

Analyzing the TCP/IP Resolution Process

Port, Name, Route and Hardware Address
Resolution

Laura Chappell

Founder | Wireshark University

SHARKFEST '08

Foothill College

March 31 - April 2, 2008

Contents

Scenario

Building the Packet

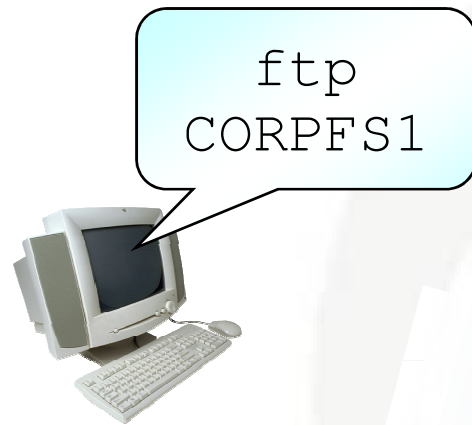
Port/Name Resolution

Local MAC Resolution

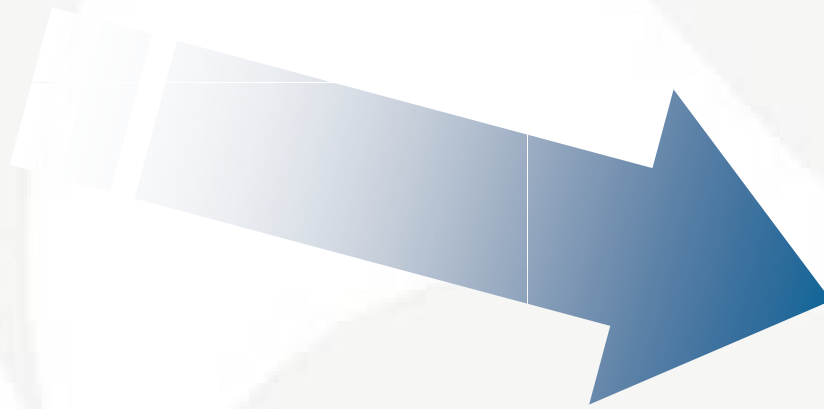
Route and MAC Resolution (Remote Target)

Complete TCP/IP Resolution Process

The Scenario



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

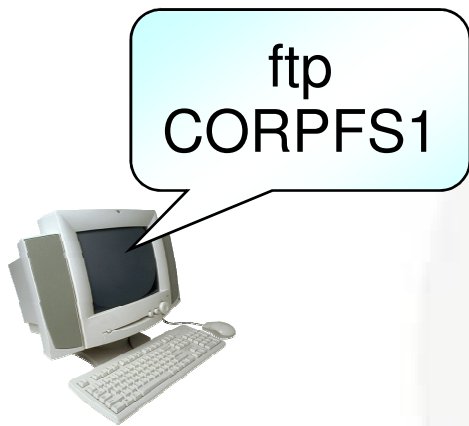


CORPFS1

MAC: B
IP: 10.2.99.99

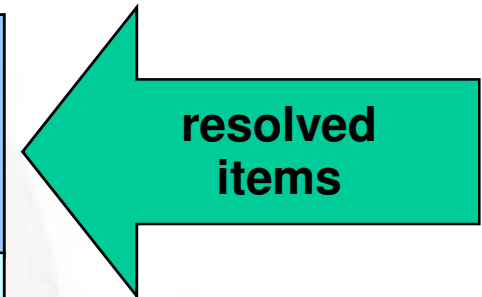


Building the Packet



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

Eth	Destination MAC:	?
	Source MAC:	A
	EtherType:	0x0800
IP	Protocol:	6 (TCP)
	Source IP:	10.1.0.1
	Destination IP:	???????
TCP	Source Port:	?????
	Destination Port:	??

