Laura Chappell presents…™

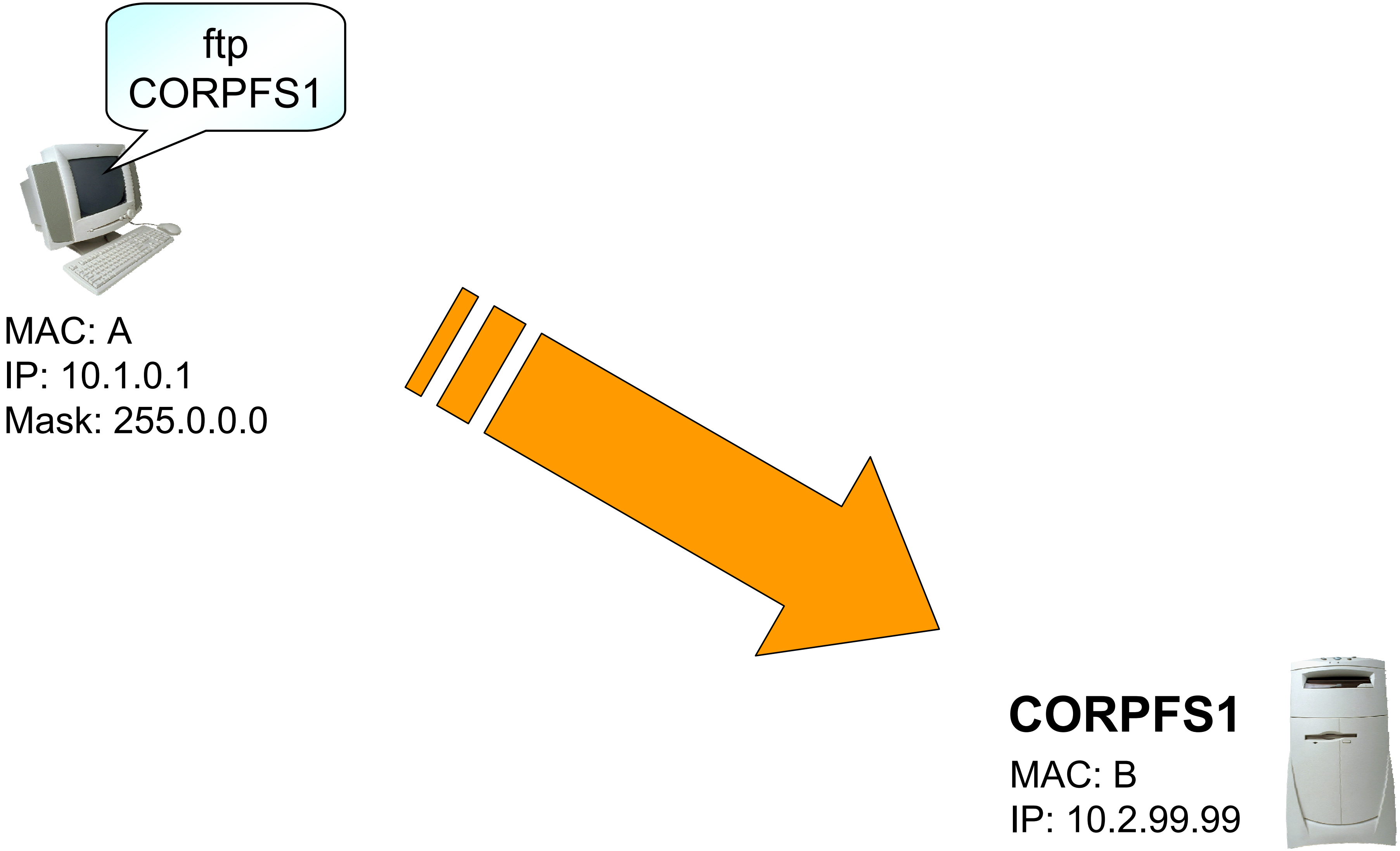
Troubleshooting TCP/IP Connections

Port resolution, name resolution, proximity resolution, route resolution and MAC address resolution – what can go wrong?

Seminar Contents

- The TCP/IP Resolution Process (local destination)
  - Port resolution
  - Name resolution
  - Route resolution
  - Address resolution
- What Can Go Wrong?
- Remote Destinations
- Remote DNS Servers
- Other Scenarios
- *Trace File Analysis Session*

The Scenario



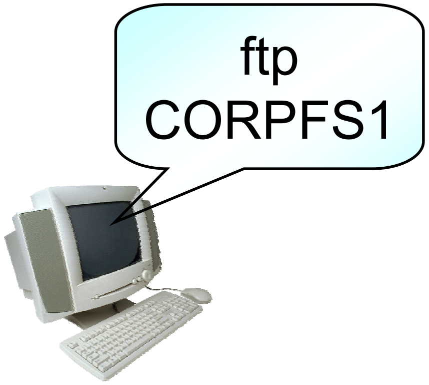
ftp
CORPFS1

MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

CORPFS1

MAC: B
IP: 10.2.99.99

What Needs to be Done?



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

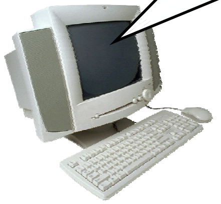
Eth	Destination MAC:	
	Source MAC:	**A**
	EtherType:	**0x0800**
IP	Protocol:	**6 (TCP)**
	Source IP:	**10.1.0.1**
	Destination IP:	
TCP	Source Port:	
	Destination Port:	

CORPFS1

MAC: B
IP: 10.2.99.99

Port Resolution

ftp
CORPFS1



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

Translate **`ftp`** to
port number 21

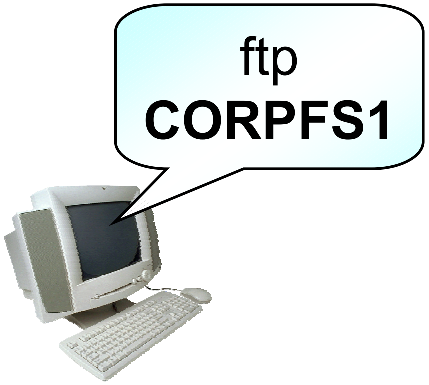
✓

services file
C:\WINNT\system32\drivers\etc

CORPFS1

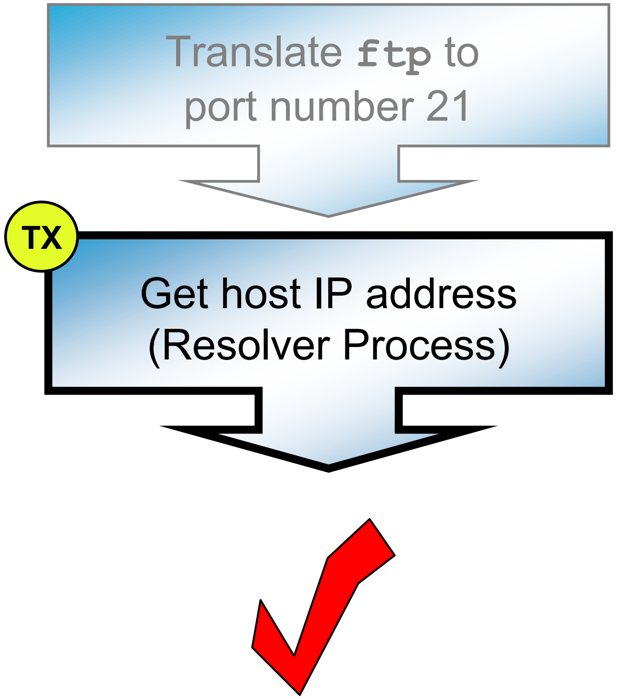
MAC: B
IP: 10.2.99.99

Name Resolution



ftp
CORPFS1

MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0



Translate `ftp` to port number 21

TX

Get host IP address (Resolver Process)

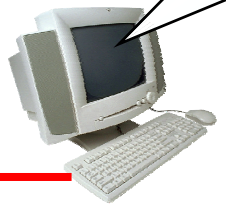
- **Cache?**
- Hosts file?
- Network?

CORPFS1

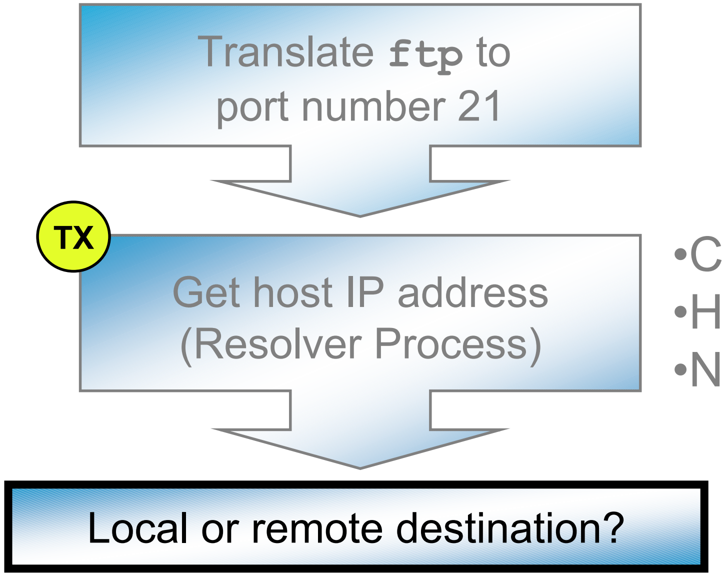
MAC: B
IP: 10.2.99.99

Local or Remote Destination?

ftp
CORPFS1



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0



Translate **`ftp`** to port number 21

TX

Get host IP address (Resolver Process)

- Cache?
- Hosts file?
- Network?

Local or remote destination?

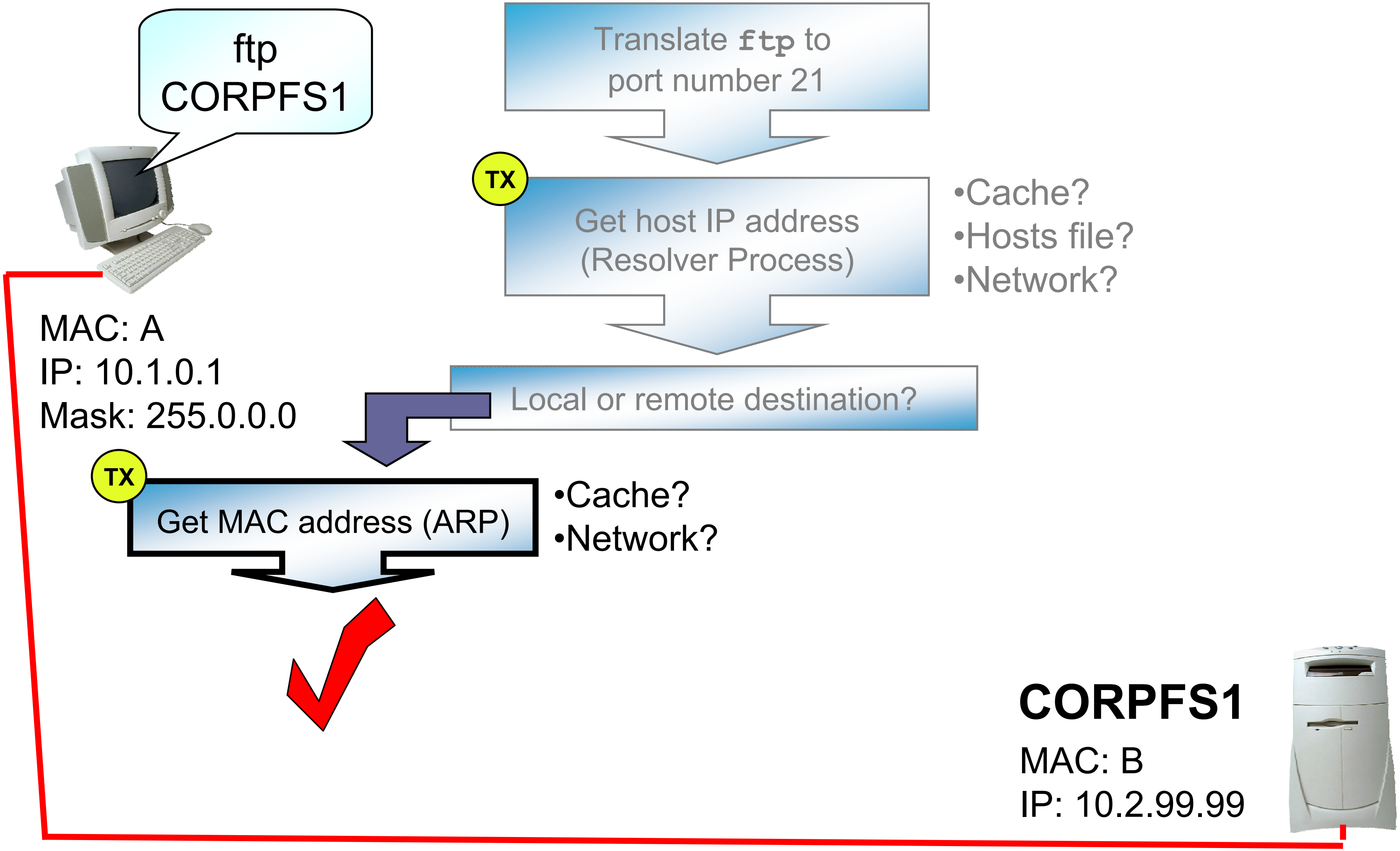
Source Address:	10.1.0.1
Network Mask:	255.0.0.0
Source Network:	**10**.0.0.0
Destination Network:	**10**.0.0.0

WE’RE ON THE SAME NETWORK!

CORPFS1

MAC: B
IP: 10.2.99.99

MAC Address Resolution



ftp CORPFS1

Translate `ftp` to port number 21

TX

Get host IP address (Resolver Process)

- Cache?
- Hosts file?
- Network?

Local or remote destination?

TX

Get MAC address (ARP)

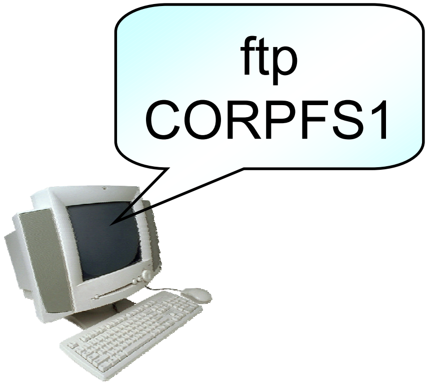
- Cache?
- Network?

MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

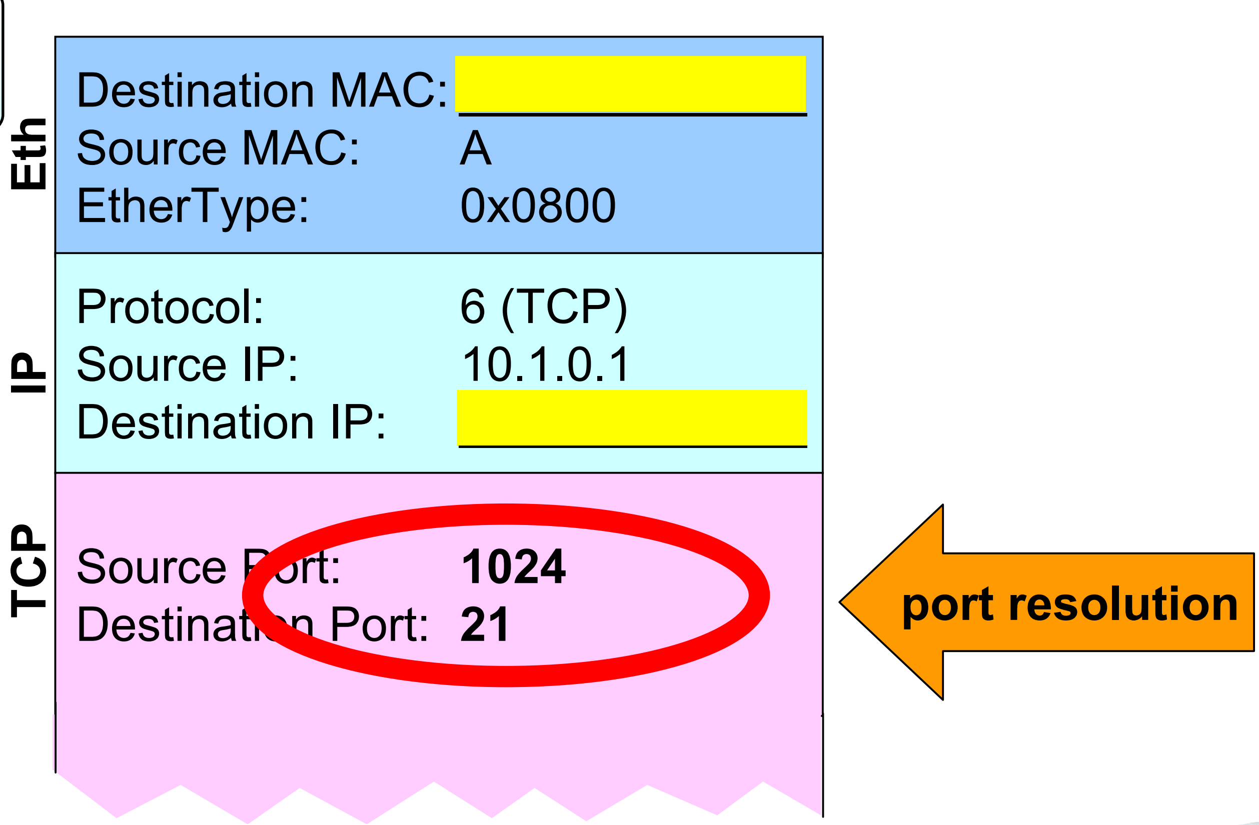
CORPFS1

MAC: B
IP: 10.2.99.99

How Does the Packet Look?



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: **1024**
Destination Port: **21**

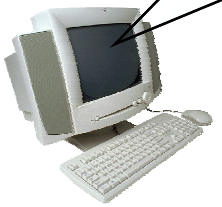
port resolution

CORPFS1

MAC: B
IP: 10.2.99.99

We’ve Got the Name/Address Info

ftp
CORPFS1



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

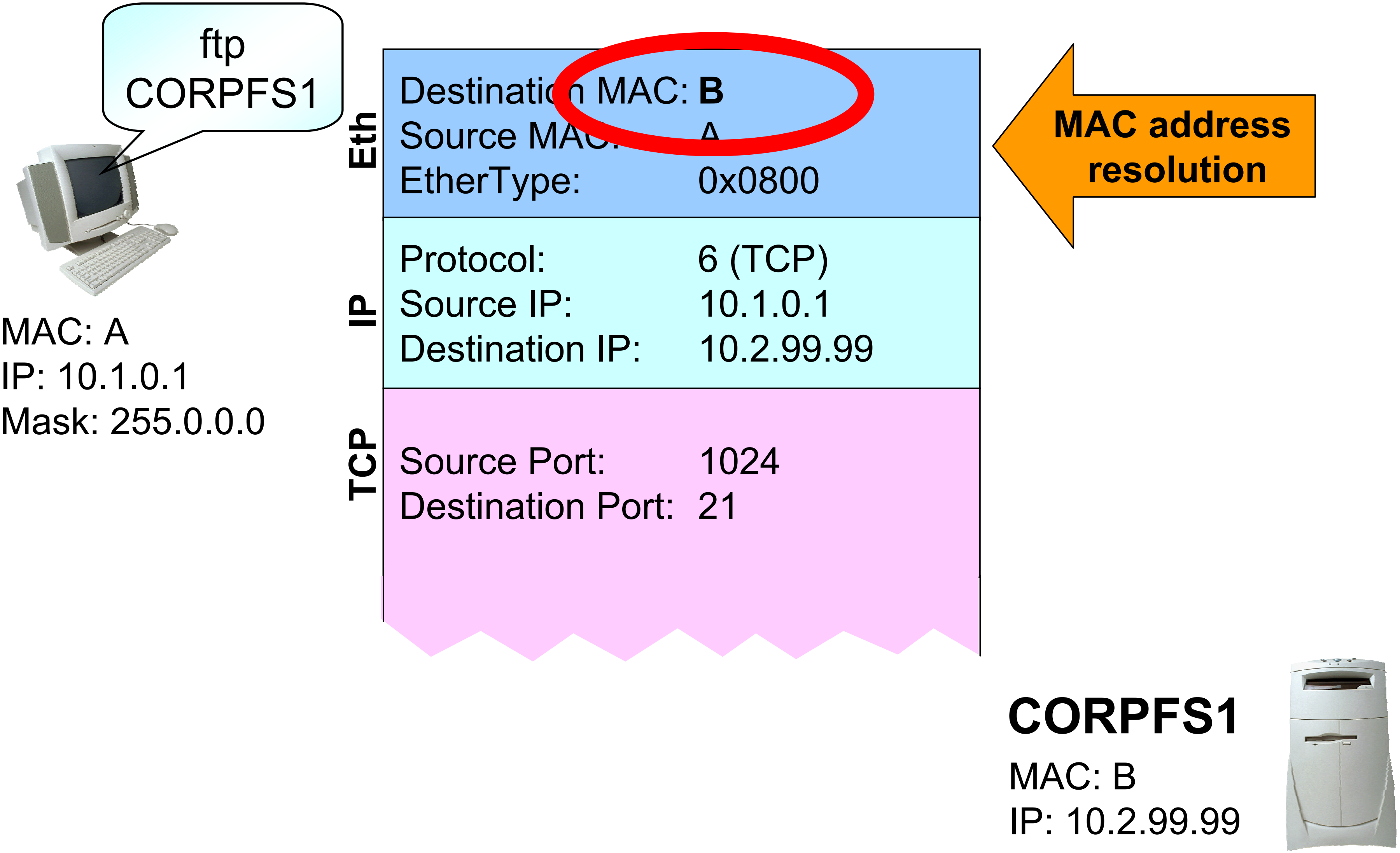
Eth	Destination MAC:	
	Source MAC:	A
	EtherType:	0x0800
IP	Protocol:	6 (TCP)
	Source IP:	10.1.0.1
	Destination IP:	**10.2.99.99**
TCP	Source Port:	1024
	Destination Port:	21

name resolution

CORPFS1

MAC: B
IP: 10.2.99.99

We’ve Got the MAC Address



ftp CORPFS1

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

MAC address resolution

CORPFS1

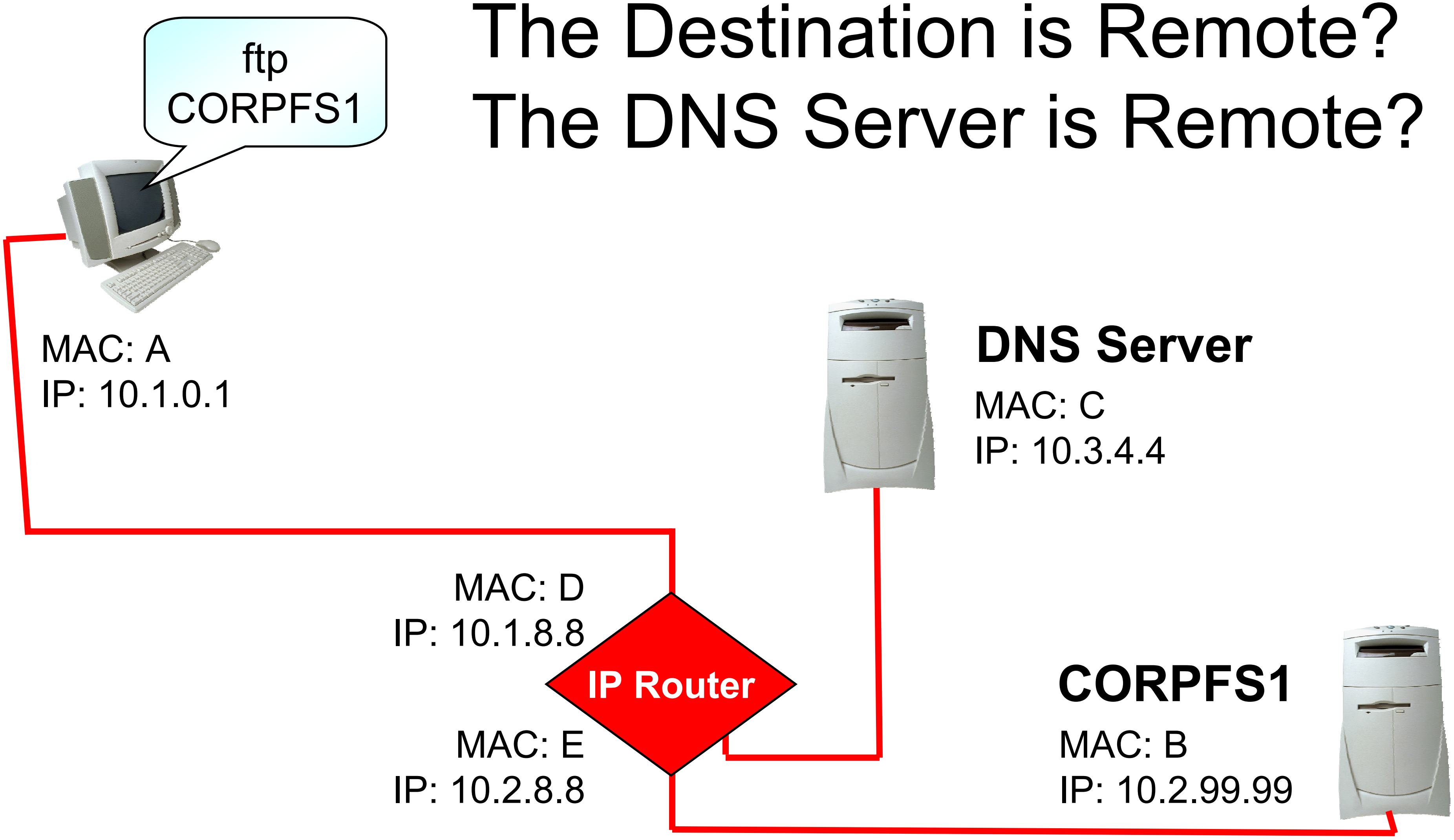
MAC: B
IP: 10.2.99.99

What Do We See on the Wire?

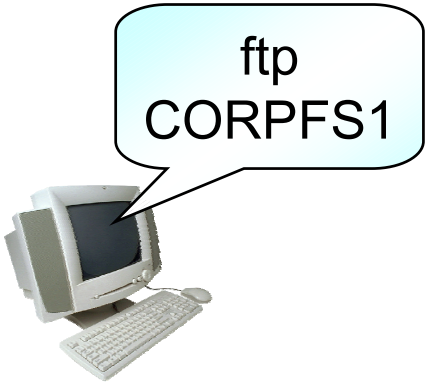
- DNS server is local
- Destination is local
  - ARP broadcast for DNS server
  - ARP response from DNS server
  - DNS query
  - DNS response
  - ARP broadcast for CORPFS1
  - ARP response from CORPFS1
  - FTP communication starts…

But… What If?

The Destination is Remote?
The DNS Server is Remote?



Route Resolution



MAC: A
IP: 10.1.0.1

Translate **ftp** to port number 21

Get host IP address (Resolver Process)

Local or remote destination?

Lookup route information

- Host?
- Network?
- **Gateway?**

Source Address:	10.1.0.1
Network Mask:	**255.255.0.0**
Local Network:	**10.1**.0.0
Destination Network:	**10.2**.0.0

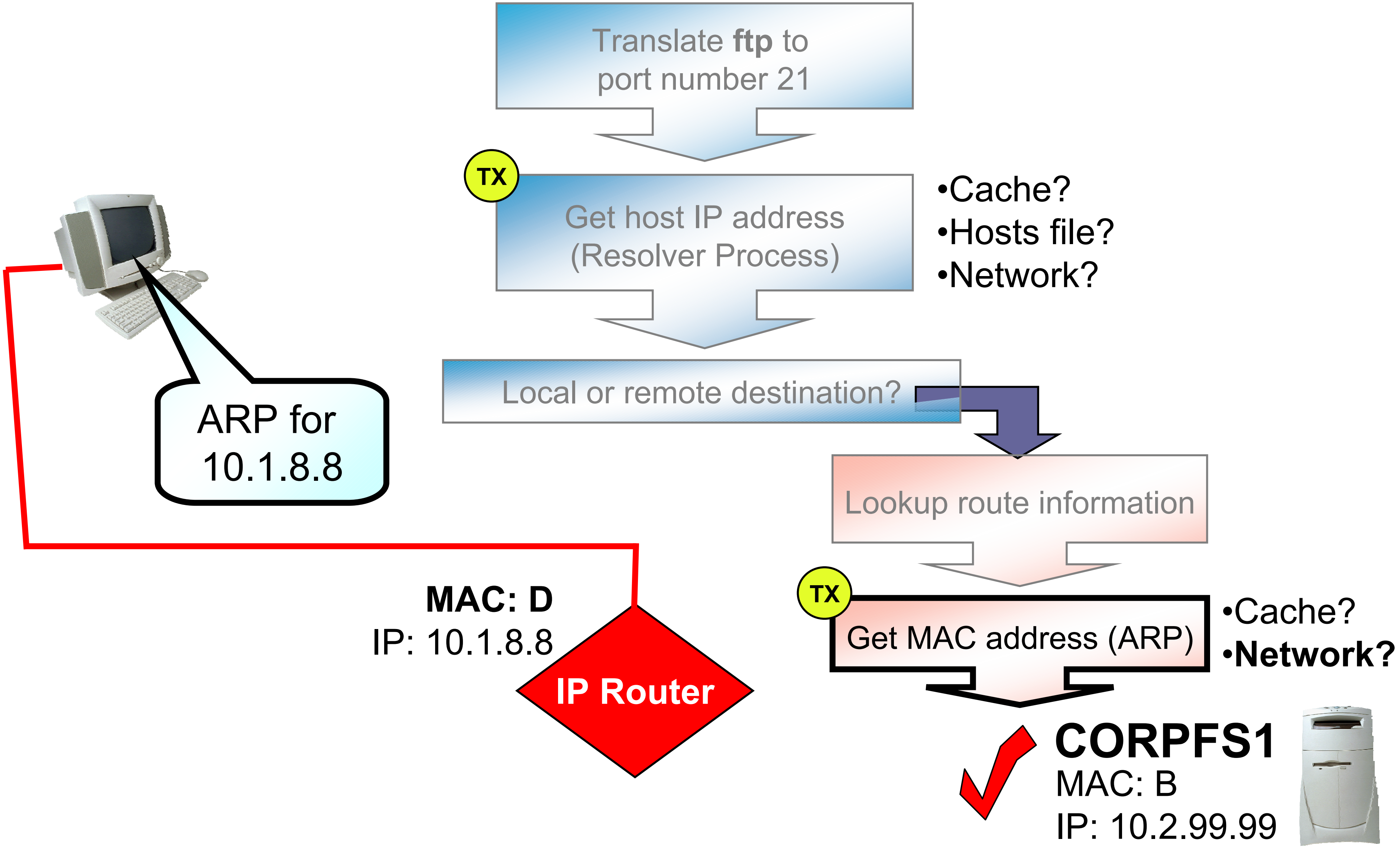
✓

WE'RE ON DIFFERENT NETWORKS!

CORPFS1

MAC: B
IP: 10.2.99.99

MAC Address Resolution



Translate **ftp** to port number 21

TX

Get host IP address (Resolver Process)

- Cache?
- Hosts file?
- Network?

