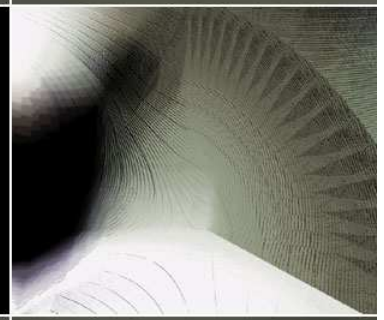
THE LAST HOPE

IPv6, the Next Generation Network Playground - How to Connect and Explore

Joe Klein
ipv6sec@gmail.com



DISCLOSURE:
I am responsible for this presentation; not my day job or organizations which I perform work for, nor my girlfriend, nor my laptop nor my dog.

I have been researching and publicly speaking on this topic for five years and … the same issues are still present.

Please contact me if you would like a copy of this presentation, or wish to use the information contained within.

July 18-20. 2008 – Hotel Pennsylvania, New York City

Agenda

- History
- Features
- Connecting
- Testing

Background on IPv4

- **IPv4 Internet**
  - Based excessively on DoD needs
  - Technical requirements and experience Derived from running NCP (Network Control Protocol), a US based network of 256 devices
- **IPv4 Internet evolves based on…**
  - 60's concepts, requirements and funding
  - 70's computing environments
  - 80's operating systems, applications, networks, and programming languages
  - 90's and 2000's operational experience, security and business practices
- **Result**
  - IPv4 is suffering under it's own success
  - IPv6 is ready to go!

Reasons to Replace IPv4 with IPv6

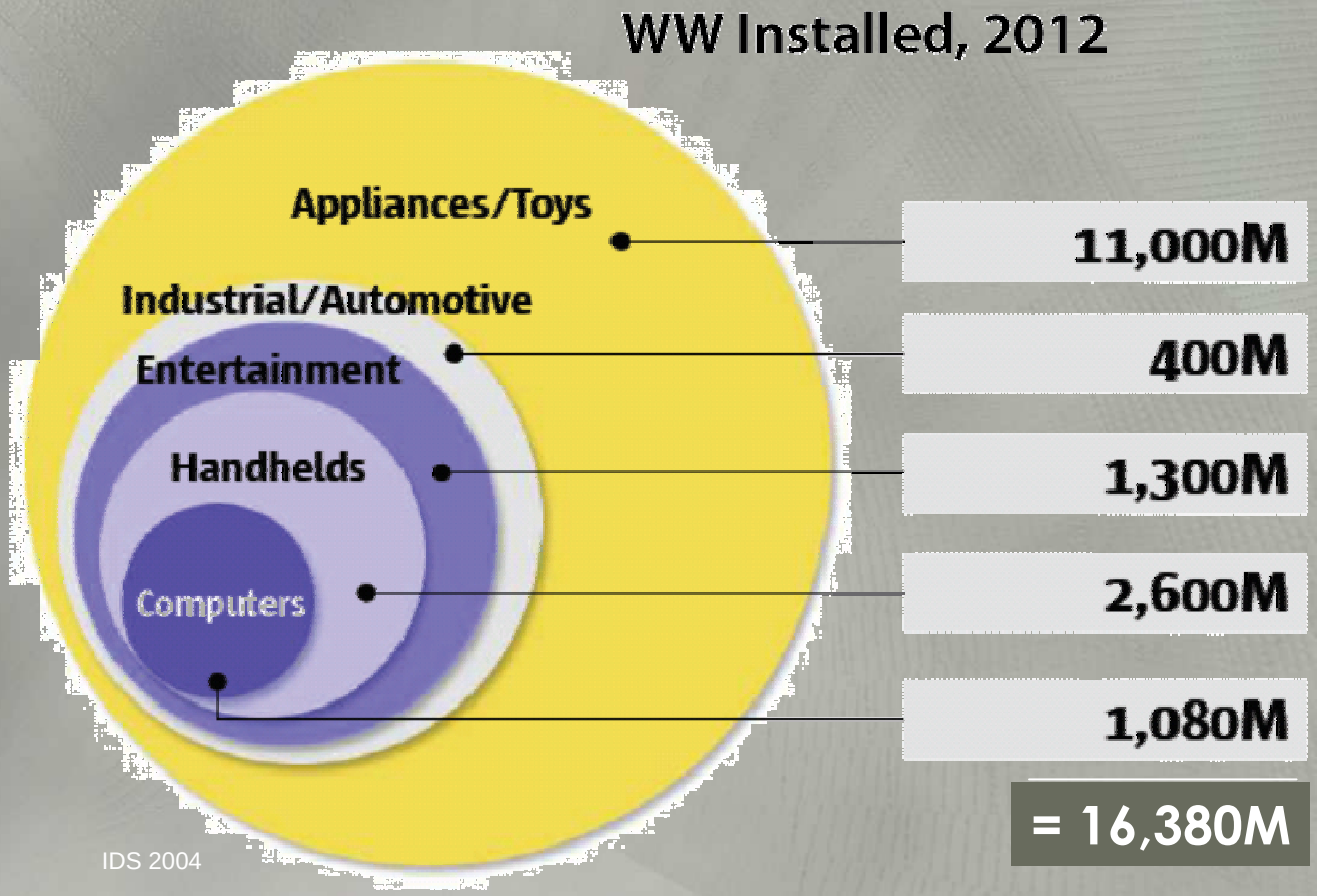
- **Current Problem :**
  - Inability to establish new servers/services & for applications to connect to servers/services
- **Reason :**
  - IPv4 address exhaustion required workaround until a replacement was available (IPv6)
  - Not enough IPv4 addresses available to many countries and organizations to meet demand
- **Workaround :**
  - Establish Gateways - Network Address Translation/Port Address Translation (NAT/PAT)
  - Establish non-global addresses (RFC 1918 addressing)
  - Mapping standard ports to non-standard ports
  - Multiple IP address ranges

Reasons to Replace IPv4 with IPv6

- **Results of workaround :**
  - Nested NAT/PAT addresses
  - Broken Applications, More Complex protocols
  - Establishment and use of NAT work around code (STUN, TURN, ICE, etc)
  - Gateways, Firewalls and Applications require NAT work around code
  - Complexity of supporting infrastructure, applications and security
  - Complexity of installing and managing multiple address pools
  - More time, energy and money spent coding and managing the workaround
  - Inability to easily identify all connected devices on an organizations network

IPv6 removes gateways, reduces application/protocol/security complexity and re-establishes end-to-end connections

