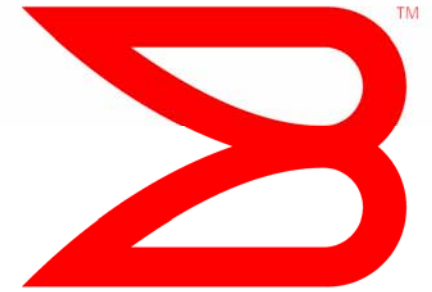


**BROCADE**



# On Duplicate MAC Addresses

T11/07-689v1

Anoop Ghanwani  
John Hufferd  
Suresh Vobbilisetty

December 5-6, 2007

# Overview

What is the problem with duplicate MAC addresses?

What are the potential consequences?

Tools and “best current practices” for dealing with duplicate MAC addresses

The goal of this presentation is to summarize the current understanding of duplicate MAC addresses and existing mechanisms for dealing with the problem



# Bridge forwarding

Bridges were designed to be plug and play

- With no forwarding entries, traffic is broadcast on all active ports in the forwarding topology
- Learning is used as a way to optimize forwarding

Learning is accomplished by learning that the source address in the frame is reachable from the port that received a frame from that address

# Implications of SA-based learning in bridges

Requires that MAC addresses be unique within a single forwarding topology

- For “shared learning” the MAC address must only appear once in the network
- For “independent learning” it is possible for the same MAC address to appear once in each VLAN

If a MAC address is learned on one port, and is subsequently seen on a different port, the MAC address is assumed to have moved to the new port

- Could happen because the station physically moved, or because a failure caused STP to reconfigure the active forwarding topology

Using different forwarding contexts for different protocols can give independent control over learning for each protocol

# Do duplicates happen in practice?

The short answer is yes

The good news is that the probability is negligible

- IEEE assigns unique OUIs
- Manufacturers of equipment ensure that addresses are unique

But...

- Errors do happen ☹
  - Manufacturing errors
  - Network administrators may reprogram the MAC address to a different value than the manufactured one and may accidentally program a duplicate
- Some older equipment was designed to be that way
  - DECnet Phase IV routers used the same MAC address on all interfaces
  - Sun servers used the same MAC address on multiple NICs
  - Network administrators had to build their LANs so these did not conflict

# What happens if we have duplicate MACs?

The typical symptom is intermittent connectivity

- Bridges will direct all traffic for a given MAC address in the direction of the station that last sent traffic with that MAC address as the SA
- All traffic goes to one station or the other so both stations will see significant packet loss and retransmissions

David Black showed some of the potential problems of duplicate MAC addresses in FCoE networks

- When 2 servers have the same MAC address, corruption can result
  - Requires FCIDs, Exchange IDs, sequence numbers, etc. to all be identical
- When a server and an FCF have the same MAC address, we could have a loop
  - Since FC frames don't have a TTL, traffic loops forever
  - David proposed 2 “port type” bits as a way to address this



# Why are duplicate MACs so hard to detect?

Inherently a distributed problem

It would be easy if the duplicates appeared at the same edge bridge

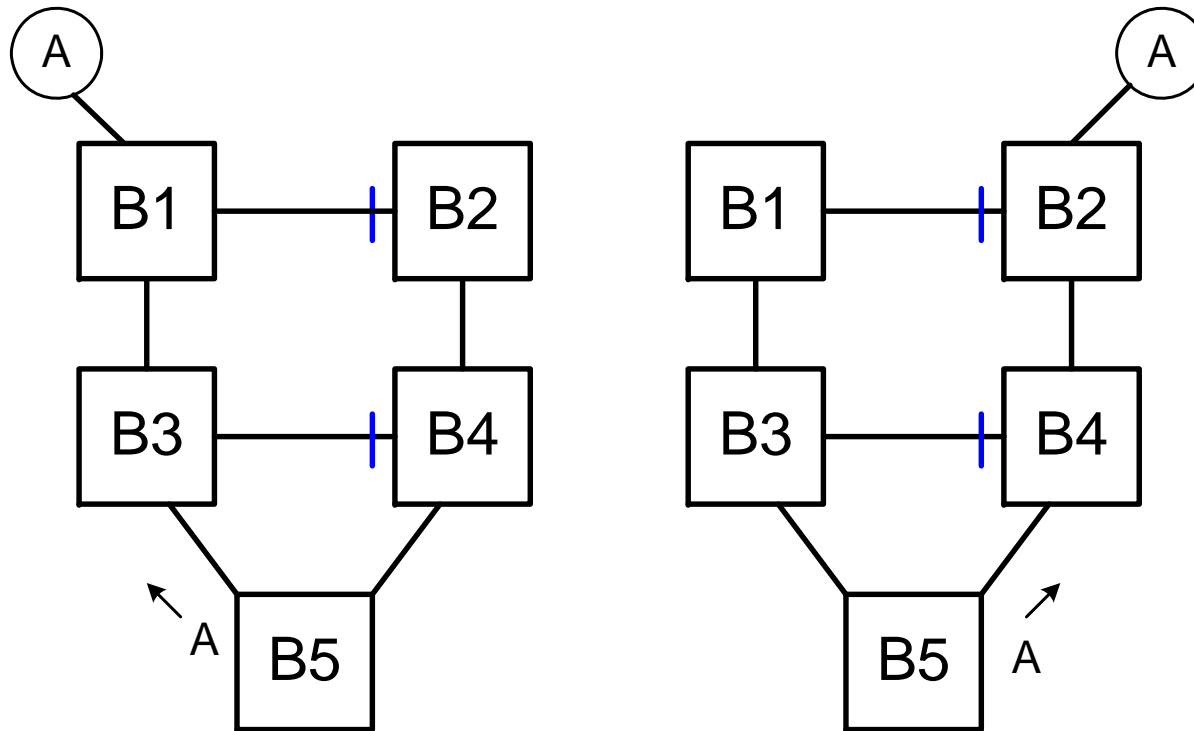
- MAC “moves” can be disabled at the edge using a feature called “MAC lockdown” – essentially an ACL

However, the stations with the same MAC address may be in different parts of the network

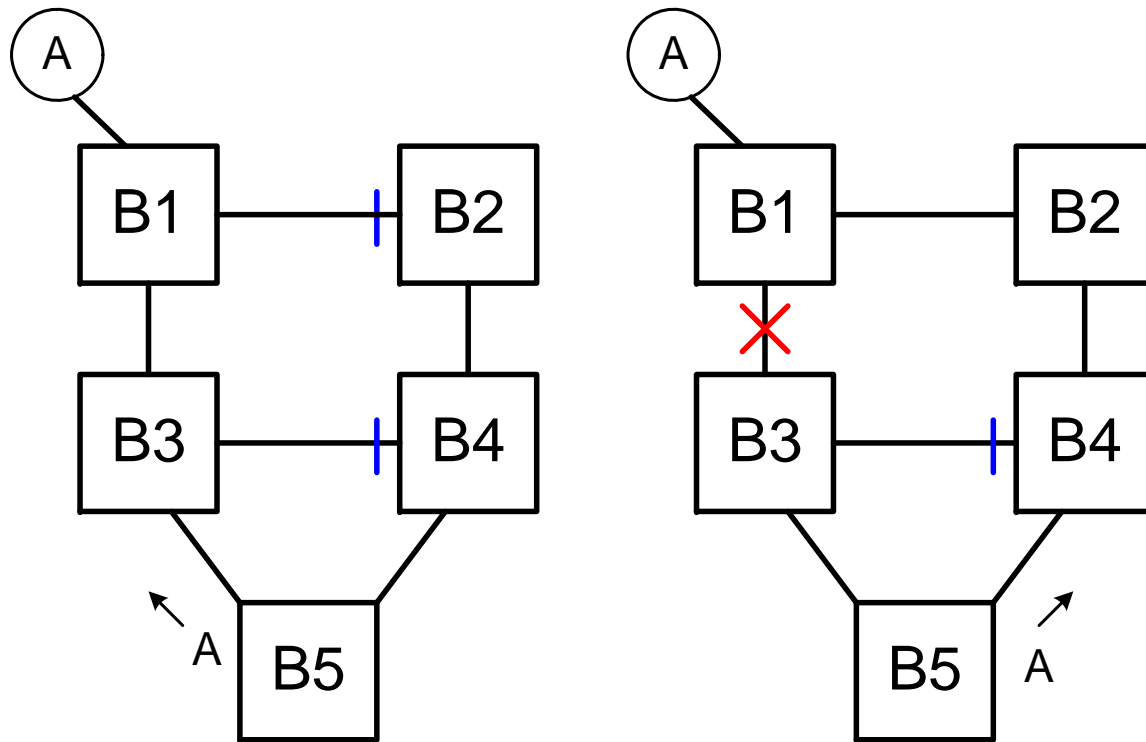
The only place where the “move” is detected is somewhere in the core

- Even in a relatively fixed environment, STP reconfiguration could result in a MAC appearing to have moved in the core
- In other words, a move is always legal in the core
- The core has no idea whether this is a real move or a duplicate MAC address

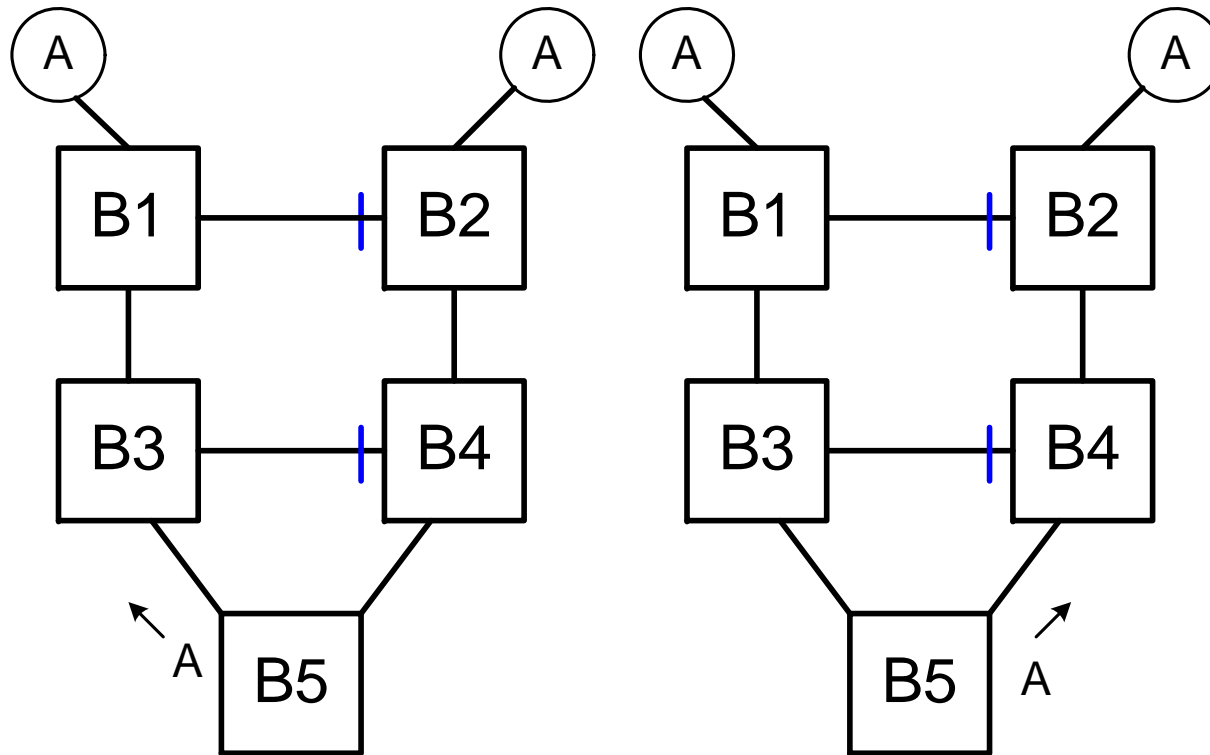
# MAC move due to station moving



# MAC move due to link failure



# MAC move due to a duplicate address



# Detecting duplicate MACs in a bridge

Some bridges detect frequent moves of large numbers of addresses and disable one of the ports

- This is considered a reasonable heuristic for detecting loops

But we have a different problem

- Only a single MAC address is moving
- Depending on activity, the move may not be frequent enough to detect an anomaly

