

dot-dot-enter: DATAPAC in 2010-2012

Release 1.0, 04/2012

Ioan Landry, Project Lead
Dave Arsenault, Developer

info@chargen.ca

Thanks to: Guy Fortin, Raoul Chiesa

Abstract

We know TCP/IP as the undisputed victor of the "Protocol Wars" and the ubiquitous technology behind an overwhelming majority of modern networking and telecommunications today, having clearly outclassed competing technologies by the year 2000 or earlier thanks to its low cost of deployment, simplicity and eventual universality.

One of the more full-featured predecessors and competitors to the TCP/IP stack was a standard known as X.25. When we think of it at all, the consensus is that X.25 is an arcane and vestigial technology used only by still-lagging telecommunication carriers for backbone purposes. However, there is still a bewildering number of devices – some of which we unwittingly depend on every day – functioning solely over such "obscure" or "legacy" networks, which predate the modern Internet and its security model. This paper will briefly cover traditional X.25 lore before focusing on one X.25 network in particular; Canada's largest packet-switched data network known as the DATAPAC family of services, with consideration given to its historic and, more importantly, current uses and functions and what this implies from a security perspective.

Table of Contents

1 – Introduction	3
1.1 – What is X.25?	3
1.1.1 – X.25, Frame Relay, TCP/IP: Contrasted and Compared	3
1.1.2 – Inside X.25	4
2 – What is DATAPAC?	5
2.1 – Use Cases	6
2.1.1 – GONet Electronic Data Transfer	6
2.1.2 – York Region Transit	7
2.1.3 – RAMQ	7
2.1.4 – Canadian Finance and Retail Industries	8
2.1.5 – Canadian Telecommunication Industry	8
2.2 – Accessing DATAPAC	8
2.3 – DATAPAC Addressing	9
2.4 – DATAPAC Return Codes	9
3 – The Project: what, why, and how...	10
3.1 – What and Why	10
3.2 – How (Introducing datascan.py)	10
4 – Results and Observations	11
4.1 – General overview of active hosts	11
4.2 – Systems identified	12
4.3 – Vendor Distribution	12
4.4 – Geographical distribution of active hosts	13
4.4 – Miscellaneous observations	13
4.5 – Raw Project Output	14
5 – Closing Thoughts	14
Annex A – Public DATAPAC Dial Ports in 2012	14
Annex B – Recommended Reading	14

1 – Introduction

1.1 – What is X.25?

The first wide area networks were deployed in the 1960's and operated under a myriad set of protocols and propriety communication standards and, as connectivity increased, the need for a a unified, standard set of protocols to maximize interoperability and the exchange of data became obvious. To help address this burgeoning problem the International Telecommunication Union (ITU) released its so-called "Orange Book" in March 1976 containing a standard protocol suite known as X.25. At its simplest, X.25 defines three levels or layers (physical, data link and packet layers) and operates as a common interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

With a standardized and reliable protocol, it didn't take long to move from theory to practice and for full-fledged X.25 networks to emerge. Both the public and private sectors were eager to reap the benefits of telecommunication and while Canada's DATAPAC may have had the honour of being among the first operational X.25 networks, others were not far behind: TRANSPAC (France) and DATEX-P both surfaced in 1978 , followed by the United Kingdom's Packet Switch Stream in 1980 and Ireland's Eirpac in 1984, to name but very few. Indeed, hundreds of X.25 networks were eventually built in as many countries, usually operated by the state's postal, telegraph, and telephone service (PTT) authority or an amalgamation of telecommunication providers, while countless more were operated by private entities such as Western Union, Barclays, and the global SWIFT network, not to mention separate X.25 facilities servicing the needs of government, military or academic institutions. Those looking for a complete listing of (nominally) operational X.25 networks and their accompanying Data Network Identification Codes (DNIC) should refer to the International Telecommunication Union's authoritative annual assignments¹.

While X.25 offered a degree of standardization to networked communications, individual networks were still effectively balkanized "walled gardens" and it took the eventual introduction of TCP/IP to offer the global interconnection and ubiquitous networking which truly changed the way we approach telecommunications in our everyday lives. However, it seems that our hyper-networked world is oblivious to the archaic architectures which predated the Internet and still play an important and unacknowledged role even today. Despite the migration to TCP/IP in the 1990's and its mass-adoption in the post-millennial IT landscape X.25 has remained an integral and critical component in the telecommunications tapestry, often the silent workhorse behind financial institutions, telecommunication service providers, civilian aeronautical controls and filling a number of niche uses to fill governmental and military capacities.

Indeed, as we will see below, far from everyone has migrated away from X.25 solutions and a surprising number of systems continue to operate over DATAPAC and other networks and it would be especially imprudent for security professionals to ignore the existence of what lurks just at the edge of their "classical" network perimeter.

1.1.1 – X.25, Frame Relay, TCP/IP: Contrasted and Compared

X.25, Frame Relay and TCP/IP are three very different technologies, often operating at different layers and fulfilling different tasks. However, we find it would be helpful to briefly elaborate on them and highlight where they contrast and complement one another.

As mentioned, the X.25 protocol suite was defined 1976 and maps out to layers 1-3 of the OSI communication model (which it predates), but will be generally referred to as a 3rd layer protocol with speeds of 56 Kbps to 2.048 Mbps (though usually operating at the lower end of that spectrum). Traditionally, most public X.25 networks were treated as a "utility" with the vendor/operator handling infrastructure and all aspects of data transport and routing while billing the user for access or usage.

X.25 defines the ground rules for communication between DTEs and DCEs – generally representing data terminals and devices such as modems, respectively. It is composed of three layers:

1 International Telecommunication Union, "List of Data Network Identification Codes", 2011, Retrieved 15/12/2011, [Link](#)

- The *Physical Layer*, most commonly implemented through the X.21, V.24 or V.35 standard, specifying the actual physical interface between DTEs and DCEs.

- The *Data Link Layer* (also referred to as the frame layer or simply the link layer) which facilitates reliable transfer of data by transferring data as a sequence of frames between DTEs and DCEs as defined by the Link Access Procedure, Balanced (LAPB) protocol.

- And the *Packet Layer* which handles end-to-end operations between DTEs such as the establishment of connections, transference of user data, and the eventual termination of connections, as well as handling error and flow control.

As X.25 data flows over fairly unreliable analog links it was designed with reliability in mind and as such it performs end-to-end error-checking and verified the integrity and sequence of each and every packet and retransmitting any failures... of course, this robustness comes with a very high overhead compared to other technologies.

Frame Relay was accepted as a standard in 1984 and operates at the 2nd layer. Depending on one's perspective, Frame Relay is either X.25 on steroids, or X.25 stripped bare - as digital replaced analog and the need for higher throughput became apparent, the telecommunication sector began questioning the significant bandwidth overhead of X.25's strict error and flow control. Frame Relay trades high-level end-to-end error checking for optimal and rapid transmission of data - if an error is detected, it simply drops the frame and moves on instead of attempting to retransmit the data. While this may sound careless it should be noted that Frame Relay typically operates over reliable links, simply leaving error correction to higher-level protocols. It is ideal for periodic traffic spurts or interconnection of remote locations over leased lines, and operates at speeds of anywhere between 56 Kbps all the way to 45 Mbps.

Finally, TCP/IP refers to a modern protocol suite, where IP (operating at the 3rd layer) is responsible for best-effort routing of data without much attention to reliability beyond rejecting malformed headers. That is to say, IP itself is flakey (at best) without supporting upper-layer protocols such as TCP at the 4th layer providing reliability, error detection and flow & congestion control, hence giving us what we know informally as the TCP/IP model we interact with each and every day. TCP/IP came to dominate the networking world thanks to its heterogeneous and vendor-neutral nature, while most X.25 implementations were "stand-alone" and often mired by proprietary protocols or inconsistencies. Frame Relay, instead, is known as a reliable and efficient WAN solution often used to interconnect remote networks and frequently transports higher-level protocols (X.25, Ethernet, etc...) through encapsulation.

1.1.2 – Inside X.25

X.25 packet sizes are usually 128 bytes, but can vary from 16 to 4096 bytes depending on the network and its facilities. For instance, DATAPAC defaults to 128 bytes but can transmit packets up to 256 bytes in size.

X.25 Control Packet

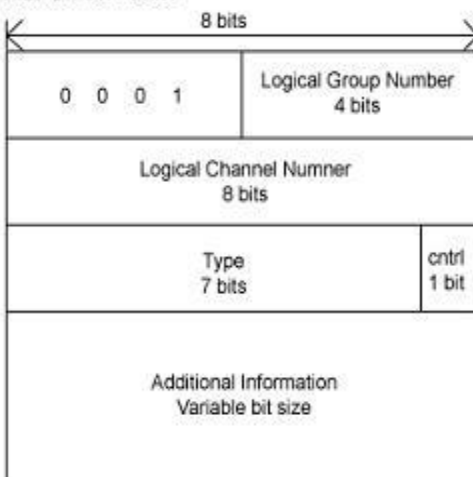


Image 1, Left
X.25 Control Packet
Responsible for handling the state of any given call.

X.25 Data Packet

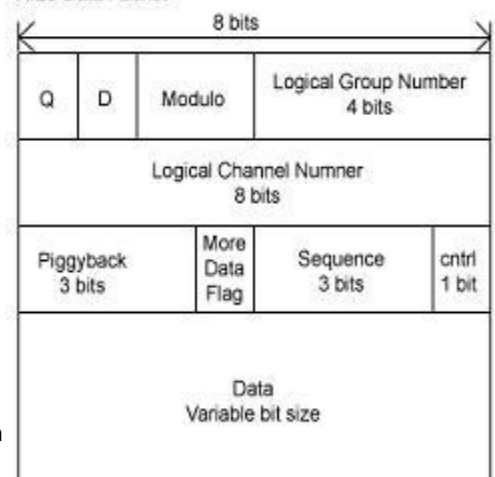


Image 2, Right
X.25 Data Packet
Responsible for the actual transmission of data.

2 – What is DATAPAC?

Without any verbosity or nuances, the simplest way to define DATAPAC is as a commercially-operated X.25 data network operating within Canada, where it was not the only network of its sort but easily the most widespread. However, before discussing the creation and evolution of DATAPAC (or any other X.25 network for that matter) it would be important to briefly discuss the fertile conditions of the time that led to the emergence of early networking technologies and eventually to the creation of the ARPANET, the world's first packet-switched network and predecessor to the Internet as we know it.

ARPANET was conceived by the Defense Advanced Research Projects Agency in the 1960's as a method to interconnect various academic and defense research centers with one another and by the Autumn of 1970 the network, growing at a steady pace, found itself connected from coast to coast for the first time, with roughly a dozen router nodes (then known as Interface Message Processors) in operation. One thing that set the ARPANET apart from earlier home-grown networking solutions around the globe was its underlying technology known as packet-switching, a fast, robust and efficient concept that outclassed the "circuit-switching" technology of the time. The success of packet-switching in the ARPANET and the fruits of data communication quickly began obvious to all and piqued the curiosity of more than one academic or researcher around the globe. Unfortunately, connectivity to the ARPANET was restricted to American universities and defense contractors with very few exceptions so early requests from Canadian universities (namely, the *Université du Québec*) to join the network were rebuffed.

Regardless, the issue of connectivity was far too important for Canada to leave to various academic institutions or private interests without an overarching strategic vision, not to mention the possible questions and conflicts of national sovereignty in over relying on an American data network. In 1971 the Science Council of Canada published a report, "*A Trans-Canada Computer Communications Network*" which stressed the importance of developing a Canadian network, and in short order dozens of disparate entities set out to work across Canada. Many early networks were developing at the academic (CANUnet, Edupac, OUnet), national (CDNnet) or military (DRENet) levels. All of these endeavors and experiments met varying degrees of success and support (best outlined in "*A Nation Goes Online - The Early Years of Internet in Canada*"), though it was Bell-Northern Research's DATAPAC that eventually emerged as Canada's most popular commercial X.25 network. DATAPAC was remarkably loyal to the CCITT specifications for packet-switched networking in an age where many home-grown solutions had difficulties operating on a common standard, and clients and end-users did not have to worry about rolling out their own infrastructure (a costly proposition in a huge country with dispersed population centers even today), only their monthly usage bills to Bell.

Though originally developed in the hallowed halls of the Bell-Northern Research labs, operative authority over DATAPAC changed hands as Canada's telecommunication landscape shifted from the Trans-Canada Telephone System (later Telecom Canada) to the loose alliance known as the Stentor Alliance², before finally returning to Bell Canada when the Stentor Alliance – more a brand than a centralized corporate entity, the whole never greater than the sum of its parts³ – fragmented or, more succinctly, reverted to provincialism.

Historically, in Bell Canada's own words, DATAPAC was relied upon for a wide variety of purposes ranging from personal banking, credit verification, retail Point of Sale (PoS), reservation and inventory systems, data entry and collection, file transfers and electronic communications of all sorts⁴. But in our age of multi-Gbs Internet connectivity, how is DATAPAC faring? Hard to tell. For many years Bell Canada has been urging merchant customers to migrate to an IP-based VPN solution⁵, claiming that DATAPAC will have reached its end-of-life in December 2009⁶. This date is also echoed by Tony Rybczynski in a December 2009 release of the IEEE's "*Communications Magazine*". Mr. Rybczynski was a key individual in the creation of DATAPAC and the ratification of the X.25 protocol suite itself, and the article in question and his earlier writings are must-reads for anyone interested.

2 Wikipedia, "*Stentor Alliance*", Date Unknown, Retrieved 3/12/2011, [Link](#)

3 Damage INC., "*The Stentor Alliance explained*", 30/06/2000, Retrieved 3/12/2011, [Link](#)

4 Bell Canada, "*Datapac: What is it?*", 1998, Retrieved 20/08/2011, [Link](#)

5 Bell Canada, "*Unleash your retail business with IP connectivity*", 2008, Retrieved 08/11/2011, [Link](#)

6 Bell Canada, "*IP VPN Point of Sale - 7. Why do I need to migrate from Datapac to an IP service?*", Date Unknown, Retrieved 07/07/2011, [Link](#)

Other than the paltry amounts of information available on their website, Bell Canada has been quiet on the issue of DATAPAC after the Stentor Alliance disintegrated. In fact, most of the publicly-available discourse of the present and future of DATAPAC has been found in the private sector, particularly among companies specializing in integration and migration towards IP-based solutions. For example, much doom and gloom is to be found from IP-based PoS integrators such as Precidia Technologies, who claim that DATAPAC *"will be eliminated in December 2009, following a phase-out path that spanned several years"*⁷. In a December 2006 release of the *"Frontier Times"*, the President of Precidia Technologies states that thanks to the introduction of EMV that Bell and Telus were phasing out DATAPAC, chiefly by denying to service new installations⁸. Finally, on December 31 2009, Robert Bostelaar of the Ottawa Citizen published an article titled *"Robust Datapac finally retires"* and while the article has since been pulled without being mirrored, a French-Canadian blogger summarized the article in his native tongue a few days later⁹.

However, despite these end-of-life statements from both Bell Canada, vested interests and "those in the know", the DATAPAC network was still alive throughout 2011 and, at the very least, early 2012. We assume the communication and planned end-of-life was not completely arbitrary, instead implying that no new installation assignments would be accepted after the cut-off date. Perhaps the continued use of DATAPAC is not solely linked to the use of important legacy systems in the telecommunication sector, but may be linked to the Canadian financial industry's delay in adopting EMV or "Chip-and-Pin". While EMV is already operational in some parts of the world the Interac Association only began their roll-out in 2008 and by their own admission complete coverage will only be achieved years later: Automated Banking Machines (ATM) will no longer accept the older cards as of December 31, 2012, and point-of-sale terminals will stop processing them as of December 31, 2015¹⁰.

2.1 – Use Cases

Being a very opaque network near its retirement age it is not easy to attribute ownership of arcane devices operating on DATAPAC to specific entities. However, in this section, we'll refer to publicly available data to shed light on how various organizations – both public and private – were using DATAPAC until very recently.

Already by 2001 (never mind 2011, when the bulk of this project took place), the network was already showing its age yet was and is still used for telecommunications, a variety of commercial functions (from handling Interac EFTPOS debit payments to reporting purchased ticket numbers in provincial lotteries), and a wide-range of other financial and governmental functions, such as the billing and invoicing between Ontario's Ministry of Health (via GONet EDT) and private healthcare providers, as well as Québec's *Régie de l'Assurance Maladie du Québec* (RAMQ) and the same.

2.1.1 – GONet Electronic Data Transfer

"GONet EDT is a service provided by the Government of Ontario for securely transmitting electronic files. The Ministry of Health makes this service available to physician providers and medical billing agents for billing transactions. OHIP Submissions may be sent, and Claims Error Reports and OHIP Reconciliation Summaries received, via modem by using this electronic service."

Private healthcare providers in the province of Ontario regularly accessed the EDT (Electronic Data Transfer) mainframes via DATAPAC with only a modem and a Bell-assigned NUI (Network User ID) in order to work out their billing arrangements with the Ministry of Health and Long-Term Care. However, in a communication dated September 2009 the MOHLTC states that *"Datapac Not Available for New EDT Enrollments - As of July 31, 2009, the Ministry of Health and Long-Term Care will no longer accept new Electronic Data Transfer (EDT) enrollments (claims submissions/overnight batch eligibility checking) that require Bell Canada's Datapac service as the connection method to the ministry."*¹¹

7 Precidia Technologies, *"Datapac Replacement Solution Helps City of Richmond"*, 2009, Retrieved 01/07/2012, [Link](#)

8 Deepak Wanner, *"Out with the Old, in with the New: Datapac and EMV in 2007"*, 12/2006, Retrieved 20/08/2011, [Link](#)

9 Francois Rodrigue, *"Le robuste réseau Datapac 3201 prend finalement sa retraite"*, 2010, Retrieved 01/07/2012, [Link](#)

10 Interac Association, *"F.A.Q. - Chip"*, 2011, Retrieved 11/11/2011, [Link](#)

11 Ontario Ministry of Health and Long-Term Care, *"Bell Canada De-Commissioning Datapac Connection by December 31, 2009"*, 09/2009, Retrieved 17/05/2011, [Link](#)

Curiously enough according to their own manual (updated July 2010) their "new" solution still requires a modem capable of a baud rate of 33,600 and recommends ZMODEM, KERMIT, YMODEM OR XMODEM for file transfers¹², not quite the cutting edge of technology.

2.1.2 – York Region Transit

"Credit and debit card transactions are processed through a third party (Moneris) using a secure data communications link provided by Bell.

Currently, the terminal ticket vending machines (multiRide) installed at terminals use a secure data communications link (Datapac 3201 Line) provided by Bell for processing credit and debit card transactions. Bell and Moneris have jointly decided to discontinue the existing data communications link between terminal ticket vending machines and their system effective December 31, 2009. The terminal ticket vending machines (multiRide) will be required to use a digital subscriber line (DSL) to continue processing credit and debit card transactions. This requires both software and hardware modifications to the existing central system, ticket vending machines and data communications network."

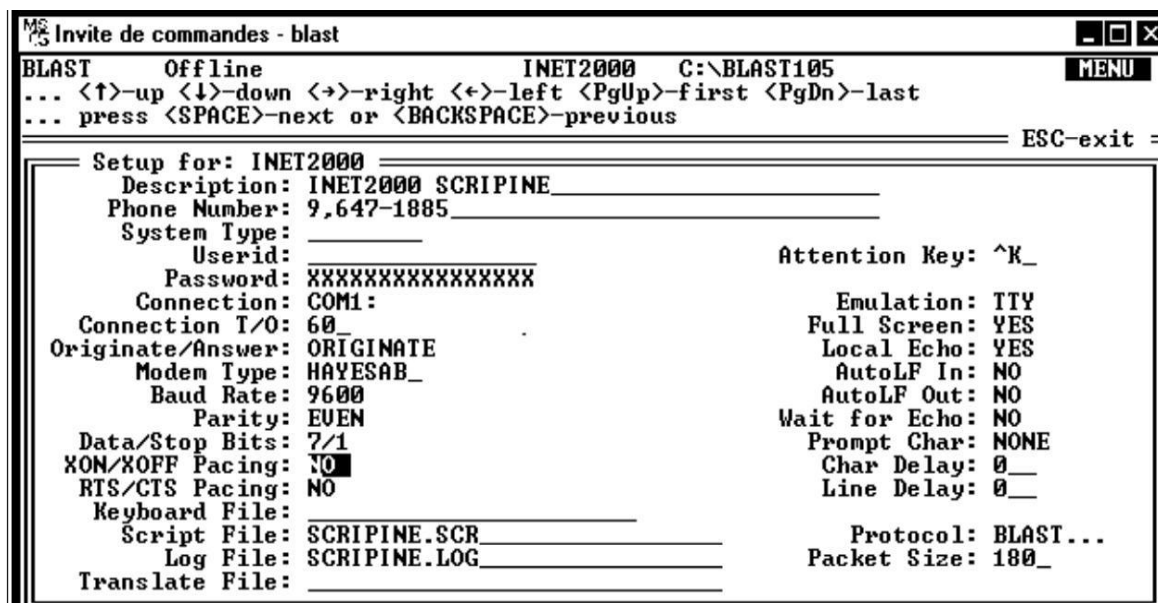
"The Canadian banks, financial institutions and other credit/debit card processing agencies are moving towards EMV (Europay, MasterCard and VISA) compliant standards, also known as "Chip cards" standards, which ensures a higher security to the credit/debit card transactions."

Excerpt from the York Regional Council Meeting, January 22 2009¹³.

2.1.3 – RAMQ

The RAMQ is Quebec's public health insurance body, covering an estimated 7.4 million people. For many years they handled billing and invoicing with private health care providers in much the same manner as Ontario's MOHLTC mentioned above. A RAMQ communication in April 2004¹⁴ urged partners to migrate from DATAPAC and their internally-developed BLAST software suite towards their IP-based "Transmission des Informations de Paiement par Internet" (Transmission of payment information via Internet), or TIP-I, though both solutions continued to operate side by side until April 2009 when the aging technology was put to rest. Those interested in the history behind BLAST should refer to "Datapac odds and ends", written by a contributor known as stelcheck for k-l1ne #50¹⁵.

Image 3 – Glory Days of BLAST



12 Ontario Ministry of Health and Long-Term Care, "Electronic Data Transfer Reference Manual", 07/2010, Retrieved 22/06/2011, [Link](#)

13 The Regional Municipality of York, "Regional Council Meeting of January 22 2009", 22/01/2009, Retrieved 20/02/2011, [Link](#) (Down 22/01/2012 - [Backup](#))

14 Régie de l'assurance maladie du Québec, "Pourquoi Remplacer BLAST?", 19/04/2004, Retrieved 15/06/2011, [Link](#)

15 "stelcheck", "Datapac odds and ends", 2007, Retrieved 18/07/2011, [Link](#)

2.1.4 – Canadian Finance and Retail Industries

A walk through any mall will show you that there are still retail locations with point-of-sale devices interfacing with DATAPAC 3201. Many Canadian consumers can attest to a 30-second waiting time when paying for goods via Interac even today. But that isn't to say there hasn't been a steady migration to IP-based solutions over the years, for example fast-food chain Burger King migrated its PoS network away from DATAPAC in 2004¹⁶, while the Liquor Control Board of Ontario followed suit in 2006¹⁷.

Moneris Solutions, Canada's largest payment processor, has a large selection of hardware payment solutions for merchants processing debit cards, credit cards and loyalty programs such as Air Miles through IP-based installations or through DATAPAC. Interestingly enough, it seems the widely-popular Air Miles program still operates solely through DATAPAC: "All AIR MILES transactions are transmitted from the POS terminal by either Datapac 3201 or Datapac 3101(dial up) communication."¹⁹

"With Datapac there was a certain amount of security by obscurity, because there's not a lot of people out there who are familiar with Datapac or who know how to crack an X.25 environment," said Lee-Yow. "But it's fairly easy to get into IP and there are plenty of people who know how to do it. Our switch is the core of our business in terms of authorization. Once we used IP, it was imperative that we provide a layer of data protection in front of our switch," said Lee Yow.

– Juniper Networks case study of Moneris Solutions, August 2010 (Emphasis added)¹⁸

2.1.5 – Canadian Telecommunication Industry

Given the systems and devices we have managed to identify on DATAPAC (see Section 3) it is evident that the telecommunications sector still has a presence on DATAPAC.

2.2 – Accessing DATAPAC

Connecting to DATAPAC is as simple as dialing the local access number with a terminal (ex: Minicom, Hyperterminal); most Canadian cities have several public dial ports assigned to them, all conveniently listed in the local Yellow Pages under "DATAPAC PUBLIC DIAL PORT 3101". Unfortunately, Bell discontinued these listings at some point in 2010 while many of the dial-ins serving smaller cities were pulled altogether; please refer to Annex A - Valid Dial-Ups to find an authoritative list of functional dial-ups as of May 2011.

Once connected via a functional public dial port we would normally point new users to the DATAPAC Information System ("*... an on-line bulletin board that contains up-to-date information about the Datapac family of services*") located at NUA 92100086 (English) or 92100086,B (French), however this host appears to have been taken offline sometime after Q4 2009 during what we interpret to be Bell Canada's slow termination of DATAPAC.

Once connected to the local public dial port you will need to type two periods followed by a return ("dot-dot-enter") to initialize DATAPAC. Upon doing so, you'll be greeted by the NUA of the PAD you are connected to as well as its supported facilities:

Example 1: Toronto dial port

```
ATDT4168684498
CONNECT 9600/V32/NONE
DATAPAC: 4680 0024
```

Example 2: Two dial ports in Ottawa - worth noting that both numbers allocate us to NUA 8540 1736

```
ATDT6137891483
CONNECT 9600/V32/NONE
DATAPAC: 8540 1736
```

¹⁶ IT World Canada, "Burger King gets a whopper of a network", 19/10/2004, Retrieved 13/05/2011, [Link](#)

¹⁷ ITBusiness.ca, "LCBO chooses GPRS to back up wireline network: IP-VPN rollout to handle all debit and credit authorization", 27/03/2006, Retrieved 10/08/2011, [Link](#)

¹⁸ Juniper Networks, "MONERIS SOLUTIONS, CANADA'S LARGEST PAYMENT PROCESSOR, SECURES ITS IP INFRASTRUCTURE WITH JUNIPER NETWORKS", 08/2010, Retrieved 08/02/2011, [Link](#)

¹⁹ Moneris Solutions, "TRANSELECT+ (T55) MERCHANT OPERATING MANUAL", 2003, Retrieved 21/06/2011, [Link](#)

ATDT6135674537
CONNECT 9600/V32/NONE
DATAPAC: 8540 1736

Example 3: Dial port in Halifax

ATDT9024538100
CONNECT 2400/NONE
DATAPAC: 7650 0227

2.3 – DATAPAC Addressing

Each node or host is assigned an NUA (a Network User Address, also known internally as a DATAPAC Network Address, DNA), which is 8 digits long. The first four digits (the prefix) designate the city and provinces (2000 – 3999 are assigned to Ontario, 6900 – 7099 to Manitoba, and 8200 – 8299 to Quebec for example) while the following four digits (suffix or host) are assigned to active hosts.

NUAs can also trail up to 10 digits long using logical channel addressing (LCN), or longer still with the use of mnemonics (kind of a primitive version of host names). Further still, both can be employed together. For example:

44400100 is an average run of the mill NUA,
4440010020 is a sub-host of that, as are
44400100,outdial (which corresponds to a sub-host offering outdial services), and
44400100,unix (which corresponds to a UNIX sub-host), and more confusingly still,
4440010020,system (which corresponds to a host named "system" under the first sub-host above).

Admittedly, DATAPAC hosts combining both LCN and mnemonics "in the wild" are rare but the technical support is there.

2.4 – DATAPAC Return Codes

During your searches, each DNA you attempt to connect to will provide you a return message, sometimes ambiguous and sometimes quite self-explanatory. Provided below is a short description of the eleven most common returns:

Call Cleared - Temporary Network Problem: This once meant there were legitimate problems at the remote end, but since 2009 there are entire prefixes corresponding to certain provinces that return this message, hinting that the problem is not so temporary after all. See Section 4.1 for more information.

Call Cleared - Address not in service: This DNA is not hosting a system or is simply not assigned. No connection is established.

Call Cleared - Access Barred: Remote system is part of a Closed User Group (CUG) or, in other words, has a "white list" approach and only accepts calls from DNAs in the same subgroup. The connection is terminated.

Call Cleared - Collect Call Refused: Remote system is not accepting the collect call charges and you lack an NUI (Network User Identifier) to handle the charges needed to connect. For this to make sense you need to understand that nodes that clear your call without a fuss are happy to carry the charges associated with the connection, while others are configured not to. The connection is terminated.

Call Cleared - Incompatible Call Options: Either you or the remote system has facilities not understood by the other. The connection is terminated.

Call Cleared - Destination not responding: Remote system is either down or ignoring incoming calls, and there does not seem to be any method to reliably confirm which. No connection is established.

Call Cleared - Destination busy: This message suggests that all logical channels on the remote system are in use, but in most cases today this message is unambiguously permanent no matter when one tries to connect to the system. The connection is terminated.

Call Cleared - Remote Procedure Error: The remote system is expecting a full NUA with mnemonics to the current prefix usually in the form of <NUA>,<MNEMONIC> and the connection is unceremoniously terminated. See Section 2.3 for more information on mnemonics.

Call Cleared - Remote Directive: Much like the "Access Barred" return, the remote system does not want to communicate with you (or, more specifically, your originating host) and the connection is terminated. Like "Remote Procedure Error" the right mnemonic sub-address can sometimes get past this, but not always.

Re-enter: A transmission error occurred on the current input line. This is usually a fat-finger error in the address.

3 – The Project: what, why, and how...

3.1 – What and Why

The genesis of this research began with the realization that both legacy network equipment and unorthodox attack vectors are virtually ignored in the security community, with its emphasis on web applications and client-side attacks. However, we the authors strongly believe that even in our age of eroding network boundaries it is important for security professionals to take a sober account of their threat surface in its entirety and discuss both the real and theoretical threats emanating from its nooks and crannies.

With this in mind, the desire to shed light on such an unreported aspect of telecommunications motivated us to go forth with the task at hand: that of mapping out DATAPAC address space as well as we could and extrapolating from the results.

3.2 – How (Introducing datascan.py)

We developed a new scanner in python aptly named 'datascan'. Reliability in connecting to and scanning DATAPAC network addresses took precedence over more advanced features; the public release of datascan scans any given range sequentially and simply logs all results to a user-defined SQLite database. It does not log "banners" or any interaction from connected hosts, simply listing them as "Call connected". Given the small number of active hosts on DATAPAC, we feel the general public can make do with this lack of scalability.

Using datascan is trivial and the few flags should be self-explanatory:

```
user@box:~$ python datascan.py -h
Usage: datascan.py [options] [start address] [end address]
```

Datascan - Datapac scanner

Options:

```
-h, --help                show this help message and exit
-d DEVICE, --device=DEVICE
                          Modem device name (default = /dev/modem)
-b BAUDRATE, --baudrate=BAUDRATE
                          Set the baud rate (default = 9600
-n DIALOUT, --number=DIALOUT
                          Dialout number (look in your local area for Datapac
                          number)
-f DBFILE, --dbfile=DBFILE
                          Database file to store results
-s START, --start=START   Start address of scan
-e END, --end=END         End address of scan
```

```
user@box:~$ python datascan.py -n 15145559905 -f scan.db -s 11110000 -e 11112000
```

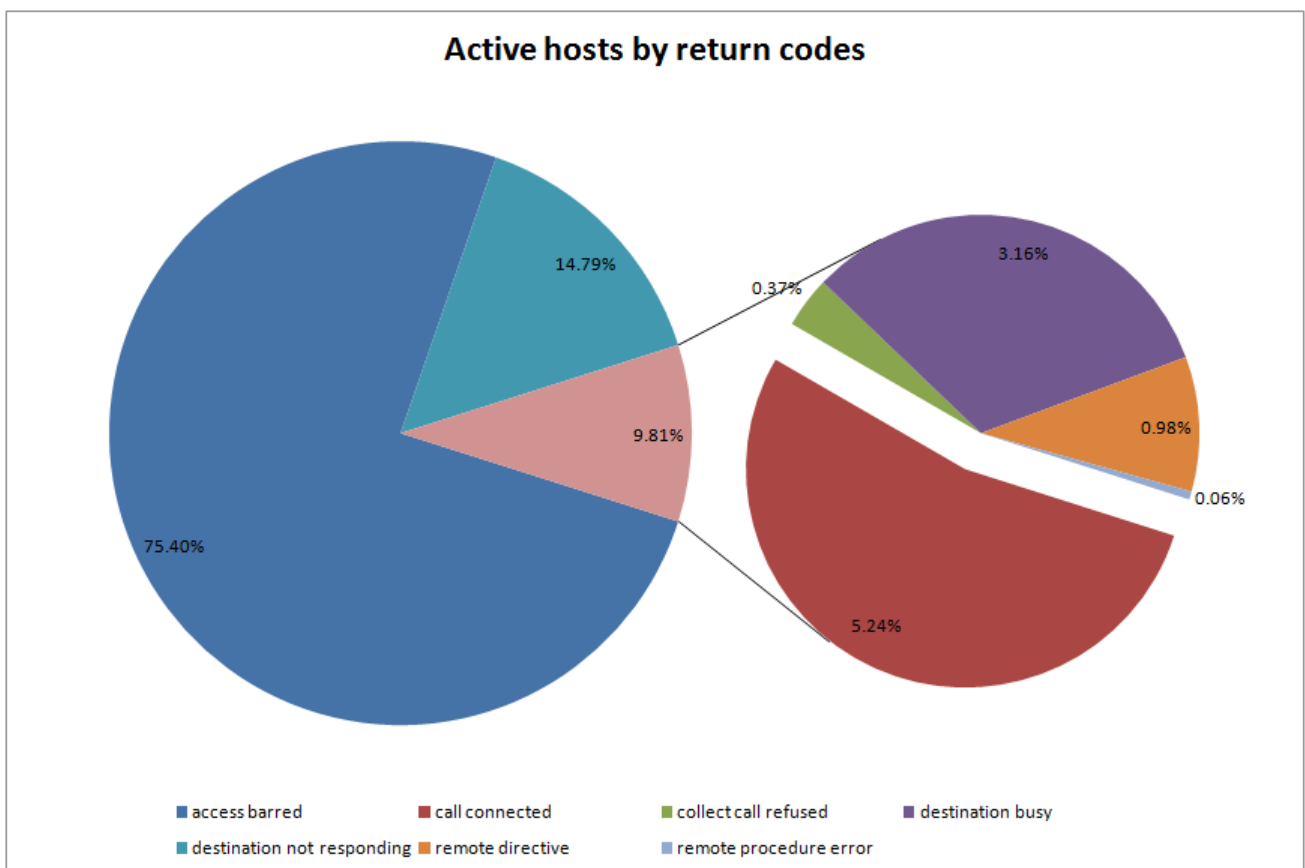
An SQLite database must be created before datascan can be utilized. The SQLite-impaired should refer to db/instructions.txt in order to be up and running in as few keystrokes as possible.

So what did we scan? Given the slow speeds we were dealing with we had to think of a way to avoid scanning each and every prefix with no rhyme or reason. Past research shows that there does not seem to be anything below prefix 2000 and valid prefixes seem to increment by 10. More interestingly, a few entrepreneurial DATAPAC enthusiasts discovered most – but not all – valid prefixes with active hosts have what appears to be an echo or test service on suffix 5000 (or in some cases somewhere between 5000-5010).