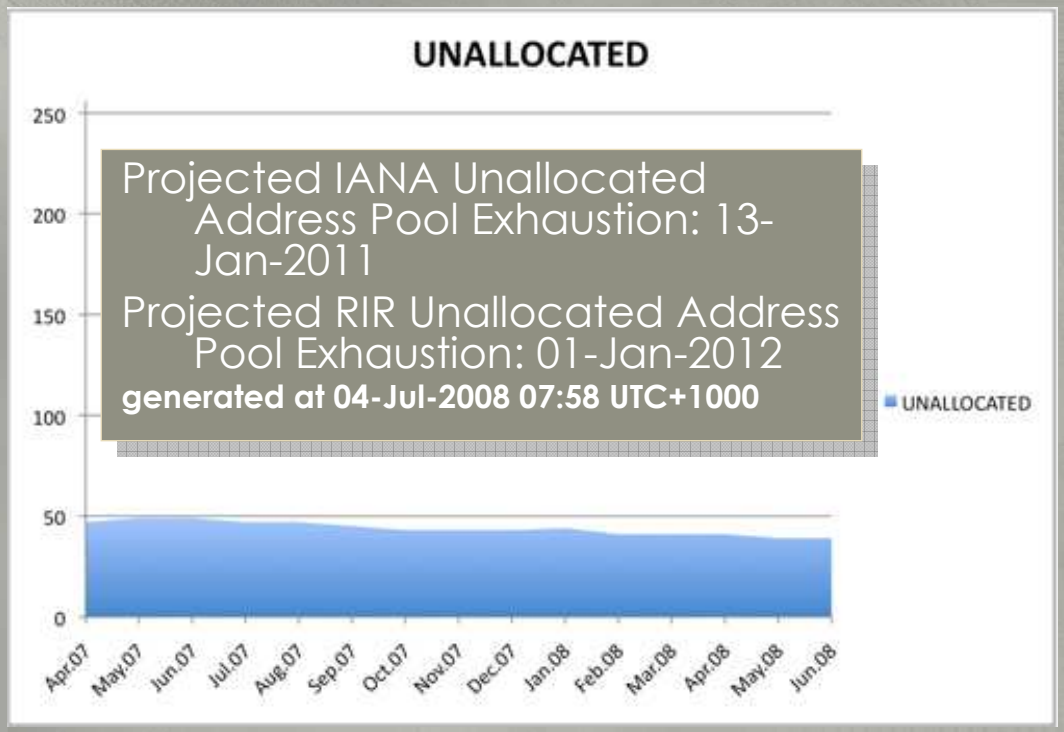
Justification for IPv6 – More Devices

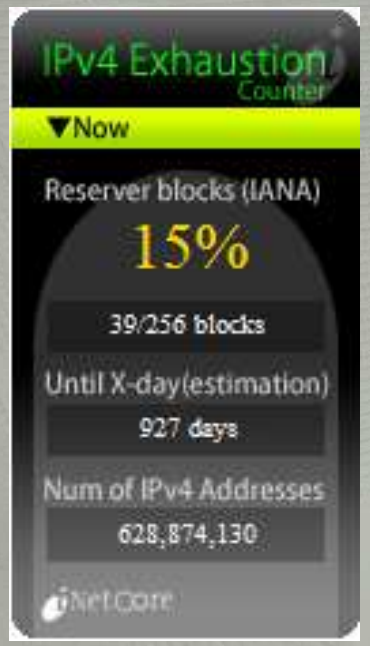


4x the size of the IPv4 Internet

Sun Microsystems estimates that including sensor and RFID networks, the world could have a trillion communicating devices in a decade!

IPv4 Address Exhaustion





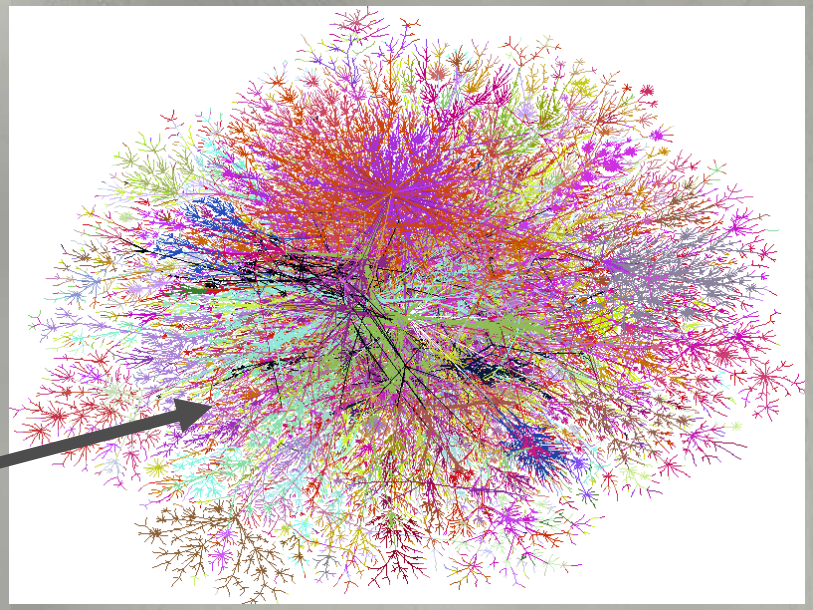
http://www.potaroo.net/tools/ipv4/index.html

This is a continuity issues! If the organizations does not have an IPv6 presence, how do they know customers are failing to access the site via IPv6? Will they lose users/customers?

Business Apathy - Denial of Service (BA-DOS)

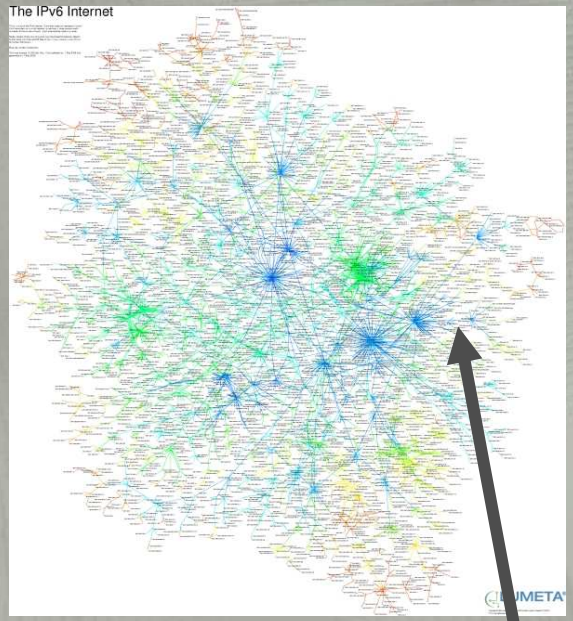
Comparing IPv4/IPv6 Network Size

You are here!



IPv4 - December 1998

http://www.cheswick.com/ches/map/gallery/wired.gif



IPv6 - May 2008

http://blog.lumeta.com/wp-content/uploads/2008/05/ipv6_map3.jpg

You might be here, but don't know it!

Review of IPv6 Features

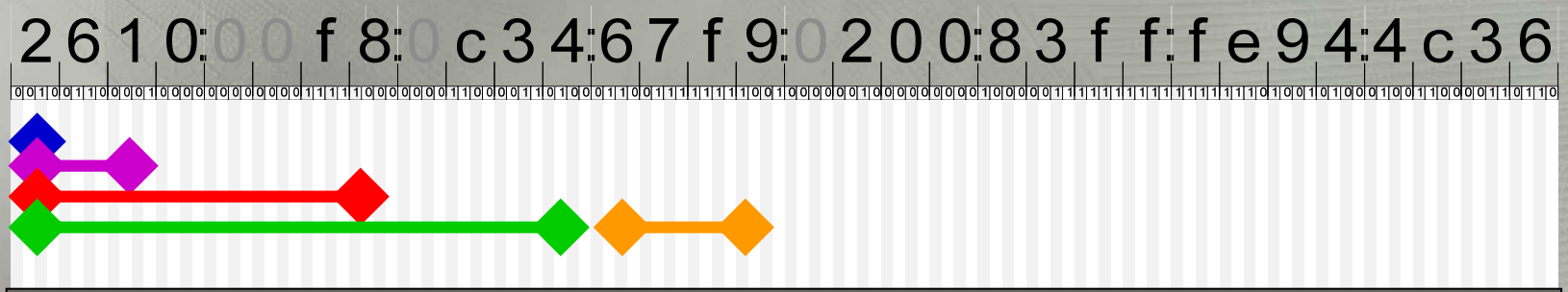
IPv4 : 32 Bits : 205.244.240.146

IPv6 : 128 Bits : 2610:00f8:0c38:0022:0000:0000:0010:0011

Besides increasing the IP address space, other features which are deployable in IPv6 (although some are available in IPv4)

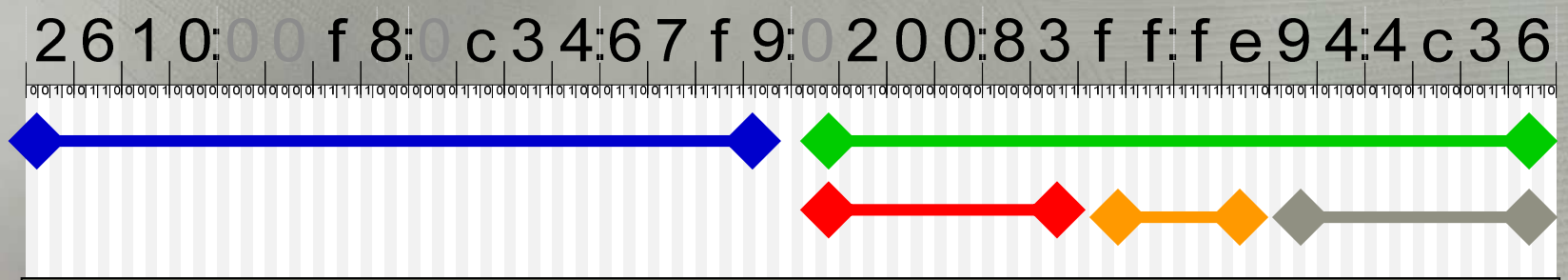
- **Link-local addresses** – self-assigned local address
- **Stateless Autoconfiguration** – allocate enterprise and global IP address with a simple configuration on a router
- **Stateful Autoconfiguration** (DHCPv6) – extensions for IPv6
- **Multicast** – a single data stream to multiple globally connected systems
- **IP Mobility** – Nodes can change locations and addresses, without breaking sessions
- **Extension Headers** - Designed for growth
- **Jumbograms** – 4 GByte Packets (64kBytes on IPv4) *((requires supporting L2))*
- **Simpler processing by routers** – everything is 64bit aligned, no L3 checksums
- **QOS** – Quality of Service – Traffic Class and Flow Label
- **Privacy Addresses** – Temporary random address assigned for outbound communications

Understanding IPv6 Address : Left Side



- IANA - 2000::/3
  - **The Current IPv6 space for unicast allocations in 1/8 of total address space (Excluding reserved addresses)**
- IANA Allocation to Registries – ::/12
  - **Example : 2a01::/16 was assigned to RIPE NCC**
- "ISP Allocations" – ::/32
  - **Regional registries make assignment to local ISPs**
- "End-Site Allocations" - ::/48 (Typical) (16 bits = 65,565 networks)
  - **Organization assignment this space – 16 bits for subnetting**
  - **Small companies / home users = ::/56 (8 bits = 256 networks)**
- "Subnet Assignments" - ::/64
  - **Unique identifier for hosts – 2^64**
- **Everything to the right of the 64 bit boundary is "locally assigned"**

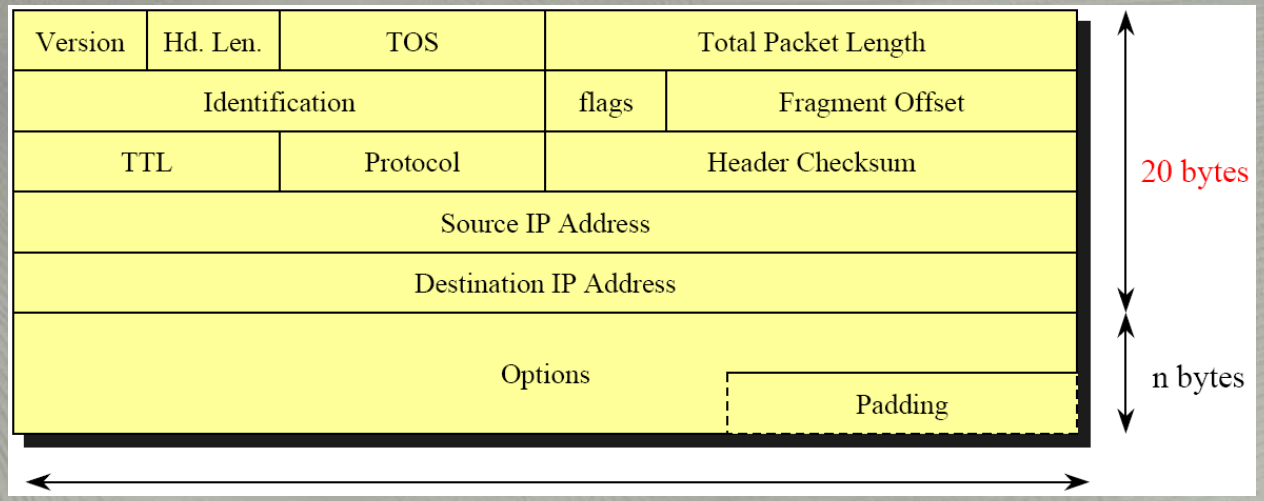
Understanding IPv6 Address : Right Side



- Network Segment *(Last Slide)*
- Local Host Assigned ::/64
  (18,446,744,073,709,600,000 hosts)
- Vendor ID (OUI)
- FFFE Identifies a Host Generated Address
  - Always the same (in AutoConfigured hosts)
  - Note: Other methods of autoconfiguration are available such as DHCPv6
- Vendor Assigned Number –24 Bits

