Plan Ceibal: A countrywide OLPC deployment in Uruguay

Introduction: The Plan Ceibal Project
Plan Ceibal is the name the OLPC (One Laptop Per Child http://laptop.org/) Project took in Uruguay. The project is managed by the ANII (Uruguayan Innovation and Investigation National Agency) through the LATU (Uruguayan Technology Laboratory). The Project’s bold objectives constitute the full extent of the OLPC vision, that is, One Laptop Per Child, plus free Internet connection to every child. To reach these objectives software and a countrywide network infrastructure had to be developed and tuned up to accommodate the ever-growing requirements.

Uruguay has 19 political divisions called departments. There is only one big metropolitan area, where half the population lives, called Montevideo, which has 1.500.000 inhabitants distributed throughout a wide 250 square kilometre area. The rest of the country is mainly made up from rural areas plus approximately 20 small cities, of around 40.000 inhabitants each, adding up to another 1.500.000 inhabitants.

There are around 300.000 elementary public school students, and every rural school, which account for 50% of total schools, gathers around 20 children in a 10km radius area; some of these come to school on horseback. So the rural students, who sum up to the 20% of the Uruguayan children are scattered throughout 90% of the territory.

Ceibal’s Goals
The project goals were divided into 2 phases:
Phase 1:
- 80% of the children who live in urban areas must have wireless Internet access somewhere within a 50-meter range from their home.
- Free Internet access must be provided for the children in every school and every public square.
- Every child must have an XO notebook.

Phase 2:
- In addition to Phase 1, at least 80% of the children who live in urban areas must have wireless Internet access somewhere in their home.
Main Challenges

- Provide Internet access to each of the 2.356 public elementary schools scattered throughout the country, some of these in places where there is neither electricity nor tap water.
- Provide Internet access to every child’s home in Montevideo. This is no easy feat as Montevideo is a low density, large metropolitan area.
- Provide Internet access to every block in small to medium size urban areas, which are filled with trees and some metallic roof houses.

The project started in March 2007 with 150 XO notebooks delivered in a small rural area elementary school in the town of Cardal (Florida), Uruguay.

Design: The network and Software

The original design goals were to have a standards-compliant, isolated and safe network for the kids.

The project required some sort of network to allow the kids to both share XO activities, and access the Internet. The network would be comprised of hundreds of APs spread across the country to ensure coverage in both rural schools and towns.

Zones

The main design definition was a zone, which was essentially a Wi-Fi broadcast domain with at least an Internet uplink. Zone complexity could range from a single AP and a single Internet uplink, to several interconnected APs, some bridged point-to-point links (PtoP) and several Internet uplinks. The complexity of each zone was determined by number of clients (XOs), geographical considerations and uplink availability.
Both electricity and connectivity were unreliable in some rural areas, where electrical spikes due to thunderstorms were not unusual. That meant, it was desirable that a zone be resilient to Internet uplink failures, and, if possible, even to electrical failures. These conditions prompted a design that could, with minimal cost, tolerate the most common failures.

**Internet uplinks**

Internet uplinks were hosted at schools, which were the only common place on every zone. Each of these uplinks required web filtering, to prevent inappropriate content to be delivered to children. Some schools, especially rural ones, lack DSL connectivity; some don’t even have electricity. A number of possible uplink alternatives were used, according to the following, in order of preference:

- **ADSL (3m/256k):** An ordinary ADSL link, mainly available at urban areas like cities, and most towns, although rural areas generally lack this possibility.
- **3G (400k/400k):** An outdoor radio base, usually used in rural areas where there are no ADSLs. Converts 3G to Wi-Fi, turning the rural school into a Wi-Fi hotspot. In addition, this radio base can operate without a regular power supply, as it also runs on solar power.
• Point-to-Point link: A wireless Point-to-Point link is setup from the nearest ADSL available town or city, to nearby rural areas with neither ADSL nor 3G infrastructures.

• GPRS (100k/100k): A solar powered outdoors GPRS to Wi-Fi converter is usually installed for remote rural locations without 3G connectivity, which are too far away for the Point-to-Point to be considered.

• Satellite (512k/512k): A satellite link is installed for remote rural locations where there is not even GPRS connectivity. As this is the most expensive alternative, it is used as a last resort.

Addressing
To simplify deployment and maintenance, all zones share the same private network, but each server has a small subset of that network. This allows easy setup and replacement of servers, tolerates unexpected zone merging, and avoids routing, which is not supported by some low end APs. A single DHCP server, chosen dynamically among the servers present in the zone, assigns and balances IPs for the whole zone. If that server were to fail, another server would take over that role.

Access Control
Access control and security were also one of the main concerns. As small kids would use the network, it was important that only XOs and authorized computers could get into the network. Also, for regulatory reasons, the design should prevent 3rd parties using the infrastructure as a transport network.

The design took advantage of servers that would have to be deployed for other purposes to implement authorization and authentication. It was preferred to have a decentralized authentication and authorization, both to avoid bottlenecks, and loss of network connectivity on the event of a link failure.
<table>
<thead>
<tr>
<th>Implementation</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunneling</td>
<td>- Simple to deploy</td>
<td>- Encapsulation overhead</td>
</tr>
<tr>
<td></td>
<td>- Works thru NAT (Layer &gt;= 4 tunnel), portals</td>
<td>- Central point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Single Point of Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Scalability of terminator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Traffic between hosts must go thru central point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- No access control at Layer 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Spoofing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Snooping</td>
</tr>
<tr>
<td>Proxy Authentication</td>
<td>- Simple to deploy</td>
<td>- Works for some protocols/applications only</td>
</tr>
<tr>
<td></td>
<td>- Central point already present</td>
<td>- Central point</td>
</tr>
<tr>
<td></td>
<td>- Works thru NAT (Layer &gt;= 4 tunnel), portals</td>
<td>- Traffic between hosts must go thru central point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- No access control at Layer 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Spoofing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Snooping</td>
</tr>
<tr>
<td>WPA/WPA2 PSK</td>
<td>- Simple to deploy</td>
<td>- Easy to compromise as PSK is on every notebook</td>
</tr>
<tr>
<td></td>
<td>- Access control at Layer 2</td>
<td>- Difficult to roll out a new PSK</td>
</tr>
<tr>
<td></td>
<td>- Natively supported by mesh</td>
<td>- Unable to de-authorize a computer without changing the PSK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WPA/WPA2 TLS</td>
<td>- X.509 certificates ensure identity of both parties</td>
<td>- Complex initial setup</td>
</tr>
<tr>
<td></td>
<td>- Access control at Layer 2</td>
<td>- Requires more sophisticated/expensive network equipment at APs</td>
</tr>
<tr>
<td></td>
<td>- Automatic key renegotiation</td>
<td>- Not natively supported by mesh</td>
</tr>
<tr>
<td></td>
<td>- Could be decentralized using CA certificates and a CRL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Could de-authorize notebooks using the CRL</td>
<td></td>
</tr>
</tbody>
</table>
WPA2 TLS with client certificates was chosen as the best option. It provides layer 2 access control, preventing unauthorized access to the network. It also provides tools to easily add custom notebooks for management or teachers. Additionally, it allows revocation and isolation of a compromised or stolen notebook.

A dynamically chosen server on the management network hosts a RADIUS server that validates access based on the issuer of the certificate, and a revocation list periodically distributed. This allows for a decentralized and redundant access control mechanism, that works even without connectivity to a central location.

**Standards Compliance**

Even though from a technical standpoint it is easier to deploy and manage a homogeneous network, it is not always practical or the most cost-effective for every scenario. A single equipment, or even vendor, is not always the best option for every location, as some may require good indoors coverage, while others require good external connectivity with multiple clients and uplinks.

For practical reasons, several integrators, each with its own vendors, were required to do the deployment in parallel, to meet the deadlines set by the political commission. As hardware availability and applicability varied, standards compliance was required to allow interoperation, and provide a common hardware/software specification to the multiple vendors that could potentially be used.

This included both a list of standards and required features for a vendor to qualify. This would, ideally, allow for no specific configuration at the AP or school server level to support the multiple APs involved. Also, a single management solution was desirable, instead of having several, vendor-specific solutions to monitor and manage each part of the network.

**The School Server design**

Each school houses a server. The goal was that a single server could keep the zone operational, even if at a degraded speed. The school server works, firstly, as a NAT firewall and web proxy with content filtering. Moreover, a provisioning server provided key renovation, and firmware upgrades to XOs. The server also implements a dynamically chosen DHCP server for address management; a dynamically chosen RADIUS server for network access control; and a DNS cache to speed up lookups for the XOs and proxy. Finally, each school server acts as a web and file server to allow local content to be stored, such as homework assignments.
Implementation and practical matters

IEEE 802.11s “the mesh”
The goal of this standard is to create an ad-hoc network defining how devices can interconnect. Since the XO comes with a built-in implementation, the first attempt was to make the better use out of this new technology, which potentially could ease the deployment of MAN networks, and therefore help fulfil one of Ceibal’s main objectives.

In theory everything looked all right, but as it usually happens, there were several practical matters encountered. Here are listed some of the 802.11g/b practical shortcomings regarding MANs and School Wi-Fi LANs, sometimes with hundreds of students:

- Wi-Fi implementations often let the user select between 11 RF channels despite of the fact that a Wi-Fi signal actually occupies five channels in the 2.4 GHz band, resulting in only three orthogonal channels: 1 (using RF Ch1 thru Ch5), 6 (using RF Ch6 thru Ch10), and 11 (using RF Ch11 thru Ch15). This means it provides a maximum of 3 non-overlapped channels, in spite of the fact of having 11 to choose from.

- In a mobile Wi-Fi network the client usually connects to the AP that offers the strongest signal. This approach sometimes leads to excessive demand on one AP and underutilization of others, resulting in degradation of overall network performance. In other words, putting several APs in a classroom may not help to balance the strain of 40 or 50 Wi-Fi clients, as all clients might all connect to a single AP.

- Wi-Fi rate control algorithms usually contain the assumption that packets sent at slow data rates are more likely to succeed than packets sent at higher data rates, although in practice sometimes this is actually not true. The node has no knowledge of whether the network degradation is due to collisions or distance, it always assumes a distance related cause, and so that is why it reduces the data rate. In a classroom environment the cause is almost never distance, sometimes it is just excessive traffic from 40+ simultaneous clients. In this situation, dropping the data rates will not only not help, but will actually worsen the problem. When manually configuring the data rate it was sometimes found that the 11Mbit rate was more likely to succeed, or had higher throughput than the 2Mbit rate.

Shortcomings found in the 802.11s XO’s implementation:
The XO comes with a single radio, and therefore it can only implement a “best effort” mesh, also known as “shared mesh”. Unlike a second or third generation mesh -called a switched mesh- that uses two or three different radios, the shared mesh provides very low performance.
In a single radio mesh node, access and mesh backhaul are collapsed onto a single radio. The total available bandwidth in the radio channel is shared between all the neighbouring nodes. Moreover, the capacity of the channel is further reduced by traffic being forwarded from node to node in the mesh, reducing the available end-to-end traffic, since in a one radio mesh the mesh node has to listen, send, and then listen again. Because bandwidth is shared amongst all nodes in the mesh, and because every link in the mesh uses additional capacity, this type of network offers much lower end-to-end transmission rates than a switched mesh, and more importantly, it degrades in capacity as nodes are added to the mesh. Even though theory predicted that 802.11s would handle up to a maximum of seven ad-hoc hops, in practice it was found out that the real limit for connectivity was around two ad-hoc hops. Furthermore, additional tests showed that the maximum usable hop count was actually one. This was true not only for the ad-hoc network piggyback clients, but for the entire Wi-Fi network, being this direct consequence of having just one radio for both access and backhaul.

Some security issues
802.11s lacks any kind of network authentication, so it is possible for anyone to connect to the backhaul and access the network, or announce a fake backhaul route and produce a DOS attack.

The search for the right Access Point (AP)
The Linksys-WRT54 AP was deployed in the first trials, which had done well in the laboratory but ultimately not so well in the real world, for example: In most rural areas the national electrical company only guaranties that the effective voltage will be anything over 190v, instead of the safe usual range between 210v and 230v; another example: Power over Ethernet did not work so well over 6 meter of cable. In addition it turned out that these APs could only handle between 10 to 12 Wi-Fi simultaneous connections, after this load they started to have problems.
So the Linksys APs would hang every 2 weeks, and Ceibal's network operators found themselves calling teachers every day to ask them to reset the routers. It quickly became clear that a more robust solution was required, as these equipments were obviously intended as family/Soho routers.
Two months later the Linksys APs were gradually replaced by MicroTik 433 and 133 APs. The MicroTik outperformed the Linksys most of the times, being much more insensitive to electrical abuse, and handling up to 40 simultaneous clients. There were also some Cisco Aironet 1240 and 1241 deployed in locations where 80+ simultaneous clients needed to be handled.
This was enough for most schools and public areas in towns and small cities, although still insufficient for some large schools. In addition, sometimes it was necessary to install PtoP Internet links between towns and small rural schools, which lacked any kind of Internet access. Here is where the Wavion WS410 came into play.
WS410 is able to provide directional antenna Point-to-Point 2.4Ghz wireless links to nearby sites and at the same time provide Wi-Fi b/g connectivity to 256 clients in a 6-block area radius. So this equipment was preferred whenever there was a medium to large school, especially when a PtoP Internet link was required by any small nearby rural school, which had neither ADSL nor 3G Internet.

**Provisioning and the logical Network**

The provisioning and management is divided in: Central management and monitoring console, school servers, and XO.

Nagios was used for the central monitoring. There are more than 5000 defined services, which comprise APs, schools servers, switches, Internet links, etc.

Currently there is little centralized network management, the system is only able to automatically update school servers and XOs using some batch procedures through SSH channels; any failing AP or server must be handled manually through a direct connection.

**The School Server implementation**

Cities, towns, rural schools, and some public zones are divided into Wi-Fi areas. Every area has at least one school server. It is possible, and recommended for redundancy, to have more than one server. In this case, only one server is promoted, using heartbeat, to be the active one.

Every server runs a Debian Linux System with several services: DHCP, DNS cache, firewall, content filtering thru DansGuardian transparent proxy, basic monitoring, and a custom provisioning daemon.

The basic monitoring just registers the number and versions of the XOs connected in the Wi-Fi area.

Provisioning daemon: Every time an XO is powered up it connects to a Wi-Fi network, obtains its configuration using the DHCP protocol, and then probes its default router for a school server. If it succeeds, the next step is to ask if there is an XO upgrade, download, verify, and install it.

Content filtering: All the school servers run a DansGuardian on top of a Squid transparent proxy. It is configured to block abusive and pornographic content. Using a transparent proxy has an important drawback, as it sometimes breaks HTTP sessions because some web pages are design to be only HTTP 1.1, but the proxy only speaks HTTP 1.0 with the client.

Firewall: The firewall mainly blocks direct DNS queries to external servers, redirects HTTP traffic to the proxy, and provides SNAT.

**The XO**

Ceibal’s XO firmware diverges slightly from OLPC’s. The main differences are: the Spanish spellchecker, some Uruguay specific activities, and the start page in the web browser. It also runs a small provisioning daemon responsible for theft control and firmware update.
Government Neutrality

An open bidding
At the beginning of Ceibal, the Uruguayan government announced an open bidding. The paper did not exclude any make of hardware or software; it mainly stated Ceibal’s objectives.
In this context, many options were considered; it was even considered the possibility of giving a desktop IBM-clone computer to every child, although it was quickly discarded as being very impractical.
Serious contenders for the hardware notebook were:
- OLPC’s XO
- Intel and Microsoft’s ClassMate
- Positivo
- Asus Eee PC

Asus was discarded because it only had around 300MB of free disk space at the time, and it had neither a collaborative nor a theft control framework. The Positivo notebook, in addition to those shortcomings, had a low-resolution, poor contrast display and short life battery.
On the other hand, the XO and the ClassMate had a theft control framework and were much affordable. Between XO and ClassMate the XO was preferred, as it is waterproof, Sugar turn out to be a very open and collaborative framework, in contrast to ClassMate’s authoritative paradigm; it has a very long battery life, it has a built-in camera, and a dual mode high-resolution display.
The next issue to consider was the Operating System and Software. It turned out that Windows XP Light was not compatible with the XO’s wireless Ethernet card, at least for the newer firmware versions of the XO. This rendered all further research irrelevant, as Wi-Fi support was mandatory, and the deadlines for elementary school deployment were almost due.
High schools, on the other hand, had a more relaxed deadline for its XO notebook deployment. They are still considering using Windows in the XO, so one of the main issues that are being currently researched are: how to extend the theft control mechanism to the Windows XP Light system, and how to overcome the Wi-Fi driver incompatibility issue.

Current and future work

Ceibal in Montevideo’s metropolitan area
There are currently more than 200,000 XO laptops deployed in 1,400 public schools around the country, each school and each public square providing free Internet access to the children and teachers. The project is currently right on schedule, although there are still 600 schools left without laptops or connectivity.
One of the project goals is to reach 300,000 XOs and free Internet connectivity in every national public School by January 1\textsuperscript{st} 2010. This will complete the first phase of the project.

To complete the second phase it is required that 80% of the children who live in urban areas have wireless Internet access somewhere in their homes. This is particularly difficult in a large and extended city as Montevideo. It would be way too expensive to install an Access Point in every corner, besides, there will no guarantee that a child living in a 10 story flat some 50 meters from the block’s corner will have free Internet access, and as it was previously noted, the built-in mesh would not be of much help to him either.

So the search for a low budget improved capillarity solution started, and currently most of this research is focused in the ADSL Ceibal sub-project.

The ADSL Ceibal

It was early noticed that if every person in Montevideo city were to share their Internet connection with his or her neighbouring children, then the Phase 2 of the project would be successfully accomplished.

There were several practical matters to this approach, although most of them could be easily overcome given the proper political aid. An affordable network appliance had to be designed and developed with the following feature-set:

- Two encrypted SSIDs, one for private use, and one for the children in the vicinity
- Tunnel encapsulation for the children’s network traffic
- Quality of Service to protect and differentiate both private and public links from potential network abuse

In addition, some benefits would have to be granted to the person who is willing to share his or her Internet link with the children, like a government-subventioned Ceibal ADSL.

This approach could potentially lead to a win-win situation for all parties involved:

- The final user benefits from a cheaper/faster ADSL connection, in addition to helping out a good cause;
- Most of the children will enjoy free Internet connectivity at their homes, fulfilling Phase 2 of project Ceibal;
- The government fulfils its social responsibility and Ceibal’s compromise through the national telephone company, at a fraction of its original cost.

It was clear from the beginning that the ADSL Ceibal could only be implemented as a Network Appliance. Minimum requirements were: One Wi-Fi interface for the LAN, one Ethernet WAN interface, Linux embedded, and above everything, it had to be very affordable. The research focused around WRT Linux appliances, and it’s currently considering the Fonera hardware [http://www.fon.com/](http://www.fon.com/)

In conclusion, many obstacles had to be overcome: dealing with multiple providers, working with new, and sometimes unpredictable technologies, trying
always to stay open and technology neutral, or adapting to local cultural and geographic characteristics. These are just a fistful of the issues surrounding any complex project such as Ceibal. As a result of this work, and brave political decisions, hundreds of thousands of children currently enjoy a personal educational laptop computer and free Internet access at their local public schools. In addition, and completing Phase 2, by January 2010, six months from now, Ceibal’s Internet Wi-Fi will reach 80% of urban children at their homes.