MICROSENS

WHITE PAPER

Safety first
Secure building networks thanks to decentralised infrastructure solutions

Safety first
Secure building networks thanks to decentralised infrastructure solutions

There is no doubt that IT infrastructures have to work securely and reliably - after all they provide the foundation on which numerous business processes and therefore corporate success are based. What is true for the building itself applies here too: If the foundation causes problems, this affects the entire structure.
While users are only too aware of the reliability and performance of their cabling, security is often neglected. Developments like BYOD (Bring Your Own Device), evermore mobile devices, which need to be integrated, and increasingly sophisticated attacks on the corporate network, demand a higher security level than ever before.
At the same time, infrastructure projects are faced with increasing pressure to reduce costs. A distributed infrastructure with decentralised switches can optimally meet all these demands.

Cabling with decentralised switching architecture, such as Fiber To The Office (FTTO) developed from MICROSENS, have long since become established as a cost-efficient in-house network in countless projects. Independent studies like the one conducted by WIK-Consult and numerous successful projects demonstrate the economic advantages of this solution time and time again. The decentralised concept is not restricted to fiber optic lines, but its specific advantages are exploited to the full in copper cabling. For both media, high-performance lines are routed through to the user area where Installation or Micro Switches are used as active elements to provide copper connections for the terminal devices, such as workplace PCs, VoIP phones, printers, laptops, Wireless LAN Access Points or IP cameras. As a technology leader for decentralised fiber optic and copper switching concepts, the technology specialist MICROSENS implements new and extensive security features in its products to guarantee users maximum network access security.

Decentralised switches offer advantages

The latest generation of decentralised switches offer a wealth of functions that were hitherto the preserve of core switches. In the switches every parameter can be configured, changed and sent to other software instances using secure protocols like SNMP V3 or HTTPS. Full IPv6 implementation is an important prerequisite for future-proof networks.

However, the decentralised concept offers a whole lot more. It's user-oriented structure enables switch intelligence and therefore monitored, managed devices where they are needed - on-site for the user.

Another plus by the way: The cabling concept with decentralised switches gives rise to significantly smaller cable bundles, which really matters especially in renovating old buildings. And smaller cable bundles lead to lower fire loads, which in turn raises safety and reduces costs. Furthermore, existing copper networks can be expanded quickly and without costly reworking of cabling and they stay up to date without new cabling.

Access security

Authentication of users of Micro Switch at the workplace ensures that a user without the necessary authorization does not even gain access to the network. Fully compliant with the IEEE 802.1X standard, it extends far beyond the requirements of the standard and offers comprehensive assurance with port security. If a terminal device attempts to register with the Micro Switch, the request is sent to the RADIUS server and the Switch makes a decision dependent on the response. Dependent on the decision, the user then enters a secure VLAN or is blocked directly at the workplace connection.

However, modern office environments with Voice over IP (VoIP) demand more than this. If a user connects his PC or laptop with the network via a VoIP phone, conventional switch solutions can cause a security problem, as there is still a network port on the authenticated phone that is not authenticated by the switch. With multi-user authentication from MICROSENS, the switch can distinguish between devices: For instance, the VoIP phone can be authenticated from the machine certificate, the laptop or workplace computer connected from the MAC address. Depending on the switch configuration, other devices are rejected.

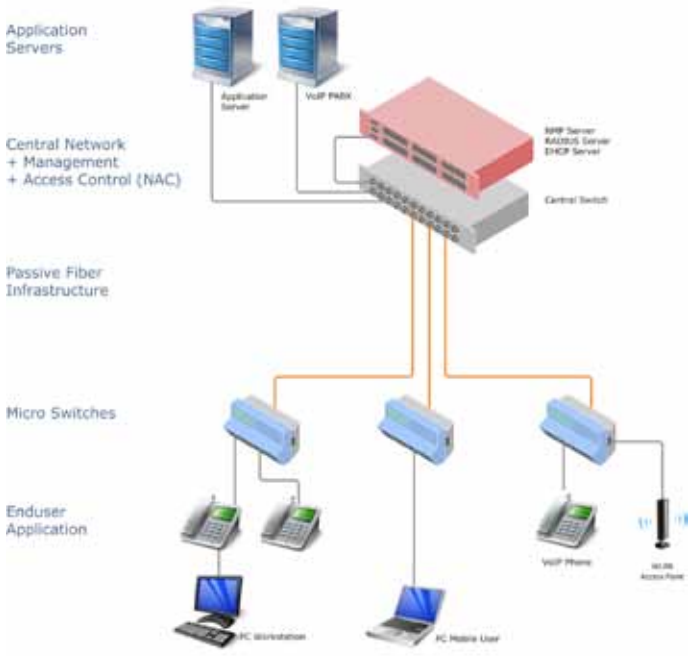
If a non-authorised terminal device attempts to register, it is switched to a guest or quarantine VLAN rather than completely blocking the switch port. This way terminal devices connected to the IP phone that are already authenticated, as well as the phone itself, remain in the network and are therefore fully functional.

Access to the switch management is also subject to RADIUS server authentication, which provides additional security.

For those who like it simpler: Access can, of course, be restricted to a single MAC address per port. If the switch port is permanently assigned to a terminal device, this offers additional protection. Other devices are denied access, which simply and effectively prevents intrusion by cascading. This does not require a RADIUS server.

Fail-safe performance

Additional redundancy can be created by cascading micro switches. Here it is sufficient to connect switches together via glass fibers or copper lines - in the simplest case with a patch cable. Even more redundancy can be achieved with dual homing, whereby each Micro Switch is connected directly via two links with one or two core switches. The Rapid Spanning Tree Protocol (RSTP) ensures safe operation and the shortest possible switching times should the main link ever fail.



Network with decentralised switching architecture and centralized network access control.

Effective anti-theft protection with Disconnect Monitoring

The Micro Switches' Disconnect Monitoring function detects whether a terminal device connected to the switch is removed. Cyclic impedance measurement of the connection via the twisted pair cable permanently monitors the switch to detect whether a terminal device is physically connected - even if it switched off. The theft of a terminal device switched off overnight can therefore be reliably ascertained and an alarm immediately triggered. Conventional switches can only detect that a terminal device is connected from the link status. Once the terminal device is switched off, removal of the device cannot be ascertained.

Alarm messages from the Disconnect Monitor can be configured as SNMP traps or Syslog and are forwarded via a suitable external service, such as SMS or e-mail. The administrator and security service can then be informed quickly and reliably.

Simply more secure

Whether glass fibers or copper cables - building infrastructures with decentralised switch architecture offer a wealth of advantages.

Less cabling work and easy expandability of existing networks without operational disruption lead to low installation and operating costs.

The Micro Switches deployed at the workplace offer all security features that were previously the preserve of core switches. With monitored, managed devices in the user's vicinity, unauthorized access can be denied even before it connects with the network. Pioneering functions, such as Disconnect Monitoring, can ascertain whether terminal devices are removed - even if the terminal device is switched off. The possibility of simple cascading and dual homing ensure increased protection against failure with a minimum of investment.

Decentralised infrastructure solutions not only offer technical, but also economic advantages, as the relevant studies have proven.

GBE Desktop Switch from MICROSENS with Disconnect Monitoring watches also switched off terminal decives and therefore provides an effective anti-theft protection.