The Internet Protocol Journal

June 2003 Volume 6, Number 2

A Quarterly Technical Publication for Internet and Intranet Professionals

In This Issue

You can download IPJ back issues and find subscription information at: **www.cisco.com/ipj**

From The Editor

Articles in *The Internet Protocol Journal* broadly fall into three categories. First, we have articles that explain well-established technologies or operational practices. Second, we offer tutorials on new or emerging protocols and systems, not yet deployed but on the horizon. Finally, IPJ brings you insights, lessons learned and opinions on aspects of networking that have not completely lived up to their promises. In this issue, you will find a mixture of all three.

Our first article is an example from the "nuts-and-bolts" category. The *Border Gateway Protocol* (BGP) is one of the core routing protocols that is widely used in the Internet and has been around for a long time. Kris Foster explains how the *BGP Community* attribute can be used in service provider networks.

Efforts to provide cellular telephones with Internet access systems have produced mixed results. Japan has been leading the way in this area with widespread deployment of iMode devices or variants thereof. Having used such a system I must say I am both impressed and somewhat frustrated. It is wonderful to receive e-mail while on a busy Tokyo train, but accessing the Internet on a tiny screen (typically a 2-inch display with a resolution of 120 x 160 pixels) is not particularly rewarding. Not to mention the bandwidth limitations inherent with this technology. Another system, the *Wireless Application Protocol* (WAP) has been implemented in most countries that offer *Global System for Mobile Communications* (GSM) cell phone service. WAP is the subject of our second article. Edgar Danielyan describes the WAP architecture and looks at some of the lessons learned from its deployment.

The push for deployment of *IP Version 6* (IPv6) is taking place on several fronts and we cover some of them in this issue. In the IETF, a recently formed group has been chartered to help design transition strategies from IPv4 to IPv6. We have a short overview of this effort starting on page 20. Additionally, both the U.S. and Japanese governments are promoting the use of IPv6 in various ways. The U.S. Department of Defense has recently adopted IPv6 as one of its official protocols. In Japan the "IPv6 Appli-Contest 2003" is underway in an effort to encourage development of software and applications for IPv6. See "Fragments," page 37–38 for further details.

Of course, not everyone is convinced that IPv6 is such a good idea, and with that in mind we bring you an opinion piece as well as a Letter to the Editor on this topic.

—Ole J. Jacobsen, Editor and Publisher
ole@cisco.com

Application of BGP Communities

by Kris Foster, TELUS

The *Border Gateway Protocol* (BGP) is the glue that binds networks and their individual policies together. Several attributes are passed along and possibly modified with each individual prefix, one of which is the *community* attribute. BGP communities are described poorly in most texts. The problem is not in explaining how they fit into the protocol, but in how to apply these to the real world. In this article I describe how they can be applied within a service provider network and between service provider networks. However, communities are not limited to service providers and can be applied creatively in enterprise networks.

The density of interconnection among service providers, and the various business agreements or political policies, means that controlling who can talk to whom over your network can become difficult. At a basic level there are two types of agreements between service providers: transit/customer and peers.

- Customers pay to receive every prefix from a transit provider.
- Customers advertise only the prefixes they own (along with their customers' prefixes) to the transit provider.
- Peers agree to send only their customers' prefixes to each other, and not other peers' prefixes.

Several methods are available to implement these policies. They can include prefix filters, *Autonomous System* (AS) path filters, and communities. With only prefix and AS path filters, service providers must ensure that as a new customer or peer is added, the prefixes and *AS Numbers* (ASNs) associated with the customer (and potentially *their* customers) are added to the filters on all of the BGP edge routers. This can be automated with scripts, possibly in combination with a route registry database. Very small service providers may be able to manage such a scheme, but as they grow and customer churn begins, this can quickly get out of control. The more time network operators spend in router configurations, the greater likelihood of human error. Communities provide an elegant solution for these problems.

The BGP Community Attribute

Within an AS, all BGP-speaking routers run *Internal BGP* (iBGP) in a full mesh to prevent routing loops (route reflectors can be used to relax this rule). This means that every BGP-speaking router passes its prefixes to each of its iBGP neighbors. ASs that are adjacent typically run eBGP on directly connected routers. All BGP routers share their prefixes—that is, the network number, network mask, and BGP attributes with each other—allowing each to run its own best-path selection algorithm. As a prefix is passed between ASs, an attribute called the AS-PATH is updated with the corresponding ASN. The AS-PATH is used to prevent routing loops between eBGP neighbors.

A community is a BGP attribute that may be added to each prefix. Communities are transitive optional attributes[1], meaning BGP implementations do not have to recognize the attribute and at the network operator's discretion carry it through an AS or pass it on to another AS. The community attribute can be thought of as simply a flat, 32-bit value that can be applied to any set of prefixes. It can be read as a 32-bit value or split into two portions, the first 2 bytes representing an ASN and the last 2 bytes as a value with a predetermined meaning. The format of the community attribute is shown in Figure 1.

The values **`0x00000000`** through **`0x0000FFFF`** and **`0xFFFF0000`** through **`0xFFFFFFFF`** are reserved. Most modern router software displays communities as **`ASN:VALUE`**. In this format the communities **`1:0`** through **`65534:65535`** are available for use. The convention is to use the ASN of your own network as the leading 16 bits for your internal communities and communities that you accept from and send to your customers.

Three communities are defined in RFC 1997[2] and are standard within BGP implementations: NO-EXPORT (**`0xFFFFFF01`**), NO-ADVERTISE (**`0xFFFFFF02`**), and NO-ADVERTISE-SUBCONFED (**`0xFFFFFF03`**). Additionally, NO-PEER (**`0xFFFFFF04`**) has been proposed in an Internet Draft[3].

NO-EXPORT is commonly used within an AS to instruct routers not to export a prefix to eBGP neighbors. For instance, subnets of a larger block can be advertised to influence external AS best-path selection, and those not required for this traffic engineering purpose may be tagged NO-EXPORT to prevent them from being leaked to the Internet (and thus contributing to unnecessary global routing table growth). If a neighboring AS accepts this community, it can be used to selectively leak more specifics for traffic engineering but limit their propagation to just one AS.

NO-ADVERTISE instructs a BGP-speaking router not to send the tagged prefix to any other neighbor, including other iBGP routers.

NO-ADVERTISE-SUBCONFED is used to prevent a prefix from being advertised to other members within a *confederation*. A confederation can be thought of as a single AS, broken down into sub-ASs. The use of confederations within service provider networks is rare or nonexistent, so they are not considered here.

Finally, NO-PEER is used in situations where traffic engineering control over a more specific prefix is required, but to constrain its propagation only to transit providers and not peers. That is, the prefix is advertised from AS to AS provided there is a transit/customer relationship, unlike NO-EXPORT, which restricts propagation of the prefix to only the adjacent AS. Because peers of the various upstream providers will not see this prefix, the larger prefix encompassing the more specific one is used for routing, thereby conserving an extra entry for some in the global routing table. At this time the community is not recognized by major vendors and requires manual implementation.

Adding Depth: The Extended Community

The current community attribute is getting an upgrade with a new transitive-optional attribute (Type 16) called the *Extended Community*[4]. Missing from regular communities was any real form of structure. The current Internet Draft defines the Extended Community as an 8-octet value as shown in Figure 1. The first octet specifies the type (and optionally the second value can specify a subtype). This value dictates the structure given to the remaining octets.

The Type field gives the community some immediate flexibility. The first is the use of bit 0 to represent whether the community is registered with the *Internet Assigned Numbers Authority* (IANA) or if it is specified by the *Internet Engineering Task Force* (IETF). The second bit gives the Extended Community a coarse scope, either *Transitive*, meaning it may be passed between ASs, or *Non-Transitive*, meaning it should be carried only within the local AS.

The Internet Draft also specifies numerous types available for use as templates.

The *Route Target Community* is already in popular use within *Multiprotocol Label Switching Virtual Private Networks* (MPLS VPNs). The Route Target Community identifies a set of routers that may receive this prefix. In the MPLS VPN context, this is necessary to limit the resources required to support individual VPN services; only routers that are part of the individual VPN need to hear about the routes within the VPN.

The *Link Bandwidth Community* gives the network operator additional control in influencing the best path selection. As prefixes are learned from eBGP neighbors, the local neighbor applies this community to specify in bytes per second the bandwidth of the link. It is a *Non-Transitive Community*, so its scope is limited to the local AS.

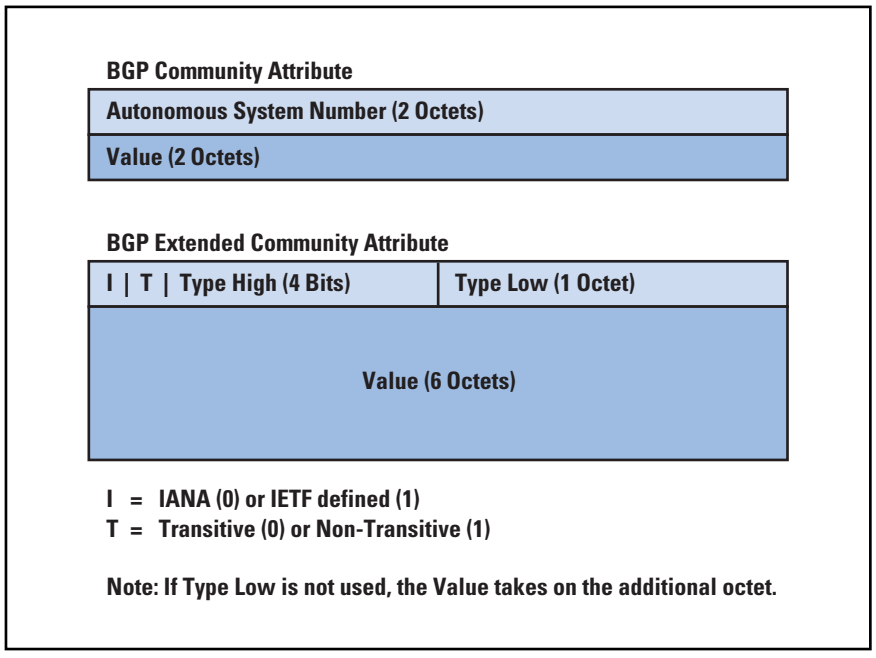


Figure 1: Community Formats

Intra-Autonomous System Communities

Policy control using communities within an AS can go farther than this, and their true value is evidenced when they are used to create new and complex policies. If we take our example of the three basic types of neighbor relationships, customers of a transit provider will want to send their customers' prefixes but not their peers' prefixes. To distinguish between a customer's prefix, a peer's prefix, and a transit provider's prefix, we can add a community to each as we learn it from the neighbor.

When advertising a prefix to a customer, peer, or transit provider, simply match all prefixes carrying the communities associated with the correct policy. As shown in Figure 2, all prefixes received from customers are tagged with **`53:100`**, peers are tagged with **`53:200`**, and transit is tagged with **`53:300`**. Our basic definition of a customer is someone who expects to receive all prefixes, so each customer-facing BGP session is preconfigured to send all prefixes matching **`53:100`**, **`53:200`**, and **`53:300`**. Again, from our definition of a peer being someone who wants to see only our customers, we would preconfigure all of our peers' BGP sessions to send only prefixes tagged with **`53:100`**.

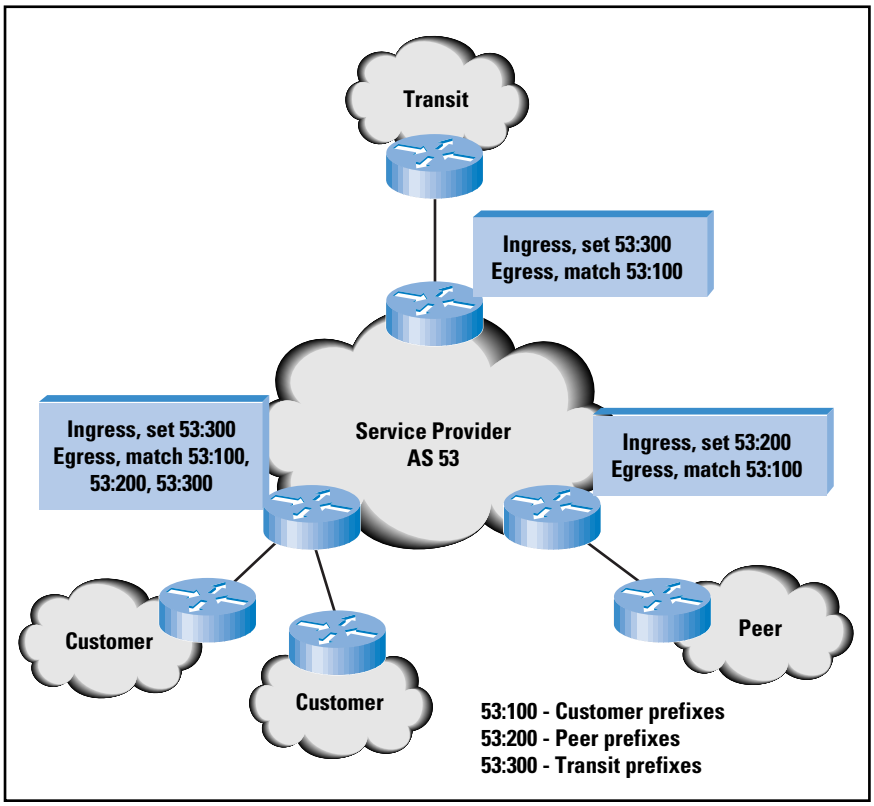


Figure 2: Internal Use of Communities for Applying a Basic Service Provider Policy

We can extend this community coding and turn it into a useful troubleshooting tool by adding more information such as where the route was learned geographically. Codes could be assigned per continent, country, state/province, city, or central office.

During redistribution from an Interior Gateway Protocol, a community can be used to specify the original protocol (for example, *Intermediate System-to-Intermediate System* [IS-IS], *Open Shortest Path First*

[OPSF], or *Routing Information Protocol* [RIP]). These can be used to quickly determine where a prefix came from without tracing it back to the point of its origination.

It is possible to assign these additional properties in two different ways (or a combination). A single community value may represent a single meaning, such as **`53:100`**, meaning a customer-learned prefix. We could then add additional communities such as **`53:1`** to mean a prefix learned on the east coast, **`53:2`** to mean central, and **`53:3`** to mean west coast. Alternatively, a single community could represent both a customer and a prefix learned on the west coast by tagging with the single tag **`53:103`**. To support these complex values, most vendors allow for pattern matching of specific values, ranges of values, and logical operators such as OR and NOT, in the form of regular expressions. Using regular expressions and complex communities can help to make a router configuration more economical and easier to read.

Inter-Autonomous System Communities

We have some options for Inter-AS traffic engineering: we can prepend additional AS numbers onto a prefix path, use *Multi-Exit Discriminators* (if the provider supports this), announce more specific prefixes or not announce prefixes at all, modify the origin type, or use communities designed by the other service provider. Communities are clean and consistent with regard to the method of signaling to an adjacent AS how each prefix should be treated.

Of most concern to downstream customers is controlling their primary and backup circuits. Small service providers and enterprises may negotiate different rates on different circuits. Customers purchasing transit with a commitment to send a high amount of traffic with a lower cost per megabit on one circuit, and on a second circuit purchase transit with a very low commitment but at a higher cost per megabit can save some money, assuming they use only the second circuit during outages on the first. Two simple communities can be used to effectively influence a service provider into using the appropriate primary and backup circuits: one value to lower and another to raise the preference of specific prefixes during the transit provider's best-path selection.

An example of adjusting Local Preference with communities can be found in RFC 1998, "An Application of the BGP Community Attribute in Multi-home Routing"[5].

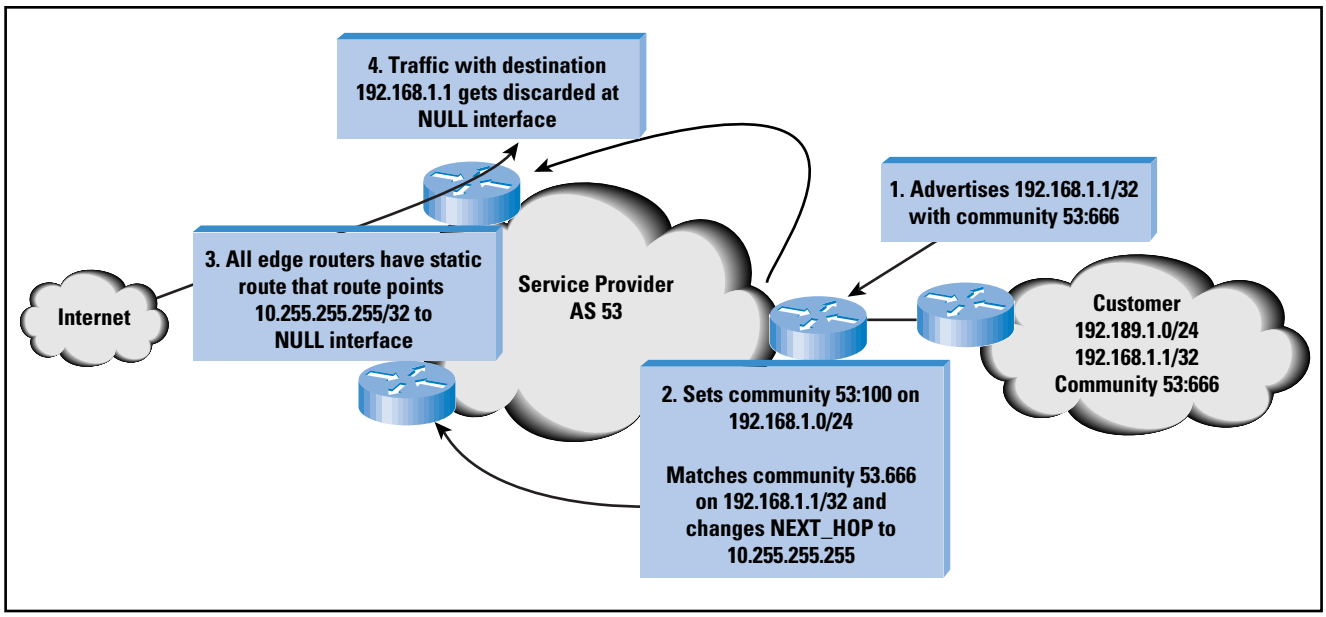
Some other traffic engineering signaling possibilities include:

- Force the adjacent AS to prepend its ASN a certain number of times to a prefix sent to customers or peers.
- Force the other side to selectively advertise a prefix to specific neighbors.
- Request that the neighbor drop all traffic to a prefix.

The last example may seem a little strange; if you are paying someone to deliver traffic, you expect to receive that traffic. Here is where communities can play a role in network security. *Denial-of-Service* (DoS) attacks may take out an entire customer's service, but the attack may be

focused on one or several hosts and not an entire network, as illustrated in Figure 3, allowing customers to tag individual host routes (a subnet consisting of a single address), the customer can signal to the provider to drop all traffic (black hole) for that specific address. To achieve this, the provider selects a single IP address and routes all traffic destined for it to the NULL interfaces on every BGP-speaking router. When a customer signals for a prefix to be blackholed, the service provider replaces the NEXT_HOP information in the BGP advertisement (which under normal circumstances is the edge router IP address) with the specific address that all other routers have statically routed to the NULL interface. When a packet arrives destined for the host under attack, the edge router performs a routing table lookup to find the BGP prefix; using the NEXT_HOP, it then performs a recursive lookup and ultimately sends the packet out the NULL interface. It is important to use other techniques such as prefix lists to prevent a third party from exploiting this technique to disrupt service for others in the Internet.

Figure 3: Customer-Initiated Black Hole to Defend Against a DoS Attack



A service provider may elect to send communities to its customers, leaving it up to the customers to decide for themselves which communities to act on. For a customer who is dual-homed to the same service provider in multiple states or countries, it may be helpful to know where a prefix was originated. A customer could use this community to prefer a connection in New York instead of a Los Angeles connection for European traffic. A single composite metric composed of all relevant geographical information is best, because this gives customers maximum flexibility in choosing the values that are meaningful to them.

Tagging the type of prefix may help other networks to selectively filter more specific addresses. Adding a community specifying if a block is a more specific part of a *Classless Inter-Domain Routing* (CIDR) block being advertised, the CIDR block itself, or if it is a more specific block but the CIDR block is not being advertised, can help the downstream network avoid incorrect filtering.

Example: Network A announces

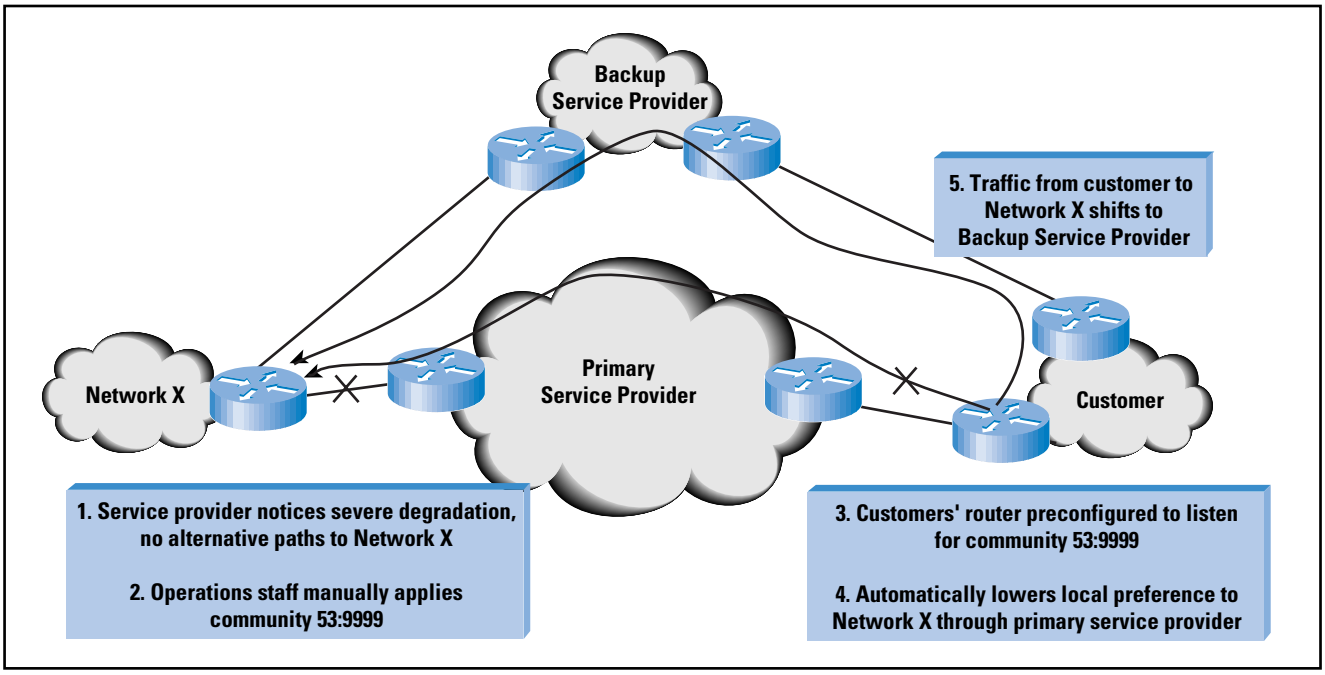
142.77.0.0/16 with a tag of **1:77**
142.77.1.0/24 with a tag of **1:88**
150.3.12.0/24 with a tag of **1:99**

1:77 means it is a CIDR block
1:88 means it is a more specific block within a CIDR block
1:99 means that the full CIDR block is not being announced

Network B then has the option of accepting the more specific **142.77.1.0/24**. It also knows that it must accept **150.3.12.0/24** because there is no other route to this network.

In extreme cases providers may find that a portion of their network has become severely degraded. Planned with customers in advance, the upstream provider manually sets a specific community on prefixes associated with the degradation to indicate that this path should be avoided. This could be helpful during natural disasters, fiber cuts, or other unanticipated network outages/degradation. The downstream customers' inbound filters would then match this community and lower the preference on the prefixes tagged with it, causing them to automatically shift traffic to an alternative source if it is available. The degradation signalling process can be seen in Figure 4.

Figure 4: Provided Initiated Signalling of Severe Route Degradation



Design Recommendations

The following are some suggestions if you are just starting out with using communities in your own network. Even the smallest network can benefit from starting early with a clean community design.

- Choose a set of internal communities that best reflects the topology and characteristics of your network. For external communities some service providers offer none, others offer only enough to allow for the tagging of primary and backup circuits, and others provide a seemingly endless list.
- Keep the set simple. Adding additional complexity typically requires changes to all the BGP-speaking edge routers. Router configurations can quickly grow to enormous proportions to accommodate the numerous community combinations. Troubleshooting a routing mess with a complex community structure can be difficult for those on the graveyard shift.
- Avoid transiting communities received from neighboring ASs blindly through your network. This could be abused intentionally or unintentionally to influence traffic to use your costly transit over settlement-free peering and revenue-generating customer circuits. Problems can be created farther out in the Internet and can be very difficult to locate. Depending on the support of your router software, you may be able to selectively add and remove communities, or failing that, you may need to remove all communities and re-add what is acceptable.
- Document your communities internally and externally. Your customers will appreciate the additional control, and your operations team will have an easier time troubleshooting.

Summary

Communities add power to BGP, changing it from a routing protocol to a tool for signaling and policy enforcement. If deployed correctly and consistently, communities can help make a network scale, easier to operate, easier to troubleshoot, and can give its customers what they want.

References

[1] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, March 1995.

[2] R. Chandra, P. Traina, and T. Li, "BGP Communities Attribute," RFC 1997, August 1996.

[3] G. Huston, "NOPEER Community for BGP Route Scope Control," Internet Draft, May 2003.

[4] S. Sangli, D. Tappan, and Y. Rekhter, "BGP Extended Communities Attribute," Internet Draft, May 2002.

[5] E. Chen and T. Bates, "An Application of the BGP Community Attribute in Multi-home Routing," RFC 1998, August 1996.

KRIS FOSTER, CCIE® #7749, currently lives in Calgary, Alberta, and spends his time in TELUS' IP backbone. His industry affiliations include the Association for Computing Machinery (ACM), the Internet Society (ISOC), and the North American Network Operators Group (NANOG). He can be reached at **kris.foster@telus.com**

WAP: Broken Promises or Wrong Expectations?

by Edgar Danielyan, Danielyan Consulting LLP

The *Wireless Application Protocol* (WAP) was once hailed as the ultimate mobile Internet solution that would revolutionize how we use the Internet and mobile phones. As you may already know, it didn't. What is to blame? Is it bad technology, wrong time, or greedy network operators? Actually, is there a reason to blame anyone? This article introduces WAP with its related technologies and tries to answer these questions. Although WAP is available on a variety of wireless mobile networks, such as those employing *Code Division Multiple Access* (CDMA) IS-95, *Time Division Multiple Access* (TDMA) IS-136, *International Mobile Telecommunications* (IMT-2000), *Universal Mobile Telecommunication System* (UMTS), and *Wideband Code Division Multiple Access* (W-CDMA), in addition to GSM/GPRS this article covers WAP over GSM/GPRS networks only.

A Case for WAP

Before looking at WAP itself, let's first recall what sparked its idea and development. As we all know, most if not all *second-generation* (2G) mobile phones and networks suffer from numerous limitations that make it impossible or impractical to use standard Internet protocols and technologies on today's mobile phones. The most visible of these limitations include the following:

- Low bandwidth (usually 9.6 kbps)
- High network latency
- Small, mostly monochrome displays
- Numeric keypads
- Slow processors
- Limited memory

All these limitations meant that it was necessary to develop an alternative suite of protocols and technologies that would work on these mobiles phones but still provide functionality comparable to the standard Internet technologies used on wired networks and desktops. WAP was developed to address these issues[1].

WAP Forum and Open Mobile Alliance

The *WAP Forum* is the industry organization behind WAP and its associated protocols and technologies. In 2002, the WAP Forum and the Open Mobile Architecture Initiative merged, creating the *Open Mobile Alliance* (OMA), which will continue work on WAP 2 and develop new mobile and wireless solutions. Nearly 200 of the world's top network operators, vendors, and content providers are members of the Open Mobile Alliance[2]. Other organizations such as the *Location Interoperability Forum* (LIF)[3], *Multimedia Messaging (MMS) Interoperability Group* (MMS-IOP)[4], *SyncML Initiative*[5], and *Wireless Village Initiative*[6] have announced their support for the new organization.

Global System for Mobile Communications

GSM, or *Global System for Mobile Communications,* is used by more than 700 million people across 190 countries[7]. In less than ten years after its introduction, GSM became the most popular and widely used digital mobile wireless communications standard in the world. GSM networks use TDMA technology and are fully digital, employing a unique voice codec known as *GSM codec* to provide relatively good voice quality using narrow bandwidth (usually 9.6 kbps). However, GSM is not as secure as many may think. Although it does use encryption and smartcard technology, this didn't result in strong security. As a result, it is possible to intercept and decrypt GSM communications, fake short text messages (*Short Message Service* [SMS]), and clone *Subscriber Identification Modules* (SIMs), miniature smartcards used to identify subscribers to the GSM network. GSM security is not the subject of this article, but it deserves attention and I hope to cover it in a separate article in this journal.

Wireless Application Environment

Before proceeding further, we should clarify one point. The term "WAP" is usually used to refer to the entire suite of protocols and technologies that are actually called the *Wireless Application Environment* (WAE)[8]. However, "WAP" is used everywhere to refer to WAE (which includes WAP). Because WAP is the commonly used term, we shall continue to use it as well.

Wireless Application Protocol

WAP protocols were expected to satisfy the following criteria in order to implement the objectives set by the WAP Forum:

- Independent of wireless network standard (bearer technology)
- Open to all
- Will be proposed to the appropriate standards bodies
- Applications scale across transport options
- Applications scale across device types
- Extensible to new networks and transports

The objectives of the WAP as defined by the WAP Forum follow:

- To bring Internet content and advanced data services to digital cellular phones and other wireless terminals
- To create a global wireless protocol specification that will work across differing wireless network technologies
- To enable the creation of content and applications that scale across a very wide range of bearer networks and device types
- To embrace and extend existing standards and technology wherever appropriate

Two major versions of WAP exist—Versions 1 and 2. WAP Version 2 is backward compatible with WAP Version 1 and tends to be more integrated with the newest Internet and Web standards than WAP 1. Although WAP uses many technologies and concepts from the Internet and Web worlds, because of their inherent limitations, WAP devices are unable to directly access Web resources on the Internet[9]. To do so, they must use a WAP gateway. The following table shows the relationship between the WAP client device, WAP gateway, and Web servers on the Internet, with their protocol layers side by side:

Web Client	WAP Gateway	Web Server
WSP	WSP/HTTP	HTTP
WTP	WTP/HTTP	HTTP
WTLS	WTLS/SSL/TLS	SSL/TLS
WDP	WDP/TCP/UDP	TCP/UDP
Bearer	Bearer/IP	IP

The table shows that the main function of the WAP gateway is to translate between WAP and Web/Internet protocols, conventions, and encodings. In some cases the WAP gateway and the Web server may be the same system, eliminating the need for a separate WAP gateway and possibly improving performance—however, for this setup to work the combined WAP/Web server has to be integrated into the mobile/wireless network provider's infrastructure. In practice, network operators provide the WAP gateway services and content providers offer WAP content on separate Web servers configured for WAP access (any standards-compliant Web server can do this).

Wireless Session Protocol

The *Wireless Session Protocol* (WSP) is the WAP session-layer protocol for remote operations between a wireless (WAP) client and proxies, gateways, and servers[10]. It functions above the *Wireless Transaction Protocol* (WTP) and the *Wireless Datagram Protocol* (WDP), and optionally, the *Wireless Transport Layer Security* (WTLS). The WSP provides a way for an organized exchange of data between client/server applications in a wireless environment. It provides such features as establishment and release of sessions between client and server; agreement on common functionality by way of negotiation; and exchange of data between client and server using compact encoding. WSP defines two subprotocols—a connection-oriented session service protocol over WTP and a connectionless service protocol over the WDP.

Wireless Transaction Protocol

WTP runs on top of the WDP and optionally, the WTLS protocol, and provides the request/response protocol used by WAP browsers to request and receive content[11]. WTP is a reliable transaction-oriented protocol specially designed for wireless networks—in WTP there are no connection setup or release phases.

Reliability in WTP is achieved using transaction IDs, retransmissions, acknowledgments, and removal of duplicates.

Wireless Datagram Protocol

WDP is the transport protocol of WAP[12]. It operates directly above the bearer technology (such as GSM CSD or GPRS) and directly below WTP described previously. WDP provides a consistent, bearer-independent interface for the upper-level protocols to the transport service provided by WDP. In addition to the GSM *Circuit Switched Data* (CSD) and the *General Packet Radio Service* (GPRS), WDP supports the following wireless bearer technologies:

GSM SMS	IDEN Packet Data
GSM USSD	FLEX
GSM Cell Broadcast	REFLEX
ANSI-I36	PHS CSD
CDPD	DataTAC
CDMA CSD	TETRA Short Data Service
CDMA Packet Data	TETRA Packed Data
CDMA SMS	DECT SMS
PDC Circut Switched Data	DECT Connection-oriented Service
PDC CSD	DECT Packed Switched Service
PDC Pacet Data	Mobitex
IDEN CSD	

When used over GSM CSD, WDP actually uses the *User Datagram Protocol* (UDP) in the following way:

Layer 4: UDP
Layer 3: Internet Protocol (IP)
Layer 2: Point-to-Point Protocol (PPP)
Layer 1: GSM CSD

When used over the GPRS, PPP at Layer 2 is not necessary, because GPRS works at Layers 1 and 2:

Layer 4: UDP
Layer 3: IP
Layers 1 and 2: GSM and GPRS

In all cases when IP is supported over a given bearer, UDP is used by WDP—actually, UDP is the WDP in these cases.

Wireless Control Message Protocol

Not surprisingly, *Wireless Control Message Protocol* (WCMP) resembles and corresponds to the *Internet Control Message Protocol* (ICMP) of TCP/IP networks[13]. WCMP is used by WDP nodes to report errors and provide network information and diagnostics. However, WCMP is not necessary and is not used with bearers that support IP—the function of WCMP in these circumstances is carried out by ICMP. In particular, this is the case with GSM CSD and GPRS bearers.

Wireless Transport Layer Security

WTLS is the transport layer security protocol of the WAE that provides privacy, integrity, and authentication services[14]. It is heavily influenced by the *Transport Level Security* (TLS) protocol Version 1 and includes additional support for optimized handshake, connectionless transport, and dynamic key refresh. WTLS, like other WAP protocols, is optimized for low-bandwidth, high-latency wireless networks and supports server and client certificates for mutual authentication. WTLS includes the following three subprotocols:

- Cipher protocol
- Alert protocol
- Handshake protocol

The following cryptographic algorithms are used by the Wireless TLS protocol:

- RSA
- SHA-1
- Diffie-Hellman (DH)
- Elliptic Curve Diffie-Hellman (EC-DH)
- DSA
- Elliptic Curve DSA (EC-DSA)
- MD5
- RC5
- DES
- IDEA

WTLS is tightly linked to and works in conjunction with the *Wireless Public Key Infrastructure* (WPKI).

Wireless Public Key Infrastructure

WPKI tries to reuse the existing *Public Key Infrastructure* (PKI) standards as much as practical to provide an adequate PKI framework for the WAE. Both X.509 and WTLS certificates can be used by WTLS[15].

Wireless Markup Language Version 1

The *Wireless Markup Language* (WML) Version 1[16] is used in WAP/WAE 1 and supported in WAE 2. Unlike usual HTML, it is a strict application of the *Extensible Markup Language* (XML), specially designed for use on narrowband devices. Also unlike HTML, WML has a metaphor of *decks* and *cards*. A deck contains one or more cards, and cards in turn contain one or more screens of user interaction. This metaphor helps increase efficiency on low-speed, high-latency wireless networks by bundling several screens into a single WML file (deck). WML supports all basic text display options, such as *italic*, **boldface**, and underlined text, as well as inter-card and inter-deck navigation using hyperlinks. The most apparent difference between HTML and WML noted by HTML developers is the fact that WML is a strict markup language and does not tolerate even seemingly little errors—an incorrectly written WML file will not display at all. Some would say this is an overkill but it is not—this feature of WML is important because compiled versions of WML files are sent to WAP clients by the WAP gateway instead of the source WML text files. This compiled bytecode is known as *WMLC*, and it considerably lessens the time it takes to download a WML document.

WML Version 2

WML version 2 is based on XHTML Basic with additional modules for support of features specific to wireless devices—this extended XHTML is called *XHTML Mobile Profile* (XHTML-MP)[17]. WML Version 2 is backward compatible with WML Version 1, so devices able to display WML 2 will also display WML 1 content. Use of XHTML shows that WAP in Version 2 is moving toward even closer integration with Internet and Web standards.

WMLScript

WMLScript is a lightweight scripting language based on ECMAScript, which is in turn based on JavaScript[18]. It is well integrated with WML and has a defined set of standard libraries, including support for cryptographic functions. Like WML, WMLScript files are also compiled into bytecode and only then sent to the requesting WAP device. Another difference between JavaScript and WMLScript is that WMLScript content is not embedded in WML pages but instead is requested separately—the necessary WMLScript functions are only referenced in WML pages. The main use of WMLScript is the client-side validation of user input—accepting only valid input is more crucial for WAP than for Web applications because of the low-speed and usually expensive nature of WAP transport.

Wireless bitmaps

The *Wireless Bitmaps* (WBMP) file format (`.wbmp`) is used by WAP devices to transmit and display small and simple monochrome bitmap images[19].

GSM CSD

CSD is the traditional data service provided by GSM networks. Also known as a *data call service*, it provides either a 9.6- or 14.4-kbps dialup facility and is supported by all GSM networks. Data calls are possible both from and to a GSM network. When used as a bearer for WAP, it serves at the physical layer of the *Open System Interconnection* (OSI) model, with PPP used in the usual way.

High-Speed Circuit Switched Data

The *High-Speed Circuit Switched Data* (HSCSD) service is similar in nature to CSD, but provides 28.8 or 43.2 kbps of bandwidth. It is not as widespread as the regular CSD, nor it is as asked-for as GPRS.

General Packet Radio Service

GPRS is an always-on, higher-speed alternative to the CSD service of GSM networks. It solves two of the most annoying issues of GSM data users—connection delay (the time it takes to set up a data call before data may be sent or received) and the bandwidth limitation, increasing the supported data rates to 48 kbps, with theoretical maximum of 171.2 kbps. Because GPRS is a connectionless packet service, GPRS terminals are always connected and may send and receive IP packets at any time. This makes possible applications such as instant messaging previously impossible or impractical with GSM CSD. Eight time slots are available for GPRS in GSM networks, but only five may be used simultaneously. The GPRS class supported by the GPRS terminal dictates what data rates are possible:

Class 2:	Uplink 8–12 kbps, downlink 16–24 kbps
Class 4:	Uplink 8–12 kbps, downlink 24–36 kbps
Class 6:	Uplink 16–24 kbps, downlink 24–36 kbps, or Uplink 24–36 kbps, downlink 16–24 kbps
Class 8:	Uplink 8–12 kbps, downlink 32–40 kbps
Class 10:	Uplink 8–12 kbps, downlink 32–48 kbps, or Uplink 16–24 kbps, downlink 24–36 kbps
Class 12:	Uplink 8–12 kbps, downlink 32-48 kbps, or Uplink 16–24 kbps, downlink 24–36 kbps, or Uplink 24–36 kbps, downlink 16–24 kbps, or Uplink 32–48 kbps, downlink 8–12 kbps

In addition to the classes of GPRS service, there are three classes of GPRS terminals:

- Class A terminals can be connected to GSM and GPRS services simultaneously.
- Class B terminals can be connected to both GSM and GPRS services, but can use only one service at a time.
- Class C terminals can be connected to either GSM or GPRS services but the user has to switch between two modes of operation.

When used as a bearer for WAP, GPRS works at the physical and data link layers of the OSI reference model. Because GPRS is connectionless and always on, there is no need for PPP—so IP works directly over GPRS.

So Why Aren't We Happy with WAP?

Many surveys of customer opinion show that the end users of WAP are not as happy as WAP developers and content providers wanted them to be. WAP service and content providers discovered that sign-up and usage rates of WAP services have not reached two-thirds of the total customer base once predicted. In short, WAP didn't change the world, and people still use their mobile phones mainly to talk to each other and send a text message or two. If you have used WAP, you probably know the reasons: the data transfer rate is slow, screens are small, charges are high, and it is tiring to type even a short URL or an e-mail message using the ten keys of a phone.

But wait a moment—are these limitations of WAP or the handsets and networks they use? Remember, WAP was required to work on devices with many limitations? So it does. Is WAP to blame that these devices have these limitations? No, that wouldn't be just. But of course it is not only the today's technology restrictions that stood in the way of the widespread usage and popularity of WAP. Scarcity of WAP content and services also contributed to this. Relatively high charges for WAP/data usage by network operators didn't help either, so the combination of these issues resulted in the situation we have today—most networks support WAP but most users don't use it anyway.

Is the technology dead, as some think? Definitely not—there are millions of WAP handsets and most wireless users will not have 3G for the foreseeable future because of both technical and economic issues, so the only available solution for these users is WAP. On the other side, 3G networks and handsets are coming and will be upon us sooner or later (they are already available in some countries), and only time will show whether tomorrow's WAP will be more popular or less relevant when 3G finally arrives. And, of course, fundamental limits of mobile phones—screen sizes, power consumption, and input methods—will still remain relevant. Other issues, such as the time it takes to set up a CSD connection, are solved by newer technologies such as GPRS, and are not really faults of WAP. You may say that if GRPS is available why would you need WAP? Why not run trusted IP? Well, this is true if you are using GPRS with a laptop or a palmtop computer, but a large majority of mobile phones don't have the resources necessary to run IP, UDP, TCP, HTTP/HTTPS, POP, and SMTP—so even if GPRS is available but your equipment cannot run the full TCP/IP suite, your only choice is still WAP.

Although WAP is clearly not as popular as its proponents and developers hoped, it is still used and developed, and handsets that support only WAP are still sold. But the hype and excitement built up by the media and the industry didn't match the reality, and it is these unrealistic expectations that have broken the promise of WAP.

Additional Acronyms

DataTAC:	*Motorola wireless data system*
DECT:	*Digital Enhanced Cordless Technology*
DES:	*Data Encryption Standard*
DSA:	*Digital Signature Algorithm*
FLEX:	*Motorola one-way paging system*
IDEA:	*International Data Encryption Algorithm*
IDEN:	*Integrated Dispatch Enhanced Network*
MD5:	*Message Digest 5*
PDC:	*Pacific Digital Cellular System*
RC5:	*Rivest Cipher 5*
REFLEX:	*Motorola two-way paging system*
SHA-1:	*Secure Hash Algorithm 1*
TETRA:	*TErrestrial Trunked RAdio* Nokia open digital professional mobile radio standard
USSD:	*Unstructured Supplementary Service Data*

For Further Reading

[1] WAP Forum: **`http://www.wapforum.org`**

[2] Open Mobile Alliance: **`http://www.openmobilealliance.org`**

[3] Location Interoperability Forum:
`http://www.openmobilealliance.org/lif`

[4] MMS Interoperability Group (MMS-IOP):
`http://www.openmobilealliance.org`

[5] SyncML: **`http://www.openmobilealliance.org/syncml`**

[6] Wireless Village: **`http://wireless-village.org`**

[7] Global System for Mobile Communications (GSM):
`http://www.etsi.org, http://www.gsmworld.com`

[8] Wireless Application Environment (WAE) Version 2.0:
`http://www.wapforum.org`

[9] Wireless Application Protocol Architecture Specification:
`http://www.wapforum.org`

[10] Wireless Session Protocol Specification: **`http://www.wapforum.org`**

[11] Wireless Transaction Protocol Specification:
`http://www.wapforum.org`

[12] Wireless Datagram Protocol Specification: **http://www.wapforum.org**

[13] Wireless Control Message Protocol Specification: **http://www.wapforum.org**

[14] Wireless Transport Layer Security Specification: **http://www.wapforum.org**

[15] Wireless Public Key Infrastructure Architecture Specification: **http://www.wapforum.org**

[16] Wireless Markup Language Version 1 Specification: **http://www.wapforum.org**

[17] Wireless Markup Language Version 2 Specification: **http://www.wapforum.org**

[18] WMLScript Specification: **http://www.wapforum.org**

[19] Wireless Bitmap Specification: **http://www.wapforum.org**

EDGAR DANIELYAN, CISSP, CCNP Security, CCDP®, SCNA, TICSA, CIWCI Security is the principal partner at Danielyan Consulting LLP (**www.danielyan.com**), an information security consultancy in London and Yerevan. He is a published author and editor specialising in UNIX, networking, and information security, having been a cofounder of a national ISP and manager of a country TLD. His book, *Solaris 8 Security*, was published by New Riders Publishing in English and by Pearson Education in Japanese. He is a member of IEEE, IEEE Standards Association, IEEE Computer Society, ACM, ISACA, USENIX, and the SAGE. E-mail: **edd@danielyan.com**

The IETF IPv6 Operations Group and the Development of a Framework for Deployment of IPv6 into IPv4 Networks

by Bob Fink,
Margaret Wasserman, Wind River,
Jun-ichiro Itojun Hagino, IIJ

During 2002, the *Internet Engineering Task Force* (IETF) determined that it was best to focus the introduction of IPv6 into the IPv4 Internet by developing deployment scenarios before further development of transition mechanisms without any clearly identified framework for their place in an IPv6 deployment.

Previously the IPv6 Transition working group of the IETF, called *ngtrans* (for IP next-generation transition), was chartered to develop mechanisms and tools to support an IPv6 transition. This work initially focused, in 1995–1996, on the development of the original IPv6 standards, and it led to the basic Transition Mechanism RFC 1933[1] and later RFC 2893[2] that defined dual IPv4 and IPv6 protocol stack operation as well as IPv6-over-IPv4 tunnels.

Subsequent attempts to define a framework for transition in 1998–1999 were not successful because there did not appear to be a single vision for a transition to IPv6. Indeed the focus became one of how to have IPv4 and IPv6 coexist for a long period of time, because most felt that a full transition could take well over 10–15 years, with many believing that it would never completely obsolete IPv4. This led to the development of many transition mechanisms and tools, some of which might possibly be more useful than others, that never fit into a coherent framework for operation of a *dual protocol,* that is, IPv4 and IPv6, network.

v6ops

Thus in 2002 the ngtrans working group was disbanded, and the IPv6 Operations working group, *v6ops,* created. The v6ops working group was chartered to:

- Solicit input from network operators and users to identify operational or security issues with the IPv4/IPv6 Internet, and determine solutions or workarounds to those issues. This includes identifying standards work that is needed in other IETF working groups or areas and working with those groups or areas to begin appropriate work. These issues will be documented in Informational or *Best Current Practice* (BCP) RFCs, or in Internet-Drafts. For example, important pieces of the Internet infrastructure such as the *Domain Name System* (DNS), the *Simple Mail Transfer Protocol* (SMTP), and the *Session Initiation Protocol* (SIP) have specific operational issues when they operate in a shared IPv4/IPv6 network. The v6ops working group will cooperate with the relevant areas and working groups to document those issues, and find protocol or operational solutions to those problems.

- Provide feedback to the IPv6 working group regarding portions of the IPv6 specifications that cause, or are likely to cause, operational or security concerns, and work with the IPv6 working group to resolve those concerns. This feedback will be published in Internet-Drafts or RFCs.
- Publish Informational RFCs that help application developers (within and outside the IETF) understand how to develop IP version-independent applications. Work with the Applications area, and other areas, to ensure that these documents answer the real-world concerns of application developers. This includes helping to identify IPv4 dependencies in existing IETF application protocols and working with other areas or groups within the IETF to resolve them.
- Publish informational or BCP RFCs that identify potential security risks in the operation of shared IPv4/IPv6 networks, and document operational practices to eliminate or mitigate those risks. This work will be done in cooperation with the Security area and other relevant areas or working groups.
- Publish Informational or BCP RFCs that identify and analyze solutions for deploying IPv6 within common network environments, such as *Internet Service Provider* (ISP) networks (including core, *Hybrid Fiber-Coaxial* [HFC] or cable, DSL, and dialup networks), enterprise networks, unmanaged networks (home or small office), and cellular networks. These documents should serve as useful guides to network operators and users on how to deploy IPv6 within their existing IPv4 networks, as well as in new network installations.
- Identify open operational or security issues with the deployment scenarios documented in the previous bullet point and fully document those open issues in Internet-Drafts or informational RFCs. Try to find workarounds or solutions to basic, IP-level operational or security issues that can be solved using widely applicable transition mechanisms, such as dual-stack, tunneling, or translation. If the satisfactory resolution of an operational or security issue requires the standardization of a new, widely applicable transition mechanism that does not properly fit into any other IETF working group or area, the v6ops working group will standardize a transition mechanism to meet that need.
- Assume responsibility for advancing the basic IPv6 transition mechanism RFCs along the standards track, if their applicability to common deployment scenarios is demonstrated.

v6ops has started by creating four efforts to define transition scenarios and subsequently to analyze them for potential solutions to the deployment scenarios. These four efforts follow:

- *Third Generation Partnership Project* (3GPP) defined packet networks, that is, *General Packet Radio Service* (GPRS) that would need IP Version 6 deployment into the IPv4 Internet.

- "Unmanaged networks," which typically correspond to home networks or small office networks.
- ISP networks, including core, HFC or coaxial, DSL, dialup, public wireless, broadband Ethernet, and Internet exchange points.
- Enterprise networks, which are networks that have multiple links and a router connection to an ISP, and are actively managed by a network operations entity.

During 2003 and 2004 it is expected that these deployment scenario efforts will lead to further analysis and identification of deployment solutions and development of appropriate mechanisms to support them.

In addition to this work, serious efforts are under way to engage the entire IETF standards process in the identification and development of appropriate solutions for an IPv6 deployment. One such effort is the *IPv4 Survey* project, which has reviewed the entire IETF RFC catalog of standards to identify what work might need to be done and to disseminate this information to the appropriate area within the IETF.

As progress is made in v6ops, follow-up articles in IPJ will inform you of these efforts.

For Further Reading

[1] "Transition Mechanisms for IPv6 Hosts and Routers," R. Gilligan and E. Nordmark, RFC 1933, April 1996.

[2] "Transition Mechanisms for IPv6 Hosts and Routers," R. Gilligan and E. Nordmark, RFC 2893, August 2000.

[3] v6ops IETF information:
http://www.ietf.org/html.charters/v6ops-charter.html

[4] v6ops Web site:
http://www.6bone.net/v6ops/http://www.6bone.net/v6ops/

ROBERT FINK is a retired U.S. national laboratory network researcher working with the IPv6 Forum. He is currently a co-chair of the IETF v6ops (IPv6 Operations) working group, and leads the 6bone project. You can reach him at: **bob@thefinks.com**

MARGARET WASSERMAN is a Principal Technologist at Wind River. She is currently a co-chair of the IETF IPv6 and v6ops working groups. You can reach her at:
mrw@windriver.com

JUN-ICHIRO ITOJUN HAGINO is a network researcher with IIJ Research Laboratory. He is currently a co-chair of the IETF v6ops working group and a member of the IETF IAB. You can reach him at **itojun@iijlab.net**

Opinion: The Mythology of IP Version 6

by Geoff Huston, Telstra

Disclaimer: This is an opinion piece and, therefore, the author takes some liberties in making his points. I hope you as the reader take this in the spirit in which it is intended—a gentle poke at ourselves that sometimes we oversell ourselves and our technology.

In January 1983, the *Advanced Research Projects Agency Network* (ARPANET) experienced a "flag day," and the Network Control Protocol, NCP, was turned off, and TCP/IP was turned on. Although there are, no doubt, some who would like to see a similar flag day where the world turns off its use of IPv4 and switches over to IPv6, such a scenario is a wild-eyed fantasy. Obviously, the Internet is now way too big for coordinated flag days. The transition of IPv6 into a mainstream deployed technology for the global Internet will take some years, and for many there is still a lingering doubt that will happen at all.

Let's look more closely at how IPv6 came about, and then look at IPv6 itself in some detail to try to separate the myth from the underlying reality about the timeline for the deployment of IPv6. Maybe then we can suggest some answers to these questions.

IPv6

The effort that has led to the specification of IPv6 is by no means a recently started initiative. A workshop hosted by the then *Internet Activities Board* (IAB) in January 1991 identified the two major scaling issues for the Internet: a sharply increasing rate of consumption of address space and a similar, unconstrained growth of the interdomain routing table. The conclusion reached at the time was that "if we assume that the Internet architecture will continue in use indefinitely, then we need additional [address] flexibility."

These issues were considered later that year by the *Internet Engineering Task Force* (IETF) with the establishment of the ROAD (*ROuting and ADdressing*) effort. This effort was intended to examine the issues associated with the scaling of IP routing and addressing, looking at the rate of consumption of addresses and the rate of growth of the interdomain routing table. The ultimate objective was to propose some measures to mitigate the worst of the effects of these growth trends. Given the exponential consumption rates then at play, the prospect of exhaustion of the IPv4 Class B space within two or three years was a very real one at the time. The major outcome of the IETF ROAD effort was the recommendation to deprecate the implicit network/host boundaries that were associated with the Class A, B, and C address blocks. In their place the IETF proposed the adoption of an address and routing architecture where the network/host boundary was explicitly configured for each network, and proposed that this boundary could be altered such that two or more network address blocks may be aggregated into a common, single block.

Side Note:

Some would argue that although CIDR was important, it was not the only reason why IPv4 has been able to defy the earlier predictions of its imminent demise. Dynamic *Network Address Translation,* or NAT, allows a network to use a local private address pool to uniquely number its devices, and then translate these private addresses into public addresses to support transactions involving local and external end points. This way, a small pool of public addresses, or even a single address, is used to service a very much larger local private network. It is difficult to estimate the number of devices that are positioned behind NATs, but a highly conservative estimate would see the Internet being at least three times as large as the directly visible part of the Internet.

