Enhanced IP

Dr. William Chimiak, Sam Patton, Stephen Janansky

What are we trying to do?

Experimental Solution for IPv4 Address Depletion

Introduction

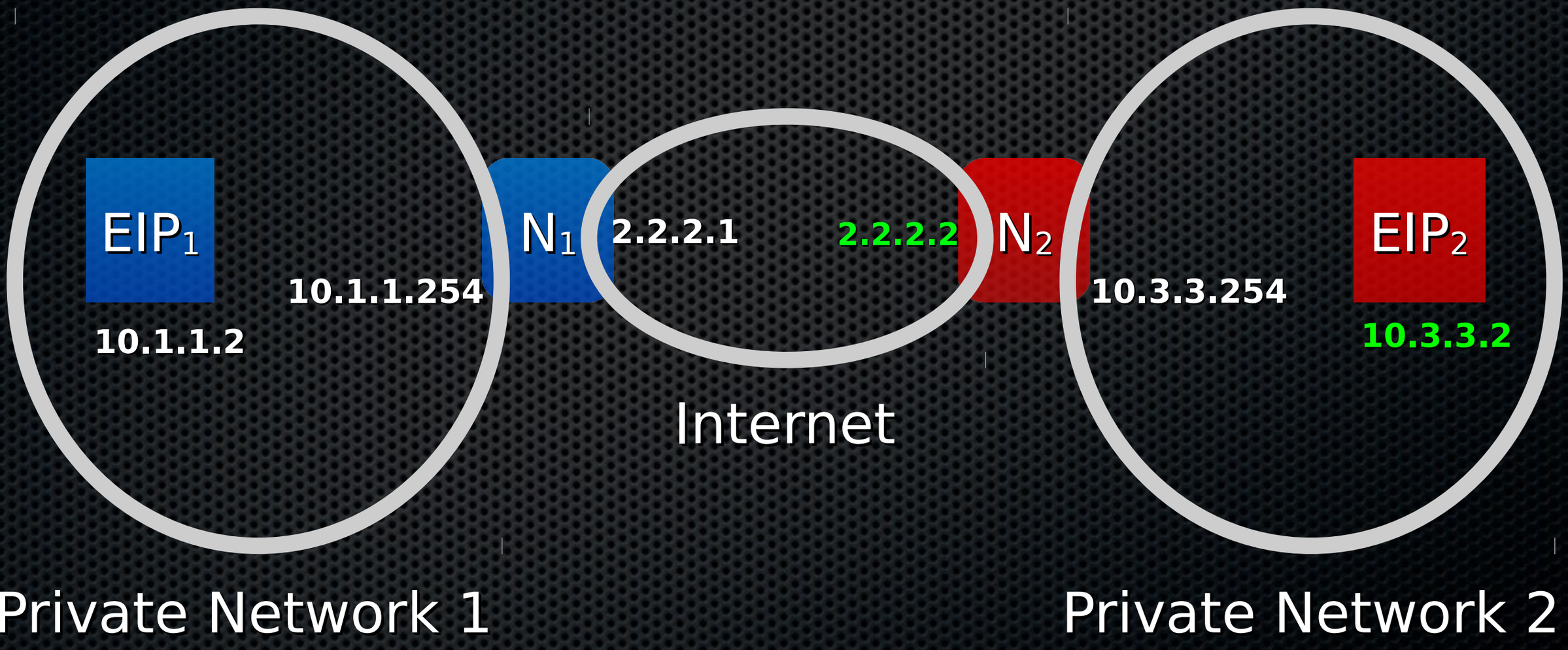
- Introduction of a new protocol (Enhanced IP)
- Security Considerations
- Transition Requirements
- Proof of Concept Implementation
- Things that still need work