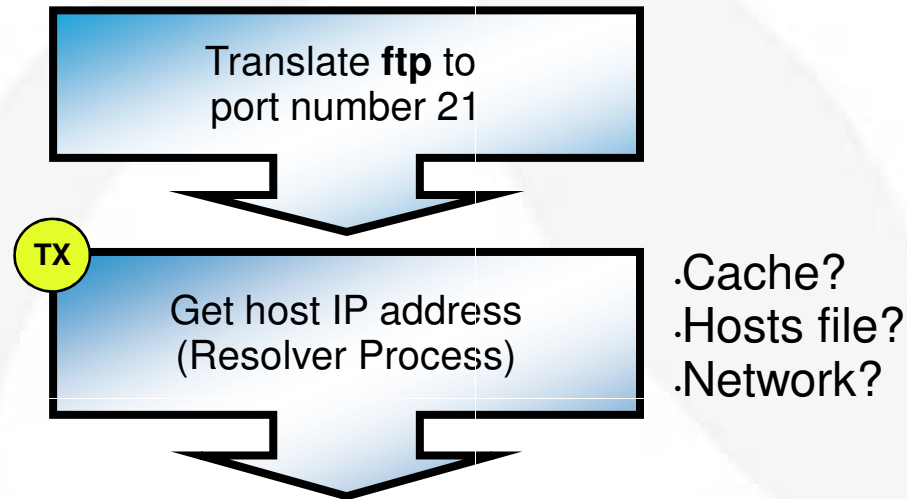


CORPFS1

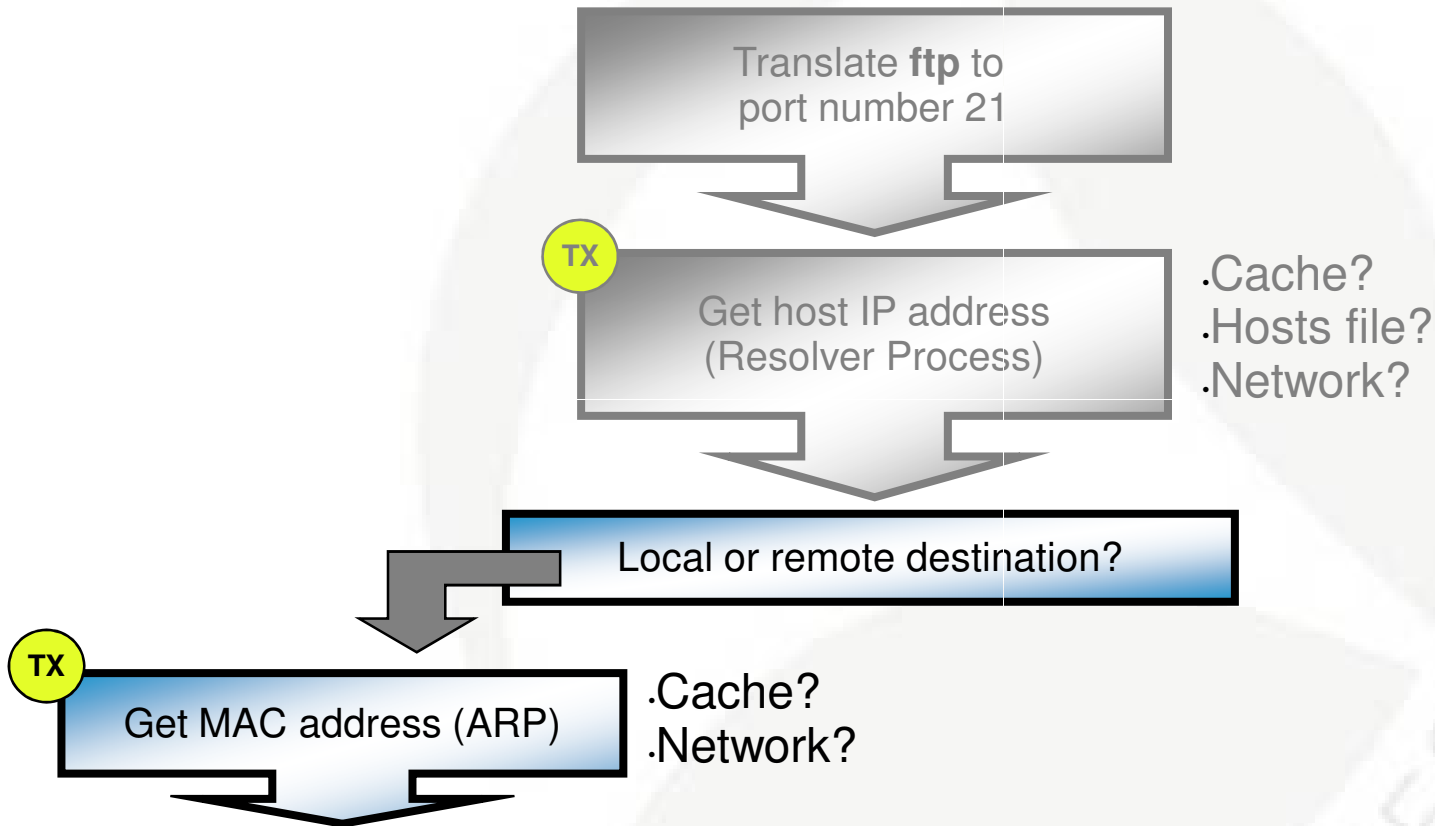
MAC: B
IP: 10.2.99.99



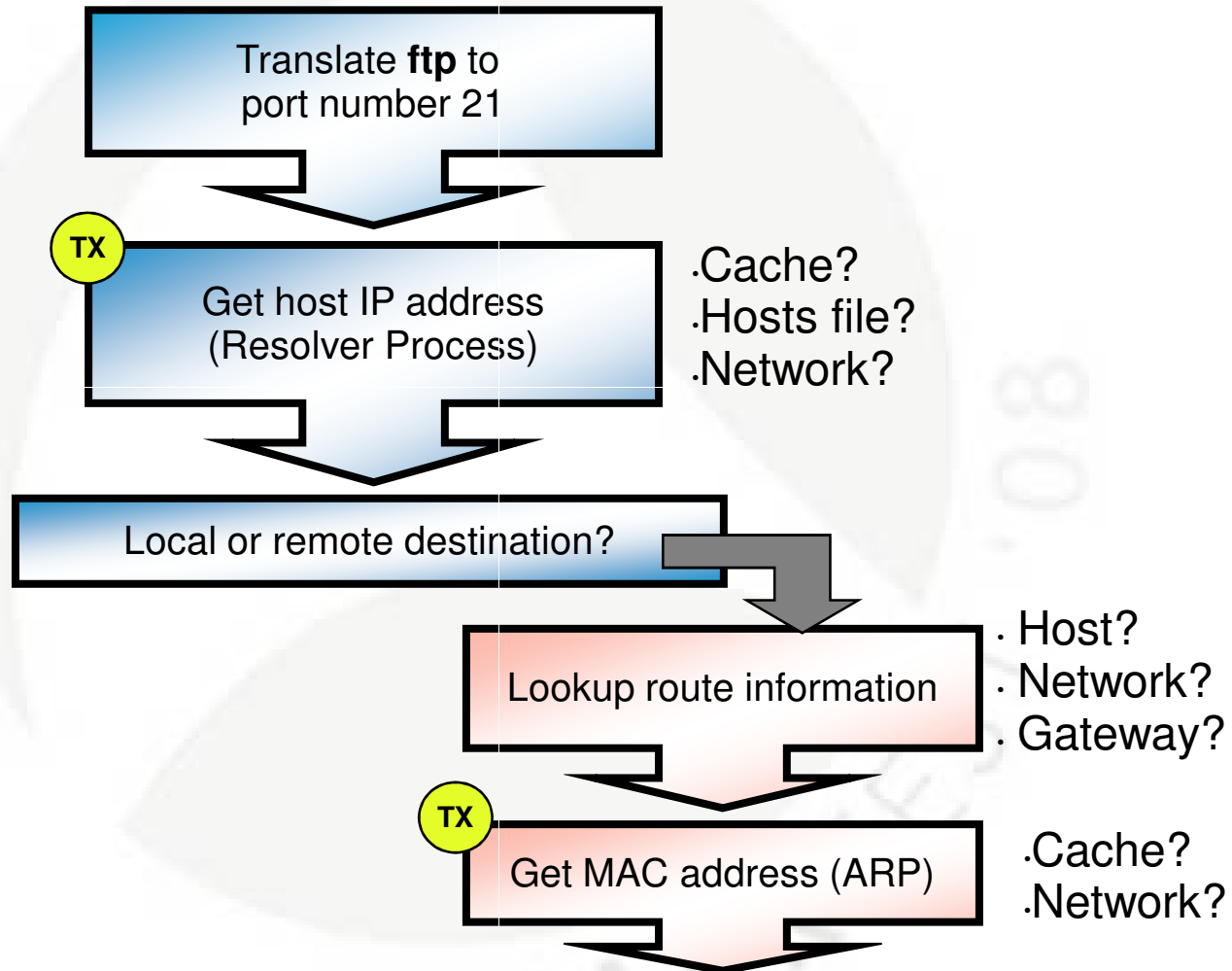
Port and Name Resolution



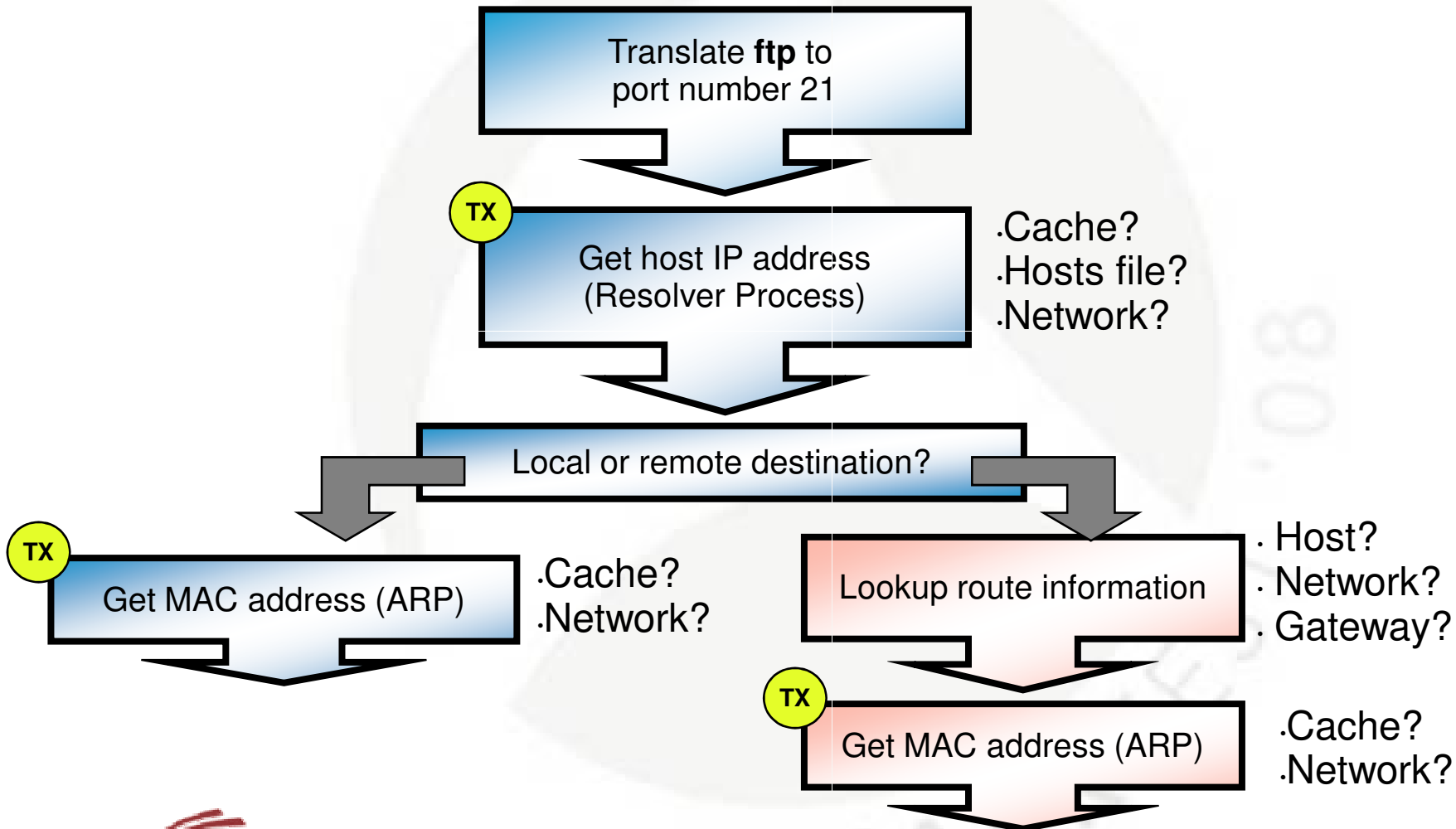
Local MAC Resolution



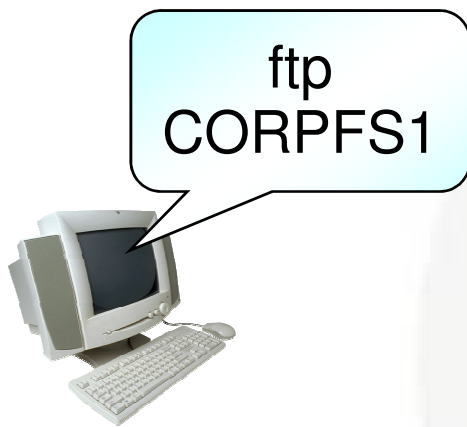
Route and MAC Resolution (Remote Target)



TCP/IP Resolution Processes



Building the Packet



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

Eth	Destination MAC:	(B)
	Source MAC:	A
	EtherType:	0x0800
IP	Protocol:	6 (TCP)
	Source IP:	10.1.0.1
	Destination IP:	(10.2.99.99)
TCP	Source Port:	(1024)
	Destination Port:	(21)

