

Flow Label Filtering Feasibility

Orla McGann and David Malone

December 2005

Stateful filtering

- Packet filter examines each packet.
- Originally done in isolation.
- Stateful stored stuff about network state.
- Does IPv6 offer anything new.

IPv4 Header

Version 4 bit	Head Len 4 bit	ToS 8 bit	Total Length 16 bit	
ID 16 bit		Flags 3 bit	Frag Offset 13 bit	
Time to Live 8 bit		Protocol 8 bit	Header Checksum 16 bit	
Source Address (32 bit)				
Destination Address (32 bit)				
Options — <i>variable</i>				

IPv6 header

Version 4 bit	Traffic Class 8 bit	Flow Label 20 bit	
Payload Length 16 bit		Next Header 8 bit	Hop Limit 8 bit
Source Address 128 bit			
Destination Address 128 bit			

Proposal

- Filter on flow label.
- Learn one direction from SYN.
- Learn other from SYN/ACK.
- Requires flowlabel to be fixed.
- Currently supposed to be immutable.

Is it actually constant?

- Measure how host/net behaves.
- Initial ad hoc testing.
- Gather list of IPv6 web servers.
- Fetch page and monitor flow label.

Initial results

- 60% of hosts set zero flow label.
- FreeBSD missing code for outgoing.
- Inconsistent on incoming.
- Found that SYN/ACK had different label.

FreeBSD

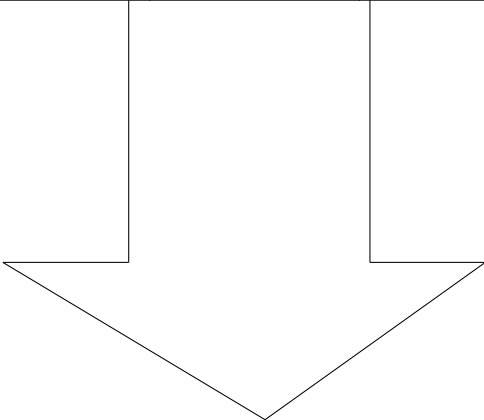
Syncache/Syncookie

- No traditional setup code.
- Syncache uses small PCB.
- Syncookie
INS = hash(IPs, sequencenumber, index).
- `/* ip6_flow = ??? */`

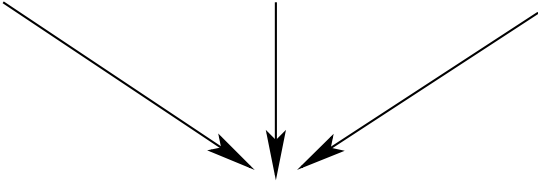
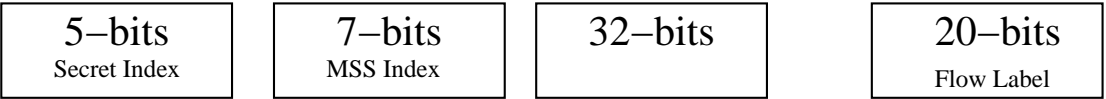
Fix

Syncache/Syncookie

- Syncache: choose any flowlabel.
- Syncookie: Must be able to reconstruct from ACK.
- Hash produces many bits, use some for flowlabel.
- If syncookies disabled could also use sequential/...



MD5 HASH



Measurements of Flow Label Consistency

TCP Hosts	Hosts	%
Flow Label set to something other than 0	427	39
Flow Label = 0	784	
Consistently setting Flow Label to 0	678	61
Flow Label to 0, change after handshake	106	
Flow Label to non-0	321	
Consistently set the Flow Label	84	20
Inconsistently set the flow	343	80

Considerations

- Do we strictly filter?
- Do we allow 1 change early in lifetime?
- Don't want to open DoS chances.
- How do we find flow ID for RST packets?

Thanks, Questions?