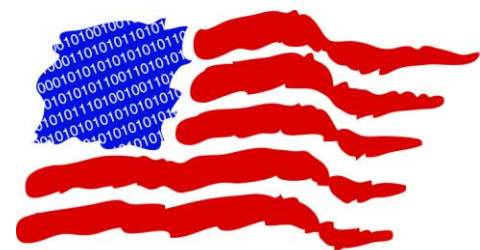


**U** CYBER CORPS  
Defending America's Cyberspace

0100101010010101010101001100101010101000010101010101010100010100100 —●

# Security Analysis of the MPLS Label Distribution Protocol

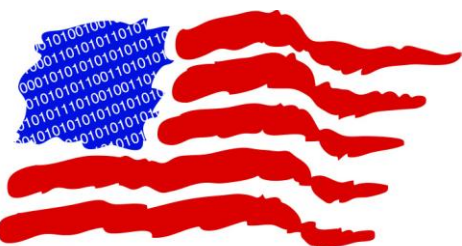
D. Guernsey, A. Engel, J. Butts, S. Sheno  
Department of Computer Science  
University of Tulsa  
Tulsa, Oklahoma 74104, USA



# What is MPLS?

010010101001010101010100110010101010100001010101010101010100010100100 —●

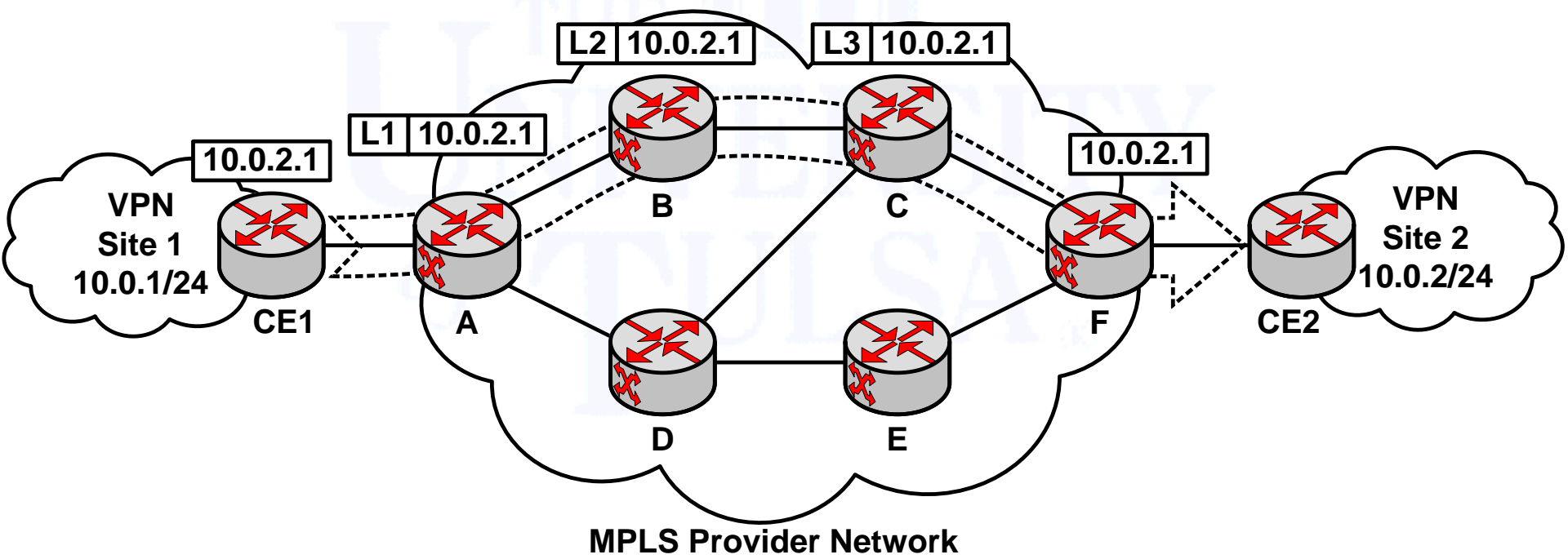
- **Multi-Protocol Label Switching**
- **Designed to make packet-switching speeds comparable to circuit-switching speeds**
- **Exceptional interoperability and flexibility**
- **Support for QoS and CoS**
- **Applications can leverage high-speed paths**

