HIRSCHMANN
A Belden Company

Redundancy

Content:

- Redundant device design
- Redundant network design
- Availability

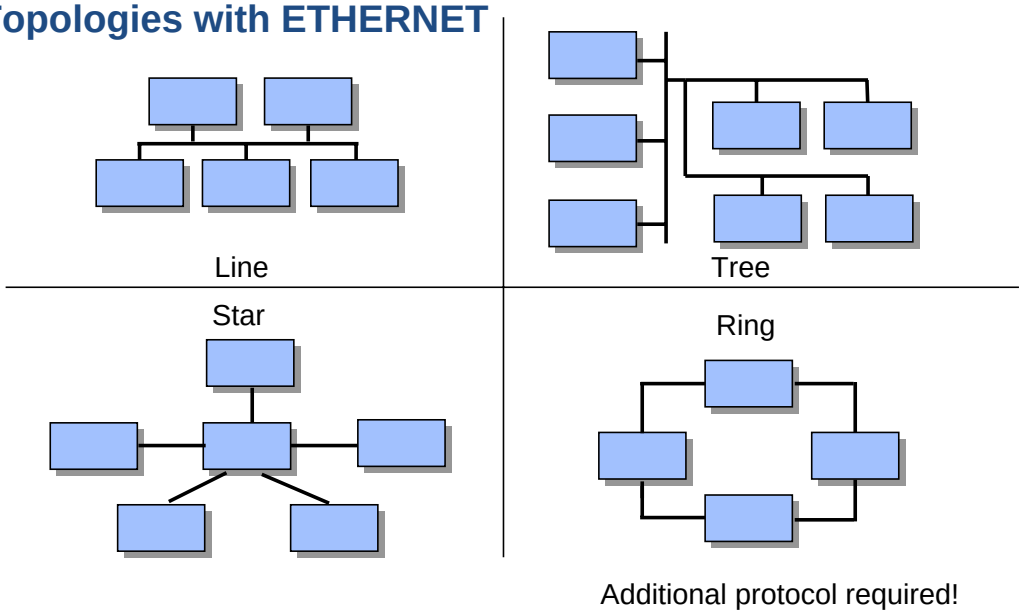
Redundant Device Design

Devices for industrial use
Wherever possible:
- fanless
- External redundant power supply

- Redundant device design is attained by
  - Redundant fans
  - Redundant power supplies and network connections.
  - Passive backplane.
  - Redundant switching engines (redundant switching cores or base boards, redundant management (agents), etc.).
    A failure must be signaled by LEDs, traps, management, OPC interface, etc.(Error management
  - All components should be hot-swappable from the front.
  - For use in industrial production fanless devices with external power supply are advantageous. Power supply units and fans have the lowest MTBF ratings in practice (meaning higher availability!).
  - Often industrial devices feature an “indicator contact”, to signal errors and failures. This is a relay which closes when an error occurs. Signaling is possible by way of a signal lamp, for example, or by evaluation in a controller.
  - The devices should also offer facilities to build redundant structures, applying standardized and proprietary methods at layer 2 and layer 3. The individual methods are dealt with in more detail in the following.
  - Dual connection of terminals likewise increases redundancy

Notes:

Topologies with ETHERNET



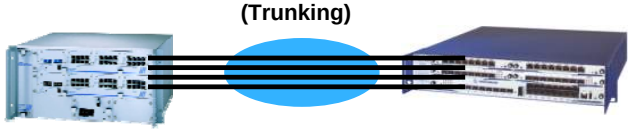
Additional protocol required!

- In general various topologies can be used with Ethernet.
- A ring structure or meshed structure must be implemented using additional protocols (spanning tree,..).
- Why ring structure?
  - Autonomous redundancy mechanisms possible, no central root
  - Fewer expensive ports are required in the central switches and routers
  - Fewer expensive fiber-optic cable to the central component
  - Clear layout
  - Ease of migration to real-time islands
  - Ring structure included in standardization proposals
  - Work groups easier to structure
  - Simple network expansion possible
  - Rings possible despite wide extent

Notes:

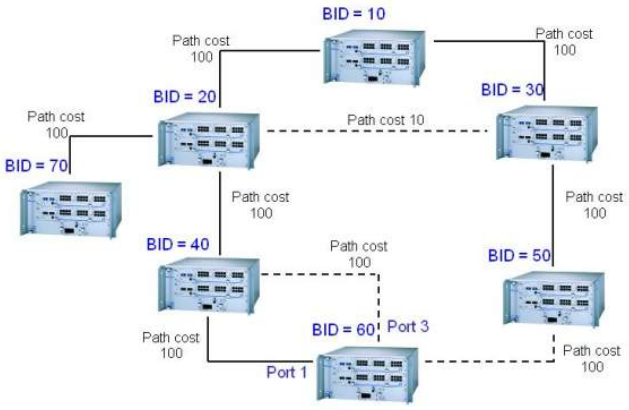
Standard Layer 2 Redundancy

802.3ad
Link Aggregation
(Trunking)



802.1D – RSTP (former 802.1w)

According to IEEE you can use as many trunked ports as possible

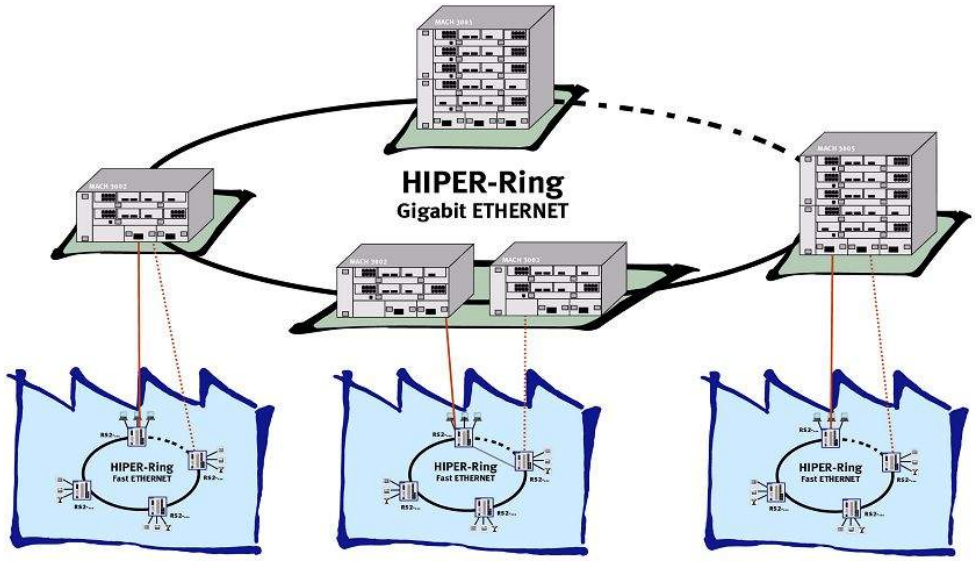


- Ethernet does not permit ring structuring or network meshing. So the standard is supplemented by additional protocols. These may be standardized, such as Rapid Spanning Tree (RSTP), while other protocols, such as the HIPER ring, are proprietary.
- Dual structures can automatically repair an error, and get the network back online. This creates redundancy. Switchovers are signaled by the management, and so can be rectified promptly based on an established maintenance concept.
- RSTP detects and monitors the topology of a network at layer 2 based on timer control. Redundant links are automatically blocked for data traffic. RSTP can be enabled and disabled for each agent or port. Priority, Max Age, Hello Time, Forward Delay can be configured at bridge level, with priority and path cost configured at port level. Important: Without a change to the defaults, the spanning tree domains must not include more than 7 switches, i.e. max. 7 cascaded switches per data path are allowed.
- With RSTP faster switching realizable based on event control, but with the following restrictions according to the standard: Packet doubling permitted, loops permitted, packet sequences can be interchanged, switchover time not defined, in case of communications problems or with downward compatibility SPT time again.
- In link aggregation, multiple physical links (typically 4) form one logical link. The algorithm for distribution of the packets is manufacturer/product dependent. The recovery time is typically < 1 s. The physical links must be FDX and must use the same speed.

Notes:

HIRSCHMANN
A Belden Company

Fast Industrial Standard Layer 2 Redundancy

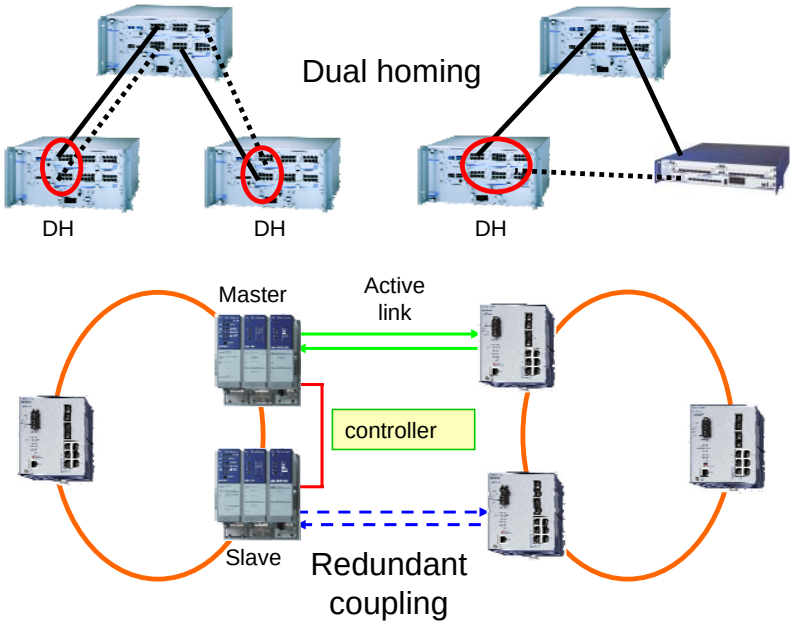


- The HIPER ring is a quasi-industrial standard with following characteristics:
  - Up to 100 switches in one ring. This means different switches (MICE, RS2 and MACH) can be used in the same ring. Various speeds (100/1000 Mbit/s ...) as well as copper and fiber-optic are possible in one ring.
  - Guaranteed redundancy switchover time max. 500ms HIPER ring II in Power MICE max. 50 ms.
  - The protocol used is a simple layer 2 redundancy.
  - Plug and Play, for DIN rail devices also programmable without management by way of DIP switches. During network operation expansion of the ring is possible easily.
  - Distances up to 5000 km total length are possible. The distance between individual switches may be more than 100 km (with special single-mode modules).
  - There is no central control unit (root). In the event of failure of the redundancy manager one line is produced.
  - Tolerable errors: Failure of a cable is completely corrected. The failure of a switch only paralyzes the users connected to it. By means of dual ring structures with node redundancy these errors, too, can be prevented.

Notes:

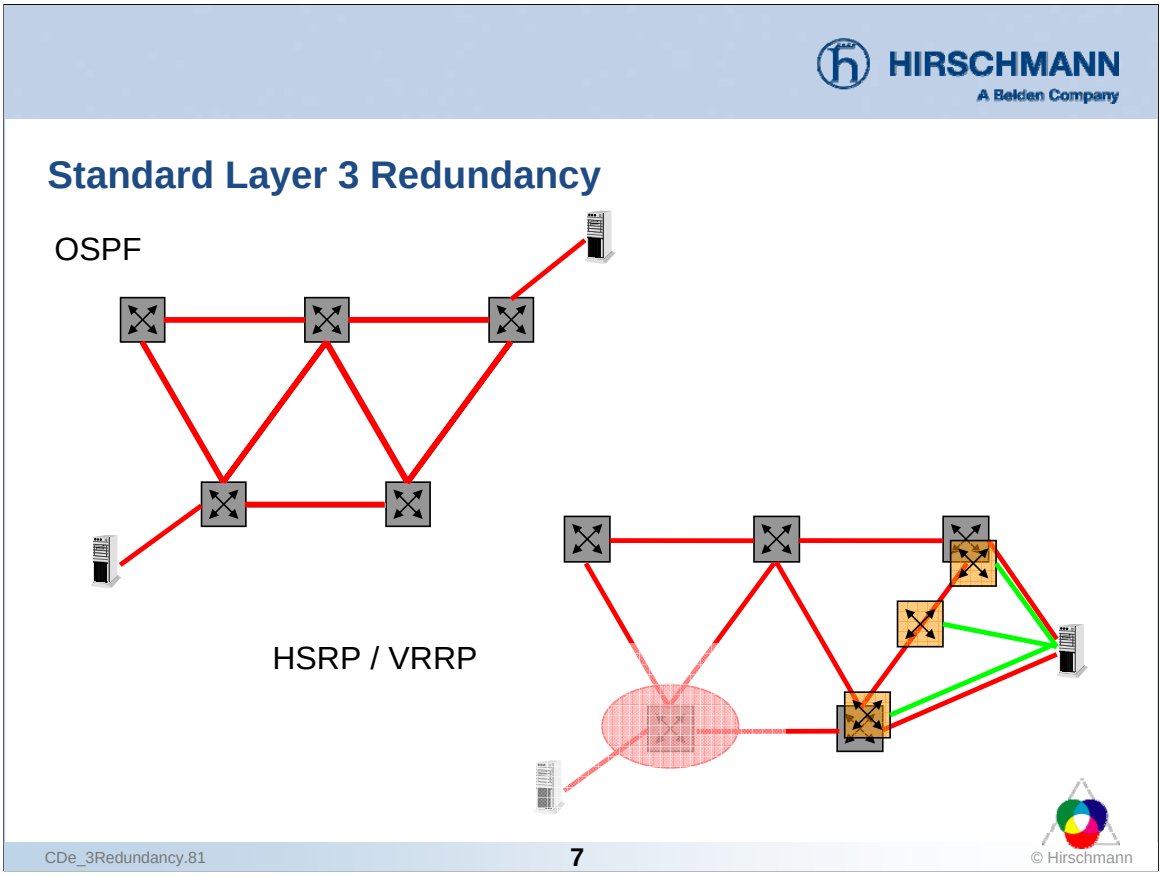
HIRSCHMANN
A Belden Company

Fast Industrial Standard Layer 2 Redundancy



- Dual homing
  - Dual homing is a proprietary redundancy method. A redundant link is used to protect the active link.
  - The switchover in case of error normally occurs in < 1-3 seconds.
  - The active and standby ports can be differently configured (speed/media type). Ports may be on different base boards
  - Error detection is achieved by means of a connection test with Link Status or L2 packets.
  - The two links in the dual homing pair can redundantly link one switch or two switches.
- Redundant ring coupling
  - Redundant ring coupling allows two rings to be coupled with redundancy for example. It is also possible to link old hub segments with the redundant ring coupling.
  - The switchover in case of error normally occurs in < 1-3 seconds.
  - A control line between two devices is provided for redundant coupling. By way of the expanded redundancy with L2 packets this control line can be omitted. Then the communication between the master and the slave takes place over the existing HIPER ring. This means the ring coupling can be used even where there are long distances between the master and slave. When using the control line, delivering shorting switchover times in case of error (< 1 sec.), appropriate MICE modules must be selected.

Notes:



- Router Information Protocol (RIP V1, RIP V2)
  - For networks with a small number of routers, maximum 14 hops.
  - Quick to set up, slow to change the topology.
  - All routers send cyclic information, resulting in a large overhead from routing updates around every 30 seconds.
- Open Shortest Path First (OSPF)
  - For networks with a large number of routers, greater configuration complexity than for RIP.
  - Slow to setup, quick to change the topology.
  - Exchange of information with LSA (Link State Advertisement packets).
  - Classification of routers into backbone routers, area border routers (ABR) and autonomy system border routers (ASBR) at the border to the Internet. Administration is primarily limited to the respective area.
  - Meshing with OSPF permits load sharing and automatic route selection, including in case of error.
- HSRP Hot Standby Routing Protocol (Cisco)
- VRRP Virtual Router Redundancy Protocol
  - Routers work in standby mode
  - Routers send HSRP status packets
  - Router have identical virtual MAC/IP addresses
  - VRRP: No significant difference to HSRP
  - Reconfiguration time about 3-4 sec.

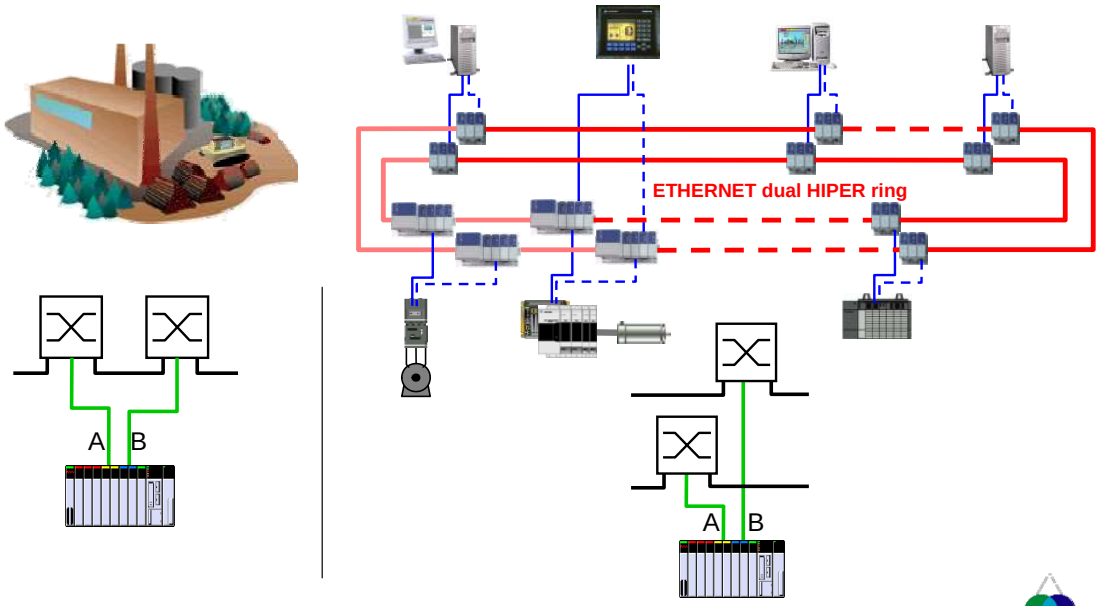
Notes:

Exercise: Increase the Redundancy of your Network

- How can you increase the redundancy of your network from the previous exercise?
- Choose whether to use layer 2 or layer 3 redundancy methods.
- Do you want to use standardized or proprietary protocols for redundancy?
- Add to your drawing from the previous exercise.
- Briefly present the result and explain the reasons for using the chosen protocol.

Notes:

Node Redundancy and Dual Ring Structure



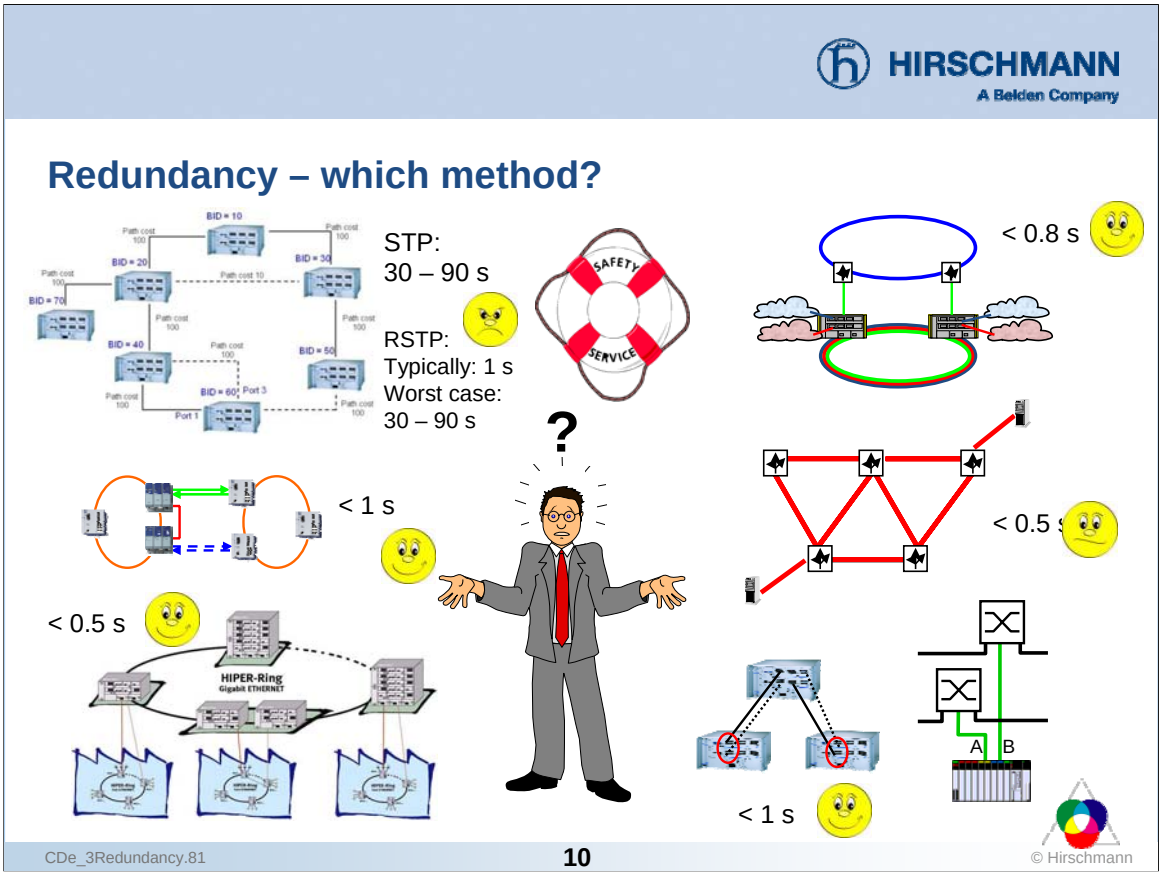
Note: The terminal redundancy must be supported by the terminal software

- To obtain even higher levels of redundancy, the entire application must be of redundant design. For this it is essential also to use redundant terminal units. These may be devices with redundant network cards (NICs), or in extreme cases even hot-standby devices (especially controllers).

- These redundant devices should then also be connected to different network devices, e.g. switches. This can be done, firstly, be connecting each terminal unit at one port to two different switches in the same network (line, meshed network, ring, etc.). High-availability networks are often also constructed from two separate networks however. In this, one port on each of the redundant terminal connections is connected to a switch in each of the two networks. No link is normally needed between the two networks. In the event of an error the terminal signals on the redundant port to all other devices that with immediate effect communication must be routed over the secondary network.

- The monitoring and switchover of the redundant device connections must generally be handled by the software in the terminal unit.

Notes:

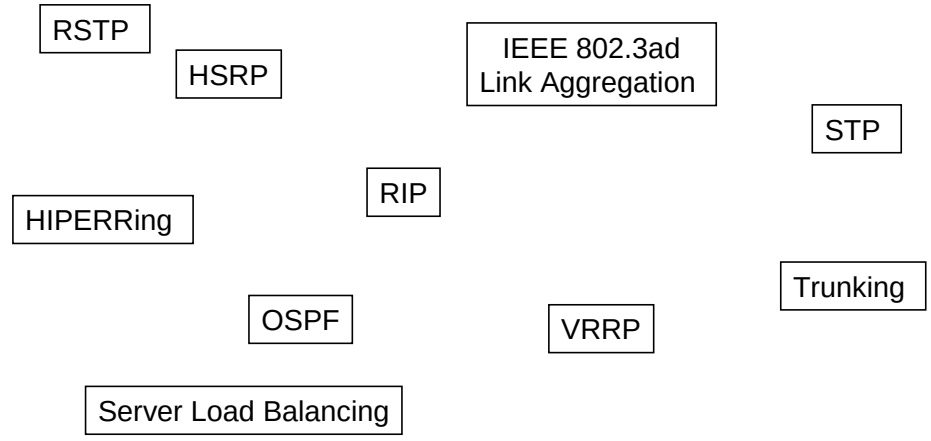


- A high-availability network must be structured with no single point of failure, i.e. completely redundant
- Redundancy is also necessary for:
  - Device design (network components, fans, passive backplane,...)
  - Network design (redundant links, various cable ducts,...)
  - Double connection of terminal units, ...
- The choice of redundancy method depends firstly on whether a layer 2 or layer 3 network is being constructed. As a general rule: The network should be designed to be as simple as possible. Wherever possible, remain at layer 2. This is not always possible, especially in large networks, and subnets have to be constructed.
- The choice of redundancy method then also depends ultimately on whether standardized protocols are to be used, or whether there is a wish to utilize the benefits of proprietary protocols, which often offer shorter and guaranteed reconfiguration times.
- In some cases the choice is also determined by the application, which might shut down the network if reconfiguration times are too long. As a general rule, new applications in production departments are often more critical in this respect than old-established office applications, in which users are merely not able to access the server for a short time when an error occurs. In the production environment there is often very precise data underlying a production outage.