Local or remote destination?

Lookup route information

TX

Get MAC address (ARP)

- Cache?
- **Network?**

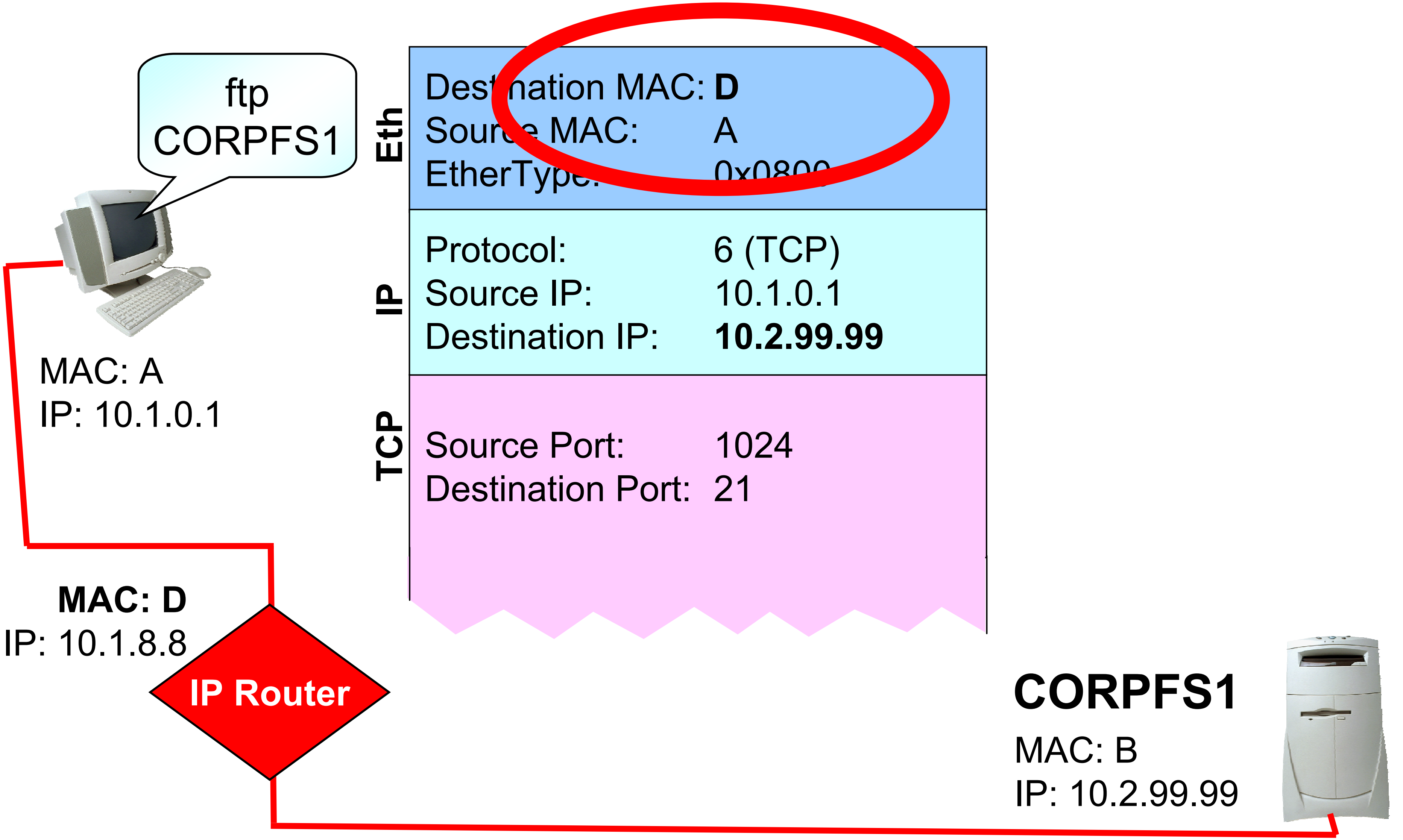
ARP for 10.1.8.8

MAC: D
IP: 10.1.8.8

IP Router

CORPFS1
MAC: B
IP: 10.2.99.99

We’ve Got the Router’s MAC Address



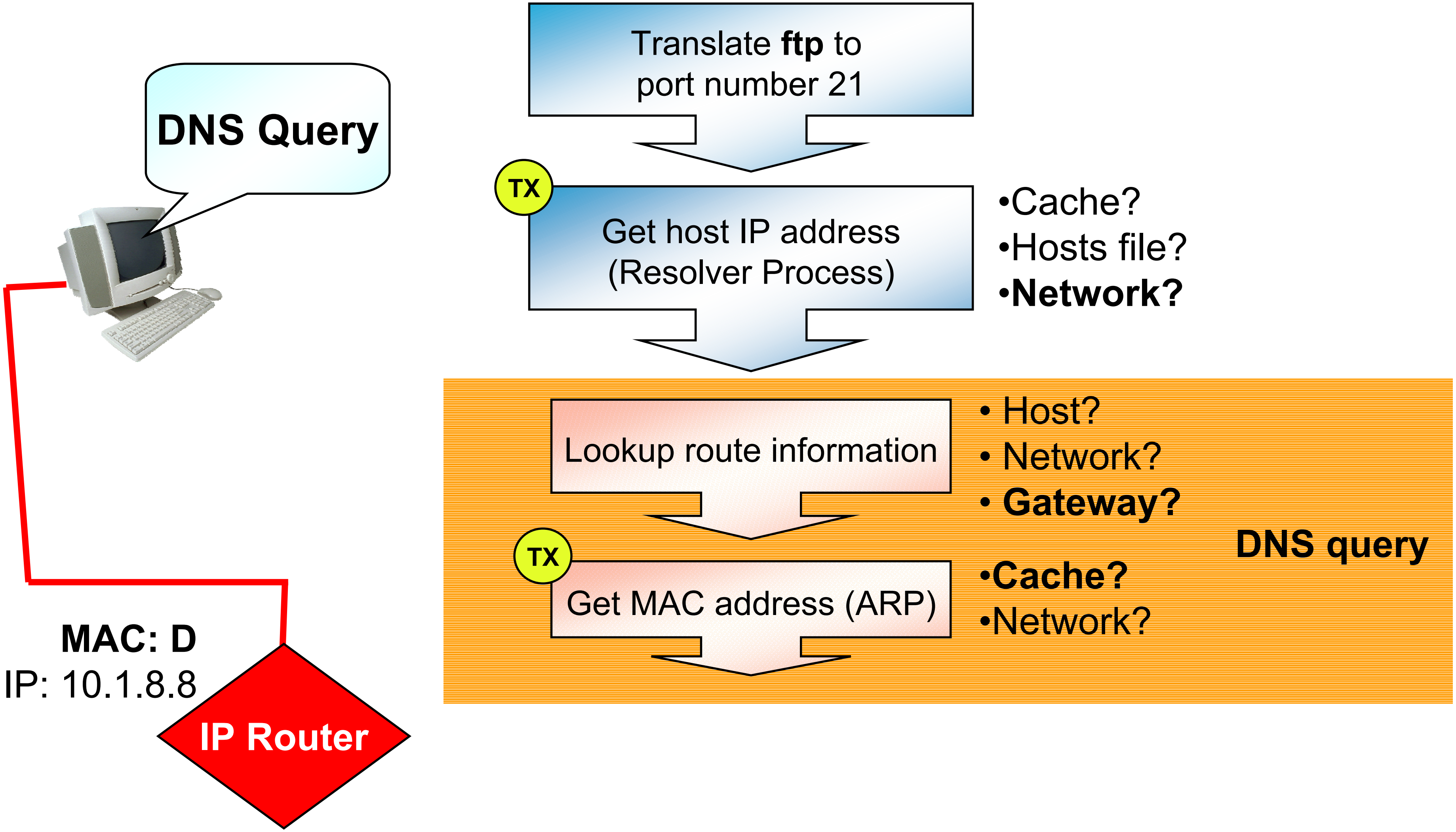
MAC: A
IP: 10.1.0.1

Eth	Destination MAC:	**D**
	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

MAC: D
IP: 10.1.8.8

CORPFS1
MAC: B
IP: 10.2.99.99

What About a Remote DNS Server



DNS Query

MAC: D

IP: 10.1.8.8

IP Router

Translate **ftp** to port number 21

TX

Get host IP address (Resolver Process)