Side Note:

At an IETF plenary session from that time, the OSI protocol suite was termed the "Road-kill of the Information Superhighway." It was not completely clear that the presenter made the comment in jest!

This approach was termed *Classless Interdomain Routing*, or CIDR. This was a short-term measure that was intended to buy some time, and it was acknowledged that it did not address the major issue of defining a longer-term, scalable network architecture. But as a short-term measure it has been amazingly successful, given that almost ten years and one Internet boom later, the CIDR address and routing architecture for IPv4 is still holding out.

The IAB, by then renamed the Internet *Architecture* Board, considered the ROAD progress in June 1992, still with its eye on the longer-term strategy for Internet growth. The board's proposal was that the starting point for the development of the next version of IP would be *Connectionless Network Layer Protocol* (CLNP). This protocol was an element of the *Open System Interconnection* (OSI) protocol suite, with CLNP being defined by the ISO 8473 standard. It used a variable-length address architecture, where network level addresses could be up to 160 bits long. RFC 1347 contained an initial description of how CLNP could be used for this purpose within the IPv4 TCP/IP architecture and with the existing Internet applications. For the IAB this was a bold step, and considering that the IETF community at the time regarded the OSI protocol suite as a very inferior competitor to its own efforts with IP, it could even be termed a highly courageous step. Predictably, one month later in July 1992, at the IETF meeting this IAB proposal was not well received.

The IETF outcome was not just a restatement of architectural direction for IP, but a sweeping redefinition of the respective roles and membership of the various IETF bodies, including that of the IAB.

Of course such a structural change in the composition, roles, and responsibilities of the bodies that collectively make up the IETF could be regarded as upheaval without definite progress. But perhaps this is an unkind view, because the IAB position also pushed the IETF into a strenuous burst of technical activity. The IETF immediately embarked on an effort to undertake a fundamental revision of the Internet Protocol that was intended to result in a protocol that had highly efficient scaling properties in both addressing and routing. There was no shortage of protocols offered to the IETF during 1992 and 1993, including the fancifully named TUBA, as well as PIP, SIPP and NAT.

This effort was part of a process intended to understand the necessary attributes of such a next-generation protocol.

The IETF formed an *Internet Protocol Next Generation (IPng) Directorate* in 1994, and canvassed various industry sectors to understand the broad dimensions of the requirements of such a protocol. This group selected the IPv6 Protocol from a set of proposals, largely basing its selection on the so-called "Simple Internet Protocol," or SIP proposal. The essential characteristic of the protocol was that of an evolutionary refinement of the Version 4 protocol, rather than a revolutionary departure from Version 4 to an entirely different architectural approach.

Side Note:

IPv6 has had a variety of names—the original IAB documents refer to IP Version 7, working on the assumption that the protocol numbers 5 and 6 were already in use in research networks. It was renamed IPng, for "next generation."

The final word from the *Internet Assigned Numbers Authority* (IANA) was that protocol number 6 was unused, and the final specification was named Version 6 of the Internet Protocol.

The major strength of IPv6 is the use of fixed-length, 128-bit address fields. Other packet header changes include the dropping of the fragmentation control fields from the IP header, dropping the header checksum and length, and altering the structure of packet options within the header and adding a flow label. But it is the extended address length that is the critical change with IPv6. A 128-bit address field allows an addressable range of 2 to the 128th power, and 2 to the power of 128 is an exceptionally large number. On the other hand, if we are talking about a world that is currently capable of manufacturing more than a billion silicon chips every year, and recognizing that even a one in one thousand address utilization rate would be a real achievement, then maybe it is not all that large a number after all. There is no doubt that such a protocol has the ability to encompass a network that spans billions of devices, which is a network attribute that is looking more and more necessary in the coming years.

Its not just the larger address fields per se, but also the ability for IPv6 to offer an answer to the address scarcity workarounds being used in IPv4 that is of value here. The side effect of these larger address fields is that there is then no forced need to use NAT as a means of increasing the address scaling factor. NAT has always presented operational issues to both the network and the application. NAT distorts the implicit binding of IP address and IP identity and allows only certain types of application interaction to occur across the NAT boundary. Because the "interior" to "exterior" address binding is dynamic, the only forms of applications that can traverse a NAT are those that are initiated on the "inside" of the NAT boundary. The exterior cannot initiate a transaction with an interior end point simply because it has no way of addressing this remote device. IPv6 allows all devices to be uniquely addressed from a single address pool, allowing for coherent end-to-end packet delivery by the network. This in turn allows for the deployment of end-to-end security tools for authentication and encryption and also allows for true peer-to-peer applications.

IPv6, as a protocol architecture, is not a radical departure from the architecture of IPv4. The same datagram delivery model is used, with the same minimal set of assumptions about the underlying network capabilities, and the same decoupling of the routing and forwarding capabilities. The use of an address field in the IP header to contain the semantics of both location and identity was not altered in any fundamental way. The changes made by IPv6 could be seen as conservative set of decisions, based on falling back to the IPv4 protocol model for guidance, on the principle that IPv4 is an operating proof of concept for this architectural approach.

In such a light, IPv6 can be seen as an attempt to regain the advantage of the original IP network architecture: that of a simple and uniform network service that allows maximal flexibility for the operation of the end-to-end application.

It is often the case that complex architectures scale very poorly, and from this perspective the core of IPv6 appears to be a readily scalable architecture.

The Mythology of IPv6

Good as all this is, these attributes alone have not been enough so far to propel IPv6 into broad-scale deployment, and consequently there has been considerable enthusiasm to discover additional reasons to deploy IPv6. Unfortunately, most of these reasons fall into the category of myth, and in looking at IPv6 it is probably a good idea, as well as fair sport, to expose some of these myths as well.

"IPv6 Is More Secure"

A common claim is that IPv6 is more "secure" than IPv4. It is more accurate to indicate that IPv6 is no more or less secure than IPv4. Both IPv4 and IPv6 offer the potential to undertake secure transactions across the network, and both protocols are potentially highly capable in attempting to undertake highly secure transactions. Yes, the IPv6 specification includes as mandatory support for *Authentication and Encapsulating Security Payload* extension headers, but no, there is no "mandatory to use" sticker associated with these extension headers, and, like IPv4 *IP Security* (IPSec), it is left to the application and the user to determine whether to deploy security measures at the network transport level. So, to claim that IPv6 is somehow implicitly superior to IPv4 is an overly enthusiastic claim that falls into the category of "IPv6 myth."

Now I should qualify this, because there is a distinction between the protocol and its environment of deployment. In the case of IPv4, this protocol capability is compromised in many environments in the face of various forms of deployed active middleware such as NAT. It's too early to tell with IPv6, but the line of argument is that NAT-based active middleware has been deployed as a means of address extension, and in a IPv6 world such devices are no longer necessary, and will not be deployed. So perhaps one could say that IPv6 enables a path toward widespread peer-to-peer authentication and transport security at the protocol level, but whether the deployment models faithfully follow along such a path remains an open question.

"IPv6 Is Required for Mobility"

It is also claimed that only IPv6 supports mobility. If one is talking about a world of tens of billions of mobile devices, then the larger IPv6 address fields are entirely appropriate for such large-scale deployments. IPv6 includes a developing concept of stateless autoconfiguration and *Neighbor Discovery* mechanisms.

But if the claim is more about the technology to support mobility than the number of mobile devices, then this claim also falls short. The key issue with mobility is that mobility at a network layer requires the network to separate the functions of providing a unique identity for each connected device, and identifying the location within the network for each device.

As a device "moves" within the network its identity remains constant while its location is changing. IPv4 overloaded the semantics of an address to include both identity and locality within an address, and IPv6 did not alter this architectural decision. In this respect, IPv4 and IPv6 offer the same levels of support for mobility. Both protocols require an additional header field to support a decoupled network identity, commonly referred to as the "home address," and then concentrate on the manner of the way in which the home agent maintains a trustable and accurate copy of the mobile node or current location of the network. This topic remains the subject of activity within the IETF in both IPv4 and IPv6.

"IPv6 Is Better for Wireless Networks"

Mobility is often associated with wireless, and again there has been the claim that somehow IPv6 is better suited for wireless environments than IPv4. Again this is well in the realm of myth.

Wireless environments differ from wireline environments in numerous ways. One of the more critical differences is that a wireless environment may experience bursts of significant levels of bit error corruption, which in turn will lead to periods of non-congestion-based packet loss within the network. A TCP transport session is prone to interpreting such packet loss as being the outcome of network level congestion. The TCP response is not only retransmission of the corrupted packets, but also an unnecessary reduction of the sending rate at the same time. Neither IPv4 nor IPv6 have explicit signaling mechanisms to detect corruption-based packet loss, and in this respect the protocols are similarly equipped, or ill-equipped as in this case, to optimize the carriage efficiency and performance of a wireless communications subnet.

"IPv6 Offers Better QoS"

Another consistent assertion is that IPv6 offers "bundled" support for differentiated *Quality of Service* (QoS), whereas IPv4 does not. The justification for this claim often points to the 20-bit flow label in the IPv6 header as some kind of instant solution to QoS. This claim conveniently omits to note that the flow identification field in the IPv6 header still has no practical application in large-scale network environments. Both IPv4 and IPv6 support an 8-bit traffic class field, which includes the same 6-bit field for differentiated service code points, and both protocols offer the same fields to an *Integrated Services* packet classifier. From this perspective, QoS deployment issues are neither helped nor hindered by the use of IPv4 or IPv6. Here, again, it is a case of nothing has changed.

"Only IPv6 Supports Auto-Configuration"

Another common claim is that only IPv6 offers "plug-and-play" auto-configuration. Again this is an overenthusiastic statement, given the widespread use of the *Dynamic Host Configuration Protocol* (DHCP) in IPv4 networks these days. Both protocol environments support some level of "plug-and-play" auto-configuration capability, and in this respect the situation is pretty much the same for both IPv4 and IPv6.

"IPv6 Solves Routing Scaling"

It would be good if IPv6 included some novel approach that solved, or even mitigated to some extent, the routing scaling issues. Unfortunately, this is simply not the case, and the same techniques of address aggregation using provider hierarchies apply as much to IPv6 as they do to IPv4. The complexity of routing is an expression of the product of the topology of the network, the policies used by routing entities, and the dynamic behavior of the network—not the protocol being routed. The larger address space does little to improve on capability to structure the address space in order to decrease the routing load. In this respect IPv6 does not make IP routing any easier, nor any more scalable.

"IPv6 Provides Better Support for Rapid Prefix Renumbering"

If provider-based addressing is to remain an aspect of the deployed IPv6 network, then one way to undertake provider switching for multi-homed end networks is to allow rapid renumbering of a network common prefix. Again, it has been claimed that IPv6 offers the capability to undertake rapid renumbering within a network to switch to a new common address prefix. Again IPv6 performs no differently from IPv4 in this regard. As long as "rapid" refers to a period of hours or days, then yes, IPv4 and IPv6 both support "rapid" local renumbering. For a shorter time frame for "rapid," such as a few seconds or even a few milliseconds, this is not really the case.