Enhanced IP

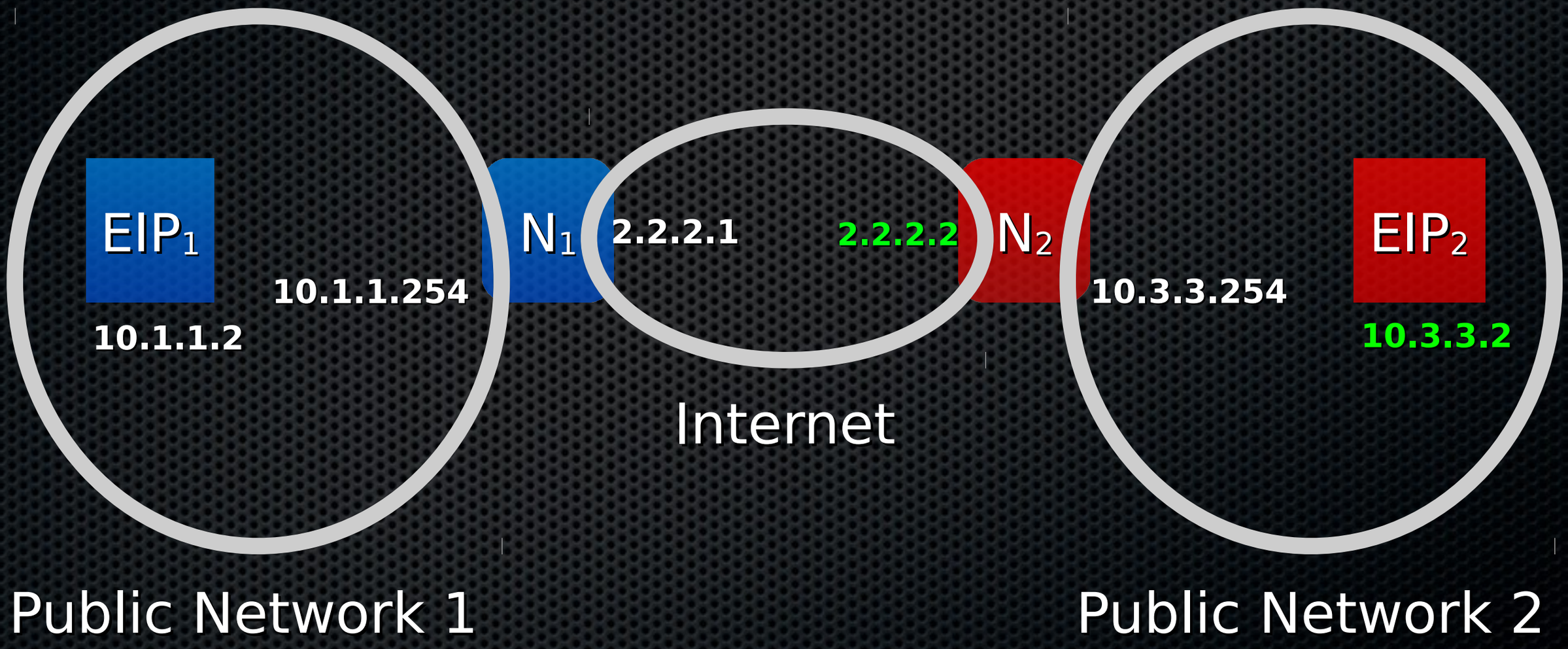
Enhanced IP

- 64-bit Enhanced IP
- **2.2.2.2.10.3.3.2**
- All Enhanced IP addresses have a site address and a host address
  - Site address: 2.2.2.2, is used to route packets over the public Internet to a router/NAT that is aware of Enhanced IP packet format.
  - Host address: 10.3.3.2, used to route packets to a node behind the router/NAT that has the outside address of 2.2.2.2