- Cache?
- Hosts file?
- **Network?**

Lookup route information

- Host?
- Network?
- **Gateway?**

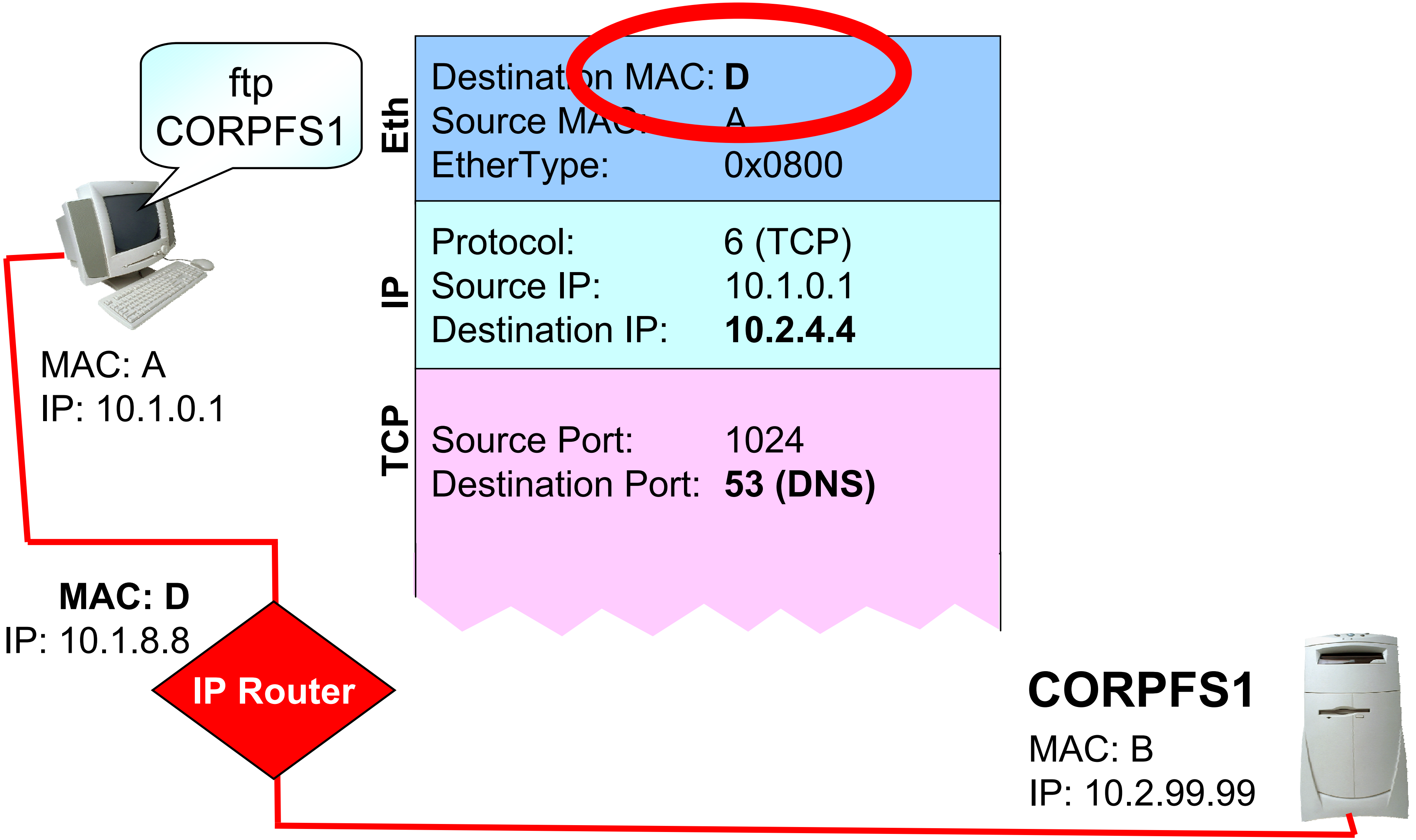
TX

Get MAC address (ARP)

- **Cache?**
- Network?

DNS query

We’ve Got the Router’s MAC Address for the DNS Query



MAC: A
IP: 10.1.0.1

Eth

Destination MAC: **D**
Source MAC: A
EtherType: 0x0800

IP

Protocol: 6 (TCP)
Source IP: 10.1.0.1
Destination IP: **10.2.4.4**

TCP

Source Port: 1024
Destination Port: **53 (DNS)**

MAC: D
IP: 10.1.8.8

IP Router

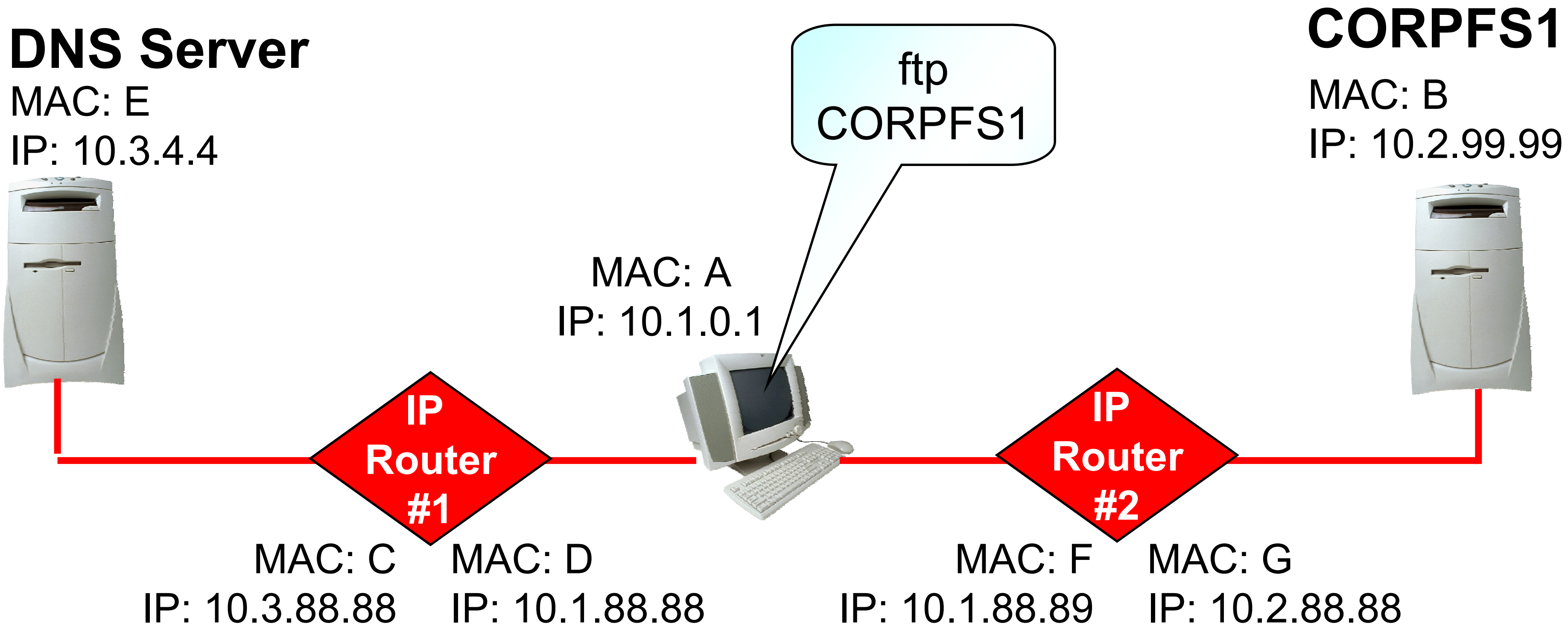
CORPFS1
MAC: B
IP: 10.2.99.99

What Do We See on the Wire?

- DNS server is remote
- Destination is local
  - ARP broadcast for router
  - ARP response from router
  - DNS query (sent to router’s MAC)
  - DNS response
  - ARP broadcast for CORPFS1
  - ARP response from CORPFS1
  - FTP communication starts…

What Would You See if…?

The DNS server is on one network
And the FTP server is on another?
[Router #2 is the Default Gateway.]



What if Router #2 is the Default Gateway?

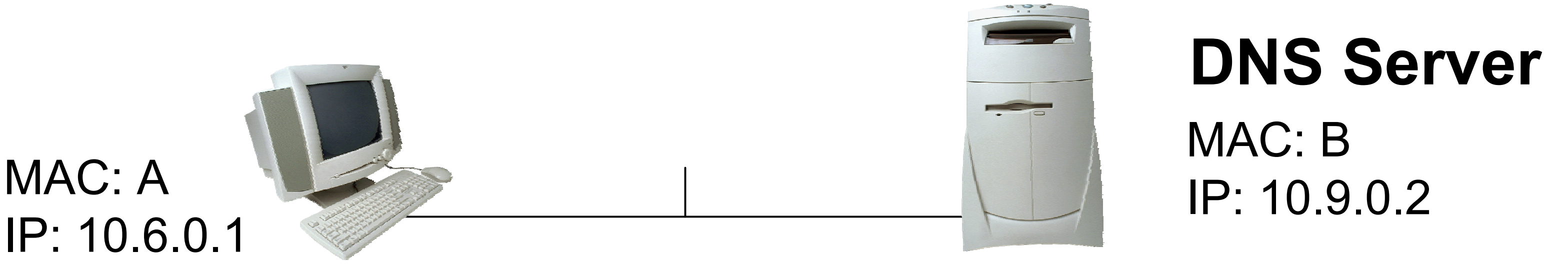
- ARP broadcast for router #2
- ARP response from router #2
- DNS query through router #2
- ICMP redirect from router #2 (“go to router #1”)
- ARP broadcast for router #1
- ARP response from router #1
- DNS query through router #1
- DNS response through router #1
- ARP broadcast for router #2 (if timed out)
- ARP response from router #2
- FTP communication starts… through router #2

What do You Know If You See…

- ARP broadcast from 10.6.0.1 for 10.9.0.2 (s.MAC=A)
- ARP response from 10.9.0.2 (d.MAC=B)
- DNS query for www.espn.com
- DNS response [www.espn.com = 204.202.132.19]
- FTP communication starts to 204.202.132.19… through d.MAC=C

What do You Know If You See…

- ARP broadcast from 10.6.0.1 for 10.9.0.2 (s.MAC=A)
- ARP response from 10.9.0.2 (d.MAC=B)
- DNS query for www.espn.com
- DNS response [www.espn.com = 204.202.132.19]
- FTP communication starts to 204.202.132.19… through d.MAC=C



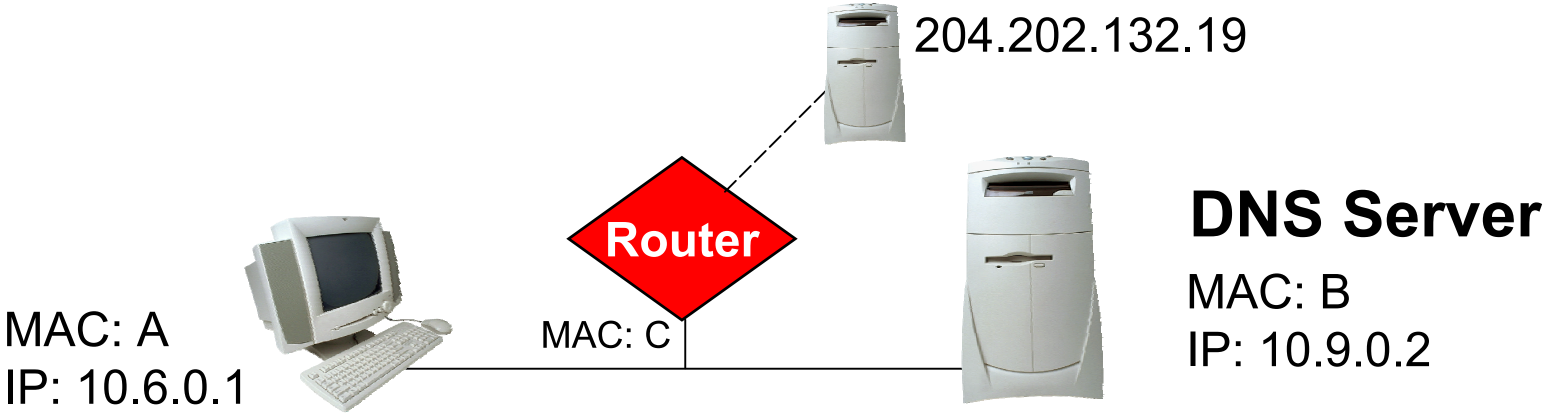
MAC: A
IP: 10.6.0.1

DNS Server

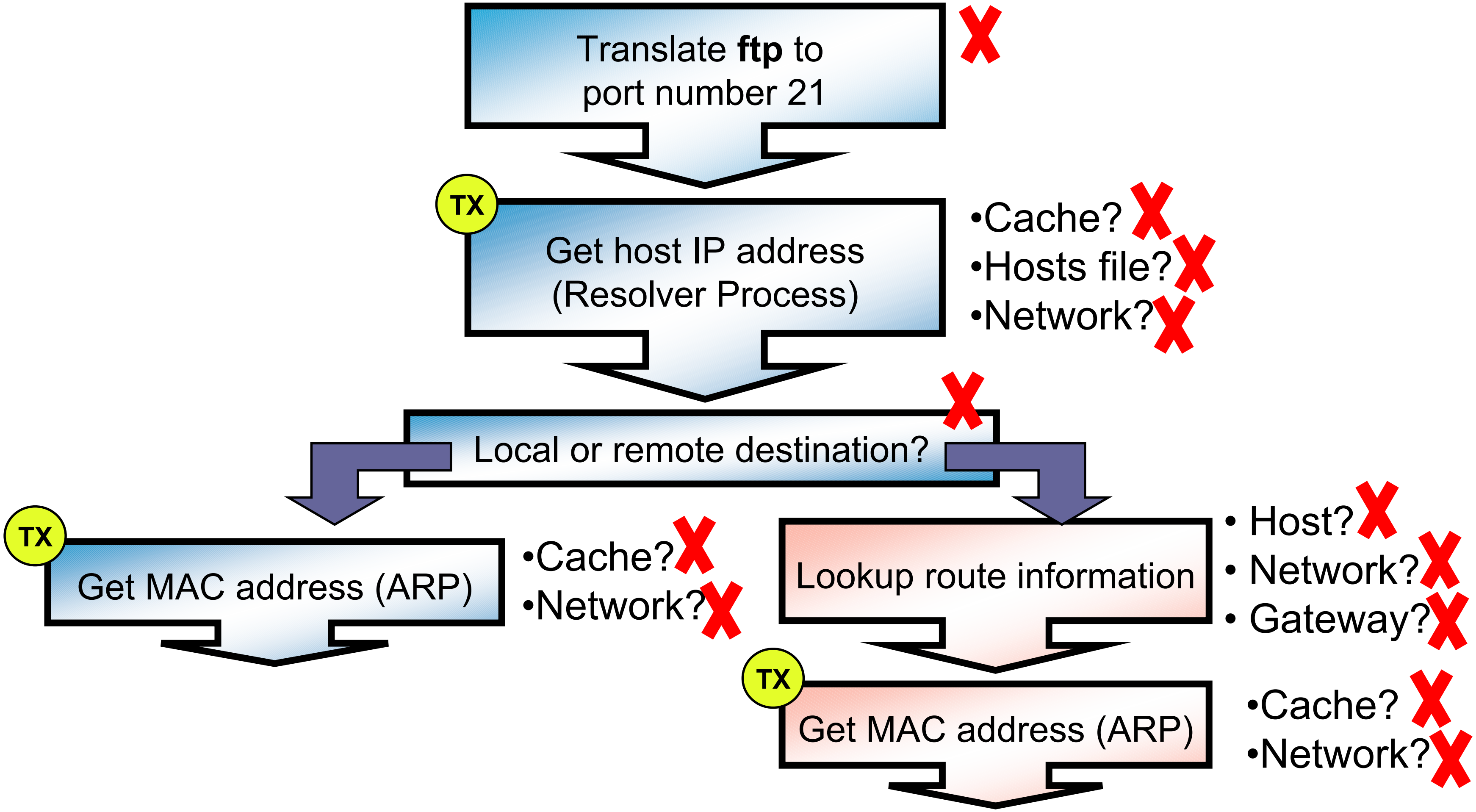
MAC: B
IP: 10.9.0.2

What do You Know If You See…

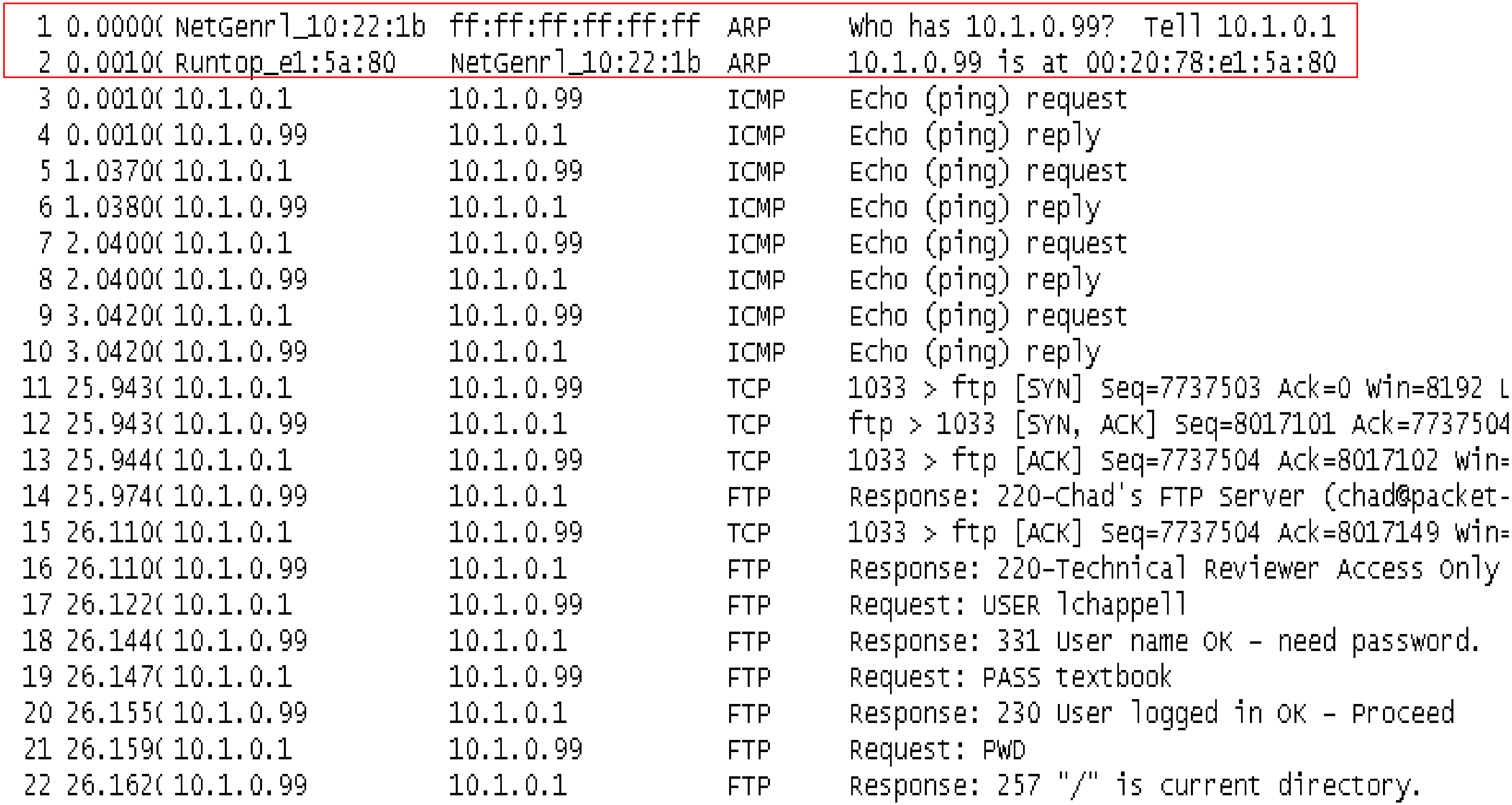
- ARP broadcast from 10.6.0.1 for 10.9.0.2 (s.MAC=A)
- ARP response from 10.9.0.2 (d.MAC=B)
- DNS query for www.espn.com
- DNS response [www.espn.com = 204.202.132.19]
- FTP communication starts to 204.202.132.19… through d.MAC=C



Where Can Things Go Wrong?



