Initial Measurements of the Cuban Street Network

Eduardo E. P. Pujol
Universidad de las Ciencias Informáticas, Cuba
kopek@riseup.net

Will Scott
University of Michigan
willrs@umich.edu

Eric Wustrow
University of Colorado
ewust@colorado.edu

J. Alex Halderman
University of Michigan
jhalderm@eecs.umich.edu

ABSTRACT

Internet access in Cuba is severely constrained, due to limited availability, slow speeds, and high cost. Within this isolated environment, technology enthusiasts have constructed a disconnected but vibrant IP network that has grown organically to reach tens of thousands of households across Havana. We present the first detailed characterization of this deployment, which is known as the SNET, or Street Network. Working in collaboration with SNET operators, we describe the network's infrastructure and map its topology, and we measure bandwidth, available services, usage patterns, and user demographics. Qualitatively, we attempt to answer *why* the SNET exists and what benefits it has afforded its users. We go on to discuss technical challenges the network faces, including scalability, security, and organizational issues. To our knowledge, the SNET is the largest isolated community-driven network in existence, and its structure, successes, and obstacles show fascinating contrasts and similarities to those of the Internet at large.

CCS CONCEPTS

• **Networks** → *Network structure*; *Wireless local area networks*;

KEYWORDS

Cuba, SNET, isolated network, community network

ACM Reference Format:
Eduardo E. P. Pujol, Will Scott, Eric Wustrow, and J. Alex Halderman. 2017. Initial Measurements of the Cuban Street Network. In *Proceedings of IMC '17*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3131365.3131395

1 INTRODUCTION

The expansion of computer networking around the world has given rise to unique local deployments as the technology has been adapted to fit local needs. Nowhere has this been more true than in Cuba, a country with a vibrant technology community but highly constrained Internet connectivity.

Cuba ranked last in the Americas in the ITU's 2016 ICT development index, having only 5.6% household Internet penetration. Typical users can only connect from a small number of WiFi hotspots [9] operated by the national telecom provider, ETECSA, and the island's international bandwidth per user measures a mere 572 bits/s [10]. The cost of access is prohibitive, with private fixed-line access costing 386% of the per-capita GDP [2].

Cubans have developed a number of organic responses to these limitations. Most widely known off the island is *El Paquete Semanal* [3], a weekly distribution of media files that is passed around on USB sticks and hard drives. There is also a growing market for sharing and resale of ETECSA Internet access. Local entrepreneurs use WiFi range extenders and hotspot apps to share accounts between multiple concurrent users and lower the per-user price [24].

Yet the largest and most technically elaborate organic network in Cuba is one that is entirely isolated from the Internet. Cuban technology enthusiasts have constructed an unsanctioned, community-driven IP network, known as the SNET or "Street Network", that connects tens of thousands of residential users across Havana. (There are also smaller equivalents in some other cities [12].) The SNET hosts hundreds of websites, including a diverse array of information and communication services. For most of its users, the SNET is the only network access available in their homes.

In this paper, we present the first systematic characterization of the SNET, with a focus on its network infrastructure and topology, available services, and user population. This research was conducted in collaboration with SNET community members, and we combine direct measurements with discussions with the network operators. While the SNET has received journalistic attention [4, 17, 20, 23], it has never before been rigorously documented. By bringing the SNET to the attention of the Internet research community, we hope to encourage further collaboration towards technical solutions that can address the SNET's unique challenges.

For the Internet measurement community, the SNET provides a unique perspective on what the Internet might have been like had it been built under different circumstances. It also provides an opportunity to learn from the SNET's approaches to some of the technical and social problems that are common to both networks.

1.1 Organization of the SNET

The SNET evolved organically, beginning in 2011 when local groups started connecting smaller neighborhood LANs that had been established for multiplayer gaming and file sharing. Today, nine large, geographically overlapping communities have interconnected.

The network has no central authority. It is managed cooperatively by several hundred part-time administrators, who operate the infrastructure in homes and apartments, using hardware purchased second-hand or scavenged from businesses. Some operators acquire equipment with financial help from their local communities, thus spreading the cost among the users who are connected.

IMC '17, November 1–3, 2017, London, United Kingdom

ACM ISBN 978-1-4503-5118-8/17/11.
https://doi.org/10.1145/3131365.3131395

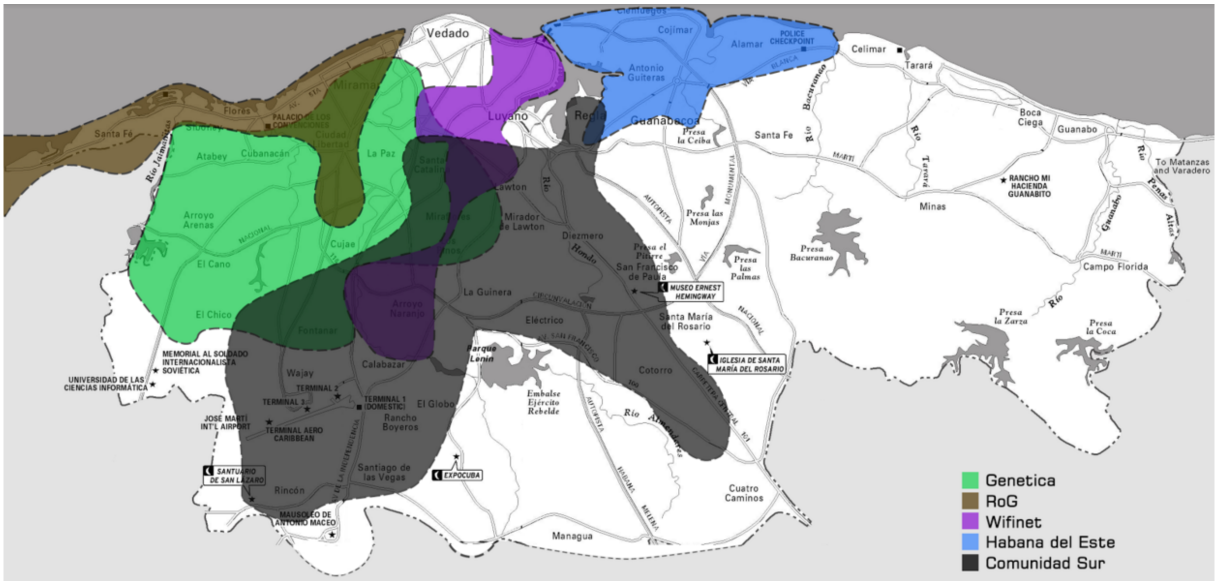


Figure 1: This community-created map shows the service areas of several SNET pillars spanning metro Havana.

Topologically, the network is organized around a core set of connection points, known as *pillars*, which connect to each other through dedicated directional wireless infrastructure. Each of these pillars connects with *nodes* within its region, where local administrators provide service (as well as technical support) to users in their immediate neighborhoods via WiFi or Ethernet links. An individual node may connect up to around 200 users, while a pillar may connect tens of regional nodes.

The pillars correspond to the hubs of the smaller networks that have interconnected to form the SNET. Each has a distinctive name, sometime reflecting geography (e.g., Havana-Este) or the SNET's origin in gamer networks (e.g., Republic of Gamers). The pillars' regions sometimes overlap, but together they cover a significant portion of the Havana metropolitan area [12], as shown in Figure 1.

Although the SNET is not officially sanctioned or regulated, the administrator community enforces its own self-imposed rules regarding acceptable use [16]. Appendix A lists prohibited activities, which include bridging the network to the Internet, discussing politics, promoting commercial interests, and distributing pornography. This self-regulation reflects that the SNET community wishes to avoid being seen by authorities as competing with sanctioned services, or as a threat to the social order [12].

The SNET's large scale and isolation from the Internet set it apart from other grassroots networks. Germany's Freifunk [11] is larger, but is connected to the Internet. Most other community wireless deployments, such as those in India [21] and Africa [1], are smaller and organized primarily to extend access to external information, rather than to host community-operated services. Also unlike these other services, the SNET is unsanctioned, which creates additional operational risks and uncertainty regarding its future.

1.2 Research Ethics

This study was performed collaboratively by U.S.-based academics and multiple SNET administrators and community members in Cuba, some of whom have chosen not to be publicly listed as authors. We have discussed the risk that increased international attention might lead to crackdowns against the network and its operators. However, we are in consensus that publication of rigorous technical measurements and documentation helps move the SNET towards legitimacy. It will increase awareness of the SNET and its challenges within the broader technical community, and it will increase the number of people who will understand what has happened if regulations harmful to the network are imposed.

We consider the risk of consequent disruption to be low, because, although the SNET is not officially sanctioned, Cuban authorities are aware of its existence [12] and have not taken systematic steps to disrupt it. Furthermore, multiple SNET community members have already publicly discussed the SNET or demonstrated it for the technical press without apparent negative consequences (e.g., [4, 17, 20, 23]). In order to minimize the potential for this work to be used to directly locate or disrupt SNET operations, we have omitted locations of nodes and a few other sensitive details.

2 CHARACTERIZING THE SNET

We performed a series of measurements in April and May 2017 in order to characterize the SNET's connectivity, the available services and content, and the network's user base. We present these measurement results in the three subsections below, and we discuss the implications in Section 3.

2.1 Connectivity

Interpillar wireless links show a preference for Ubiquiti Networks directional WiFi devices [22], based on the observed "AirOS" configuration pages. These devices cost around $200 and are widely available on Revolico, a Cuba-focused Craigslist-style site [19]. Many routers are MicroTik devices [13]. These boxes handle routing at the node level, manage an OSPF routing topology, and perform DHCP

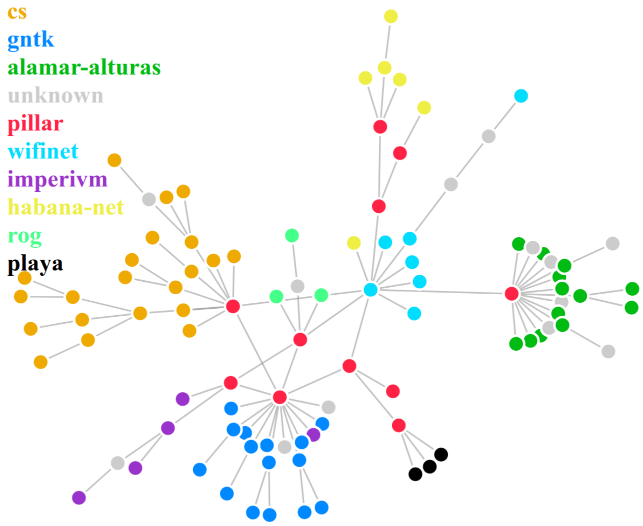


Figure 2: *The SNET's network topology, as measured from a single node*—Each dot represents a distinct subnet. Interconnected *backbone pillars* (red dots) support one or multiple levels of edge-facing *downstream nodes.*

for local clients of the node. Servers are typically desktop or laptop machines purchased by individuals. During our measurements, two subnetworks were inaccessible from our vantage point, a level of instability that we were told was not unusual.

2.1.1 Routing Topology. We mapped the network topology by using `mtr` [14], a tool similar to `traceroute`. For each of 204 /24 subnets in which we observed a responsive host, we performed an `mtr` query to a single address in the subnet. This resulted in 204 paths from our measurement point, with router IP addresses along the way. These paths reveal 97 unique router IPs, including pillars, nodes, and other end-user routers. We note that this measurement represents a conservative lower-bound on the network topology: we only probed a subset of the address space, and only from a single vantage point at one node. Routers that are not on the paths we measured, as well as routers or links that were not online at the time, do not appear. Hosts behind NAT or other middlebox firewalls will not be revealed by this type of mapping.

Despite these limitations, our measurements illuminate the general structure of the SNET. Figure 2 shows the topology we inferred. Nodes are colored by the pillar they belong to based on IP address, following a mapping we inferred from the dataset and DNS nameservers. The core pillar connections we show here are equivalent to the graphical depictions of the SNET created by node operators.

While we probed from a single vantage point, we nonetheless discovered multiple paths being utilized between some pairs of nodes. For example, the GNTK pillar and nodes were seen in three distinct paths through the pillars of the Republic of Gamers (ROG), ComunidadSur (CS), and Playa. This was not due to load balancing across wireless links, but rather temporal variation and division of the address space routing announcements. This reveals the interconnected structure of the SNET at the pillar level, a fact corroborated by the network administrators' assertion that each pillar is connected to at least two others.

Our measurements also uncovered several routing loops: out of the 204 paths, 6 of them contained the same IP address multiple times in non-adjacent hops. In all but one case, the loop existed between a pillar IP address (10.254.0.0/16) and the immediate next hop router. This type of loop is likely due to differing static routing tables in the pillar and the next router, causing both routers to believe it is the responsibility of the other to deliver packets to the probed destination. This is a symptom of the limits of OSPF routing and of manual coordination between pillars, and we expect the problem to get worse as the network's size and complexity grow.

2.1.2 Addressing. The SNET uses addresses entirely within the RFC 1918 allocations [18]. Each of the pillars occupies a distinct /16 within this space; for instance HabanaNet uses the 10.18.0.0/16 space for nodes and services. Individual nodes typically occupy /24 subnets with each /16. The pillars are interconnected in the 10.254.0.0/16 space. This structure is illustrated in Figure 3.

In addition to 10.0.0.0/8, several services occupy the address range 192.168.0.0/16, including services in the GNTK and Alamar Alturas pillars. We also observed many routers and other node infrastructure in the 172.16.0.0/12 address space. These addresses correspond with each pillar's /16 address range. For example, HabanaNet, which uses 10.18.0.0/16 for edge hosts, also uses 172.18.0.0/16 for node routers. We did not find any services running on the 172.16.0.0/12 address range, though our scans of HTTP and TLS services revealed several AirOS and Mikrotik devices.

In practice, many SNET services are accessed by their IP addresses directly, although the network operators have recently deployed an internal DNS infrastructure (see Section 2.2.2).

2.1.3 Bandwidth. We measured the traffic passing through core routers at two of the SNET pillars, ROG and GNTK. The average utilized bandwidth over a 24-hour period was 120 Mb/s, with a maximum throughput of 250 Mb/s. Throughput is generally constrained by the available bandwidth of the long-distance WiFi links between pillars. In order for a node to be connected to an SNET pillar, the

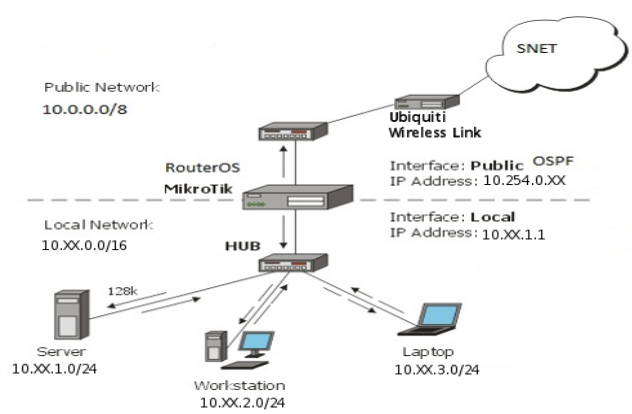
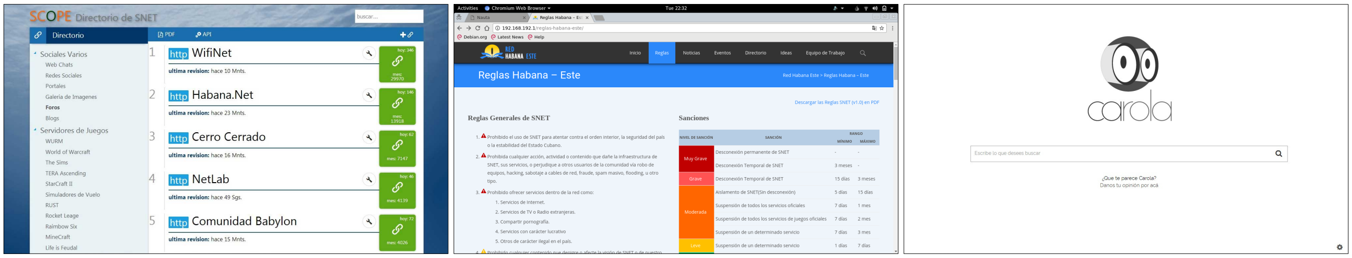


Figure 3: *Structure and addressing of a typical SNET pillar*—Multiple nodes, each consisting of a /24 subnet, connect to the pillar, which interconnects to one or more other pillars.



(a) Scope Portal (b) SNET Rules (c) Carola Search Engine

Figure 4: *Examples of SNET sites*—The SNET hosts hundreds of websites, including: (*a*) Scope, a categorized directory of other SNET sites; (*b*) A Rules page, with color-coded penalties for infractions; and (*c*) Carola, a search engine developed by Netlab.

administrators typically require a minimum bandwidth of 20 Mb/s between the node and its pillar. This constrains the topology such that it is not simply a star from a small number of well connected pillars, but instead extends outwards over multiple interpillar hops.

In order to use this limited bandwidth efficiently, pillar operators restrict bulk file-transfer applications during peak hours. Bandwidth intensive transfers, like FTP servers hosting *El Paquete*, are only allowed from 3 A.M. until noon. This allows lower-bandwidth applications, such as social networking and chat services, to function more responsively throughout the day. For the most part, the policy is enforced through coordination between individual server operators and the network administrators. During our tests outside of the allowed time window, downloading from certain FTP servers appeared to be capped by the server at 1 KB/s. We are not aware of QoS or similar prioritization techniques being employed on routers or other network infrastructure.

2.2 Sites and Services

One of the most impressive aspects of the SNET is the amount of effort that has gone into the creation and operation of the hundreds of services and websites found on the network. In Figure 4, we show a small sample of SNET sites. There are an array of thriving chat rooms, forums, and information resources. *El Paquete*, the weekly distribution of TV shows and media content that propagates around Cuba [3], can be found on the network, as can snapshots of Wikipedia and a range of Coursera courses. There are weekly streaming radio broadcasts, and a continued focus on gaming.

Category	Sites	DNS Name	Active
Gaming	73	30%	54%
Social Networking	68	40%	71%
Internet Mirror	37	14%	43%
Technology	27	41%	88%
FTP Servers	23	17%	52%
Commerce	23	39%	90%
Other	45	44%	90%

Table 1: *SNET sites by category*—We show the number of sites listed under various categories by the SNET pillar portals. We also show the fraction of the sites that were linked to using a DNS name instead of an IP address, and the fraction that were available when we attempted to visit them.

2.2.1 Content. In Table 1, we show the primary categories of services present on the SNET. Most pillars run a "portal" or "homepage" for their users that contains a directory of available services. Categorization was in rough agreement among the different pillar portals, with a focus on gaming and communication services. The top-level categories are relatively broad; for instance the "Social Networking" category contains web chat, forums, social networks, and blogs. We found that between 50% and 90% of listed servers were responsive when we attempted to connect.

We crawled the responsive pages via recursive `wget` and analyzed the resulting HTML to measure the prevalence of various features. Table 2 shows that PHP is a dominant server language within these sites, and jQuery is a ubiquitous client-side framework. Interestingly, around half of the services we crawled had an explicit "rules" page, highlighting the community's emphasis on good conduct. We also note the high rate of site-specific registration forms, which is a product of the network's lack of identity providers.

To understand how comprehensive the pillar portal directories are, we compare them to the set of hosts revealed by using `zmap` [7] and `nmap` [15] to comprehensively scan the SNET's address space. Table 3 shows the number of listening IP addresses for three common ports. These IPs include many hosts that are not listed in the directories, although the majority of these are routers or end-user computers, rather than services meant for general SNET users.

2.2.2 DNS. SNET operators have recently deployed DNS servers to translate SNET-specific hostnames into IP addresses. Each pillar appears to maintain its own authoritative root DNS server, with authority connected to each of the other pillars' root servers. All domains use the `.snet` suffix, with a pillar-specific name serving as the second-level domain. For example, `wow.rog.snet` is a gaming service that operates in the `rog.snet` pillar.

We were able to enumerate the zones in the SNET DNS. With access to the `habana.snet` root server, we issued `AXFR` zone transfer queries to each of eight other pillars. This returned a total of 147 domain names under the `.snet` root. Two pillar root servers were configured not to allow `AXFR` at the time of our queries.

Many records have associated `RRSIG` and `DNSKEY` records, indicating server support for DNSSEC. However, we see no evidence of client support, or of the root keys being widely distributed. It is likely a default feature of the DNS server implementations.

We also performed a port scan for DNS servers across the active SNET address prefixes, and discovered 46 responding resolvers

Technology or Feature	Fraction of Sites
jQuery	78%
PHP	39%
WordPress	32%
Registration Form	81%
Rules Page	50%
Teamspeak Contact	22%

Table 2: *Site characteristics*—Fractions of SNET sites displaying commonly observed technologies and features. Registration with each service remains a major usability hurdle.

Service	Responsive Hosts
tcp/80 (HTTP)	2,986
tcp/21 (FTP)	2,052
udp/53 (DNS)	48

Table 3: *Popular ports*—Number of SNET IPs serving on three common ports. Scanning revealed many active hosts, including routers, not listed in the SNET site directories.

Link Destination	Fraction of Sites
Any off-network site	81%
GitHub	51%
Facebook	32%
Twitter	32%
WordPress	23%

Table 4: *External links*—Most SNET sites contain (broken) hyperlinks to Internet resources. We show the fraction of crawled sites that linked to several popular external sites.

spread across the address space. Most of these did not appear to respond to queries for domains in the `.snet` zone, either indicating disconnection from the root or a separate DNS root. We queried these hosts with a `version.bind` TXT query and received responses from 10 of them. The results are remarkably heterogeneous: version strings included several versions of `dnsmasq`, multiple versions of `bind` running on Debian, and a single Microsoft DNS server. The versions corresponded with software releases from 8 years out of date to as recent as 1 year prior to our scan.

2.2.3 External Connectivity. Many SNET sites consist of mirrors of content copied from the Internet, or are interactive services based on open-source software that expects to be run from Internet-connected servers. As expected, these pages frequently contain broken links to Internet content. However, we also observed the presence of links to off-SNET content in user postings and forums. This suggests that, while the SNET itself is not bridged to the Internet, many of its users have at least intermittent Internet access, such as while visiting ETECSA WiFi hotspots.

To measure this, we revisit the services from Table 2 to look for links to and presence of the community on the external Internet. As shown in Table 4, 81% of the sites in our sample linked to off-SNET content, with GitHub and social networks being common destinations. Many sites contain attribution links to the tools used in their development (such as WordPress). The most common external domain linked by absolute volume of links was `revolico.com`, due to a small number of sites mirroring its content. By comparison, 54% of observed sites had links to a `.snet` domain, though far more referenced other SNET sites by their IP addresses directly.

2.3 Users and Usage

The SNET appears to have a large and diverse user base, but measuring this population is challenging. Identities on the SNET appear to be largely pseudonymous. For instance, one popular service lists its points of contact as "Counter", "°oOo°oOo°", and "Ripper". There is no central user-identify provider on the SNET, and not even an active email system. (This may be to avoid the appearance of competing with the ETECSA email system, which is widely available on mobile phones despite the lack of mobile Internet service [9].) This means that account registration and identity across the network does not support either email verification or any form of automated account recovery. For the purposes of our study, it also makes correlating user identities across SNET sites very difficult.

As a lower bound on the size of SNET's user base, we consider the WifiNet forums, a general community messaging board hosted by one of the pillars, which is thought to be one of the network's most popular sites. The forums have 56,000 registered users. At the time of our observations, which were during an off-peak hour, more than 500 forum users were active. In this community, the self-reported gender distribution was 30% female and 70% male.

For a point of comparison to this general demographic, we surveyed the active "seeking work" listings on the largest SNET service for classified advertisements, Timbirichi. There were 66 active posts in the category. Nine of the job-seekers identified as male, and 14 identified as female.

2.3.1 Case Study: The Netlab Open-source Community. In order to illustrate the vibrancy of activity on the SNET, we focus on one particular subcommunity, a suite of service branded "Netlab". This emergent community has existed since 2014, but has entered a phase of rapid growth in the last year (see Figure 5).

Netlab focuses on open-source development, and runs a forum, GitLab instance, and mirrors of NPM and PHP package repositories. The Netlab forum has more than 6000 registered users who had made 81,000 posts at the time of measurement. Roughly 1100 of the users had logged in within the previous month.

In Figure 6, we show the average hourly activity of the Netlab forum over a 24-hour period, as observed from analytics captured by the hosting web server. The site was most active between about 9 A.M. and 1 A.M., with a peak at 11 P.M.

The Netlab community is an example of a secondary subcommunity creating a thriving space within the larger network. It has a been involved in a number of SNET firsts. For instance, Netlab users developed Carola (Figure 4c), the first custom search engine for the SNET. The community is also one of the successful examples of SNET crowd-funding. A general post soliciting help to purchase additional storage space resulted in contributions from users with whom the Netlab administrators had not personally interacted.

Some Netlab forum posts contain detailed original technical guides on subjects where users have unusual expertise, including

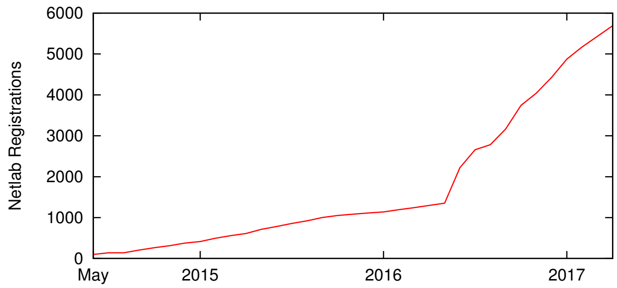


Figure 5: *Netlab growth*—Registration dates of Netlab users since its creation show accelerated growth over the past year.

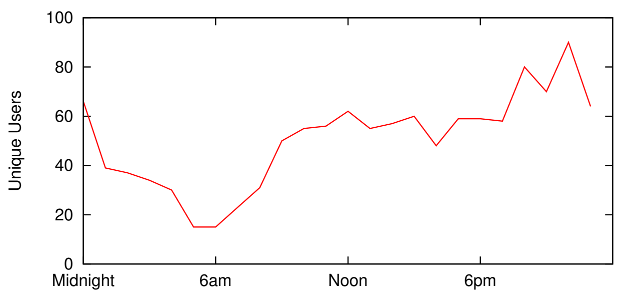


Figure 6: *Netlab usage*—Unique active visitors per hour on the Netlab forum over a 24-hour period in April 2017. Usage peaks in the evening, as expected in a residential network.

Android device repair. This has led to nascent conversations within the Netlab community about establishing mechanisms for *exporting* knowledge from the SNET to the broader Internet community.

3 DISCUSSION AND CHALLENGES

The SNET has never been a stable environment, and has faced rapid growth, insufficient infrastructure, sporadic local crackdowns by the authorities, and interpersonal conflicts among operators. Moreover, most of the network's volunteer administrators have little or no training in networking or security. This context is essential for understanding the challenges and opportunities facing the network.

3.1 Infrastructure

There are three infrastructural challenges operators agreed constrain the SNET today physically: spectrum availability, theft, and cost. All of the wireless links operate in a noisy 5GHz band, since most of the RF spectrum is not licensed for consumer use in Cuba. This restriction limits the reliability of links, since other devices in the same band introduce noise. Operators have reported theft of devices, especially antennas and radios placed on roofs. Many operators run links from their apartment windows, or enclose devices outside within electrified housings to deter theft. Finally, as a distributed network run entirely by individuals, operators are limited in the types of equipment they can afford. These challenges may constrain the network's ability to add nodes and scale backbone bandwidth, since the community has no easy ways either to raise funds or to acquire higher bandwidth radio equipment.

3.2 Organization

Like that of the Internet, the distributed organization of the SNET has evolved with the network. Today, the network is large enough that many separate subcommunities exist in parallel, with different visions and uses of the technology. These varied and sometimes conflicting motivations have made coordinated changes difficult, and they partially explain why improvements such as DHCP and DNS have been inconsistently and slowly rolled out.

While such difficulties exist, they are a consequence of the community's continued preference for distribution. Distributed infrastructure and decision making are critical to preserving the SNET's resilience. They ensure that the network will continue to exist even if parts of it becoming unavailable, whether due to hardware failures, crackdowns, or volunteer operators losing interest.

Coordination on the SNET today occurs through three mechanisms we were able to observe. The first is through direct personal relationships. The second is through the TeamSpeak chat system running on many of the SNET servers, which includes channels for node operators within a pillar and for coordinating issues between pillars. The third is a forum for SNET issues where less transient discussion and coordination of longer-term issues occurs. This forum has just over 100 registered users and more than 6000 messages.

3.3 Security

Security on the SNET is extremely poor compared to the Internet, but, due to the network's small size and tight-knit community, there are relatively few reports of problems being exploited to harm users.

The network lacks most of the security infrastructure on which the modern Internet depends. There are only a very limited number of services offered over HTTPS, and, since there is no SNET CA, the certificates are all self-signed. Furthermore, the legal status of encrypted communication in Cuba is unclear [5], so many SNET administrators are hesitant to adopt TLS-protected services.

With no account recovery system for most services, forgetting a password can result in a lost account, and poor password practices are thought to be common. Limited Internet connectivity has led to epidemic use of unpatched software with exploitable vulnerabilities, including in core infrastructure such as routers and DNS servers.

We heard anecdotal reports of such vulnerabilities being exploited to nefariously gain backdoor access to servers. Rather than turn to the authorities, the community self-polices such infractions, as with other rule violations. When perpetrators can be identified, they are subjected to social bans or disconnection of service.

4 CONCLUSION

Even in the face of significant challenges, the SNET is thriving. It provides a vibrant set of online communities, information, and interactive services to the residents of Havana, most of whom have little or no access to the Internet. In partnership with SNET community members, we conducted the first systematic characterization of the network's infrastructure, available services, and user base.

We hope this study will contribute to a wider understanding not only of the SNET community's needs but also of its remarkable accomplishments. While the SNET's ultimate fate remains unclear, it continues to evolve with surprising rapidity, and we are cautiously optimistic about its future.

ACKNOWLEDGMENTS

We are grateful to the anonymous SNET community members who collaborated in this work, without whom the study would not have been possible. We also thank David Robinson for many insightful discussions.

REFERENCES

[1] Backens, J., Mweemba, G., and Van Stam, G. A rural implementation of a 52 node mixed wireless mesh network in Macha, Zambia. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (2009).
[2] Bischof, Z. S., Rula, J. P., and Bustamante, F. E. In and out of Cuba: Characterizing Cuba's connectivity. In *Proc. 15th ACM Internet Measurement Conference (IMC)* (2015).
[3] Concepción, J. R. La cultura empaquetada: Análisis de la distribución y el consumo audiovisual informal del Paquete Semanal por jóvenes de La Habana. B.S. thesis, University of Havana, 2017. In Spanish. http://www.academia.edu/31051650.
[4] Crecente, B. Inside Cuba's secretive underground gamer network. Polygon, May 15, 2017. https://www.polygon.com/features/2017/5/15/15625950/cuba-secret-gaming-network.
[5] Cuban Ministry of the Interior. Que pone en vigor los reglamentos para la criptografia y el servicio cifrado en el territorio nacional y para el servicio central cifrado en el exterior, 2002. In Spanish. http://www.fcmjtrigo.sld.cu/resoluciones/resol2_1999.pdf.
[6] Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., Weaver, N., Adrian, D., Paxson, V., Bailey, M., and Halderman, J. A. The matter of Heartbleed. In *Proc. 15th ACM Internet Measurement Conference (IMC)* (2014).
[7] Durumeric, Z., Wustrow, E., and Halderman, J. A. ZMap: Fast Internet-wide scanning and its security applications. In *Proc. 22nd USENIX Security Symposium* (2013).
[8] ETECSA. Acceso público a Internet. In Spanish. http://www.etecsa.cu/internet_conectividad/internet/.
[9] ETECSA. Espacios públicos de conexión inalámbrica (WIFI). In Spanish. http://www.etecsa.cu/internet_conectividad/areas_wifi/.
[10] International Telecommunication Union. ICT development index 2016. https://www.itu.int/net4/ITU-D/idi/2016/.
[11] Johnson, D., Matthee, K., Sokoya, D., Mboweni, L., Makan, A., and Kotze, H. Building a rural wireless mesh network. Meraka Institute. African Advanced Institute for Information & Communications Technology, 2007.
[12] Larry press. Might Cuba's street net, SNET, become legitimate? The Internet in Cuba blog, Mar. 3, 2016. http://laredcubana.blogspot.com/2016/03/might-cubas-street-net-snet-become.html.
[13] MikroTik routers and wireless product listing. https://mikrotik.com/product/RBSXT5nDr2.
[14] MTR. http://www.bitwizard.nl/mtr/.
[15] Nmap: the network mapper. https://nmap.org/.
[16] Reglas generales y código de sanciones de SNet, Sept. 2016. In Spanish. Available at http://www.cubadebate.cu/wp-content/uploads/2016/09/Reglas-Generales-y-C%C3%B3digo-de-Sanciones-de-SNet.pdf.
[17] Reinaldo, O. F., and Domínguez, L. E. SNet: La primera comunidad inalámbrica en Cuba, Sept. 16, 2016. Available at http://www.cubadebate.cu/noticias/2016/09/16/snet-la-primera-comunidad-inalambrica-en-cuba-fotos-infografia-y-pdf.
[18] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and Lear, E. Address Allocation for Private Internets. RFC 1918, 1996.
[19] Revolico: Anuncios clasificados en Cuba. In Spanish. https://www.revolico.com/.
[20] Rodríguez, E. D. The state of news in Cuba. Nieman Reports, Sept. 26, 2014. http://niemanreports.org/articles/the-state-of-news-in-cuba/.
[21] Surana, S., Patra, R. K., Nedevschi, S., Ramos, M., Subramanian, L., Ben-David, Y., and Brewer, E. A. Beyond pilots: Keeping rural wireless networks alive. In *Proc. 5th USENIX Symposium on Networked Systems Design and Implementation (NSDI)* (2008).
[22] Ubiquiti Networks NanoStation. https://www.ubnt.com/airmax/nanostationm/.
[23] Weissenstein, M. Cuban youth built a secret internet network. Associated Press, Jan. 26, 2015. Available at http://www.businessinsider.com/cuban-youth-built-a-secret-internet-network-2015-1.
[24] Xynou, M., Filastò, A., and Basso, S. Measuring Internet censorship in Cuba's ParkNets, 2017. https://ooni.torproject.org/post/cuba-internet-censorship-2017/.

A APPENDIX: SNET RULES

SNET rules are largely consistent across communities, as they are drafted through a process of consensus among the groups of operators. This translation shows one community's rules and penalties:

- *Minimum 3 month disconnection:* Use should not violate the internal order, the security of the country, or the stability of the Cuban State.
- *Minimum 3 month disconnection:* Activity or content that damages the SNET infrastructure, its services, or harms other users of the community, such as hacking, mass spam, flooding, or fraud.
- *Minimum 3 month disconnection:* Running services within the network for external Internet, foreign TV or radio, pornography, self profit, or illegal activity.
- *Minimum 3 month disconnection:* Promotion or commerce of illegal drugs.
- *Minimum 7 day suspension:* Ignorance of the rules does not relieve responsibility.
- *Minimum 7 day suspension:* Promotion or commercialization of SNET off-network.
- *1–7 day suspension:* Posting content that is discriminatory, or which contains extremist ideology.
- *Individually handled:* Engaging in political or religious debate.