"IPv6 Provides Better Support for Multihomed Sites"

This leads on to the more general claim that IPv6 supports multi-homing and dynamic provider selection. Again this is an optimistic claim, and the reality is a little more tempered. Multihoming is relatively easy if you are allowed to globally announce the network address prefix without recourse to any form of provider-based address aggregation. But this is a case of achieving a local objective at a common cost of the scalability of the entire global routing system, and this is not a supportable cost. The objective here is to support some form of multihoming of local networks where any incremental routing load is strictly limited in its radius of propagation. This remains an active area of consideration for the IETF and clear answers, in IPv4 or IPv6, are not available at present. So at best this claim is premature, and more likely the claim will again fall into the category of myth rather than firm reality.

"IPv4 Has Run Out of Addresses"

Again, this is in the category of myth rather than reality. Of the total IPv4 space, some 6 percent is reserved and another 6 percent is used for multicast. Forty-one percent of the space has already been allocated, and the remaining 37 percent (or some 1.5 billion addresses) is yet to be allocated. Prior to 1994, some 36 percent of the address space had been allocated. Since that time, and this includes the entire Internet boom period, a further 15 percent of the available address space was allocated. With a continuation of current policies it would appear that IPv4 address space will be available for many years yet.

So Why IPv6 Anyway ?

The general observation is that IPv6 is not a "feature-based" revision of IPv4—there is no outstanding capability of IPv6 that does not have a fully functional counterpart in IPv4. Nor is there a pressing urgency to deploy IPv6 because we are about to run out of available IPv4 address space in the next few months or even years within what we regard as the "conventional" Internet.

It would appear that the real drivers for network evolution lurk in the device world. We are seeing the various wireless technologies, ranging from Bluetooth for personal networking through the increasingly pervasive IEEE 802.11 "hot-spot" networking to the expectations arising from various forms of *third-generation* (3G) large radius services being combined with consumer devices, control systems, identification systems, and various other forms of embedded dedicated function devices. The silicon industry achieves its greatest advantage through sheer volume of production, and it is in the combination of Internet utility with the production volumes of the silicon industry that we will see demands for networking that encompasses tens, if not hundreds, of billions of devices. This is the world where IPv6 can and will come into its own, and I suspect that it is in this device and utility mode of communications that we will see the fundamental drivers that will lead to widespread deployment of IPv6 support networks.

GEOFF HUSTON holds a B.Sc. and a M.Sc. from the Australian National University. He has been closely involved with the development of the Internet for the past decade, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. Huston is currently the Chief Scientist in the Internet area for Telstra. He is also the Executive Director of the Internet Architecture Board, and is a member of the APNIC Executive Committee. He is author of *The ISP Survival Guide,* ISBN 0-471-31499-4, *Internet Performance Survival Guide: QoS Strategies for Multiservice Networks,* ISBN 0471-378089, and coauthor of *Quality of Service: Delivering QoS on the Internet and in Corporate Networks,* ISBN 0-471-24358-2, a collaboration with Paul Ferguson. All three books are published by John Wiley & Sons. E-mail: **gih@telstra.net**

Letters to the Editor

SIP Typos

Dear Mr. Stallings, and Mr. Jacobsen,

The *Session Initiation Protocol* article by Mr. Stallings in the *Internet Protocol Journal,* Volume 6, Number 1, March 2003, provides an excellent tutorial on the subject, IMHO.

The article does an extraordinary job at presenting what is quite a complicated protocol (SIP) in simple terms. However, there seem to be some typographical errors in the article, which I wanted to bring to your attention:

- In Figure 2, message number 10 should be "180 Ringing" as opposed to "100 Ringing."
- In Figure 2, the line under message number 14 should be pointing in the opposite direction (that is *from* Bob's proxy *to* Alice's proxy).
- In Figure 2, message number 16 should read only "ACK" not "180 ACK."
- In Figure 2, message number 15 should perhaps read as "200 OK" as opposed to just "OK"
- In Figure 3, message number 5 should read "200 OK" as opposed to "200 Trying"
- Figure 4 message number 5 and 7 should perhaps read as "NOTIFY <Signed In>" as opposed to "<Not Signed-In>"
- Figure 4 "User Agent Bob" should be labelled as "(signed in)" as opposed to "(not signed in)"
- There are missing closing angular brackets in the SIP INVITE message listing on page 27:

  To: Bob **<sip:bob@biloxi.com>**
  From: Alice **<sip:alice@atlanta.com>;tag=...**
- There are missing closing angular brackets in the SIP 200 OK message listing on page 28:

  To: Bob **<sip:bob@biloxi.com>;tag=....**
  From: Alice **<sip:alice@atlanta.com>;tag=...**

Sincerely,

—Rajnish Jain, Excel Switching Corp.
rajnishjain@xl.com

The author responds:

Rajnish,

Thanks for the comments. I am embarrassed that so many errors slipped through, even though I and several reviewers for Ole checked the paper.

—Bill Stallings
ws@shore.net

DoD and IPv6

Dear Geoff,

After reading your article, I couldn't help but notice the U.S. Department of Defense's announcement concerning their intentions to adopt IPv6 in the coming years (see "Fragments," page 38). Given that you've made some strong statements about the value of IPv6 in your article, would you care to offer some views about this announcement?

—Ole

Dear Editor,

As I said in the article, the true value of IP v6 lies in the massive amount of coherent address space that allows literally billions of devices to be uniquely addressed. Address uniqueness is a strong value proposition when you want an identifier space to cover a very large deployment space. As an example of this, one of the two properties of the original Digital-Intel-Xerox Ethernet II specification that remains in today's 10 Gigabit Ethernet specification is unique MAC addresses. All of that highly innovative CSMA/CD thinking that at the time we thought was the fundamental property of Ethernet has been dispensed with.

The general observation is that any communications systems requires any party to be able to uniquely identify any other party in order to initiate a private communication session. If you cannot perform that most basic of communications functions, then you simply do not have a functional peer-to-peer communications network.

But doesn't that mean that the stories of IPv4 address exhaustion have some substance? With the large amount of addressable devices hidden behind NATs, and the associated move to using domain names as the underlying identifier space for many communications applications, the pressure on consumption of IPv4 address space has been reduced considerably. This has implied that in a world of human-driven screens and keyboards we see some considerable lifetime left in the admittedly comfortable world of IPv4 as we know it. To support this model we've actually moved away from the IP address as the unique identifier token for many applications, and substituted an application model that is driven from domain names. As an example, consider the virtual hosting mechanism as implemented in Apache Web servers to see this shift in communications identifiers from address to domain name. And both as consumers of the technology and as an industry we can live with this for some time yet, because we appear to concentrate our use IP addresses as a routing and forwarding framework and increasingly use the DNS as the identifier realm of an application.

But our world is a world where the device is subservient to the user, and the applications we associate with the Internet of today are applications that are essentially human pastimes, such as e-mail, Web browsing, or high-value automated transactions, such as those commonly bracketed into the e-commerce area. And we've now established a highly valuable global industry upon these foundations.

But in so doing we should recognize the emergence of a second set of communications realms populated by uniquely identified devices that number in their billions, where the inter-device traffic is not human mediated, and the value of the device transactions are, on an individual transactions value level, far lower than the value of the human-driven realm of IPv4. In other words, in a device rich communications realm, it's likely that the human value we'd ascribe on average to each packet is far lower than our current Internet IPv4 world of human-mediated communications. And it's this extravagantly device-equipped world that we see the U.S. Department of Defense heading. If your stock in trade is one of quite astounding feats of logistical deployment of large numbers of people and large numbers of items of equipment, then the communications requirement is of a different order of scale to that of the retail Internet markets, and, yes, I'm sure that there are entirely effective arguments behind that decision to look forward to a communications realm with a uniform base protocol identifier domain in a scale that is 2 to the power 96 times larger than the entire IP address identifier domain of IPv4.

But I would be cautious about high levels of expectation that this immediately translates into an impetus in the market where you and I converse. My host here where I'm typing this message is already IPv6 capable, and if you are running a recent version of host software, then it's a reasonable assumption that yours is too. But I'll send this message over IPv4 and you'll receive it over IPv4, and between my mail sender and your mail receiver the transport channel will also be IPv4. Should we use IPv6 instead? Would I pay my provider additional money to compensate it for part of its additional expenditure to support a simultaneous IPv6 capable network between you and me? To send precisely the same message? In precisely the same time? Along the same path? Using the same transport TCP session? Obviously, to me, as a (hopefully) economically rational consumer of such services, and no doubt to you, in a similar role, there is no value in spending more money to achieve outcomes in IPv6 that are identical to what we can already do today in IPv4. And in the retail Internet world that remains the basic IPv6 conundrum. Why should any provider spend additional resources to service the same market with identical services, and in so doing be unable to raise additional revenue to offset their additional service costs? One interpretation is that there is no natural motivation for such activities in today's market, otherwise it would already be very widespread indeed.

What we've seen in the mainstream Internet world is an emerging mythology about IPv6 that somehow this additional expenditure, ultimately on the part of the consumer, provides some additional benefit for the consumer, motivating them to switch from IPv4-only services to some hybrid of mixed v4 and v6 and ultimately to a v6 world, and thereby funding the additional provider expenditure associated with such a massive transition.

The reality is more sobering in that in the retail Internet world there is so far nothing obvious in the "additional benefit" category. I'm using *Network Address Translation* (NAT) right now, using an *ssh* session back to my mail server that drives through NAT boxes to make a secure SMTP session, across a first step of 802.11 wireless in order to send this message to you.

I've auto-configured in the wireless world, and for me I'm living in a plug-and-play world that supports my level of roaming access. Would IPv6 make this session any more secure? Any different in terms of *Quality of Service* (QoS) ? In plug-and-play models of roaming? Would there be any visible difference in terms of my ability to communicate with you? To all of these questions the basic answer is still "no."

So, for you and I, we look inside the IPv6 technology box, and find nothing new there to motivate us to spend more money for our existing Internet-based communications services, and for some time to come it would appear that this will still hold.

On the other hand there are circumstances where there is a need to operate in a much larger base protocol address space. These include situations where one wants to take advantage of Internet applications that operate across a world of literally billions of devices, large and small. The application space may want to gather constant reports on the characteristics of the "thing" it is attached to, from a ration pack to a component of a large naval vessel. You may want to use supply channels for such devices such that the deployment is a plug-and-play world without a massive variety of detailed configuration processes. You may be looking to an architecture that would be stable for many years. In such circumstances you really want take advantage of a uniform set of Internet application technologies that potentially span massive numbers of addressable devices. Here a large base address space is a definite asset. And for such industry sectors in voicing such requirements where there is also a somewhat different ultimate value proposition for the supported communications activity, then it's quite understandable that there can be an attractive proposition offered by immediate adoption of IPv6.

