Recommendations for Wi-Fi setup at big training events

This document is not meant to replace or serve as a technical manual of any kind, but contains merely views expressed based on experiences of support staff to assist in more effective planning for future events.

This guide and recommendations are based on the joint experiences of HISP-SA and Wirelexx support staff in supporting the Internet infrastructure at PEPFAR's PALS event in Johannesburg over two weeks 11-22 September, 2017.

The event hosted an estimated 250 participants each week with many hands-on Internet-intensive sessions.

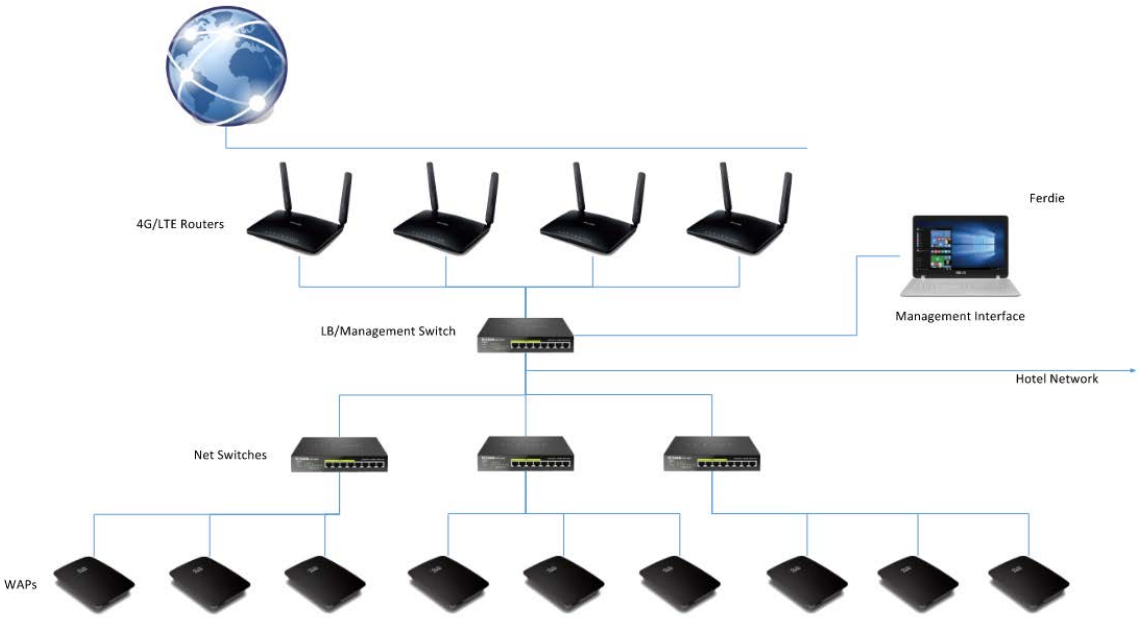
Contents

Recommendations for Wi-Fi setup at big training events 1

Overview of the equipment and network setup 2

Major Challenges Experienced 7

Key considerations for future events 8



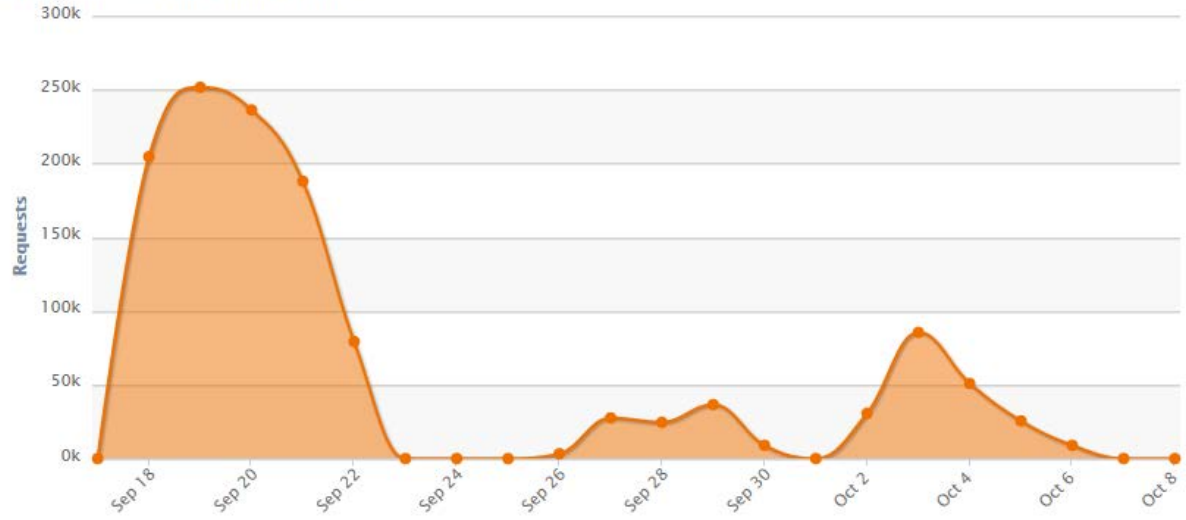
Network monitoring tools and procedures

- **OpenDNS**
  OpenDNS is a company and service that extends the Domain Name System (DNS) by adding features such as phishing protection and optional content filtering in addition to DNS lookup, if its DNS servers are used.
  The company hosts a cloud computing security product suite, Umbrella, designed to protect enterprise customers from malware, botnets, phishing, and targeted online attacks. OpenDNS assisted quite immensely with reducing unwanted traffic on the network as it blocked URLs which was not needed for the event. However at the start of the event this caused some issues due to the fact that the sites whitelisted would use other sites to extract data from, for example youtube.com would also need Akamai.com to stream videos. If youtube.com was whitelisted without Akamai.com it would not function.

  Some statistics pertaining to OpenDNS:

Total Requests for PALS

September 17, 2017, to October 8, 2017

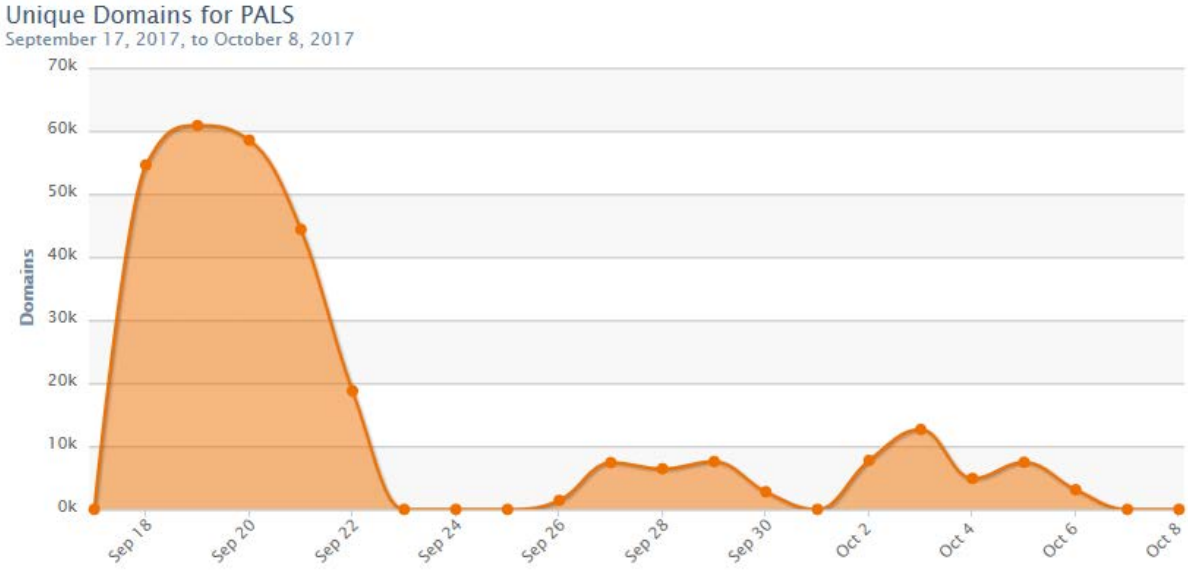


DATE	REQUESTS
Sunday 9/17	0
Monday 9/18	204,632
Tuesday 9/19	251,682
Wednesday 9/20	236,355
Thursday 9/21	188,014
Friday 9/22	79,366
Saturday 9/23	3
Sunday 9/24	2
Monday 9/25	6
Tuesday 9/26	3,292
Wednesday 9/27	27,520
Thursday 9/28	24,595
Friday 9/29	36,597
Saturday 9/30	8,988
Sunday 10/1	0
Monday 10/2	30,648
Tuesday 10/3	85,496
Wednesday 10/4	50,923
Thursday 10/5	25,469
Friday 10/6	8,983
Saturday 10/7	0
Sunday 10/8	0

Blocked Domain Requests:

RANK	DOMAIN	REASON	REQUESTS
1	api.huddle.com	File Storage	48,370
2	www.icloud.com	File Storage, ...	28,444
3	client-lb.dropbox.com	File Storage	18,660
4	bolt.dropbox.com	File Storage	18,528
5	client-cf.dropbox.com	File Storage	16,989
6	d.dropbox.com	File Storage	11,082
7	*.youtube.com	Video Sharing	8,628
8	client.dropbox.com	File Storage	8,596
9	t0.ssl.ak.dynamic.tiles.virtualearth.net	Software/Technology, ...	8,239
10	graph.instagram.com	Photo Sharing	7,801
11	init.itunes.apple.com	Music	7,374
12	t0.ssl.ak.tiles.virtualearth.net	Software/Technology, ...	5,128
13	keyvalueservice.icloud.com	File Storage, ...	3,591
14	api.accuweather.com	News/Media, ...	3,317
15	api.twitter.com	Blogs, ...	2,939
16	api.weather.com	News/Media, ...	2,938
17	cdn.onenote.net	File Storage	2,323
18	log.getdropbox.com	File Storage	2,311
19	dl-debug.dropbox.com	File Storage	2,287
20	p27-keyvalueservice.icloud.com	File Storage, ...	2,175
21	p20-btmmdns.icloud.com	File Storage, ...	2,064
22	twitter.com	Blogs, ...	1,971
23	p47-keyvalueservice.icloud.com	File Storage, ...	1,915
24	cdn1.evernote.com	File Storage, ...	1,892
25	geo-um.btrll.com	Adware, ...	1,667

Unique Domains Requests:



The impact of network containment measures is clearly visible as the event progressed.

- **Unifi Security Gateway**

  The UniFi Security Gateway extends the UniFi Enterprise System to provide cost-effective, reliable routing and advanced security for your network.

  The UniFi Controller software conducts device discovery, provisioning, and management of the UniFi Security Gateway and other UniFi devices through a single, centralized interface.

  The Unifi Security Gateway gave us the ability to do deep packet inspection ensuring unnecessary bandwidth usage is kept to a minimum.
  Sample user interface:

- **Mikrotik Graphs**

Graphing is a tool to monitor various RouterOS parameters over time and put collected data in nice graphs.

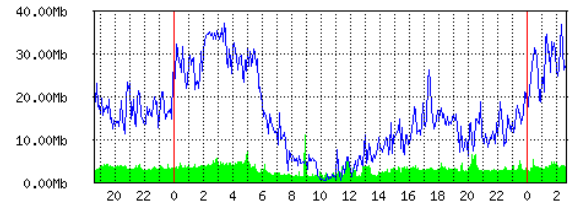
The Graphing tool can display graphics for:

- Router board health (voltage and temperature)
- Resource usage (CPU, Memory and Disk usage)
- Traffic which is passed through interfaces
- Traffic which is passed through simple queues

These graphs were extensively to monitor and ensure correct bandwidth allocation on the load balanced LTE-A modems.

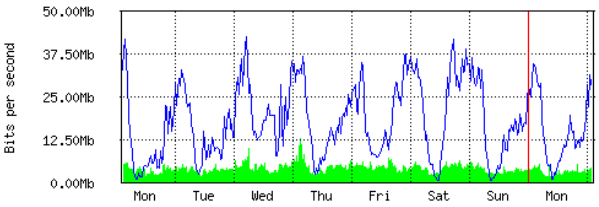
Following are some monitoring graph examples:

"Daily" Graph (5 Minute Average)



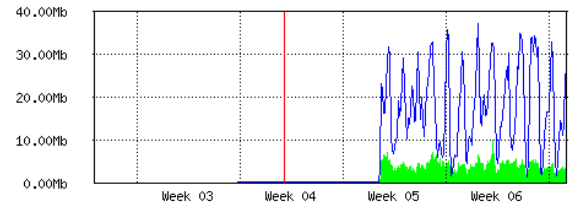
Max In: 10.89Mb; Average In: 3.04Mb; Current In: 3.39Mb;
Max Out: 37.32Mb; Average Out: 16.03Mb; Current Out: 27.14Mb;

"Weekly" Graph (30 Minute Average)



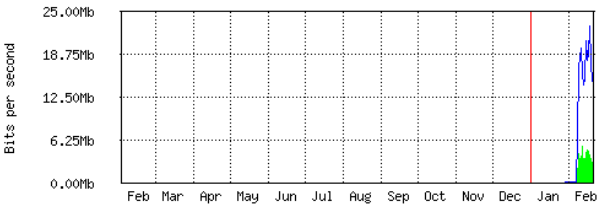
Max In: 12.53Mb; Average In: 3.80Mb; Current In: 4.03Mb;
Max Out: 42.78Mb; Average Out: 17.75Mb; Current Out: 28.62Mb;

"Monthly" Graph (2 Hour Average)



Max In: 9.82Mb; Average In: 2.23Mb; Current In: 3.31Mb;
Max Out: 37.25Mb; Average Out: 10.03Mb; Current Out: 25.39Mb;

"Yearly" Graph (1 Day Average)



Max In: 5.28Mb; Average In: 2.13Mb; Current In: 2.95Mb;
Max Out: 22.98Mb; Average Out: 9.56Mb; Current Out: 14.86Mb;

Major Challenges Experienced

In the first week we encountered a series of difficulties not relating to each other, it took quite a substantial amount of time to correct all errors. Listed below all errors encountered:

1. Kopanong Hotel's Fibre was patched into our router for failover/extra bandwidth, the configuration of the Hotel's network was not on standard and a substantial amount of errors was found on the network as soon as we combined the 2 networks, our biggest challenge was duplicate IPs on multiple routers on Kopanong's network. This caused the fibre to drop intermittently, the router in the hotel was replaced and all Layer 3 communication was moved to one router instead of 3.

2. There was a printer connected to our wireless network through a small SOHO Router that acted as a "wireless bridge", this router had a rogue DHCP Server on, as a result some clients connecting to the wireless network would receive an IP from the SOHO router instead of the core router, this had a major effect on performance for the clients connecting to this router as the wireless connection to it was only for printing and not the data intensive sessions clients was attempting. This error was only picked up once we had an engineer on site during the sessions.

3. Load-balancing on access points: Specifications on the access points stated that a maximum of 256 clients is allowed per access point, in practice this was not the case. Where more than one AP was placed in a big hall, all clients would connect to the same AP with a result that its CPU usage runs very high and the AP adjacent to it would have no load at all, this was solved by reducing the number of clients allowed to each access point immensely, in some cases as little as 30 clients per AP, this together with correct frequencies made the big difference in the start of week 2.

4. At the start of the event only 4 of the Access Points had wired connections with the other 4 forming a wireless mesh. Wireless connections lose 50% bandwidth on each hop, in theory this would not have made a difference as the access points has wireless capability of up to 1167Mbps. However it was different with this event as the hotel itself had more than 70 SSID's causing interference on all frequencies. The only way to eliminate this problem was to cable all the AP's, which was done during the first week.

Key considerations for future events

1. Assume high wireless interference and do not rely on wireless mesh topologies.
2. Where possible, do not bridge 2 networks to provide more backbone or redundancy
3. Reduce internet bandwidth usage to the absolute minimum (critically required) during "event hours"
    a. Implement a local server with all large data files (or even local "training" instances of the application if possible at all - this will drastically improve available internet bandwidth and response times to user devices as local traffic between a local such server and users is transferred at much higher rates.
    b. The fact that 250 users had to stream video and other very data intensive content from international URLs put a lot of strain on the whole network which could have been eliminated by placing a local server from the start.
    c. Do not assume that all activities use the same amount of bandwidth – some application processes such as multiple generations of the same report at the same time not only have a huge bandwidth impact, but may even drastically reduce the application and database servers' response times.
4. Do not allow any devices to download updates un-related to the session topic – it is not only impacting on other parallel sessions' internet response times, but also lead to attendees' distraction and overall negatively impact the success of a session. Instead, make a separate space/disjointed network available for personal use, served by separately purposed access points and devices. If possible, a separate physical or Virtual Private network should be established for such purposes.
5. It is critical to blacklist sites that are not necessary for the purpose of the event for the same reasons as described above. If available, users will use it. A blacklisting time-schedule (active/de-active status) will also help to allow users to still access emails during 'open' hours.
6. The option of URL white-listing is also attractive, but proved to be immensely admin-intensive and is virtually impossible to be effective in case of a heterogenic attendee group of users.
7. Ensure load-balancing is done on both backhauls and access points, this is critical to ensure performance.
8. Use network access points and communication devices with a minimum of 802.11ac compliancy to ensure maximum performance on the wireless network
9. Get a location layout-map of the building(s) where sessions/network access needs to be provisioned. Set-up a network frequency and device density hotspot map is done to optimise access point coverage of the user areas. Review and optimise placement as reality and planning starts to meet up.
10. Users congregate to collaborate, and they will do that wherever they feel comfortable, not where you have put your access points. They also have multiple devices. (An estimated 2.5 devices (connections) per user were statistically observed at one stage during the event). This means that for 250 users, 650 active connections were requesting its own chunk of bandwidth usage. Such device density lead to airtime contention, meaning that devices had to compete for access to the available network – and eventually requiring much more than the available bandwidth – which caused devices to be unable to gain access – which subsequently caused the perception that the network is unstable.
11. It is always an option to increase bandwidth (as we did nearing the end of week one) – and always at a premium! The analogy of a water-pipe within which flow-limiting

connections are moved around comes to mind. The slowest/smallest connection will determine the maximum throughput – regardless of the input and/or output capacity and the endpoints.

12. Ensure availability of high-quality tools for the job – including network wiring and testing tools. If possible, cable diagnostic tools may add to enhanced service delivery, especially in cases where large networks needs optimal maintenance, on-the-fly fault detection etc.
13. If enough budget is available, fail-over devices, backup power supplies and UPS devices may assist in maintaining device stability. Network devices are sensitive to electricity voltage fluctuations and may even cause ‘intermittent’ disruptions of connectivity.
14. For high-level events, an on-site network engineer proved to be a valuable addition to the “back-office team” – especially during initial set-up and high-use timeslots. Remote assistance is valuable and less costly, but also has its limitations when communication breakdowns are to be diagnosed.