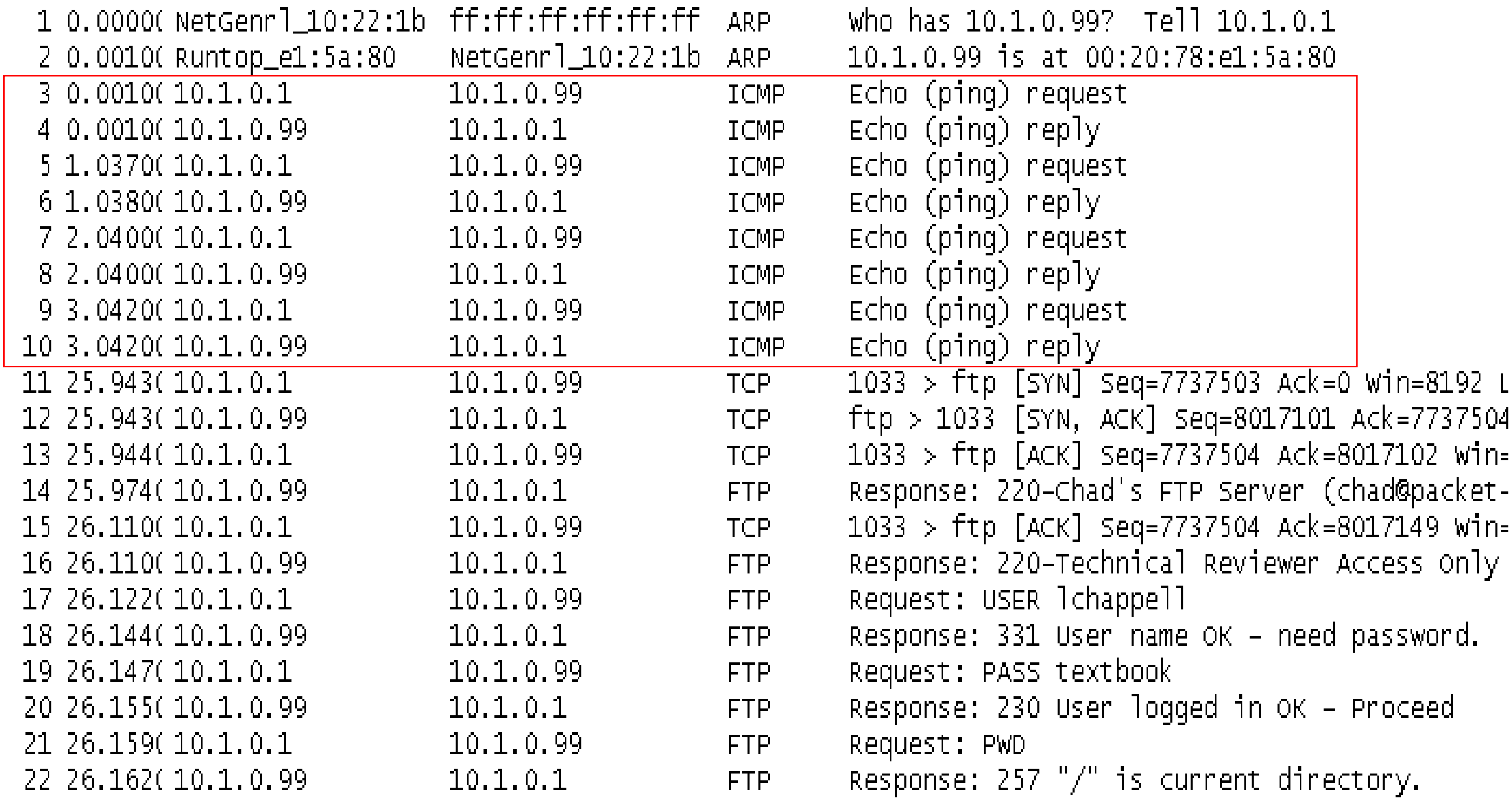
Analysis Answers



```
 1 0.0000( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff  ARP     Who has 10.1.0.99?  Tell 10.1.0.1
 2 0.0010( Runtop_e1:5a:80    NetGenrl_10:22:1b  ARP     10.1.0.99 is at 00:20:78:e1:5a:80
 3 0.0010( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 4 0.0010( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 5 1.0370( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 6 1.0380( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 7 2.0400( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 8 2.0400( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 9 3.0420( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
10 3.0420( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
11 25.943( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [SYN] Seq=7737503 Ack=0 Win=8192 L
12 25.943( 10.1.0.99          10.1.0.1           TCP     ftp > 1033 [SYN, ACK] Seq=8017101 Ack=7737504
13 25.944( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017102 Win=
14 25.974( 10.1.0.99          10.1.0.1           FTP     Response: 220-Chad's FTP Server (chad@packet-
15 26.110( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017149 Win=
16 26.110( 10.1.0.99          10.1.0.1           FTP     Response: 220-Technical Reviewer Access Only
17 26.122( 10.1.0.1           10.1.0.99          FTP     Request: USER lchappell
18 26.144( 10.1.0.99          10.1.0.1           FTP     Response: 331 User name OK - need password.
19 26.147( 10.1.0.1           10.1.0.99          FTP     Request: PASS textbook
20 26.155( 10.1.0.99          10.1.0.1           FTP     Response: 230 User logged in OK - Proceed
21 26.159( 10.1.0.1           10.1.0.99          FTP     Request: PWD
22 26.162( 10.1.0.99          10.1.0.1           FTP     Response: 257 "/" is current directory.
```

(continued)

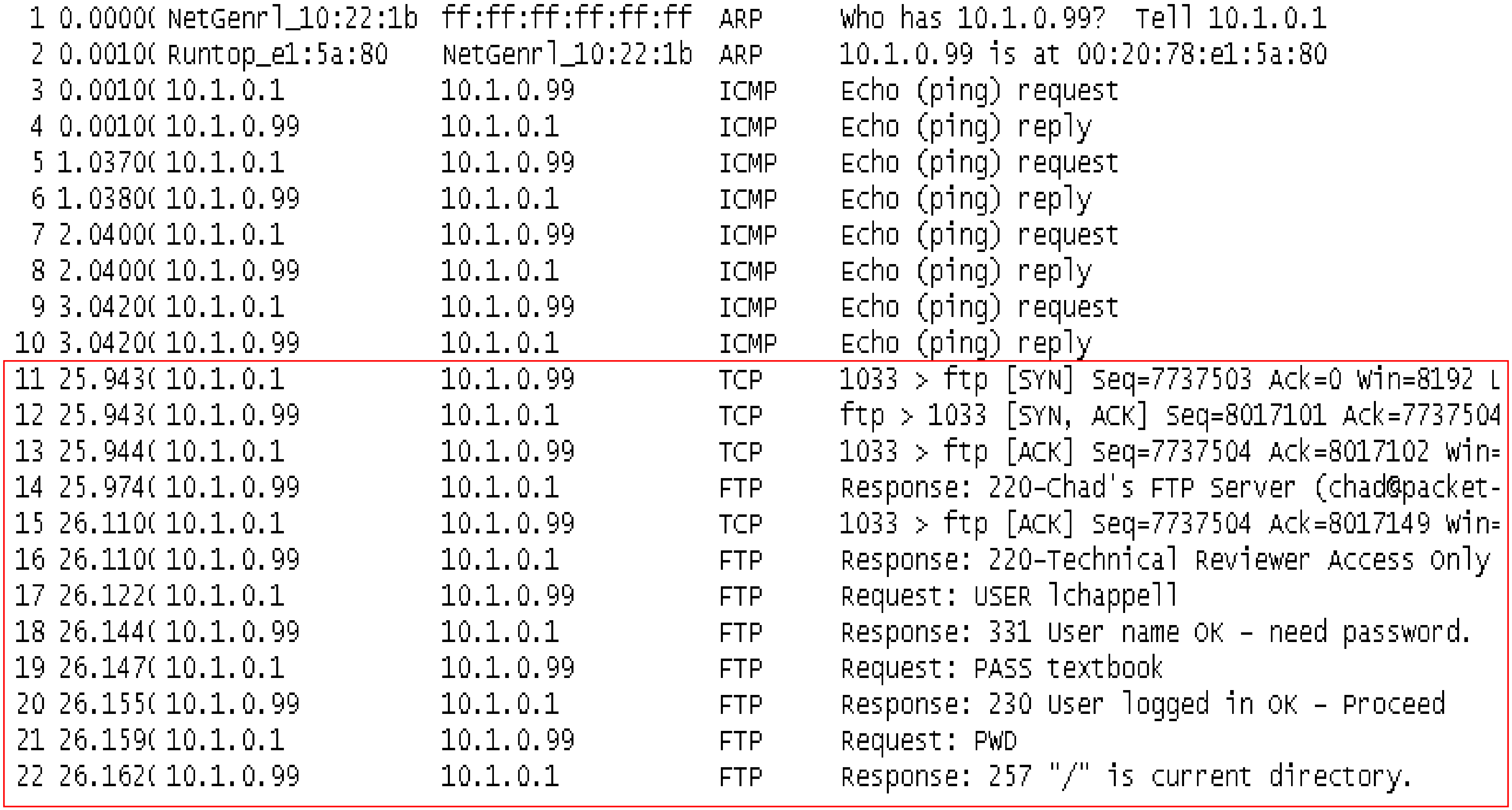
Analysis Answers



```
 1 0.0000( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff  ARP     Who has 10.1.0.99?  Tell 10.1.0.1
 2 0.0010( Runtop_e1:5a:80    NetGenrl_10:22:1b  ARP     10.1.0.99 is at 00:20:78:e1:5a:80
 3 0.0010( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 4 0.0010( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 5 1.0370( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 6 1.0380( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 7 2.0400( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 8 2.0400( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 9 3.0420( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
10 3.0420( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
11 25.943( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [SYN] Seq=7737503 Ack=0 Win=8192 L
12 25.943( 10.1.0.99          10.1.0.1           TCP     ftp > 1033 [SYN, ACK] Seq=8017101 Ack=7737504
13 25.944( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017102 Win=
14 25.974( 10.1.0.99          10.1.0.1           FTP     Response: 220-Chad's FTP Server (chad@packet-
15 26.110( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017149 Win=
16 26.110( 10.1.0.99          10.1.0.1           FTP     Response: 220-Technical Reviewer Access Only
17 26.122( 10.1.0.1           10.1.0.99          FTP     Request: USER lchappell
18 26.144( 10.1.0.99          10.1.0.1           FTP     Response: 331 User name OK - need password.
19 26.147( 10.1.0.1           10.1.0.99          FTP     Request: PASS textbook
20 26.155( 10.1.0.99          10.1.0.1           FTP     Response: 230 User logged in OK - Proceed
21 26.159( 10.1.0.1           10.1.0.99          FTP     Request: PWD
22 26.162( 10.1.0.99          10.1.0.1           FTP     Response: 257 "/" is current directory.
```

(continued)

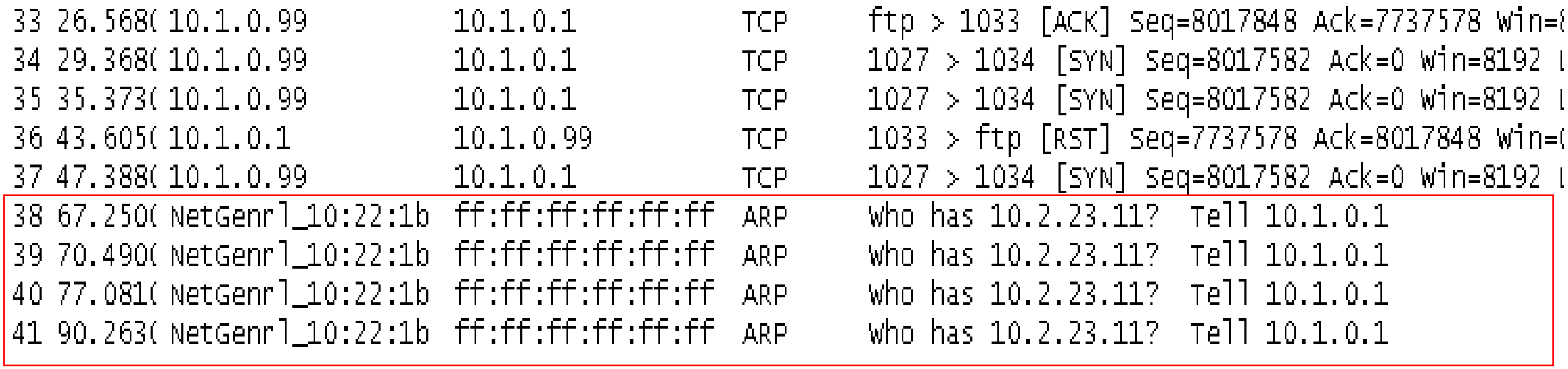
Analysis Answers



```
 1 0.0000( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff  ARP     Who has 10.1.0.99?  Tell 10.1.0.1
 2 0.0010( Runtop_e1:5a:80    NetGenrl_10:22:1b  ARP     10.1.0.99 is at 00:20:78:e1:5a:80
 3 0.0010( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 4 0.0010( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 5 1.0370( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 6 1.0380( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 7 2.0400( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
 8 2.0400( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
 9 3.0420( 10.1.0.1           10.1.0.99          ICMP    Echo (ping) request
10 3.0420( 10.1.0.99          10.1.0.1           ICMP    Echo (ping) reply
11 25.943( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [SYN] Seq=7737503 Ack=0 Win=8192 L
12 25.943( 10.1.0.99          10.1.0.1           TCP     ftp > 1033 [SYN, ACK] Seq=8017101 Ack=7737504
13 25.944( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017102 Win=
14 25.974( 10.1.0.99          10.1.0.1           FTP     Response: 220-Chad's FTP Server (chad@packet-
15 26.110( 10.1.0.1           10.1.0.99          TCP     1033 > ftp [ACK] Seq=7737504 Ack=8017149 Win=
16 26.110( 10.1.0.99          10.1.0.1           FTP     Response: 220-Technical Reviewer Access Only
17 26.122( 10.1.0.1           10.1.0.99          FTP     Request: USER lchappell
18 26.144( 10.1.0.99          10.1.0.1           FTP     Response: 331 User name OK - need password.
19 26.147( 10.1.0.1           10.1.0.99          FTP     Request: PASS textbook
20 26.155( 10.1.0.99          10.1.0.1           FTP     Response: 230 User logged in OK - Proceed
21 26.159( 10.1.0.1           10.1.0.99          FTP     Request: PWD
22 26.162( 10.1.0.99          10.1.0.1           FTP     Response: 257 "/" is current directory.
```

