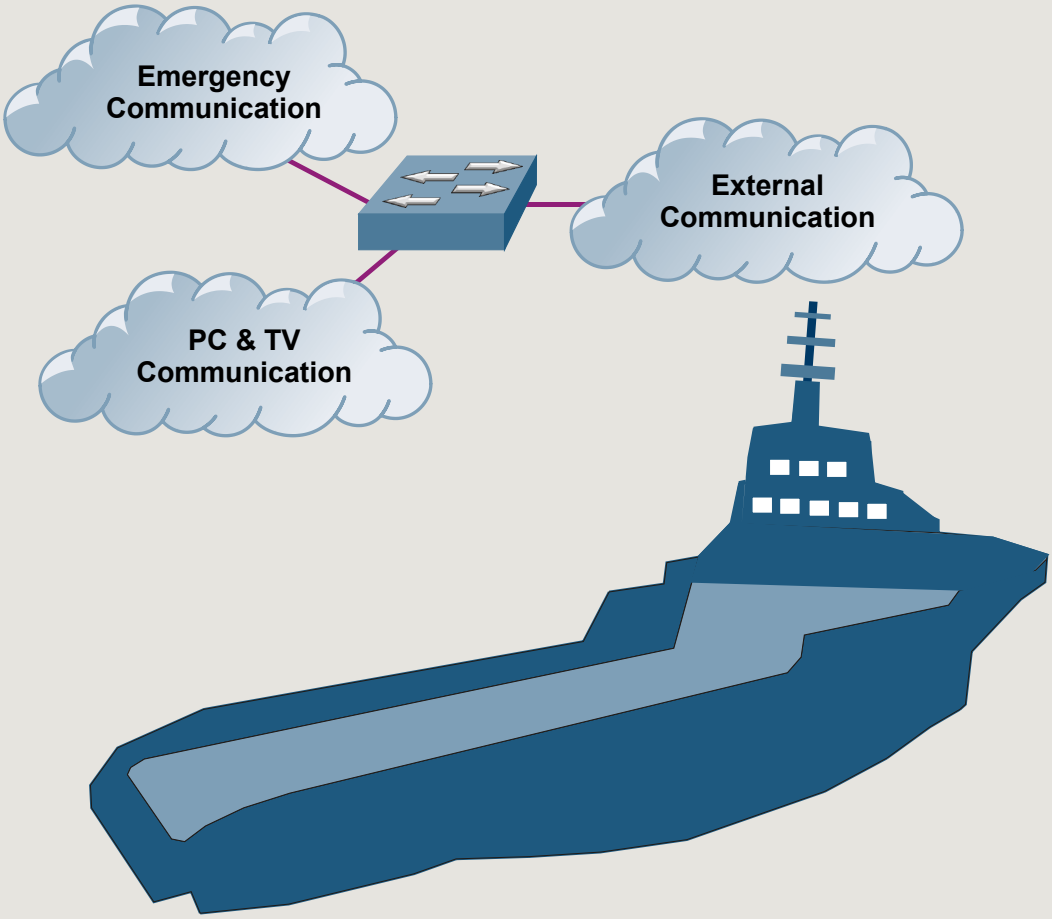
# Data Network Guidelines for Ships

VINGTOR ACM Solution

VINGTOR




DEPLOYMENT GUIDE

A100K10649

# Contents



# Figures

# 1 Introduction

## 1.1 About this Document

The scope of this document is to provide guidelines for implementing a data network on ships in order to comply with the type-approved emergency communication requirements for the VINGTOR ACM solution.

## 1.2 Revision Information

| Rev. | Date | Author | Status |
|---|---|---|---|
| 1.0 | 3 Feb 2010 | HKL | final |

## 1.3 Related Documentation

| Document no. | Subject |
|---|---|
| A100K10647 | ACM Family System Overview and Installation |
| A100K10646 | User Guide for ACM Emergency Functions |
| A100K10587 | ACM-M-A-V2 ACM Telephone System |
| A100K10369 | SPA-V2 Public Address and General Alarm System |

## 1.4 DNV Type Approval Regulations

| | |
|---|---|
| 1 | DNV requirement for internal communication on ships, Doc. “Rules for Ships. January 2006 Pt. 3 Ch. 3 Sec. 11” |
| 2 | DNV Rules for Classification of Ships, High Speed & Light Craft and DNV’s Offshore Standards. Type Approval Programme No. 800 Appendix A (827.50.3) |
| 3 | DNV Type Approval Programme No. A-848.21. Automatic Telephone System |
| 4 | DNV Type Approval Programme No. A-848.22. Public Address / General Alarm System |
| 5 | DNV Type Approval Programme No. A-848.XX. Handsfree Voice/Talkback |
| 6 | DNV rules for cable infrastructure |

## 1.5 DNV Type Approval Certificates

| |
|---|
| DNV Certificate No. A-10738, VINGTOR SPA-V2 System |
| DNV Certificate No. E-8001, Data transmission cables and systems |

## 1.6 Acronyms

| | |
|---|---|
| ACM | AlphaCom Marine |
| GA | General Alarm |
| LACP | Link Aggregation Control Protocol |
| PA | Public Address |
| PoE | Power over Ethernet |
| RSTP | Rapid Spanning Tree Protocol |
| STP | Spanning Tree Protocol |
| UPS | Uninterruptible Power Supply |
| VID | VLAN Identifier |
| VLAN | Virtual Local Area Network |

# 2 System Overview

## 2.1 Emergency Functions

The ACM system supports marine emergency functions for:

- Two way communication
- Handsfree, two-way communication (talkback)
- Public address for conventional vessels
- Public address for passenger vessels
- Integrated public address and general alarm

## 2.2 System Architecture

The VINGTOR ACM system comprises the following main types of equipment:

- ACM Main System Rack
- ACM Field Equipment

In addition, an ACM installation consists of the following supplementary systems:

- VINGTOR SPA-V2 Public Address System
- Data Network System

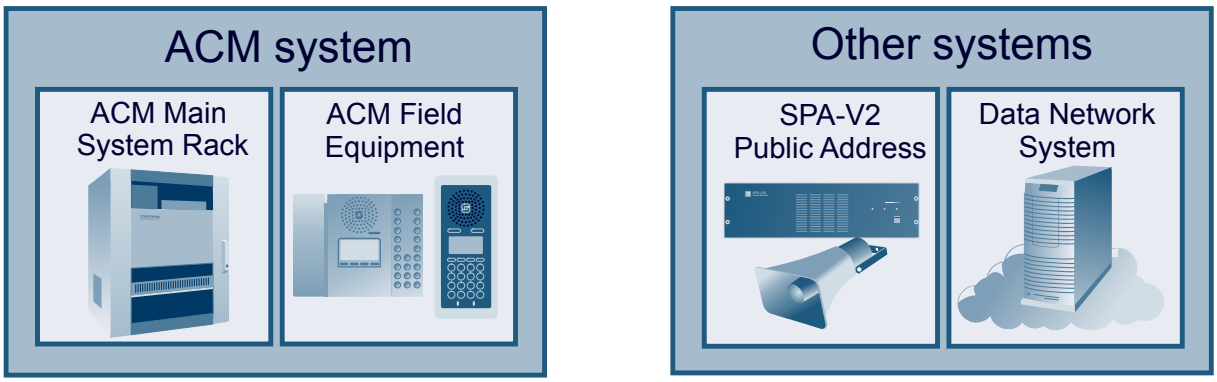



*Figure 1 ACM System*

### 2.2.1 ACM Main System Rack

The ACM Main System Rack is the central unit in the system. It connects all the field equipment together and provides all the main central services. Several system racks can be connected via the data network.

The different ACM systems are built around a STENTOFON AlphaCom E intercom exchange. AlphaCom E is an advanced communication switch designed to meet the growing needs of internal and external communications onboard ships. The exchange features advanced functions such as 1-Bit audio technology (18.5 kHz audio), IP, Web services, and a wide range of integration options.

### 2.2.2 VINGTOR SPA-V2 Public Address System

The SPA-V2 Public Address System is integrated into the overall solution to provide public address coverage using 100V speaker loops in areas

where PA/GA coverage using intercom stations is impractical and where redundant PA/GA coverage is a requirement.

The SPA-V2 system is type approved by DNV as a public address and general alarm system. Refer to *DNV Certificate No. A-10738, VINGTOR SPA-V2 System.*

### 2.2.3 Data network system

The data network system is used to provide network connectivity between the ACM main system rack and IP intercom stations.

# 3 Data Network Overview

## 3.1 Data Network and Type Approval for Marine Emergency Communications

Emergency services include public addressing, general alarm telephone, and talkback. A marine emergency communication system shall comply with the following main requirements:

- Operate 30 minutes after a mains power failure using the ship's 24 VDC emergency supply or UPS (230 VAC) with battery backup.
- Remain viable and be able to complete calls when part of the network infrastructure is down
- Systems providing integrated PA/GA shall provide no single point of failure for broadcasting PA/GA in cabins and public areas
- Always have sufficient bandwidth to provide emergency services
- Protected from unauthorized use and interference
- Cabling infrastructure shall be approved for marine use

Refer to document no. 1 under section 1.4 *DNV Type Approval Regulations* and all other DNV certificates under sections 1.4 and 1.5 for further details.

## 3.2 Network Overview

The following main services onboard a ship require data networking:

- Emergency services (PA/GA, telephony, talkback)
- TV/Radio
- Internet access (Web, e-mail)
- Office services (File, Print, IT administration)
- External communications

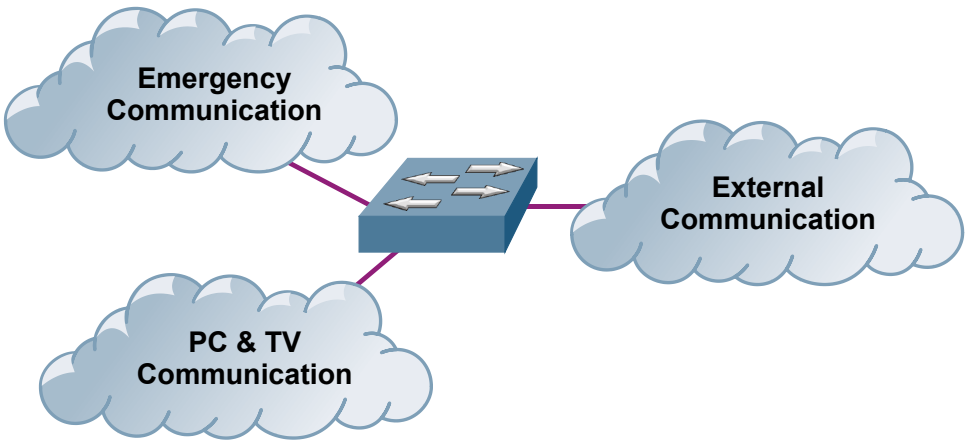



*Figure 2 Network overview*

The emergency services onboard a ship will have different demands on the data network infrastructure from the other data services. In order to manage and implement the requirements that are mandatory for emergency services according to rules and regulations, the emergency communication shall have a dedicated emergency data network.

Figure 2 shows an example of data networks onboard a ship. In order to enable communication between the different networks, a router or gateway is required. It should be noted that special requirements are placed on how the router and gateway is set up in order to prevent unauthorized interference on the emergency services. For further information, see section 5.

# 4 Technology overview

## 4.1 IEEE 802.1Q Standard

The IEEE 802.1Q standard was developed originally to solve the problem of breaking large networks into smaller parts so that broadcast and multicast traffic would not use more bandwidth than necessary. The 802.1 specification established a standard method for inserting Virtual LAN (VLAN) membership information into Ethernet frames. (See figure 3 below)

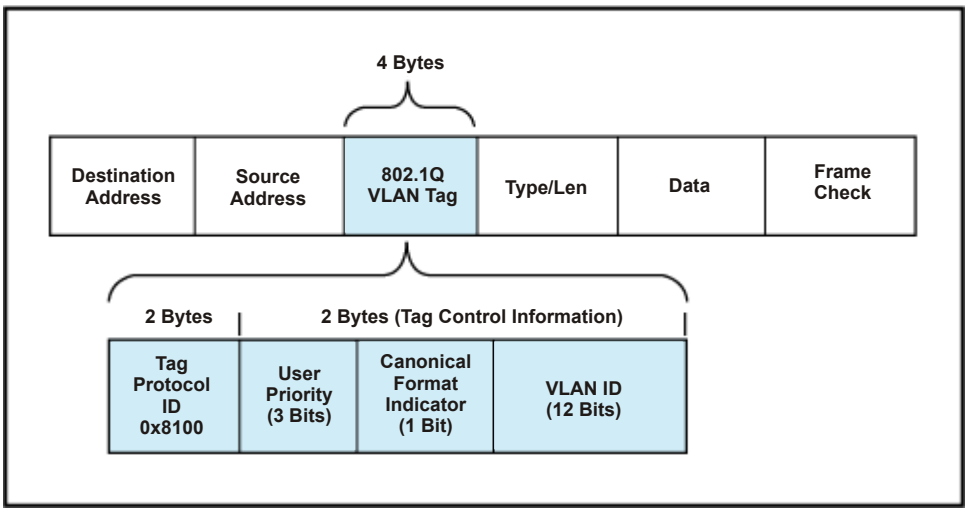



*Figure 3 Insertion of 802.1Q Tag in Ethernet*

VLAN is a logical grouping of end stations that share a common characteristic. The internal networks such as VoIP and data can coexist on the same subnet (LAN) with different VLAN Identifiers (VID) or on two different subnets with different VIDs.

The separated VoIP VLAN and data network can be assigned a priority bit in the same Ethernet tag to ensure Quality of Service (QoS) privileges to the appropriate service such as VoIP on the VLAN.

## 4.2 High Performance

Since network protocols rely on broadcast queries to let end stations discover one another, devices on two different LANs can not see each other without any network layer devices such as a router with ports in both LANs. The router is normally the bottleneck in most network designs. But in the case of VLAN, a managed network switch can perform this service instead. So, communication between two different VLANs is only a matter of determining where a router function is required. The managed switch acts as an intelligent traffic forwarder. Communication between two different VLANs requires a router if the devices/ports involved are not members of the same VLAN. The communication between two devices with membership in the same VLAN is carried out without any broadcast. The managed switch provides delivery of data to the particular VLAN and does not broadcast to all devices on the network such as for normal LAN.

In a VLAN environment with managed switches, the router takes over the functionality of forwarding data with high capacity. Managed/network switches can be configured to transmit tagged or untagged frames. All these result in enhanced performance value while more devices can communicate with each other at the same time without increasing data traffic across the network. As a result, VLAN technology offers the most suitable network solution for VoIP and data without the need for cabling a physical environment for each subnet.

## 4.3 Ease of Management

In a network with managed network switches, the network administrator has more flexibility. The administrator can create, move and change the membership of a user from one VLAN and broadcast domain to another without physically reconnecting the cable on the switch. Hence, VLAN is called an administratively configured LAN or broadcast domain.

VLAN offers greater scalability then normal LAN because it can span over several switches. Sharing VLANs between switches is achieved by inserting a VLAN Identifier (VID). A VID must be assigned for each VLAN on the network. By assigning the same VID to VLANs on many switches, one or more VLAN (broadcast domain) can be extended across a large network.

## 4.4 Security

Tagged data from one port/device is only sent to the destination port/device belonging to the particular tagged VLAN. This method of dividing networks offers a simple network security device optimized to a higher level, especially in combination with the firewall function in the router. The method helps to provide a higher level of security between segments of internal networks. The ability to group end stations/users to different broadcast domains by setting membership profiles (VLAN tagging) for each port on centrally managed switches is one of the main advantages of IEEE 802.1Q. Tagged frames only get sent to the ports where the destination device is attached. Several VLANs can exist on the same switch by assigning different ports to different VLANs.

At the same time, the network requires an authentication mechanism that controls the devices attached to the VLAN. This is a part of the IEEE 802.1 group of networks, and is easy to implement in the network because the IP desktop stations provide the client part and are normally supported by most network switches.

## 4.5 Trunking

The single Ethernet cable provides both the VoIP service and the PC connection. The same line/physical connection on the wall side provides both services (VLAN). This feature is called trunking. (See figure 4 below.)

The figure shows an example of two switches. The same feature is used between two switches, and between the switch and end user. The end user, in our case, is the IP intercom station supporting the trunking feature.

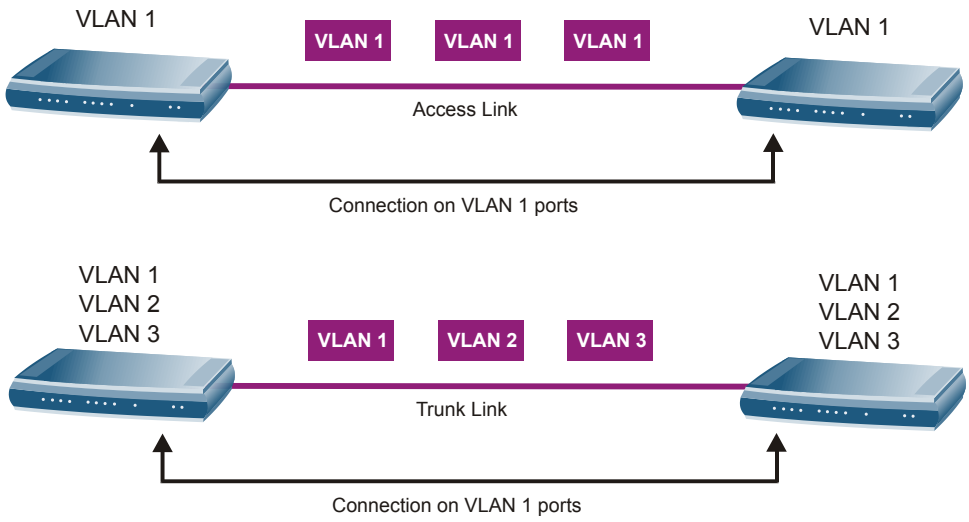



*Figure 4 Difference between conventional access link and trunk link*

## 4.6 Cost Effective

The IP intercom station has two Ethernet ports. One port is dedicated to the network connection while the other port is for PC connection. A single cable provides the intercom service and data network to each user. The patch panel for this type of network is in a simple and uncomplicated format and results in cost savings in network design.

## 4.7 QoS Based Network – Quality of Service

In a network design with support for QoS, better voice transport capabilities over the network is enabled. In most VoIP based networks, the delay and latency times are the most important parameters that need to be considered. Network resources must be carefully allocated to keep total end-to-end delay to a minimum. When QoS is deployed within the network, a more dynamic resource allocation can be realized which does not require dedicating the bandwidth to any particular service. The QoS feature is supported in many low cost network switches as standard and only requires that the end station is capable of tagging the CoS bits in the Ethernet frame so as to make it possible to prioritize voice over data all the way through in the network. Some networks may require that the network switch itself can support port-based QoS. Port-based QoS prioritizes any device connected to the particular port.

# 5 Guidelines and Requirements for Data Networks

## 5.1 General Data Network Structure

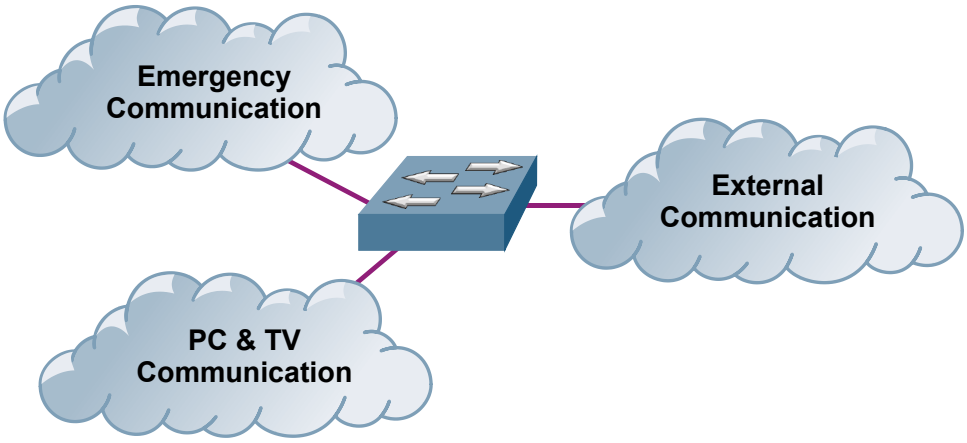



*Figure 5 Network overview*

**Dedicated emergency data network**

A dedicated data network for emergency communication services (PA, GA, talkback, telephone) should be implemented. This will protect emergency services from unauthorized use as well as making it easier to manage and implement the mandatory requirements according to the rules and regulations for data networks on ships (See section 3.1).

**Routing and access to emergency data network**

Access to the emergency communication network from other data networks onboard shall be restricted. Only users and servers with special administration rights shall have access to the network. VoIP traffic to external communication networks shall go through proxy servers or voice gateways.

## 5.2 Managed Network for Emergency Data

The network shall be configured and managed to always have sufficient bandwidth to provide emergency services in all situations. QoS implementation will ensure transportation of important data, especially when data traffic is high on that part of the network

The selection of backbone network switches is the most important part of designing and planning emergency communication and the daily operations of the main core network.

### 5.2.1 Protection from unauthorized use & interference

Onboard ship, crew members of different ranks have different access privileges to services; this will also apply to data networks. The emergency communication data network shall only be dedicated to emergency services (PA, GA, talkback, telephony). Access to the emergency network from other networks shall be restricted.

## 5.3 Guidelines for Different Areas Onboard

Emergency services (PA, GA, telephony and talkback) shall be provided to the following main areas onboard:

- Cabins
- Bridge and control room
- Public and open deck areas

Refer to manual no. A100K10647 *ACM Family System Overview and Installation* for more information.

### 5.3.1 Cabin arrangements

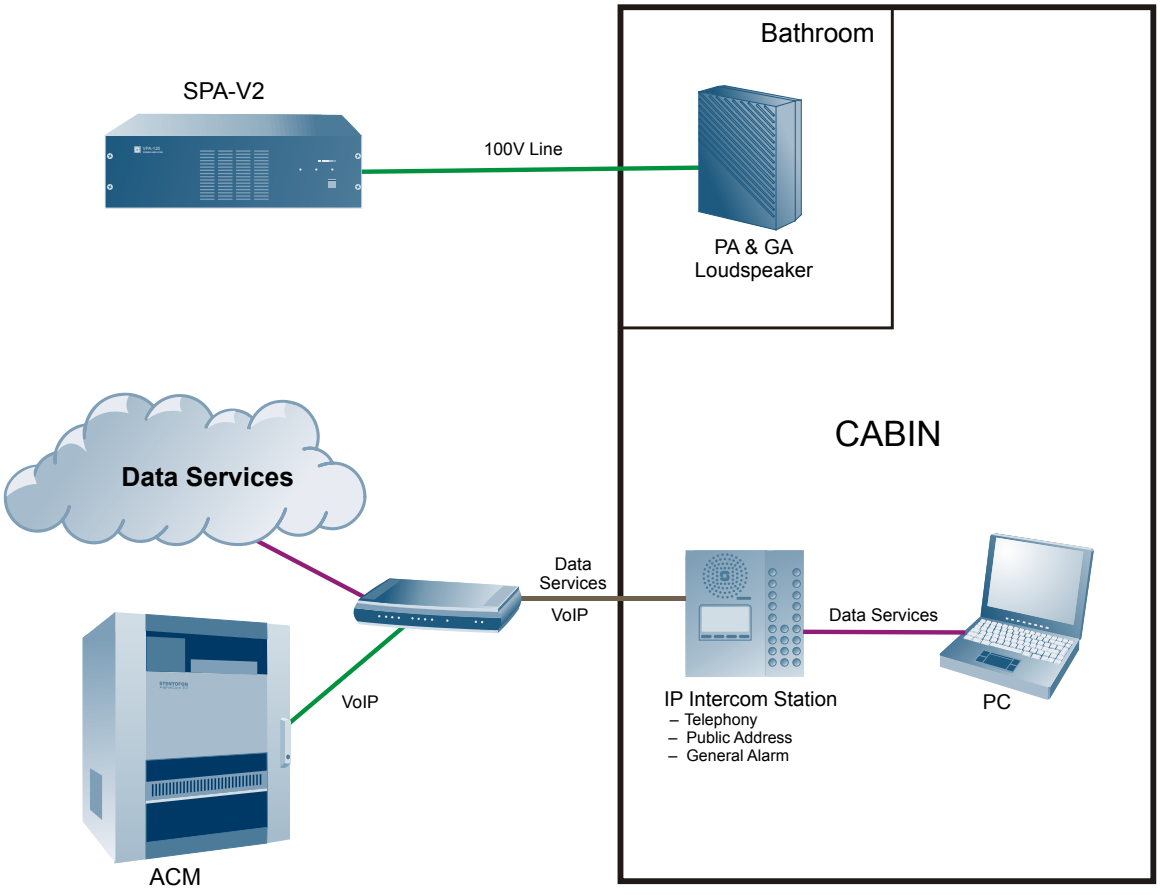



*Figure 6 Cabin network communication*

In a cabin it will often be required to have both PC as well as emergency communication (PA, GA and telephone) services.

**Emergency communication**

The emergency communication services are implemented with IP Master Display intercom stations. The volume override feature on these stations ensures that maximum volume is attained during GA and Emergency PA broadcasts.

In addition, a separate loudspeaker from the SPA-V2 system must be installed in the bathroom of the cabin for PA/GA broadcasts to ensure that there is no single point of failure when PA and GA are integrated in the same system.

**Data networking and PC services**

There will be one data cable between the wall socket in the cabin and the system rack. The IP intercom station is connected to the wall socket (See Figure 7).

The IP intercom station should be supplied with power from the system rack over the data cable according to the IEEE 802.3af PoE standard.

### 5.3.2 Dedicated Emergency Communication

The IP intercom station provides a separate data port for PC services, as well as supports VLAN and trunking. The trunking feature makes it possible to connect the PC to the second Ethernet port of the intercom station and, at the same time, separate the data from the VoIP network.

This will ensure that the audio quality in the IP intercom station will not be affected even in situations where large amounts of data is downloaded to or uploaded from the PC connected to the second Ethernet port of the station. Voice traffic (VID VoIP) will always have priority over data traffic (VID Data) in the IP intercom station. Also, LAN network capacity is not an issue, as a VoIP call with G.722 codec (7 kHz) only requires a bandwidth of about 140 kbps. The normal bandwidth on a LAN is 100 Mbps.

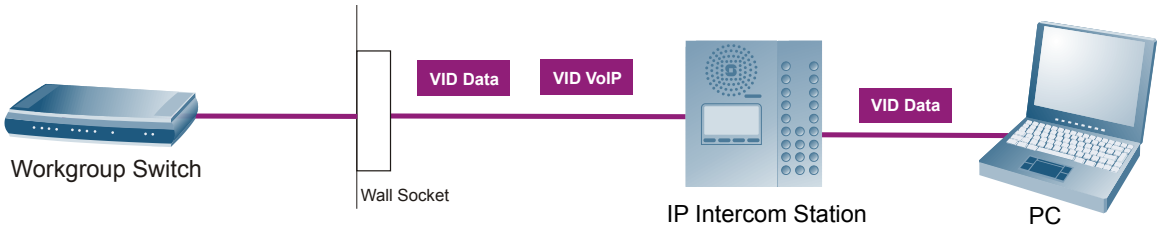



*Figure 7 Dedicated Voice and Data Traffic*

### 5.3.3 Arrangements in other areas

In the other areas onboard the vessel such as the bridge, engine control room, machine room, and open deck, it is not required to have emergency services mixed with other data services on the same data cable.


*Figure 8 Configuration in other areas*

#### 5.3.3.1 Bridge and Engine Control Room

IP intercom stations located in the bridge and engine control room areas are powered by PoE from the workgroup switch but if this is not available, 24 VDC from the ACM cabinet should be used.

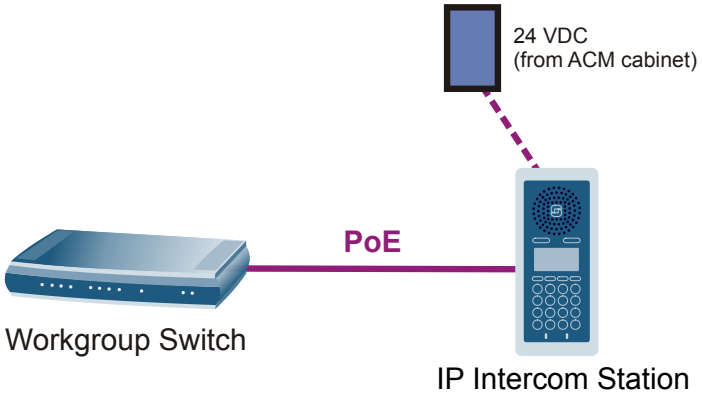



*Figure 9 Configuration in Bridge and ECR*

## 5.4 Power Supply

- PoE (Power over Ethernet) supplying power over the same cable as the VoIP and data network according to IEEE 802.3af standard.
- Central backup of IP telephones and network switches in the event of a power failure with Uninterruptible Power Supply (UPS).
- Power Rating PoE switch: Must be able to supply 7.5W to all PoE ports simultaneously.
- 24 VDC from the ACM cabinet is only available for the IP Flush Master Station.

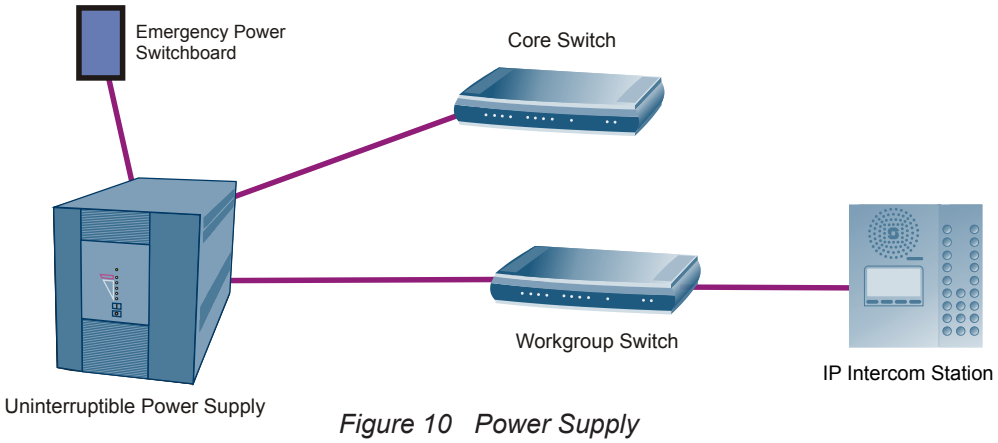



*Figure 10 Power Supply*

## 5.5 Single Point of Failure

To ensure that there is no single point of failure when PA and GA are integrated in the same network system, the following requirements shall be complied with:

- Systems providing integrated PA/GA shall provide no single point of failure for broadcasting PA/GA in cabins and public areas
- The system shall remain viable and be able to complete calls when part of the network infrastructure is down
- Star cabling network from the main ACM rack shall be standard delivery
- An IP station providing PA/GA coverage in the cabin with SPA-V2 system shall be used as backup

## 5.6 Cabling Infrastructure

The data network cabling infrastructure depends on the services that the network is supposed to provide. There are two main types of cabling infrastructures, namely networks with or without core switches.

A network that includes servers running a set of services (e.g. file server) should have both a core switch and a set of workgroup switches. For the difference between a core switch and a workgroup switch, see Appendix A.

Figure 10 shows a network with a core switch and several workgroup switches with STP/RSTP support. This is to ensure that a single point of failure will only bring down a part of the network. The other part of the network will still be functioning normally.

In the given example, some signal paths/links are blocked in order to prevent loops in the network. If a link is broken, or a switch goes down, some loops will cease to exist. The switches will detect this, and some of the blocked links will be opened. In this way, redundant links are provided, hence preventing the whole system from going down due to a single point of failure.

If the data network does not incorporate a core switch, the cabling infrastructure will be as shown in Figure 11. Here, STP/RSTP can also be implemented to eradicate the single point of failure in the data network.

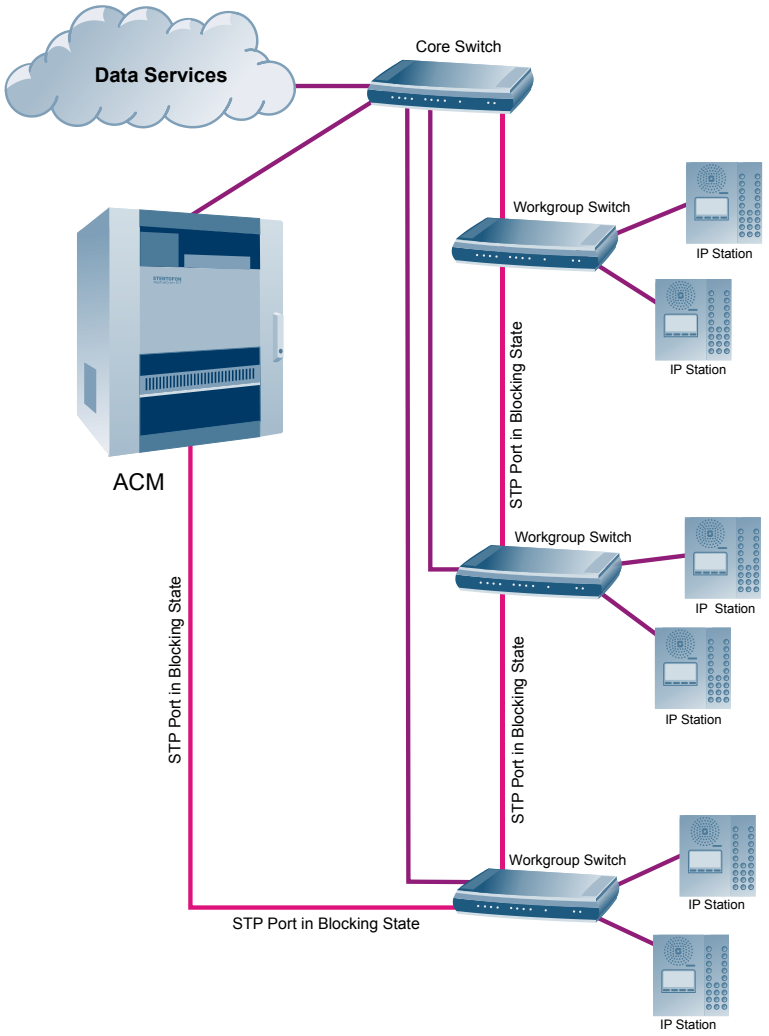



*Figure 11 Cabling Infrastructure with Core Switch*

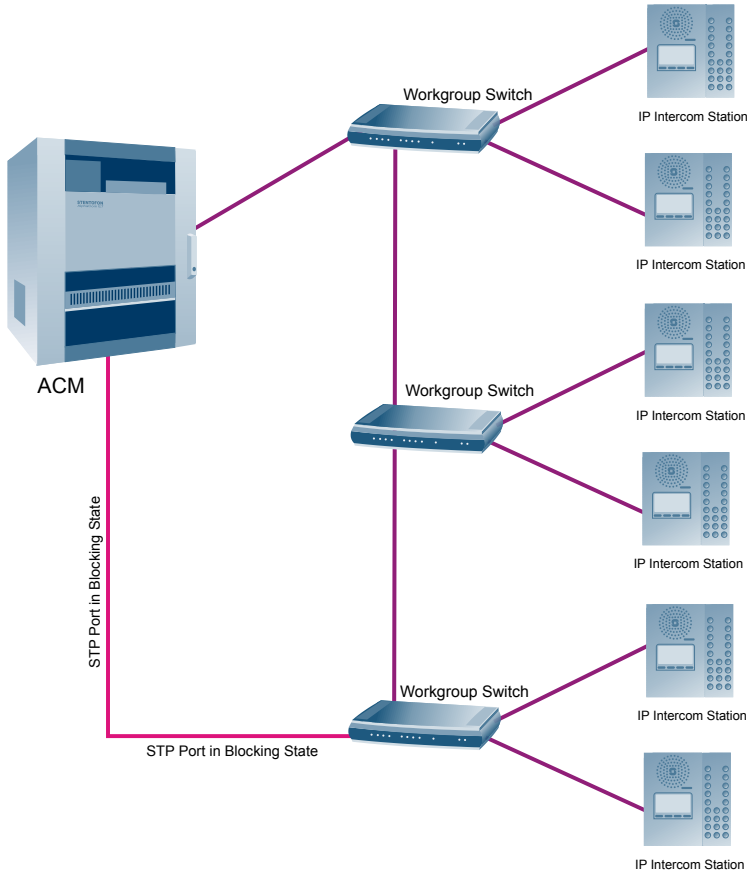



*Figure 12 Cabling Infrastructure without Core Switch*

### 5.6.1 Best practice cabling

When possible, the principle of interleaving should be implemented for cabling on a ship. This means that in addition to providing redundant links through the use of STP/RSTP, adjacent network points throughout a ship should be connected to different workgroup switches. Figure 12 shows how this best practice principle of interleaving has been implemented: IP intercom stations in adjacent cabins are connected to different workgroup switches, while stations in the fore and aft of the bridge are likewise connected to different switches. If one switch goes down, IP intercom stations connected to that switch will be rendered non-functional. But adjacent IP intercom stations will still be functioning normally and be able to provide emergency communication and/or PA/GA in the vicinity of the non-functioning intercom stations.

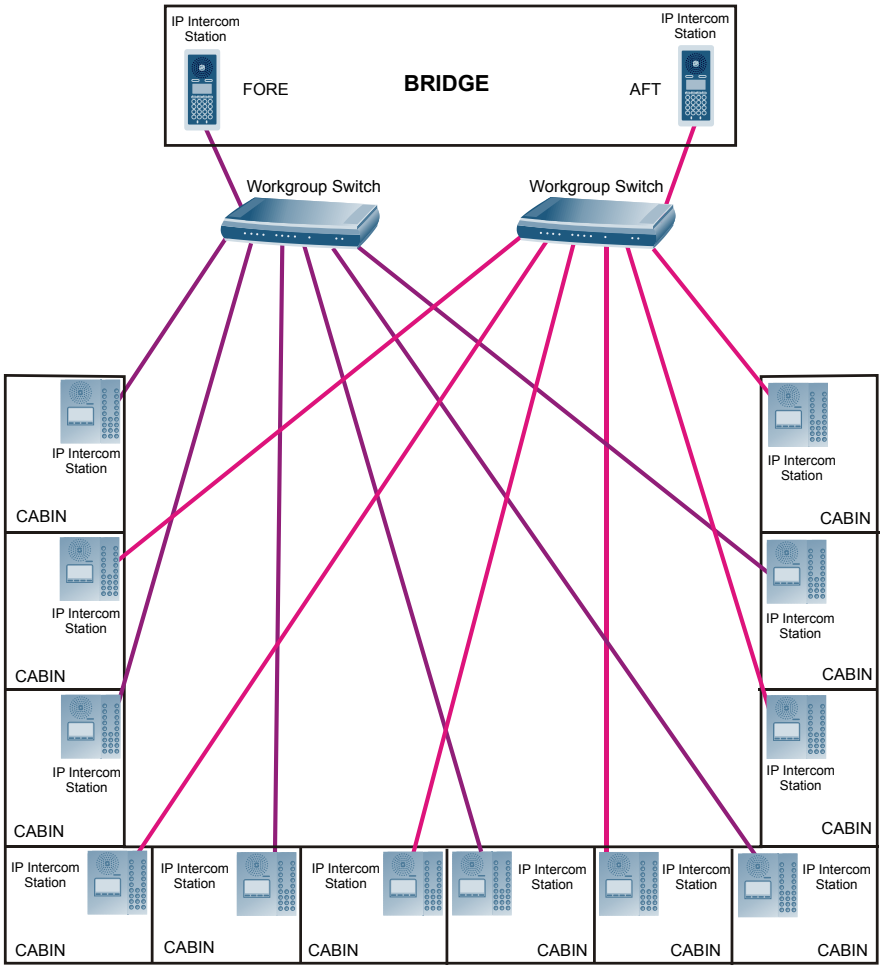



*Figure 13 Cabling with Interleaving*

# A Network Switch Specifications

## A.1 Workgroup Switch Specifications

| Feature | Description | Mandatory | Recommended |
|---|---|---|---|
| **Layer 2** | | | |
| Ports | RJ-45 Connectors for 10BASE-T/100BASE-TX/1000BASE-T | | X |
| Standard IEEE 802.3 | 802.3u (100 Mbps)<br>802.3z (1000 Mbps)<br>802.3ae (Gigabit Ethernet)<br>802.3x flow control | | X |
| Cabling type support | Cat 5e, Cat 6, Cat 7 or better | | X |
| MAC table size | 8K or more | X | |
| **PoE - Power over Ethernet** | | | |
| PoE | Po802.3af PoE (2008) or better if available (IEEE 802.3at). Should support minimum 7.5 W to all ports at same time. Power should be dynamically allocated. | X | |
| Switching capacity | 7.4 Gbps non-blocking or better | X | |
| Standard IEEE 802.3ac | Max. frame size extended to 1522 bytes to allow Q tag | X | |
| Standard IEEE 802.3ad | Link aggregation for parallel links (LACP) | X | |
| **Standard IEEE 802.1Q** | | | |
| VLAN | 802.1Q tag-based and Port based VLAN included management VLAN | X | |
| Port Trunking | Port Trunking support on 2 or more ports | X | |
| **Security** | | | |
| Storm Control | Broadcast and multicast | X | |
| Spanning Tree | IEEE 802.1D Spanning Tree and PortFast | X | |
| **QoS** | | | |
| Priority level | Minimum 3 or more | | X |
| Scheduling | Priority queuing | | X |
| Class of Service | 802.1p VLAN priority based and Port based | | X |

## A.2 Core Switch Specifications

| Feature | Description | Mandatory | Recommended |
|---|---|---|---|
| **Layer 3** | | | |
| IP Routing | Routing between subnets | | X |
| **Layer 2** | | | |
| Ports | RJ-45 Connectors for 10BASE-T/100BASE-TX/1000BASE-T / Fiber optic | X | |
| Standard IEEE 802.3 | 802.3u (100 Mbps)<br>802.3z (1000 Mbps)<br>802.3ae (Gigabit Ethernet)<br>802.3x flow control | X | |
| Cabling type support | Cat 5e, Cat 6, Cat 7 or fiber optic | | X |
| MAC table size | 8K or more | X | |
| **Standard IEEE 802.1Q** | | | |
| VLAN | 802.1Q tag-based and Port based VLAN included management VLAN | X | |
| Port Trunking | Port Trunking support on 2 or more ports | X | |
| **Security** | | | |
| Storm Control | Broadcast and multicast | X | |
| Spanning Tree | IEEE 802.1D Spanning Tree and PortFast | X | |
| **QoS** | | | |
| Priority level | Minimum 3 or more | | X |
| Scheduling | Priority queuing | | X |
| Class of Service | 802.1p VLAN priority based and Port based | | X |

www.vingtor.com

Zenitel Norway AS



support@vingtor.com