IPv4 vs. IPv6 Packets

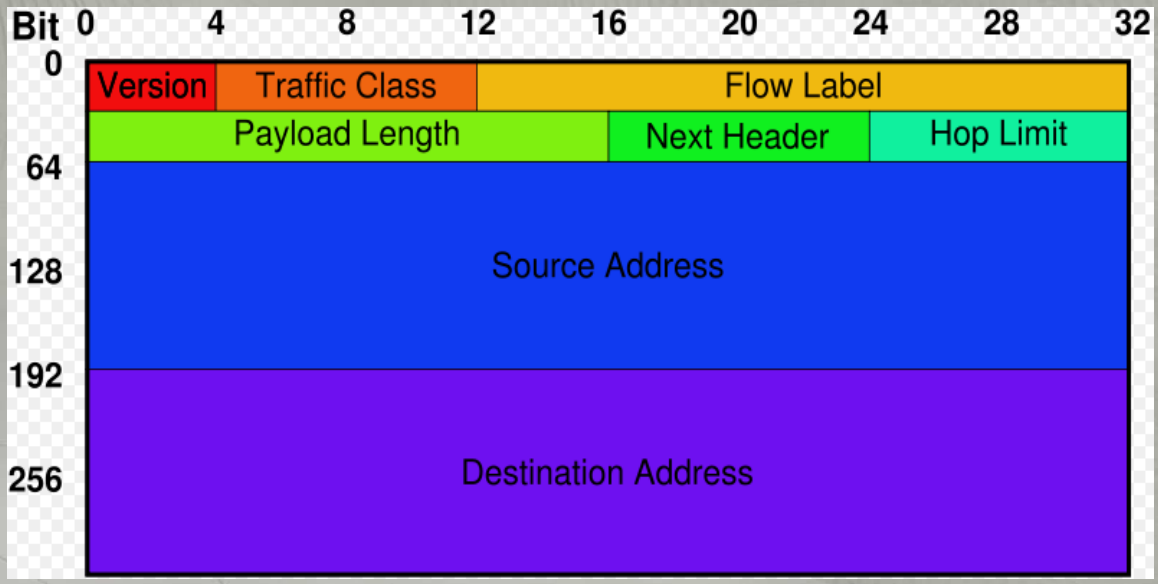
IPv4 = Variable 20 to 60 bytes long



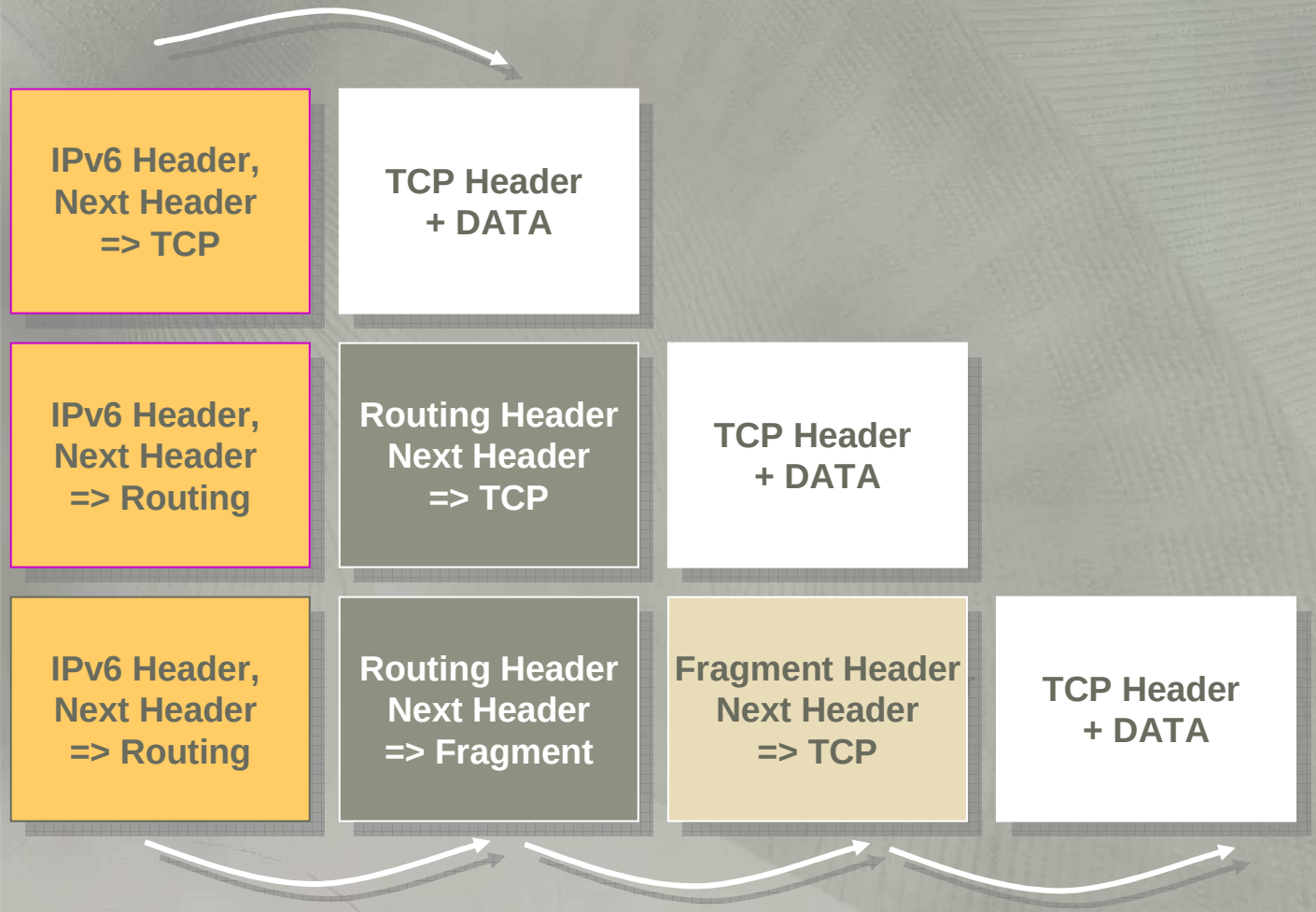
Not to scale

IPv6 = Fixed 40 bytes long

Everything falls on 64 bit boundaries



IPv6 Extension Headers



IPv6 Extension Headers

- Hop-by-hop (jumbogram, router alert)
  - If present, must be first EH
  - Replace options, and then some
  - Analyzed by every hop
- Destination
- Routing (loose source routing, mobility)
- Fragmentation
- Authentication (AH)
- Encryption (ESP)

Others exist, and more can readily be defined

Steps : Configuring IPv6

1. Ensure your device(s) (Host/Router) support IPv6?
2. Check if IPv6 is already enabled
   - If not, enable IPv6
3. Connect to the IPv6 Internet
   - Native
   - Transition
   - Tunneled

IPv6 Systems Requirements

Operating System	Capable	On by Default
Microsoft 2000 (2000)	Yes	No
Microsoft XP (2002)	Yes	No
Microsoft Vista (2007)	Yes	Yes
Solaris 2.10	Yes	Yes
Linux 2.4 Kernel	Yes	No
Linux 2.6 Kernel	Yes	Yes
OpenBSD / NetBSD / FreeBSD ('96)	Yes	Yes
Linux 2.1.6 Kernel ('96)	Yes	No
AIX 4.2 ('97)	Yes	No
AIX 6	Yes	Yes
Solaris 2.8 (2000)	Yes	Yes
IBM AS/400 (2002)	Yes	Yes
HP-UX 11iv2 (2007)	Yes	Yes
Open VMS (2007)	Yes	Yes

IPv6 Systems Requirements

OS	Capable	On by Default
Macintosh OS/X Current	Yes	Yes
Cisco IOS (12.x and Later)(2001)	Yes	No
Juniper (5.1 and Later) (2002)	Yes	Mostly
Linksys Routers (2006)	Yes, Upgrade to DD-WRT	No
Apple Airport Extreme (2007)	Yes	Yes
Window 95/98/ME/NT 3.5/NT 4.0 (2000)	Yes, Add on	No
IBM z/OS (2002)	Yes	Yes
Apple OS/10.3 (2002)	Yes	Yes
Cell Phone – Many (2006)	Yes	Yes
Cell Phone – BlackBerry	No	No

Is your System Currently Running IPv6?

Testing:

Test 1: netstat –na

Result: [::] or an IPv6 address

Test 2: ifconfig or ipconfig

Result: an IPv6 address

Test 3: ping or ping6 ::1

Result: pinging ::1

Enabling:

XP ipv6 install
netsh interface ipv6 install

IPv6 Infrastructure Requirements

Internet Service Provider

- IPv4 Only
  - Use a transition or tunnel
- IPv4 + Transition Support of IPv6
  - Vendor Limitations
- Full IPv4 and IPv6
  - No additional configuration required
- IPv6 Only

Note: All Major US Carriers & Cable Companies have projects to upgrade their internal Infrastructure to support IPv6 but, delivery to customer is a different story. It is common to hear “no-firm-date”, “future event”, “it’s on the roadmap, no we will not show you the road map”, “Customers are not asking for it”

IPv6 Infrastructure Requirements : Default IPv6 Transition

	OS	Protocol	Address
6 to 4	All	41	IPv4: 192.88.99.1 (Anycast) (Default) 192.88.99.0/24 (Default) IPv6: 2002::/16
	Public 6to4 Endpoints: http://www.ipv6tf.org/index.php?page=using/connectivity/6to4		
ISATAP	All	41	IPv4: isatap.
Teredo **Miredo**	2k/XP/Vista Linux/BSD/OSX	UDP 3544 (Default)	IPv4 : platform manual/automatic selection IPv6 : 2001:0000::/32
	Public Teredo Endpoints: http://www.sixxs.net/tools/aiccu/brokers/		

IPv6 Infrastructure Requirements : Tunnel

Provider	Coverage	Subnet	NAT	Mobility	RDNS	IRC	NIC handle	Config
Hurricane Electric www.he.net	United States, Europe (Germany, UK)	/64 /48 subnet	no	no	yes	yes	no	Website
SixXS www.sixxs.net	United States, Europe (13 countries), New Zealand[4]	/64 /48 subnet	yes	yes	yes	yes	yes	Website or TIC/AICCU (Linux)
Hexago/Go6 www.go6.net	United States, Canada	/48 subnet	yes	yes	yes	yes	no	Website or TSP

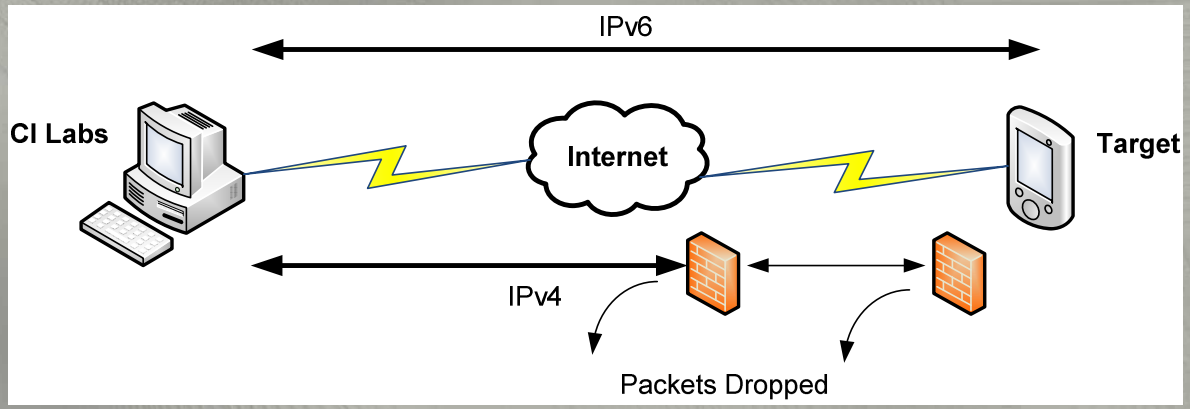
1. Provides enough addresses for a single system or a router for a network
2. All Have Commercial, Free Home user and Anonymous access

Common Vulnerabilities and Tools

Top 7 Common IPv6 Vulnerabilities

1. **IT & Security Management**
   - Unaware of the risk, unwilling to fund
2. **Network Administrator, System Administrator, Security Administrator**
   - IPv6 is already on your system, do something about it!
3. **Security Auditors/Testers**
   - If you are not testing for IPv6, then compliance testing you are doing is NOT VALID! I wonder if your customers know this?
4. **IPv6 capable Firewalls**
   - Not installed/enabled/configured
5. **IPv6 capable IDS/IPS**
   - Not installed/enabled/configured
6. **Security Product Industry**
   - Not (or at least not fully) supporting IPv6 in their product line
7. **Un-patched Systems**
   - Apply security patches (70+ IPv6 specific vulnerabilities)

Example of all 7 issues



IPv4

IPv6

```
C:\Users\dbg1.000>ping 68.247.18.13
Pinging 68.247.18.13 with 32 bytes of data:
Ping statistics for 68.247.18.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\dbg1.000>tracert
Tracing route to 2002:44f7:120d::44f7:120d over a maximum of 30 hops
  1    4 ms    2 ms    2 ms  2610:f8:c38::1
  6   622 ms   389 ms   444 ms  2002:44f7:120d::44f7:120d

Nmap Scan showed the following ports were open:
80, 113, 135, 137, 5980 (ephemeral), WAP Push, blackjack, SQL…
```

V4 Firewalled

V6 Open!!!

IPv4	68	247	18	13
IPv6	44	F7	12	0d

DEFAULT 6to4 Tunnel!

IPv6 Tools

IP Lookup

- **Address Information** – Breaks down the meaning of the address
- **Related IP Addresses** – Returns NS lookup and IPv4/IPv6 addresses
- **IP owner info** – Whois reverse lookup
- **Domain owner info** - Whois IPv4/IPv6 record
- **Conversions (ipv4/IPv6)** – Conversion between IPv6 and Ipv4
- **Ping** – ICMPv6
- http://ip-lookup.net/tools.php

IPv6 Tools

WiBerg IP-Tools

- Ping & ping6
- Traceroute and Traceroute6
- Nslookup
- Whois
- http://www.wiberg.nu/iptools.php

IPv6 to IPv4 Website Gateway

- On IPv6 and want to check IPv4 websites
- http://ipv6gate.sixxs.net

IPv4 to IPv6 Website Gateway

- On IPv4 and want to check IPv6 websites
- http://ipv4gate.sixxs.net

IPv6 Tools

NMap 4.60 - fyodor

- TCP scan (-sT)
- Connect-style ping scan (-sP)
- List scan (-sL)
  - Notes: Must
    - Specify the -6 option
    - Provide IPv6 numbers or DNS names
      Service scan
- http://nmap.org/

- Many IPv4 options do not work on IPv6!
- You can not scan IPv4 and IPv6 at the same time!
- You can not provide a range of addresses