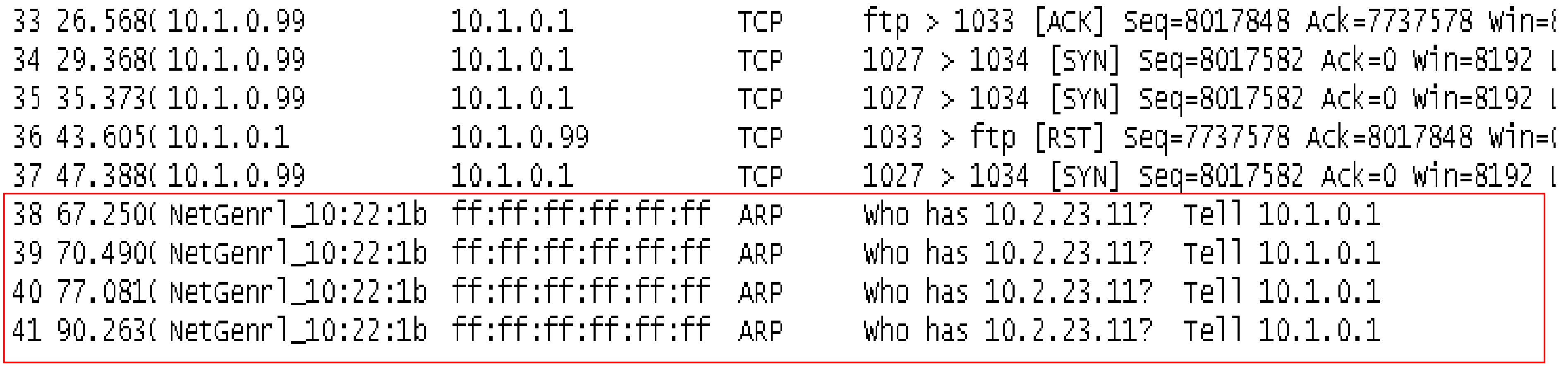
(continued)

Analysis Answers

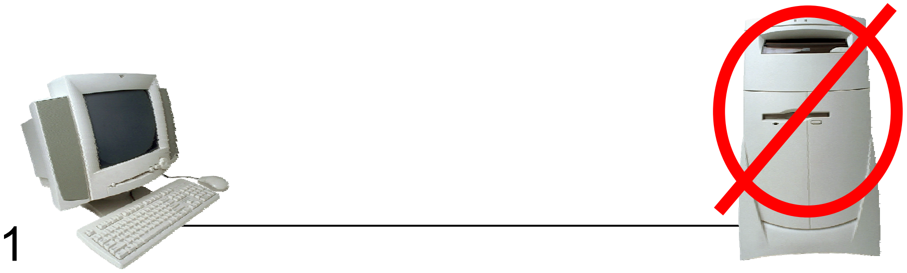


```
33 26.568( 10.1.0.99         10.1.0.1           TCP     ftp > 1033 [ACK] Seq=8017848 Ack=7737578 Win=8
34 29.368( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
35 35.373( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
36 43.605( 10.1.0.1          10.1.0.99          TCP     1033 > ftp [RST] Seq=7737578 Ack=8017848 Win=(
37 47.388( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
38 67.250( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
39 70.490( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
40 77.081( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
41 90.263( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
```

Analysis Answers



```
33 26.568( 10.1.0.99          10.1.0.1            TCP      ftp > 1033 [ACK] Seq=8017848 Ack=7737578 Win=8
34 29.368( 10.1.0.99          10.1.0.1            TCP      1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
35 35.373( 10.1.0.99          10.1.0.1            TCP      1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
36 43.605( 10.1.0.1           10.1.0.99           TCP      1033 > ftp [RST] Seq=7737578 Ack=8017848 Win=(
37 47.388( 10.1.0.99          10.1.0.1            TCP      1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 L
38 67.250( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff   ARP      Who has 10.2.23.11?  Tell 10.1.0.1
39 70.490( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff   ARP      Who has 10.2.23.11?  Tell 10.1.0.1
40 77.081( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff   ARP      Who has 10.2.23.11?  Tell 10.1.0.1
41 90.263( NetGenrl_10:22:1b  ff:ff:ff:ff:ff:ff   ARP      Who has 10.2.23.11?  Tell 10.1.0.1
```

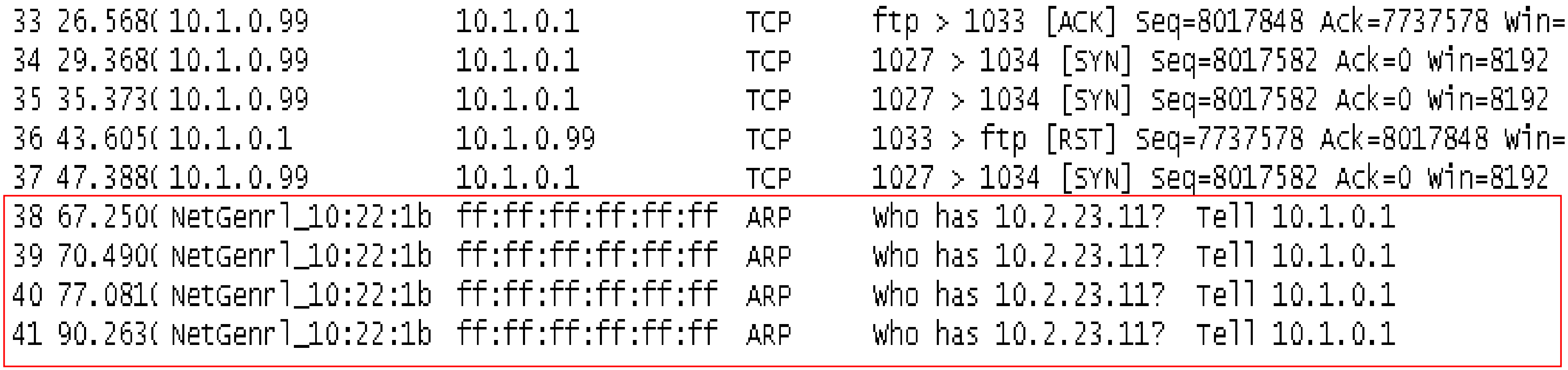


MAC: A
IP: 10.1.0.1

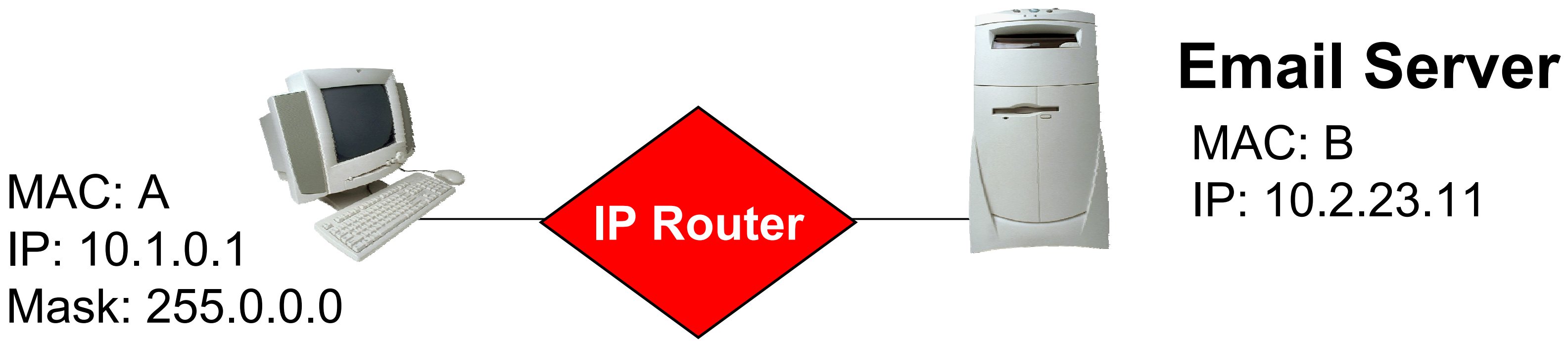
Email Server

MAC: B
IP: 10.2.23.11

Analysis Answers



```
33 26.568( 10.1.0.99         10.1.0.1           TCP     ftp > 1033 [ACK] Seq=8017848 Ack=7737578 Win=8
34 29.368( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 l
35 35.373( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 l
36 43.605( 10.1.0.1          10.1.0.99          TCP     1033 > ftp [RST] Seq=7737578 Ack=8017848 Win=(
37 47.388( 10.1.0.99         10.1.0.1           TCP     1027 > 1034 [SYN] Seq=8017582 Ack=0 Win=8192 l
38 67.250( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
39 70.490( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
40 77.081( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
41 90.263( NetGenrl_10:22:1b ff:ff:ff:ff:ff:ff  ARP     Who has 10.2.23.11?  Tell 10.1.0.1
```



MAC: A
IP: 10.1.0.1
Mask: 255.0.0.0

IP Router

Email Server

MAC: B
IP: 10.2.23.11

Conclusion

- TCP/IP communications follows a standard pattern of functionality.
- There are many places where TCP/IP communications can fail.
- Knowing this process helps troubleshoot TCP/IP communications.
- Go get some traces!