# Tools for detecting duplicate MACs

Duplicates can be detected through a tool with network-wide visibility

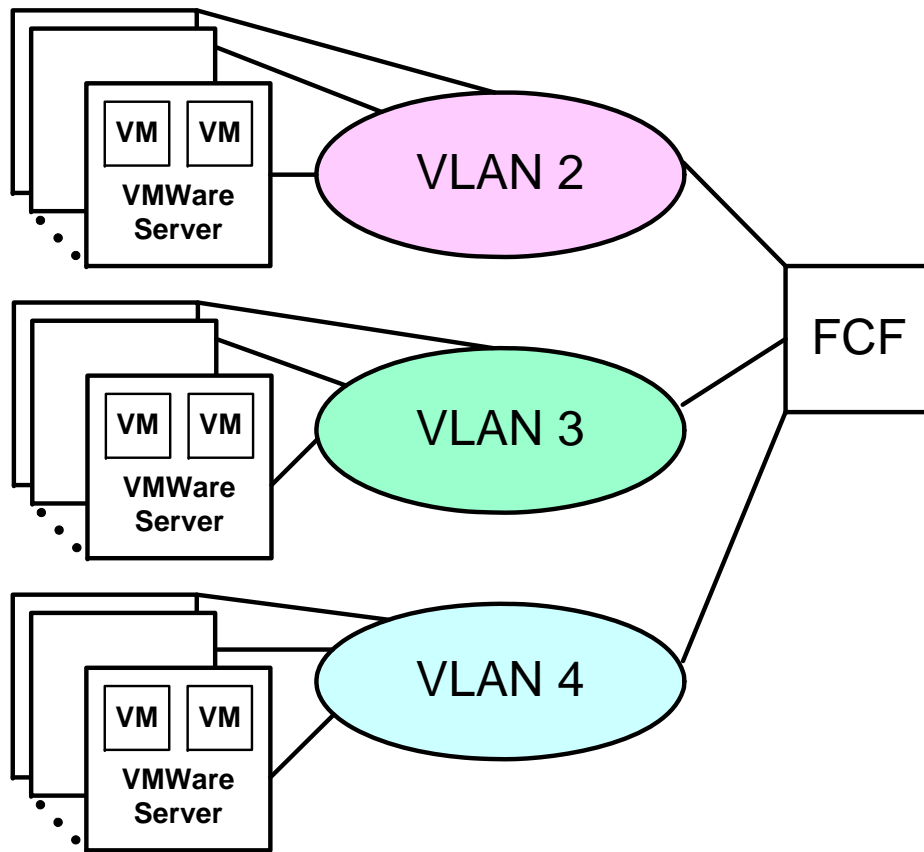
- Periodically poll the forwarding tables at all bridges in the network
- If the same MAC address shows up at an edge port in multiple bridges, alert the operator about a duplicate
- Detection time will depend on polling frequency

Many LAN administrators use homegrown scripts for this

Commercial tools for network inventory are also available

- Some of these provide built-in support for detection of duplicate MACs
  - 3Com Transcend, CiscoWorks, Extreme EPICenter
- Others can do it with additional plugins
  - Spiceworks (free), HP Openview

# Duplicate MACs and VMWare



VMWare uses separate MAC addresses for each virtual machine within a given server

VMWare guarantees the uniqueness of MAC addresses within a cluster

In the absence of other duplicate MAC address checks in the system, it would be safe to simply assign each cluster to its own VLAN

Alternatively, the administrator can use VMWare's Virtual Center to guarantee uniqueness of all MAC addresses even across clusters

# Guidelines for the network administrator

Reduce the probability of accidental duplicate addresses

- Use a database to track every MAC address in the network
- Ensure uniqueness of the MAC address before enabling the bridge port to which it connects to accept FCoE traffic
- When using VMWare, either
  - Use VMWare Virtual Center to avoid duplicates
  - Design the network so that each VMWare cluster is in its own VLAN and use IVL

In the event that a duplicate happens

- Use tools that perform network-wide monitoring to detect duplicates
- Disable one of the stations awaiting further administrative action



# Can we do anything in T11 for FCoE?

A couple of possibilities

- Leverage the FCoE Discovery Protocol to detect and recover from duplicate MACs
- Enhance FC-SW, FC-GS to include the FCoE N\_Port MAC address and have duplicates detected by dNS (Sec 9.3 FC-SW)

Others?



# In summary

Duplicate MACs pose a problem in the operation of bridged LANs

- They are rare, but they do happen

An administrator can minimize the probability of seeing duplicate MAC addresses by following “best current practices”

Should they occur, there are several existing tools to help with duplicate MAC address detection

We could also enhance FCoE protocols to detect duplicate MAC addresses