System Integration

Specification

Authors:

Schoberlechner

Table of Contents

1 Document Status

Version	Date	Edition notes, reason for changes	Name
V1.0	7.2.2008	First edition	Schoberlechner
V1.1	22.10.2008	Alterations to the Topology and VcIP switch	Schoberlechner
V2.0	11.6.2010	Segmentation, Redundancy and IP Addresses	Schoberlechner
V2.1	21.12.2012	Examples of the system segmentation	Schoberlechner
V2.2	17.07.2013	POE extension	Schoberlechner
V2.3	18.09.2013	NSP protocol extension	Schoberlechner

2 Introduction

The document describes the system integration and assignment of IP addresses.

A fixed assignment is required for the IP addressing in the nursecall system's operation. The individual issuing of addresses of devices is only carried out during the commissioning process, centrally from the configuration using a *Network Setup Server*. During ongoing operation of the nursecall system these IP addresses are then managed by a *Network Setup Master* and assigned to a *Network Setup Device*.

The *Network Setup Server* is a service which runs permanently on the centralised components or is executed temporarily on a Service PC (e.g. on a laptop).

The *Network Setup Master* is a service which is permanently run on every VcIP Switch. The *Network Setup Master* ensures, for example, that if the *Patient terminal* is disconnected and connected elsewhere, that it can be assigned to the correct room and bed in accordance with its new position when it restarts.

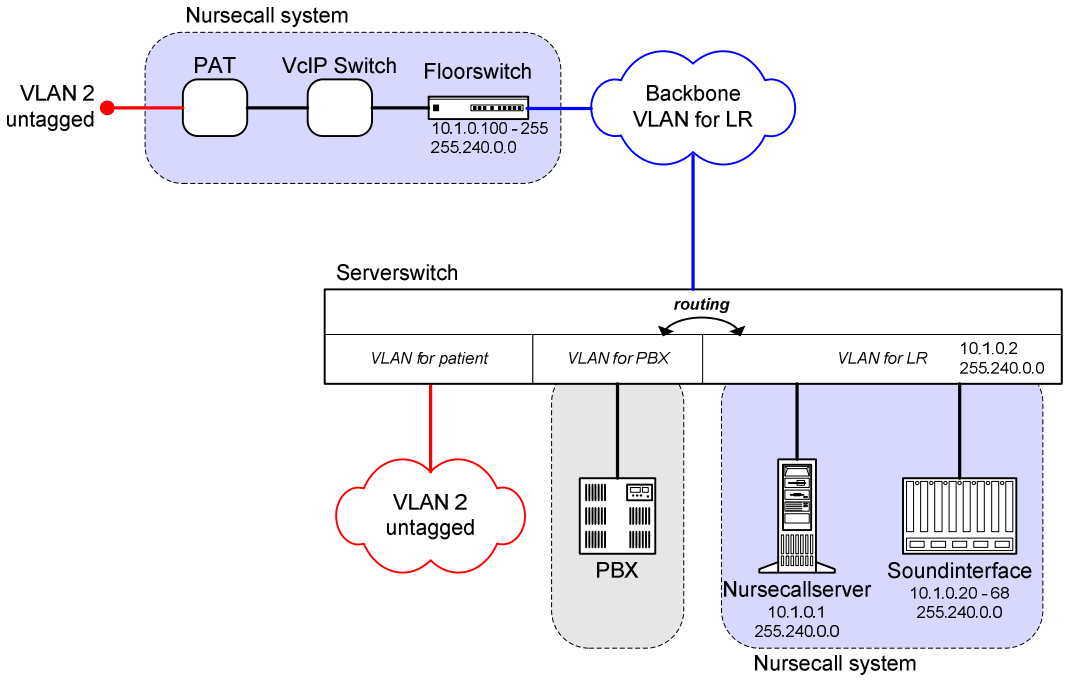
3 System Structure

By definition, according to the standard *VDE 0834* transmission paths of other systems are not allowed to be used for the call system. A ward or a floor is defined as the smallest unit of a nursecall system for VcIP. The interconnection of the separate nursecall systems is carried out using a *Backbone* which in accordance with the standard is no longer a part of the nursecall system. The ward or floor loop must be created in accordance with the standard as a stand-alone network and its galvanic isolation from the *Backbone* must be ensured by using a fibre optic *uplink*.

When using several services, it must be ensured by the *Backbone*, that the nursecall data is prioritised and isolated from all other services which are transported over the VLAN. A routing of nursecall data within the *Backbone* is only allowed via a *Logical Delivery Point* (see also 3.1), as the network configuration is carried out on layer 2.

The transport of services other than nursecall, such as Internet, TV streaming etc. is always carried out over a defined system interface. This interface is realised from the switch in the *Patient terminal* (PAT) centrally to a network switch. This interface is, by default, separated by the VLAN 2 (see also 5.2.1) from the nursecall system. The prioritisation of VLAN 2 is set permanently by the configuration to *lowest*.

For connecting external systems, such as telephony, billing etc. a VLAN 2 is only established on a centralised *Serverswitch*. This VLAN 2 can then be routed in accordance with the *Serverswitch* into the nursecall network on layer 3. The gateway address for the VLAN PBX at the *Serverswitch* must also be configured in the nursecall system, in order to be able to enter the relevant route on the individual *PAT* modules.

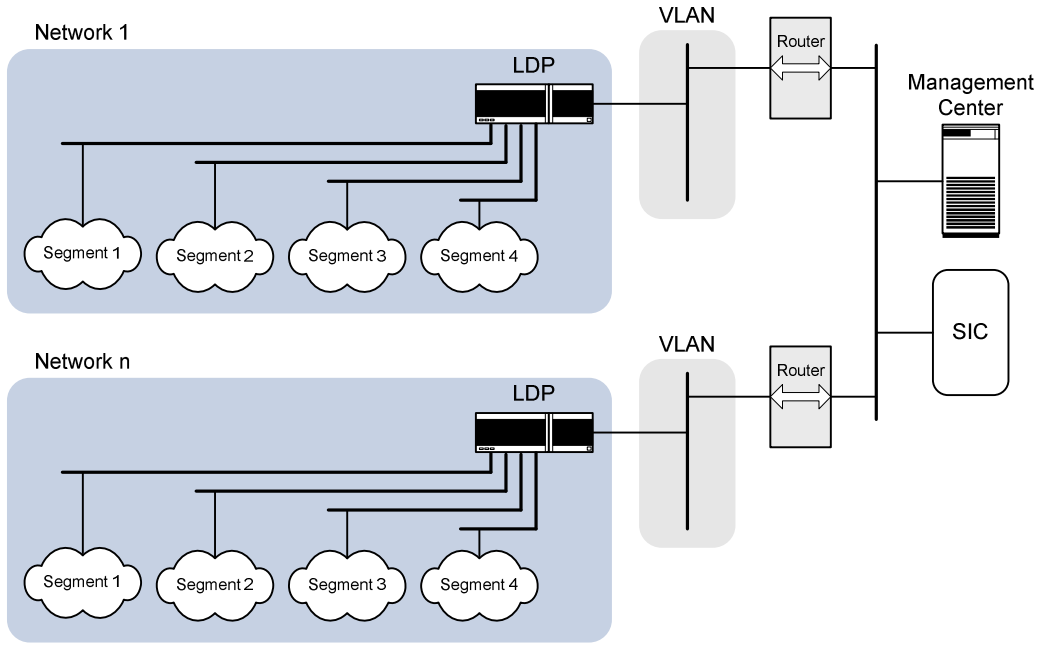


3.1 Segmentation of the Networks

The *Logical Delivery Point* functions as a gateway between the individual VcIP networks and through to the *Management Center*. The individual VcIP segments are, thereby, physically separated from each other. Therefore, if a complete VcIP segment fails, the other segments are not affected.

In addition, the *LDP* also serves as a central configuration node for its four segments. A change of firmware or configuration may then be incorporated into the *LDP*s individually. This results in a partial update being able to be carried in a larger system. Furthermore, the *LDP* is also provided for small systems, as a replacement for the *Management Center*, as long as no central services are needed.

It is to be ensured that the segments of an *LDP* continue to be achieved as Layer2 networks. A routing function between the individual networks is only made available through the *uplink* of the *LDP*. The individual routes in the backbone are to be considered optional, as a pure Layer2 connection of the backbone is possible.



4 LDP – Logical Delivery Point

The LDP fulfils the criteria of standard VDE 0834, and is part of the nursecall system. It is therefore in network technology terms not a switch in conventional terms.

Protocols:

Layer 2 “Network Setup Protocol” Ethernet Type 0x3000

IEEE 802.1p Priority

IEEE 802.1Q VLANs

RFC 768 UDP

RFC 783 TFTP Protocol (revision 2)

RFC 793 TCP

RFC 826 ARP

RFC 2236 IGMPv2

Uplink:

1 RJ-45 auto-sensing 10/100/1000 port (IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE 8023y)

Media Type: Auto-MDIX

Duplex: half or full

Port 1 to Port 4

4 RJ-45 auto-sensing 10/100 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX)

Media Type: Auto-MDIX

Duplex: half or full

Service:

1 RJ-45 auto-sensing 10/100 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX)

Media Type: Auto-MDIX

Duplex: half or full

5 SWI9 – VcIP System Switch

The VcIP switch fulfils the criteria of standard *VDE 0834*, and is part of the nursecall system. It is therefore in network technology terms not a switch in conventional terms.

Protocols:

Layer 2 “Network Setup Protocol” Ethernet Type 0x3000

IEEE 802.1p Priority

IEEE 802.1Q VLANs

RFC 768 UDP

RFC 783 TFTP Protocol (revision 2)

RFC 793 TCP

RFC 826 ARP

RFC 854 TELNET

RFC 951 BOOTP

RFC 2236 IGMPv2

Uplink:

1 RJ-45 auto-sensing 10/100 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX)

Media Type: Auto-MDIX

Duplex: half or full

Backbone loop Detection

Port 1 to Port 7:

7 RJ-45 auto-sensing 10/100 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX)

Duplex: half or full

Power over LAN: 24V 500mA monitored

Security: “Hardware detection”

Interface for diagnostic socket at bed (galvanically isolated 24V 150mA monitored)

Port 8:

1 RJ-45 auto-sensing 10/100 port (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX)

Media Type: Auto-MDIX

Duplex: half or full

Power over LAN: 24V 500mA monitored

Redundancy capable for increased system security

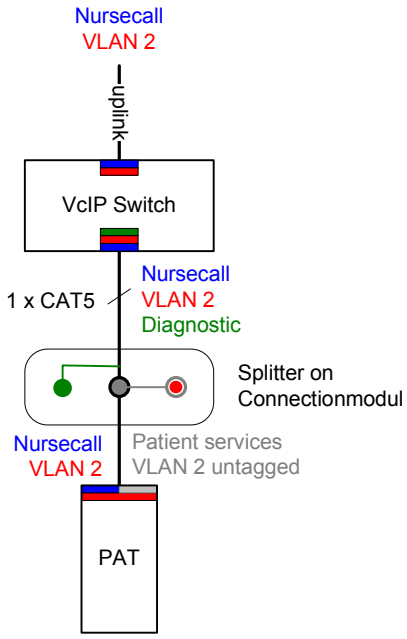
VLAN untagging

5.1 “Hardware detection”

Ports 1 to 7 are equipped with “*Hardware detection*”. The VcIP switch blocks the connection as long as there is not a nursecall device connected. That means that both LAN sockets on the connection module at the patient bed are unavailable without a *Patient terminal*.

The VcIP switch detects a *Patient terminal* using a specific *Signature Measurement* at the relevant LAN Port. Only if a *patient terminal* is detected at the port, is the connection released by the VcIP switch. Thereafter, the LAN socket for patient services is made available by the *Patient terminal* by means of its internal switch.

5.2 Splitting of Services



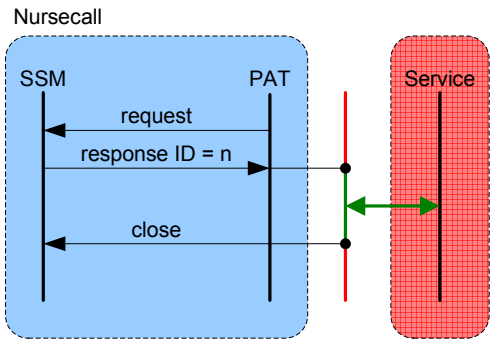
The *patient terminal* makes the nursecall including telephony service available. The freely accessible LAN connection on the connection module at the bed is isolated from nursecall by the VLAN. Customer-specific services can be made available at this connection, which are made available to the patient using a router.

Since the different nursecall and patient services are isolated from one another for safety reasons, only a static port-based VLAN can be seen to increase security. Since the VLAN assignment is rigidly bound to the switch port in the *patient terminal* and therefore also to the physical network socket at the bed, a potential intruder is only able to gain physical access to VLAN 2, i.e. that for patient services.

5.2.1 Dynamic VLANs

In order, for example, to be able to split the patient services in the backbone into different VLANs, dynamic switching of the VLANs at the *Patient terminal* is available.

The LAN connection at the bed is always served by the “unsecure” VLAN 2 with ID 2. This can either be blocked completely by the floor switch, or can make standard services available. Only once the required service has been logged onto at the centralised *Security Service Manager* (SSM) by the nursecall system, is the LAN socket switched over to the relevant VLAN ID by the *Patient terminal*.

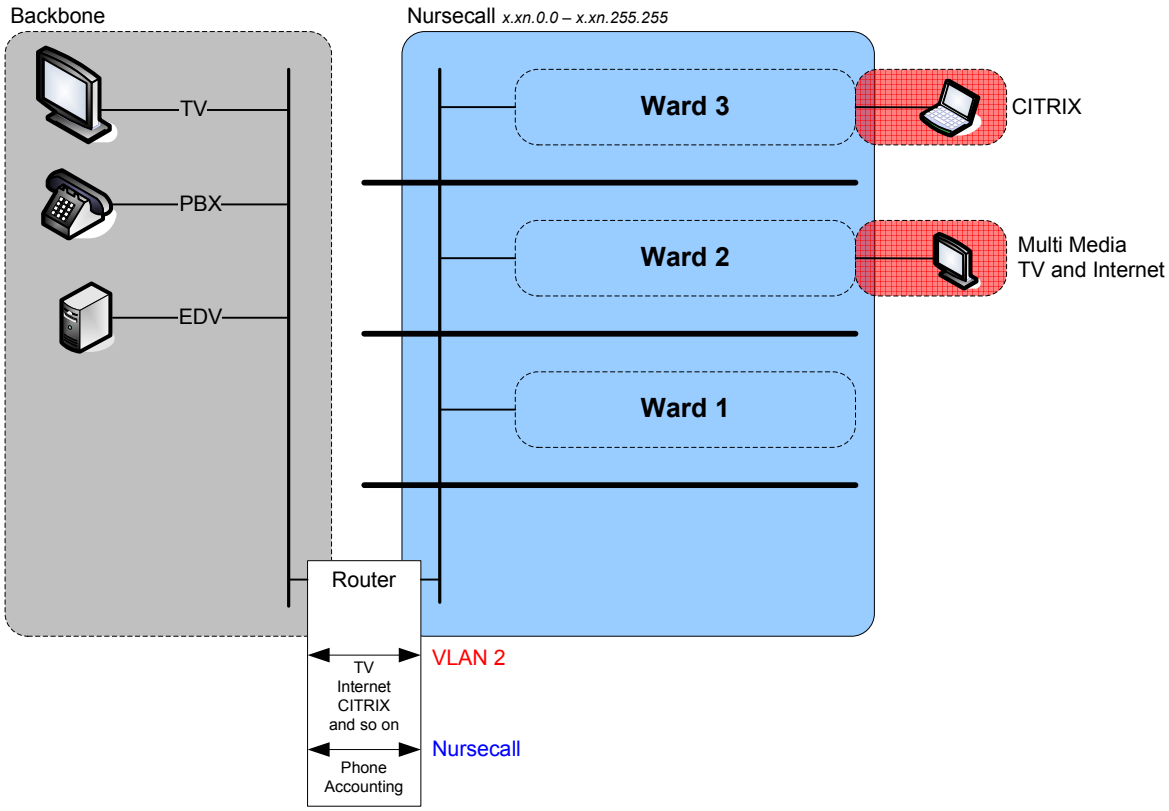


The VLAN assignment therefore continues to be one of a static port-based VLAN, however, there is a dynamic switchover based on the service that is actually required. Only one VLAN or service can be activated at the same time. When connecting to a Schrack Multimedia Terminal, the toggling is automatically done on the multimedia VLAN ID.

The *Security Service Manager* logs every login and logout from services, and can also make this information available to the billing system.

Example:

The patient wishes to surf the Internet using his notebook. To do so, he activates the “Internet” function in a menu on the *Patient terminal*. The *Patient terminal* requests the “Internet” service at the SSM, and receives the requisite VLAN ID back from it. After the port has been switched over, the patient can use the Internet function. Access is ended again through the menu on the *Patient terminal*, or by unplugging the notebook.



5.2.2 VLAN Untagging on Port 8

On port 8, a static VLAN with an ID of 2 – 4094 can be set up as an option. So there is the option, for example, of providing TV streams from the multimedia VLAN to a set-top box on port 8 untagged.

5.3 Loop Protection

The *uplink* monitors the network on a loop in the backbone. If a loop is detected, the SWI9 separates its *uplink* from the backbone for at least 5 minutes. The *uplink* is then checked again after 4 minutes for whether the loop continues to be available. If this is the case, the *uplink* remains disconnected, and the next review is started after a minute.

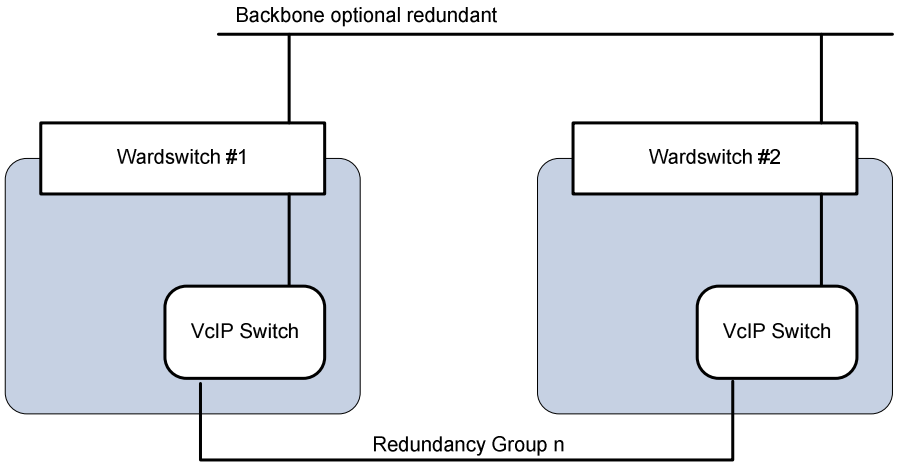
By disconnecting the *uplink* an "island mode" of the individual SWI9 is also guaranteed with a loop. Cabling the PAT, KMT and IO bus of a room to an SWI9 or a redundancy pair, the *VDE 0834* paragraph 5.6.2. is fulfilled to the extent that the display on the room light will still function if communications break down.

5.4 Redundancy via Port 8

A redundancy of the backbone is not strictly necessary for the redundancy function of the SWI9. It is to be noted, however, that a complete whole-ward redundancy is only guaranteed if the complete backbone redundancy is run. The configuration of the backbone can be done through STP *Spanning Tree* or RSTP *Rapid Spanning Tree*. This configuration is to be considered independently of the redundancy function of VcIP. A coordination of the backbone with the redundancy function of VcIP is not necessary.

The redundancy function of SWI9 only covers the failure of a ward switch. With a failure of the second ward switch, only an emergency mode of both SWI9 is possible any more through the *Redundancy Group* line.

By assigning a ward to two independent ward switches, the redundancy function of the SWI9 prevents failure of the complete ward independently of the backbone structure with a failure of a ward switch.



6 Network requirements

POE must be disabled on all SWI9 ports!

6.1 Backbone

- VLAN up to the central serving of the patient services
- Static VLAN LR for nursecall to all floors and server with the highest priority
- QoS with *Differential Service Field*
- IGMP snooping with IGMP *querier* for VLAN LR and VLAN 2, IGMP Version 2

6.2 Floor Switch

- SNMP access with read access
- QoS with *Differential Service Field*
- IGMP snooping for nursecall and VLAN 2, IGMP Version 2

6.3 Server Switch

- VLAN 2 untagging at the central serving point with priority of 1
- IP routing between external systems and the nursecall network
- 1 Port with 1Gbit for the Management Center
- 1 Port with 100Mbit for each SIC with 2 radio channels from the *sound interface*
- QoS with *Differential Service Field*
- IGMP snooping for VLAN LR and VLAN 2, IGMP Version 2

6.4 Bandwidths

- Nursecall 10MBit
- Per nursecall conversation 64kBit
- Per radio channel 64kBit
- Per telephone call 64kBit
- Per TV stream 5MBit

6.5 IP addresses used

The size of the network is, in principle, geared towards the choice of available components in the network, and is independent of the distribution on the segments. However, a minimum number of 1024 addresses is reserved for a network. This produces the smallest possible network mask with 255.255.252.0.

H/2 is always reserved by the host addresses H for the service mode. Therefore, 511 host addresses are available with the smallest possible configuration. As the address range from 1 to 255 is reserved as fixed, 256 component addresses are left. If more component addresses are needed in a system, the network mask is to be adjusted accordingly.

The number of component addresses is assigned according to the following key:

Control panels: $$\left(\frac{H}{2} - 255\right) \times 0.05 = \lfloor L_1 \rfloor$$

Devices $$\frac{H}{2} - 255 - L_1 = G_1$$

In the smallest possible system with 1022 host addresses, 12 addresses are therefore available for the control panels and 244 addresses for the devices.

The fixed host addresses are assigned as follows:

Address		Description
x.1		Management Center
x.2	x.19	Reserved for other system servers
x.20	x.68	Sound Interface Cards
x.69	x.99	Unused
x.100	x.239	SNMP for system switches
x.240	x.255	DHCP for service computers

The important network masks needed depending on network size:

Network Mask	Host	Addresses	Max. Control Panels	Max. Devices
255.255.252.0	1022	511	12	244
255.255.248	2046	1023	38	730
255.255.240	4094	2047	89	1703
255.255.224.0	8190	4095	192	3648

x ... Network set up according to the relevant network mask, and can be freely configured.

H .. host addresses $2^{32 - n} - 2$

For broadcasting multimedia services, the following multicast groups are used with a TTL of 31. Each Media Gateway sends its Media offer to the group 239.0.3.0. Through this group, all the clients obtain the information on which multicast group and port the corresponding media stream can be received.

Group	Usage
239.0.3.0	Multimedia offer information
239.0.3.1 – 239.0.3.32	Radio channels 1 to 32

7 Examples of network segmentation

In network segmentation, a standalone network must be assigned for each system. In addition, a **separate** network must always be assigned for the *uplink* connection for routing in the backbone.

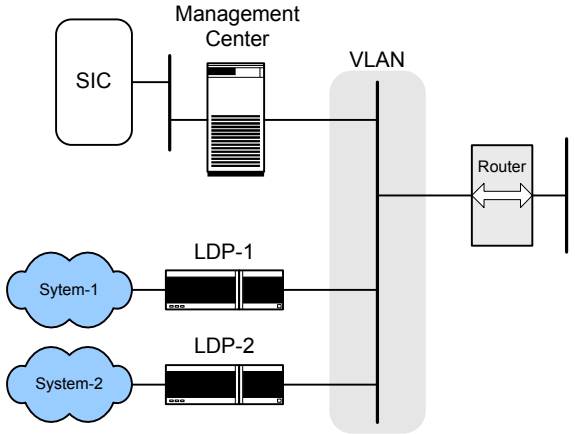
For the system route on the gateway, the “next hop” address is always the respective *uplink* IP address of the LDP or MMC here!

7.1 Network segmentation without a system router

For dividing a large system into smaller subsystems without external system routing, the individual systems are only connected with the *uplink* via a separate VLAN. Connection of the telephone system and to the external system is carried out via a central gateway (router).

Example:

Two systems, each with max. 1703 devices are implemented via LDP-1 and LDP-2. The *sound interfaces* are centrally assigned to the *management centre*. The *uplink* connections of the LDPs and of the *management centre* are connected to each other via a separate VLAN in the backbone network.



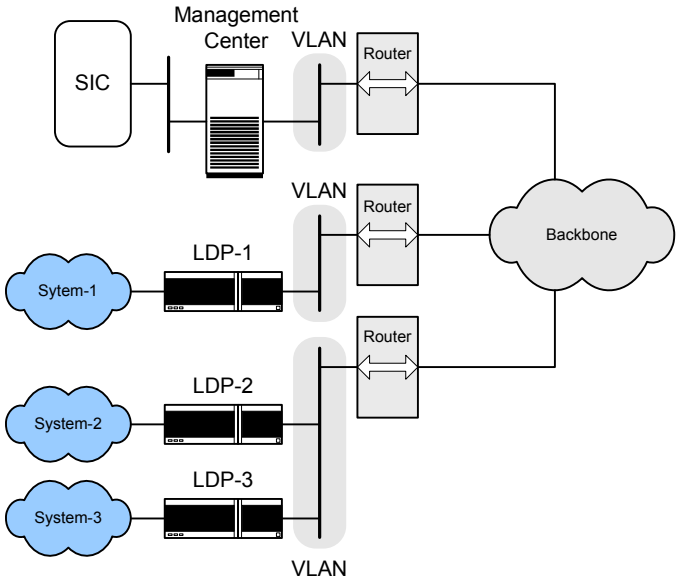
System			Uplink		
Name	Network	Netmask	Address	Netmask	Gateway
MMC	172.16.0.0	255.255.240.0	10.112.168.1	255.255.255.0	10.112.168.250
LDP-1	172.16.32.0	255.255.240.0	10.112.168.2	255.255.255.0	10.112.168.250
LDP-2	172.16.64.0	255.255.240.0	10.112.168.3	255.255.255.0	10.112.168.250

7.2 Network segmentation with a system router

For dividing individual systems via a routed backbone connection, the systems are connected to the network of the gateway (router) via the *uplink*. The routers then make the corresponding routes available for the system networks via the backbone. Connection of the telephone system and to the external system is also carried out via a central gateway in the backbone.

Example:

Three systems, each with max. 1703 devices are implemented via LDP-1 to LDP-3. The *sound interfaces* are centrally assigned to the *management centre*. The *uplink* connections of the LDPs and of the *management centre* are connected to the system routers via a separate VLAN. LDP-2 and LDP-3 additionally form local network segmentation.



System			Uplink		
Name	Network	Netmask	Address	Netmask	Gateway
MMC	172.16.0.0	255.255.240.0	10.112.101.1	255.255.255.0	10.112.101.250
LDP-1	172.16.32.0	255.255.240.0	10.112.102.1	255.255.255.0	10.112.102.250
LDP-2	172.16.64.0	255.255.240.0	10.112.103.1	255.255.255.0	10.112.103.250
LDP-3	172.16.96.0	255.255.240.0	10.112.103.2	255.255.255.0	10.112.103.250