MACMON VLAN MANAGER

macmon
nac smartly simple

Additional protection by network segmentation: static and dynamic VLANs

VLANs (Virtual Local Area Networks) provide the option of segmenting the network regardless of the physical structure. Segmenting a network reduces the broadcast load in the individual segments and also supports security concepts by separating the different areas from each other.

Working groups and assignment

Working groups formed using VLANs can thus communicate without any restriction, as if they are part of the same LAN regardless of their physical location. Sensitive resources can thus be safeguarded from general access. VLANs can either be formed statically, that is, through fixed assignment of the individual switch ports to specific VLANs, or dynamically. The dynamic assignment can take place based on the MAC address (layer 2 VLAN) or based on a higher protocol layer as well as 802.1X.

Key facts

- ✓ Quicker and controlled network access to the LAN and WLAN for guests and their mobile devices like laptop, iPhone or Android.
- ✓ Simple control and handling using a voucher system: The visitor has to just login using a Web service with a voucher code.
- ✓ Easy to operate even by non-IT staff like reception, secretary's office or staff in special departments. Thus the IT department is relieved from routine activities.
- ✓ Ensuring the security of IT infrastructure and the overview and traceability of network accesses.
- ✓ Support for VLAN concepts on basis of Layer-2, 802.1X or mixed mode.

Visitor or quarantine VLAN

Devices that are not trustworthy can be connected to a visitor or quarantine VLAN by macmon as they appear in the network.

These may be mobile workstations of employees who are travelling, systems of service providers or external devices of visitors. Based on group membership or an individual qualifier, macmon can classify the device as less trustworthy and then respond.

Once the device leaves the network, macmon reassigns the switch port to its original VLAN. Because the rules are flexible to setup, this can be restricted to specific switches, network segments or areas. For example, if devices of the type “visitors“ are allowed only in designated areas in a “visitor VLAN“ but are completely prohibited in other areas, then this requirement can be flexibly and easily implemented using the macmon vlan manager.

Even devices that have not been connected to the network for a long time or are classified as unsafe after a “Compliance Check“, can be kept in a quarantine network till the status is clarified. These devices indeed have access to the latest security patches and the latest virus scanner but cannot view the other services and thus cannot cause any damage.

Dynamic VLANs on MAC layer (Layer 2 VLANs)

In case of the dynamic layer 2 VLAN, the assignment to a network segment takes place via the endpoint, wherein the device is identified using the MAC address. The advantage of such a concept is that the user, regardless of the location of a device, always has access only to that area of the network which he requires for his work. Even after relocation or while using mobile equipment, the user always lands in the correct segment and there is no need to reconfigure in the network area. The same functionality is as well available with 802.1X based authentication.

Implementing such a concept is easy using macmon VLAN manager where you assign a VLAN to each device using a WEB GUI. If you manage the VLAN assignment using the macmon groups, then the operating effort is considerably reduced.

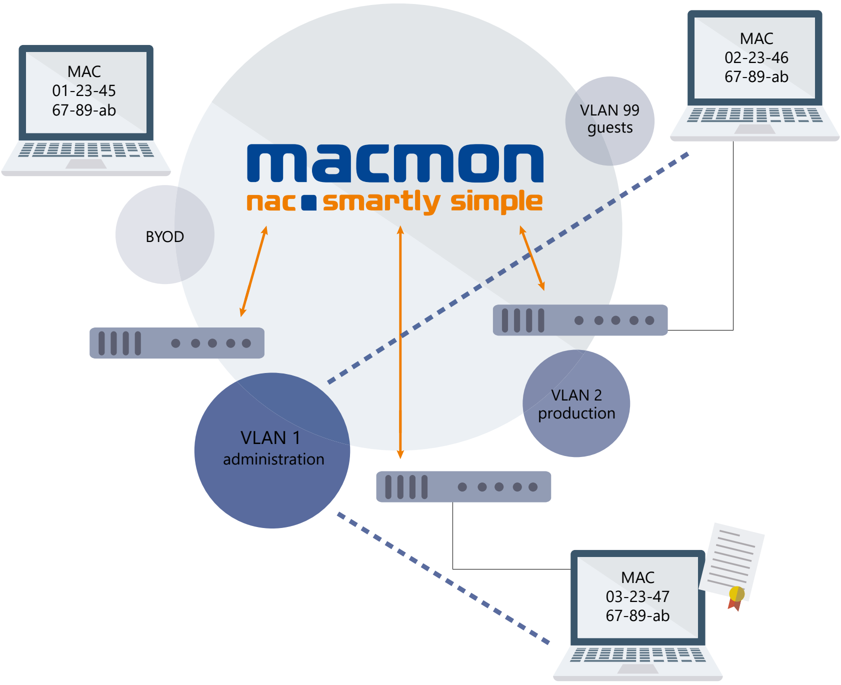
macmon constantly monitors to see whether the switch ports, where the devices are being operated, are present in the correct network. If there has been a change here, then the corresponding switch port is automatically reconfigured.

Safeguarding all the unused switch ports from being misused

Do you want to ensure that unauthorised devices cannot eavesdrop in the network? You can do this with macmon. macmon ensures that all the switch ports where a device is not being actively operated, are assigned to a VLAN where no services are provided. If a device is now connected, it is identified by macmon as soon as it sends a data packet. Depending on the status, it is switched to the assigned network, the guest VLAN or to a remediation VLAN if it has not been seen for a long time in the network.

Devices that are connected to the network and does not exchange data, remain in the "No-Go network" till they login. This also prevents "eavesdropping attacks".

The macmon VLAN manager should bepurchased as an extension to a macmon license. It includes the VLAN management modules, the switch-specific control modules and the generation of solution-specific scripts. The macmon VLAN manager already supports many switch types. Since VLAN management differs depending on the manufacturer, it may be necessary to customize the VLAN management module to the switches that you use, which is why the temporary access is required for such a switch.



Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin | Germany
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu