OSPF MD5 Authentication

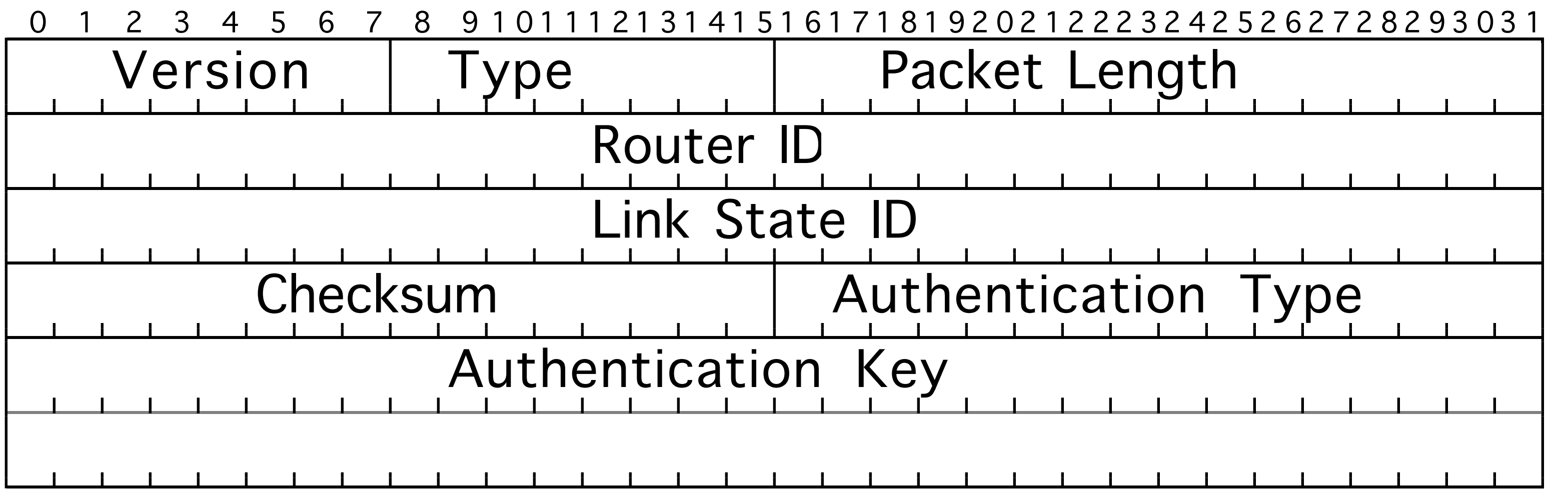
Fred Baker

Problem Statement

It Ain't Good Enough

- Today's OSPF runs either no authentication or simple password
- subject to attacks
- Proposal: Use MD5 with a sequence number

Present OSPF Header



OSPF Message under MD5 Authentication

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Version	Type	Packet Length	
Router ID			
Link State ID			
Checksum		Authentication Type = MD5	
Offset to Digest		Reserved	
Non-Decreasing Sequence Numbe			
OSPF PDU Contents			
MD5 Message Digest			
Zero or more bytes of pad			
64 bit message length			