

Endpoint Identification Using System Logs

Stephen W. Melvin

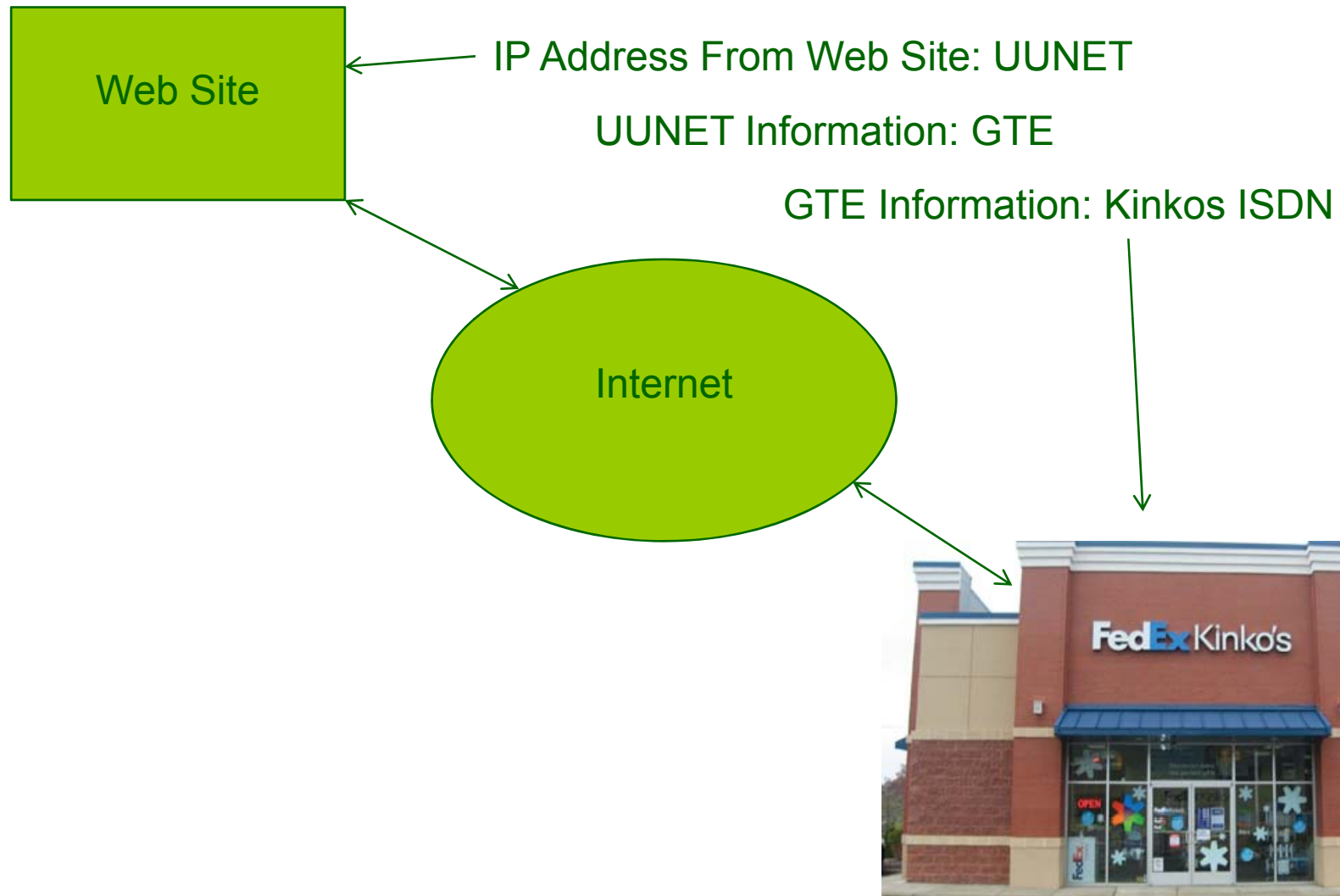
October 14, 2009

Outline

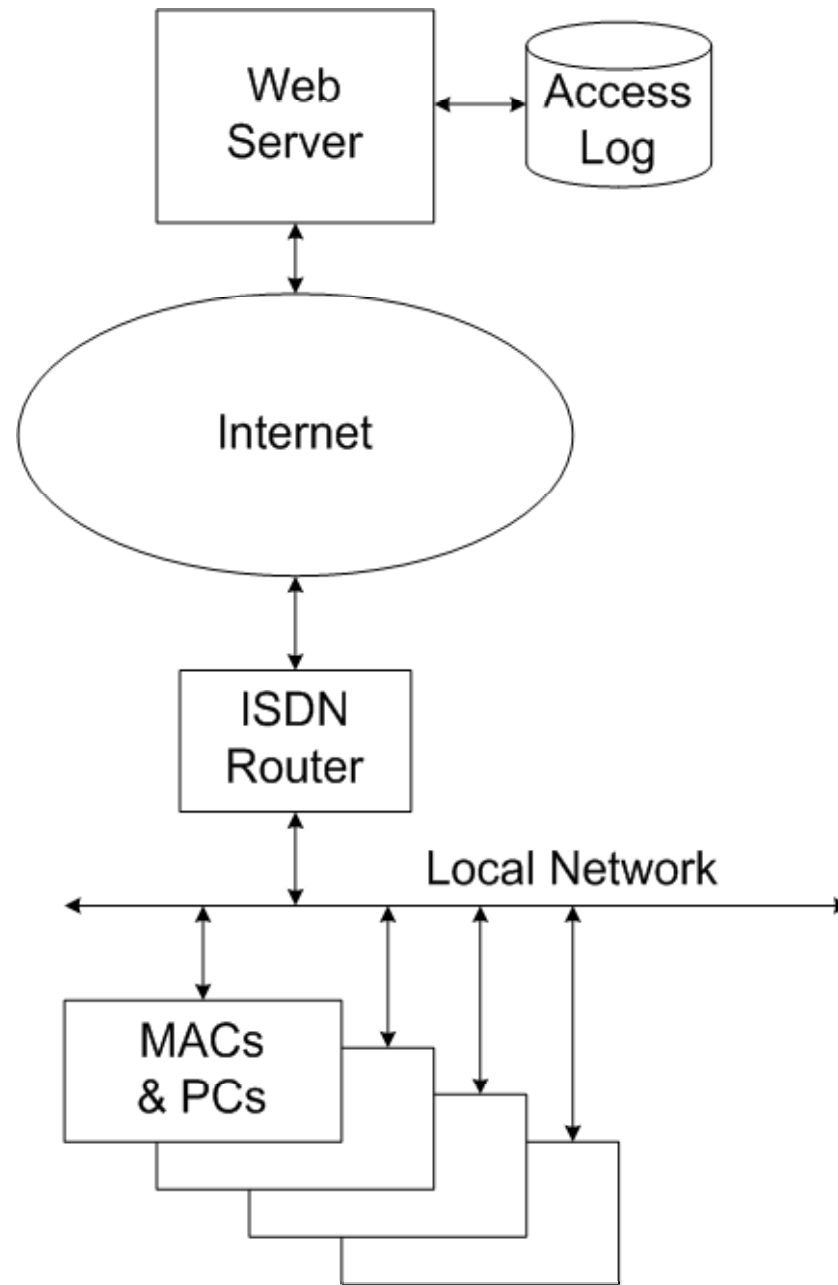
- A Case Study
- Endpoint Identification Logging
- MAC Address Validation
- Log State Management
- Why Identify Endpoints?
- Conclusions

A Case Study

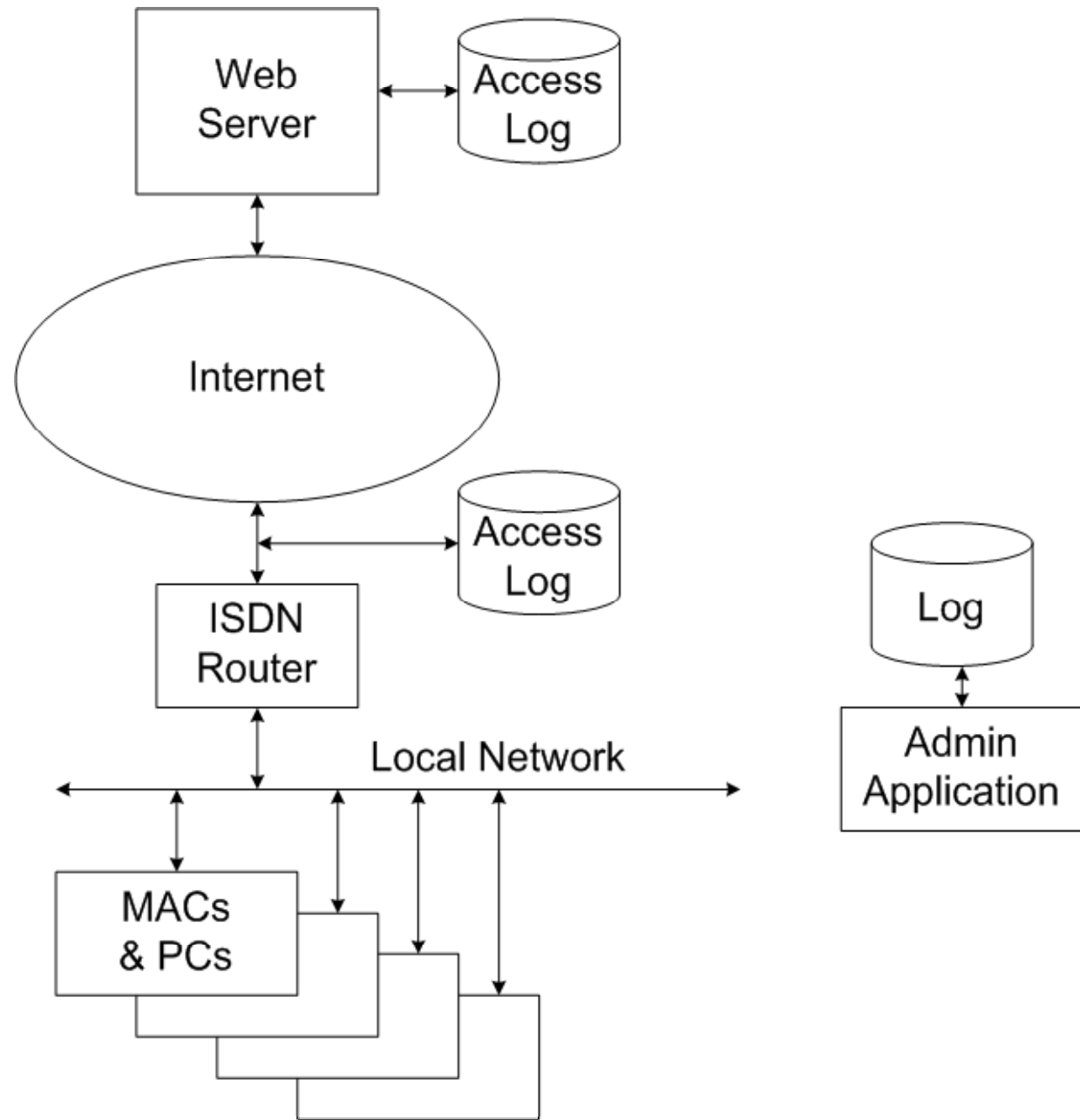
Trace of Message Posting by IP Address



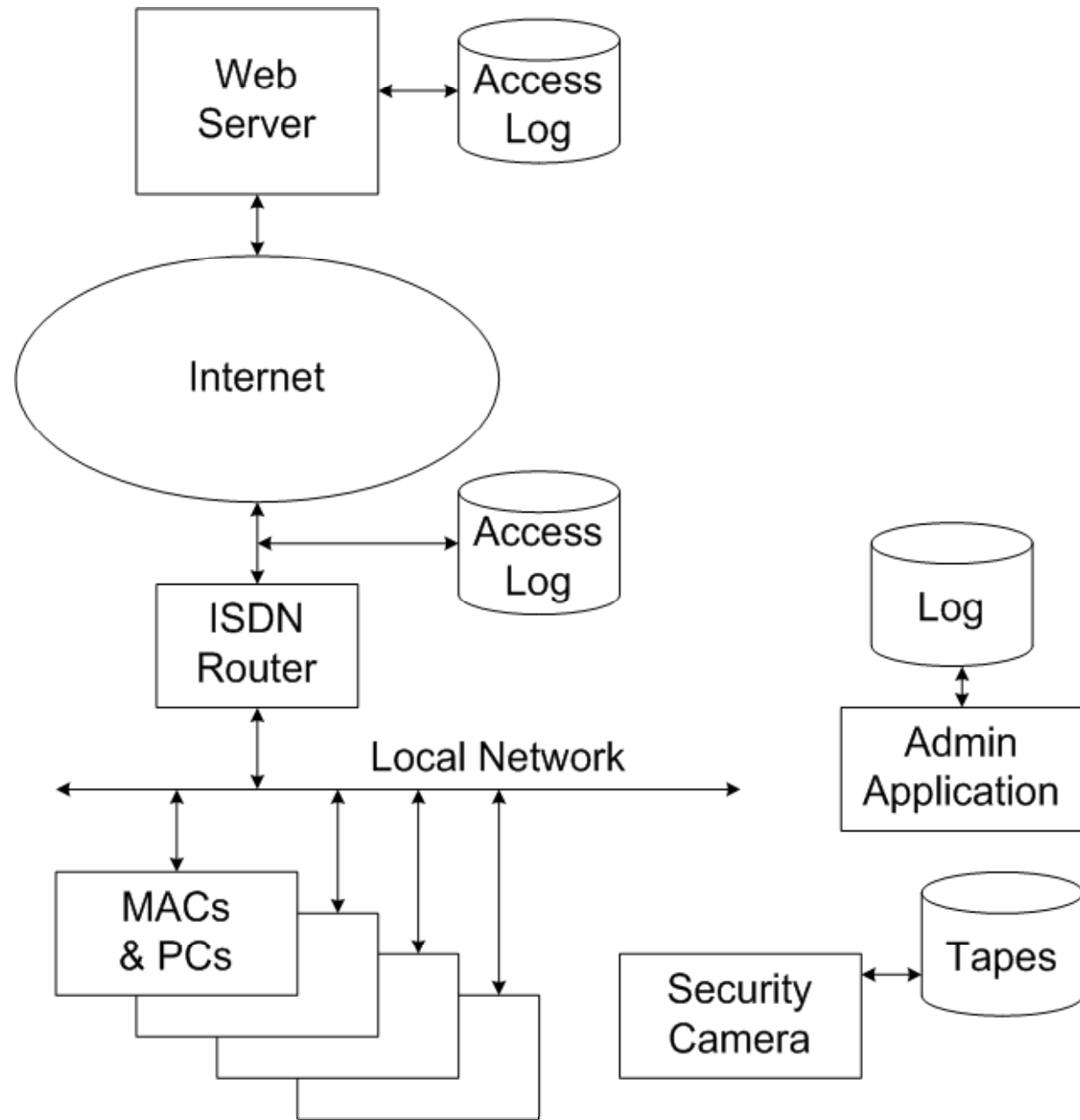
A Case Study



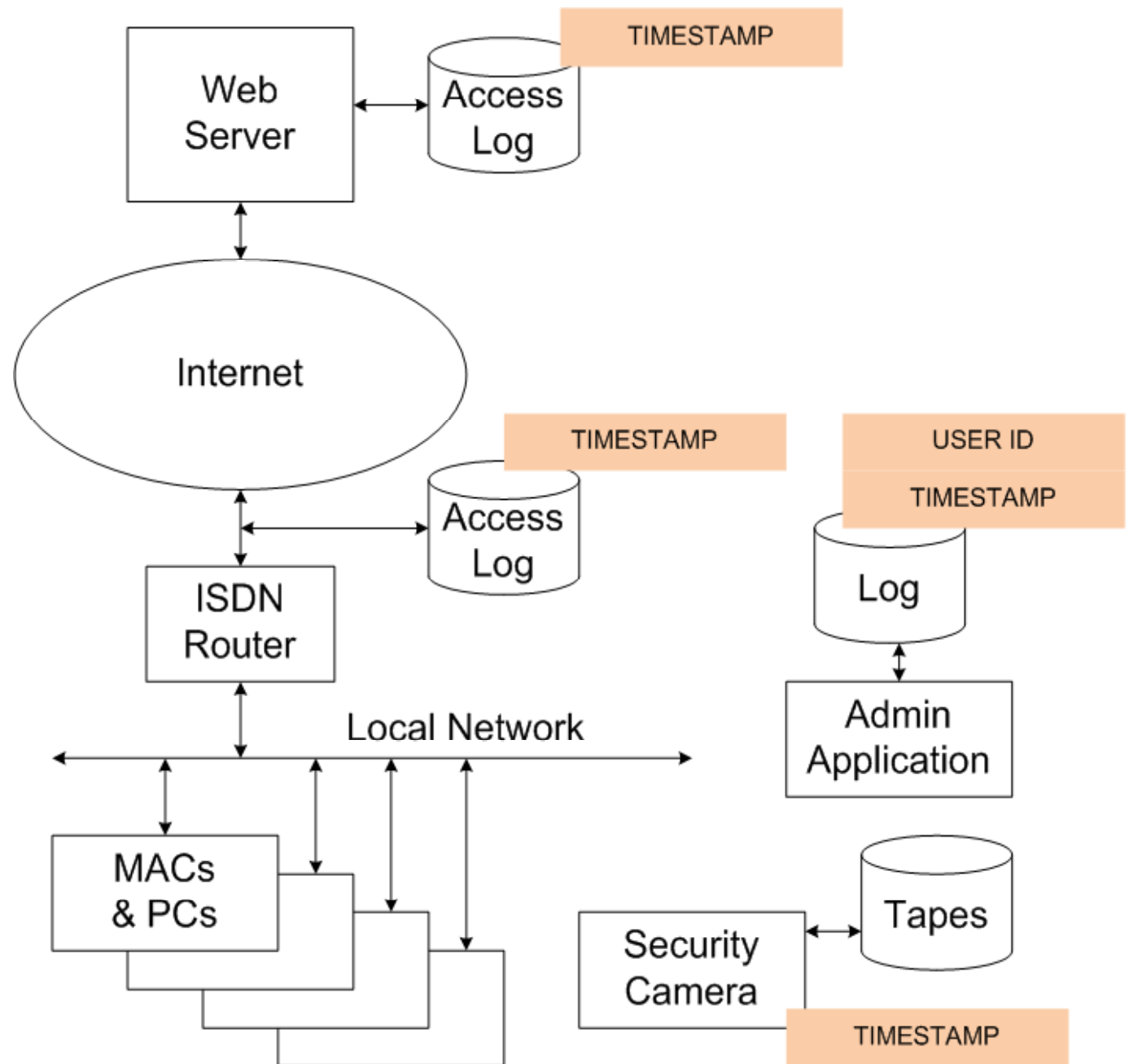
A Case Study



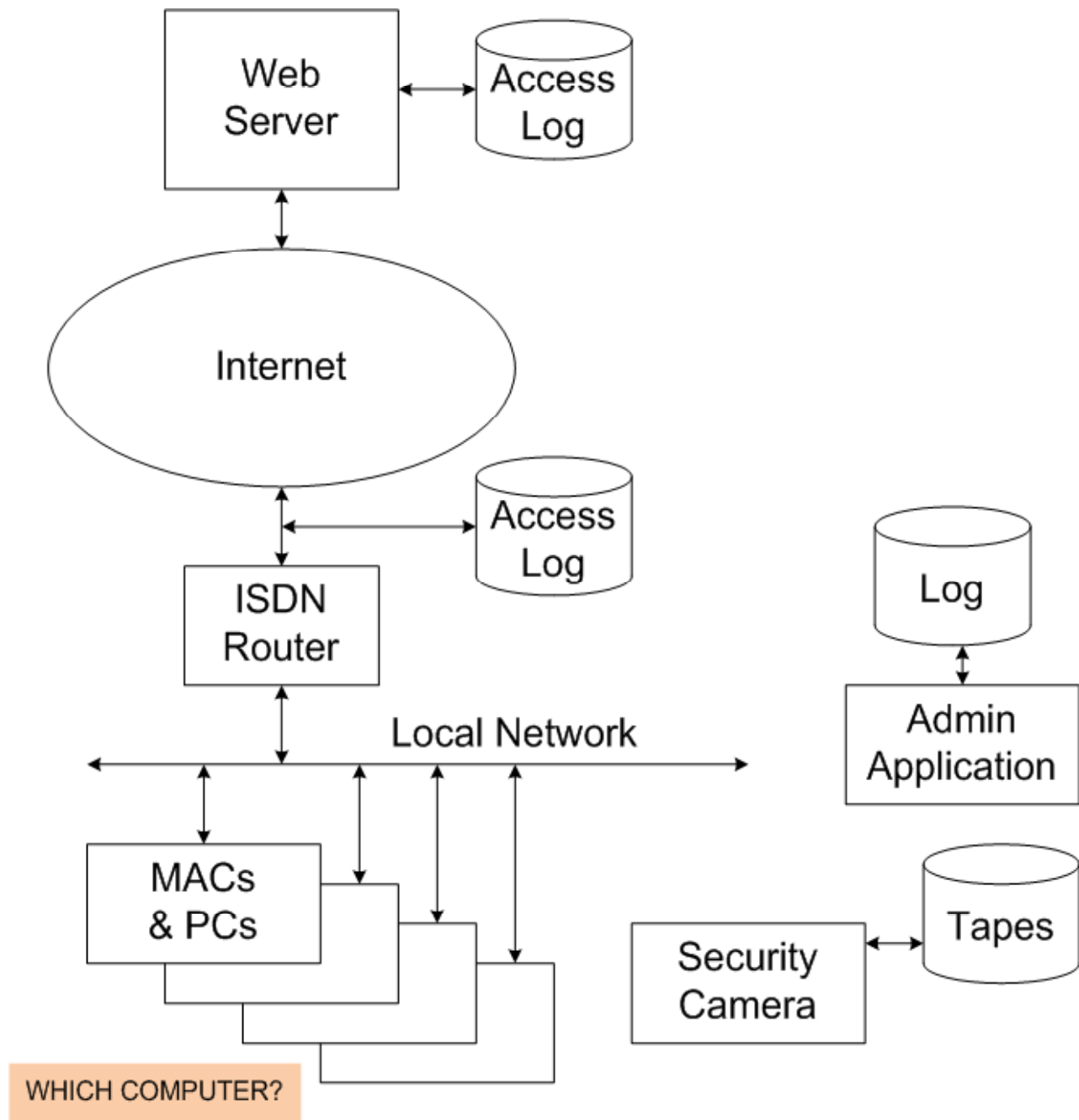
A Case Study



A Case Study



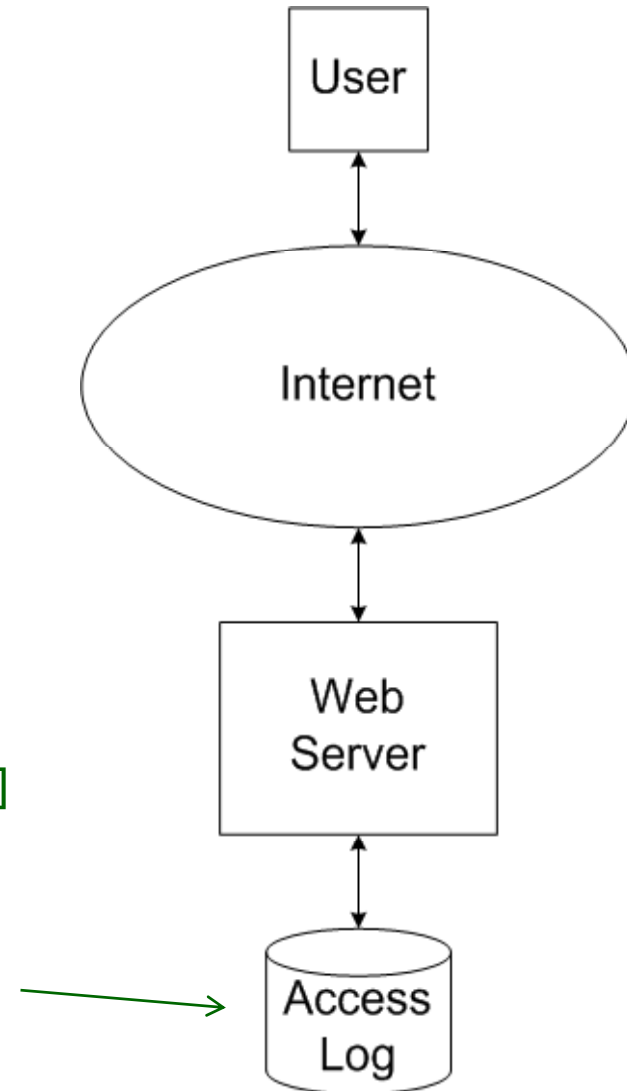
A Case Study



Endpoint Identification - Logging

Typical Web Server Logging

```
76.75.8.40 - - [14/Oct/2009:13:55:36 -0700]  
"GET /apache_pb.gif HTTP/1.0" 200 2326  
"http://www.example.com/start.html"  
"Mozilla/4.08 [en] (Win98; I ;Nav)"
```

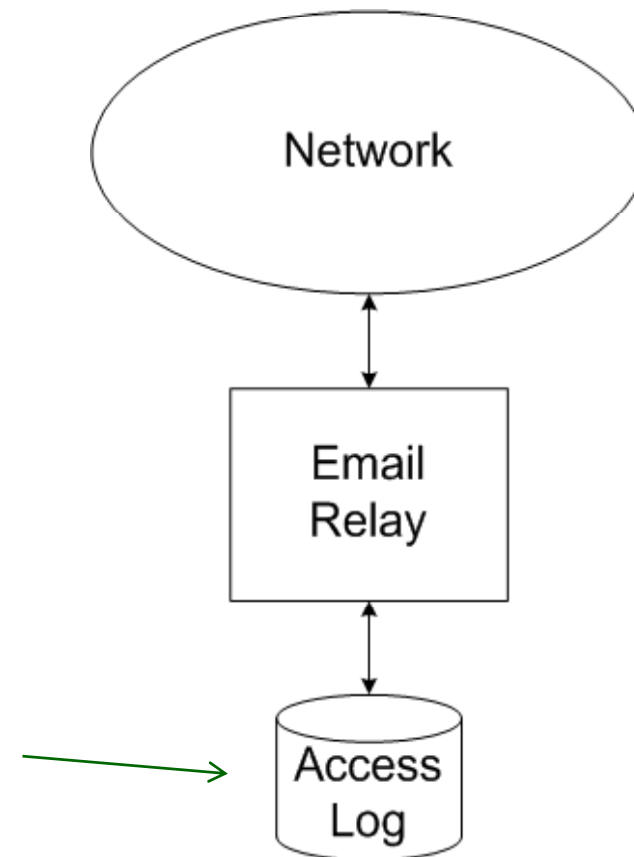


Endpoint Identification - Logging

Typical Email Relay Logging

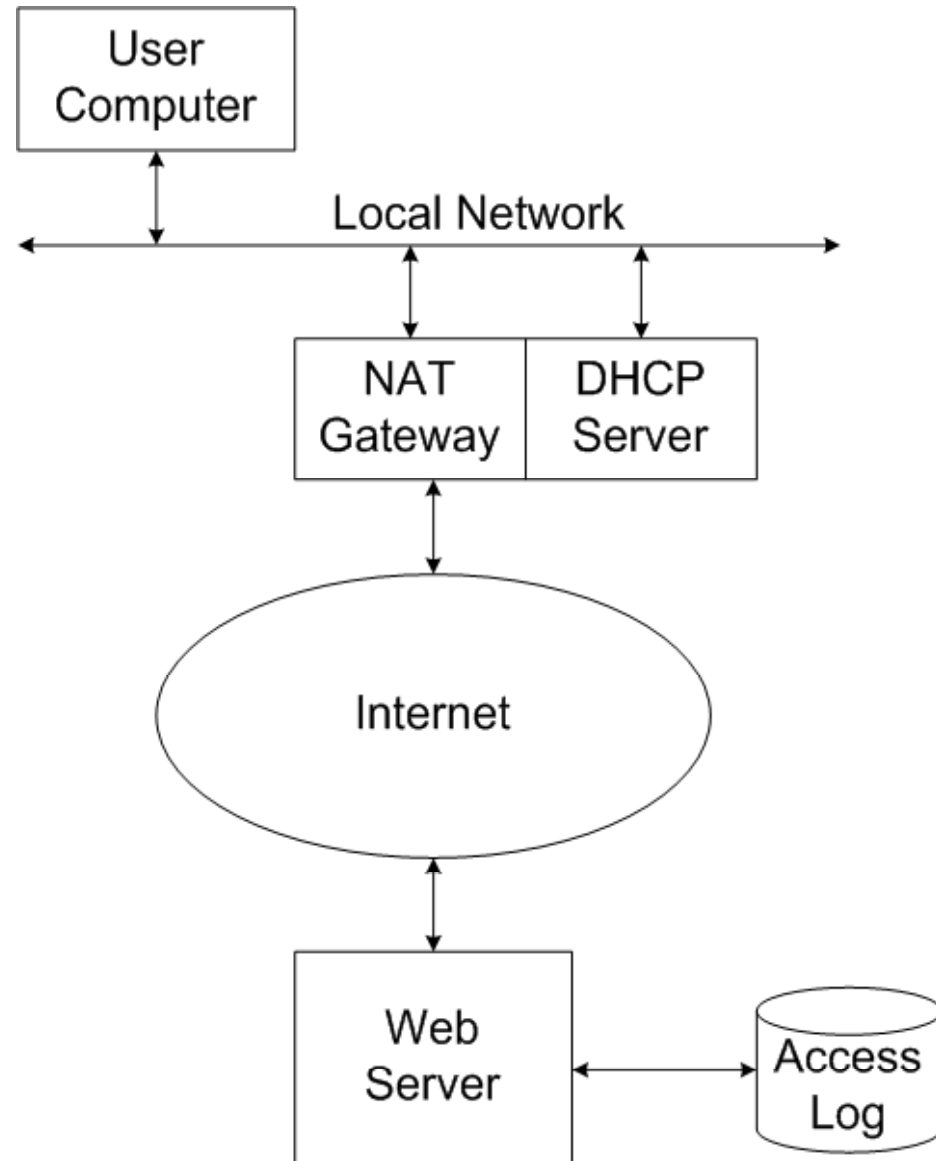
<date> <host> sendmail[pid]: <qid>:
<what>=<value>, ...

