve important problems in the enterprise today.

However, when price-performance and cost-effective scalability become important, new innovations are needed to enable Web 2.0 application deployment in small to large enterprises. Multiple network design trends are pushing intelligence to the network edge:

- General trends for building high-performance, cost-effective, scalable networks focusing on building intelligence at the edge. The core of the network comprises aggregation switches and serves as a “fat pipe” for connecting the intelligent edge switches.

- New "de-perimiterized" usage models create an open and dynamic local area network (see Figure 1). In this model, IT managers need ways to visualize what users are doing and enforce policies right at the edge. Enforcing policies at the core is a centralized approach that does not scale adequately in the de-perimiterized enterprise, as not all "east-west" traffic is guaranteed to flow through aggregation switches, and multipath routing complicates deploying devices that need to inspect traffic in both directions.

- As discussed earlier, Web 2.0 traffic can include rogue traffic that burdens the network, destroying productivity. IT managers need to protect the oversubscribed access layer from such traffic. The LAN edge must be able to classify such traffic and enable necessary policies right where the traffic enters the network.

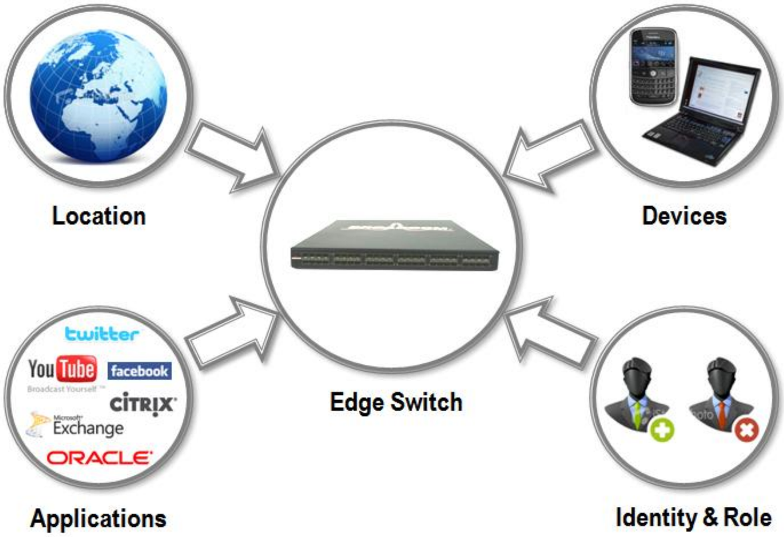


Figure 1: The need for intelligence at the edge of the enterprise network

.

Introducing App-IQ and Benefits

App-IQ is a new technology that enables enterprise wiring closet edge and aggregation switches to recognize applications running over HTTP and those that do not use standard ports – typical characteristics of Web 2.0 applications. It enables unprecedented traffic visualization at the edge of the enterprise network, where Web 2.0 traffic is initiated by end-user devices. IT managers can now provision enterprise edge switches to understand and analyze Web 2.0 traffic, and can collect application-based traffic statistics and apply policies to help improve productivity and the user experience as easily as they can using ACLs today.

Figure 2: Broadcom App-IQ for ubiquitous application-level intelligence in the enterprise LAN

Since App-IQ is available as an integrated silicon feature in the latest generation of Broadcom StrataXGS enterprise LAN switch solutions, OEMs can now enable application-level intelligence in cost-effective access and aggregation layer switch systems. App-IQ is an incremental feature added to the proven and well-deployed Broadcom ContentAware™ engine, which is available in existing StrataXGS enterprise LAN switch solutions. Currently deployed ContentAware classification and policy implementations in management software can be easily extended to enable Web 2.0 application-level intelligence.

In addition, App-IQ is lightweight and flexible, offered as an integrated switch solution for ubiquitous deployment. Application-level intelligence is no longer limited to specialized appliances or expensive "sidecar" processors. Using these flexible StrataXGS switch silicon solutions that also implement integrated wireless LAN features, significant system-level innovation and differentiation can be achieved in the lucrative fields of enterprise network visibility and mobility.

App-IQ Operation and Scope

At a high level, App-IQ includes the following operational characteristics:

- Traffic is first classified based on the traditional L2, L3, or L4 header information and can allow or deny the traffic.
- Application signatures are then applied to the allowed traffic to identify the application based on unique application content, which might be present anywhere in packets at arbitrary offsets.
- Statistical, transaction, and other unique properties of traffic can be collected and used to apply additional context-based signatures to detect or refine application identification.

All of the above functions are executed at line rate. The application recognition features, including signatures, are self-contained within the Broadcom StrataXGS switches that implement App-IQ. No additional processor or memory is required. The number of users and applications supported using the on-chip App-IQ technology is optimized for scaling in wiring closet applications. There is minimal load on the host CPU, as all required processing is accomplished using on-chip processing pipelines. External signature matching can be enabled as an option for additional scaling for certain use cases, such as classification by means of an external URL database. Using these integrated functions, IT managers can implement, for example, the following policies:

- **Analytics:** Identify what applications are running on the network. Provide flow-based statistics by application. Provide visibility to user and switch port.
- **Compliance:** Enforce acceptable use policies. Allow approved mission-critical apps. Block unapproved, unproductive apps.
- **Application Optimization:** Deploy a branch office router with constrained bandwidth link. Priority is given to mission- critical applications and to others on a best-effort basis.
- **Parental Controls:** Block sites with objectionable content. Enable URL filtering.
- **P2P Controls:** Block illegal or objectionable P2P traffic, while allowing others that help productivity or enhance user satisfaction.

It is important to note here that App-IQ resources (processing pipeline, memory for user and application flows) are optimized for enterprise edge deployments, with optimal price and performance characteristics. The implementation paradigm is different from WAN-based centralized and specialized appliance implementations, where the focus is on very large scaling of user and application flows at lower speeds.

App-IQ User Experience and Sample Use Cases

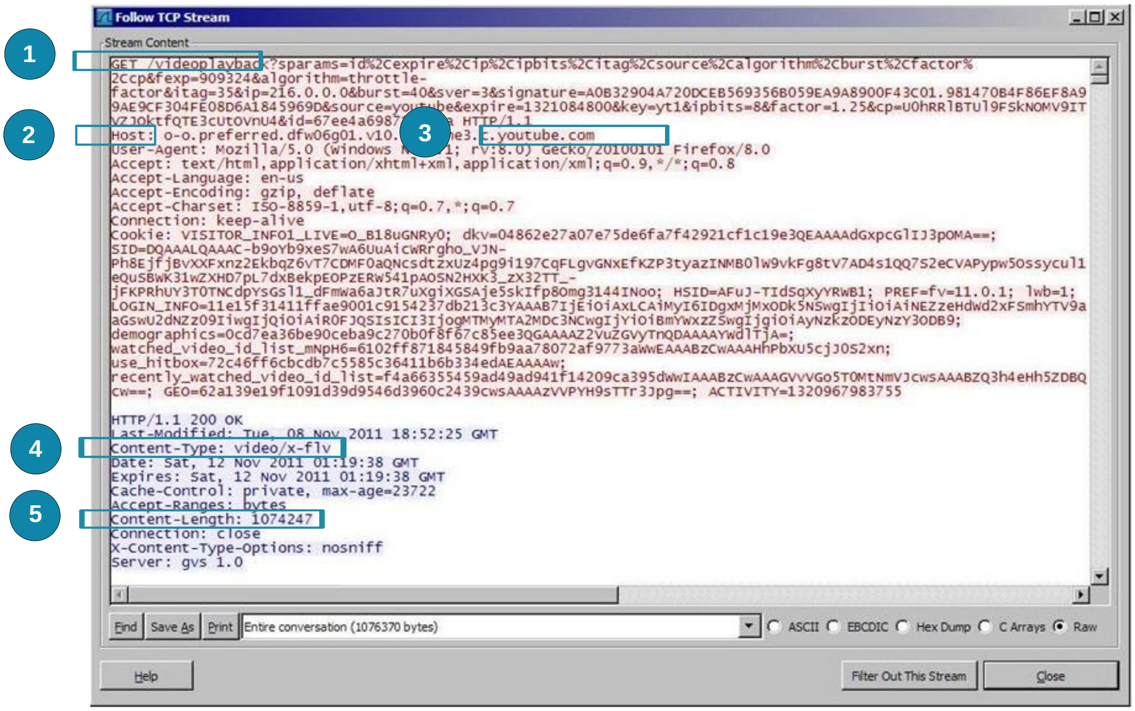
In Broadcom StrataXGS switch solutions, App-IQ is built as an incremental feature over its well-established ContentAware technology, which is used for traditional traffic classification and policy decisions. When App-IQ-based management provisioning software is implemented, Web 2.0 applications can simply appear as new traffic class options. The following is a command line interface (CLI) example for implementing quality of service (QoS) for a set of Web 2.0 applications that are grouped as unproductive applications. The applications included in this traffic class called “badapps” are Facebook Games, Yahoo Games and BitTorrent. The policy is to severely rate-limit these unproductive applications. Without App-IQ enabled, such applications cannot be classified.

```
# Enter configuration mode
BCM> config

# Define a traffic class named “unproductive”

BCM-config> define class badapps
BCM-config-class-badapps> match app http-facebook-games
BCM-config-class-badapps> match app http-yahoo-games
BCM-config-class-badapps> match app bittorrent
BCM-config-class-badapps> exit

# Configure a traffic policing QoS policy, and apply the QoS policy to the
incoming packets of GigabitEthernet 2/0/1.

BCM-config> define action severely-rate-limit
BCM-config-action-severely-rate-limit> car 0 cir 64 yellow discard
BCM-config-action-severely-rate-limit> exit
BCM-config> define qos-policy unproductive
BCM-config-qos-policy-unproductive> class bad action severely-rate-limitBCM-
config-qos-policy-unproductive> exit
BCM-config> interface gigabitethernet 2/0/1
BCM-config-GigabitEthernet2/0/1> qos apply qos-policy unproductive
BCM-config-GigabitEthernet2/0/1> exit
BCM-config> exit
```

Next, three example use cases are described. These examples use TCP screen shots from the popular Wireshark application to highlight how App-IQ is used to identify such applications.

Example 1: Recognize large video downloads

A TCP stream capture is shown in Figure 3. App-IQ processing and actions are applied to contents in the stream. First, a match is performed on the URI and Host names in the HTTP request. The relevant matches are “GET /videoplayback” and “Host:” followed by “youtube.com”, with intervening wildcard characters, as shown in boxes 1, 2, and 3. If these strings match, the next step is to match on Content-Type and Content-Length in the HTTP response. The relevant matches are: “video/x-flv”, which is the download content name, and the six-digit length field, indicating a large download. See boxes 4 and 5.



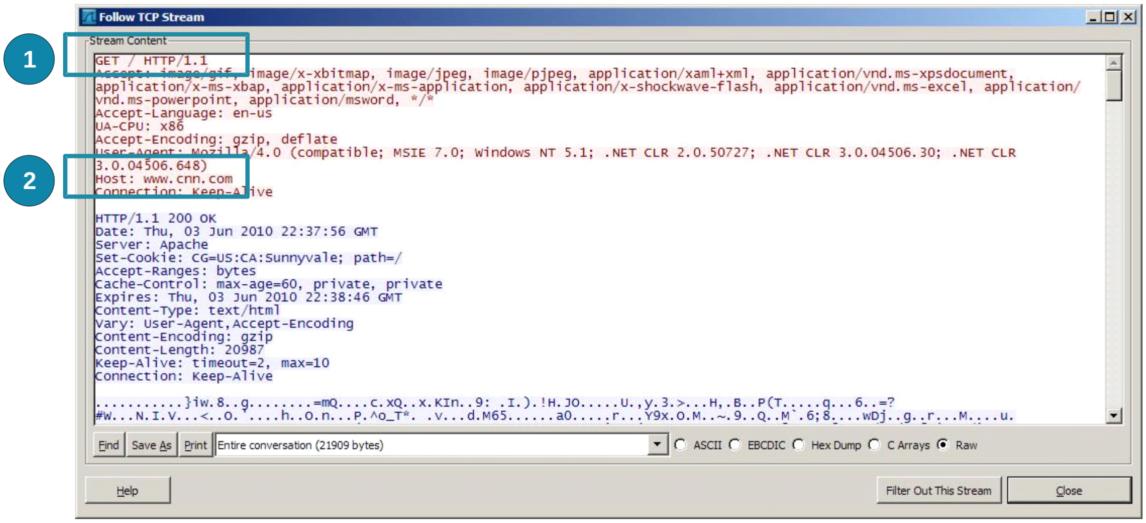
```
GET /videoplayback?sparams=id%2Cexpire%2Cip%2Cipbits%2Citag%2Csource%2Calgorithm%2Cburst%2Cfactor%
2Ccp&fexp=909324&algorithm=throttle-
factor&itag=35&ip=216.0.0.0&burst=40&sver=3&signature=A0B32904A720DCEB569356B059EA9A8900F43C01.981470B4F86EF8A9
9AE9CF304FE08D6A1845969D&source=youtube&expire=1321084800&key=yt1&ipbits=8&factor=1.25&cp=U0hRRlBTUl9FSkNOMV9IT
VZJOktfQTE3cUtOvnU4&id=67ee4a6987[illegible]a HTTP/1.1
Host: o-o.preferred.dfw06g01.v10.[illegible]e3.c.youtube.com
User-Agent: Mozilla/5.0 (Windows N[illegible]1; rv:8.0) Gecko/20100101 Firefox/8.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Cookie: VISITOR_INFO1_LIVE=O_B18uGNRy0; dkv=04862e27a07e75de6fa7f42921cf1c19e3QEAAAAdGxpcGlIJ3pOMA==;
SID=DQAAALQAAAC-b9oYb9xeS7wA6UuAicWRrgho_VJN-
Ph8EjfjBvXXFxnz2EkbqZ6vT7CDMF0aQNcsdtzxUz4pg9i197CqFLgvGNxEfKZP3tyazINMB0lW9vkFg8tV7AD4s1QQ7S2eCVAPypw5Ossycul1
eQuSBwK31wZXHD7pL7dxBekpEOPzERW541pAOSN2HXK3_zX32TT_-
jFKPRhUY3TOTNCdpYsGsl1_dFmwa6aJtR7uXgiXGSAje5skIfp8Omg3144INoo; HSID=AFuJ-TIdSqXyYRWB1; PREF=fv=11.0.1; lwb=1;
LOGIN_INFO=11e15f31411ffae9001c9154237db213c3YAAAB7IjEiOiAxLCAiMyI6IDgxMjMxODk5NSwgIjIiOiAiNEZzeHdwd2xFSmhYTV9a
aGswU2dNZz09IiwgIjQiOiAiR0FJQSIsICI3IjogMTMyMTA2MDc3NCwgIjYiOiBmYWxzZSwgIjgiOiAyNzkzODEyNzY3ODB9;
demographics=0cd7ea36be90ceba9c270b0f8f67c85ee3QGAAAAZ2VuZGVyTnQDAAAAYWdlTjA=;
watched_video_id_list_mNpH6=6102ff871845849fb9aa78072af9773aWwEAAABzCwAAAHhPbXU5cjJ0S2xn;
use_hitbox=72c46ff6cbcdb7c5585c36411b6b334edAEAAAAw;
recently_watched_video_id_list=f4a66355459ad49ad941f14209ca395dwwIAAABzCwAAAGVVVGo5TOMtNmVJcwsAAABZQ3h4eHh5ZDBQ
Cw==; GEO=62a139e19f1091d39d9546d3960c2439cwsAAAAzVVPYH9sTTr3Jpg==; ACTIVITY=1320967983755

HTTP/1.1 200 OK
Last-Modified: Tue, 08 Nov 2011 18:52:25 GMT
Content-Type: video/x-flv
Date: Sat, 12 Nov 2011 01:19:38 GMT
Expires: Sat, 12 Nov 2011 01:19:38 GMT
Cache-Control: private, max-age=23722
Accept-Ranges: bytes
Content-Length: 1074247
Connection: close
X-Content-Type-Options: nosniff
Server: gvs 1.0
```

Entire conversation (1076370 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 3: TCP stream capture for a large video download

Example 2: Blocking by domain name

A TCP stream capture is shown in Figure 4. App-IQ processing and actions are applied to contents in the stream, as shown by box 1 and box 2. In this case, standard ACL matching on IP address would be inadequate, because global load-balancing schemes can distribute content from "anycast" addresses. App-IQ, on the other hand, can recognize the domain by looking up protocol and packet content: the HTTP request (in box 1) and the Host header field that contains“cnn.com” (in box 2), respectively.



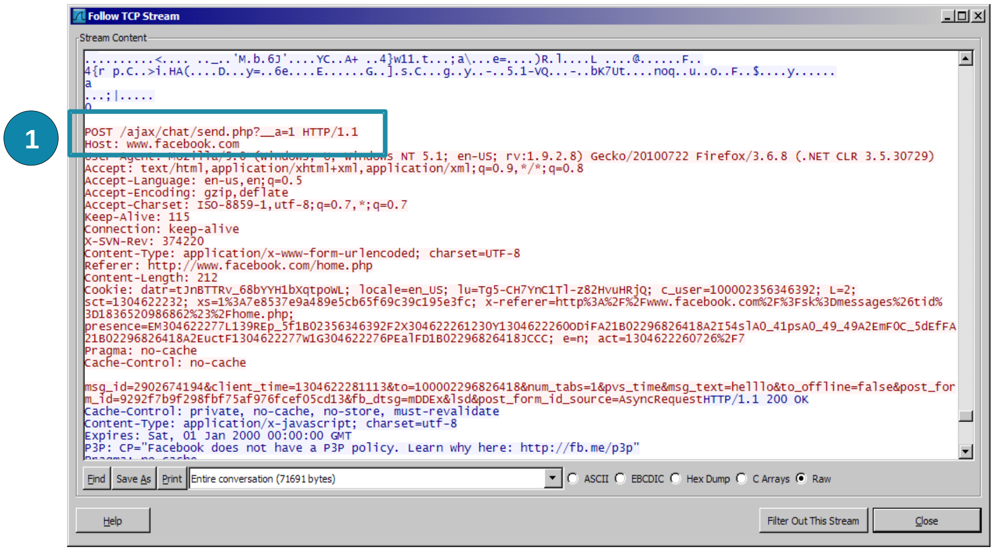
```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml, application/vnd.ms-xpsdocument,
application/x-ms-xbap, application/x-ms-application, application/x-shockwave-flash, application/vnd.ms-excel, application/
vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR
3.0.04506.648)
Host: www.cnn.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 03 Jun 2010 22:37:56 GMT
Server: Apache
Set-Cookie: CG=US:CA:Sunnyvale; path=/
Accept-Ranges: bytes
Cache-Control: max-age=60, private, private
Expires: Thu, 03 Jun 2010 22:38:46 GMT
Content-Type: text/html
Vary: User-Agent,Accept-Encoding
Content-Encoding: gzip
Content-Length: 20987
Keep-Alive: timeout=2, max=10
Connection: Keep-Alive

..........}iw.8..g........=mQ....c.xQ..x.KIn..9: .I.).!H.JO.....U.,y.3.>...H,.B..P(T.....q...6..=?
#W...N.I.V...<..O. ....h..O.n...P.^o_T*. .v...d.M65......a0.....r...Y9x.O.M..~.9..Q..M`.6;8....wDj..g..r...M.....u.
```

Entire conversation (21909 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 4: TCP stream capture for domain name related content

Example 3: Facebook chat session send

A TCP stream capture is shown in Figure 5. App-IQ processing and actions are applied to contents in the stream, as shown by the box 1. App-IQ can recognize a Facebook chat session “send” by looking up the POST method, URI string, and Host name, as shown in box 1. New transactions are matched during an HTTP persistent connection.



```
..........<.... .._..'M.b.6J'....YC..A+ ..4}w11.t...;a\...e=....)R.l....L ....@......F..
4{r p.C..>i.HA(....D...y=..6e....E......G..].s.C...g..y..-..5.1-VQ...-..bK7Ut....noq..u..o..F..$....y......
a
...;|.....
0

POST /ajax/chat/send.php?__a=1 HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
X-SVN-Rev: 374220
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://www.facebook.com/home.php
Content-Length: 212
Cookie: datr=tJnBTTRv_68bYYH1bXqtpoWL; locale=en_US; lu=Tg5-CH7YnC1Tl-z82HvuHRjQ; c_user=100002356346392; L=2;
sct=1304622232; xs=1%3A7e8537e9a489e5cb65f69c39c195e3fc; x-referer=http%3A%2F%2Fwww.facebook.com%2F%3Fsk%3Dmessages%26tid%
3D1836520986862%23%2Fhome.php;
presence=EM304622277L139REp_5f1B02356346392F2X304622261230Y1304622260ODiFA21B02296826418A2I54slA0_41psA0_49_49A2EmF0C_5dEfFA
21B02296826418A2EuctF1304622277W1G304622276PEalFD1B02296826418JCCC; e=n; act=1304622260726%2F7
Pragma: no-cache
Cache-Control: no-cache

msg_id=2902674194&client_time=1304622281113&to=100002296826418&num_tabs=1&pvs_time&msg_text=helllo&to_offline=false&post_for
m_id=9292f7b9f298fbf75af976fcef05cd13&fb_dtsg=mDDEx&lsd&post_form_id_source=AsyncRequestHTTP/1.1 200 OK
Cache-Control: private, no-cache, no-store, must-revalidate
Content-Type: application/x-javascript; charset=utf-8
Expires: Sat, 01 Jan 2000 00:00:00 GMT
P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"
Pragma: no-cache
```

Entire conversation (71691 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 5: TCP stream capture for a Facebook chat session

App-IQ Deployment Scenario

App-IQ is available in Broadcom StrataXGS switch solutions for the enterprise campus or branch edge and aggregation layer switching. Figure 6 shows a scenario where App-IQ is deployed in the enterprise campus and branch office edge switches, along with integrated WLAN capability (using the CAPWAP[3] technology available in Broadcom StrataXGS switch solutions). An integrated CAPWAP WLAN-based mobility and App-IQ-based visibility management controller can be deployed for enterprise-wide policy implementation. As users are added to the network, this edge intelligence-based deployment enables easy and cost-effective scaling by adding enterprise edge switches. App-IQ application recognition can also be implemented in the aggregation layer (not shown in Figure 6) to further enhance application flow scalability by loading an incremental set of application signatures, beyond those loaded in the edge switches.

[3] CAPWAP stands for Control and Provisioning of Wireless Access Points. CAPWAP is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points.

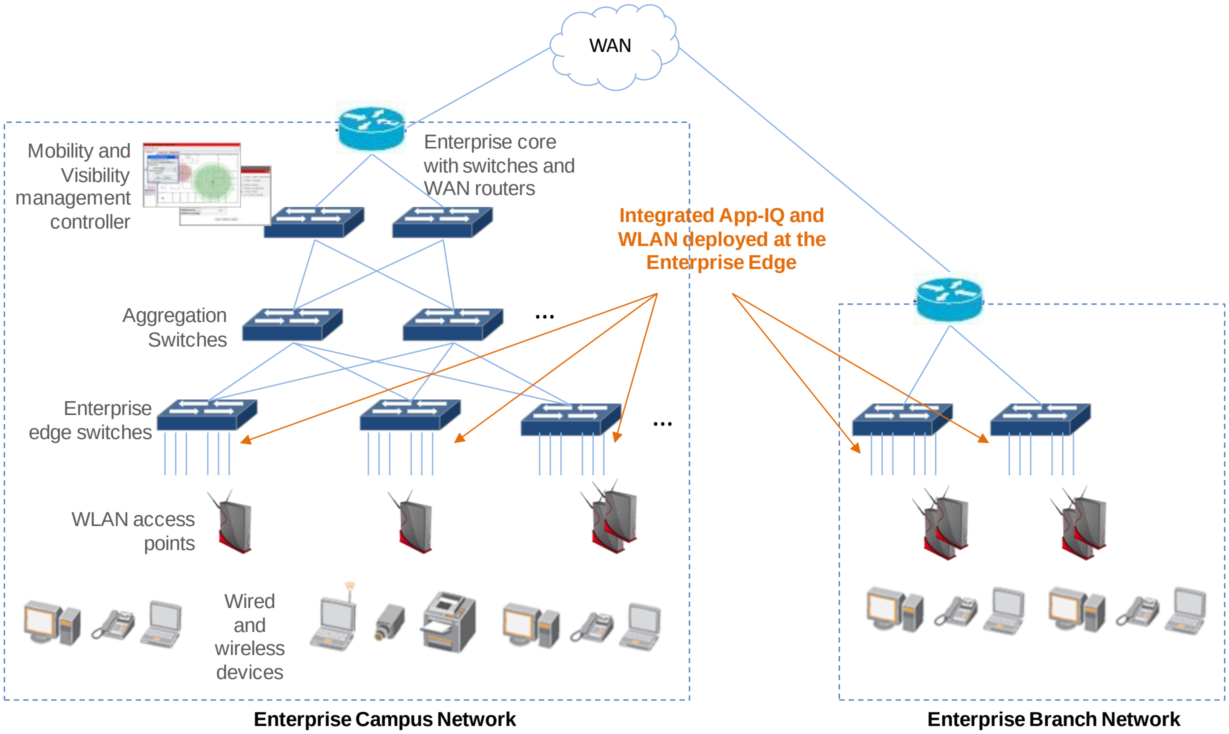

WAN
Mobility and Visibility management controller
Enterprise core with switches and WAN routers
Integrated App-IQ and WLAN deployed at the Enterprise Edge
Aggregation Switches
…
Enterprise edge switches
…
WLAN access points
Wired and wireless devices
Enterprise Campus Network
Enterprise Branch Network

Figure 6: Example of App-IQ deployment in campus and branch networks

Figure 7 shows a one-tier, or flat, access and aggregation layer implementation using either a spine-leaf architecture, which is built with stand-alone switches, or a chassis switch. Such an implementation enables high-performance connectivity and can simplify management by providing a single logical device view of the entire network and of a collection of switches or line cards in a chassis. This serves as a very high performance L2 and L3 switching fabric. Value-added functions for mobility and visibility, as required in the enterprise, are implemented in cost-effective port extender (also known as fabric extender of FEX) switches. The high-performance L2 and L3 switching fabric acts as a parent switch to the port extenders, where the latter relies on the former for all forwarding, QoS and policy services. The port extender and its parent switch enable a large multipath, loop-free, active-active enterprise LAN topology, without the use of Spanning Tree Protocol (STP). App-IQ and CAPWAP are implemented in the port extender switches to supplement the high performance L2 and L3 switching fabrics, adding unprecedented visibility and mobility features, respectively.

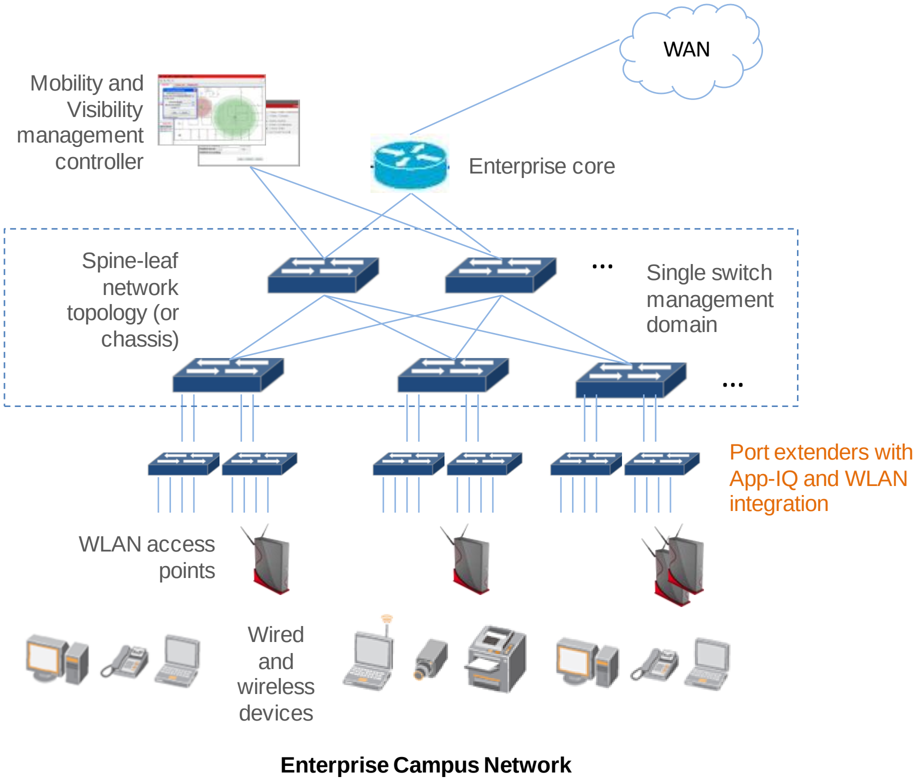

WAN
Mobility and Visibility management controller
Enterprise core
Spine-leaf network topology (or chassis)
Single switch management domain
Port extenders with App-IQ and WLAN integration
WLAN access points
Wired and wireless devices
Enterprise Campus Network

Figure 7: Port extender-based App-IQ deployment example (Branch network not shown)

Summary

Industry studies indicate that there is an increasing use of social networking, P2P, and browser-based file-sharing applications in the enterprise. There are significant differences between past and present enterprise applications. For example, many Web 2.0 applications ride over HTTP and, therefore, classification mechanisms based on well-known port numbers are simply not adequate. They consume a lot of bandwidth, are sometimes productive and at other times unproductive, and may have legal implications. Traditional network switches and firewalls lack full visibility into such applications. Sophisticated and expensive equipment is needed to enable effective policies for such applications. Currently available solutions for classifying Web 2.0 traffic and enforcing policies are designed for the WAN and are typically deployed at the core of the network. When price-performance and cost-effective scalability become important, new innovations are needed to enable Web 2.0 application deployment in small to large enterprises. Broadcom’s App-IQ technology enables unprecedented traffic visualization at the edge of the enterprise network, where Web 2.0 traffic is initiated by end-user devices. IT managers can now provision enterprise edge switches to understand and analyze Web 2.0 traffic, collect application-based traffic statistics, and apply policies to help improve productivity and the user experience.