Notes:

Exercise: Redundancies

- Assign the following terms to logically related groups of Layer 2, 3 or higher.

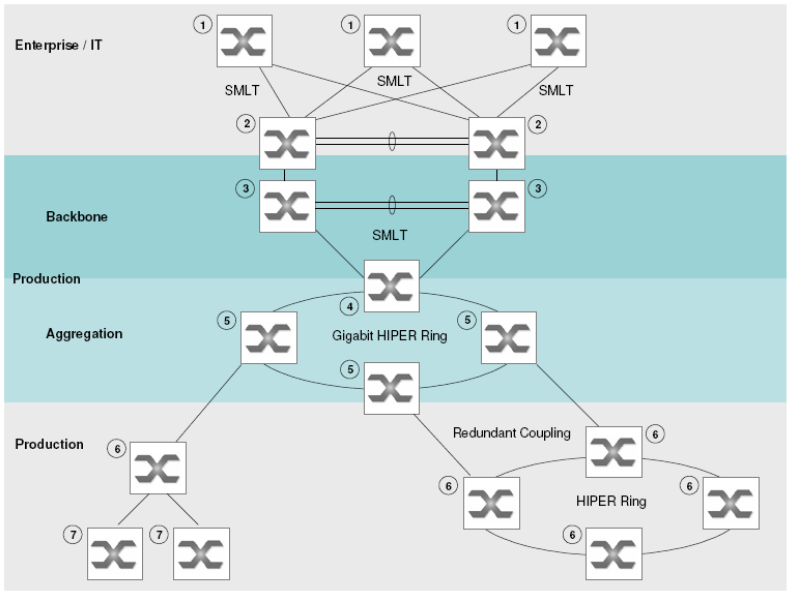


- Assign the following terms to logically related groups.

Notes:

Solution:
L2: STP, RSTP, Link Aggregation, Trunking
L3: RIP, OSPF, HSRP, VRRP
>L3: Server Load Balancing

Application on Layer 2



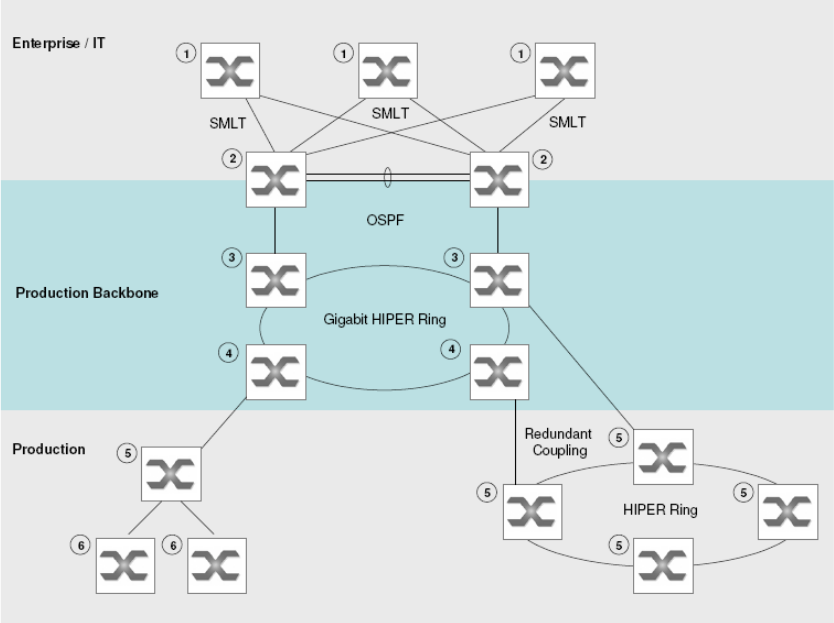
Notes:

Application on Layer 2

No	Type of Product	Vendor	Product/Note
1	Switch	Nortel	ES 460/470 Stack, ERS 2500 Stack, ERS 4500 Stack, ERS 5500 Stack
2	Switch	Nortel	Core Switch ERS 8600
3	Switch	Nortel	Routing Switch ERS 5500, ERS 8300
4	Switch	Hirschmann	MACH4002, MAR10xx, RS30, MS30 with SW L2P (Layer 2 Professional)
5	Switch	Hirschmann	MACH4002, MAR10xx, RS30, MS30 with SW L2E or L2P (Layer 2 Enhanced or Professional)
6	Switch	Hirschmann	RS20, MS20, OCTOPUS with SW L2E or L2P
7	Switch	Hirschmann	RS20 with SW L2B (Layer 2 Basic), SPIDER

Notes:

Application on Layer 3 (I)



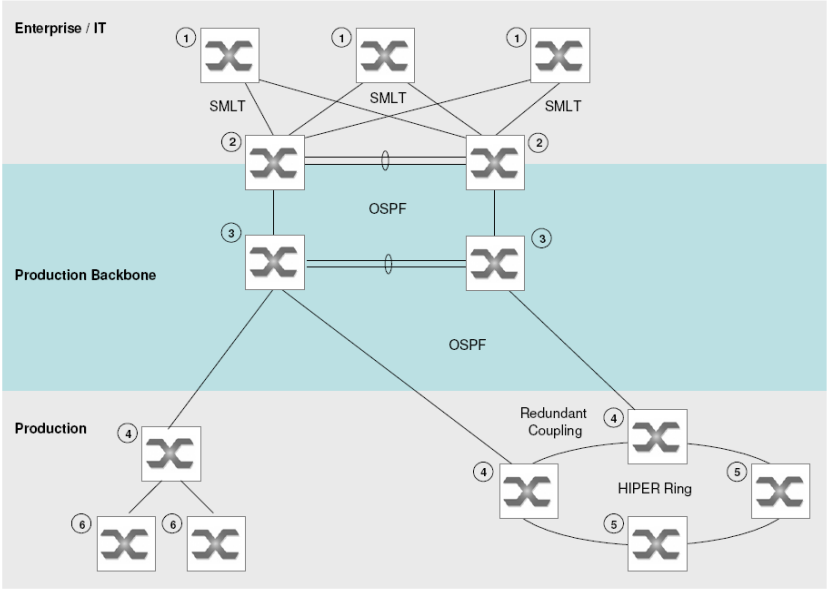
Notes:

Application on Layer 3 (I)

No	Type of Product	Vendor	Product/Note
1	Switch	Nortel	ES 460/470 Stack, ERS 2500 Stack, ERS 4500 Stack, ERS 5500 Stack
2	Switch	Nortel	ERS 5500, ERS 8300, ERS8600
3	Switch	Hirschmann	with SW L3P (Layer 3 Professional) e.g. MACH4002, MS4128
4	Switch	Hirschmann	MACH4002, MAR10xx, RS30, MS30 with SW L2E or L2P (Layer 2 Enhanced or Professional)
5	Switch	Hirschmann	RS20, MS20, OCTOPUS with SW L2E or L2P
6	Switch	Hirschmann	RS20 with SW L2B (Layer 2 Basic), SPIDER

Notes:

Application on Layer 3 (II)



Notes:

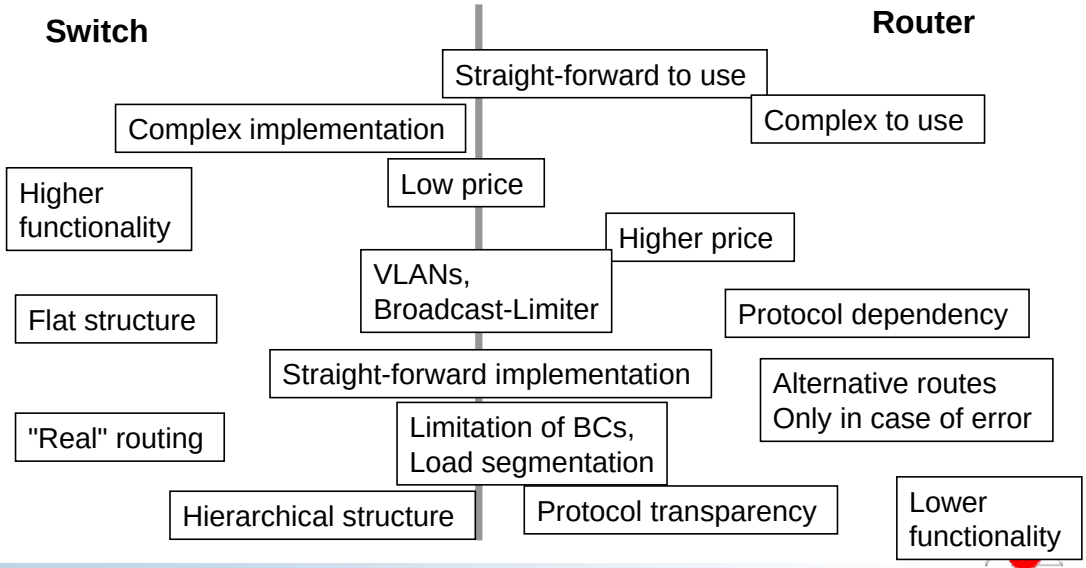
Application on Layer 3 (II)

No	Type of Product	Vendor	Product/Note
1	Switch	Nortel	ES 460/470 Stack, ERS 2500 Stack, ERS 4500 Stack, ERS 5500 Stack
2	Switch	Nortel	ERS 5500, ERS 8300, ERS 8600
3	Switch	Nortel	ERS 5500, ERS 8300, ERS 8600
4	Switch	Hirschmann	MACH4002, MAR10xx, MS4128 with SW L3P (Layer 3 Professional)
5	Switch	Hirschmann	MACH4002, MAR10xx, RS30, MS30 with SW L2E or L2P (Layer 3 Enhanced or Professional)
6	Switch	Hirschmann	RS20 with SW L2B (Layer 2 Basic), SPIDER

Notes:

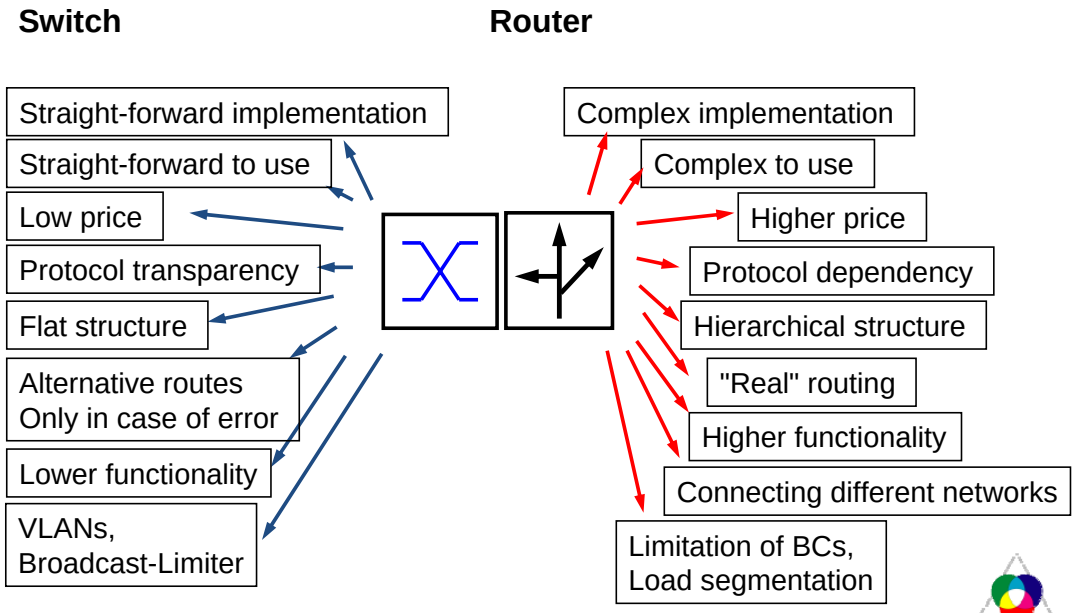
Exercise: Comparison Router/Switch

- Assign the following terms to Switches (S) and Routers (R)