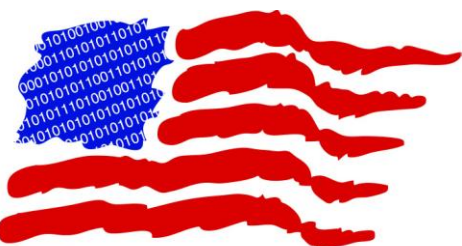


# MPLS Forwarding

01001010100101010101010011001010101010000101010101010101010100010100100

- Similar to US Postal ZIP codes
- Penultimate hop popping

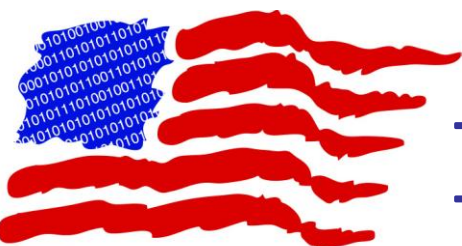




# Control Plane

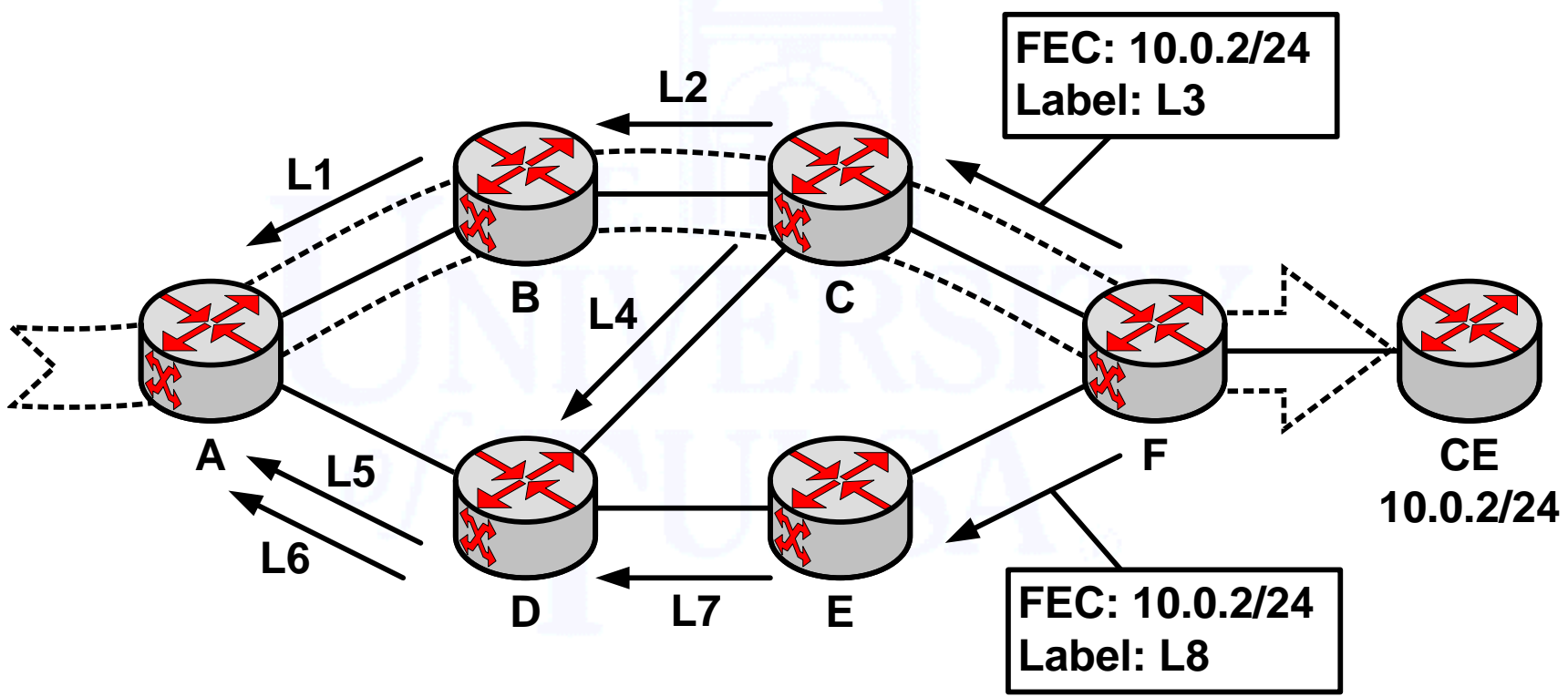
01001010100101010101010011001010101010000101010101010101010100010100100 —●

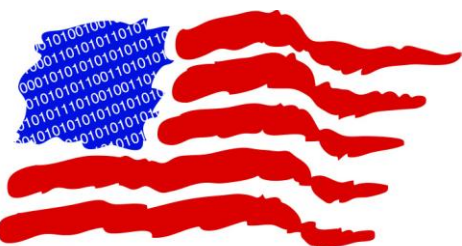
- **Paths to emulate IP**
  - Must be constructed and distributed by some protocol
- **Two options**
  - Piggyback onto existing protocols (MP-BGP, RSVP-TE)
  - Create a new protocol (LDP)
- **Label Distribution Protocol**
  - Essentially transforms routes from IP tables into Label Switched Paths
  - Creates paths used by other protocols to satisfy QoS and CoS requirements and connect remote VPN sites



# Label Distribution Protocol

01001010100101010101010100110010101010100001010101010101010100010100100

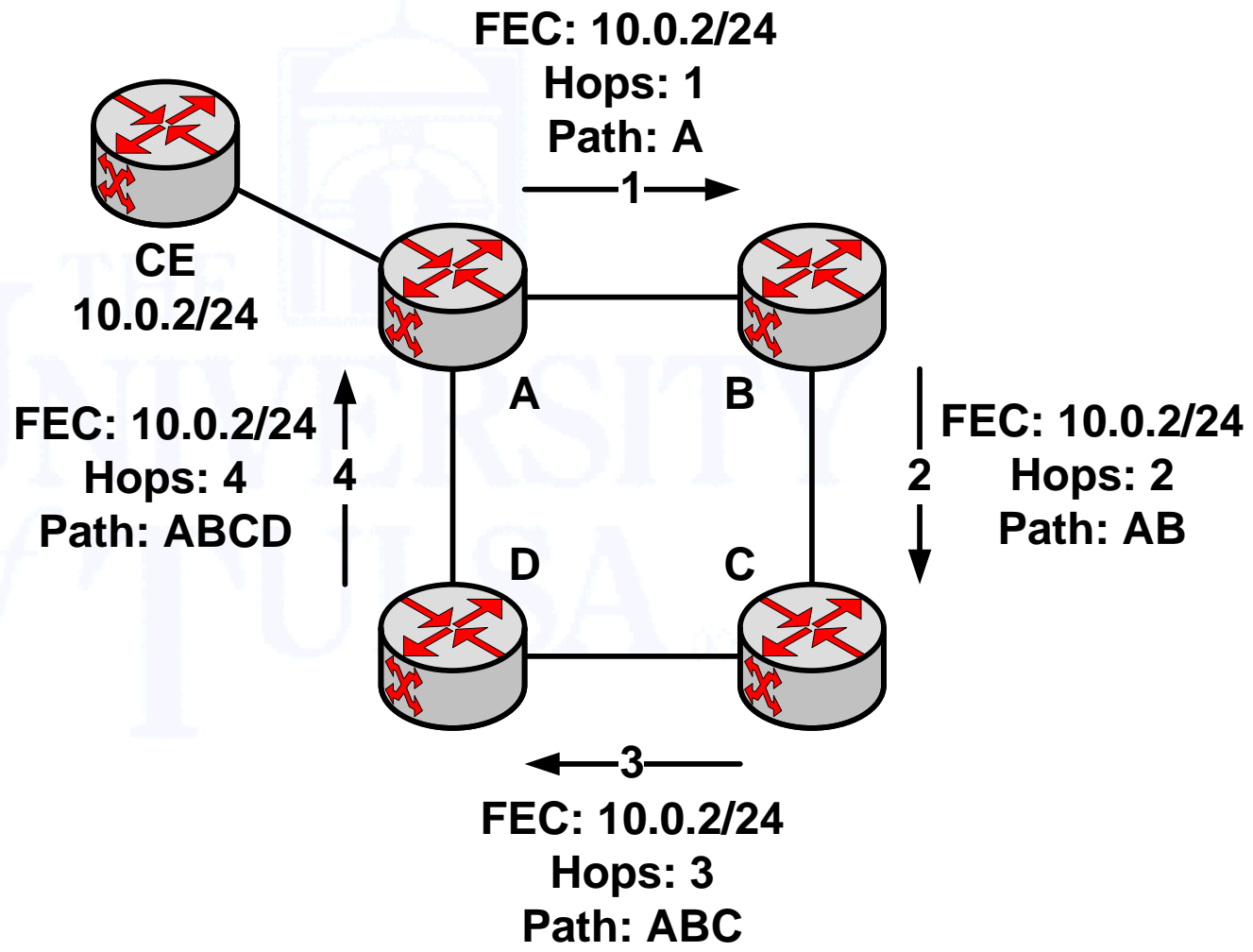


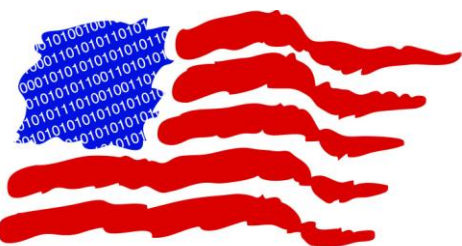


# Loop Detection

010010101001010101010100110010101010100001010101010101010101000010100100

- Hop count
- Path vector



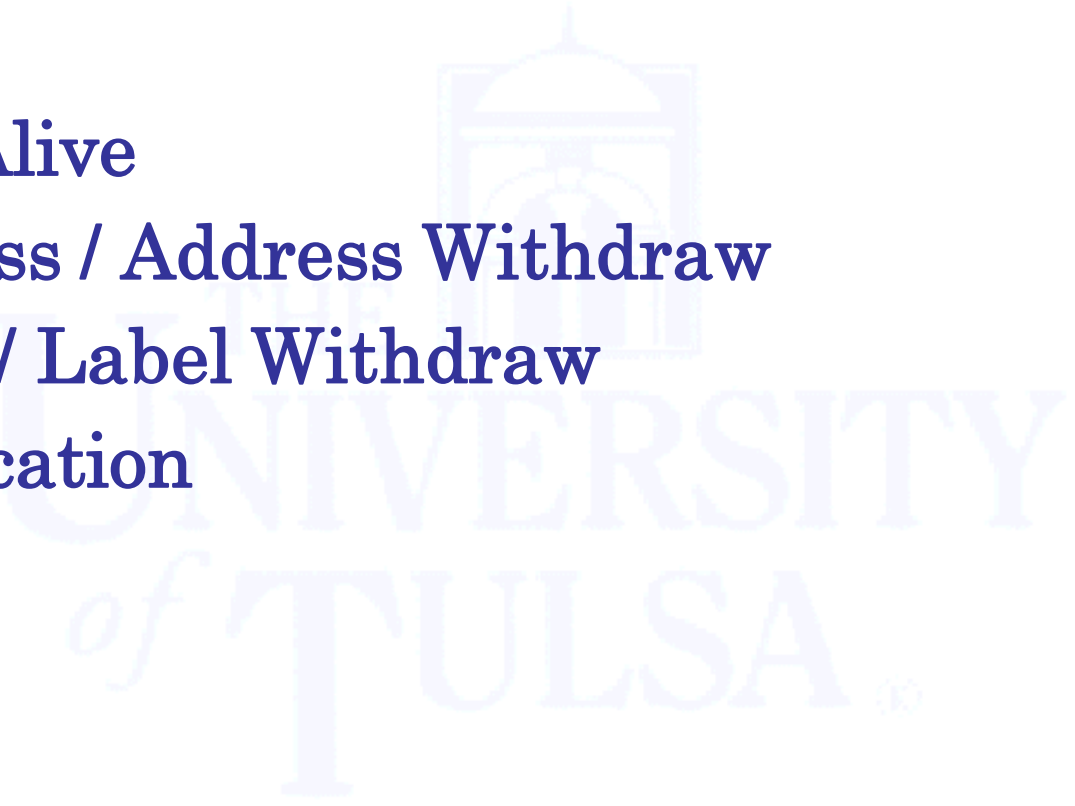


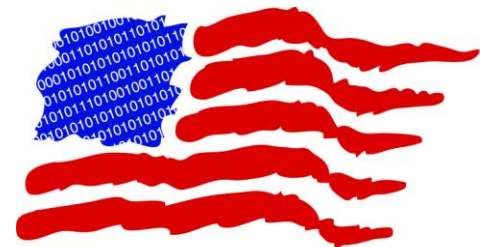
# Message Types



010010101001010101010100110010101010100001010101010101010100010100100 —●

- Hello
- KeepAlive
- Address / Address Withdraw
- Label / Label Withdraw
- Notification

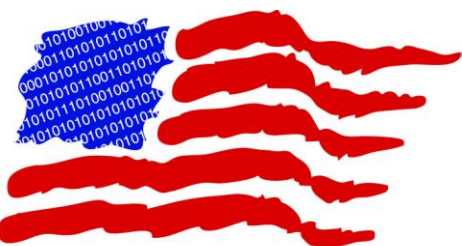




# Vulnerabilities

01001010100101010101010011001010101010000101010101010101010100010100100 —●

- **LDP specification**
  - Inherent protocol weaknesses
  - All LDP network susceptible
- **Service provider implementation**
  - Code flaws
  - Configuration errors
- **Underlying infrastructure**
  - IT / network assets
  - Policy

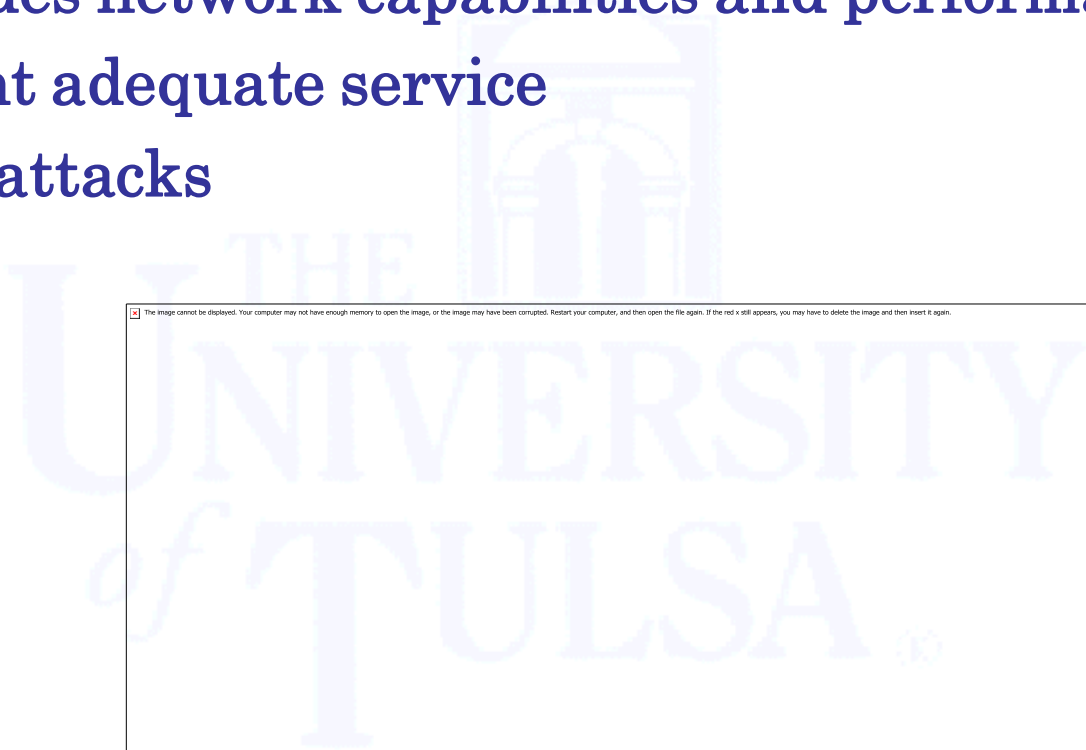


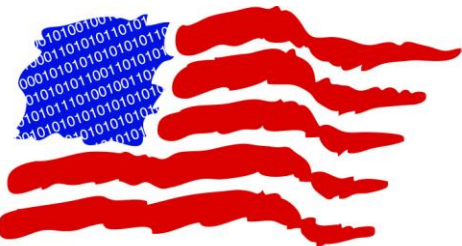
# Denial of Service



010010101001010101010100110010101010100001010101010101010100010100100 —●

- Degrades network capabilities and performance
- Prevent adequate service
- 6 DoS attacks





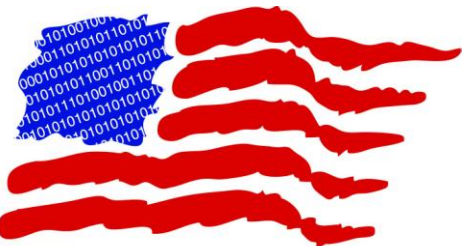
# Fabricating Notification Messages



0100101010010101010101001100101010101000010101010101010100010100100 —●

- Targets a network link
- A and B remove learned labels
- Cascading withdrawal of labels





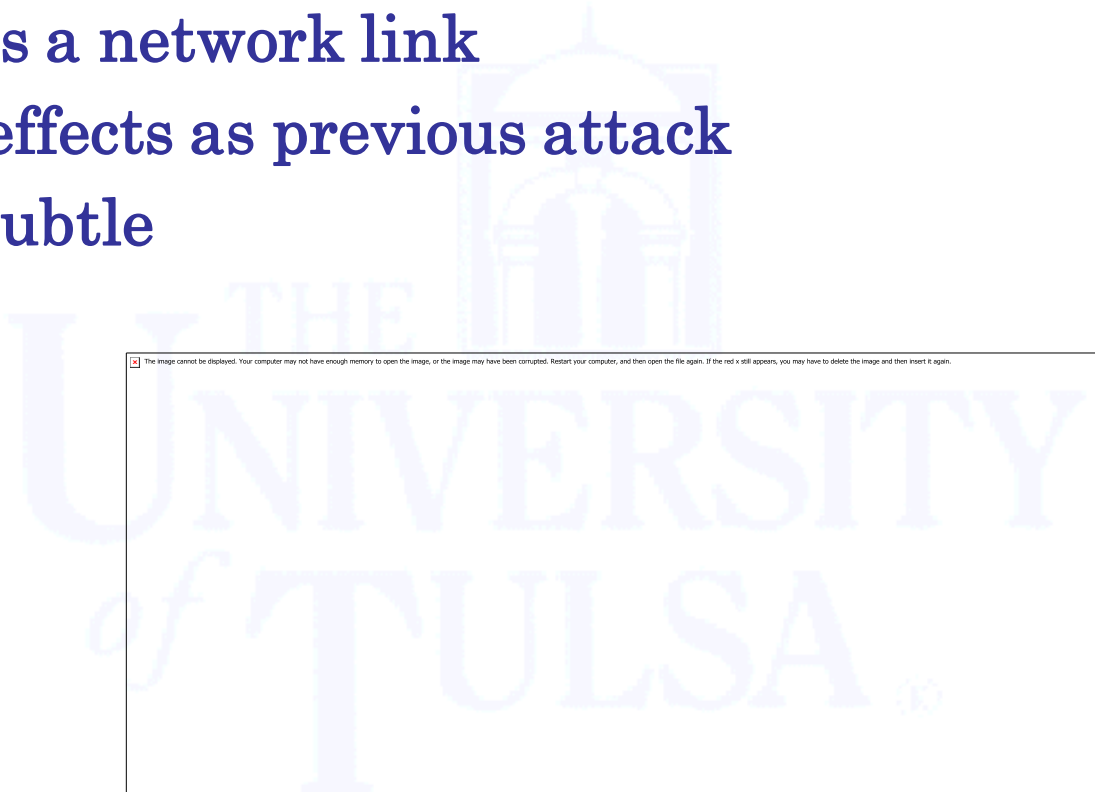
**U** CYBER CORPS  
Defending America's Cyberspace

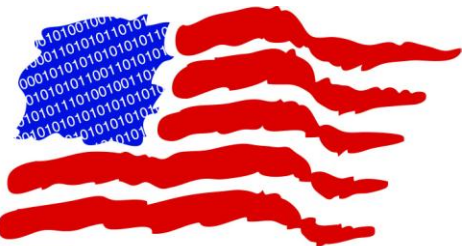
# Blocking KeepAlive Messages

0100101010010101010101001100101010101000010101010101010100010100100 —●

- Targets a network link
- Same effects as previous attack
- More subtle

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.



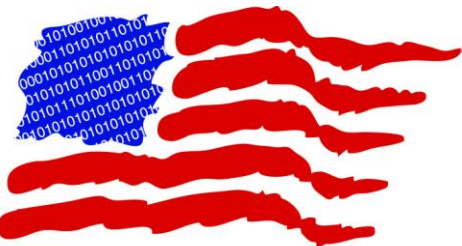


# Fabricating Address Withdraw Messages

010010101001010101010100110010101010100001010101010101010100010100100 —●

- Targets a sequence of three routers
- Attacker can target BAC or BAD.
- A withdraws from B its address to D
- Destroys all paths traversing BAD



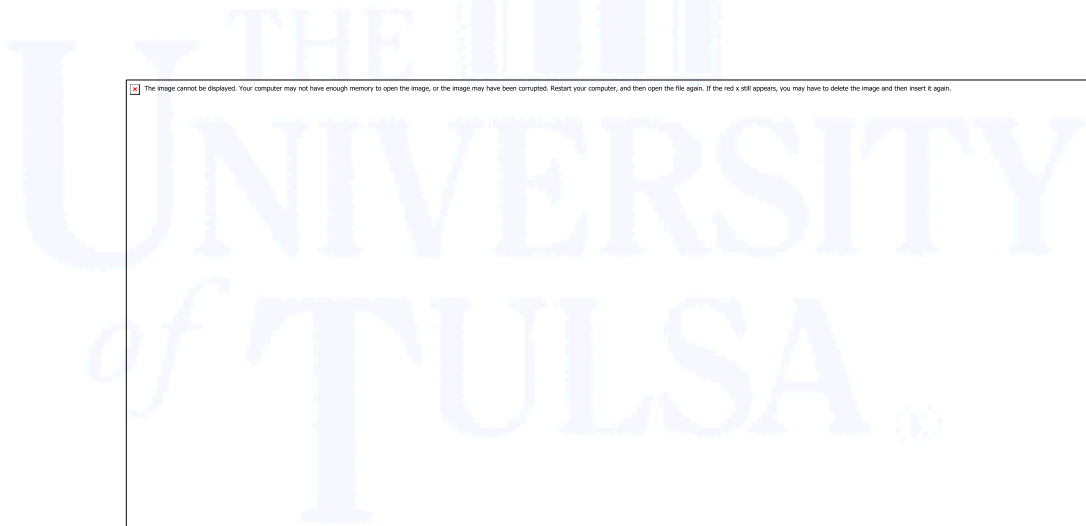


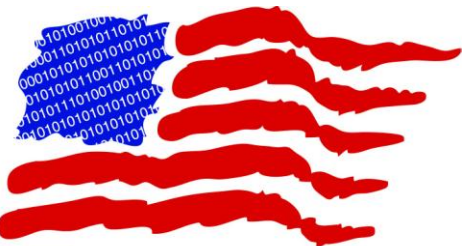
# Fabricating Label Withdraw Messages

010010101001010101010100110010101010100001010101010101010100010100100 —●

- Targets a specific LSP
- Access anywhere on the path
- Affects merged paths

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.





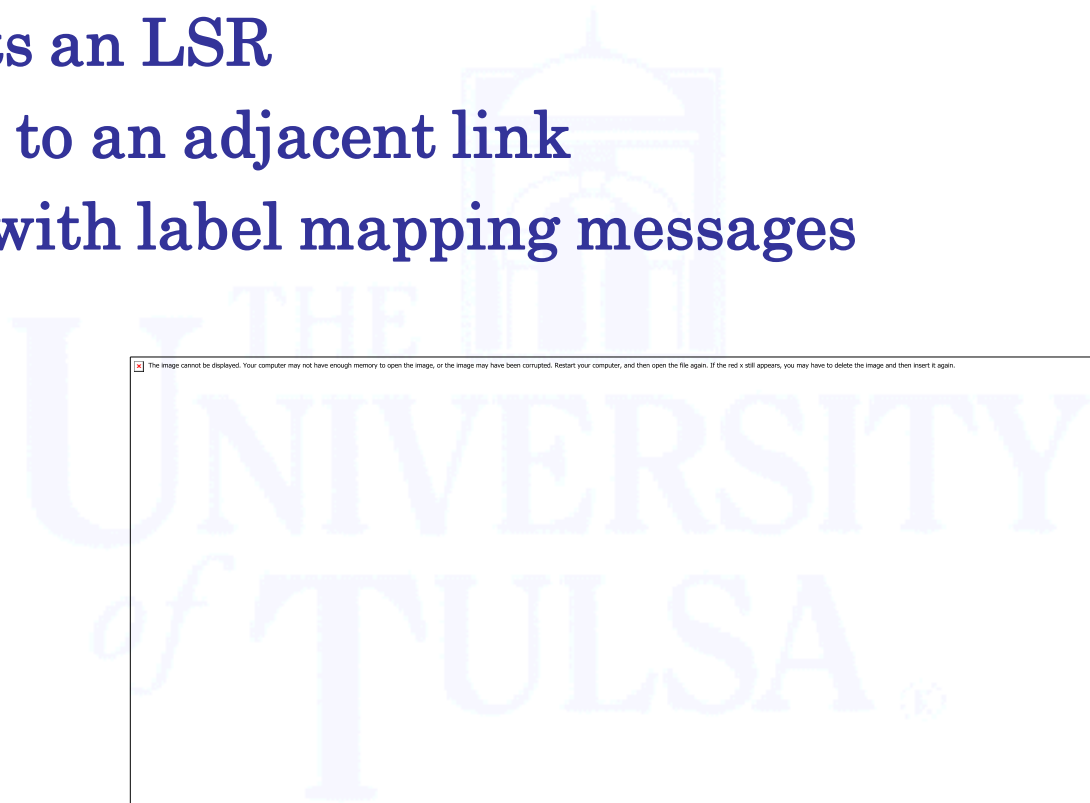
# Exhausting Label Memory

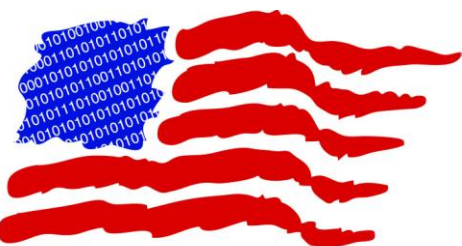


010010101001010101010100110010101010100001010101010101010100010100100 —●

- Targets an LSR
- Access to an adjacent link
- Flood with label mapping messages

 The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

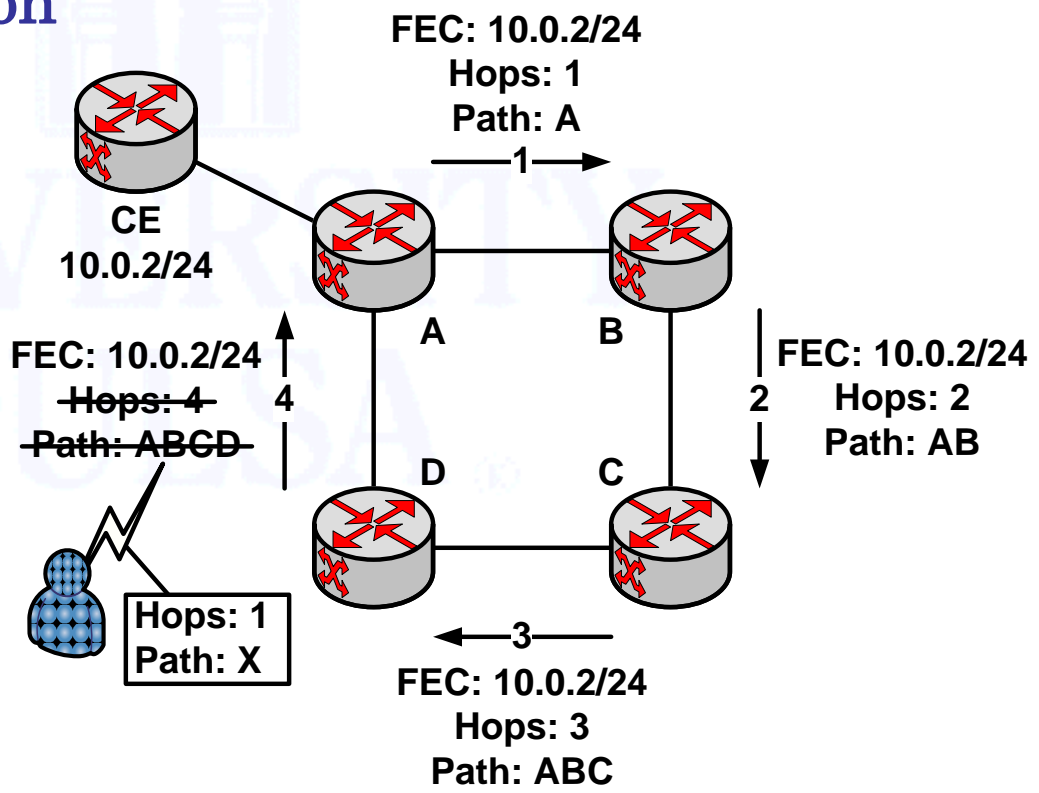


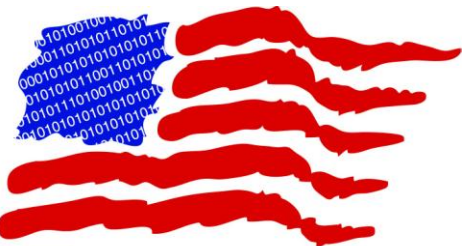


# Creating Loops

0100101010010101010101010011001010101010000101010101010101010100010100100

- Degrades performance in some portion
- Need access on a potential loop
- Modifying loop detection message parameters

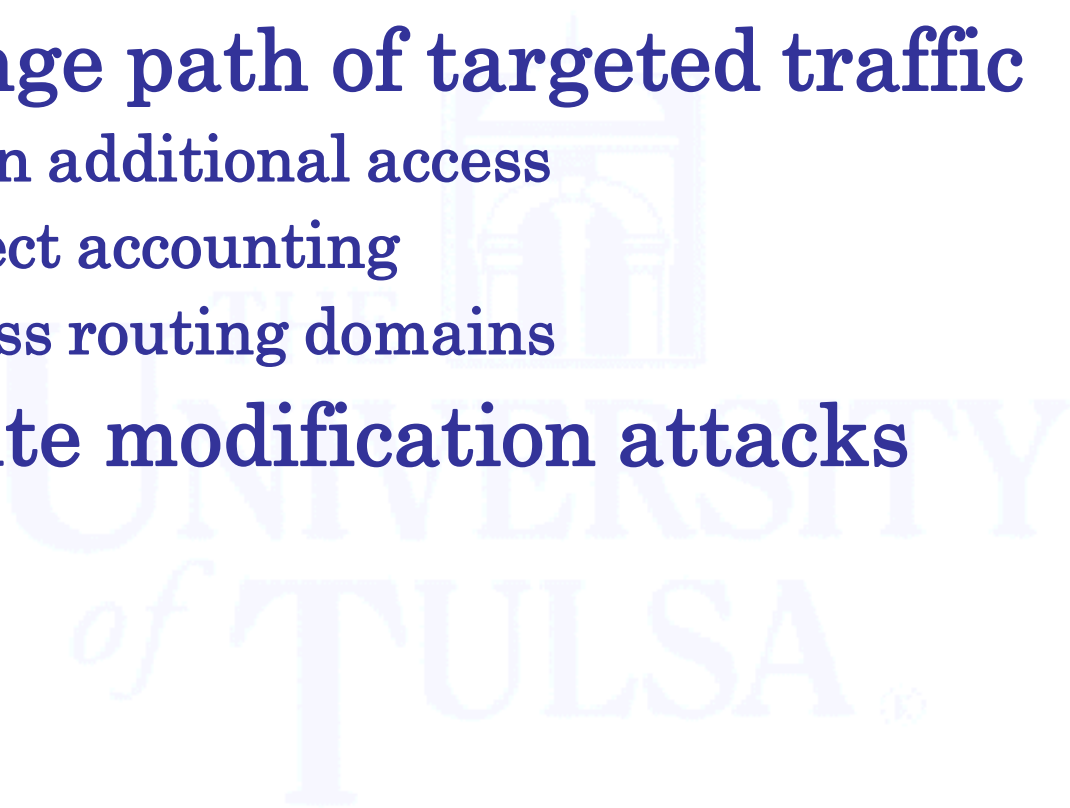


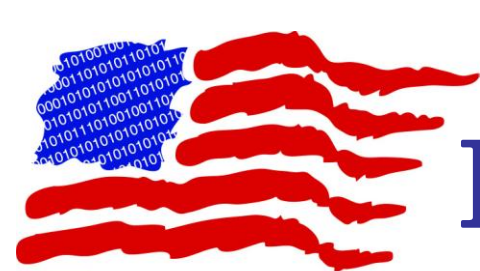


# Route Modification

010010101001010101010100110010101010100001010101010101010100010100100 —●

- **Change path of targeted traffic**
  - Gain additional access
  - Affect accounting
  - Cross routing domains
- **4 route modification attacks**

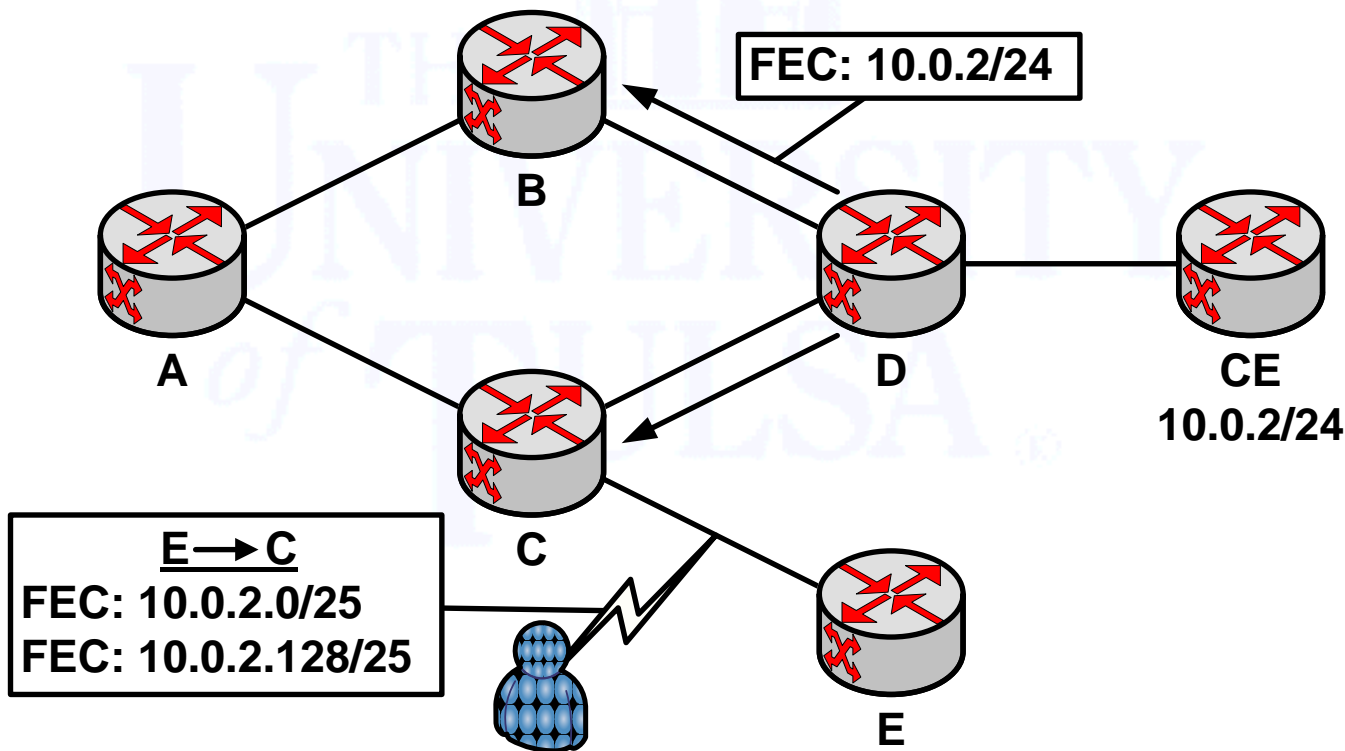




# Exploiting FEC Specificity

0100101010010101010101001100101010101000010101010101010101000010100100

- Exploits “longest match” algorithm for FEC assignment
- Attacker distributes bindings with better FEC matches



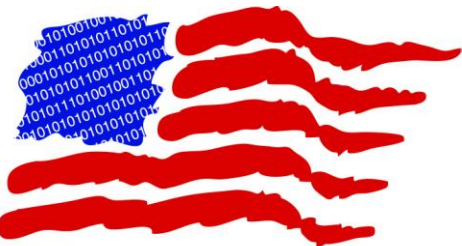


# Fabricating Label Mapping Messages

 **CYBER CORPS**  
Defending America's Cyberspace

010010101001010101010100110010101010100001010101010101010100010100100 —●

- Aids in loop creation
- Requires knowledge of downstream labels
  - Can be obtained via sniffing
- Modifies labels in Label Mapping messages
- Causes upstream router to adjust its LIB
  - Applies the wrong label
  - Downstream router mistakes packets as belonging to a different FEC
- Used in cross-domain attacks

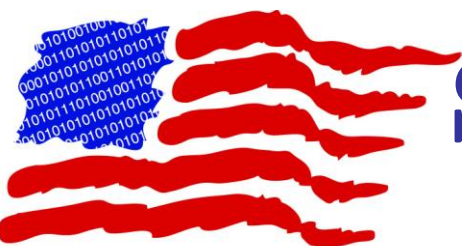


**U** CYBER CORPS  
Defending America's Cyberspace

# Fabricating Address Messages

01001010100101010101010011001010101010000101010101010101010100010100100 —●

- Aids in loop creation
- Manipulates “least cost” mechanism
- Attacker fabricates Address message claiming to have address of the IP next hop
- Affected node constructs new LSPs through the compromised link

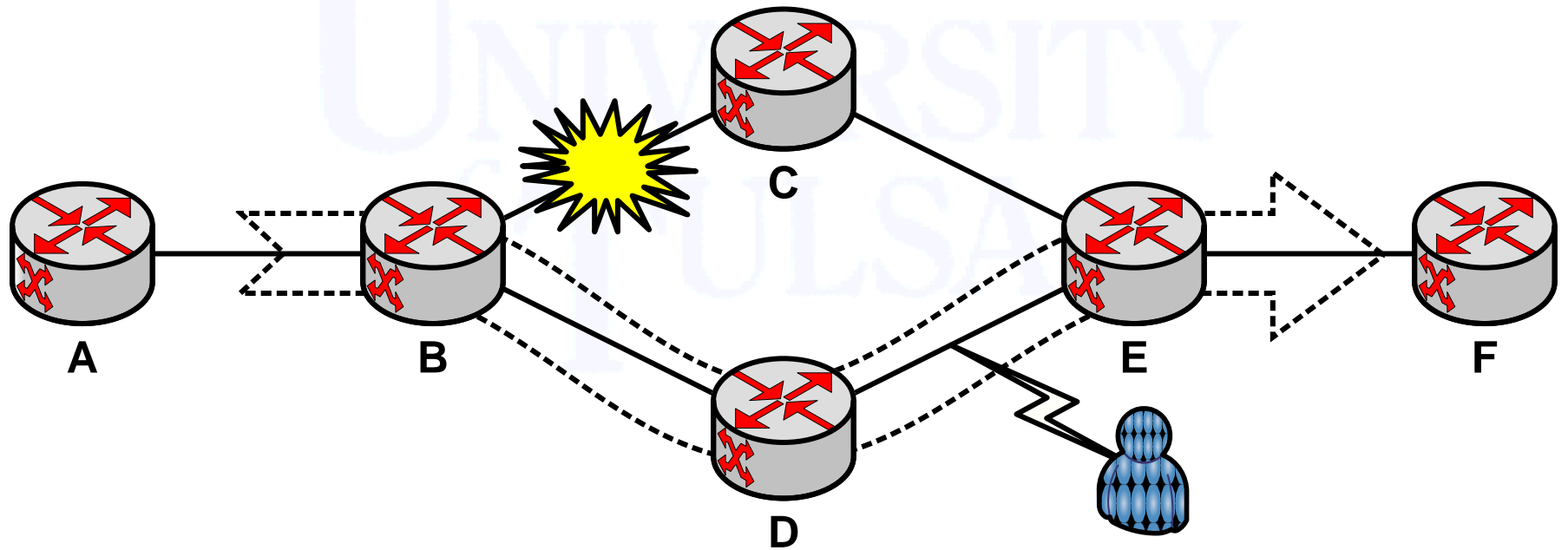


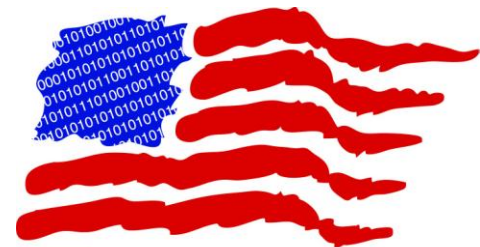
# Strategic Placement of DoS Attacks



0100101010010101010101001100101010101000010101010101010100010100100

- The attacker forces traffic through desired paths
- Disables other portions of the network
- Less granular

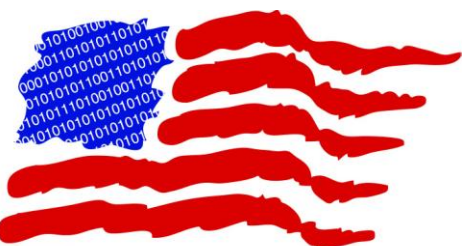




# Mitigation

010010101001010101010100110010101010100001010101010101010100010100100 —●

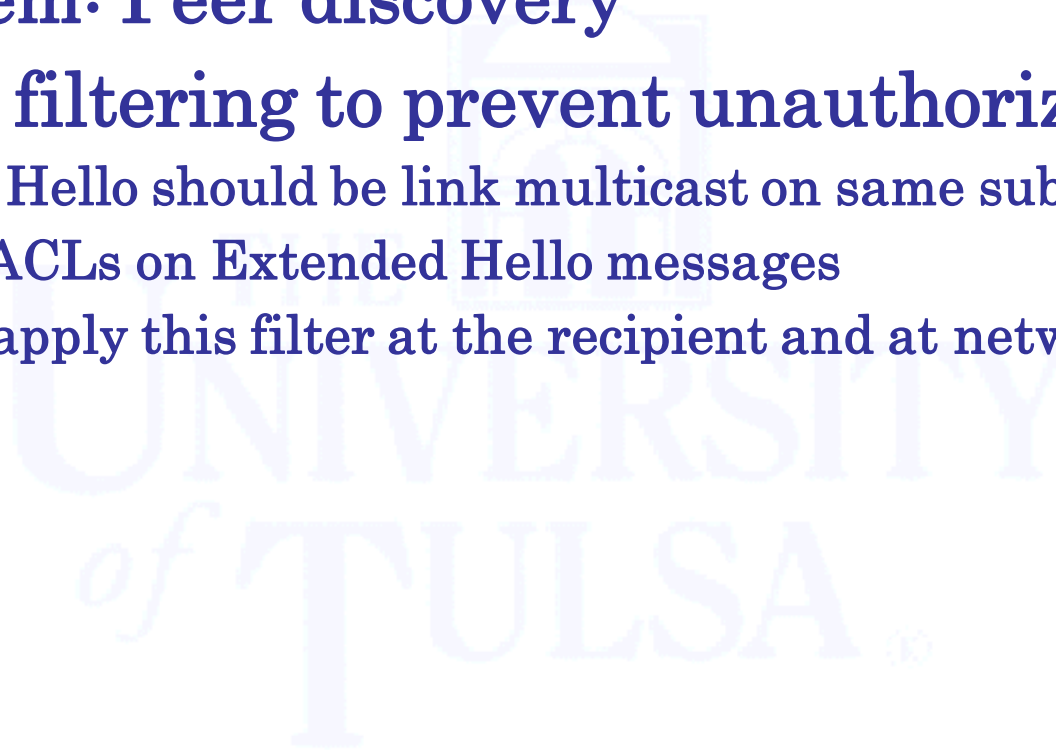
- **Problem: Few security mechanisms**
- **Most mitigated by TCP MD5/SHA-1 checksum**
  - Key management
  - RFC 3562: 90-day cycle
  - Strict distribution guidelines
  - No manageable implementation demonstrated
- **Not implemented or not implemented well**
  - Need an effective key distribution and management scheme

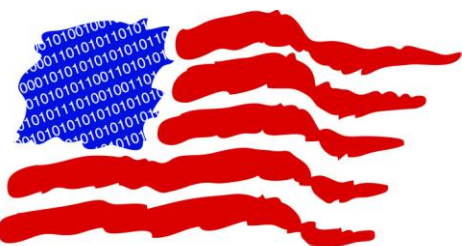


# Mitigation

010010101001010101010100110010101010100001010101010101010100010100100 —●

- **Problem: Peer discovery**
- **Apply filtering to prevent unauthorized peering**
  - Link Hello should be link multicast on same subnet
  - Use ACLs on Extended Hello messages
  - Can apply this filter at the recipient and at network perimeter



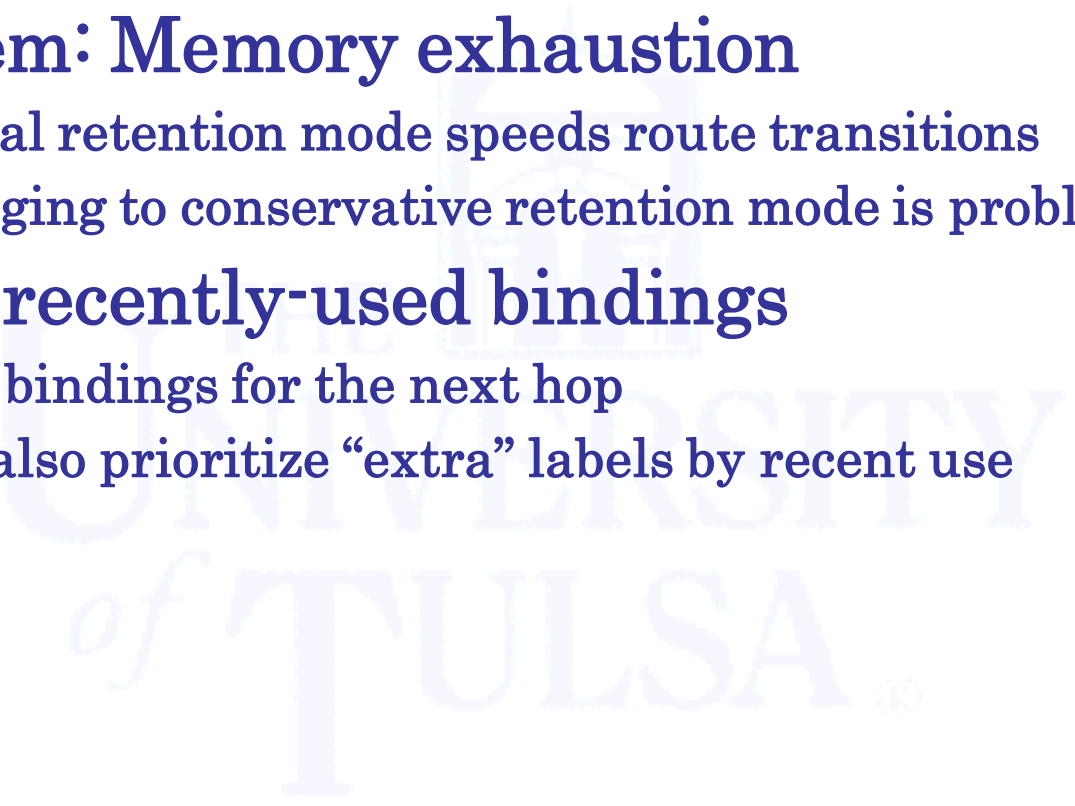


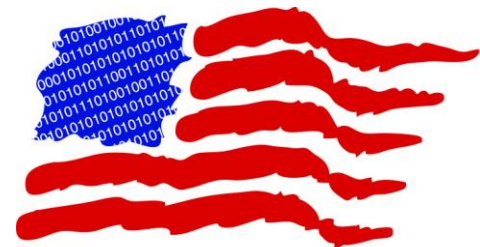
# Mitigation



01001010100101010101010011001010101010000101010101010101010100010100100 —●

- **Problem: Memory exhaustion**
  - Liberal retention mode speeds route transitions
  - Changing to conservative retention mode is problematic
- **Favor recently-used bindings**
  - Keep bindings for the next hop
  - May also prioritize “extra” labels by recent use



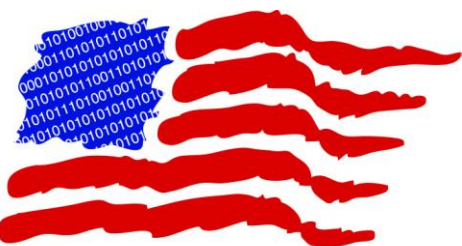


# Conclusions

010010101001010101010100110010101010100001010101010101010100010100100 —●

- A persistent attack on an MPLS network could cripple corporate, national and global operations
- LDP is a critical component in constructing MPLS routes
- LDP is vulnerable to several attacks

Security measures are needed to protect against internal AND external attacks



**U** CYBER CORPS  
Defending America's Cyberspace

010010101001010101010100110010101010100001010101010101010100010100100 —●

# Questions