But back in the communications realm where you and I currently exchange our messages, such requirements remain in a future framework that is still waiting for relevant value propositions that allow it to gain traction with you and me. And as I attempted to point out in the article, adding some elements of mythology and over-stating the IPv6 value case won't help here.

Maybe we just need to be patient. Steam ships did not halt operation the first day a diesel powered vessel appeared. It was a much slower process that lead to an outcome of the change of the maritime fleet—the next generation of mechanization offered cheaper services, and, as often happens, market price won in that commodity market.

Market price often wins in competitive commodity markets. And the Internet retail market is, in many parts of the world and in many sectors, a strongly competitive space with all the characteristics of a commodity offering. In addressing such initial specialized dedicated communications requirements with IPv6 technology as represented by the U.S. DoD, there is a distinct possibility that there may be some effective use of initial investment that translates into the retail world in some form of efficiency gain for IPv6-capable providers.

And there no doubt that if you and I could communicate in precisely the same fashion as we do today, with precisely the same applications and service environment, using precisely the same host devices and operating systems as we do today, but at some attractive fraction of today's price, then I'm sure that neither of us would care in the slightest that our data was encapsulated using a packet framing format and address tokens that used the IPv6 protocol specifications.

Kind regards,

—Geoff Huston, Telstra
gih@telstra.net

Book Review

Google Hacks

Google Hacks: 100 Industrial-Strength Tips & Tools, by Tara Calishain and Rael Dornfest, ISBN 0-596-00447-8, O'Reilly & Associates, 2003, 329 pages.

Hmm, this is a hard one. This is the second go at writing a review—the first one made me sound like a grumpy luddite and I don't want my secret identity to be revealed yet. So, put on some suitable music ("So What" from "Kind of Blue" by Miles Davis) and this time, to start with, "just the facts, ma'am" and we'll get back to the grumpiness later.

What we have here are "100 Industrial-Strength Tips & Tools" for using the Google search engine (or g**gling as we are not allowed to say). All the usual O'Reilly positives about layout and presentation apply so we can take those as read (and the usual negative about murky grey scale illustrations). The tips/tools are gathered into separate sections dealing with searching (surprise!), services, scraping, using the API, games and Web mastering. All the tips have some description, some have code and others have URLs that take you to the code or the service described. And indeed some of these are quite interesting and useful, but, and the grumpiness is starting to creep in again, many of them are really not. Tip #1 for instance—"Setting Preferences." Since when has a brief description of how what you can find on the Google preferences page been "Industrial-strength"? Too many of the tips are like this—simple stuff that you can get from many places on the Web (including Google itself) with little added value. Someone starting out using Google is not going to buy a book called *Google Hacks* because its title is off-putting, and someone who is a regular user of the service is going to know (or not be interested in) most of the content. Why do we need a 300 page paper copy of this information? Much of what is in here could be boiled down into a small, cheap guide just like those O'Reilly have for programming languages, and the rest of the stuff is irrelevant anyway (for instance the TouchGraph browser is fun and interesting, but it isn't really that useful—everyone I know has played with it for 5 minutes and then never returned).

I had better hopes of the API programming material, but it was not to be. I know I am in a tiny minority here, so don't complain, but most of the program examples provided in the book use *Perl*. "Hurrah" say you, "Boo" say I—I don't like Perl, never have and never will. Just like celery. I can put up with it, but I won't pick it when I have a choice.

Note, I am not knocking the Google APIs (though they are a bit baroque, and it would be nice to be able to get more than 10 results at time, and...). Being able to call up a search engine from within a program is a good thing, even if you do have to use Web Services (I'm not that keen on them either—are you surprised?). This book certainly tells you how to do that (at least from within Perl) but again you can pick that info up from the Web for free and it doesn't run to more than twenty pages tops. Most of the programming examples may have been fun to write and think up but are about as useful as a flowchart stencil.

Oh, and "Googlewhacking"[1] is not new—people were doing that on AltaVista long (in Internet terms) before Google appeared.

All things considered, I don't see this book being worth $25. If you know how to use Google even a little bit you ought to be able to use it to find all this information without it. And what of the stablemate book *Amazon Hacks* which is due to appear soon? I fear a miracle of padding there.

—Lindsay Marshall, University of Newcastle upon Tyne
Lindsay.Marshall@newcastle.ac.uk

[1] Googlewhacking is the art of finding a two-word query that has only one result. The two words may not be enclosed in quotes, and the words must be found in Google's own dictionary (no proper names, made-up words, etc).

Would You Like to Review a Book for IPJ?

We receive numerous books on computer networking from all the major publishers. If you've got a specific book you are interested in reviewing, please contact us and we will make sure a copy is mailed to you. The book is yours to keep if you send us a review. We accept reviews of new titles, as well as some of the "networking classics." Contact us at **ipj@cisco.com** for more information.

Several Landmarks Define Push toward IPv6 Deployment in Japan

In April 1998, the KAME Project, **http://www.kame.net/**, an extension of the WIDE Project (**http://www.wide.ad.jp/**; representative Professor Jun Murai, Keio University), was established with eight core members from seven Japanese vendors. Work began under a two-year timeframe to provide free IPv6/IP Security (IPSec) reference code for UNIX BSD variants. The KAME Project remains active today.

The Japanese government's commitment to taking a leadership role in worldwide IPv6 research and deployment was outlined in a speech to open the September 2000 Diet session by then Prime Minister Mori. Mori identified IPv6 as a key discussion area for the national IT Strategy Council—a strategic pillar toward the "rebirth of the nation."

The *IPv6 Promotion Council of Japan* was established shortly thereafter, in Oct. 2000. Its founding members numbered only 18. As of March 2003 the Council's membership body consisted of 320 organizations from a variety of business fields; carriers, *Internet Service Providers* (ISPs), hardware vendors, software vendors, finance companies, general trading companies, automobile manufacturers, etc.

The Council is the most active and influential IPv6 organization in Japan, and is the formal contact point appointed by the Japanese government to handle requests from overseas private IPv6 promotion bodies, such as the various regional IPv6 Task Force bodies, for technical and deployment cooperation.

The Promotion Council is currently running the "IPv6 Appli-Contest 2003." The contest awards developers of applications and software who help to create new possibilities in the IPv6 Internet world, see: **http://www.v6pc.jp/apc/en/concept.html**

Supported by the Ministry of Public Management, Home Affairs, Posts and Telecommunications, and the WIDE Project, the contest is drawing on the cooperation of IPv6 bodies in the EU, North America, India, Korea, Taiwan, and China with the goal of creating a library of freely available IPv6 software.

Details on rules and regulations for entry can be found at the following URL: **http://www.v6pc.jp/apc/en/regulations.html**.
The deadline for entries is August 31, 2003.

Six entries will be selected as "Award of Excellence" winners and will share 1,500,000 JPY in prize money. Award of Excellence winners will also be eligible for the "Grand Prize" of 1,000,000 JPY to be presented at a ceremony during WPC EXPO 2003 to be held September 17–20, 2003, in Tokyo.

An excellent, up-to-date overview of the current status of IPv6 research and commercial service offerings in Japan, including IPv6 case studies and technology tutorials, can be found at IPv6style:
http://www.ipv6style.jp/en/index.shtm

US Department of Defense adopts IPv6

Implementation of the next-generation Internet protocol that will bring the Department of Defense closer to its goal of net-centric warfare and operations was announced on June 13, 2003 by John P. Stenbit, assistant secretary of defense for networks and information integration and DoD chief information officer.

The new Internet protocol, known as IPv6, will facilitate integration of the essential elements of DoD's Global Information Grid—its sensors, weapons, platforms, information and people. Secretary Stenbit is directing the DoD-wide transition.

The current version of the Internet's operating system, IPv4, has been in use by DoD for almost 30 years. Its fundamental limitations, along with the world-wide explosion of Internet use, inhibit net-centric operations. IPv6 is designed to overcome those limitations by expanding available IP address space, improving end-to-end security, facilitating mobile communications, enhancing quality of service and easing system management burdens.

"Enterprise-wide deployment of IPv6 will keep the warfighter secure and connected in a fast-moving battlespace," Secretary Stenbit said. "Achievement of net-centric operations and warfare depends on effectively implementing the transition."

Secretary Stenbit signed a policy memorandum on June 9 that outlines a strategy to ensure an integrated, timely and effective transition. A key element of the transition minimizes future transition costs by requiring that, starting in October 2003, all network capabilities purchased by DoD be both IPv6-capable and interoperable with the department's extensive IPv4 installed base.

For more information, see:

`http://www.dod.gov/news/Jun2003/d20030609nii.pdf`

`http://www.dod.gov/releases/2003/nr20030613-0097.html`

`http://www.dod.gov/news/Jun2003/n06132003_200306134.html`

`http://www.dod.gov/transcripts/2003/tr20030613-0274.html`

Call for Papers

The Internet Protocol Journal (IPJ) is published quarterly by Cisco Systems. The journal is not intended to promote any specific products or services, but rather is intended to serve as an informational and educational resource for engineering professionals involved in the design, development, and operation of public and private internets and intranets. The journal carries tutorial articles ("What is…?"), as well as implementation/operation articles ("How to…"). It provides readers with technology and standardization updates for all levels of the protocol stack and serves as a forum for discussion of all aspects of internetworking.

Topics include, but are not limited to:

- Access and infrastructure technologies such as: ISDN, Gigabit Ethernet, SONET, ATM, xDSL, cable fiber optics, satellite, wireless, and dial systems
- Transport and interconnection functions such as: switching, routing, tunneling, protocol transition, multicast, and performance
- Network management, administration, and security issues, including: authentication, privacy, encryption, monitoring, firewalls, trouble-shooting, and mapping
- Value-added systems and services such as: Virtual Private Networks, resource location, caching, client/server systems, distributed systems, network computing, and Quality of Service
- Application and end-user issues such as: e-mail, Web authoring, server technologies and systems, electronic commerce, and application management
- Legal, policy, and regulatory topics such as: copyright, content control, content liability, settlement charges, "modem tax," and trademark disputes in the context of internetworking

In addition to feature-length articles, IPJ will contain standardization updates, overviews of leading and bleeding-edge technologies, book reviews, announcements, opinion columns, and letters to the Editor.

Cisco will pay a stipend of US$1000 for published, feature-length articles. Author guidelines are available from Ole Jacobsen, the Editor and Publisher of IPJ, reachable via e-mail at **ole@cisco.com**

The Internet Protocol Journal

Ole J. Jacobsen, Editor and Publisher

The Internet Protocol Journal is published quarterly by the Chief Technology Office, Cisco Systems, Inc.
www.cisco.com
Tel: +1 408 526-4000
E-mail: ipj@cisco.com

The Internet Protocol Journal, Cisco Systems
170 West Tasman Drive, M/S SJ-7/3
San Jose, CA 95134-1706
USA

ADDRESS SERVICE REQUESTED

PRSRT STD
U.S. Postage
PAID
Cisco Systems, Inc.