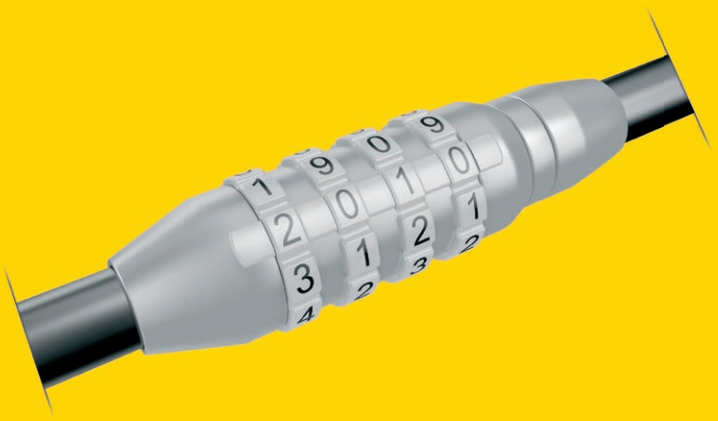
STENTOFON



IP NETWORKING AND SECURITY

ADVANCED NETWORKING AND SECURITY FUNCTIONS IN STENTOFON'S IP STATION RANGE

IP NETWORKING AND SECURITY FUNCTIONS

IP networking has become the communication technology of choice for newly deployed security systems.

STENTOFON has introduced a set of advanced networking and security functions in its IP station range to optimize the deployment of IP security devices such as IP intercom and CCTV cameras. These new functions provide:

- Protection from unwanted access
- Quality of Service (QoS) by managing data traffic
- Increased system availability through redundant LAN infrastructure
- Cost efficient installation by providing shared network connections through the integrated data switch

PROTECTION FROM UNWANTED ACCESS

Today, everyone benefits from the convenience of IP technology through plug and play connectivity to fixed as well as wireless IP networks.

However, the very convenience of IP technology comes with one critical issue - i.e. how to secure networks from UNWANTED ACCESS. Unwanted access both consumes network capacity, hence disrupting service, and introduces the risk of malicious intrusion and manipulation.

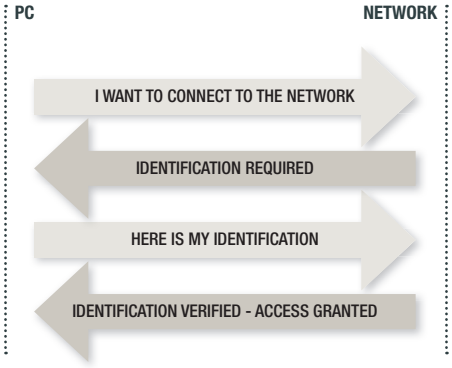
In particular, wireless IP networks are prone to unwanted access as they lack any physical protection; the way these networks are managed and secured point to system deficiencies that can be resolved.

A similar lack of physical protection becomes apparent in IP security devices which are deployed in public areas; in many cases it is possible for an intruder to get physical access to the network port used for the IP security device.

NETWORK ACCESS CONTROL (IEEE 802.1X)

STENTOFON has built the IP intercom station to conform to the same standard that is used for the protection of wireless networks, i.e. IEEE802.1x.

IEEE 802.1X is an IEEE Standard for port-based Network Access Control ("port" here means a single point of attachment to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN; it either establishes a point-to-point connection on authentication or it prevents such a connection if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP).



Upon detection of the new client (supplicant), the port on the switch (authenticator) is enabled and set to the "unauthorized" mode. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is blocked at the network layer (Layer 3). The authenticator sends out the 'EAP-Request identity' to the supplicant and the supplicant responds with the 'EAP-response packet' that the authenticator forwards to the authenticating server. If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed. When the supplicant logs off, it sends an EAP-logoff message to the authenticator. The authenticator then sets the port back to the "unauthorized" mode, once again blocking all non-EAP traffic.

A recent Gartner survey indicates that 50% of enterprises plan to implement 802.1X in their wired networks by 2011. Gartner believes that momentum will increase strongly, and that actual enterprise adoption will reach 70% by 2011.

Gartner, "Findings: Wired 802.1X Adoption on the Rise," Lawrence Orans and John Pescatore, July 28, 2008

SERVICE QUALITY BY MANAGING DATA TRAFFIC

Different types of data services may interfere with each other if they share the same data switch or network connection. For instance, a file transfer service may consume capacity required for a VoIP service, hence reducing audio quality, or a guest logon service may introduce a security risk to trusted data services. For a cost efficient installation, it is of particular interest if remote IP devices such as intercom stations and cameras can share a network connection while still maintaining quality of service and security.