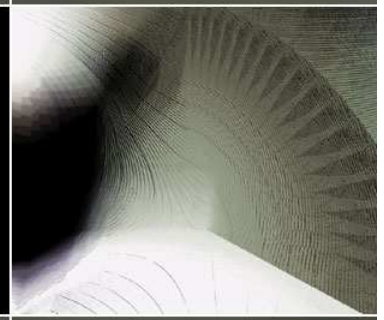
IPv6 Tools

THC-IPV6 - van Hauser

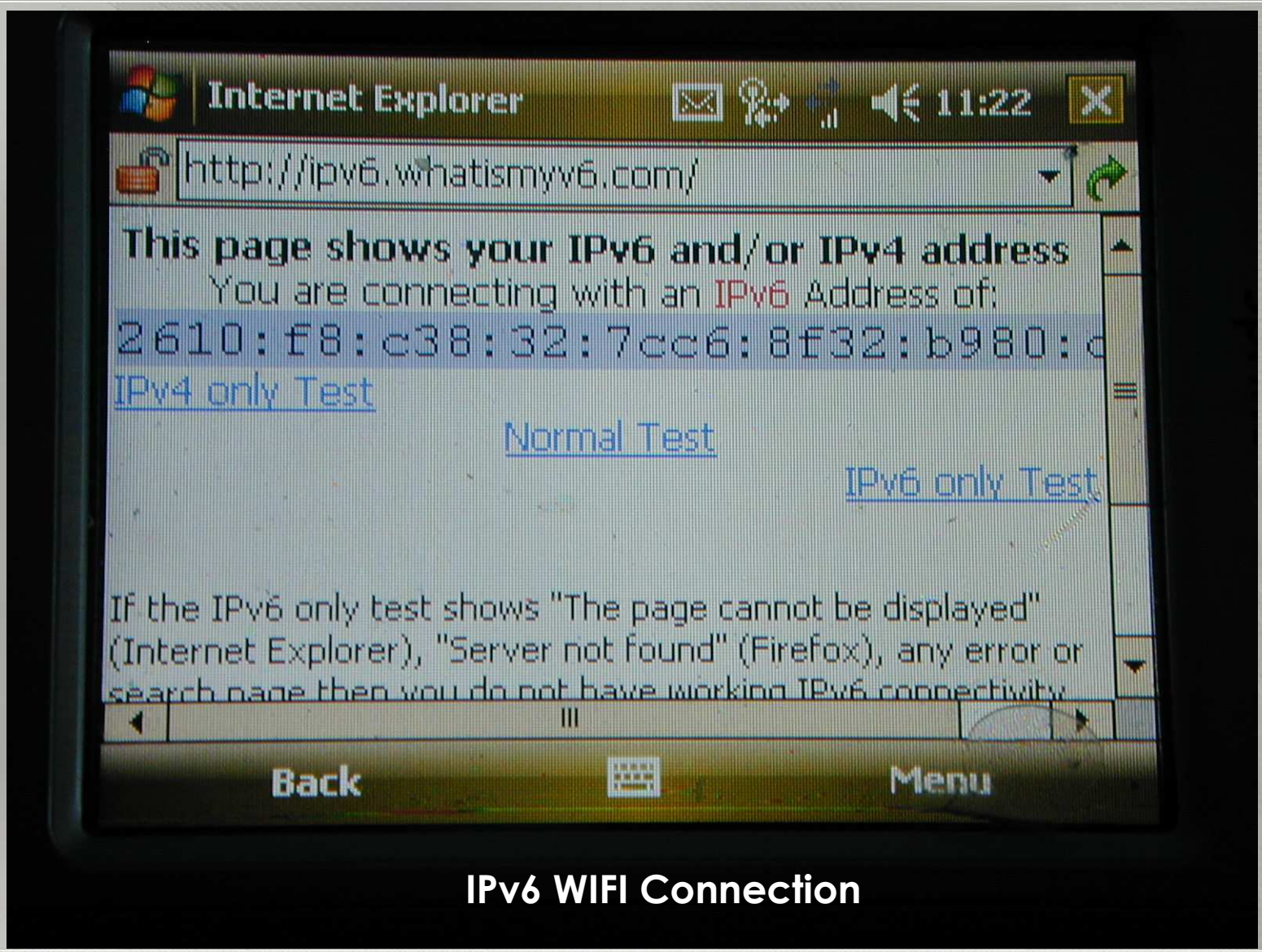
- **PARSITE6** - ICMP Neighbor Spoofer for Man-In-The-Middle attacks
- **DOS-NEW-IPV6** - Denial any new IPv6 system access on the LAN (DAD Spoofing)
- **REDIR6** - Redirect traffic to your system on a LAN
- **FAKE_ROUTER6** - Fake a router, implant routes, become the default router, …
- **SMURF6** - Local Smurf Tool (attack you own LAN)
- **RSMURF6** - Remote Smurf Tool (attack a remote LAN)
- **TOOBIG6** - Reduce the MTU of a target
- **Alive6** - Find all local IPv6 systems, checks for aliveness of remote systems
- **Protocol Implementation Tester** - Fragmentation + Routing Header, Mass Headers, Invalid Pointers and more
- http://freeworld.thc.org/releases/thc-ipv6-0.7.tar.gz

Demo? Interested?

An example of IPv6

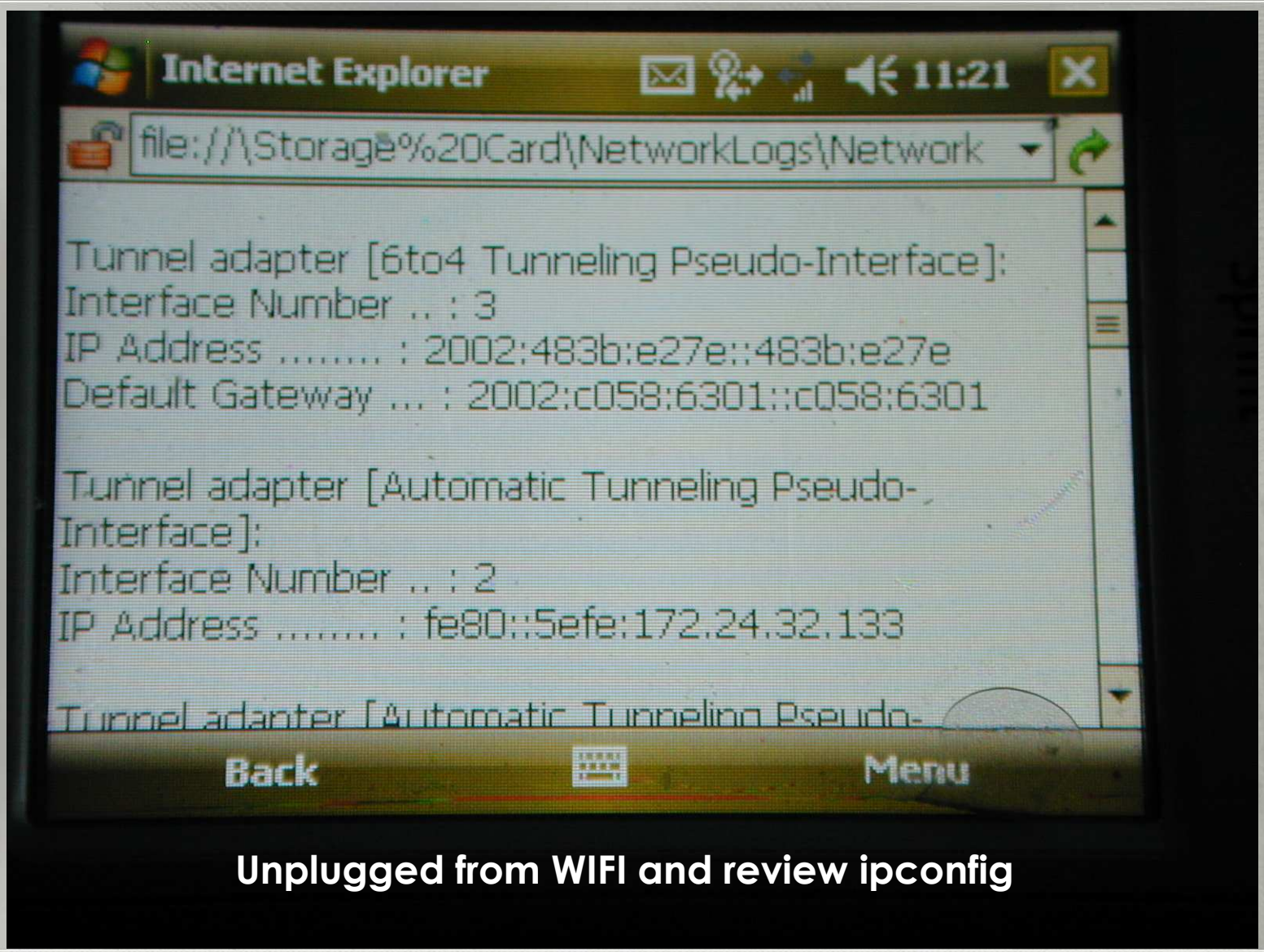


Identifying if phone supports IPv6



IPv6 WIFI Connection

Identify the IPv6 Address



Unplugged from WIFI and review ipconfig

A Bit more Poking

- **Restart Phone:**

  Tunnel adapter [6to4 Tunneling Pseudo-Interface]:
  Interface Number .. : 3

  IP Address ..... : 2002:44f5:6ee1::44f5:6ee1

  Default Gateway ... : 2002:c058:6301::c058:6301

- 2002:: It's running 6to4
- FE80::5efe:<IPv4 Address> It's ISATAP Enabled

- It's the same Gateway on both
- Try again with browser, not connected to WIFI

- **What can we still do with the IPv6 addresses…**

What is the IPv4 Address Ranges?

First IPv6 Address on Phone

IPv6 Address	48	3b	e2	7a
IPv4 Address	72	59	226	122
IPv4 Block Range	72.56.0.0 - 72.63.255.255			

Second IPv6 Address on Phone

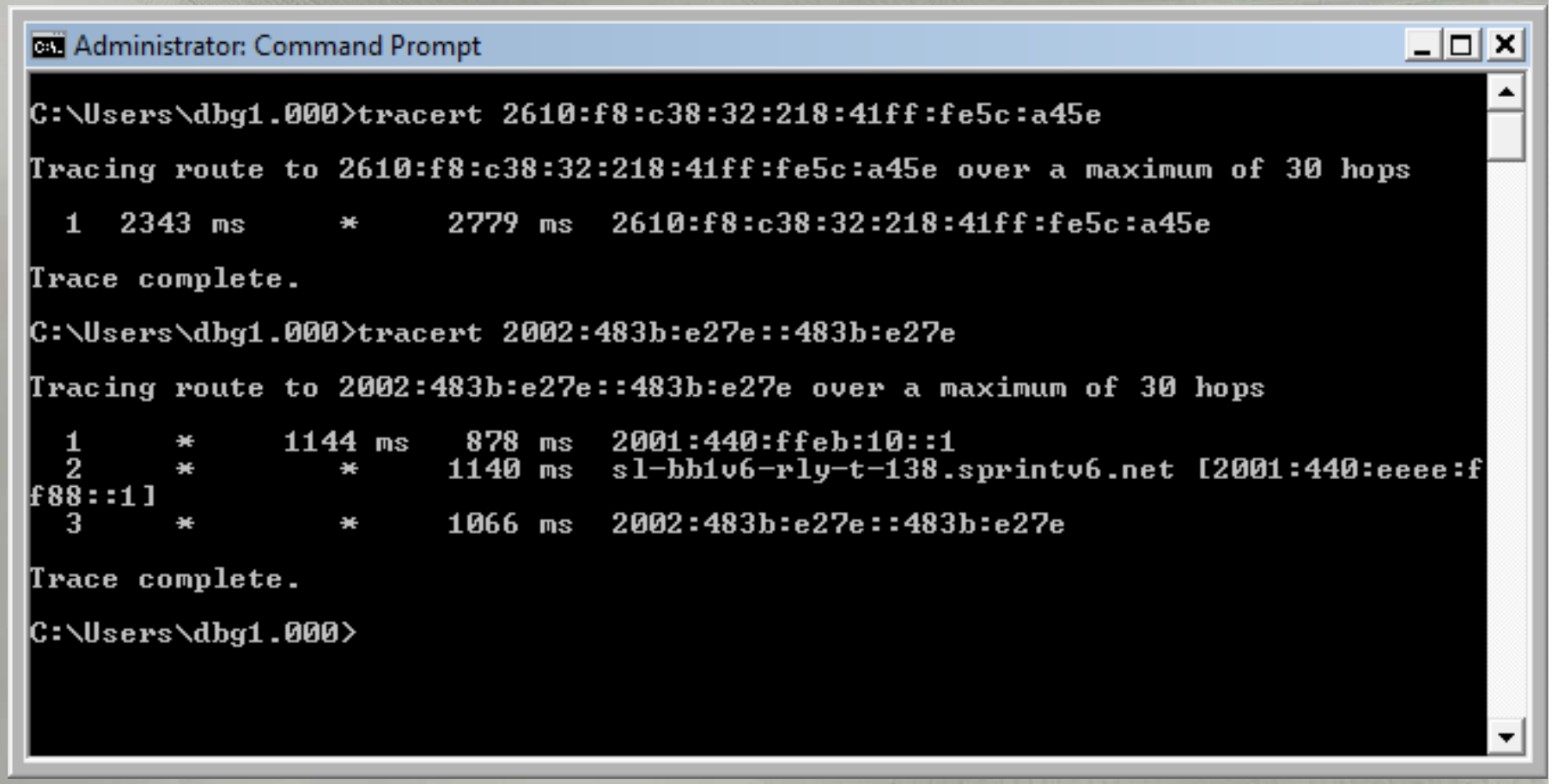
IPv6 Address	:	44	f5	:	6e	e1	
IPv4 Address		68	. 245	.	110	.	225
IPv4 Block Range	68.240.0.0 - 68.247.255.255						

The Gateway (Inside to out)

IPv6 Address		c0	58		63		1
IPv4 Address		192	. 88	.	99	.	1

But Can I traceroute and ping the IPv6 addresses?

Traceroute to Target



Traceroute from an
IPv6 connected network to the phone
But can we port scan the IPv6 address?

Can we Port Scan it?

2 yrs, 1.5 years, and Three Months ago:

- **IPv4**
  - No ports open
- **IPv6**
  - 80, 113, 135, 137, 5980 (ephemeral), WAP Push, blackjack, SQL…
  - Does anyone know which OS this is?

Can we Port Scan it?

Two Weeks ago:

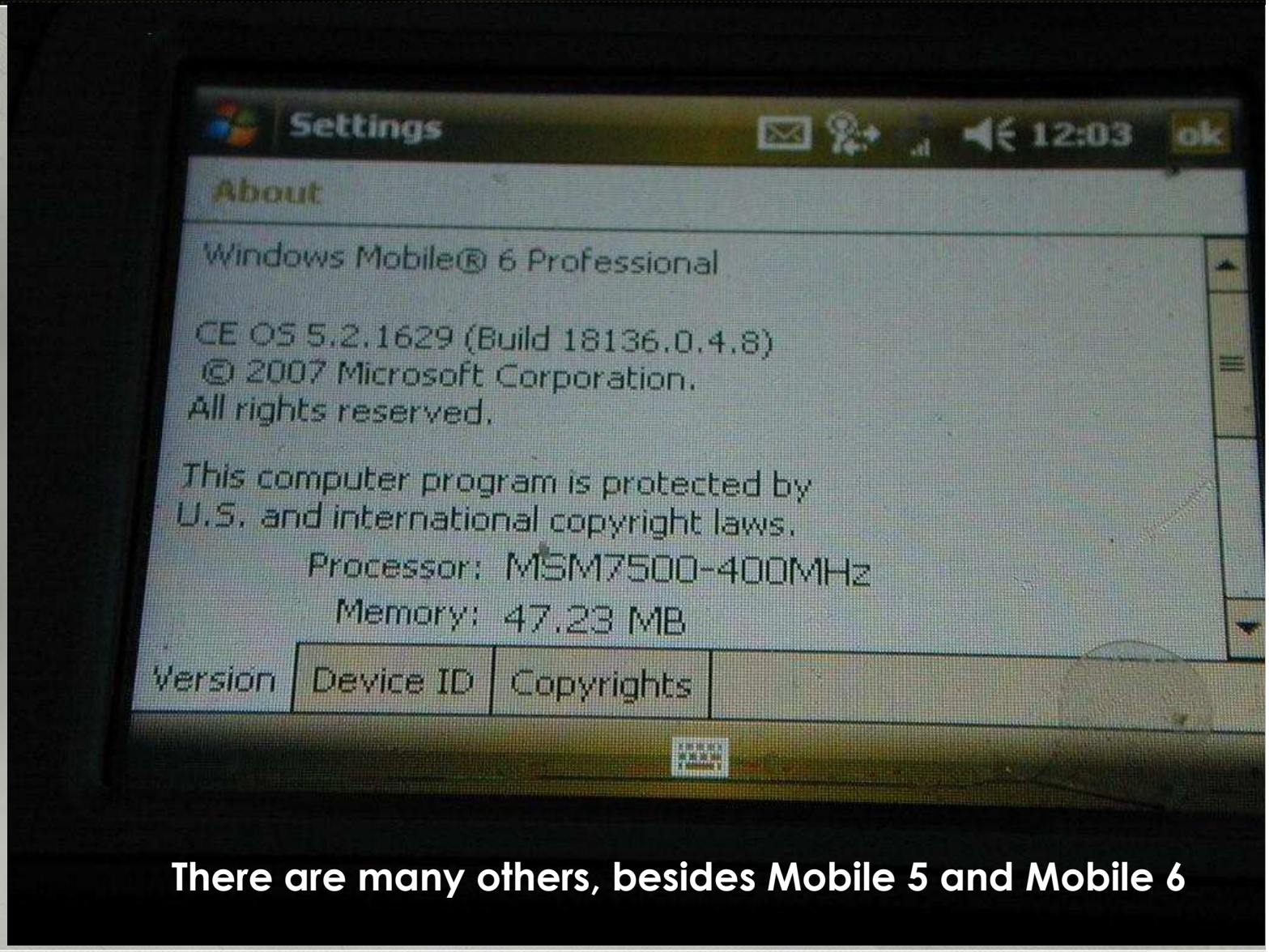
- After I publishing the date of this presentation… things changed
- Default 6to4 gateway, was installed internally
- DNS AAAA was disabled
  - No more browsing IPv6 websites via the provider data network, bummer.
- IPv4 shows
  - All ports filtered
- IPv6
  - Nmap responses with, no ports open… But
    - Data service on the phone fails
    - The battery of the life dramatically reduces
    - The device gets "HOT" – Required a reboot for the device to begin working as before

Insert Badness Here

Good Stuff

Censored

What Operating System are we running?

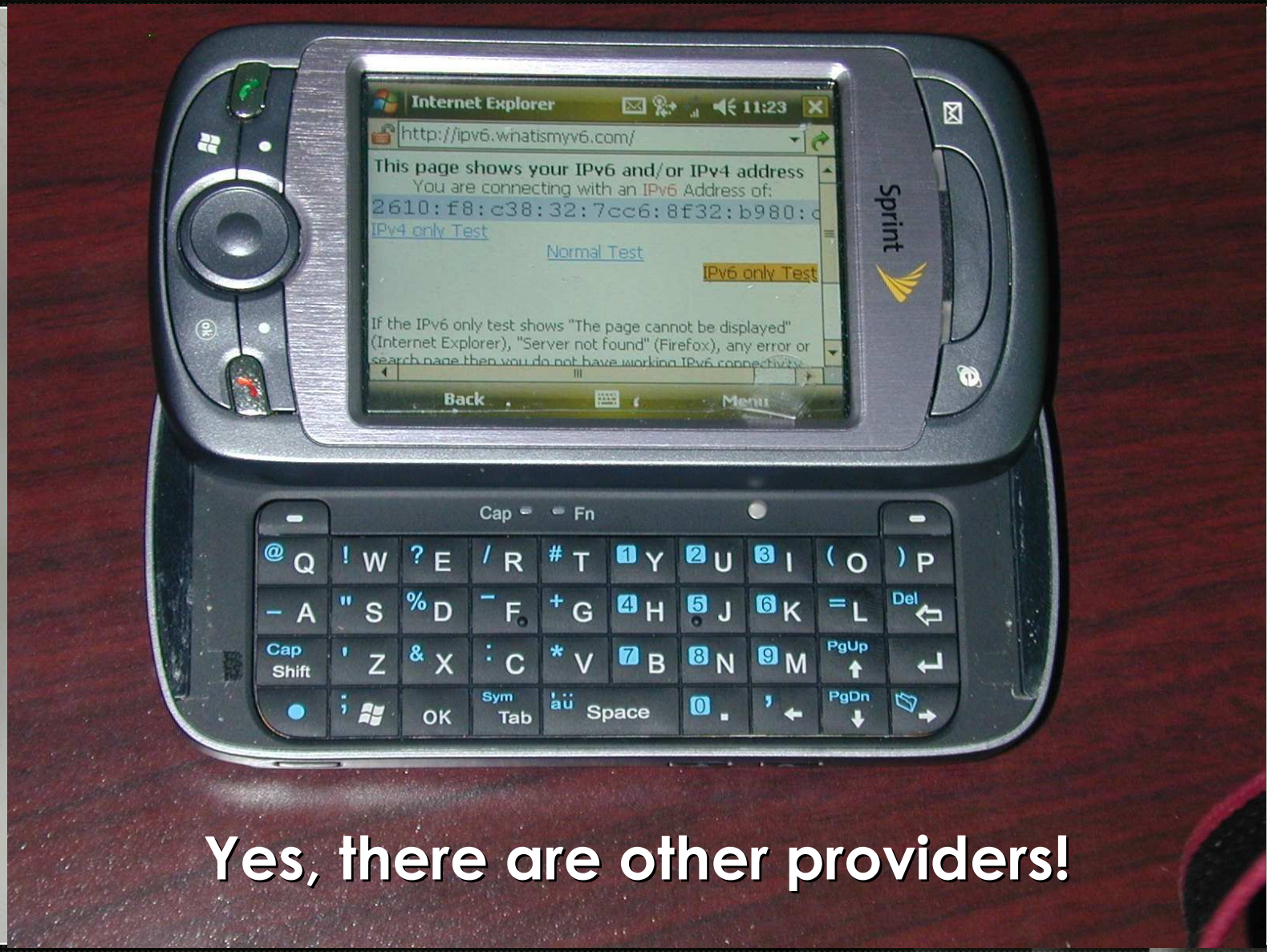


There are many others, besides Mobile 5 and Mobile 6

Are there Other Phones?

Yes, many more, here are a few….

And the Provider?



Yes, there are other providers!

THE LAST HOPE

IPv6, the Next Generation Network Playground - How to Connect and Explore

Joe Klein
ipv6sec@gmail.com