Notes:

Solution: Comparison Router/Switch



- Switch
  - OSI layer 2
  - Coupling of networks with same technology
  - Independent of transport protocol
  - Separates networks physically, not logically
  - Load separation by MAC addresses
  - Create collision domains
  - Low delays
  - Links fixed, static
- Switch with routing function
  - Function like switch, additionally ...
  - Coupling different network technologies, e.g. Ethernet/FDDI
  - Routing of a protocol, e.g. IP
- Router
  - OSI layer 3
  - Coupling of different network technologies
  - Dependent on transport protocols
  - Separates networks physically and logically
  - Load separation by network addresses
  - Formation of broadcast domains
  - Large delays
  - Dynamic path selection
  - Optimum bandwidth use possible
  - Reduced transmission charges in WAN (LAN/ISDN router)

Notes:

Availability

Notes:

HIRSCHMANN
A Belden Company

MTBF Times - a Measure of Fail-safety

Telecordia

MIL-HDBK-217F

Definition according to MIL-HDBK-217F:

$$MTBF = \frac{1}{FR1 + FR2 + FR3 + FR4} \qquad FRn \text{ (Failure rate)}$$

Examples:

- RS2-3TX/2FX = 585,023 h = 66.8 years
- RS2-TX/TX = 204,108 h = 23.2 years
- PC motherboard = 50,000 h = 5.7 years.

- Fail-safety is specified in MTBF times (Mean Time Between Failure). This means that after this time, statistically a fault can occur in the device. Calculation of the MTBF estimate is based on MIL-HDBK-217F; Parts Stress
  Reliability Prediction.
  This is a calculation incorporating the failure rates of all parts of a device. As the calculation is performed by way of the reciprocal, the component with the shortest life expectancy (highest failure rate) thus determines the MTBF time of the overall device. Moving parts subject to wear therefore have the shortest times. This means that being fanless has a positive effect on the MTBF time of a device. Non-redundant network components likewise shorten the MTBF time. It is thus also advantageous in this respect to be able to use an external redundant power supply. As a result, the usually quite high failure rates of power supply units are likewise not included in the MTBF figure.

- Sometimes other methods, such as Telecordia or statistical return calculations, are used to determine MTBF. Such methods also deliver higher MTBF figures, which are not always realistic and so should be treated with caution.

- The operating temperature also plays a role in calculating based on the MIL standard. Usually a figure of 25°C is specified. At higher temperatures the MTBF times decrease.

Notes:

HIRSCHMANN
A Belden Company

Calculation of Product Availability

Product availability = (device life - downtime) / device life

Downtime = fault rectification + software updates during the life of the device

Example:

- Device life = 5 years = 43,800 hrs.
- Downtime = 5 software updates (5 min. for each),
  5 failures (M min. for each),
  1 device replacement (2 hrs.)

Product availability = **(43,800 - 2.5) / (43,800)** = 99.994 %

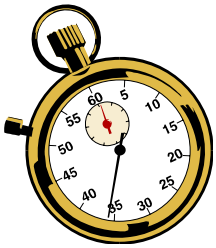
- The overall product availability (not specifying the time of failure) as a percentage is calculated using the formula shown on the slide.
- The device life is the time for which the device is in use. It differs from the MTBF time of a device. Usually the device life depends on the time for which a system is used before it is replaced by a newer system. In our example here we are assuming 5 years. In fact, in industrial systems, such as in the process industry, 10 or 20 years are no rarity. In this there are also on occasions problems with spares procurement. No wonder, considering the lives of PC components.
- The downtime also needs to be calculated, though in most cases it can only be assumed. The downtime consists of the time needed to restore functionality in the event of failure of the product. For systems requiring high availability, this can be effected by means of spare parts. In such cases the time for a replacement needs to be calculated. In other cases a reboot or configuration change by the management system may be enough to rectify the error. Software updates over the course of the device life also need to be taken into account. In making the calculation, assumptions were also made which can doubtless improve experience with specific system in practice. Even a complete replacement of the device (spare parts!) was included, estimated at 2 hours. This time may quite possibly be extended for complex devices (in order to restore the configuration!).

Notes:

HIRSCHMANN
A Belden Company

Calculation of Fault-free Operation

Fault-free operation in 5 years = e - (Period in hours / MTBF)



Example:

- MTBF time RS2-3TX/2FX = 585,023 h = 66.8 years
- 5 years = 43,800 h
- 43,800 / 585,023 = 0.07487
- Fault-free operation in 5 years = e **- 0.07487** = 0.9279 (92.79 %

- The probability of fault-free operation over a specific device life is calculated,
- specifying a given period. It makes good sense, here too, to apply the device life determined by the life of the system (application). This has already been described.
- The MTBF time is also necessary to calculate the period of fault-free operation. It is calculated or specified by the device manufacturer. The possibilities for this have likewise already been described previously.
- Then, using the e-function, the fault-free operation over a given period can be determined based on the formula shown on the slide.
- What the value obtained here ultimately says is:
  The probability that the device will still be functioning after a period of 5 years is 92.79%.
- Or: 92.79% of all devices will still be functioning after 5 years.
- This figure can be used to determine the quantity of spare parts needing to be held in stock for the system over its complete lifetime. This can be of great benefit especially in respect of systems operated in countries where import or export controls are in place. In our example that means that in concrete terms a figure of 10% for the quantity of spare parts would be a safe choice.

Notes:

HIRSCHMANN
A Belden Company

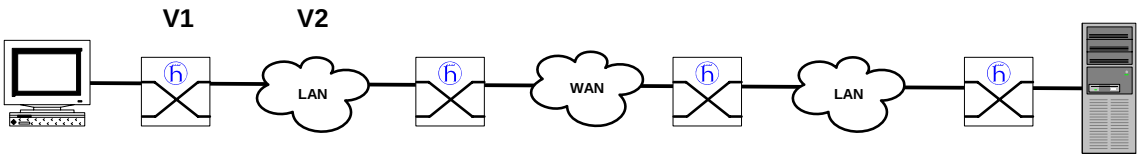
Availability and Failure Duration

Architecture	Availability	Typical failure duration	Downtime per year
Interruption-free	100%	No	No
Fault tolerant	999999%	Clock cycles	0.5 minutes
Failover (cluster)	99999%	Seconds	5 minutes
Fault resilient	99,99%	Seconds / minutes	Max. 53 minutes
High availability	99,90%	Minutes	Max. 8.7 hours
Standard 1	99,50%	Minutes to hours	2 days
Standard 2	99%	Hours	3.5 days

- The network availability is determined not only by the active network components used, it must be based on all the components in an application
- The availability of systems is often expressed for the various architectures (network designs) as a percentage. These percentages can then be converted into days, hours and seconds for which a network may be unavailable. A distinction is made in this between:
  - The sum total failure duration over a time span (e.g. 5 hours in a year)
  - Duration of the failure (e.g. 1 hour)
  - Example: It may be possible to tolerate one network failure of 5 hours in one year, but not 5 network failures of 1 hour each.
- Redundancy is also necessary for:
  Device design (power supplies, fans, passive backplane,...), network design (redundant paths, different cable ducts,...), double connection of the terminal devices,..
- Paths without redundancy are jeopardized by distributed statistical failures of all elements involved (user error, cable error, patchfields, active components,...)
- Depending on the redundancy method applied, an architecture can no longer be classified as "error tolerant" when using STP, for example, because in the worst case it may also involve reconfiguration times of 30-90 seconds.
- "Actual" network availability can only be determined with software tools as "end-to-end availability".

Notes:

Availability based on a Line Structure



0.99 x 0.99 x 0.99 x 0.99 x 0.99 x 0.99 x 0.99 x 0.99 x 0.99

= 0,9135

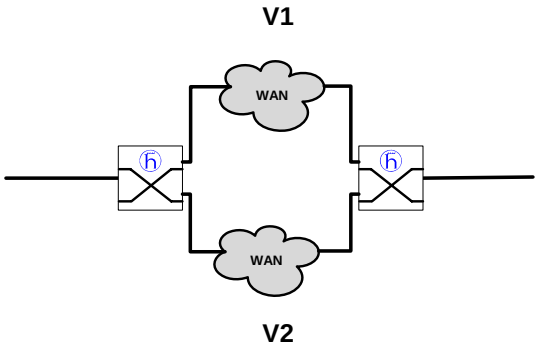
Calculation of the availability of a line *(VL)* :

***VL* = V1 x V2 x V3 x V4 .....**

- The availability of a system is calculated by multiplying together the availability of the components, if they are configured in-line.
- Multiplying together the availabilities of the individual components thus reduces the availability of the overall system as each component is added. As it can usually be assumed that no component has 100% availability, the system availability deteriorates with each component added.
  Analyzing such a structure comprising 9 in-line components, with individual component availabilities of 99%, the availability of the overall system is an alarmingly poor 91.35%. This would mean that our overall system would be available on only 333.43 days in the year - a total downtime of some 31.57 days.
- Another factor to consider in this respect is that terminal units and other devices always run with firmware. It, too, is subject to error, and needs to be included in the product availability calculation and thus also in the calculation of system availability.
- In the following consideration is given to what possibilities exist for increasing system availability. Generally a system always comprises a very large number of individual systems and components. There is therefore no point in considering the availability of an individual component - the overall system must always be analyzed.

Notes:

Availability of a Parallel Structure (Redundancy)



Calculation of availability of a parallel structure *(VP)* :

$$V_P = 1 - \left(1 - V_E\right)^n$$

***VP* = 1 - ((1-V1) x (1-V2) x .....)**

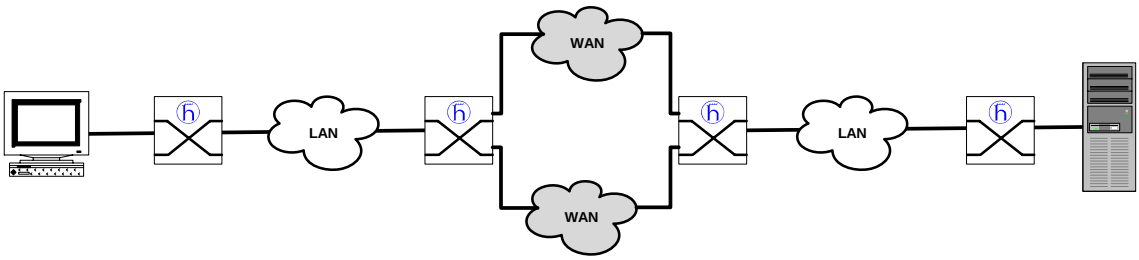
- What can we do to increase availability? How can we obtain a higher availability of the overall system based on the same components.
- The solution is extremely simple, and is termed "parallel structures". More precisely, it involves the use of redundant systems and components.
- The formula shown on the slide calculates the availability of a system, a component with parallel structures, i.e. redundancies, which increase availability. The calculation shows that it very rapidly becomes more and more involved and expensive to keep on increasing availability.
- It should usually be sufficient to configure a system with a single level of redundancy. It should be considered in this that it is highly effective to have dual availability of a component, because a configuration of individual components does not always deliver the desired effect. You may then have redundant network connections, but what about the software (firmware) controlling the whole thing?!
- Redundant systems (also links, lines between two devices) can (with appropriate monitoring by network management systems and immediate repair in case of error) be rated at 100% availability. If calculations are possible, this can also be determined precisely of course.
- Another aspect ultimately to be considered is that with redundant systems and components the switchover times, which in some redundancy methods should not be neglected, also need to be factored in.

Notes:

HIRSCHMANN
A Belden Company

Increase Availability by Means of Parallel Structures

Line and parallel structure:



0.99 x 0.99 x 0.99 x 0.99 x $1-(1-0{,}99)^2$ **x 0.99 x 0.99 x 0.99 x 0.99 x 0.99**

0,9999

= 0,9226

- The availability of a system can be increased by means of parallel structures of the individual components.
- The example demonstrates that in a line comprising 9 components just one parallel structure in a component increases the availability of the overall system by 0.0091%, in effect representing 3.32 days' more availability. Thus, with more parallel structures the overall system can be brought up to the desired level of availability.
  The precondition for this is of course a certain level of product availability, which requires single products and components of appropriate quality.
- Summary:
  A high-availability network must be structured without a single point of failure, i.e. completely redundant

Notes: