# Understanding Block-level Address Usage in the Visible Internet

Xue Cai John Heidemann
USC/Information Sciences Institute {xuecai,johnh}@isi.edu

## ABSTRACT

Although the Internet is widely used today, we have little information about the edge of the network. Decentralized management, firewalls, and sensitivity to probing prevent easy answers and make measurement difficult. Building on frequent ICMP probing of 1% of the Internet address space, we develop clustering and analysis methods to estimate how Internet addresses are used. We show that adjacent addresses often have similar characteristics and are used for similar purposes (61% of addresses we probe are consistent blocks of 64 neighbors or more). We then apply this block-level clustering to provide data to explore several open questions in how networks are managed. First, we provide information about how effectively network address blocks appear to be used, finding that a significant number of blocks are only lightly used (most addresses in about one-fifth of /24 blocks are in use less than 10% of the time), an important issue as the IPv4 address space nears full allocation. Second, we provide new measurements about dynamically managed address space, showing nearly 40% of /24 blocks appear to be dynamically allocated, and dynamic addressing is most widely used in countries more recent to the Internet (more than 80% in China, while less than 30% in the U.S.). Third, we distinguish blocks with low-bitrate last-hops and show that such blocks are often underutilized.

## Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Network topology*; C.2.3 [**Computer-Communication Networks**]: Network Operations—*Network management*

**General Terms:** Measurement

**Keywords:** Internet address usage, survey, pattern analysis, clustering, classification, availability, volatility, median-up, low-bitrate, RTT

## 1. INTRODUCTION

Previous Internet topology studies focused on AS- and router-level topologies [5, 7, 9, 12, 23, 27, 28]. While this work explored the core of the network, it provides little insight into the edge of the Internet and the use of the IPv4 address space. The transition to classless routing (CIDR, [11]) in the mid-1990s has made the edge opaque. Only recently have researchers begun to study edge-host behavior using server logs [31], web search engines on textual addresses [29], and ICMP probing [13].

Yet the network edge has seen great change and deserves study. How is CIDR applied? How is dynamic addressing used? How widespread are low-bitrate edge links? In this paper we use active probing to study these properties of the edge of the Internet.

**Assumptions:** In this paper we begin to explore the potential of *clustering of active probes to infer network address usage*. Our work makes three assumptions:

1. Many active addresses will respond to probes,
2. Contiguous addresses are often used similarly, and
3. Patterns of probe responses and response delay suggest address usage.

While there are cases where these assumptions do not hold, we believe the assumptions apply to a large fraction of the Internet and so active probing can provide insight into address usage.

We examined the first assumption and previously showed that active probes detect the majority of addresses in use, as verified with tests against a university and a random sample of the general Internet [13].

While this prior work established the collection methodology and error bounds; this paper provides the first evidence for the next two assumptions and their application to understand network usage. The second assumption is contiguous use, which follows from the traditional administrative practice of assigning blocks of consecutive addresses to minimize routing table sizes. While there is no requirement that adjacent addresses be used for the same purpose, we will show that they are often used similarly (§[4.1]).

Finally, we assume that repeated active probing with ICMP provides information about how addresses are used. We take advantage of both the pattern of positive, negative, or missing response, and the round-trip time (RTT) of the response. While a single ICMP response provides only limited information (consent of the address to reply), repeated probing can tell much more. For example, we use response patterns to distinguish intermittent from continuously used addresses, and we show that RTT can identify low-bitrate edge links.

Figure 1 shows an example of what can be learned from probing one block of 256 addresses with prefix[1] $p$. In this figure, the 256 addresses in prefix $p$ are mapped into two dimensions following a Hilbert curve (each quadrant of the square shows one-quarter of addresses, recursively). Different shades indicate different ping response patterns from

*SIGCOMM '10,* August 30–September 3, 2010, New Delhi, India.
Copyright 2010 ACM 978-1-4503-0201-2/10/08 ...$10.00.

[1] Recall that IPv4 addresses are 32-bit numbers, usually written in the form $a.b.c.d$, where each component is an 8-bit portion of the whole address. Addresses are organized in *blocks* (sometimes called subnetworks) that are sized to powers of two. Blocks have a common *prefix*, the leading $p$ bits of the address, written $a.b.c.d/p$. For example, 128.125.7.0/24 indicates a /24 block with 256 addresses in it of the form 128.125.7.$x$. We sometimes talk about blocks as $p$.0/24, where $p$ represents the anonymized prefix.

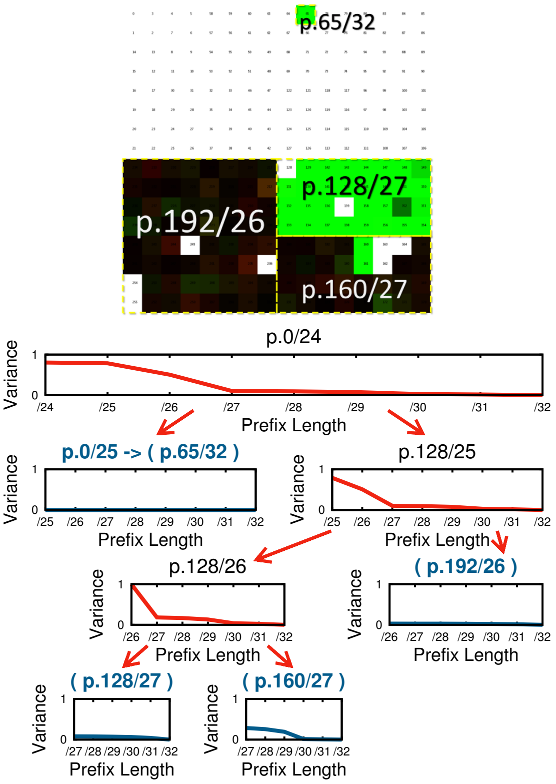

**Figure 1: Top: a /24 block (prefix is anonymized to $p$) with 4 plausible regions of different use. Bottom: our *BlockSizeId* algorithm ($\epsilon = 2.0$) identifies these regions (§[3.3]), with best-fit variance in (parentheses).**

each address (white is non-responsive; green, availability; red, volatility; metrics we define later in §[3.2]). Two green areas are blocks of addresses that are almost always up: the single address $p$.65/32 at the top center, and the 32-addresses block $p$.128/27. The two dark areas (the lower left quarter, $p$.192/26, and bottom right eight, $p$.160/27) are used only infrequently, with low availability and volatility. We can often confirm these probe-based observations against other sources (§[5] discusses hostnames and operator-provided ground truth). The bottom of the figure shows how we automatically identify these regions (§[3.3]).

**Approach and Validation:** From these assumptions we develop new algorithms to identify blocks of addresses with consistent usage (§[3]). We start with Internet survey data, where each address in around 24,000 /24 address blocks is pinged every 11 minutes for around one week [13]. From this dataset we derive several metrics about address usage. We then use these statistics to automatically identify blocks of consistent responsiveness.

Before applying these algorithms, we evaluate how often our assumptions hold. Our first question is therefore *are adjacent addresses used consistently* and *can we discover them reasonably accurately?* Before classless IP addressing [11] allocation strategies were aligned with externally visible address allocation, but since then there has been no way to easily evaluate how addresses are used. We explore these basic questions in §[ and §4.1][5.1.1].

**Applications:** A first application of this approach is to understand how addresses are managed, beginning with what block sizes are typical (§[4.1]). We find that 2,529,216 addresses, or 61% of the probed address space, show consistent responses in blocks of 64 to 256 adjacent addresses (/26 to /24 blocks). Also, we observe that most addresses (around 55%) are in /24 or bigger blocks.

Another application is understanding how effectively addresses are used (§[4.2]). We find that many blocks are only lightly used (about one-fifth of /24s show less than 10% utilization). Improving utilization is increasingly important as the IPv4 address space nears full allocation; improving IPv4 efficiency is a cost to compare compared to IPv6 transition.

Third, we detect and quantify the use of dynamic address assignment (§[4.3]). Dynamic addresses are used in some spam detection algorithms [31], and identifying dynamic addresses is important to estimate the number of computers that connect to the Internet [13]. We observe that nearly 40% of /24 blocks appear to be dynamically allocated, and dynamic addressing is much higher in countries most recent to the Internet (more than 80% in China, while less then 30% in the U.S.).

Finally, we distinguish blocks connected mainly by low-bitrate edge links from those with broadband connections, identifying blocks used by dial-up and older mobile phones (§[4.4]). Study of edge bitrate can help understand trends in technology deployment, and automatic identification of users of low-bitrate networks may allow websites to *automatically* match content and layout. Edge links and policies also interact with address utilization (§[4.4]); we show low-bitrates links are correlated with short connect-times and sparse usage.

The contribution of this paper is therefore to develop new approaches to classify Internet address usage and to apply those approaches to answer important questions in network management. As with other studies of the live Internet, our approach must employ incomplete information: our surveys cover randomly selected /24 blocks (not larger) and do not inform us about addresses that refuse to respond. However, we suggest that the approach is promising and our preliminary results provide new techniques, adding to what is currently known.

## 2. RELATED WORK

Much prior work has explored the Internet topology [5,7,9,12,23,27,28]. Recent work has begun exploring edge host behavior [13,29,31]. Our work builds upon this prior work and the specific work listed below.