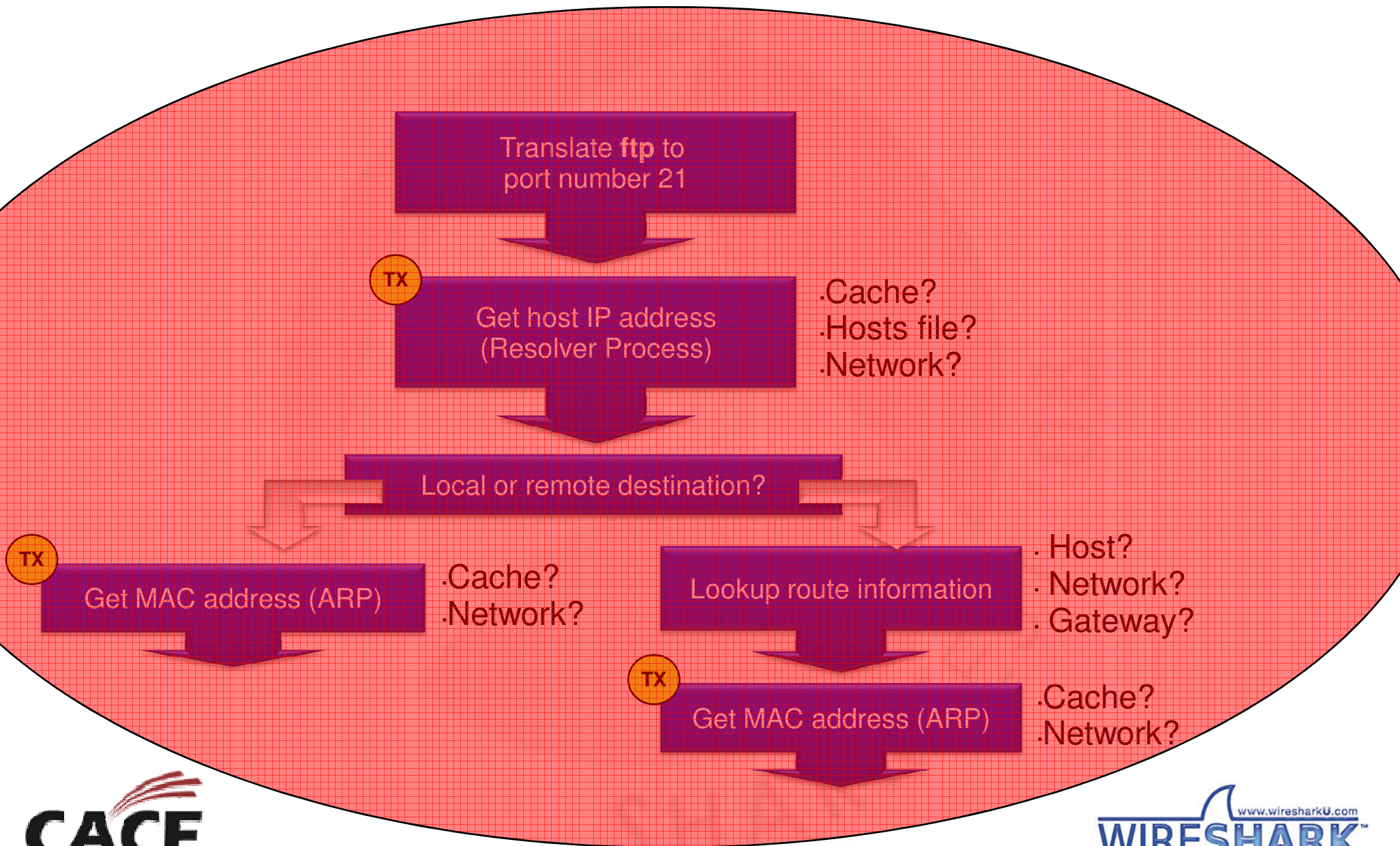


CORPFS1

MAC: B
IP: 10.2.99.99

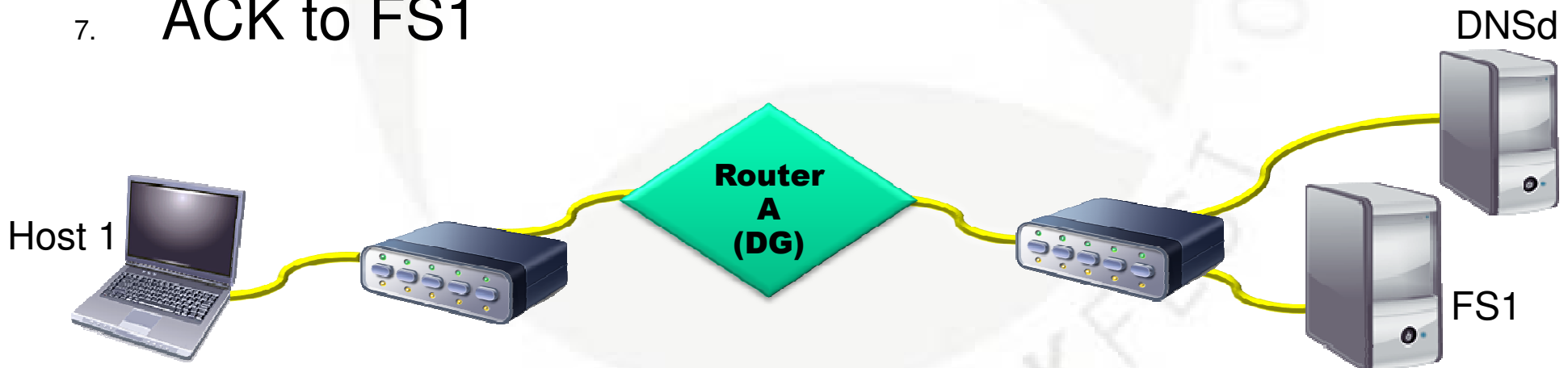


Where Can Things Go Wrong?