MANAGED DATA SWITCH WITH VLAN

VLAN (Virtual LAN) technology provides the means to manage a data switch and IP network with regards to traffic flow and security.

STENTOFON has upgraded the integrated IP switch in their IP stations to be a managed data switch supporting VLAN, meaning that STENTOFON IP stations allow a single network connection to be shared between CCTV cameras, PCs and multiple IP intercom stations without disrupting service quality or violating security.

VLAN technology uses the concept of tagging. Each Ethernet data packet gets a VLAN IEEE 802.1Q field, see figure 1. This field includes a VLAN identifier as well as a packet priority value.

Figure 2 shows an example of how a single network link can be shared between an IP intercom station and an IP camera. The managed switch in the intercom station can be assigned to fast forward (separate priority queue) and tag VoIP intercom packets with higher priority than video packets. This will ensure that the important real-time requirements for voice are kept, thus maintaining good audio quality.

FIGURE 1 - IEEE 802.1Q VLAN TAG IN ETHERNET FRAME

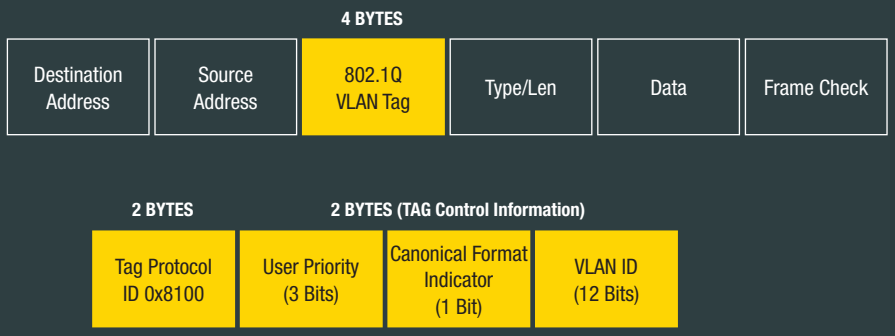
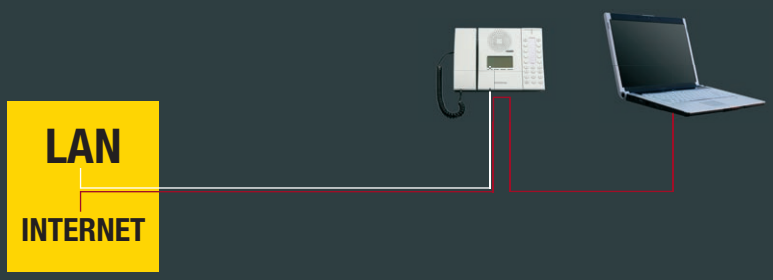


FIGURE 2 - VLAN PRIORITY ENSURING SERVICE QUALITY

Figure 3 shows how two services with different security and quality parameters may share the same network link. The IP intercom station will assign packets from the PC to a separate VLAN. Only then is the PC given access to the Internet.

FIGURE 3 - VLAN SEPARATION FOR SECURITY



REDUNDANT LAN INFRASTRUCTURE SUPPORT IN IP STATIONS

The integrated IP switch in the STENTOFON IP station supports the Spanning Tree and Rapid Spanning Tree protocols. This makes it possible to provide a very cost efficient deployment of IP intercom where multiple intercom stations are daisy chained to maintain connections in case of a cable break. See Figure 4 and 5.

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path is allowed to exist between two points, and STP resolves this issue.

To provide path redundancy, STP defines a tree that spans all switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the spanning tree becomes unreachable, or if STP costs change, the spanning tree algorithm reconfigures its topology and re-establishes the link by activating the standby path.

FIGURE 4 - LAN INFRASTRUCTURE WITHOUT REDUNDANCY

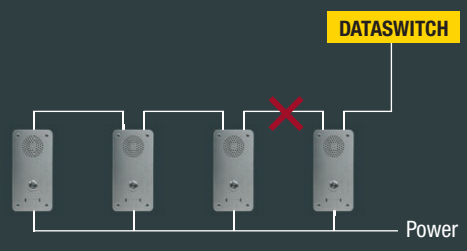
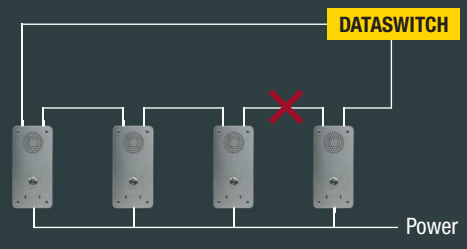


FIGURE 5 - LAN INFRASTRUCTURE WITH REDUNDANCY



www.stentofon.com

DOC NO
A100K10749

sales@stentofon.com