IPv6 Security

Ruy Flávio de Oliveira
Product Manager – Security Solutions

Agenda

- Fundamentals
- Differences between IPv4 and IPv6
- What doesn’t change
- Final Considerations

Fundamentals

Why IPv6?

- The simple answer
  - IPv4 address exhaustion
- Added benefits
  - Eliminates the network need for address translation (PAT, NAT)
  - Simplifies address assignment and renumbering when changing providers (problems stated in RFCs 2071 and 2072) rendering CIDR obsolete
  - Stateless Address Configuration
  - Jumbograms
  - …

IPv4 Exhaustion

- **Why?**
  - **Mobile Devices (3G, DTV, …)**
  - **Always-on connections**
  - **Internet demographic growth**
  - **Inefficient address assignment**
- **Mitigation**
  - **NAT, PAT, Private Networks**
  - **DHCP**
  - **Tighter assignment controls**
  - **Address reclaiming**

IPv4 Exhaustion

- In 2003 – Exhaustion by 2023, according to current allocation criteria
- In 2005 – Exhaustion in 4 to 5 years
- In 2007 – Exhaustion by 2011

- Mitigation techniques can be (and have been) used to extend this deadline, but not by much

IPv6 Address Dimension

- IPv4 – 2^{32} addresses, or ~4.3 billion addresses
- IPv6 – 2^{128} addresses, or ~3.4×10^{38} addresses
  - ~3,400,000,000,000,000,000,000,000,000,000,000,000
  - ~5×10^{28} addresses to each person alive today (6.5 billion)
    - 50,000,000,000,000,000,000,000,000 addresses per person
  - ~ 4,503,599,627,370,500 to each star in the known universe

Problems for IPv6 adoption

- Legacy equipment
- Ensuring equipment has sufficient resources to handle IPv6
- Investments in developing software for IPv6 support
- Publicity to persuade end-users to prepare to upgrade existing equipment
- Publicity to inform end-users to create demand for IPv6-capable equipment
- ISPs not preparing for IPv6

Who pays the bill???

And what about Security?

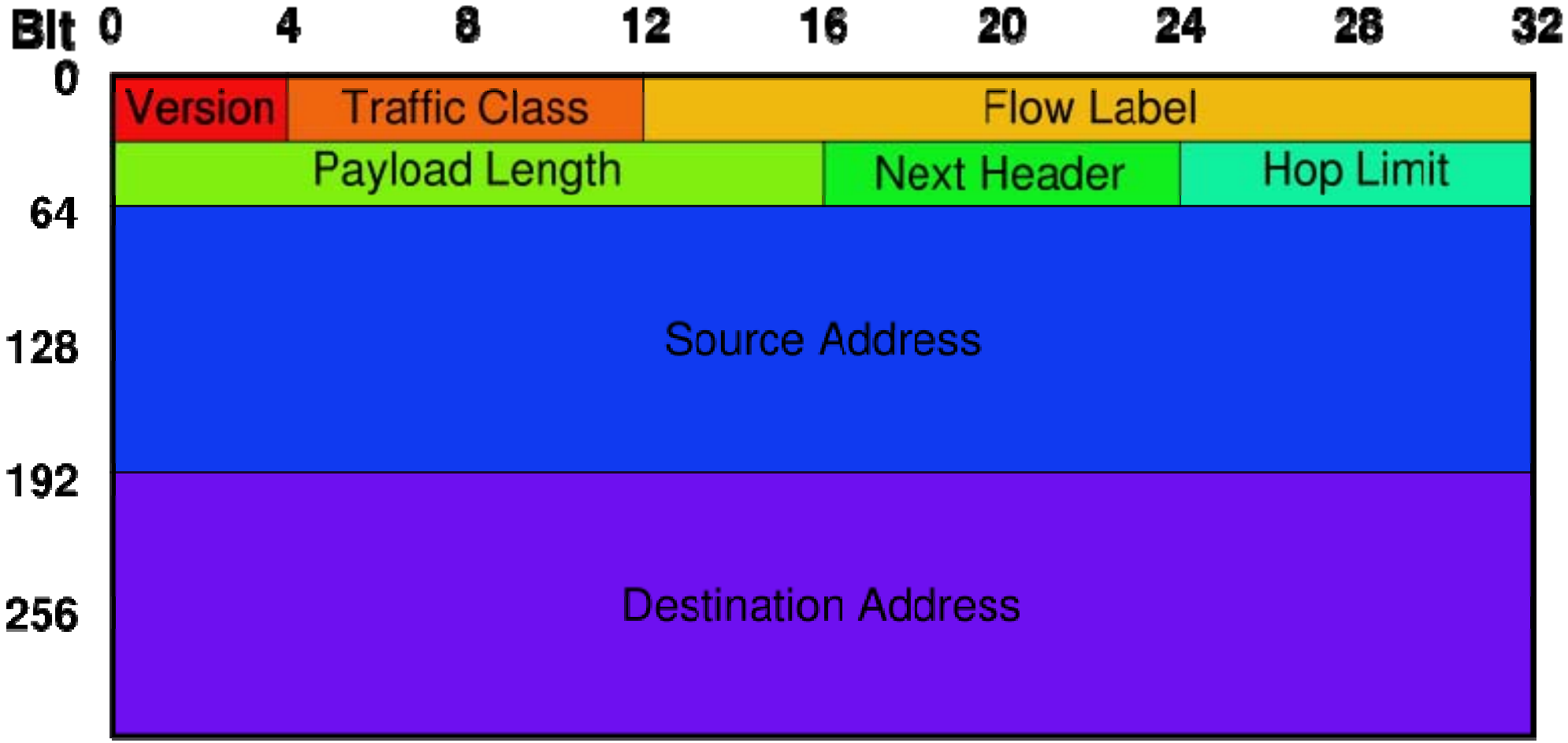
“…our soldiers need better information in order to make better decisions—who to help and who to kill. The lack of security and flexibility in the current IPv4 protocol is a drag on our wing. This isn't about do you trust the Internet for your kid's homework, it's do you trust your kid's life. If we fail, people die.”

John Osterholz
Director of Architecture and Interoperabilty, DoD
***Market Wire*, June 26, 2003**

How does IPv6 security supposedly work?

- IPsec
- NAT returns to its original purpose
  - Security
- IP address scan is an intractable problem

IPv6 Packet



IPv6 Packet

- Version – IPv4 or IPv6
- Class and Flow Label – fields related to real time traffic
- Payload Length – data size following the header
- Next Header
  - *Hop-by-Hop options*
  - Routing
  - Fragmentation
  - *AH: Authentication Header*
  - *ESP: Encrypted Security Payload*
  - Destination options
- Hop Limit – replaces TTL

Translation:
IPsec is mandatory

Differences Between IPv4 and IPv6

IPv6 IPsec support

- **IPSec is mandatory**
  - **Configuration and use is identical in IPv4 and IPv6**
- **Use, however is *not* mandatory**
- **Although it dates from 1995, it's still scarcely adopted outside L2TP-based VPNs**
  - **Much more ubiquitous support for TLS and its predecessor SSL**
  - **IPsec and NAT don't mix well**

A small digression: IPsec vs SSL

- **IPsec > SSL**
  - **Provides better protection for packet headers**
  - **Provides confidentiality, accountability, and authentication**
  - **No more spoofed headers, etc.**
- **SSL > IPsec**
  - **It's here right now**
  - **Works well for just about everything you want to do**

IPv6 and NAT

- **NAT won’t go away in IPv6**
  - **Instead, it will be used for its original purpose: to add security by screening internal networks from the outside**
  - **NAT is cheap to implement and easy to configure**

IPv6 and address sparsity

- Many IPv4 worms and cracking tools do scans of IPv4 address space to find hosts
- IPv6 increases the size of the address space by over 79,000,000,000,000,000,000,000,000,000 times
  - Properties of the address structure can pare down the search space a little
  - Nevertheless, brute force search of IPv6 address space will be completely intractable
  - PRO – It does eliminate a primary technique of a great deal of malware (and some legitimate research efforts)
  - CON – Lists of hosts to attack will be harvested from system configuration files, e-mail addresses, Web sites, server logs, etc.

IPv6 and MAC addresses

- **Standard IPv6 addresses contain the MAC address in the lower 64 bits of the addresses**
  - **This is information that was usually confined to a single broadcast domain before**
  - **The manufacturer of your NIC is now public knowledge and may associate you with a known vulnerability**

What doesn’t change

Things that stay the same in IPv6

- IPv6 doesn’t change TCP or UDP at all
- IPv6 doesn’t patch vulnerabilities in individual applications or OSes
- IPv6 doesn’t force network administrators to do outgoing traffic filtering (egress filtering)
- IPv6 doesn’t make mandatory the use use of any security features

Things that stay the same in IPv6

- A recent survey of CERT's top 100 vulnerabilities shows only one of them to be specific to IPv4
- IPv6 still elicits
  - e-mail trojans
  - buffer overflow
  - macro viruses
  - SYN floods
  - RST attacks
  - OS fingerprinting
  - hijacked connections
  - …

Code Maturity

- Most of the IPv6 code in the world is new and untested in comparison to IPv4
- IPv6 code potentially contains more deficiencies and vulnerabilities than its IPv4 equivalents
  - It's larger and much more complex
  - It has not yet stood the test of time—or attacks
- This situation will slowly improve over time
  - IPv6 isn't low-hanging fruit yet, so there's little motivation to attack it

New code, new vulnerabilities

- **Deficiencies will be opened in existing applications as they are ported from IPv4 to IPv6**
  - **IPv6 involves many more programming changes than just bigger addresses**
- **New code will be written to interface with (or reinvent) third-party libraries that do not handle IPv6 and cannot be modified**

Router Maturiry

- Issues with code and protocol maturity come together in the routers
  - A vulnerable host may result in the loss of a single system
  - A vulnerable router may result in the loss of a substantial piece of the network
- Circular reference: router vendors can’t spend too much on testing IPv6 stacks until IPv6 gets more popular, and IPv6 can’t get more popular until router vendors spend more time testing their IPv6 stacks

Final Considerations

Best Practices

- Be prepared to devote considerable resources to development and maintenance of key infrastructure if you plan to use IPsec
- Adopt new features of IPv6 sparingly until their standards processes are finalized
- Allow for the existence of more undiscovered deficiencies in IPv6 code when assessing risks
- Subject ported applications to the same level of review and testing as new ones

Best Practices

- Have clear definitions of “IPv6 ready” and “IPv6 aware” when you compare vendors’ products
- Pay close attention to new RFCs as they come out—and changes in the status of old ones
- Design new protocols in such a way that they will continue to operate through a NAT
- Don’t write IPv6-only applications; make them dual-stack instead

Conclusions

- So, is IPv6 more secure than IPv4?
  - At the moment? NO.
  - IPv6 does not make for a completely different world of security
- Expect a low level of incidents initially (obscurity), followed by a much higher level (exploitation), followed by a slow decline to the level we see now with IPv4 (stasis)
  - The “million dollar question”: how long will each level be?

Questions

Ruy Flávio de Oliveira
ruyf@cpqd.com.br
telefone: (19) 3705-4125

Thank You!