Enhanced IP Network



Enhanced IP Network



Enhanced IP

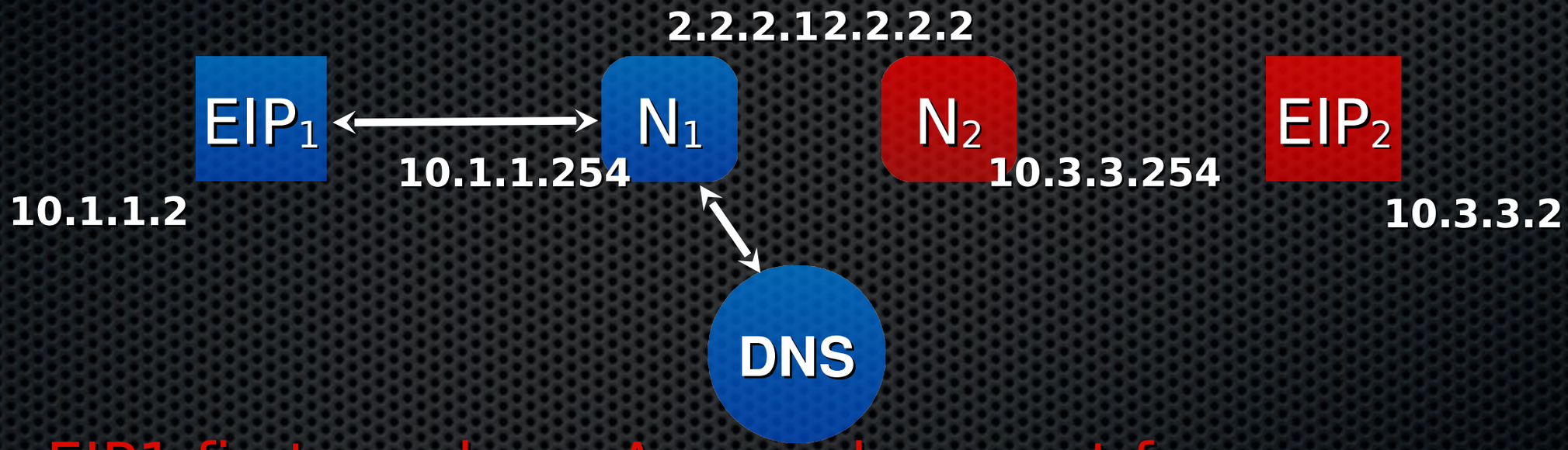
- Minimal changes at layer 2 and 3 of OSI to implement
  - does not replace ARP, routing protocols
- Uses IP Option 26 to extend the length of the IP header, 12 bytes per packet
- The NAT functionality used in Enhanced IP is stateless as opposed to the stateful nature of IPv4 NAT.
- Over time IP Option 26 MUST become part of fast path implementations.

Version	IHL	ToS	Total Length
Identification		Flag	Fragment Offset
Time to Live	Protocol	Header Checksum	
10.1.1.2			
2.2.2.2			
0x9a	12	0	1	0
255.255.255.255			
10.3.3.2			

Version	IHL	ToS	Total Length	
Identification			Flag	Fragment Offset
Time to Live	Protocol	Header Checksum		
2.2.2.1				
2.2.2.2				
0x9a	12	1	1	0
10.1.1.2				
10.3.3.2				