*Are contiguous addresses consistent and what are the typical block sizes?* Although addresses are usually assigned as blocks and represented in prefixes by classful [24] and classless addressing [11], there is no guarantee that contiguous addresses in the same block will be used in the same way. Huston's report has analyzed the common prefix lengths in BGP routing table [14]. But it cannot look at usage at granularities smaller than BGP prefixes. Our approach is able to look at these smaller block sizes through active probing.

*Are allocated addresses efficiently utilized?* Several researchers have studied rates of IPv4 address consumption, predicting IANA will exhaust its allocation pool in 2011 [14]. However, full allocation does not necessarily imply full use. Prior researchers inferred address utilization by detecting allocated but not advertised prefixes in BGP routing table [22]. But what is routed may differ from what is actively used. Our work tries to track active use; and our study of individual addresses can reveal changes that happen to blocks inside an organization (smaller than are typically routed).

*How many addresses are dynamically assigned?* Xie et al. have begun to explore this question with a goal of identifying dynamic blocks to assist spam prevention [31]. Their work is based on passive collection of Hotmail web server logs, while our method uses a completely different approach by active probing and so can extend and corroborate their findings. In our prior work, we provide another perspective based on active probing with ICMP [13]. While this prior work focused on censuses (occasional but complete probing) and establishing the methodology, here we study survey data (frequent probing of a sample of the Internet) and add significant new analysis to identify block sizes and low-rate edges.

CAIDA has long studied Internet topology with active probing [18]. They traceroute to one address for each routed /24 address block. Our datasets differ by probing only a fraction of /24s (but all addresses in them, and much more frequently). Probing /24s allows us to take the advantage of locality to study address usage. Because contiguous addresses are usually administrated together and used in the same way, analyzing the whole block instead of sampling one address from each block can provide information not previously available. In addition, our frequent sampling shows temporal changes useful for identifying dynamic address allocation.

Regional Internet Registries (RIR) have another potential source of data, as they require organizations to state the usage of current addresses and the planned usage of new addresses [2, 3]. Such data is not generally available, but it is another possible means of future validation.

*Identifying edge-link bitrates?* A great deal of work has explored identification of edge-link bitrates (or link capacity) and available bandwidth. While we cannot review it all here, key results include packet pair [19] and pathchar [16]. We explore the use of variance as a new approach to estimate edge-link bitrates (§[3.5]).

# 3. METHODOLOGY

This section introduces our methodology: collecting raw data through an Internet survey, transforming that data into relevant observations, identifying blocks of consistent use, classifying blocks into ping-observable categories, distinguishing between low-bitrate and broadband blocks.

## 3.1 Data Collection: Surveying the Internet

We would like as much data about Internet addresses or hosts as possible, but we must balance that desire against today's security-conscious Internet culture. Our data collection builds on prior *Internet ICMP surveys* that ping each address of about 1% of the allocated Internet address space approximately every 11 minutes for one week or longer [13].

We use a previous selection methodology [13], selecting around 24,000 /24 blocks from those that were responsive in a prior census of all allocated addresses. We select blocks of addresses rather than individual addresses so we can study how addresses are allocated and used. Our choice of /24 blocks limits our ability to observe very large allocations, but allows the identification of blocks smaller than 256 addresses (§[4.1]). As with prior work, half of the selected blocks are kept consistent across multiple surveys and half are chosen randomly, enabling longitudinal studies while providing a subset that is selected with very little potential bias. We compare two surveys in §[5.3], showing that our study of 1% of the address space represents a large enough fraction of the space to be representative.

Approximately every 11 minutes, each address is probed. Probes are dispersed over this period and sent in pseudo-random order to avoid correlations due to outages. Probes taken every 11 minutes limit our ability to detect very rapid churn of dynamic addresses, however prior studies of dynamic addresses placed typical use durations at 75 or 81 minutes [13, 20], suggesting we have reasonable precision. Responses can be classified into three broad categories: positive (*echo reply*), negative (for example, *destination unreachable*), and non-response. In this paper we ignore all non-positive responses. Packet loss can cause measurement inaccuracy, so we use 1-loss repair to cope with singleton packet losses [13] (1-repair assumes an absent response between two consistent responses is loss and interpolates accordingly). Network outages can also distort our survey. We manually examine our survey and select a period that has no local network outages.

All surveys but *IT16ws* [30] cover more than one week, allowing us to detect diurnal and weekly cycles.

Of course, using ICMP for probing has significant limitations. The most serious is that large parts of the Internet are firewalled and choose not to respond to our probes. Some form of this bias is inherent in any study using active probing. Prior studies of a large university and a random sample of Internet addresses suggest ICMP probing undercounts hosts by a factor of 30–50%, and that ICMP is superior to TCP-based probing [13]. We recognize this limitation as fundamental to our methodology, but we know of no evidence or inference to suggest that the firewalled portions of the Internet use significantly different allocation strategies than the more open parts of the Internet. In addition, we confirm the accuracy of our results at USC (§[5.1]), and we show similar accuracy for manual inspections of blocks drawn at random from the Internet in §[5.2]. However, we are exploring additional ways to verify this assumption, and investigation of the firewalled Internet is future work.

Table 1 shows the datasets we use in our paper. We use two ICMP surveys taken by USC [13]: *IT17ws*[2] and *IT16ws*; *IT17ws* is the main dataset used in this paper, while we use *IT16ws*, *IT30ws*, *IT31ws* for validation in §[5.3]. Not all /24 blocks we picked respond to our pings, however, most of them did respond at least once by one IP address. We collected *LTUSCs* to compare our inferences with network operators as discussed in §[5.1]. Finally, we use a domain name survey from ISC [15] to validate our conclusions (§[5]).

## 3.2 Representation: Observations of Interest

Since one survey provides more than 5 billion observations, it is essential to map that raw data into more meaningful metrics. We call this step *data representation*. We define three metrics to characterize address usage: *availability*, the fraction of time an address is responsive; *volatility*, a normalized representation of how many consecutive periods the address is responsive; and *median-up*, the median duration of all up periods. And we characterize edge bitrate with

[2] The name *IT17ws* indicates: Internet Topology, the 17th full collection, "w" collected at ISI-west in Marina del Rey, and "s" indicates a survey rather than a full census.

| | **Start Date** | **/24 Blocks** | | |
|---|---|---|---|---|
| **Name** | (# days) | **probed** | **respond.** | **Use** |
| *IT17ws* [30] | 2007-06-01 (10) | 22,367 | 20,849 | all |
| *IT17wvs* | 2007-06-01 (10) | 100 | 100 | §5.2 |
| *IT17wbs* | 2007-06-01 (10) | 200 | 200 | §5.2 |
| *IT16ws* [30] | 2007-02-16 (6) | 22,365 | 20,900 | §5.3 |
| *IT30ws* [30] | 2009-12-23 (14) | 22,381 | 20,227 | §5.3 |
| *IT31ws* [30] | 2010-02-08 (14) | 22,376 | 19,909 | §5.3 |
| *LTUSCs* [30] | 2007-08-13 (9) | 768 | 299 | §5.1 |
| *ISC-DS* [15] | 2007-01 | hostnames | | §5 |
| *RIR* [25] | 2007-06-13 | block allocation | | §4 |

**Table 1: Datasets used in this paper.**

two metrics: *median-RTT* and *stddev-RTT*, the median and standard deviation of RTT values of all positive responses.

### 3.2.1 Metrics characterizing addresses usage

To define *availability*, *volatility* and *median-up*, let $r_i^*(a)$ be the positive (1) or non-positive (0) measurements for address $a$ (for all $i \in [1\,..\,N_p]$, where $N_p$ is the number of probes). We analyze these values after 1-loss repair [13]:

$$r_i(a) = \begin{cases} 1, & r_i^*(a) = 1 \lor (r_{i-1}^*(a) = 1 \land r_{i+1}^*(a) = 1) \\ 0, & \text{otherwise} \end{cases}$$

If each probe is made at time $t_i$, we can define the series of up durations of an address in a survey as

$$u_j(a) = t_{e_j} - t_{b_j},\ \forall j \in [1\,..\,N_u] \ \text{ where}$$
$$r_i = 1, \forall i \in [b_j\,..\,e_j] \text{and } r_{(b_j)-1} = 0, r_{(e_j)+1} = 0$$

(each up duration is a consecutive run of positive probes from $b_j$ to $e_j$, inclusive). There are $N_u$ up durations in total, where $N_u < N_p$. We can now clarify that availability, volatility, and median-up are given as:

$$\begin{aligned} A(a) &= \frac{1}{N_p}\sum_{1}^{N_p} r_i \\ V(a) &= N_u / \lceil N_p/2 \rceil \\ U^*(a) &= \text{median}(u_j,\ \forall j \in [1\,..\,N_u]) \end{aligned}$$

Availability is normalized, the fraction of times a host is reachable. Volatility is normalized by $\lceil N_p/2 \rceil$, the maximum number of states (alternating value each time). (We also sometimes use un-normalized volatility, $V^*(a) = N_u$, simply the count of up periods.) We considered normalizing median-up to measurement duration, but chose not to because such normalization distorts observations about hosts that are not nearly always present.

While these metrics are not orthogonal, each has a purpose. Availability shows how effectively addresses are used. High volatility indicates addresses that are intermittently used and often dynamically allocated. Median uptime suggests how long an address is used.

These estimates assume the $r_i$ observations are correct and represent a single host. Because we know our data collection omits firewalled hosts (§[3.1]), we generally ignore addresses that never respond. More troubling are addresses used by multiple computers at different times—such addresses actually represent *multiple* hosts. The purpose of dynamically allocated addresses is exactly to share one address with multiple computers, and we know dynamic assignment is common (see §[4]). If those hosts are used for different purposes (servers sometimes, and clients others), usage inference will be difficult and unreliable. However, we believe that it is relatively uncommon for a dynamic address to transition between client and server use, since servers usually require stable addresses. (There is some use of dynamic DNS to place services on changing addresses. We believe such use is rare for most of the world but plan to explore this issue in future work.)

### 3.2.2 Metrics characterizing edge bitrate

While address usage considers all ICMP responses (positive and negative), round-trip time estimates are only present in positive responses. To estimate bitrate, we therefore define $R^*(a)$ be the set of RTT values extracted from positive responses for address $a$, that is, the set of all $R_i^*(a)$ where $r_i^*(a) = 1, \forall i \in [1\,..\,N_p]$. (So $|R^*(a)| \leq |r^*(a)|$.) From this set we compute standard deviation of $R^*(a)$: $R^*_{\mu_{1/2}}(a)$, when we have sufficient samples ($|R^*(a)| \geq 10$).

We use these metrics to identify low-bitrate edge links. Median-RTT tracks typical response bitrate, while stddev-RTT estimates variance. In §[3.5] these metrics can identify low-bitrate blocks.

## 3.3 Block Identification

We next use our observations about addresses to evaluate block size using a clustering algorithm that considers the address hierarchy.

We assume blocks are allocated in sizes that are powers of two, so block identification is the process of finding a prefix where addresses in the block are used consistently. We find that some blocks are *not* used consistently, and different addresses show very different stability. In our analysis we will keep dividing these *mixed-use blocks* until they are consistent, if necessary devolving to a single address per block. Another challenge is that many blocks have gaps where a few addresses are used differently, or are not responsive, perhaps because they are unused or firewalled. Our algorithm weighs choice of larger blocks with some inconsistencies against smaller but more homogeneous blocks.

We only consider /24 blocks and smaller because current data collection method gathers samples of that size. Exploration of larger blocks is an area of potential future work.

We use partitional clustering [17] to determine blocks that appear to be used consistently based on their responsiveness. A *pattern matrix* defines the features of patterns (i.e., addresses) being clustered: ($A(a)$, $V(a)$, $U^*(a)$) across the space of disjoint /24 blocks. (We also use ($R^*_{\mu_{1/2}}(a)$, $R^*_{\sigma}(a)$) later in §[3.5] to identify block connection types.) Each /24 block has a $256 \times 3$ pattern matrix $x_{ij}^*$, where $j$ enumerates the three features, and $i$ enumerates each address in a /24 block. From our 24,000 /24 blocks we get 24,000 pattern matrices in total. To give each features equal weight, we employ *feature normalization*. And we define the normalized pattern matrix as $x_{ij} = (x_{ij}^* - \mu_j)/\sigma_j$, where $\mu_j$ and $\sigma_j$ are the feature's mean and standard deviation. We then use Euclidean distance to measure dissimilarity between two patterns. Because Internet addresses impose a unique restriction that addresses are only grouped into blocks that are contiguous, sizes of powers of two, and aligned at multiples of the size, we cannot directly use traditional algorithms such as $K$-means. We therefore employ an *elbow criterion*, a common rule of thumb to determine the number of clusters. We split each cluster into two whenever splitting adds significant information, and we stop when we pass the "elbow" of the curve and more clusters add little benefit.

### 3.3.1 Our algorithm to identify block sizes

Our algorithm follows the basic structure from above: we define a pattern matrix of addresses by features, normalize the features, then recursively search for clusters until reaching the elbow. We fill in the details next.

The algorithm is a recursive function, *BlockSizeId*, taking an address-feature matrix $256 \times (A(a), V(a), U^*(a))$ and a given prefix length $P$. Since the blocks in our survey are disjoint, we iterate over each /24 block in our survey separately, beginning with $P = 24$.

*BlockSizeId* then computes the intra-block unnormalized variance, $vsum_p$, for all possible prefix lengths $p$ ($P \leq p \leq 32$). It then selects the smallest prefix length $p_{elbow}$ where longer prefixes show minimal change.

$$\begin{aligned} n_p &= 2^{p-P}, s_p = 2^{32-p}, \mu_{bj} = \frac{\sum_{i=(b-1)s_p+1}^{bs_p} x_{ij}}{s_p} \\ v_b &= \sum_{j=1}^{3} \sum_{i=(b-1)s_p+1}^{bs_p} (x_{ij} - \mu_{bj})^2, 1 \leq b \leq n_p \\ vsum_p &= \sum_{b=1}^{n_p} v_b, P \leq p \leq 32 \end{aligned}$$

Here $n_p$ is the number of sub-blocks with prefix length $p$, $s_p$ is the size of sub-blocks (number of addresses) with prefix length $p$. For example, if $P = 24$ and $p = 27$, then $n_p = 8$ and $s_p = 32$. $m_{bj}$ is the mean value of the $j^{\text{th}}$ feature of addresses in the $b^{\text{th}}$ sub-block. $v_b$ is the intra-block unnormalized variance of the $b^{\text{th}}$ sub-block. In this example, it would be the intra-block unnormalized variance of the $b^{\text{th}}$ /27 sub-block.

We define minimal change in the elbow algorithm with an empirically selected constant threshold, $\epsilon = 2.0$. We select $p_{elbow}$ as the smallest $p$ such that $vsum_{i+1} - vsum_i < \epsilon, p \leq i \leq 31$. If $p_{elbow} = P$, then *no* division of this block reduces variance significantly and we terminate our recursive algorithm, declaring $P$ the consistent block size. If this case does not hold, we have determined there are splits of the block that appear to be more consistent. We then split the block in half and recurse, calling *BlockSizeId* with the next longer prefix $P = p+1$ on each half of the data. In principle, a block could be split repeatedly until it is composed on a single address (since singletons will drive variance to zero). In §[4.1] we show that, in practice, our threshold causes the majority of the Internet addresses fall into larger blocks of consistent use.

### 3.3.2 A block identification example

To illustrate *BlockSizeId* we next show analysis of an example /24 block taken from the Internet. The top of Figure 1 shows the whole block, while the bottom graphs show how the algorithm identifies four sub-blocks. As described earlier (§[1]), a human identifies two bright green areas (or light grey) indicating high availability: $p.65/32$ and $p.128/27$, and two dark areas showing low availability and volatility, $p.160/27$ and $p.192/26$. Hostnames for this block show it is used for wireless access, and the green areas are servers and routers, while the dark areas are dynamically assigned by DHCP.

The first graph in the middle of the figure shows the first pass of *BlockSizeId*, with $P = 24$ covering all of block $p.0/24$. In the graph, the $y$-axis shows variance for division of the block into each possible power-of-two smaller size. Here $p_{elbow} = 25$ and $p_{elbow} > P$, so we recurse to $P = 25$.

The second row of two graphs shows these recursive invocations, $p.0/25$ on the left and $p.128/25$ on the right. For $p.0/25$ with only one responsive address, the left graph shows a consistent variance regardless of subdivision, and $p_{elbow} = P = 25$, so this prefix is consistent and this recursion terminates. For $p.128/25$ on the right, a subdivision reduces variance and so we recurse again to $P = 26$.

The algorithm continues until either $p_{elbow} = P$ or $P = 32$. In this example, the initial /24 block is divided into $p.65/32$, $p.128/27$, $p.160/27$, and $p.192/26$.

## 3.4 Ping-Observable Block Classification

We can now take remote measurements, convert them into observations, and use them to identify blocks of consistent neighboring addresses. We generalize our observations on addresses into observations about a block $b$ by taking the median value of each observation:

$$(A(b), V(b), U^*(b)) = \text{median}(A(a), v(a), U^*(a)) \, \forall a \in b$$

We then classify these blocks into five *ping-observable categories*, using $(A(b), V(b), U^*(b))$. We use four thresholds, $\alpha_H = 0.95$, indicating high availability, $\alpha_L = 0.10$, indicating low availability, $\beta = 0.0016$, for low volatility ($V(b) = \beta$ is equal to $V^*(b) = 1$, i.e., only up for once), and $\gamma = 6$ hours, corresponding to a relatively long uptime.

**Always-stable**: highly available and stable.

$$(A(b) \geq \alpha_H) \wedge (V(b) \leq \beta)$$

**Sometimes-stable**: changing more often than always-stable, but frequently up continuously for long periods (high $U^*(b)$).

$$(U^*(b) \geq \gamma) \wedge (A(b) \geq \alpha_L) \wedge (A(b) < \alpha_H \vee V(b) > \beta)$$

**Intermittent**: individual addresses are up for short periods (low $U^*(b)$):

$$(U^*(b) < \gamma) \wedge (A(b) \geq \alpha_L) \wedge (A(b) < \alpha_H \vee V(b) > \beta)$$

**Underutilized**: although addresses are occasionally used, they show low $A(b)$ values.

$$A(b) < \alpha_L$$

**Unclassifiable**: we decline to classify blocks with few active responders, currently defined as any block where fewer than 20% of addresses respond.

