

DNS – the protocol

David Morgan

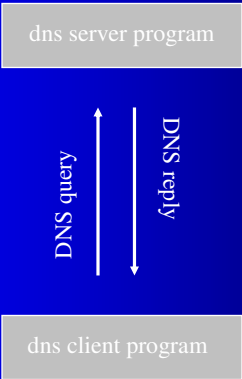
© David Morgan 2003-2015

DNS as a language

- spoken between pairs of programs
 - a dns client program, e.g., the resolver
 - a dns server program, e.g., BIND
 - they're written specially to speak it
- discussing server giving info it has, or gets, to client
- simple query-response behavior

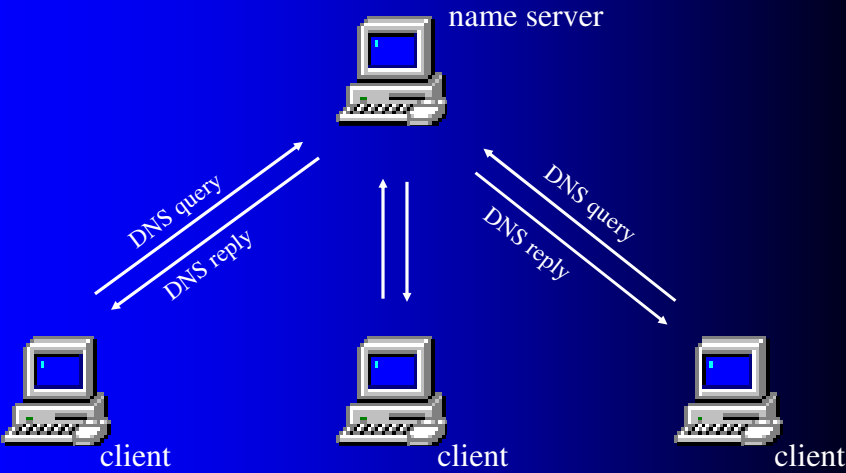
© David Morgan 2003-2015

A DNS conversation



© David Morgan 2003-2015

Typical configuration...



© David Morgan 2003-2015

DNS particles of speech

- DNS messages
- 2 kinds
 - query messages
 - reply messages
- both have same format

© David Morgan 2003-2015

DNS message format

Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
Questions (variable number)	
Answers (variable number of resource records)	
Authority (variable number of resource records)	
Additional info (variable number of resource records)	

© David Morgan 2003-2015

A DNS query

The screenshot shows a packet capture in Wireshark. The packet list pane shows two packets: a DNS Standard query (No. 1) and a DNS Standard query response (No. 2). The packet details pane for Frame 1 (76 on wire) is expanded to show the Domain Name System (query) section. The Flags field is circled in red, with an arrow pointing to the text "this is a query message (number F45E)". The Questions field is also circled in red, with an arrow pointing to the text "...containing the single question, 'What is the address...'. The Queries section shows a single query for "homepage.smc.edu" with type A and class inet, with an arrow pointing to the text "...for 'homepage.smc.edu'". The packet bytes pane at the bottom shows the raw hex and ASCII data.

© David Morgan 2003-2015

The DNS reply

The screenshot shows a packet capture in Wireshark. The packet list pane shows two packets: a DNS Standard query (No. 1) and a DNS Standard query response (No. 2). The packet details pane for Frame 2 (92 on wire) is expanded to show the Domain Name System (response) section. The Flags field is circled in red, with an arrow pointing to the text "this is a reply message (matches query number F45E)". The Answer RRs field is circled in red, with an arrow pointing to the text "the original query". The Answers section shows the response for "homepage.smc.edu" with type A and class inet, with an arrow pointing to the text "The answer to the query is, 'homepage.smc.edu's address is 198.147.67.246'". The packet bytes pane at the bottom shows the raw hex and ASCII data.

© David Morgan 2003-2015

Biblio

- RFC 1034 “Domain names - concepts and facilities”
- RFC 1035 “Domain names - implementation and specification”
- DNS and BIND, Albitz and Liu, O’Reilly, 4th ed. 2001, Appendix A “DNS Message Format and Resource Records”