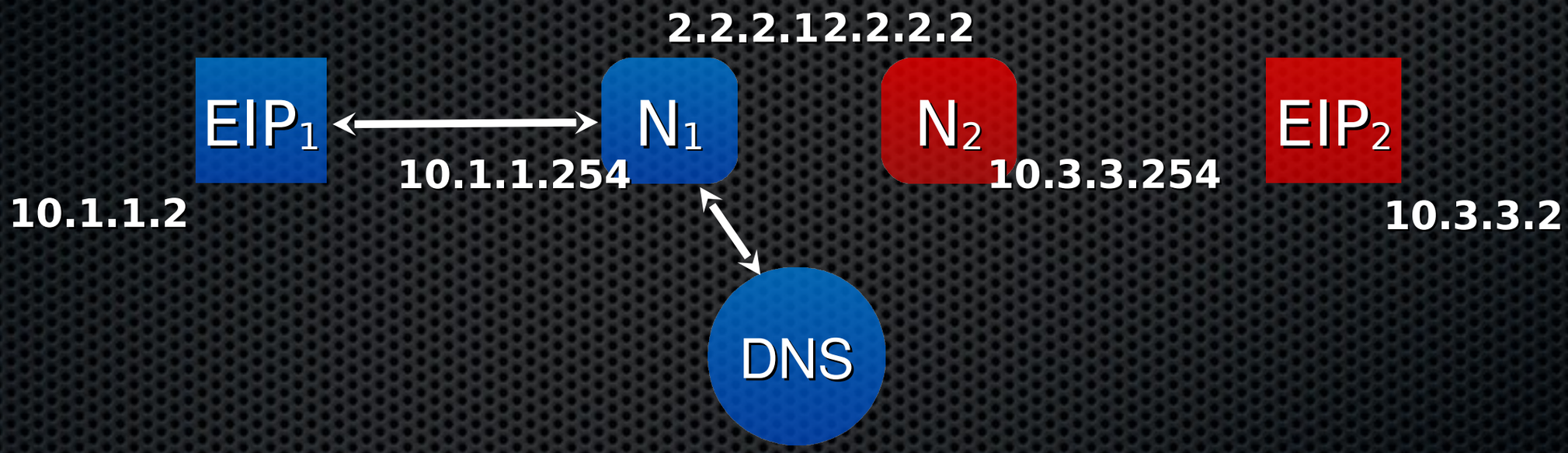
Version	IHL	ToS	Total Length	
Identification			Flag	Fragment Offset
Time to Live	Protocol	Header Checksum		
2.2.2.1				
10.3.3.2				
0x9a	12	1	0	0
10.1.1.2				
0.0.0.0				

DNS: Using AAAA to lookup 64 bits



- EIP1 first sends an A record request for eip2.somesite.com and receives a failure back because there is no A record.
- EIP1 then sends a AAAA request for eip2.somesite.com and receives back 2001:0101:0202:0202:0a03:0302::0

DNS: Using AAAA to lookup 64 bits



2001:0101:0202:0202:0a03:0302::0 is really 2.2.2.2.10.3.3.2

Code

- Patches for Linux NAT
- Patches for OpenWRT
- Linux client/server
  - Runs ssh, samba, apache, firefox, etc, without modification or recompile of programs
- Versions of ping & traceroute that include IP options, netcat-like program

Security Considerations

- Similarly to IPv6, Enhanced IP means increased connectivity for IP addresses that were previously unreachable because of NATs.
- Firewall software is not presently aware of Enhanced IP addresses.
- Enhanced IP NAT devices must only forward packets to networks that are directly connected (e.g. 10.0.0.0/8)

Enhanced IP: Transition

Our Assumptions

- The core of the Internet is closer to being ready to pass packets with IP options en masse than it is for passing IPv6 packets en masse.
- Edge networks will allow the packets we'll be introducing in this presentation if the economics of Enhanced IP makes sense to them.

What to do next?

- On Cisco
  - “ip options ignore”
- On Juniper
  - allow-ip-options 26
- Router not listed here:
  - Send command to sam@enhancedip.org

http://www.enhancedip.org/docs/router-references

What to do next?

- Please pass IP option 26
- Email: sam@enhancedip.org
- Tweet: @EnhancedIP
- www.enhancedip.org

Questions?

Useful socket options

- setsockopt(fd, IPPROTO_IP, IP_OPTIONS, optdata, len);
- kernel equivalent is kernel_setsockopt()

At a high level

- glibc changes to getaddrinfo - 2001:0101 needs to return a struct sockaddr_ein. As opposed to a struct sockaddr_in6.
- connect() changes in the kernel to support a new struct sockaddr type
- 8 line change in existing NAT code to bypass inspection of Enhanced IP packets
- New NAT netfilter module to perform Enhanced IP address swapping and checksum update functions.
- Subtracts 12 bytes from TCP MSS to account for overhead of larger IP header caused by including the 12 bytes of options.