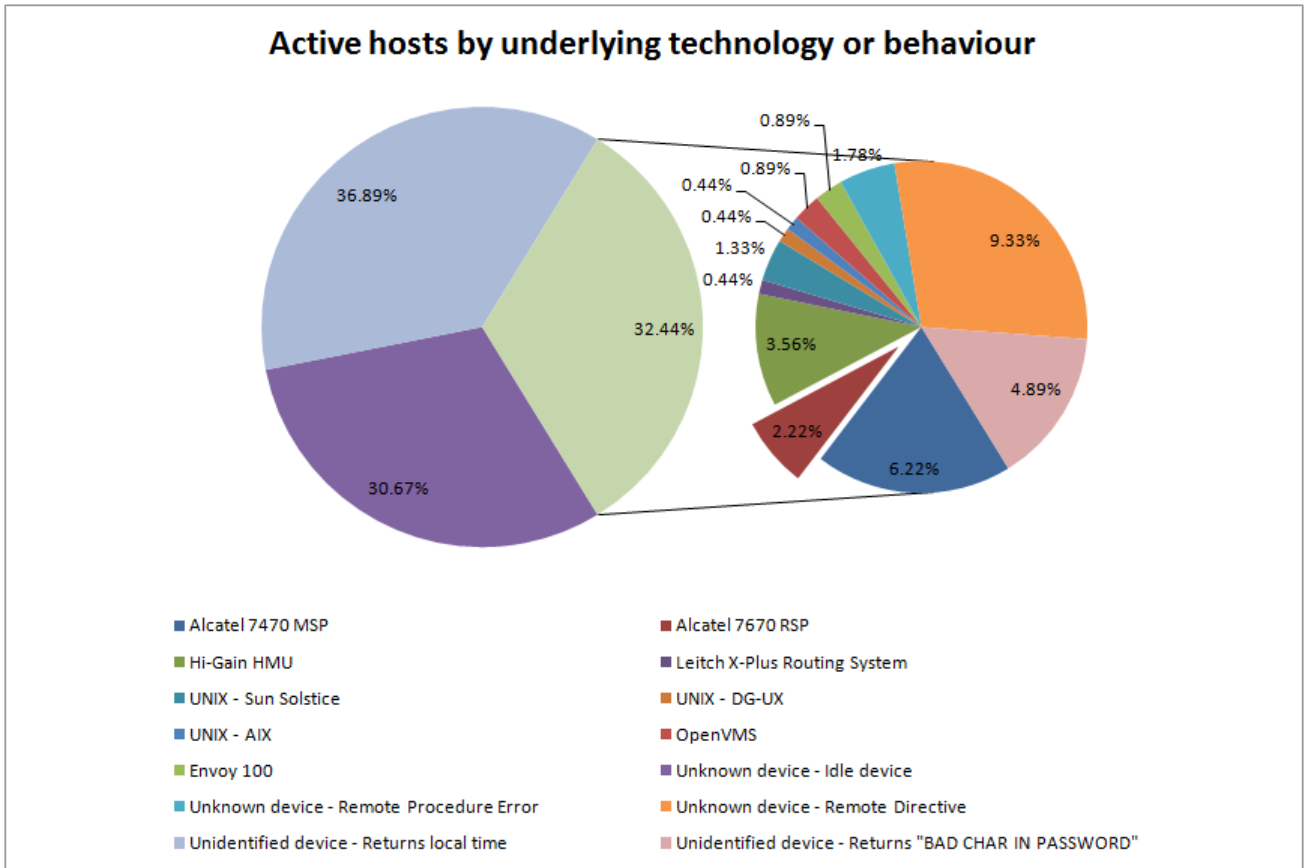
With this in mind, our scanning methodology was simple and scripting a series of short scans against 0000 5000-5010 to 9999 5000-5010, incrementing the prefixes in blocks of 10 (2000, 2010, 2020, etc...) netted us with a complete list of supposedly (hopefully?) healthy and active prefixes to focus our efforts and resources on. Once we finished with these we did explore other prefixes with mixed results.