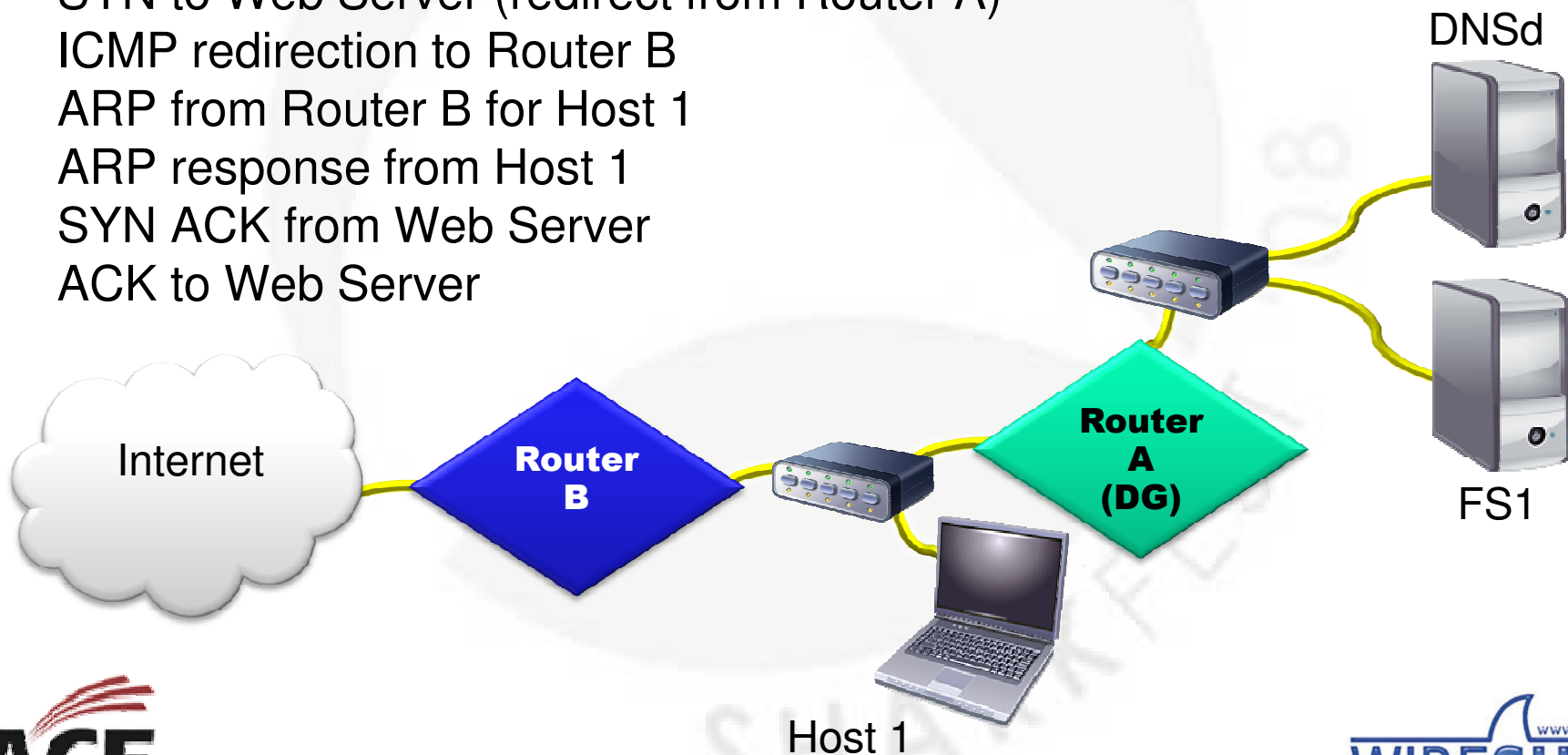
Scenarios – Simple (Remote DNS/FS)

1. ARP for Router
2. ARP response
3. DNS query
4. DNS response
5. SYN to FS1
6. SYN ACK from FS1
7. ACK to FS1



Scenarios – Redirection

1. ARP for Router
2. ARP response
3. DNS query
4. DNS response
5. SYN to Web Server
6. SYN to Web Server (redirect from Router A)
7. ICMP redirection to Router B
8. ARP from Router B for Host 1
9. ARP response from Host 1
10. SYN ACK from Web Server
11. ACK to Web Server



What's Next?

Laura's Lab Kit v9

In show bags as well as...

ISO image: www.novell.com/connectionmagazine/laurachappell.html

