

Troubleshooting DNS



Betty DuBois
PACKET DETECTIVE

@PacketDetective www.bettydubois.com



Module Goals



Isolate cause and resolve DNS outages

Identify single point of failure

Evaluate DNS error replies and slow responses



DNS Outage Common Causes

**Hardware or
network failures**

DDoS Attack

Human Error



Demo



Isolate and resolve two DNS outage scenarios



DNS Single Point of Failure

Best defense against single points of failure in networking

Fault tolerance, load balancing, and redundancy

Causes of single point of failure

1

Relying on a
single
Authoritative
provider

2

Not realizing
your backup
DNS provider is
in same
geographical
location

3

Not monitoring
DNS





Troubleshooting DNS Using Wireshark

Is it slow? Or is it no?



Users are complaining about slow access to the Internet

Checklist for silence, errors and slowdowns

- Can you ping the outside?
- Can you ping the local Resolvers?
- Are there errors? Log files or packets?
- What is the response time?
 - Is there a pattern in the slows?



Demo



Silence

Error responses

Slow responses



Summary



Isolate cause and resolve DNS outages

Identify single point of failure

Evaluate DNS error replies and slow responses



Up Next:
Securing DNS

