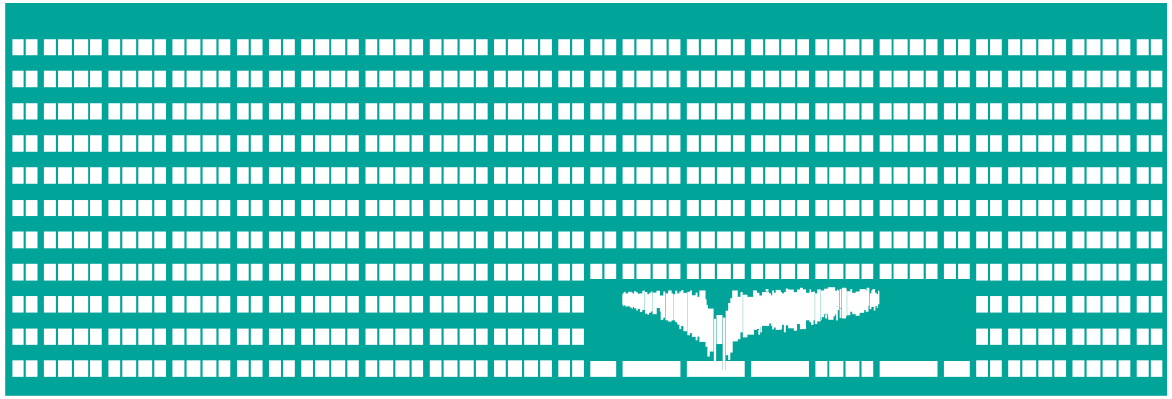
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Switched Ethernet Virtual LANs



Computer Networks Lecture 4

Switched Ethernet

LAN Switches

- Behave as bridges (operates in the logical tree topology)
- Switching is implemented by hardware (CAM table)
  - Low latency
  - Switch frames between multiple segments **simultaneously**

Switching Advantages

- collision-free => higher overall transfer rate
  - No data loss due to collisions
  - Different pairs of network segments may communicate at the same time
- switch may potentially enforce more deterministic network behaviour
  - Such as frame priorities, flow control etc.
- better security – only frames destined for a node are passed to its NIC (after a CAM table is learned)
  - Makes eavesdropping more difficult
- Easiest network maintenance
  - Isolation of faulty segment
  - broadcast-storm control
  - intruder detection (using source MAC addresses)

Switching Methods

- Store-and-forward – the whole frame is read into memory, CRC is checked then and after that the frame is forwarded to the destination port
  - Inevitable in case of asymmetric switching, i.e. switching between segments with various port bandwidths
- Cut-through – The frame is being transmitted just after the destination MAC address is read
- Fragment Free (sometimes called differently)
  - Combines advantages of the two previous methods
  - Operates as Cut-through, but the beginning of the transmission is delayed until there may not happen a collision on the source port (provided that the physical network cabling is desiged properly)
  - Useful in network designs that combine switches and hubs (group switching)

