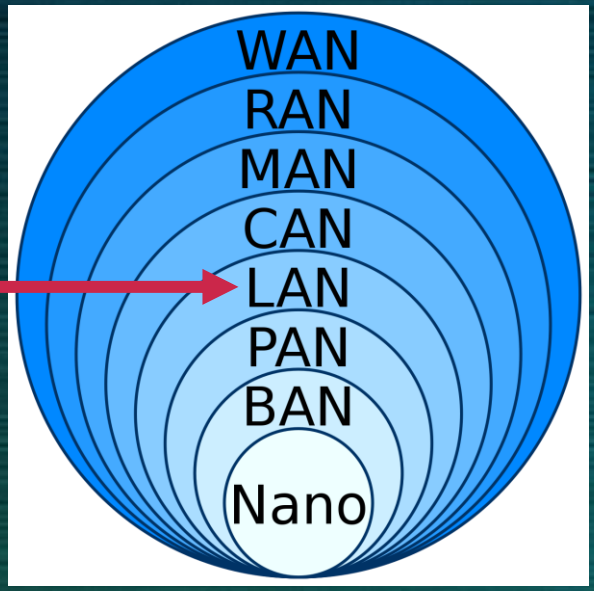
IT/CYBR 4323, Chapter 3:

Advanced Ethernet

Mr. Donald Privitera, Mr. Gennadiy Kemelmakher
Kennesaw State University
Marietta Campus
College of Computing and Software Engineering
IT Department
dprivit2@kennesaw.edu, gkemelma@kennesaw.edu

What is VLAN

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.



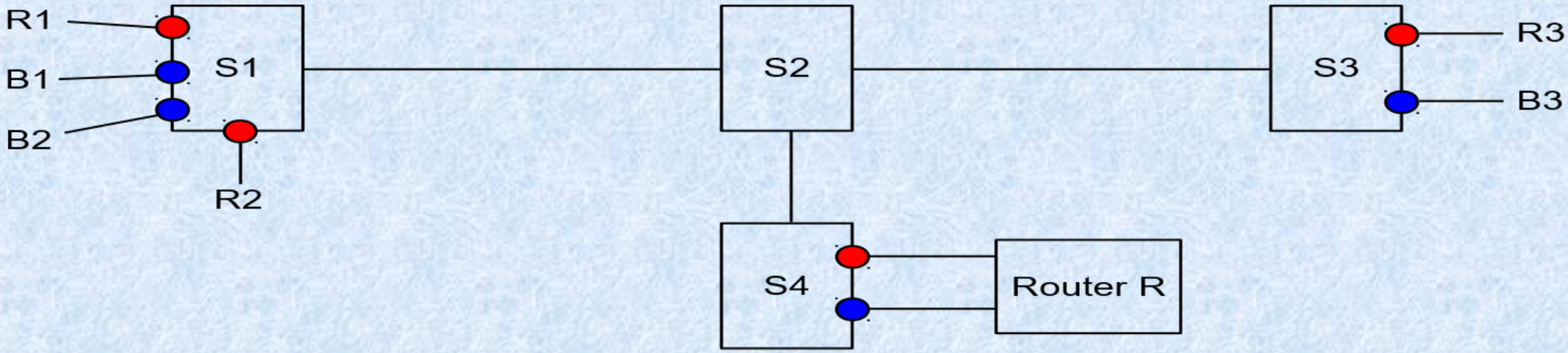
Advantage of VLAN

VLAN provides following advantages:-

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

Virtual LANs

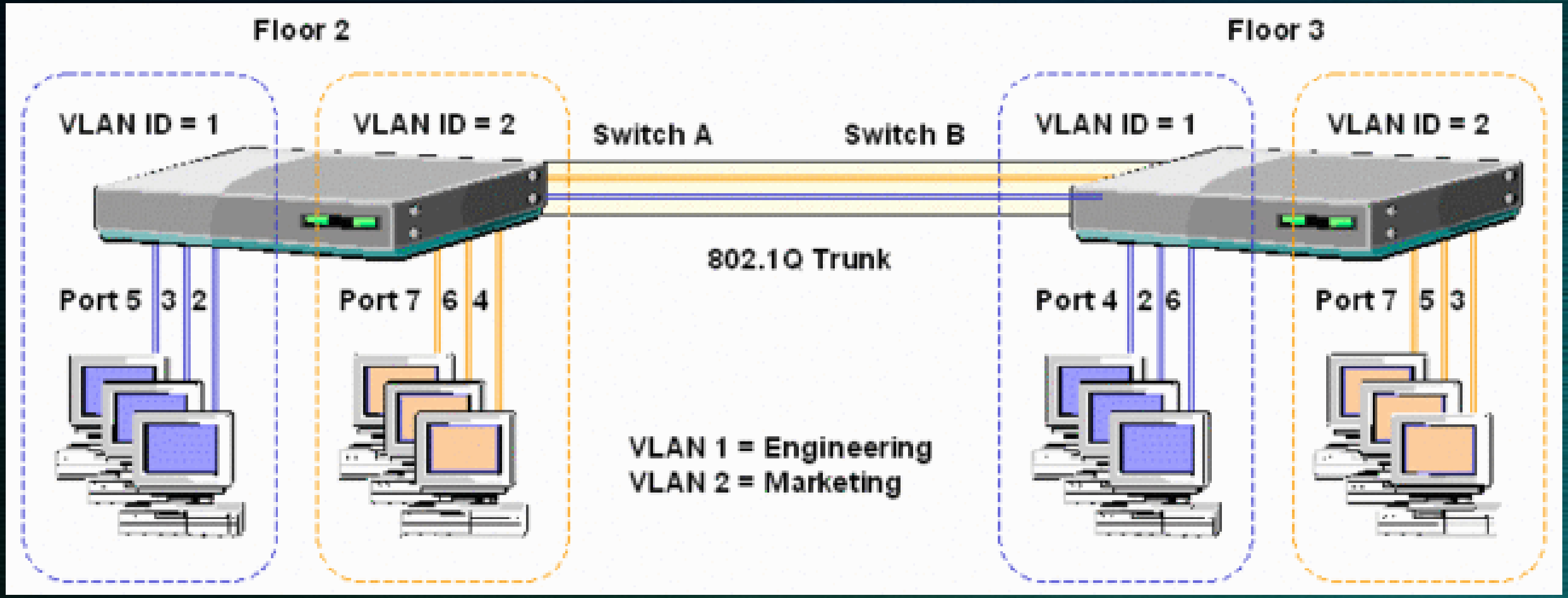
are a mechanism by which disjoint subsets of the hosts on a large Ethernet can be sequestered from one another, with packet exchanges only under controllable conditions. For example, Sales and Engineering workstations can be physically commingled, but kept logically separate.



One network of switches S1-S4 divided into two VLANs, red and blue

The switch network S1-S4 will deliver traffic only when the source and destination ports are the same color. Red packets can be forwarded to the blue VLAN *only* by passing through the router R, entering R's red port and leaving its blue port. R may apply firewall rules to restrict red–blue traffic.

An example:



A switch with 2 VLAN's configured. Ethernet traffic tagged as VLAN 1 is for "engineering's" traffic. Ethernet traffic tagged as VLAN 2 is for "marketing's" traffic.

https://upload.wikimedia.org/wikipedia/commons/5/5e/Vlan-fig2.gif

VLAN’s allow the hardware layer to be simulated thus creating virtual hardware links as opposed to having to run costly physical media to achieve the same purpose. Thus traffic can be aggregated over the same media.

This approach involves considerable planning to achieve optimal use of the physical layer without over saturating it.

Cyber attacks have demonstrated that VLAN traffic can be traversed and intercepted and decoded. VLAN’s can make a hacker’s job easier because many different kinds of traffic can be intercepted on one medium. Running physical media would be more secure but more costly.

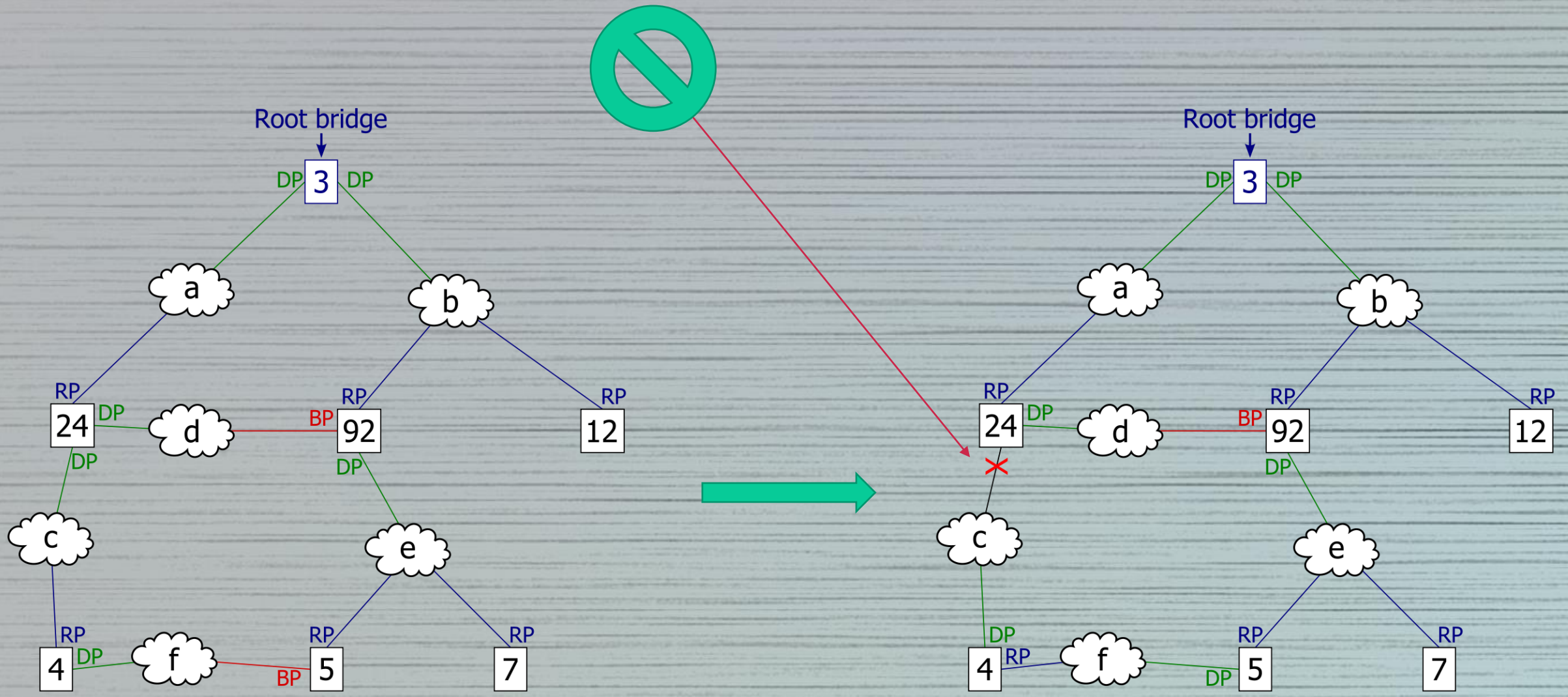
D. Privitera

The spanning tree algorithm:

Loop: your former foe – becomes a friend!

In general, any loops or recursive situations – are undesirable in IT, especially if there is no exit condition.

However, in networking – a loop can serve a redundancy purpose by providing a path to retain connectivity.



The algorithm blocks the connection from “C” to “24” preventing a loop, but should other connections break down – the same algorithm would restore the link, ensuring 100% connectivity.

Picture: *Silviu Angelescu (2010). CCNA Certification All-In-One For Dummies. John Wiley & Sons.* Text: *G. Kemelmakher*

Switches hardware:

Shared-memory model: single CPU, single memory and peripheral busses, and multiple Ethernet cards. Doesn't support high-performance.

Crossbar switch fabric model: grid of N×N normally open switch nodes that can be closed under CPU control. Allows *parallel* connections between any of N inputs and any of N outputs. Used in high-speed switches that support multiple parallel transfers.

Content-Addressable Memory, or CAM: allows for the search of the forwarding table in a single memory load. Each memory register simultaneously compares the value on the bus with its own data value; if there is a match, the register triggers its output line.

Ternary CAM, or **TCAM**: each memory register is paired with a corresponding "mask" register. Most useful when the addresses being looked up are IP addresses rather than Ethernet addresses.

Peter L Dordal "An Introduction to Computer Networks"

Software-Defined Networking (SDN)

The core idea of SDN is to place the forwarding mechanism of each participating switch under the aegis of a **controller**, a user-programmable device that is capable of giving each switch instructions on how to forward packets.

The controller can be a single node on the network, or can be a distributed set of nodes. The controller manages the forwarding tables of each of the switches.

Switches are often configured to report new *source* addresses to the controller, so that the controller can tell all the other switches the best route to that new source.
SDN controllers can be configured as simple firewalls, disallowing forwarding between selected pairs of nodes for security reasons. For example, if a datacenter has customers A and B, each with multiple nodes, then it is possible to configure the network so that no node belonging to customer A can send packets to a node belonging to customer B.

Types of server load-balancing via SDN:

- Software (round-robin to assign different users to different servers)
- Hardware (a devise for forwarding at the IP layer (via routing) or at the TCP layer, or at the application layer

Peter L Dordal “An Introduction to Computer Networks”