4 – Results and Observations

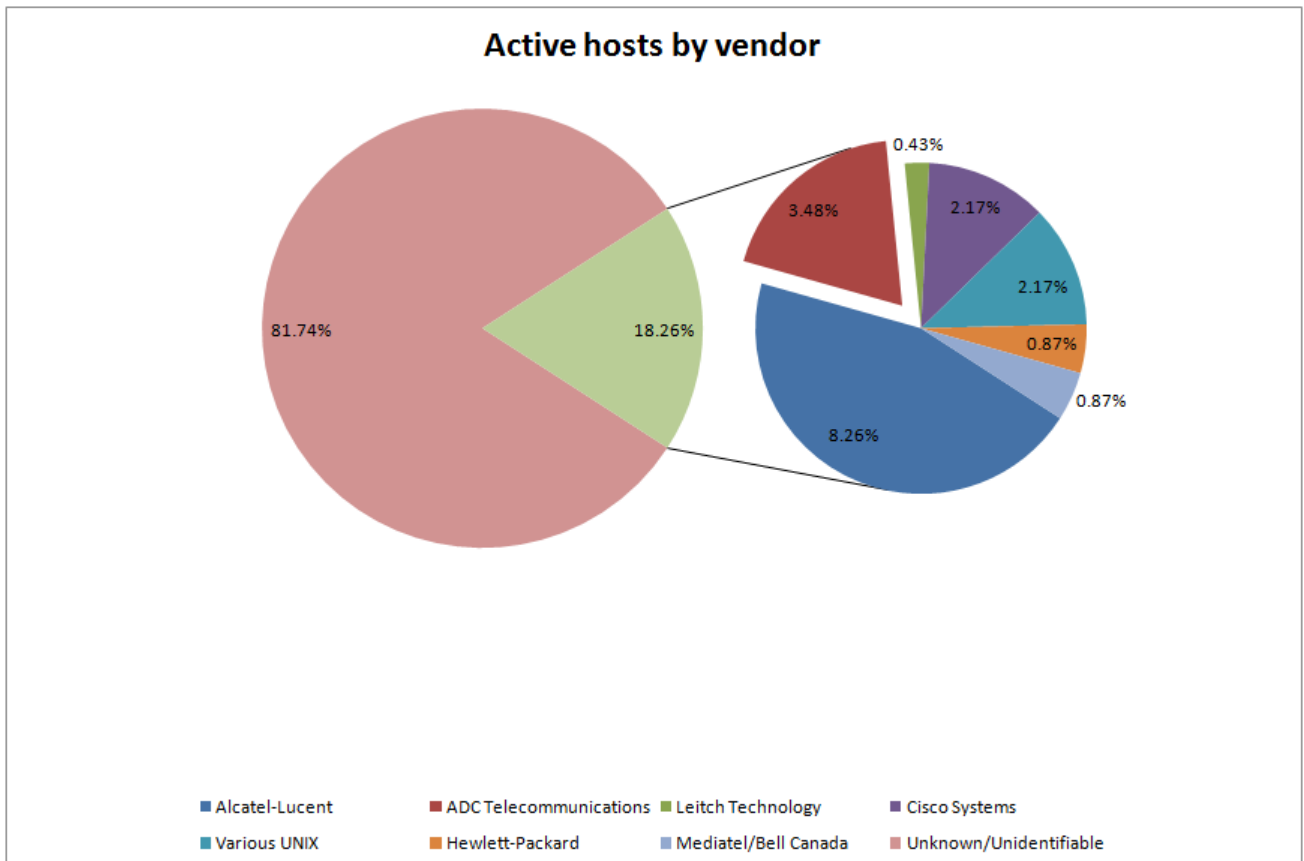
4.1 – General overview of active hosts



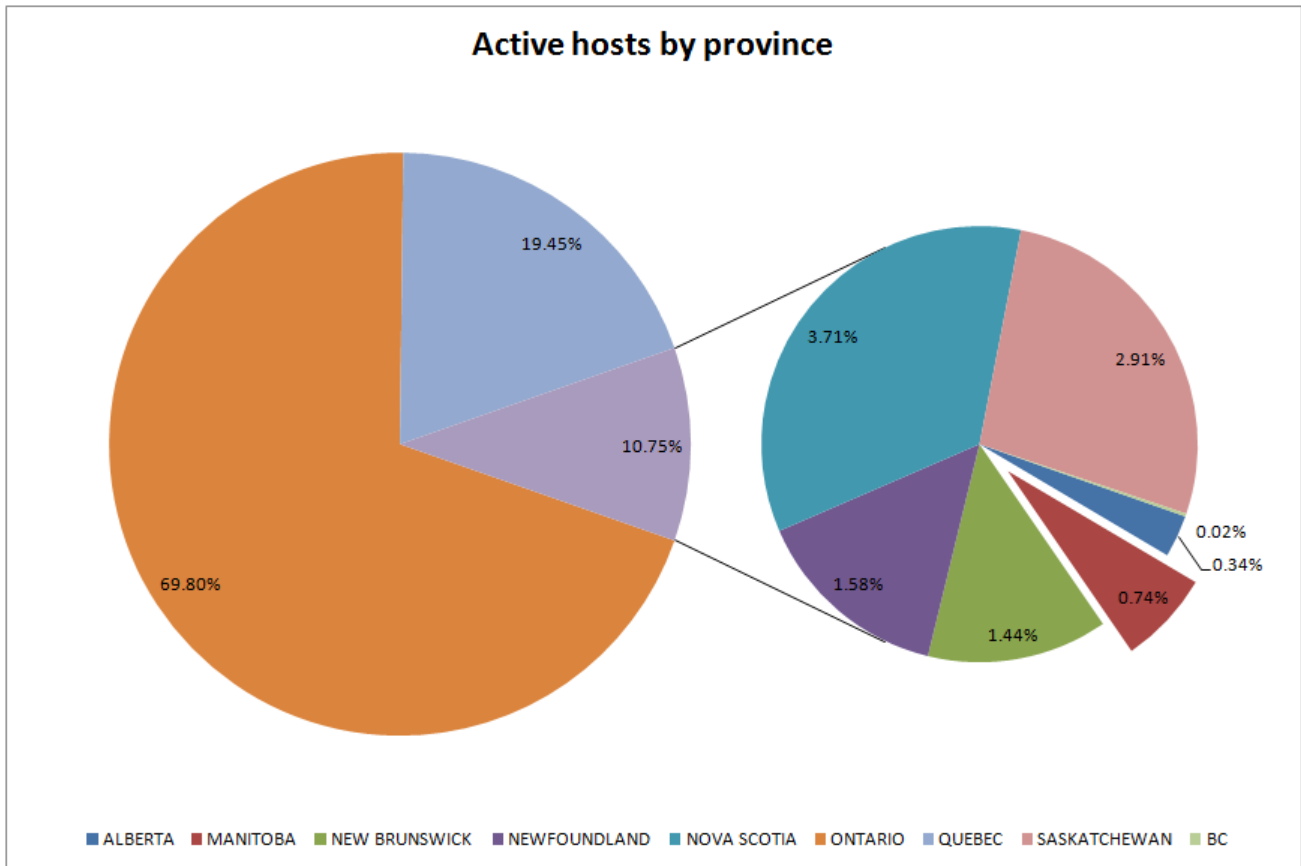
4.2 – Systems identified



4.3 – Vendor Distribution



4.4 – Geographical distribution of active hosts



4.4 – Miscellaneous observations

It appears that entire prefixes have gone missing over the past few years, specifically the prefixes associated with the provinces of Alberta and British Columbia. Furthermore, we've managed to observe several anomalies or curiosities in the field:

Throughout 2010, *every* host we attempted to connect to on prefixes 1014, 1240, 1250, 1260, 1270 and 1280 generated the error "Temporary Network Problem". This is anomalous as historically there has not been any active hosts operating on prefixes lower than 2020 and the expected return would be a simple "Call Cleared – Address not in service". Stranger still, By September 2011, some of prefixes changed behavior: 1014, 1240-1270 then returned a simple "Call Cleared – Address not in service", as expected. Finally, by March 2012, prefixes 1220, 1230, 1240, 1250, 1260, 1280 and 1290 reverted back to generating "Temporary Network Problem" on suffixes between XXXX0000 and XXXX1999, 2000 and above responding with a generic "Call Cleared – Address not in service" error. We are clueless as to the *raison d'être* or operative purpose behind this strange behavior.

Prefixes 58XX and 59XX are entirely offline serving the North-West Territories & Yukon (5800 – 5849) as well as Alberta (5850 – 6399). 6XXX is entirely nonoperational as of the Summer of 2009, and it served Alberta (as mentioned), British Columbia (6400 – 6899) and Manitoba (6900 – 7099). Finally, prefix 83XX is offline as the summer of 2010, which served British Columbia exclusively (from 8300 – 8399). Any given NUA one attempts to connect to on the mentioned prefixes respond with "Temporary Network Problem", though the nature of the problem is far from temporary.

As if entire prefixes disappearing from DATAPAC wasn't bad enough, the venerable DATAPAC Help Service operating at NUA 92100086 has been taken offline sometime between late 2009 and the Spring of 2010.

4.5 – Raw Project Output

An SQLite database containing all scan results as well as a list of functional NUAs garnered throughout 2010-2011 are available upon request.

5 – Closing Thoughts

Obviously, many of our comments and views on DATAPAC and its idiosyncrasies were formed from a purely outside perspective, given the scarcity of public information on the matter. As such we appreciate any elaboration, correction or clarification of anything within this document.

As said at the beginning of this paper: we hope that security professionals and enthusiasts approach X.25 and PSTN technologies not as complicated outlier risks but as very real and potentially very serious. With DATAPAC in its twilight years, the fact remains that there are many other X.25 networks operational today, some more active than others... and some of them in the strangest of places, acting as much more than simple historical relics. Take heed.

Annex A – Public DATAPAC Dial Ports in 2012

Please refer to "Annex A – Dialports.pdf".

Annex B – Recommended Reading

Datapac X.25 service characteristics, A. M. Rybczynski and D. F. Weir - [Link](#)

A Nation Goes OnLine: The Early Years of Internet in Canada, CANARIE - [Link](#)

Commercialization of packet switching (1975-1985): A Canadian perspective, Tony Rybczynski - [Link](#)

X.25 Virtual Circuits - Transpac in France - Pre-Internet Data Networking, Rémi Després - [Link](#)

Here be Dragons – Hacking non-IP networks, Morgan Marquis-Boire ('headhnr') - [Link](#)

X.25 Hacking in the 21st Century, Raoul Chiesa - [Link](#)

X.25 Network Communications Overview, International Business Machines Corporation - [Link](#)