We selected these categories to split the majority of the $(A(b), V(b), U^*(b))$ space, informed by evaluations of dozens of blocks (573K addresses in total) backed by manual probing of hosts and hostnames (details, see [4]).

While we have defined these categories based on what we can observe, the categories are correlated to real-world address usage. *Always-stable* is typical of servers, routers and always-up end hosts. Manual inspection of randomly chosen reverse hostnames indicates that more than 80% servers and routers have always-stable addresses. *Sometimes-stable* correlates addresses with hostnames that indicate statically-assigned user computers, businesses (names containing “biz” or “business”), some dynamically assigned but always-on connections (cable modems or DSL connections). *Intermittent* characterizes the majority of cable and DSL hosts and some active dial-up hosts. We find many address blocks, often identified as dial-up by hostname, are categorized as *underutilized*. (More than 50% of hostnames that indicate dial-up have $A(b) < \alpha_L$.)

We examine sensitivity to our choices in §[5.3].

## 3.5 Identifying Low-bitrate Blocks

Block categories correlate with edge link technologies, but they are not one-to-one—we find that dial-up and DSL appear as both intermittent and underutilized. To better understand technology trends, we next show that variance across repeated RTT measurements can identify blocks with low-bitrate edge links. We define low-bitrate as less than 100Kb/s, such as dial-up (56Kb/s) and GPRS (57.6 Kb/s). We first present a RTT model, and then apply it.

### 3.5.1 Background: components of RTT

Round-trip time has several components:

$$RTT = 2(D_{cpu} + D_{prop} + D_t + D_q)$$
$$\text{where } D_t = S/B \text{ and } D_q = nD_t$$

The first two components, per-hop processing delay in the routers ($D_{cpu}$), and distance-based propagation delay ($D_{prop}$) are largely independent of the edge link. Transmission delay ($D_t$), however, is based on packet size ($S$, approximated as constant for this simple model) and the bottleneck link's bitrate, $B$. Queuing delay ($D_q$) is a multiple of $D_t$ based on queue length. (All terms are for the full round-trip and do not require path symmetry; we assume the prober is well connected.)

Our goal is to distinguish addresses with low-bitrate edge links from broadband links. In the simplest possible case, we first assume the targets are one-hop from our prober and there is no congestion, so $D_{cpu}$ and $D_{prop}$ are negligible and $D_q = 0$. Here the only difference is transmission delay, and we can easily distinguish common edge technologies since $D_t$ dominates RTT. Here even a simple threshold of $R^*(a)$ would distinguish slow edge links, since our 64B probe takes 9ms over a 56kb/s dial-up link but much less than 1ms at broadband (1Mb/s or faster).

In practice, our prober is distant from most of the Internet and we encounter interfering traffic. At long distances, $D_{cpu}$ and $D_{prop}$ can dominate RTT, often approaching 200ms for communications between continents, completely obscuring the effects of the edge we wish to observe via $D_t$.

Queuing delay is another source of noise, but it also provides the *means to see through* distance. With queuing delay, $D_q = nD_t = n(S/B)$, where $B$ is the bitrate on the backlogged link. Queuing delay can happen at any location along the path, either in the backbone or the edge link. We assume that most queuing occurs at the edge link, since although backbones are highly multiplexed, they consist of high-bitrate, carefully managed links, and we expect queues to be short ($n$ is low) and to clear quickly (since $D_t < 1\mu$s at 1Gb/s, even for a 1500B interfering packet). For slow edges, each packet in the queue ahead of a probe adds tens or hundreds of milliseconds, since ($D_t$ is 1ms for 1Mb/s ADSL, and almost 10ms for dial-up, and $D_q = nD_t$. If we assume slow links are likely at the edges, then queuing ($D_q$) and RTT are dominated by the effects of this edge link.

### 3.5.2 Identifying low-bitrate links from RTT

We next turn to identifying blocks with low-bitrate edge-links with three steps: isolating the $D_q$ component of RTT, and generalizing results to blocks, and then classifying blocks as low-bitrate.

Any given RTT observation is made up of the four components identified previously. With one observation we cannot separate those contributions. However, a week-long survey provides hundreds of observations for most addresses. If routing is generally stable, all components of RTT are constant except for queuing delay, while $D_q$ varies depending on how backlogged the edge link each time it is probed. We therefore look at *variation* in RTT to infer $D_q$, as measured by $R^*_\sigma(a)$ , the standard deviation of the RTT. Routing techniques such as load balancing or wide geographic distribution of adjacent addresses [10] are sources of noise; we utilize a fairly high threshold to mitigate their effects.

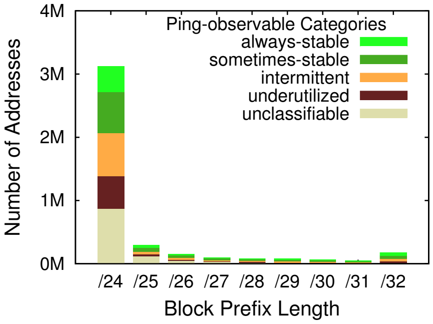

**Figure 2: Number of addresses in each block size and ping-observable categories in *IT17ws*.**

Standard deviation is well defined only with multiple measurements and for positive probe responses; we ignore $R^*_\sigma(a)$ when $|R^*(a)| < 10$ as statistically invalid, and RTTs for negative responses since they may be generated by a router on either side of the edge link. There are many addresses that fail to reply positively to probes: in our survey, only about 41% of addresses from blocks that have any responses at all respond, and about one-twentieth of these respond fewer than 10 times. Our analysis of networks shows that most are composed of large, homogeneous blocks (we show this data in §[4.1]), so we extend our address-level observations to blocks by defining a block-level estimate of RTT variance as the median of all address-level standard deviations: $R^*_{\mu_{1/2},\sigma}(b) = \text{median}(R^*_\sigma(a))\ \forall a \in b$.

**Low-bitrate block**: We therefore identify low-bitrate blocks from broadband by large variance:

$$R^*_{\mu_{1/2},\sigma}(b) > \delta$$

We select $\delta = 300ms$, because it is roughly 1.5× the delay of a full-size packet at dial-up speeds (1500B takes 212ms at 56kb/s), and based on evaluation of dozens of low-bitrate blocks. We examine the validity of this classification approach and the threshold in §[5].

# 4. APPLICATIONS

We next use the data to explore several questions in network management: what are typical sizes of consistently used Internet address blocks? How effectively are they being used? And how prominent is dynamic addressing?

To help answer these questions we compare our observations with the allocation data from the regional Internet registries (RIRs) [1]. This RIR data includes the time and country to which each address block is assigned. Although not completely authoritative, this data is the best public estimate for address delegation of which we are aware. We collect data from each of the RIRs, selecting data dated June 13, 2007 to closely match our survey data.

## 4.1 Block Sizes

We begin by considering block sizes. Figure 2 and Table 2 show our analysis of *IT17wvs*.

This data shows that addresses in the Internet are most commonly managed in blocks with /24 prefixes. In fact, even though there are more opportunities for small blocks, we find more /24 blocks than blocks of size /25 through /29. Since our data collection only probes consecutive runs of 256 addresses, this prevalence suggests we may need to

| **size** | | | **sometimes-** | | | **classifiable** | **unclassifiable** | **blocks** | **addresses** |
|---|---|---|---|---|---|---|---|---|---|
| pfx | addrs | **always-stable** | **stable** | **intermittent** | **underutilized** | (100%) | | *[100%]* | |
| **/24** | 256 | 1,603 (18%) | 2,517 (29%) | 2,673 (30%) | 1,994 (23%) | 8,787* | 3,411 *[27%]* | 12,198 | 3,122,688 |
| **/25** | 128 | 323 (23%) | 523 (38%) | 295 (21%) | 237 (17%) | 1,378* | 920 *[40%]* | 2,298 | 294,144 |
| **/26** | 64 | 346 (21%) | 617 (38%) | 378 (23%) | 274 (17%) | 1,615* | 787 *[33%]* | 2,402 | 153,728 |
| **/27** | 32 | 432 (20%) | 855 (40%) | 506 (23%) | 361 (16%) | 2,154† | 872 *[29%]* | 3,026 | 96,832 |
| **/28** | 16 | 759 (20%) | 1,301 (34%) | 993 (46%) | 734 (19%) | 3,787† | 1,139 *[23%]* | 4,926 | 78,816 |
| **/29** | 8 | 2,077 (21%) | 3,190 (32%) | 2,355 (24%) | 2,227 (23%) | 9,849† | 0 | 9,849 | 78,792 |
| **/30** | 4 | 3,312 (19%) | 5,656 (33%) | 4,679 (27%) | 3,707 (21%) | 17,354† | 0 | 17,354 | 69,416 |
| **/31** | 2 | 4,195 (16%) | 9,867 (37%) | 7,864 (30%) | 4,566 (17%) | 26,492† | 0 | 26,492 | 52,984 |
| **/32** | 1 | 52,646 (30%) | 42,847 (24%) | 43,266 (25%) | 36,707 (21%) | 175,466† | 0 | 175,466 | |
| **entire *IT17ws* dataset:** | | | (1,603,086 addrs. in non-responsive blocks) + (4,122,866 in responsive blocks) | | | | | 22,367 | 5,725,952 |

**Table 2: Number of blocks of each size in *IT17ws* (10 days). Unclassifiable percentages relative to all blocks; other percentages relative to classifiable blocks. Asterisks: consistent blocks, daggers: non-consistent.**

probe larger consecutive areas to understand if even larger blocks are common but not seen in our survey.

There are a very large number of the smallest blocks, with about as many /29s as /24s, and roughly twice as many /30s as /29s, and /31s as /30s. These results may be artifacts of our block discovery algorithm: it is statistically easier for an address to be consistent with a few neighbors in a small block than with 128 neighbors in a /25. We next re-examine the second assumption underlying our work: are contiguous addresses often used similarly? If we define consistent usage as just the largest three block sizes (/24 through /26) that we successfully identify, we find 2,529,216 addresses are used consistently, or 44% of the probed address space.

While clearly defined, this percentage does not accurately present how much of the Internet is consistently used. Some of the probed address space is unclassifiable (with consistent usage but fewer than 20% of addresses responding), or completely non-responsive. We cannot say anything about blocks that fail to respond at all. The status of unclassifiable blocks is uncertain, but a conservative position is to declare them inconsistent. A more representative evaluation of the Internet is therefore to compare how much is definitely used consistently (2.5M addresses in large blocks) against that is effectively inconsistent (the 506,178 addresses in small blocks) and the possibly inconsistent (the 1,087,472 addresses in unclassifiable blocks). This computation suggests that a lower bound of *61% of the responsive Internet is used consistently*, We believe this supports our second assumption: **the majority of contiguous addresses are used consistently**.

## 4.2 Address Utilization

Given block sizes, we next evaluate how efficiently addresses are used in those blocks. Inefficient IPv4 usage represents an opportunity for improvement, but greater efficiency comes with greater management cost. Management cost of IPv4 should be weighed against simpler-to-manage IPv6.

### 4.2.1 Quantifying underutilization and possible causes

The *underutilized* ping-observable category is defined as a sequence of addresses that are used less than 10% of the time (§[3.4]). Large blocks of such infrequently used, public IP addresses generally indicate inefficient address utilization. (Such low utilization seems to make sense only in unusual circumstances, such as a DTN satellite only infrequently in view [8].)

The underutilized column of Table 2 shows that these blocks are quite common, accounting for 17–23% of blocks of each size, Although not shown in the table, the mean availability of addresses in /24 underutilized blocks is only 3.2% of our 10-day observation (*IT17ws*). Manual examination of addresses shows the mean number of up periods is less than 5 ($V^*(b) = 4.6$), typically for around 1 hour ($U^*(b)$).

To understand causes of underutilized blocks we examine the address hostnames of these /24 blocks. We find 63% of addresses provide hostnames, and many of these hostnames (34%) include keywords that suggest how the address is used. For example, dial and dsl suggest edge link technologies, and dynamic or pool suggest dynamic address assignment. (Full details [4] are omitted here due to space.) Among the various usage suggested by hostnames, underutilized blocks are correlated with *pool* (68%), *ppp* (56%) and *dial* (54%) hostname categories.

We hypothesize that this low utilization is tied to dial-up technology itself. Dial-up lines are often shared with voice communication, encouraging short, intermittent use. Yet dial-up POPs must be provisioned to handle peak loads. A secondary factor may be trends shifting customers from dial-up to higher speed connections. Perhaps old dial-up provisioned blocks are simply in lower demand than previously. Finally, while dial-up utilization is low, we cannot tell how many users each dial-up address serves. Perhaps address reuse is high enough to make these apparently under-provisioned addresses a bargain relative to supporting the same number of users with always-on connections. Further study to understand these trade-offs is future work.

Reversing the question, we can ask *which blocks are well utilized*? Still by examining the hostnames, we found that blocks with keywords *static, cable, biz, res, server, router* have very few underutilized addresses. Static addresses are usually assigned to fixed-location desktops or businesses, and these computers tend to maintain Internet connection and occupy their address for a fairly long time. In addition, static addresses are often billed at a flat rate per month, while dynamic addresses may incur a time-metered charge.

### 4.2.2 Locations and trends of underutilization

Evaluating underutilization by country may highlight policy differences by regional registries or ISPs. After merging our data with RIR data, Table 3 shows utilization by country. We see that the United Kingdom and Japan have the largest fraction of underutilized blocks, 40–60%, suggesting potential local policy differences. We expected a large number of underutilized blocks in the U.S. because of wide deployment of dial-up. While the U.S. has the largest absolute number of underutilized blocks, its fraction is relatively low.

Table 4 shows that the fraction of underutilized blocks is fairly consistent across all five RIRs, suggesting differences are likely due to country, not RIR policies.

Finally, the lower right graph in Figure 3 shows when underutilized blocks were allocated. The fraction of blocks by

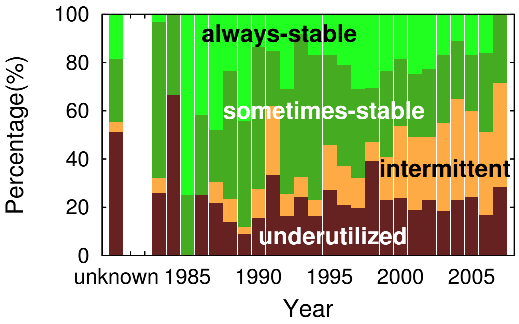

**Figure 3: Trend of ping-observable category change in *IT17ws* /24 blocks**

age seems fairly evenly distributed, except for peaks in very early allocations (1984 and unknown), where more than 60% of the blocks assigned are underutilized. We believe these earliest allocations were made with relatively little assessment of organizational need, and large initial allocations allow continued use with minimal concern for efficiency.

## 4.3 Intermittent and Dynamic IP Addressing

Addresses are intermittently used by statically addressed hosts that are only sometimes connected to the network, or by hosts that obtain dynamically assigned addresses from a pool, typically with DHCP [6].

Dynamic assignment of addresses allows ISPs to multiplex many users over fewer addresses. Dynamic addressing also provides ISPs the business opportunity of offering static addresses as a higher-priced service, and potentially makes it more difficult for users to operate servers. Dynamic addressing has been promoted to users as a security advantage, on the theory that a compromised computer is more difficult to contact if its IP address changes. Dynamic addressing prevents users from running services or accepting unsolicited inbound connections (for example, for incoming SIP calls), although applications employ work-arounds such as STUN [26].

Recent studies [13, 29, 31] have examined dynamic addressing for several reasons. First, dynamic addresses complicate some network services, such as reputation systems. They also are correlated with spam; some spam filters penalize dynamic addresses because of the frequent exploitation of dynamically addressed home computers by spammers. We next show that our approach can identify dynamic addressees and suggest the causes and trends that have been previously invisible.

### *4.3.1 Quantifying dynamic addressing*

We believe that the *intermittent* and *underutilized* ping-observable categories correspond to the short-term dynamically assigned addresses of interest. Although we cannot quantify what fraction of these categories actually use DHCP, our belief is supported by hostname analysis. Hostnames shows that intermittent blocks commonly include keywords *cable* (57%), *dynamic* (48%) and *dsl* (41%), all of which often use short- or moderate-term dynamic addressing, and underutilized blocks often include keywords for *pool* (68%), *ppp* (56%) and *dial* (54%).

Table 2 shows that 40–50% of classifiable blocks (depending on block size) appear to be dynamic. Even with wide deployment of always-on connectivity, nearly half of Internet addresses are used for short periods of time. For intermittent blocks, the mean availability is just under 30%, with nine use periods over the week and a mean $U^*$ around 2.5 hours.

### *4.3.2 Locations and trends for dynamic addressing*

Analysis by country can suggest how political, cultural and policy factors affect addressing. Table 3 shows that nearly two-thirds of Chinese blocks are intermittent, with Germany, Korean, and Brazil all nearly half or more. Several factors may contribute to this use.

China has a very large population and is a relative latecomer to the Internet; from the beginning of commercial deployment in China. ISPs have planned to make best use of the relatively few IPv4 addresses per potential user. They have therefore promoted dynamic use to improve address utilization. An interesting direction for future work would be to evaluate how effective their utilization is. Unfortunately we only know address responsiveness, not the number of actual computers users per address needed to answer this question.

Time-metered billing is another reason for intermittent use. Parts of China and Germany employ metered billing, encouraging intermittent use even with broadband. Other potential reasons for intermittent use include turning off a router to conserve energy, or carrying over habits learned from dial-up use to broadband, and potentially continued use of dial-up connections shared with voice communication.

Evaluation of usage by registry (Table 4) shows larger differences in use. We see that intermittent blocks are very prominent under APNIC and LACNIC (40–53%), five times more common than for ARIN in North America (9%). We believe these differences stem largely from policies of the countries the RIRs serve, not the RIRs themselves. We discussed Chinese practice above; several Latin American countries have limited choice in ISPs, with national providers adopting pricing or policies that strongly favor dynamic address assignment even for business use (as confirmed by LACNIC personnel [21]). We speculate that the large number of sometimes-stable blocks in ARIN is because of long DHCP lease times and always-on use by home users, enabled by relatively plentiful numbers of IPv4 addresses per user.

Finally we consider trends in dynamic addressing. The lower left of Figure 3 shows that intermittent blocks are more common in new address allocations. This observation is consistent with a recognition of eventual full allocation of the IPv4 address space and efforts to manage addresses in countries newer to the Internet. The rise in intermittent blocks matches a corresponding fall in always-stable blocks (top left, Figure 3). In addition to growing demand for dynamic addressing, this trend suggests most new addresses are added to provide service for home users, intermittently. While the absolute numbers of always-stable businesses and servers grows, its fraction of all addresses is shrinking.

## 4.4 Understanding Edge Bitrates

To understand causes for utilization, we next look at block connectivity to the Internet.

In §[3.5.2] we suggested that RTT variance can indicate low-bitrate edge links such as dial-up and pre-3G mobile telephones. Here we apply this analysis to provide a new tool to understand how edge networks correlate with underutilization. Future work includes using this analysis to evaluate deployment trends and to automatically adapt websites to the user's network.

To understand the usage of low-bitrate blocks, Figure 4 shows the availability for blocks broken into low- and non-

| code | country | always-stable | sometimes-<br>stable | intermittent | underutilized | classifiable<br>(100%) | unclassifiable | blocks<br>*[100%]* |
|---|---|---|---|---|---|---|---|---|
| **US** | US | 673 (27%) | **1,106 (45%)*** | 231 (9.3%) | 472 (19%) | 2,482 | 1,383 *[36%]* | 3,865 |
| **CN** | China | 39 (4.1%) | 117 (12%) | **615 (65%)*** | 171 (18%) | 942 | 132 *[12%]* | 1,074 |
| **JP** | Japan | **383 (48%)*** | 50 (6.2%) | 18 (2.2%) | **350 (44%)*** | 801 | 288 *[26%]* | 1,089 |
| **DE** | Germany | 65 (10%) | 125 (20%) | **388 (61%)*** | 62 (9.7%) | 640 | 56 *[8.0%]* | 696 |
| **KR** | Korea | 21 (4.6%) | 131 (29%) | **237 (52%)*** | 68 (15%) | 457 | 142 *[24%]* | 599 |
| **FR** | France | 18 (4.1%) | **227 (52%)*** | 167 (38%) | 28 (6.4%) | 440 | 58 *[12%]* | 498 |
| **GB** | UK | 39 (13%) | 37 (12%) | 52 (17%) | **179 (58%)*** | 307 | 180 *[37%]* | 487 |
| **BR** | Brazil | 7 (3.9%) | 35 (19%) | **86 (48%)*** | 52 (29%) | 180 | 58 *[24%]* | 238 |
| **all others** | | 358 (14%) | 689 (27%) | 879 (35%) | 612 (24%) | 2,538 | 1,114 *[31%]* | 3,652 |
| **/24 blocks in entire *IT17ws* dataset:** | | | | | | 8,787 | 3,411 *[27%]* | 12,198 |

**Table 3: The distribution of /24 blocks in ping-observable categories of 10 countries. Bold and asterisks indicate the categories with more than 40% of blocks. Colors indicate categories and each country's dominant category. Countries are sorted by total number of blocks.**

| registry | always-stable | sometimes-<br>stable | intermittent | underutilized | classifiable<br>(100%) | unclassifiable | blocks<br>*[100%]* |
|---|---|---|---|---|---|---|---|
| **RIPENCC** | 408 (14%) | 798 (27%) | **1,084 (37%)*** | 661 (22%) | 2,951 | 990 *[25%]* | 3,941 |
| **APNIC** | 473 (18%) | 422 (16%) | **1,091 (40%)*** | 716 (27%) | 2,702 | 795 *[23%]* | 3,497 |
| **ARIN** | 706 (27%) | **1,185 (45%)*** | 258 (9.7%) | 512 (19%) | 2,661 | 1,481 *[36%]* | 4,142 |
| **LACNIC** | 13 (3.2%) | 94 (23%) | **218 (53%)*** | 86 (21%) | 411 | 120 *[23%]* | 531 |
| **AFRINIC** | 3 (4.9%) | 18 (30%) | **21 (34%)*** | 19 (31%) | 61 | 19 *[24%]* | 80 |
| **/24 blocks in entire *IT17ws* dataset:** | | | | | 8,787 | 3,411 *[27%]* | 12,198 |

**Table 4: The distribution of /24 blocks in ping-observable categories of 5 regional registries. Bold and asterisks indicate the categories with more than 40% of blocks. Colors indicate categories and each registry's dominant category. Registries are sorted by total number of blocks.**

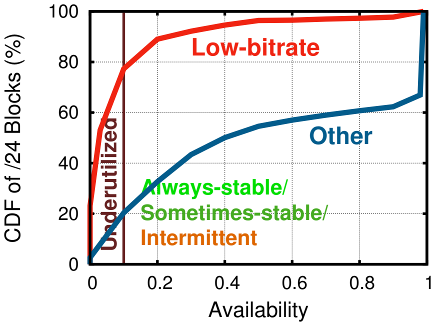

**Figure 4: Comparison of availability for low-bitrate (top line) and non-low-bitrate (bottom line) classifiable /24 blocks in *IT17ws*.**

low-bitrate groups by RTT stability (as defined in §[3.5.2]). From the underutilization threshold of $A(b) < 0.1$, we see that nearly 80% of low-bitrate blocks are underutilized, compared to only 20% of non-low-bitrate blocks. Therefore low-bitrate connections strongly correlate with sparse use.

To explain this correlation between edges and underutilization, we use hostnames and whois to infer *operational usage*—roughly, how blocks are managed (dynamic or static) and what type of edge-link they are (dial-up, PPP, DSL, etc.). Such inferences are less than ideal, but they provide the best available ground truth about the general Internet. Among the 200 randomly selected low-bitrate blocks, we successfully inferred the operational usage of 46 blocks: 41 dial-up, 2 PPP, and 3 DSL blocks. Dial-up and PPP are indicator of low-bitrate edge connection while DSL is one representative of broadband connection. While not providing definitive causes of underutilization, this suggests correlation between low use rates, low bitrates, and dial-up edge networks.

To support this explanation, we studied the median-uptime $U^*$ for both low-bitrate and broadband blocks (data omitted due to space). We found that up durations in the vast majority of low-bitrate blocks are quite brief: 85% of low-bitrate blocks have a $U^*(b) < 0.5$ hours, compared to only 15% of other blocks. This observation suggests that low-bitrate, dial-up blocks are provisioned for a large number of potential users who do not use the network concurrently.

# 5. VALIDATION

We have now shown data to support our three assumptions: addresses respond to probes (the subject of prior work [13]), adjacent addresses have similar use (§[4.1]), and probes suggest use (§[4.2]). These results have two limitations, however. First, since they are based on active probing, they are only available for the portion of the Internet that respond to probes. Evidence suggests that somewhat more than half of the publicly addressed hosts respond [13]; extension of these results to the whole Internet is an area of continuing work. Second, our conclusions are based on data taken from one survey (*IT17ws*) from the general Internet. While not biased, we cannot compare these results to the true network configuration that is distributed across thousands of enterprises.

We next present three additional studies to further validate these assumptions and address the second limitation. First we evaluate data taken from USC, a smaller and potentially biased dataset, but one where we have ground truth from the network operations staff. We then extract small random subsets of the general Internet and infer the ground truth by manual inspection using ISC-DS hostname data [15] and the whois database. Finally, we compare our Internet-wide results with additional data taken one-half to two years later to verify that our conclusions do not reflect something unusual in a single measurement or time.

## 5.1 Validation within USC

We first compare our methodology against ground truth obtained directly from the network operators at USC. This

| category: | blocks | percentage | |
|---|---|---|---|
| in routing table | 243 | 100% | |
| false negative | 105 | 43% | |
| not in use | 19 | | |
| not responding | 28 | | |
| few responding | 12 | | |
| single-block multi-usage | 46 | | |
| /25 to /27 | 9 | | |
| /28 to /32 | 37 | | |
| blocks identified | 147 | | 100% |
| correctly identified | 138 | 57% | 94% |
| false positive | 9 | | 6.1% |
| multi-block single-usage | 9 | | |

**Table 5: Evaluation of accuracy of block identification USC to ground truth sizes.**

section uses dataset *USCs* and applies the same analysis used on our general Internet dataset.

Block identification and classification at USC shows a similar prevalence of /24 blocks (85% of USC addresses are in /24s, compared to 61% in the Internet). However, USC shows many fewer intermittent and underutilized blocks compared to the Internet (only 8% among classifiable /24 blocks); we expect such variation across enterprises. We next use this data to evaluate how our assumptions affect our ability to accurately find block size, consistency, and usage.

### 5.1.1 Validation of block identification and sizes

To validate our estimation of block sizes, we compare our analysis with the internal routing table from our network administrators. This data helps quantify the accuracy of our approach, measuring the *false positive rate*, blocks that we detect but that do not actually exist, and the *false negative rate*, blocks that exist but we fail to detect.

Table 5 summarizes our comparison for all /24 blocks. (Smaller blocks are not present in our ground-truth routing table.) We find our approach correctly identifies 57% of all blocks in ground truth. Although we find the majority of blocks, we have a significant number of false negatives, failures to detect blocks. For this dataset, these false negatives show *our approach is somewhat incomplete*. On the other hand, if we evaluate our algorithm by what it says, we see very few false positives, correctly identifying 94% of all blocks we detect. For this dataset, almost no false positives show *our approach is quite accurate in what it asserts*.

To understand accuracy, we looked at when our approach incorrectly identifies blocks. All nine false positives are due to multiple blocks with common usage. We examined each incorrect block and found that USC administrators had placed two logically different blocks on adjacent addresses, but these administratively different blocks were used for similar purposes. Since our evaluation is based on external observations of use, we believe there is no way *any* external observer could determine these administrative distinctions.

For false negatives, we found several sources of missed block identification. We found that many blocks were either in the routing table but not assigned to locations or services (19 not in use), or in the routing table and assigned, but with no ping responses (28 not responding), or filled with only a few responders (12 few responding). In each case, our algorithm refuses to make usage assertions on unused or sparsely used space. Non- or few-responding blocks may be due to firewalls, reflecting a limitation of our probing method. Not-in-use blocks would be impossible for any external observer to confirm. In principal our algorithm could identify non-responsive blocks, but it is difficult for external observation to distinguish unused from firewalled space.

| category: | blocks | percentage |
|---|---|---|
| classified | 138 | 100% |
| unclassifiable (*false negative*) | 52 | 38% |
| incorrectly classified (*false positive*) | 3 | 2.1% |
| always stable (dynamic) | 3 | |
| correctly classified (*true positive*) | 83 | 60% |
| intermittent (dynamic) | 4 | |
| sometimes stable (dynamic) | 5 | |
| intermittent (VPN) | 1 | |
| underutilized (VPN/PPP) | 2 | |
| always stable (lab) | 2 | |
| sometimes stable (lab) | 2 | |
| always stable (building) | 25 | |
| sometimes stable (building) | 42 | |

**Table 6: Evaluation of block classification accuracy at USC to ground truth.**

Finally, other false negatives occur due to blocks that have been administratively assigned as /24s but then are used for different purposes. Nine of these show large, consistent patterns, possibly indicating delegation at the department level that is not visible to university-wide network administrators. If so, these represent incompleteness in our ground-truth data. Smaller mixed-use blocks represent violations of our assertion that adjacent addresses are used consistently.

### 5.1.2 Validation of block classification and usage

Table 6 shows the accuracy of our approach for the 138 blocks we classify. We declare 38% unclassifiable (false negatives); here we have discovered the correct block size but decline to declare a ping-observable category because the block is only sparsely responsive. We correctly classify the majority of blocks, selecting ping-observable categories that are consistent with the use of 60% of blocks. We mis-identify three blocks (a 2% false positive rate), all reported as dynamically allocated but observed as always stable. These blocks perhaps represent DHCP-assigned addresses with very long lease times for computers that are always up.

### 5.1.3 Validation of edge bitrate

We also validated our edge-bitrate assessment. USC has only two low-bitrate blocks (dial-up blocks running PPP). Experimental evaluation of *LTUSCs* successfully identifies both as low-bitrate, and does not mis-identify any of the 136 other blocks as low-bitrate. While this 100% accuracy is reassuring, the proximity of prober and target suggests that our validation with random Internet blocks (§[5.2.3]) is a more general result.

## 5.2 Validation in the General Internet

Our main validation results use USC because there network operations can provide ground truth. We would like to evaluate how well our approach works on the general Internet as well, since commercial use may differ from USC. We evaluate our ping-observable classification results for 100 randomly selected /24 blocks, and enlarge the sample size for our edge-bitrate validation in §[5.2.3].

While we cannot get ground truth from network operations for the general Internet, we can get clues about block size and usage from hostnames and the *whois* database. Hostnames are often assigned in patterns that suggest common administration and access method. For example, hostnames in 4.168.174/24 follow the convention `dialup-4.168.174.*.dial1.losangeles1.level3.net`. Such consistent naming conventions strongly suggest a common administrator

| category: | blocks | percentage | |
|---|---|---|---|
| /24 randomly selected | 100 | 100% | |
| decided (/24 inferred from hostname) | 37 | 37% | 100% |
| correct | 25 | | 68% |
| wrong (false negative) | 12 | | 32% |
| few responding | 6 | | |
| single-block multi-usage | 6 | | |
| undecided | 63 | 63% | |
| no hostname | 45 | | |
| few hostnames | 7 | | |
| potential /24 inferred | 7 | | |
| correct | 7 | | |
| has sub-/24 groupings | 4 | | |

**Table 7: Evaluation of block identification accuracy of random Internet blocks.**

(in this case, Level 3). Second, the presence of "dial" in the name suggests dial-up usage and low-bitrate connection. Whois information provides an alternative view. For example, hostnames in 70.204.31/24 follow the convention `*.sub-70-204-31.myvzw.com`. Names suggest common administration, but not how it is used. Whois indicates this block is assigned to *Cellco Partnership DBA Verizon Wireless*, suggesting mobile phone usage.

### 5.2.1 Validation of block identification and sizes

We randomly select 100 /24 blocks probed, and compare their clustering results with our best estimates about the ground truth from manual analysis of hostname and whois in Table 7 (37 are identified as /24 by hostnames).

As shown in Table 7, the correctly identified rate (68%) is even higher than the one in USC validation (57%). The reason is that address space in the general Internet is used in a bigger granularity than campus network, thus, blocks tend to be more consistent.

### 5.2.2 Validation of block classification and usage

To validate the ping-observable classification, we look at the 25 correctly identified /24 blocks in the previous 100 random /24 blocks. To validate the low-bitrate classification, because of the low percentage of low-bitrate blocks, we enlarged our random sample to 200 /24s.

About ping-observable classification, of the 25 correctly identified /24 blocks, we classified 20 of them; 5 were unclassifiable because of lack of hostname and whois information. We omit the details due to space, but we found 85% (17 of the 20) were correctly classified, using a loose mapping from hostnames to our ping-observable categories, while we only incorrectly classified one. For example, hostnames for three blocks suggested servers; two of those were identified as always stable (a true positive), one was identified as sometimes stable, our only false positive. Because the mapping from hostname-to-ping-inferred category is not one-to-one, our estimates of "ground truth" here are imprecise and we do not claim this result is definitive, but merely suggestive that our classification works well over the general Internet.

### 5.2.3 Validation of edge bitrate

Among the random 100 /24 blocks, only 10 of them (6 dsl & 1 cable, 1 dial & 2 mobile-phone) can be used as ground truth to validate our edge-bitrate assessment. Known low-bitrate blocks are rare in the Internet, thus we want to have more samples to validate our edge-bitrate assessment. Simply adding more random blocks to the previous 100 blocks and manually inspecting them is time-consuming. So we use an automatic way, although a little coarser, to add more samples. We randomly pick only classifiable /24 blocks with consistent naming convention in hostnames that have certain keywords (dsl, cable, dial) indicating edge access link type. This process can be easily automated with hostname data only without querying the whois database. Thus, in addition to the previously identified 10 blocks, we add 26 random hostname-inferrable edges blocks, for a total of 36 blocks as ground truth. Table 8 summarizes our analysis.

| category: | blocks | percentage |
|---|---|---|
| hostname-inferrable edges | 36 | 100% |
| low-bitrate blocks (6 dial, 2 mobile) | 8 | |
| $R^*_{\mu_{1/2},\sigma}(b) > \delta$ (true positive) | 8 | |
| $R^*_{\mu_{1/2},\sigma}(b) \leq \delta$ (false negative) | 0 | 0% |
| broadband (21 dsl, 4 cable, 3 3G) | 28 | |
| $R^*_{\mu_{1/2},\sigma}(b) > \delta$ (false positive) | 0 | 0% |
| $R^*_{\mu_{1/2},\sigma}(b) \leq \delta$ (true negative) | 28 | |
| clear hostname | 25 | |
| confusing hostname | 3 | |

**Table 8: Evaluation of low-bitrate block classification accuracy of commercial blocks.**

For the 36 blocks where we can infer edge types to evaluate accuracy, we successfully classify all low-bitrate blocks and all broadband blocks. Our low-bitrate detection algorithm provides an 0% false-negative rate and a 0% false-positive rate. There were three confusing-hostname broadband blocks classified into low-bitrate. These blocks have *dial* in their hostnames. However, when we confirmed with the ISP's network operations, these blocks are actually fast 3G/UMTS wireless connections. Their $R^*_\sigma$ values are 20ms, 41ms and 43ms respectively, suggesting 1Mb/s links or faster.

## 5.3 Consistency Across Repeated Surveys

We next wish to understand if the parameters of our data collection or analysis have a disproportionate effect on our conclusions about Internet-wide address usage. To do so, we compare analysis of *IT17ws* with that of three new datasets, *IT16ws*, taken five months earlier; *IT30ws* and *IT31ws*, taken 30 months later. These surveys allow us to consider both adjacent surveys at two different times, and longer-term trends. Half of the /24 blocks in the survey are consistent across each survey, and half are randomly chosen in each survey (full details of selection methodology are elsewhere [13]). This comparison therefore observes whether network changes alter observations of the same blocks, and whether different sets of blocks show very different behavior.

Our estimates of the block size distributions are almost identical in the four surveys. If we define $s_p$ as the vector of number of blocks of prefix length $p$, the correlation coefficient of the vectors for *IT17ws* against all other surveys are all above 0.9989. We conclude that a random sample of 1% of the Internet is large enough that the block size observations are hardly affected if half of the sample is changed.

Our work assumes that contiguous addresses are often used consistently. Following §[4.1], we consider blocks of size /24 through /26 as consistent, and size /27 through /32 as inconsistent. These percentages are quite consistent in adjacent surveys, with a possible slow downward trend over time: In *IT17ws*, 44% of probed Internet, going to 43% in *IT16ws*, and 38% later in both *IT30ws* and *IT31ws*. Results are similar if we consider percentage of the responsive Internet, with 60% and 61% in *IT16ws* and *IT17ws*, and 57% and 58% in the later two surveys.

Finally we consider the temporal consistency of our ping-observable classification across four surveys. We show that temporarily adjacent surveys show consistent classification results, while more distant surveys show greater divergence. First we compare each adjacent pair of surveys. For *IT17ws* and *IT16ws*, initially we found the correlation of the number of blocks in each category to be generally good but not great across all block sizes—it ranged from 0.663 to 0.938 for blocks smaller than /29, but the correlation for /24 blocks was only 0.349. Examination showed that around 500 blocks were shifting between always- and sometimes-stable. This shift occurred because of a change in volatility and our selection of the always-stable requirement that $V(b) \leq \beta$ and $\beta = 0.0016$. For very stable hosts, a few outages can change $V^*(b)$ significantly. Examination showed that *IT16ws* and *IT17ws* are of different duration (6 and 10 days). A longer duration makes it easier to distinguish between sometimes- and always-stable blocks. When we keep the observation duration constant by considering only a 6-day subset of *IT17ws*, the correlation coefficient for /24 classification rises to 0.626. We conclude that most ping-observable classifications are good, but the separation between sometimes- and always-stable categories is somewhat sensitive. We plan to investigate the sensitivity in future work by down-sampling the survey data in time. We confirm this result by comparing the later surveys, where full 14-days of *IT30ws* and *IT31ws* show the correlations ranging from 0.77338 to 0.987. Thus we conclude that results taken near the same time are fairly consistent.

We next compare surveys taken two years apart: *IT17ws* and a 6-day subset of *IT31ws* (data for *IT31ws* is in [4] due to space constraints). There are two main differences: first, many blocks shift from sometimes-stable to always-stable, where *IT31ws* has 2,459 always-stable /24 blocks compared to only 2,001 before (33% vs. 23%). The percentage of intermittent and underutilized blocks is similar. Second, we see a larger number of /32 blocks in the later survey, up to 198k from 179k, with many of the new blocks shown as /32 always-stable blocks. This change may represent additional servers on the Internet. As described above, we know the always/sometimes-stable border is sensitive to observation duration, so future work is required to understand whether these shifts are meaningful.

## 6. CONCLUSION

We have shown that active probes can identify how Internet addresses are used, confirming that contiguous addresses are often used similarly. We have validated our claims at USC, against randomly selected Internet blocks, and over multiple years. Within the constraints of active probing, our approach provides a new tool to understand Internet use and trends.[3]

## 7. REFERENCES

[1] American Registry for Internet Numbers. RIR statistics exchange format. Technical report, ARIN, Sept. 2008.

[2] APNIC. IPv4 initial delegation criteria. web page http://www.apnic.net/services/apply-for-resources/check-your-eligibility, May 2010.

[3] ARIN. Template: ARIN-NET-ISP-4.1. web page https://www.arin.net/resources/templates/net-isp.txt, Apr. 2010.

[4] X. Cai and J. Heidemann. Understanding Block-level Address Usage in the Visible Internet (Extended). Technical Report ISI-TR-2009-665, USC/ISI, July 2010.

[5] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, kc claffy, and G. Riley. AS Relationships: Inference and Validation. *ACM CCR*, 37(1):29–40, Jan. 2007.

[6] R. Droms. Dynamic Host Configuration Protocol. RFC 2131, Mar. 1997.

[7] B. Eriksson, P. Barford, and R. Nowak. Network Discovery from Passive Measurements. In *ACM SIGCOMM*, Aug. 2008.

[8] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. In *Proc. of ACM SIGCOMM*, Aug. 2003.

[9] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On Power-Law Relationships of the Internet Topology. In *Proc. of ACM SIGCOMM*, pages 251–262, Cambridge, MA, Sept. 1999.

[10] M. Freedman, M. Vutukuru, N. Feamster, and H. Balakrishnan. Geographic Locality of IP Prefixes. In *ACM IMC*, Oct. 2005.

[11] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. RFC 1519, Sept. 1993.

[12] L. Gao. On Inferring Automonous System Relationships in the Internet. *ACM/IEEE Trans. on Networking*, 9(6), Dec. 2001.

[13] J. Heidemann, Y. Pradkin, R. Govindan, C. Papadopoulos, G. Bartlett, and J. Bannister. Census and Survey of the Visible Internet. In *ACM IMC*, pages 169–182, Oct. 2008.

[14] G. Huston. IPv4 Reports. http://bgp.potaroo.net/index-ale.html, Apr. 2009.

[15] Internet Software Consortium. Internet Domain Survey. web page http://www.isc.org/solutions/survey, Jan. 2007.

[16] V. Jacobson. pathchar—a tool to infer characteristics of Internet paths. MSRI talk, Apr. 1997.

[17] A. Jain and R. Dubes. *Algorithms for Clustering Data*. Prentice Hall, Englewood Cliffs, NJ, 1988.

[18] kc claffy, Y. Hyun, K. Keys, M. Fomenkov, and D. Krioukov. Internet Mapping: from Art to Science. In *IEEE DHS CATCH*, Washington, US, Mar. 2009. IEEE.

[19] S. Keshav. A Control-Theoretic Approach to Flow Control. In *Proc. of ACM SIGCOMM*, pages 3–16, Sept. 1991.

[20] M. Khadilkar, N. Feamster, M. Sanders, and R. Clark. Usage-based DHCP Lease Time Optimization. In *Proc. of 7th ACM IMC*, pages 71–76, Oct. 2007.

[21] LACNIC. LACNIC Policy Manual (v1.2 - 11/03/2009). http://www.lacnic.net/en/politicas/manual3.html, Apr. 2009.

[22] X. Meng, Z. Xu, B. Zhang, G. Huston, S. Lu, and L. Zhang. IPv4 Address Allocation and the BGP Routing Table Evolution. *ACM CCR*, 35(1):71–80, Jan. 2005.

[23] W. Mühlbauer, O. Maennel, S. Uhlig, A. Feldmann, and M. Roughan. Building an AS-Topology Model that Captures Route Diversity. In *ACM SIGCOMM*, Sept. 2006.

[24] J. Postel. Internet Protocol. RFC 791, Sept. 1981.

[25] Regional Internet Registry. Resource ranges and geographical data. web page ftp://ftp.afrinic.net/pub/stats/afrinic/, ftp://ftp.apnic.net/pub/stats/apnic/, ftp://ftp.arin.net/pub/stats/arin/, ftp://ftp.lacnic.net/pub/stats/lacnic/, ftp://ftp.ripe.net/ripe/stats/, June 2007.

[26] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. STUN—Simple Traversal of User Datagram Protocol Through Network Address Translators. RFC 3489, Dec. 2003.

[27] R. Sherwood, A. Bender, and N. Spring. DisCarte: A Disjunctive Internet Cartographer. In *Proc. of ACM SIGCOMM*, pages 303–314, Aug. 2008.

[28] L. Subramanian, S. Agarwal, J. Rexford, and R. H. Katz. Characterizing the Internet Hierarchy From Multiple Vantage Points. In *Proc. of IEEE Infocom*, pages 618–627, June 2002.

[29] I. Trestian, S. Ranjan, A. Kuzmanovic, and A. Nucci. Unconstrained Endpoint Profiling (Googling the Internet). In *Proc. of ACM SIGCOMM*, pages 279–290, Aug. 2008.

[30] USC/LANDER project. Internet address census/survey datasets. http://www.isi.edu/ant/traces.

[31] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber. How Dynamic are IP Addresses? In *Proc. of ACM SIGCOMM*, Kyoto, Japan, Aug. 2007. ACM.

[3] **Acknowledgments:** We thank Brian Yamaguchi and Muareen Dougherty for help understanding USC, Roque Gagliano for LACNIC, and Anja Feldman for Deutsche Telekom. We thank Yuri Pradkin for the probing software, Paul Vixie for ISC DNS data, and John Wroclawski, the reviewers, and our shepherd, Yinglian Xie, for writing improvements. The authors are partially supported by the U.S. DHS, contract number NBCHC080035, and by NSF, grant number CNS-0626696. The conclusions of this work are those of the authors and do not necessarily reflect the views of DHS or NSF.