e.g.:
relay=76-75-8-40.vnet-inc.com [76.75.8.40]



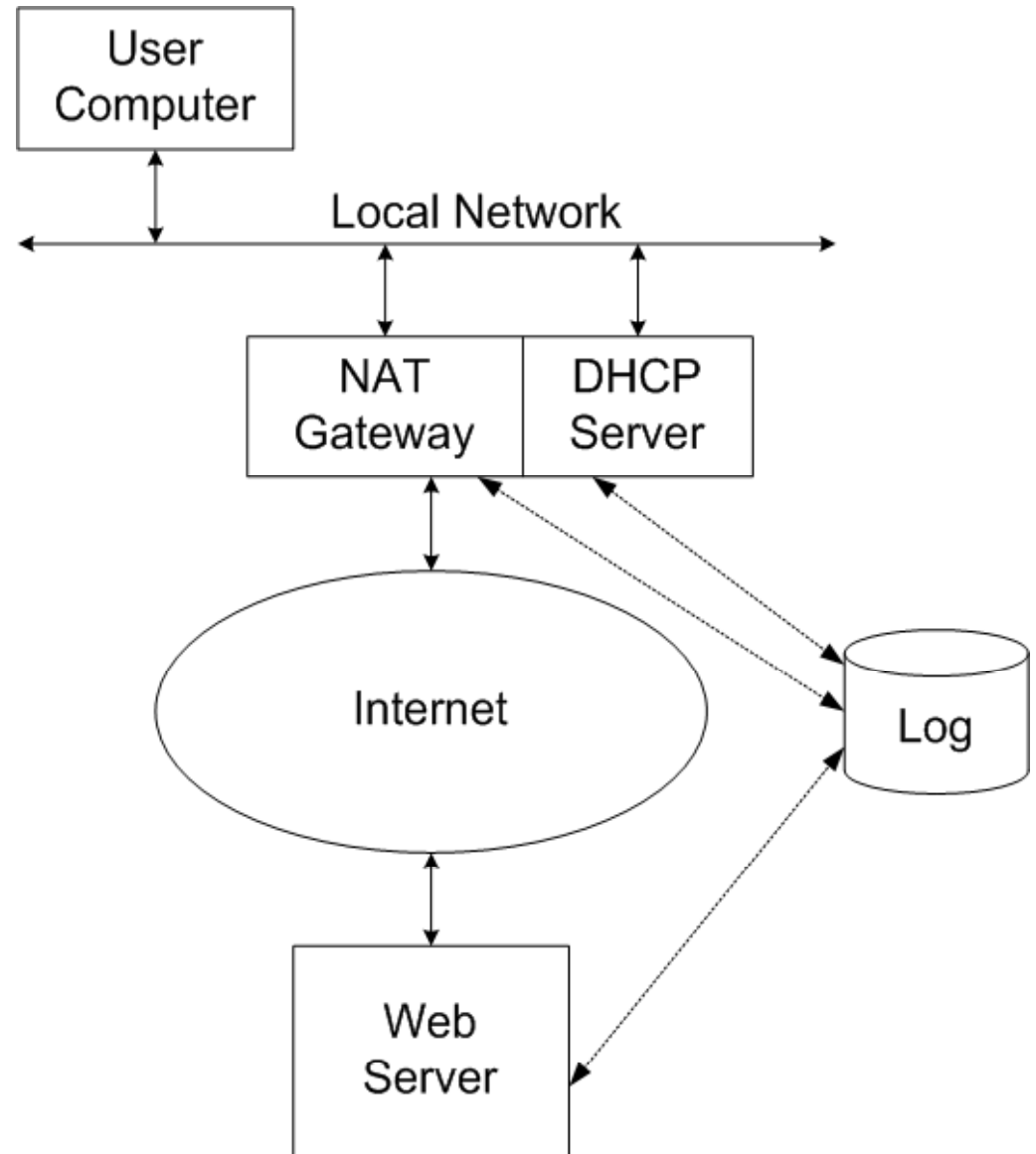
Endpoint Identification - Logging

Common Network Arrangement



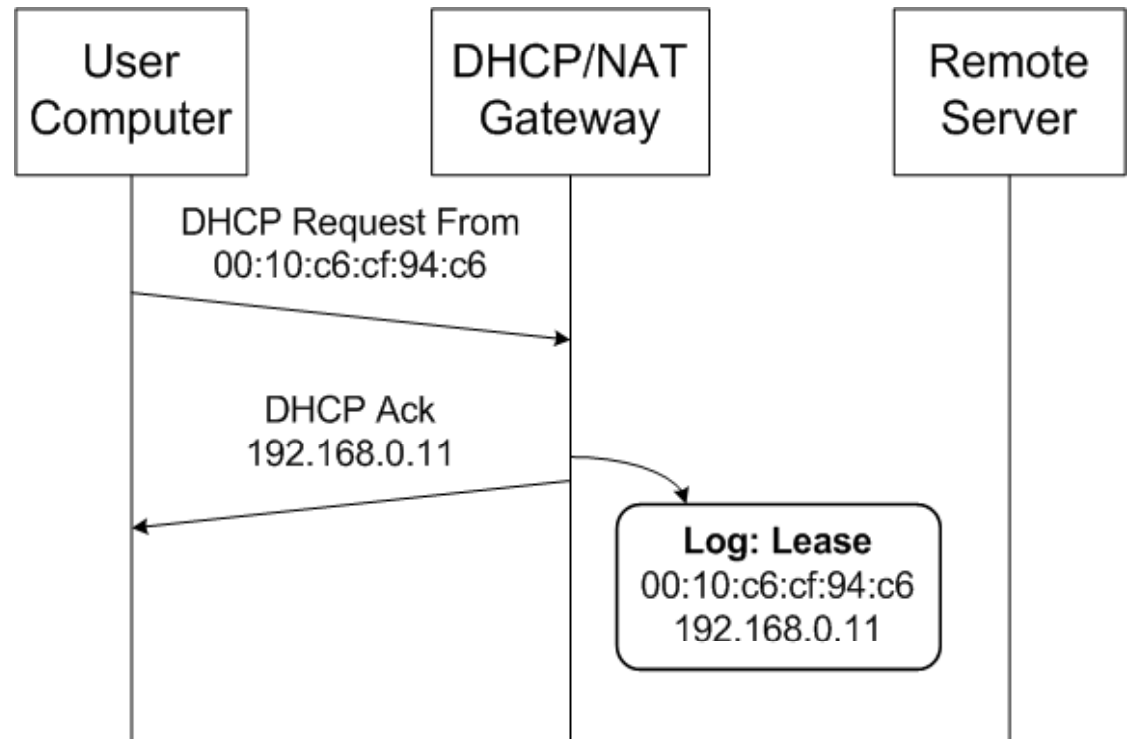
Endpoint Identification - Logging

Logging From Three Sources
DHCP Server
NAT Gateway
Web Server



Endpoint Identification - Logging

DHCP Lease Logging



User → Server: DHCPDISCOVER from 00:10:c6:cf:94:c6

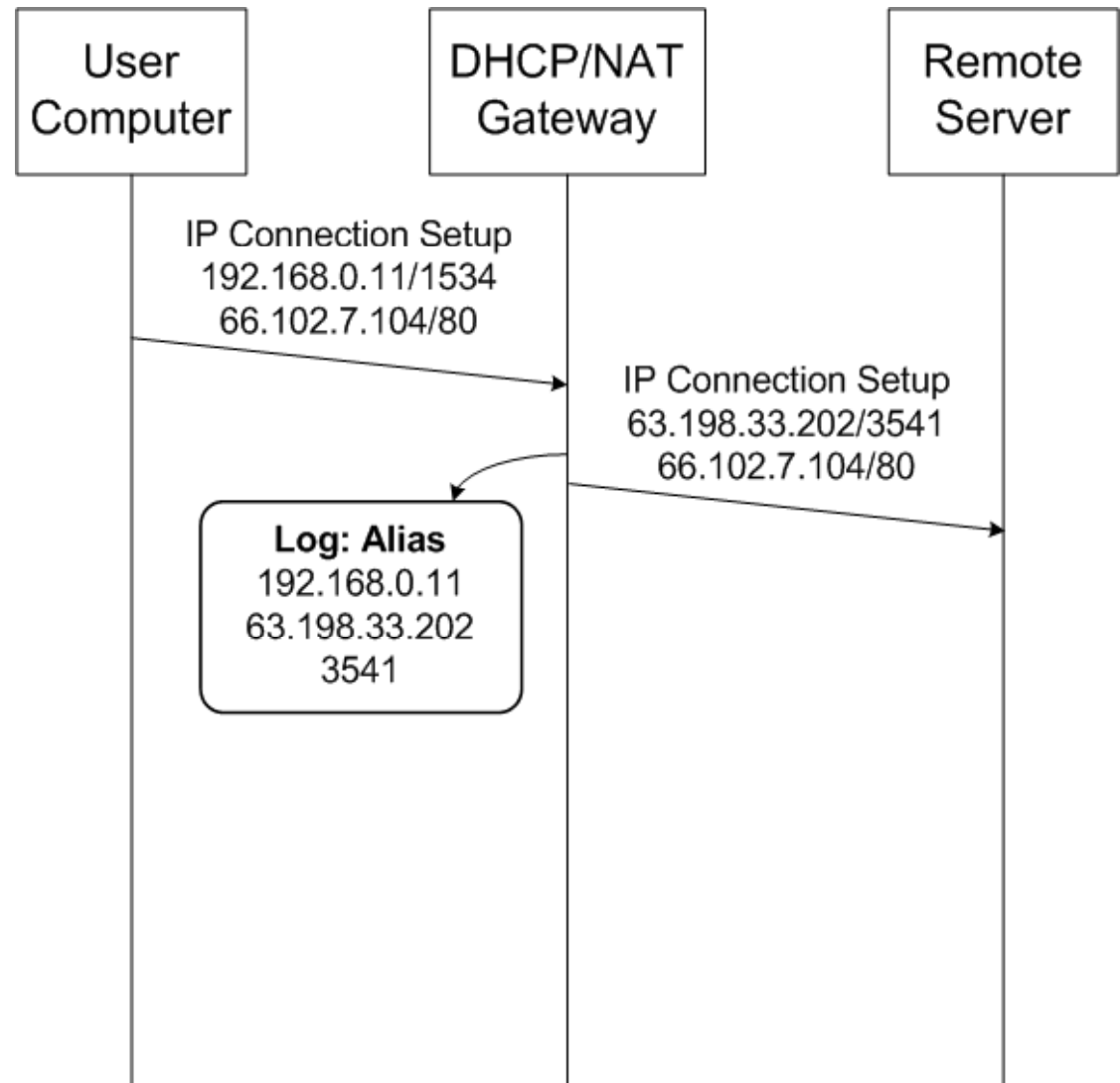
Server → User: DHCPOFFER on 192.168.0.11 to 00:10:c6:cf:94:c6

User → Server: DHCPREQUEST for 192.168.0.11 from 00:10:c6:cf:94:c6

Server → User: DHCPACK on 192.168.0.11 to 00:10:c6:cf:94:c6

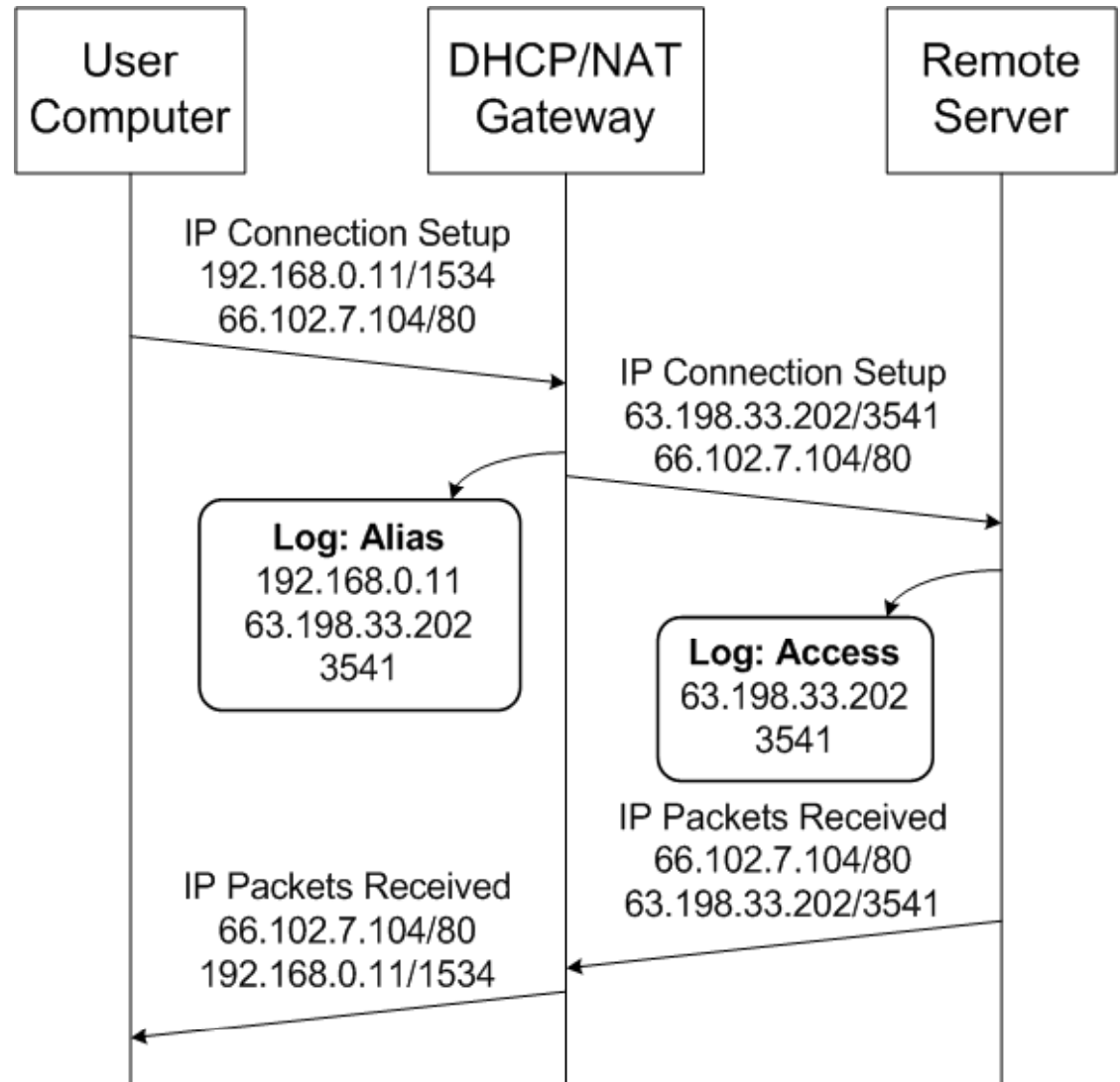
Endpoint Identification - Logging

NATD Alias Logging
Internal IP Address
External IP Address
External IP Port



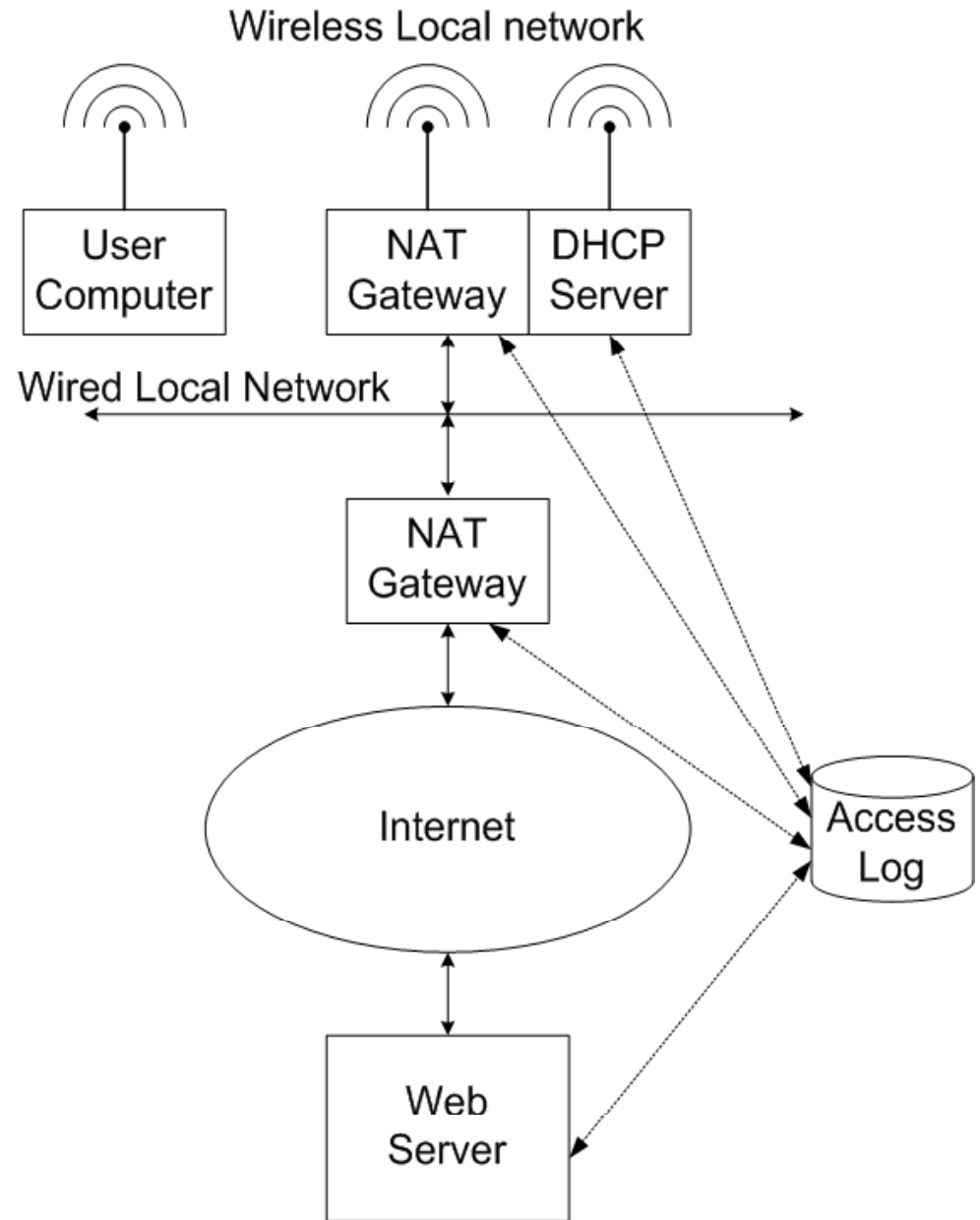
Endpoint Identification - Logging

Server Access Logging
Source IP Address
Source IP Port



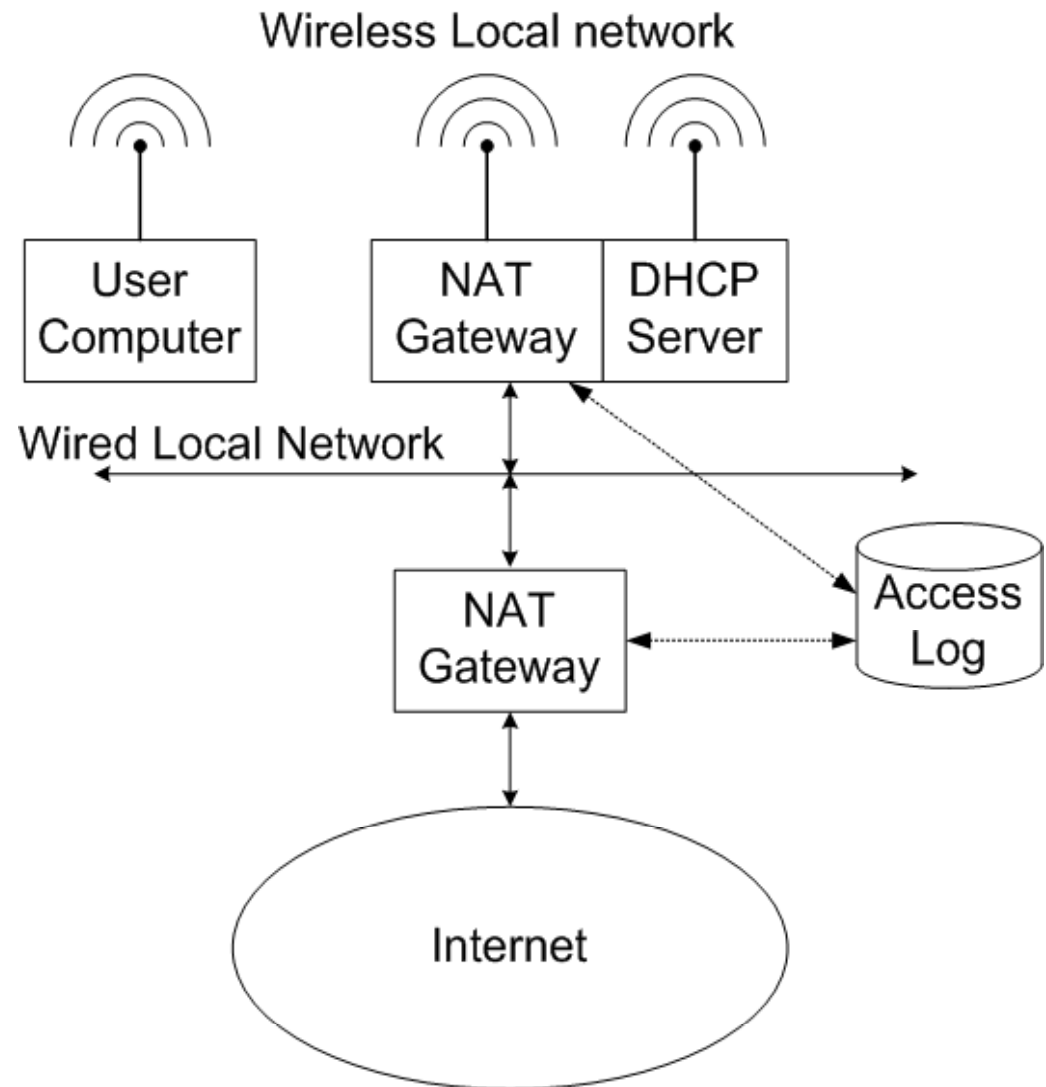
Endpoint Identification - Logging

Multiple NAT Gateways



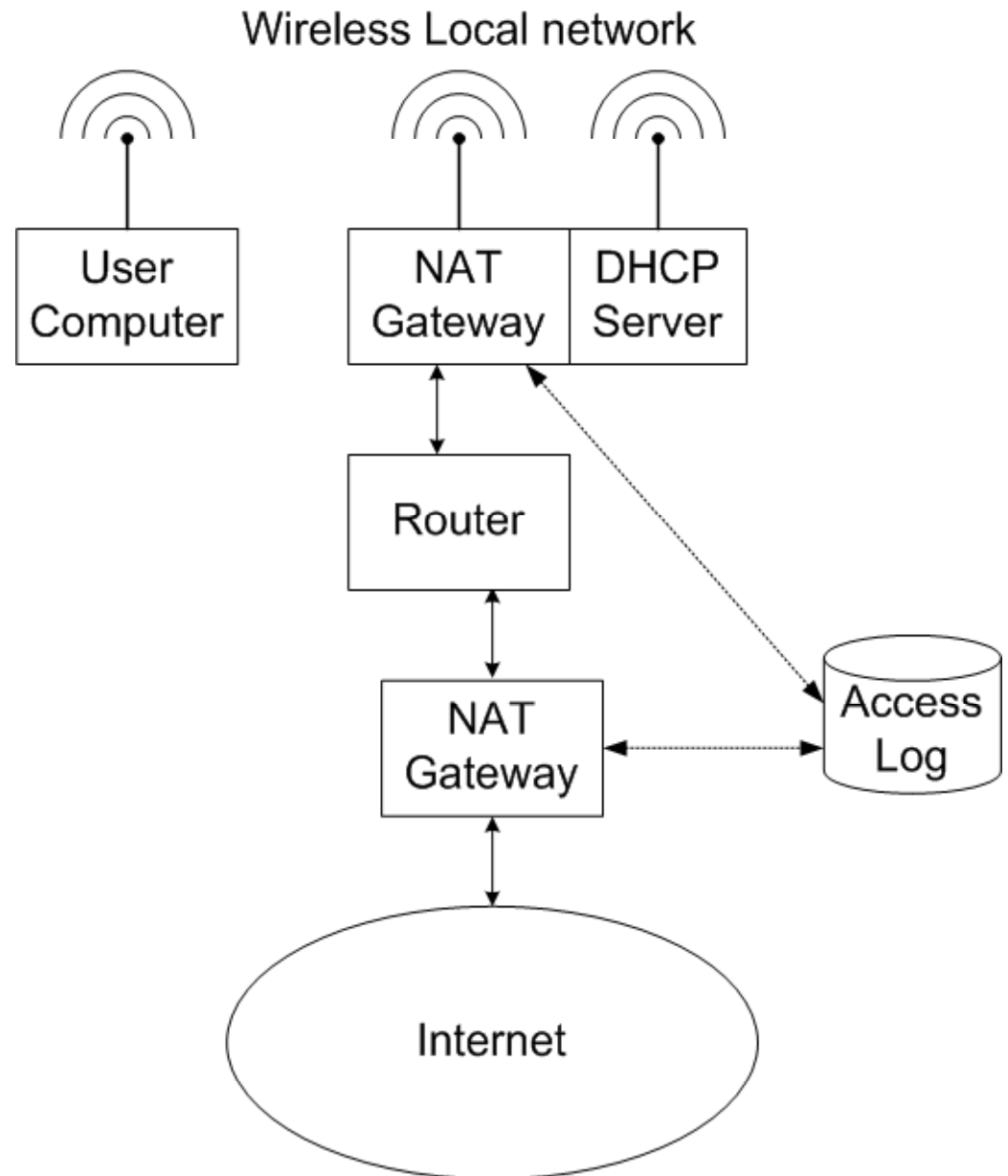
Endpoint Identification - Logging

Combination of
Lease (DHCP) and Alias (NAT)
Logging



Endpoint Identification - Logging

Combination of
Lease (DHCP) and Alias (NAT)
Logging

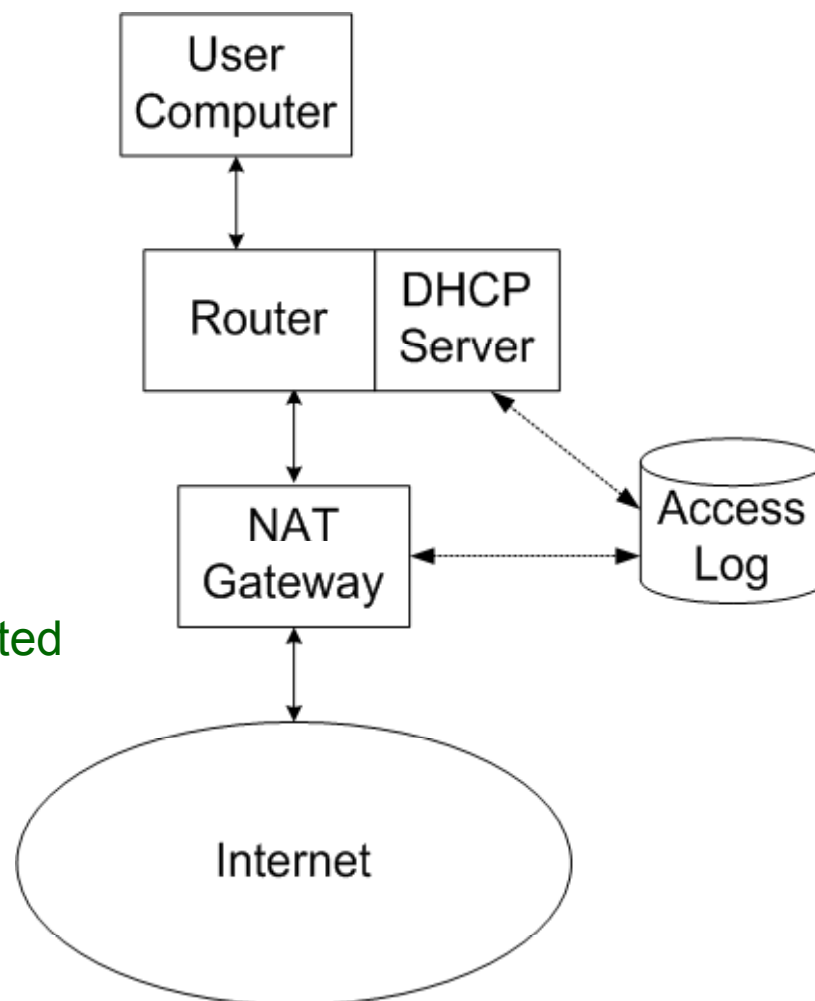


Endpoint Identification - Logging

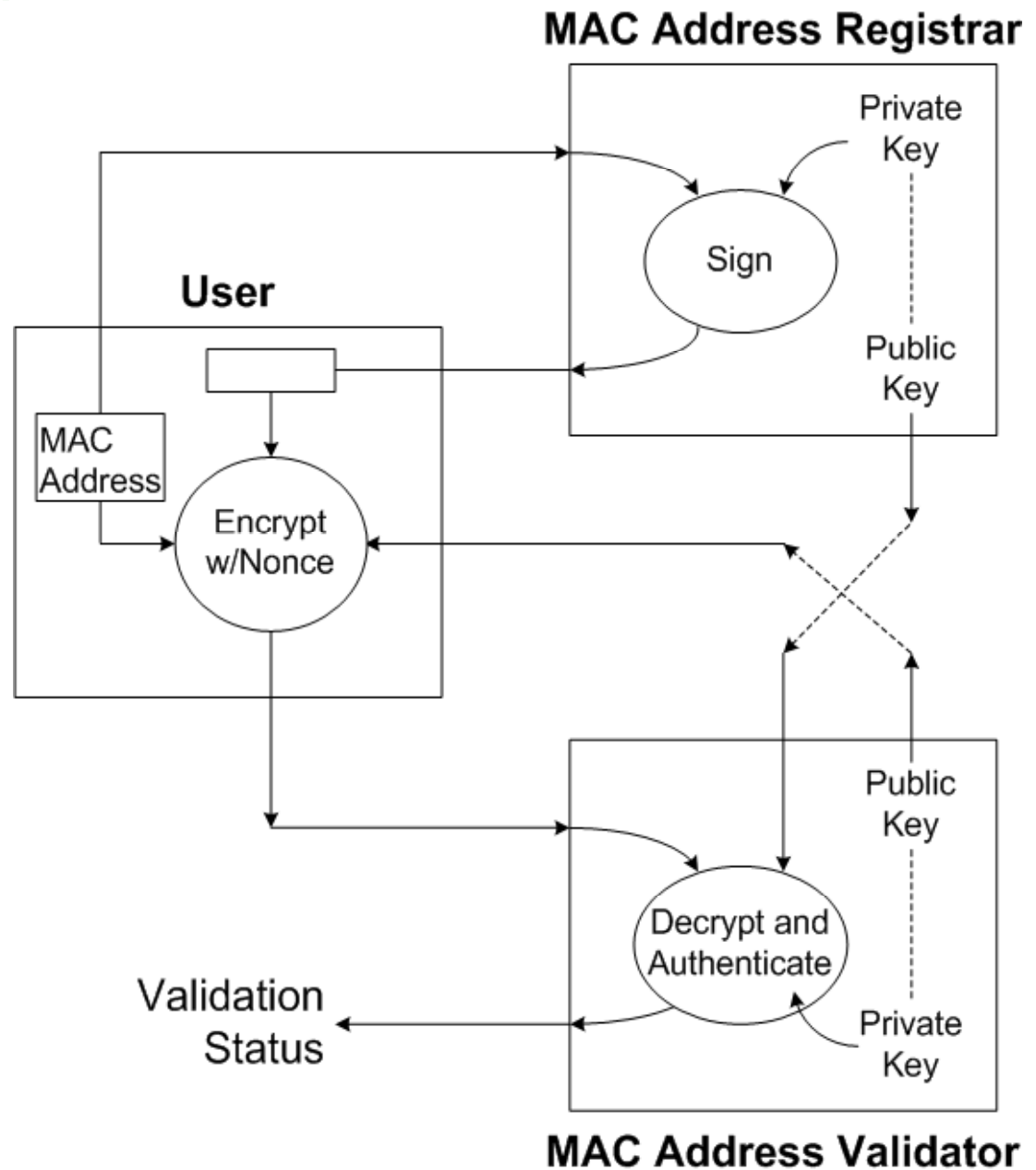
Combination of
Lease (DHCP) and Alias (NAT)
Logging

Summary:

1. MAC and IP Address of Originating Computer
2. Each Point Where IP Address Is Translated

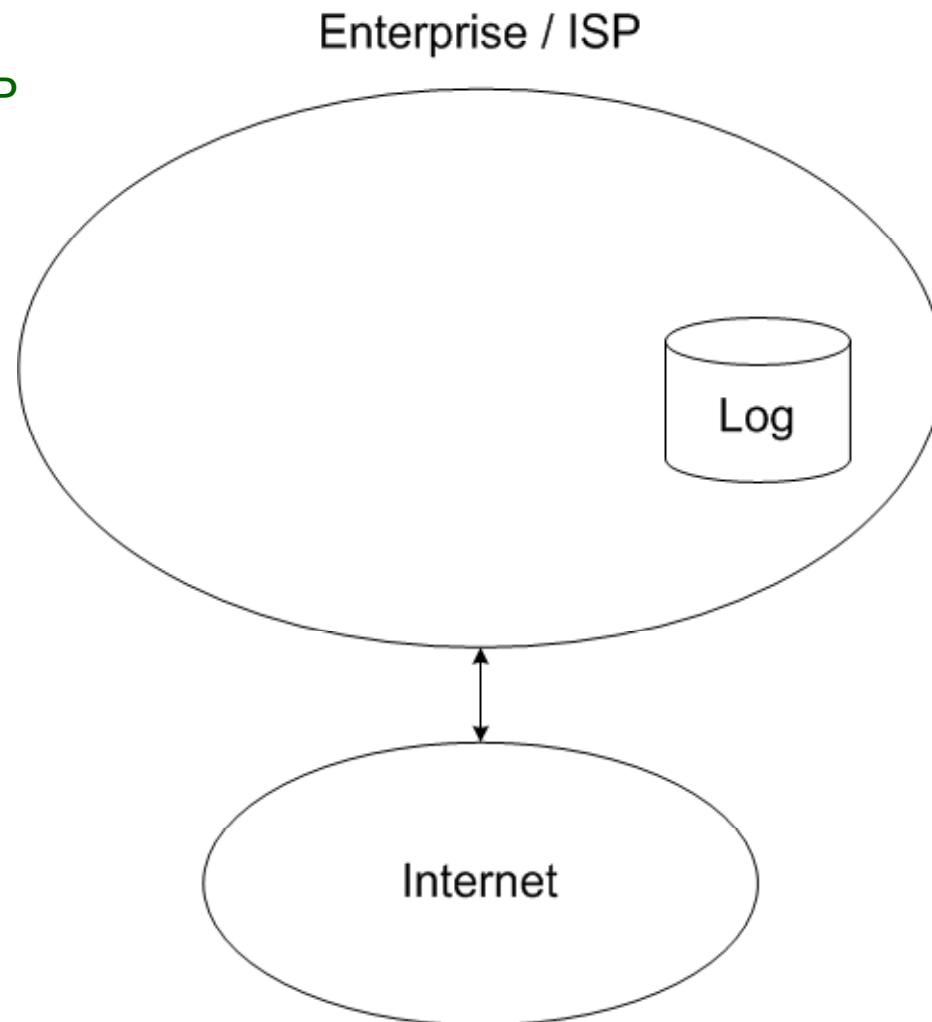


MAC Address Validation



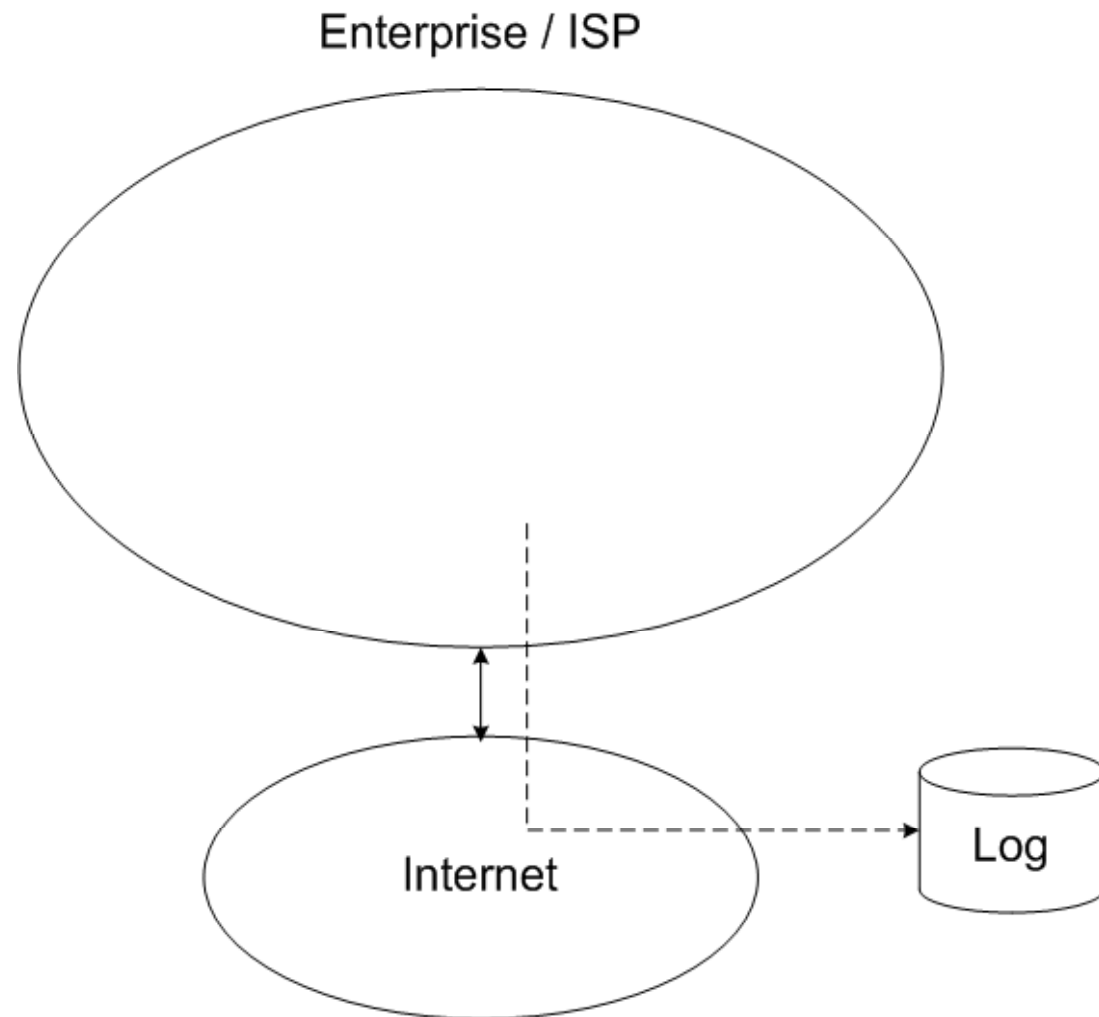
Log State Management

Source Log Files Stored
Internal to Enterprise / ISP



Log State Management

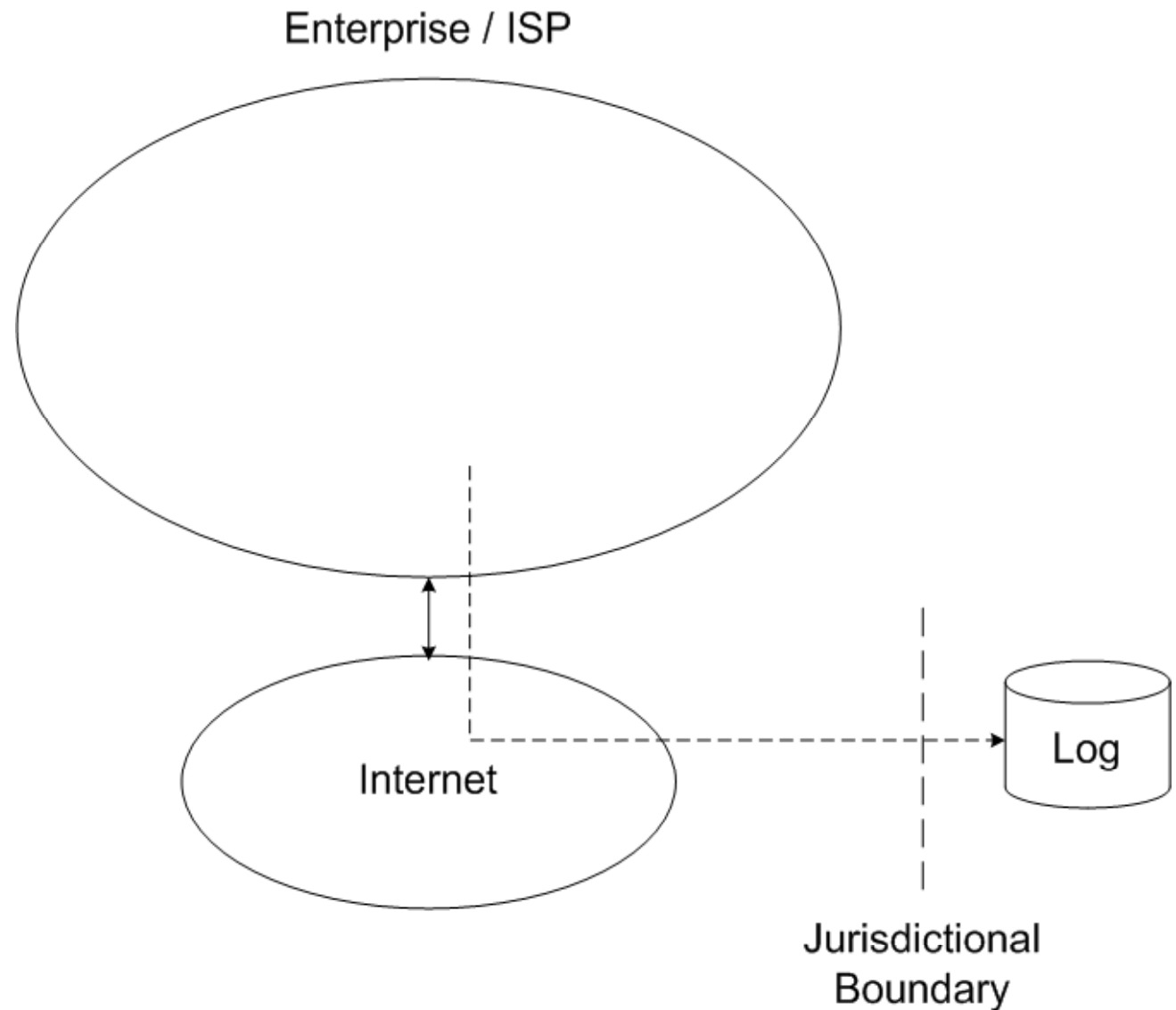
Source Log Files Stored Remotely



Log State Management

Source Log Files Stored
Remotely And Outside
Jurisdiction

“Virtual Deletion”



Why Identify Endpoints? – Social Issues

Motivation

Debugging - Monitoring

Liability