Parameters of LAN Switches

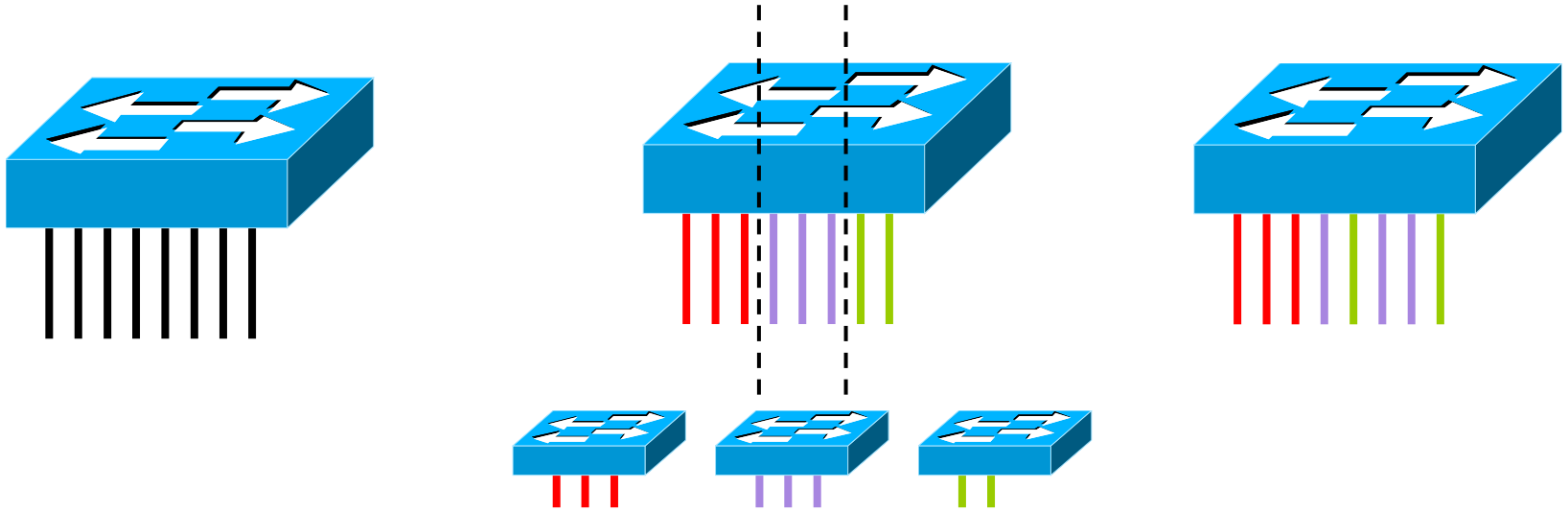
- Number of MAC addresses per port
  - Allows to connect just one station or a hub (group switching)
- Total number of MAC addresses (number of rows in the CAM table)
- Methods of address-to-port assignment
  - Dynamic (self-learning, flooding of frames with unknown addresses)
  - Static (supports an intruder detection)
- Administration method and port monitoring capabilities – Telnet, SNMP, WWW
- SPAN ports (Switched Port Analyser)
- Additional functions
  - Multicast processing
  - Traffic filtering, VLAN support, …

Half-duplex and Full-duplex mode in switched networks

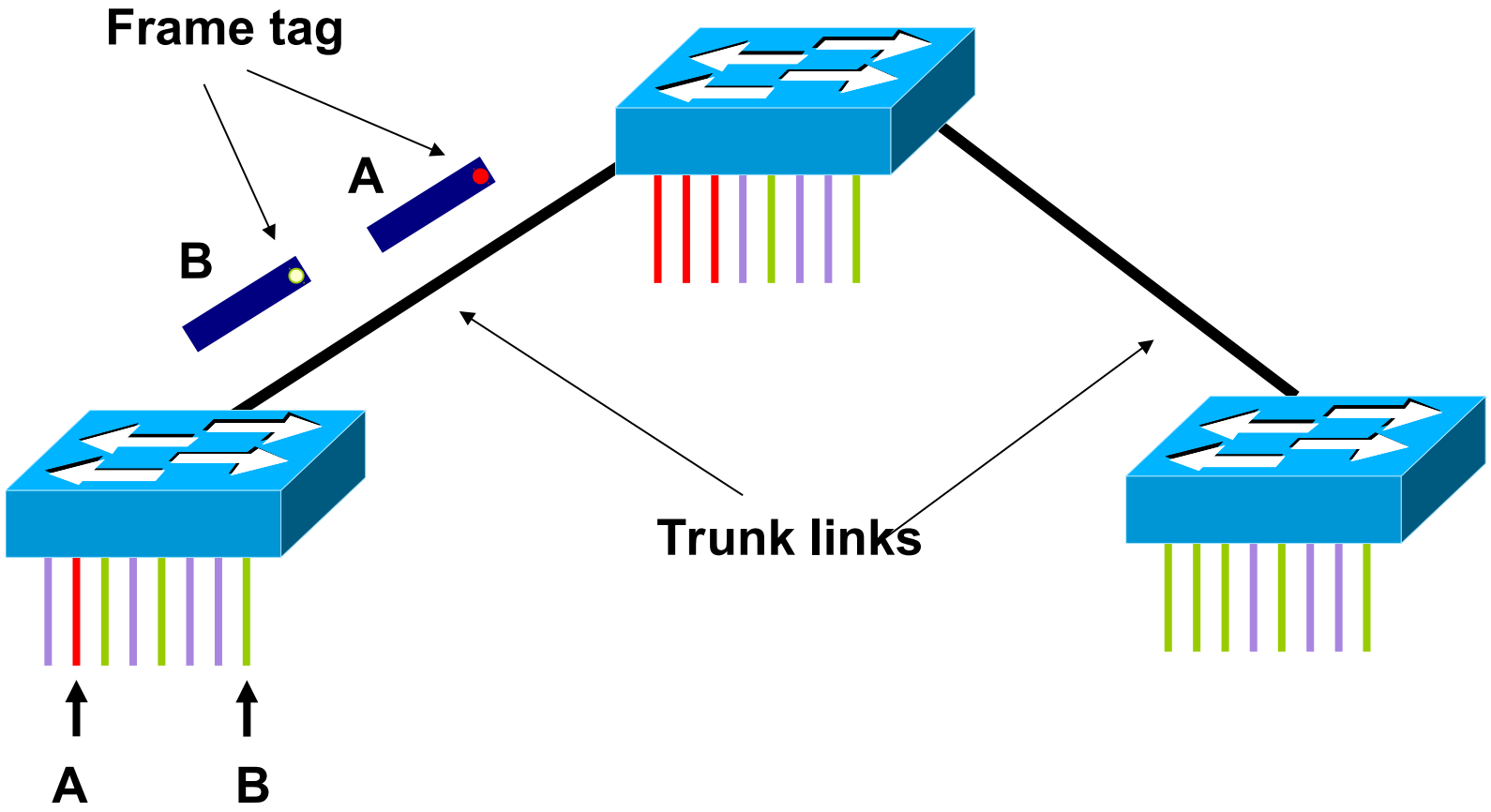
- Full duplex
  - collision-free, longer reach (no timing requirements for CSMA/CD)
- Half duplex
  - the switch port and station's NIC contend for the medium (collisions may occur)
- Every switch port may operate in different mode
  - Half duplex is still supported because of the old NICs and backward compatibility

Virtual LANs (VLAN)

Principle of VLANs (single switch)



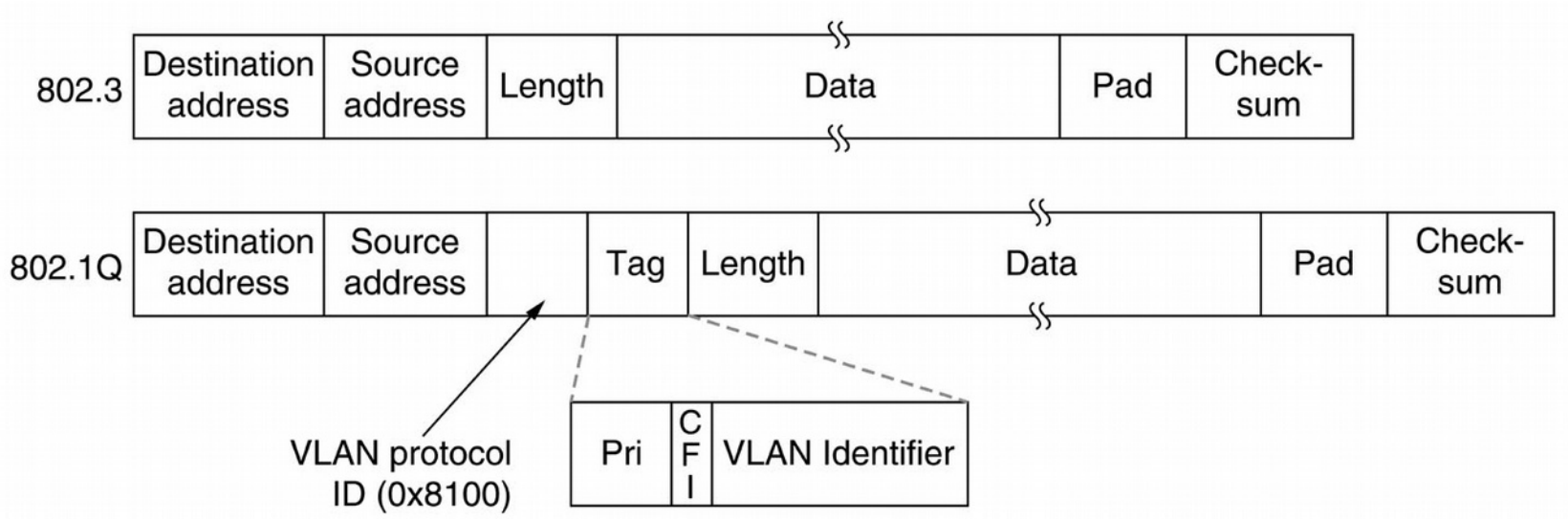
Principle of VLANs (multiple switches)



Trunk links

- Carry traffic of multiple VLANs
  - We may specify VLANs that are allowed on particular trunk line
- Normal (non-trunk, access) ports belongs just to a single VLAN
  - The assignment is most often configured permanently
- Frames are appended with IEEE 802.1q header on trunk links to differentiate traffic of different VLANs

802.1q Header



- VLAN ID is placed at the beginning of frame data field
  - together with specification of the frame priority (802.1p)
- The presence of 802.1q header is indicated by a dedicated EtherType value
  - The original EtherType value is moved into the frame data part behind the 802.1q header

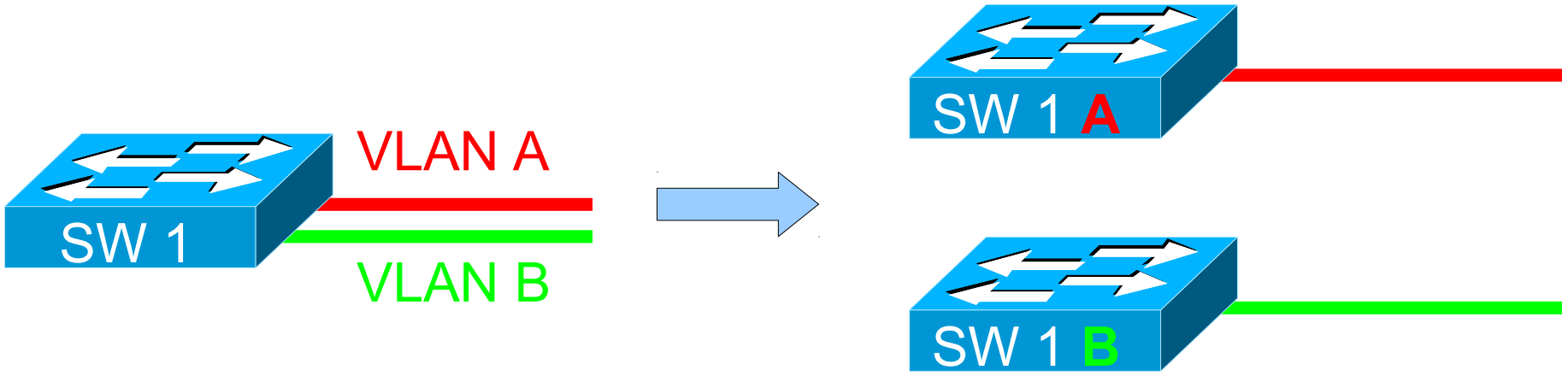
Usage of VLANs

- Allows to create a logical topology different of the physical network topology
  - Just by software configuration of LAN switches, no cabling changes needed
- Allows to separate various user and traffic types (priorities) on the same physical infrastructure

Advantages of Network Segmentation (most often implemented using VLANs)

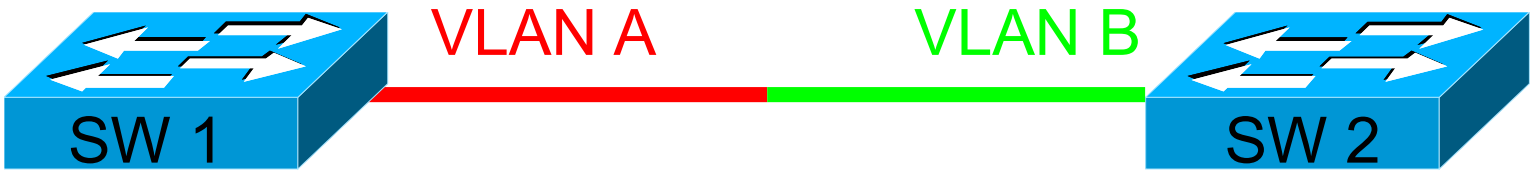
- Network segmentation
  - Limits the processing of broadcasts by stations not involved in the communication
- Increased security
  - Separation of different traffic types regardless of the physical topology
- Changes made easily just by configuration of switches
  - Telnet, WWW, SNMP

An Equivalent Layer 3 Topology Corresponding to a Network with VLANs



- How the topology would look like if we replaced logical topology with VLANs with physical topology featuring individual switches
- The view from network layer of ISO-OSI model
  - But we still include the L1 and L2 devices to make the network model easier to understand

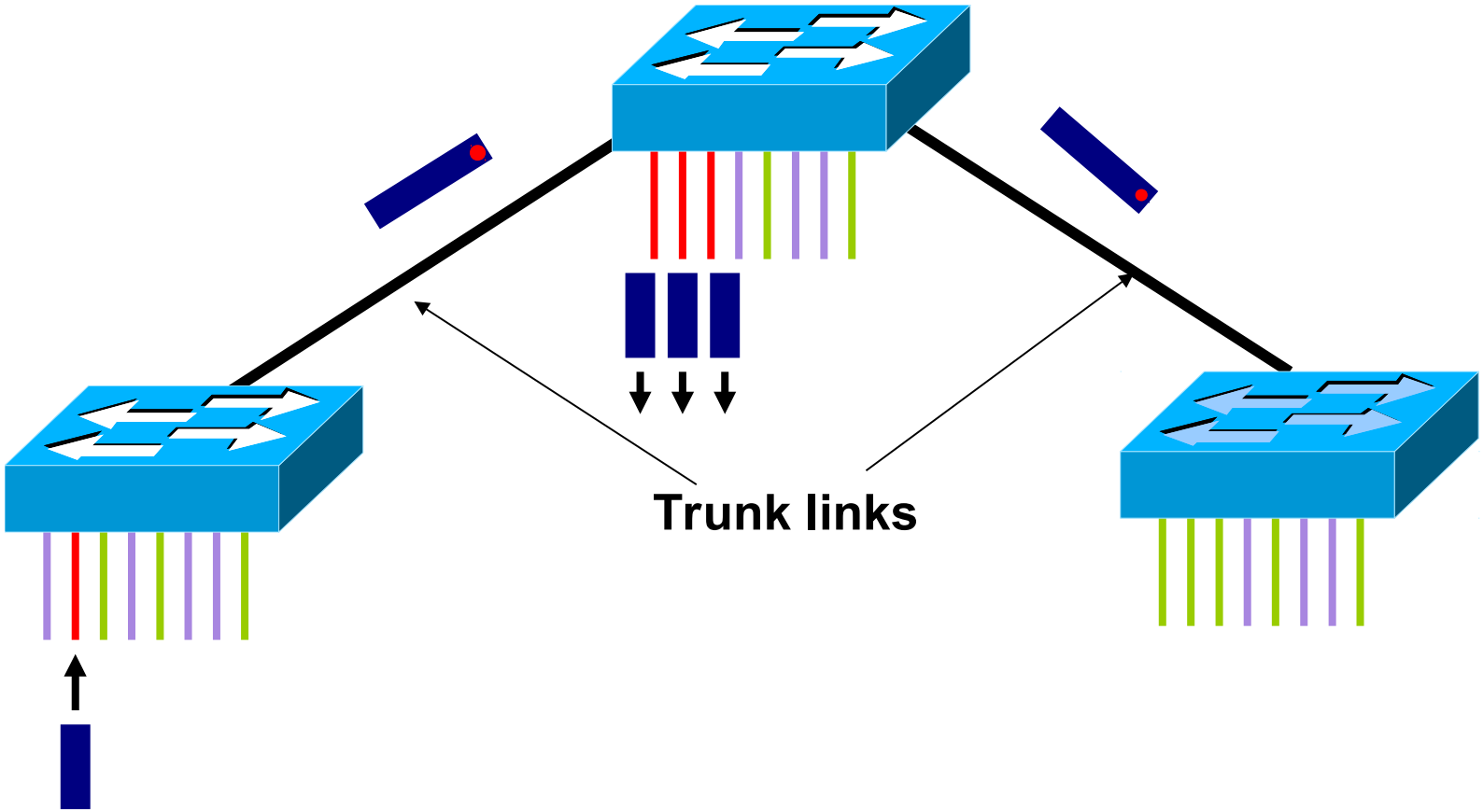
Behaviour of direct interconnection between ports at different VLANs



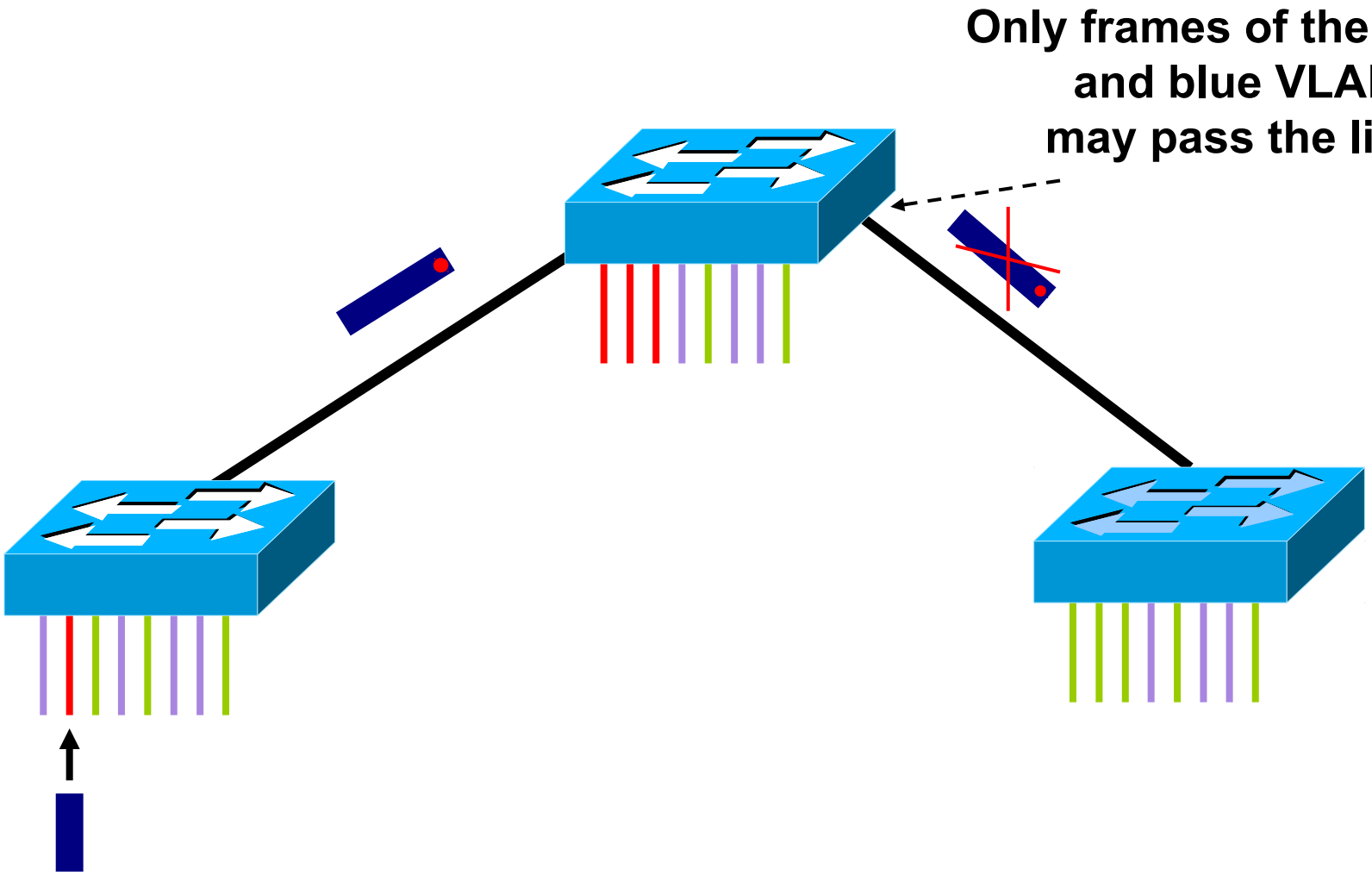
- No VLAN tagging on standard ports with stations → frame leaving VLAN A on SW1 will be placed to VLAN B on SW2
- Some managed switches may contain manufacturer specific protocol to exchange information about VLANs on given port → VLAN mismatch warning messages

Optimizations of VLAN Operation

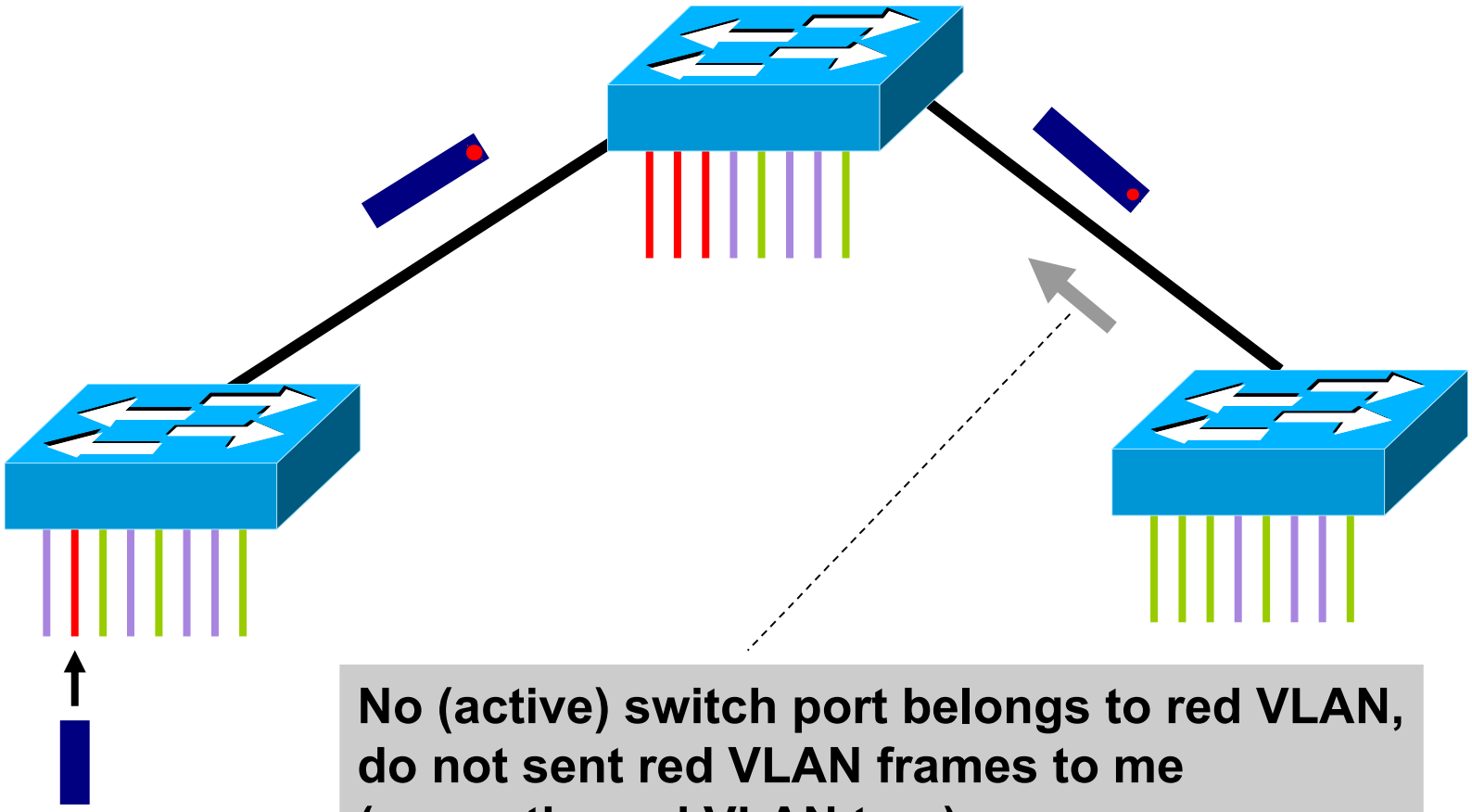
Flooding of broadcasts and Frames with Unknown Destination Address



VLAN Filtering on Trunk Links



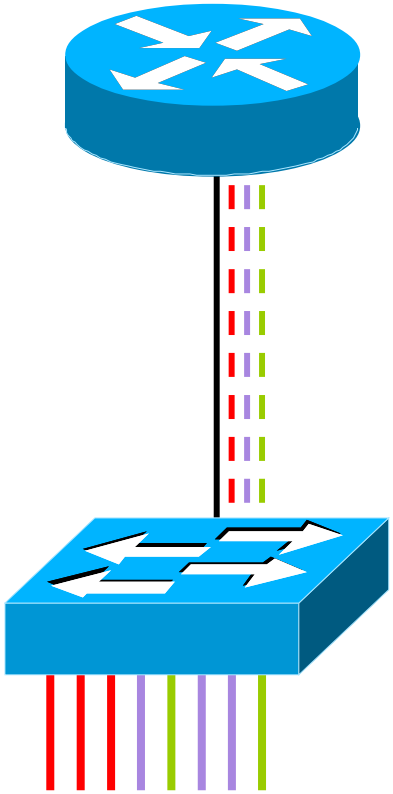
Automatic Pruning



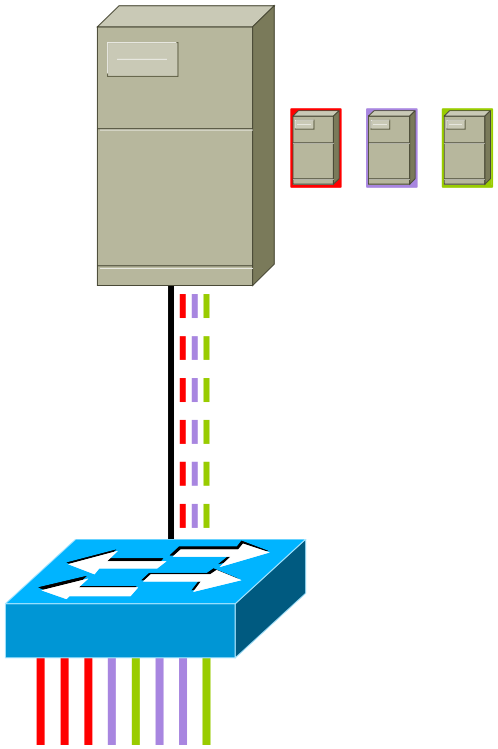
No (active) switch port belongs to red VLAN, do not sent red VLAN frames to me (prune the red VLAN tree)

Other VLAN Applications

„Router-on-the-stick“ (routing between VLANs)



Trunk Link to Server with a VLAN-capable NIC



Where One Can See the 802.1q Headers ?

- On trunk links between switches
  - Switch port has to be explicitly configured as trunk
- On trunk link between switch and router
  - Used for inter-VLAN routing
- On trunk link between switch and VLAN-capable server NIC

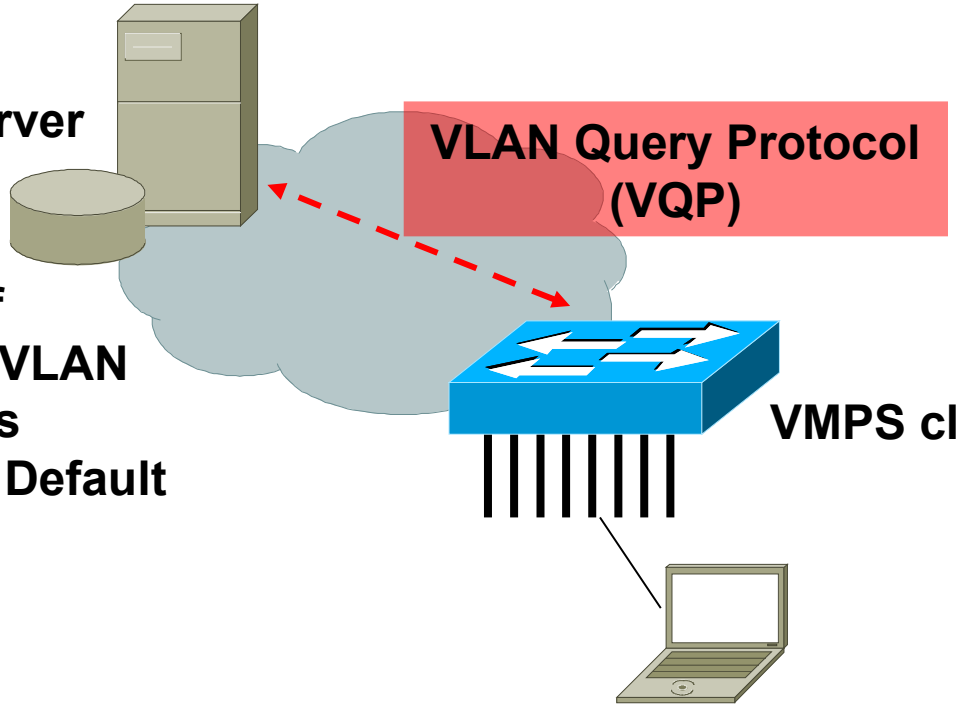
Whenever a frame is forwarded to a non-trunk port assigned to a single VLAN, 802.1q header is removed

VLAN Membership

Assignment of User Stations into VLANs

- static (port-based) – most common
- dynamic – according to a station MAC adress, L3 protocol, ...
  - switches ask the VLAN Membership Server (VMPS) for station-to-VLAN membership whenever they see a new MAC address on a port with dynamic VLAN membership configured
  - only some proprietary solutions are available today for this task

Dynamic VLAN Assignment (Cisco proprietary solution)



User device with a given MAC address (sends e.g. DHCP request after booting)