"1995 - The Year of the Virtual LAN"

IEEE Conference, Maui, July 1995

mmcnealis@cisco.com

Agenda

- Where are we today ?
- Virtual LAN Technologies
- IEEE 802.10 Virtual LANs
- vLANs and IEEE 802.1d
- Conclusion

Where are we today ?

- vLANs over-hyped and under-defined.
- vLAN membership criteria:
  - Port-Centric
  - Protocol/Subnet
  - MAC Address
- Standardization Process.
  - vLAN Identification
  - Automated Configuration
  - vLAN Management

vLAN Technologies

- vLAN Signaling.
- vLAN Tagging.
- LAN Emulation for ATM backbones.

vLAN Signaling

- Switches maintain lists of MAC Addresses associated with a particular vLAN.
- Exchange this information with other switches connected to the backbone.
- Enables intelligent forwarding/directed broadcasting.

vLAN Signaling Evaluation

- Advantage:

  Preserves the original packet format

- Disadvantages:

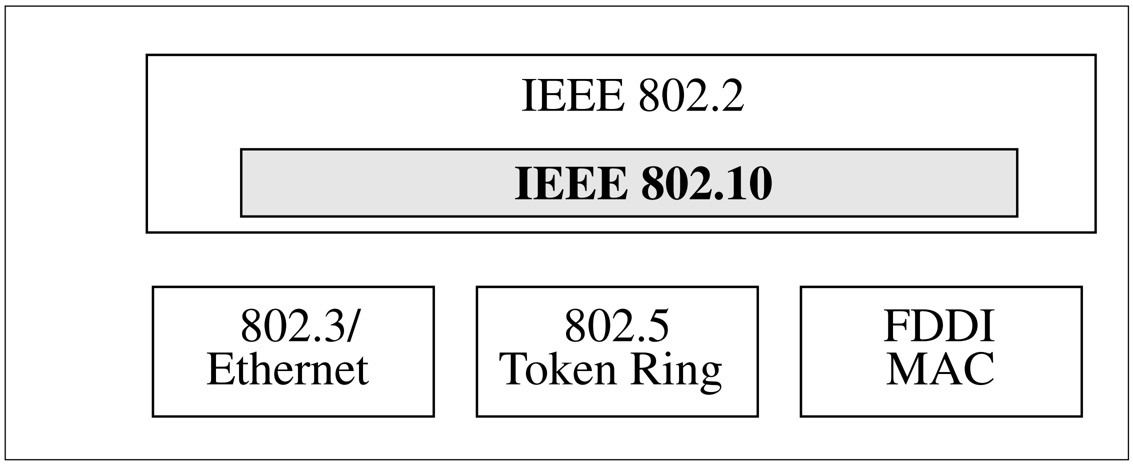
  Requires “routing-like protocol” to distribute MAC <--> vLAN tables

  Scalability

  Requires unique addressing

Suitability for vLAN Tagging

- Functions at the Data Link Layer:-



- Scalability - 4 byte vLAN Identifier field.
- Media independent/transparent to non 802.10 vLAN devices.
- Simple to implement/low overhead.
- Potential security benefits.

IEEE 802.10 Framing

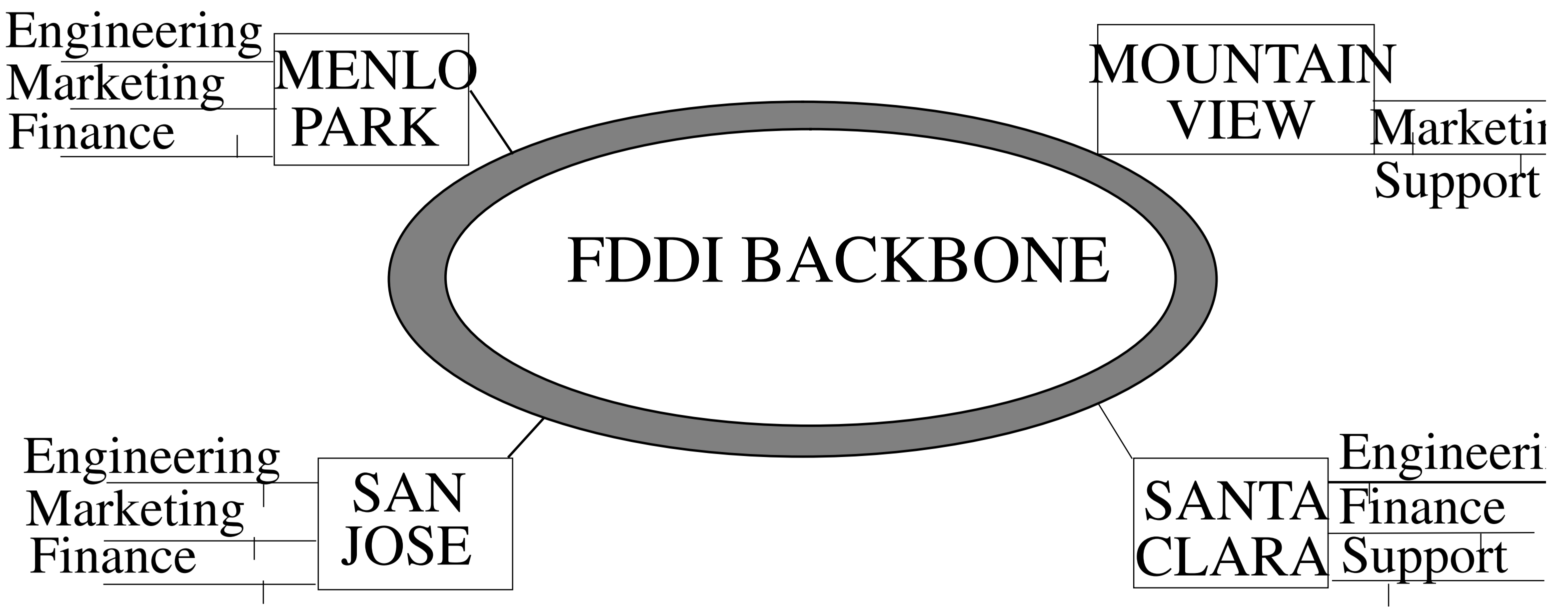
- Single Secure Data Exchange (SDE) PDU.
- 802.10 header inserted between frame's MAC and Data:

MAC	Clear Header	Protected Header	DATA

MAC	802.10 LSAP	SAID *(vLAN ID)*	MDF	Station ID	DATA	ICV

- VLAN ID carried in the 4 byte SAID (Security Association Identifier) field.

802.10 Frames on the backbone



- Entry/Exit points of a shared backbone configured to accept supported colors
- 802.10 header inserted/removed as packets forwarded to/from the shared backbone

vLAN Tagging

- Packets traversing shared backbone carry vLAN ID within the packet header.
- Remote switches make intelligent forwarding decisions based upon vLAN tag.
- vLAN tag inserted/removed as packets enter/ exist shared LAN backbone.

vLAN Tagging Evaluation

- Advantages:

  Scalable.

  Independent of vLAN “membership criteria”.

  Supports multiple vLANs per source.

  Facilitates inter-vLAN routing.

  Low processing overhead.

- Disadvantage:

  potential MTU violation.

The IEEE 802.10 Standard

- Interoperable LAN/MAN Security (SILS) Standard for Secure Data Exchange (SDE).
- Addresses the need for traffic segmentation and network security.
- Optional support for:

  Fragmentation.

  Authentication.

  Encryption.

  Security Management Information Base (SMIB).

vLANs and IEEE 802.1d

- Autonomous Spanning Tree topology computed for each Virtual LAN.

  Better resilience and network stability

  Extend scalability by tunneling BPDUs across vLAN back-bone

- Requires Bridge ID per vLAN supported.

- Backwards compatibility may mandate new Group Address.

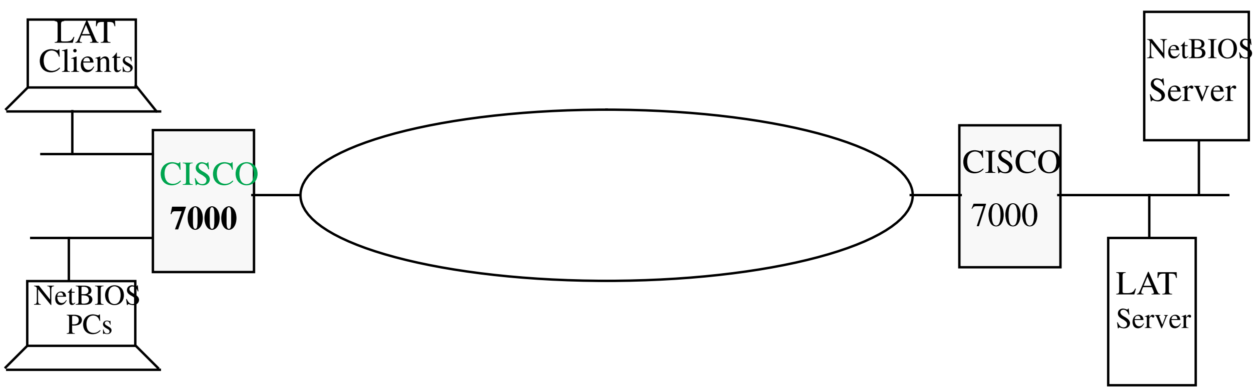
Conclusion

- Standardization on vLAN Identification is the first of three parts to achieving virtual networking interoperability.

- IEEE 802.10 is a legitimate vLAN tagging mechanism well suited to vLAN switching and should be endorsed.

VLAN membership based on port/protocol combination

- Existing VLAN membership is at 'interface level'
- In Client/Server environment clients on different LANs currently share the same VLAN/ traffic



vLAN Signaling Evaluation

- Advantage:

  Preserves the original packet format

- Disadvantages:

  Requires "routing-like protocol" to distribute MAC <--> vLAN tables

  Scalability

  Requires unique addressing