Detection of Abuse

Regulation

Why Identify Endpoints? – Social Issues

Accountability

Contrast With Protection

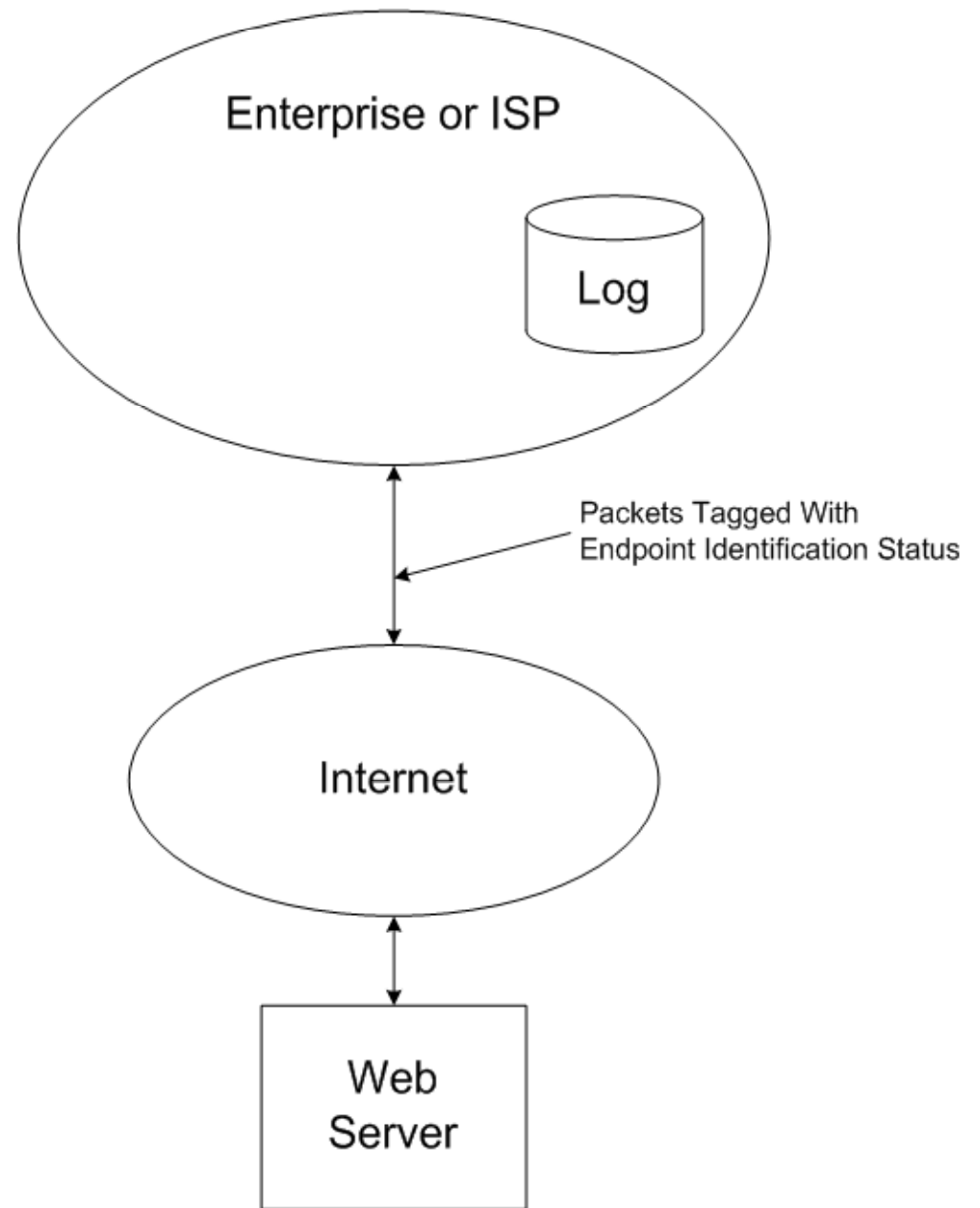
Retrospective vs. Real Time

Anonymity

Privacy Issues

Packet Tagging

Packets Tagged With Status
Identification Status
MAC Validation Status
Core / Server Use
Access Control
Differentiated Services



Summary

- Endpoint Identification Logging
 - MAC to IP Association (e.g. DHCP)
 - IP Address Translation – All (e.g. NAT)
 - IP Address & Source Port at Server
- MAC Address Validation
- Log State Management
- Social Issues