

ODVA
2007

CIP Networks Conference
and 12th Annual Meeting

Areas for Redundancy in EtherNet/IP Systems with focus on the Ethernet Networks

Dominic Iadonisi
Ruggedcom Inc.

Technical Track

www.odva.org

Definitions

The definition of Reliability, according to Webster's is:

noun

- ▶ the quality of being dependable or reliable [syn: dependability]
- ▶ the extent to which an experiment, test, or measuring procedure yields the same results on repeated trials

The definition of Redundancy (in relation to electronics and systems), according to Webster's is:

- ▶ Duplication or repetition of elements in electronic equipment to provide alternative functional channels in case of failure.
- ▶ Repetition of parts or all of a message to circumvent transmission errors.

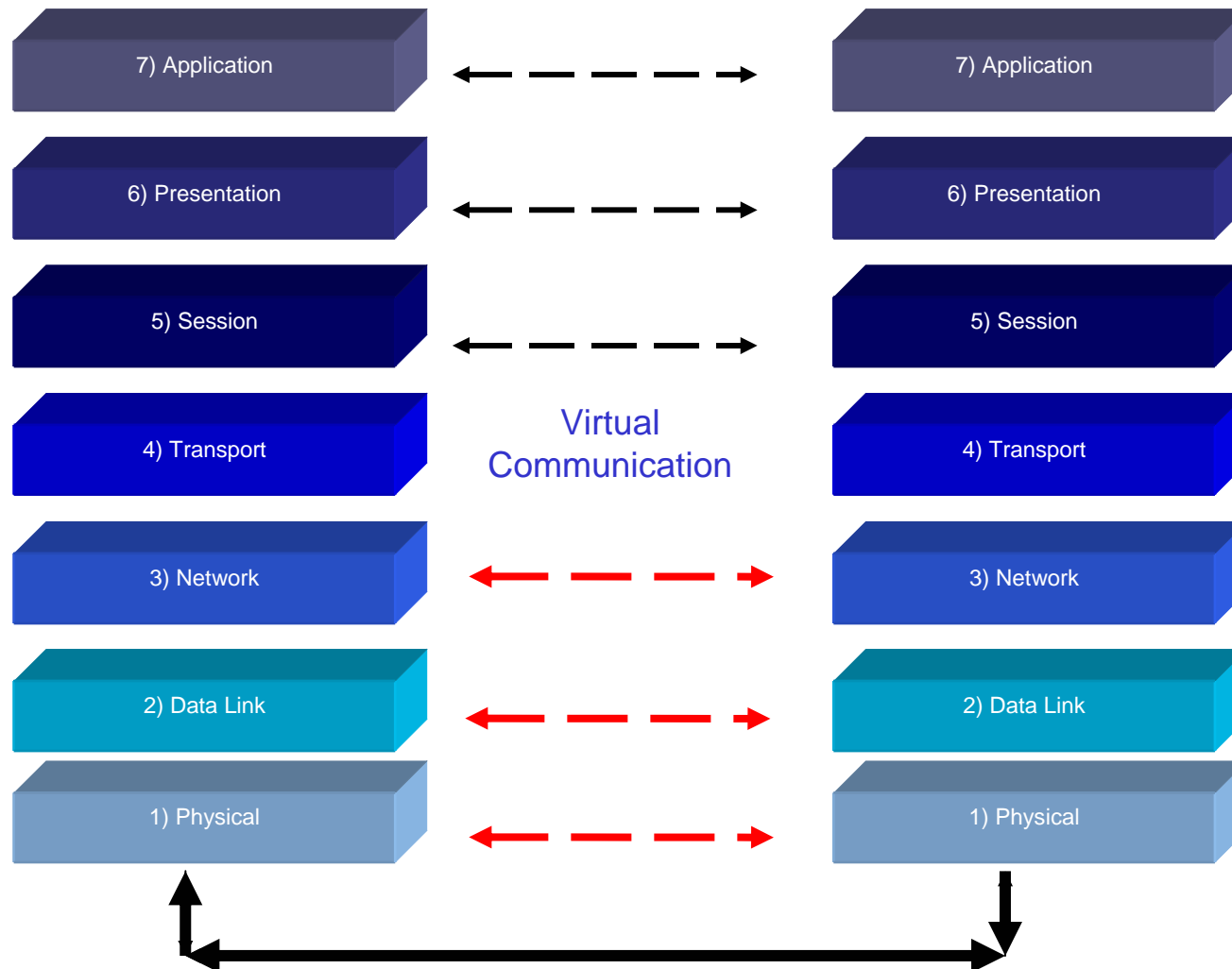
The entire system, from edge devices to the network and communications should be held to the same set of standards for optimum uptime and supportability.

- ▶ Industrial System Reliability covers multiple areas-
- ▶ Robustness of the Application
- ▶ Handling Environmental Stresses
- ▶ Data handling and path redundancy
- ▶ Data integrity

Environment Comparison

	Enterprise	Industrial
Installation	<ul style="list-style-type: none"> ▪Fixed basic installation in the building ▪Typically use RJ45 connectors kept “in the clear” ▪Network is normally centrally located in wiring closets 	<ul style="list-style-type: none"> ▪Plant dependent cabling and cable ducting ▪Field attachable connectors with ratings up to IP67 ▪Network is distributed throughout the plant in panels and small cabinets
Data	<ul style="list-style-type: none"> ▪Medium to Large data packets ▪Medium to high network availability ▪Predominantly acyclic transmission-file downloads, printing, Internet, etc. ▪Real-time behavior not necessary 	<ul style="list-style-type: none"> ▪Small data packets ▪Very high network availability ▪Predominantly cyclic transmission-know data rate with programmed request/reply intervals ▪Real-time behaviour necessary, especially where coordinated motion is used (IEEE 1588)
Environment	<ul style="list-style-type: none"> ▪Normal temperature range ▪Little dust, moisture and vibration ▪Hardly any mechanical loads or problems with chemicals ▪Low EMI/RFI/EMC Requirements 	<ul style="list-style-type: none"> ▪Extended temperature ranges- very low to very high ▪Dust, moisture and vibration likely ▪Risk of mechanical damage or problems with chemicals in hazardous environments ▪High EMI/RFI/EMC requirements

OSI Communications Model

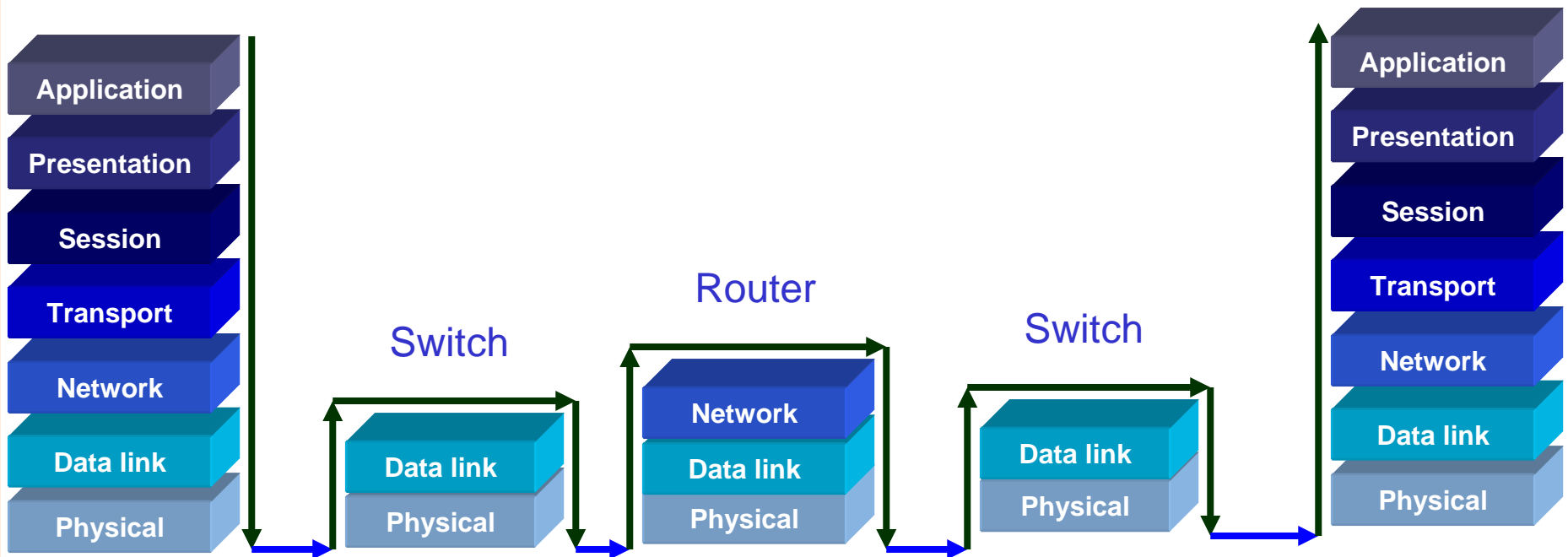


Example of the OSI model at work...

PC
192.168.1.10

Router Interfaces
192.168.1.x- 192.168.2.x

PC
192.168.2.10





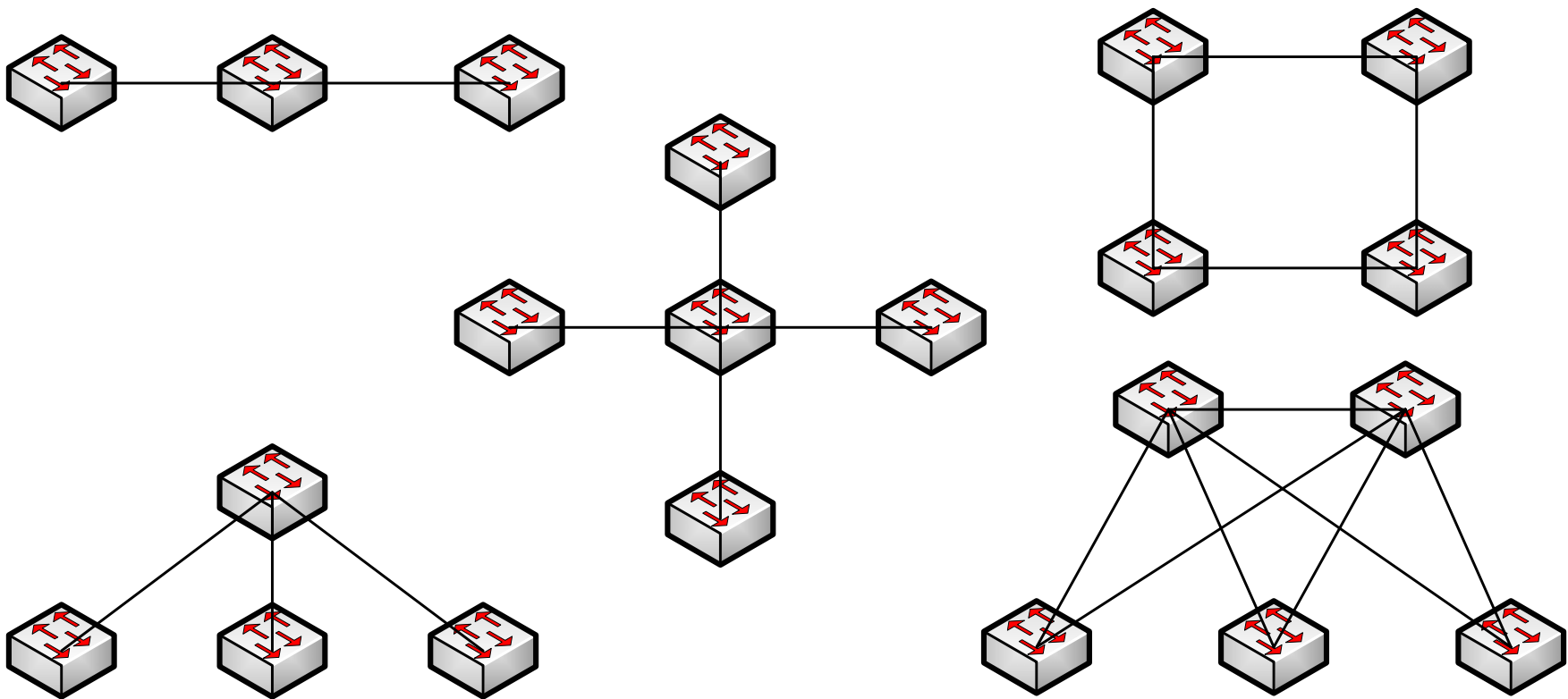
Physical Redundancy- OSI LAYER 1

Physical Redundancy

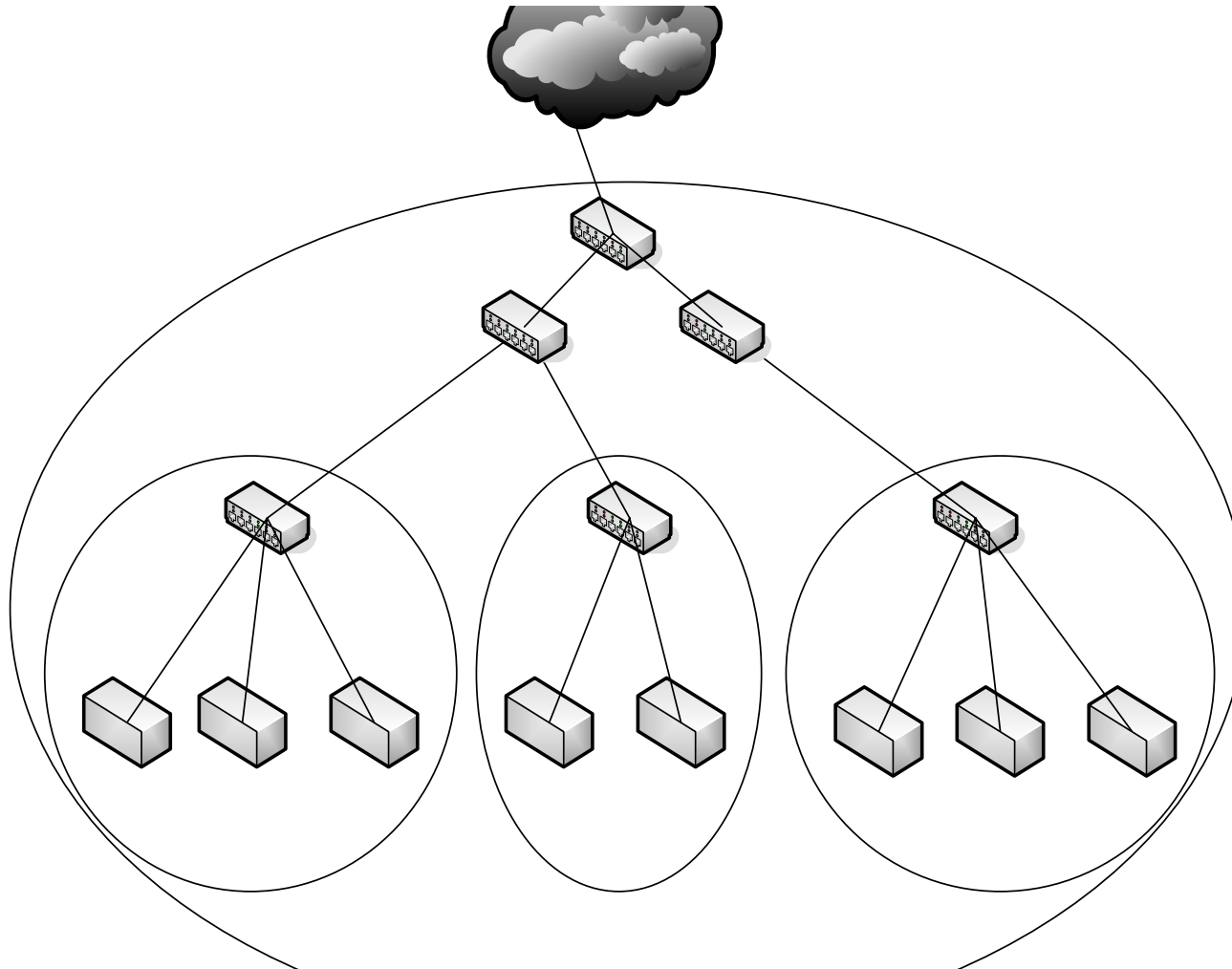
Physical redundancy covers the physical Ethernet network connections (and Ethernet equipment) AND the physical hardware the connections go between. Network redundancy focuses upon the multiple routes that can be used between edge devices. The more available routes edge to edge, the more failures the network can sustain and still keep the process alive and functioning. Physical redundancy normally follows two scenarios:

- ▶ **Diverse routing of cabling-** if a cable tray or conduit is damaged in some way cutting link on the cabling in it, there is another way to get where you need to by providing cabling by another route to maintain connection reliability.
- ▶ **Redundant hardware-** having multiple connections on a controller or other hardware allows the controller reliable connectivity in cases where a connection or port has suffered a failure. This also involves having redundant network hardware in case of failures, including multiple power supplies, multiple CPU cards on controllers, etc.

Ethernet Topologies



Common Industrial Network View





Data Link/MAC Redundancy- OSI LAYER 2



Spanning Tree

Spanning Tree is a redundant topology in that it provides network redundancy instead of just path redundancy while preventing loops in a network. For Ethernet to function properly only one active path can exist between devices.

To provide redundancy, Spanning Tree relies on having multiple paths or connections to different switches and configures some of these paths into standby (Blocked) state.

If a network segment becomes unreachable, spanning tree reconfigures and reestablishes link by activating the "Blocked" links.

Standardized

!Designed for Office/Enterprise environments!

Types of Spanning Tree Protocol

Spanning Tree- There are several flavors of Spanning Tree.

- ▶ STP (Spanning Tree Protocol)- Standardized in 1996 as IEEE 802.1D, it is the first and slowest of the Spanning Tree protocols. Average failover time for STP started at 30 seconds and went up. Way too slow for any industrial Process. Next came...
- ▶ RSTP (Rapid Spanning Tree Protocol)- Standardized in 1998 as IEEE 802.1w, it was an evolutionary leap for STP. It is more rapid, with failover times from about 500msec to up to 12 seconds, so it was better than STP. Still an issue with the speed of failover for Industrial processes.
- ▶ MSTP (Multiple Spanning Tree Protocol)- Originally standardized as IEEE 802.1s and then incorporated into IEEE 802.1Q 2003, it allows multiple instances of Spanning Tree Protocol per Virtual LAN. This means that in a single physical network, there can be multiple virtual network groupings, each with their own instance of Spanning Tree Protocol.
- ▶ There are proprietary implementations of Spanning Tree that are optimized for use in Industrial Networks. They are based upon standard RSTP, but are not designated as a standard STP protocol.



Spanning Tree

All switches in the LAN gather information about each other through an exchange of data messages called BPDU's or Bridge Protocol Data Units. The exchange of messages causes the following:

1. The election of a "Root" switch for stability.
2. The election of a designated switch.
3. The removal of loops by placing redundant switch ports in a backup state.

The "Root" switch is considered to be the "logical" center of the Spanning tree network. All paths that are not needed to reach the "Root" switch from anywhere in the network are placed in backup mode.

Spanning Tree

Spanning Tree uses a particular type of data packet to send network information between switches participating in Spanning Tree redundancy.

BPDU's (Bridge Protocol Data Units) contain information about the transmitting switch it came from and it's ports including:

1. Unique switch Identifier or MAC address.
2. Switch priority
3. Port priority
4. Port cost.

Spanning Tree uses this information to elect the "Root" switch and "Root" port for the switched network.

Spanning Tree

The switches send configuration BPDU's to configure the spanning tree topology. All switches connected to the LAN receive the transmitted BPDU. The BPDU's are not forwarded by the switch, but the information contained in the BPDU can be used by the receiving switch to transmit a new BPDU.

The resulting action of this communication is:

- One switch is identified as the Root.
- The shortest distance to the root is determined for each switch.
- A designated switch or switch closest to the Root is selected.
- An active port from each switch is selected and the others are blocking.



Spanning Tree

If all the switches are enabled with default settings, the switch with the lowest MAC address becomes the root by default. However, due to traffic patterns, number of forwarding ports or just simply physical location, this may not be the best switch to be the root.

By increasing the priority (lowering the actual numerical value of the priority number) of the ideal switch so that it becomes the root, you are forcing spanning tree to recalculate and form a new topology.

The same can be said for which port is active and which port stays in standby.

By increasing the priority (lowering the actual numerical value of the priority number) of the ideal port so that it becomes active, you are forcing spanning tree to recalculate and form a new topology.

Spanning Tree

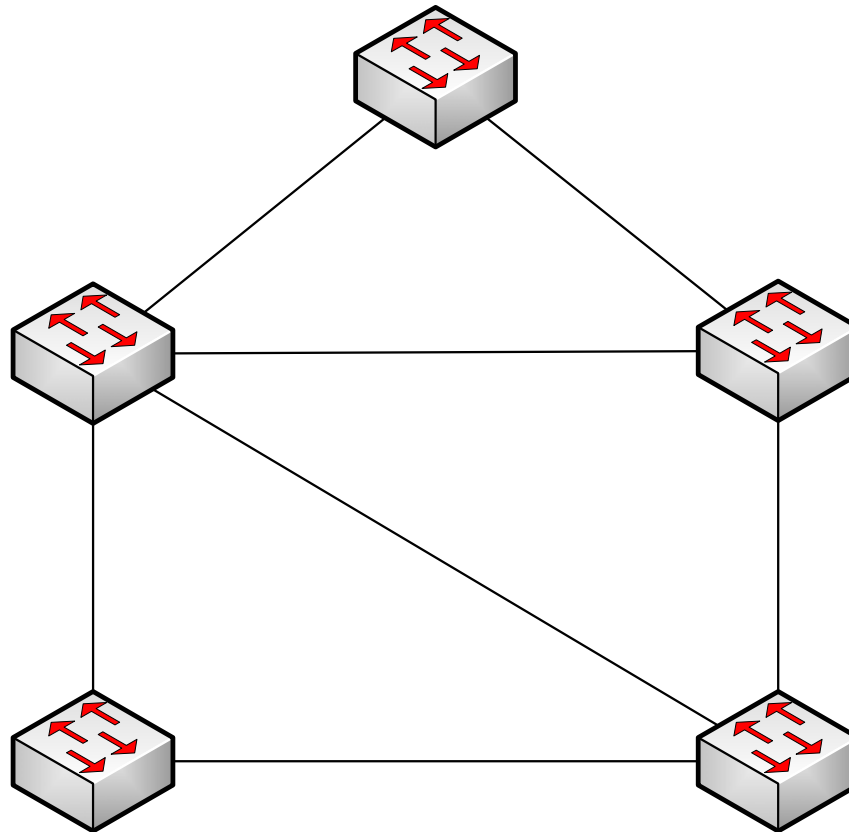
Each port on a switch using spanning tree protocol in one of five states:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

Each port moves through these five states as follows:

- From Initialization to blocking
- From Blocking to Listening or disabled
- From Listening to Learning or to Disabled
- From Learning to Forwarding or to Disabled
- From Forwarding to Disabled

Spanning Tree





Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (IEEE 802.1ad) provides redundancy without the use of Spanning Tree. It enables users to be able to bundle groups of ports between switches to form 1 virtual link with the bandwidth of the member links. LACP provides several functions:

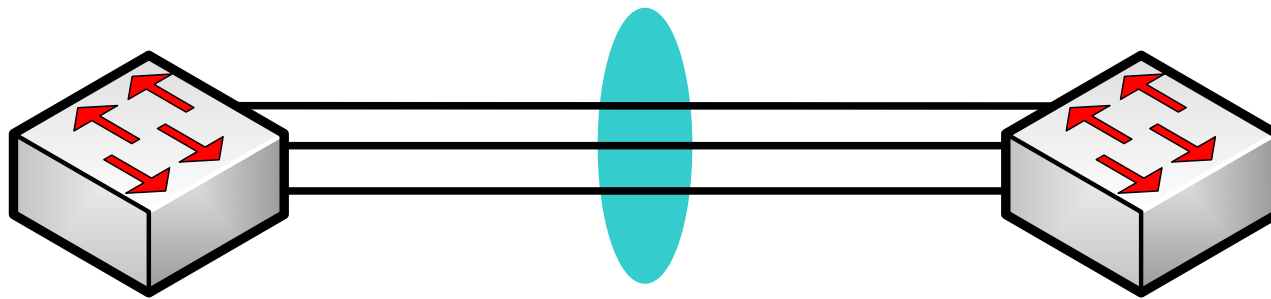
Higher bandwidth

Enhanced Bandwidth Granularity

Load sharing across the member links to balance bandwidth across the member links

Fault tolerance provided by offloading data to working member links when a member link fails

LACP is a method of providing needed extra bandwidth between Ethernet switches that have extra non-utilized ports without buying a switch or switches with higher bandwidth ports. For example, moving from 100Mbps switching to Gigabit Ethernet switches.



3 Physical Connections
1 Virtual Link



Network Redundancy- OSI LAYER 3

Network Layer Overview

It is growing more and more apparent that as EtherNet/IP networks expand, the use of a single IP subnet is not enough. In order to facilitate communication between IP Subnets, you need to use a Layer 3 network device, namely, a router. Routers can provide data movement in 2 ways: Statically via routes that are mapped by hand (Static Routing) or dynamically via designated routing protocols (Dynamic Routing).

Static routing can be useful for small routing areas, but does not provide fast failover because it requires user interaction to program and alternate route manually. Dynamic routing is required where a hand off failover is required or the routing environment is large. Routing protocols are inherently slower on failover than layer 2 protocols.

Routers support several types of protocols to communication like OSPF (Open Shortest Path First) and RIP (Routing Information Protocol) that have a communications redundancy built in as long as the physical network architecture remains in place.

There is also a router redundancy protocol that supports redundant router replacement. If one router fails, its designated backup is placed into service seamlessly as if the original never left. This is called VRRP, Virtual Router Redundancy Protocol.



Distance vector vs. Link State routing

Distance vector-

- ▶ Sends routing table info only to neighbors, so change communication may need one min/router
- ▶ Also called “routing by rumor”
- ▶ Easy to configure, but slow

Link state-

- ▶ Floods routing information about itself to all nodes, so changes are known immediately
- ▶ Efficient, but complex to configure

RIP Routing Protocol

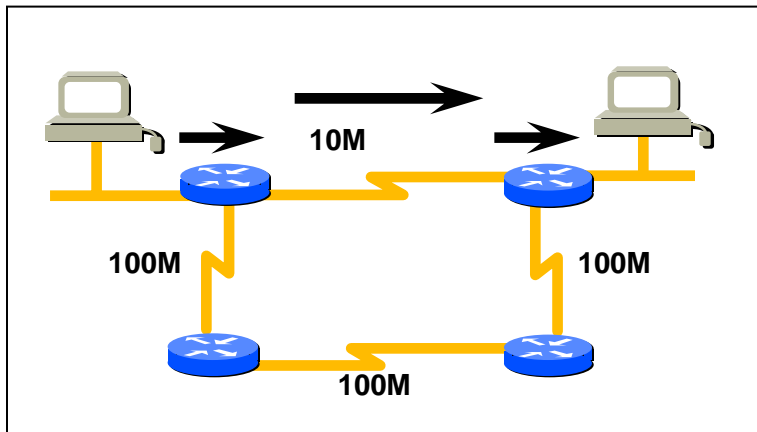
RIP and RIP II are types of Distance Vector protocols.

Distance vector algorithms compute distances from a node by finding paths to all adjacent nodes and by using the information these nodes have about continuing on the paths adjacent to them, router hop by router hop.

Distance vector algorithms can be computationally intensive, a problem that is alleviated somewhat by defining different routing levels. They rely upon the number of hops in a particular direction between the source router and destination router.

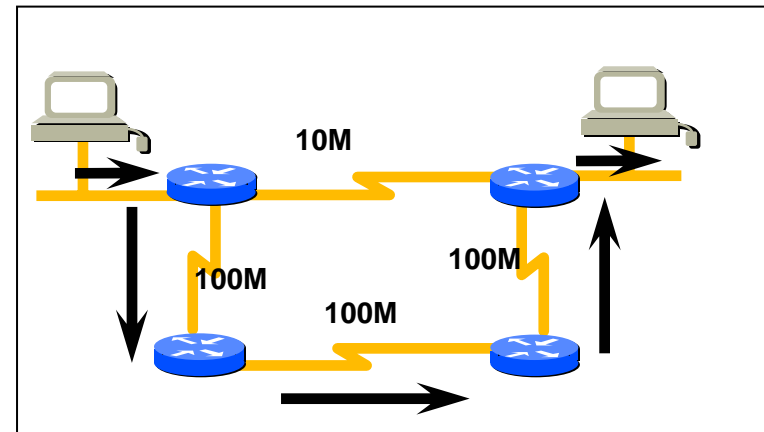
They do not take into consideration the speed of the physical media, so it is possible to move traffic across a suboptimal link

RIP Example



RIP

Industry standard that selects the path with the fewest hops



RIP II

RIP II has the ability to select the faster path (using load, distance, etc.)

OSPF Routing Protocol

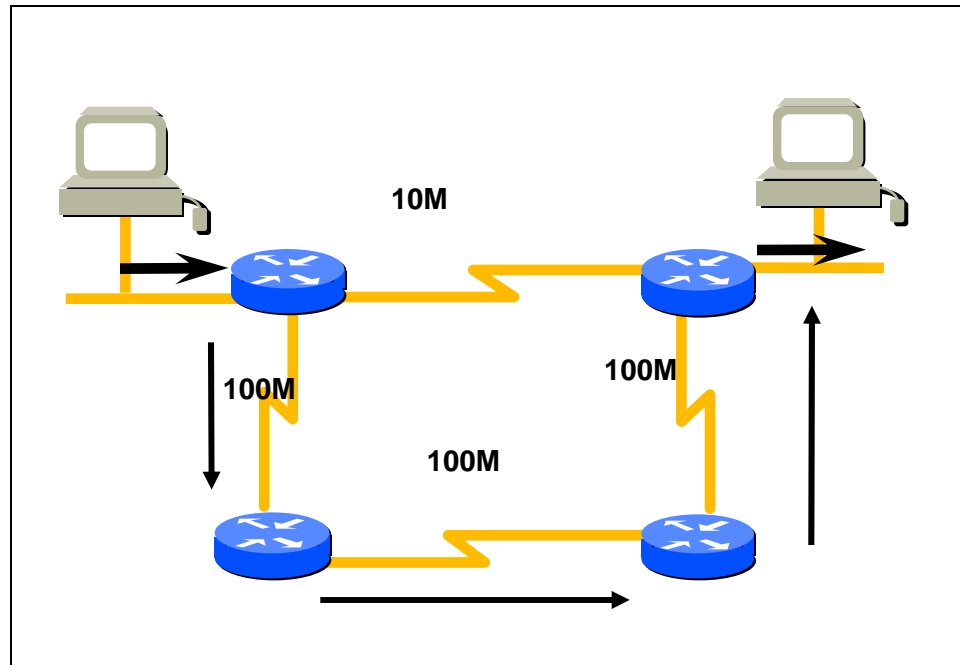
OSPF is referred to as a Link-State Routing protocol.

The best routes from router to router are based upon the A class of routing algorithms in which each router broadcasts connection information to all other routers on an internetwork. This saves the routers from checking for available routes but adds the memory requirement of storing all the routing information.

This algorithm relies upon the cost of the links between routers, not the number of hops. The cheaper the cost on a connection indicates a higher bandwidth capability.

OSPF keeps in memory ALL of the possible routes, not just the active routes.

OSPF Example



OSPF

Industry standard that selects the path with the lowest cost



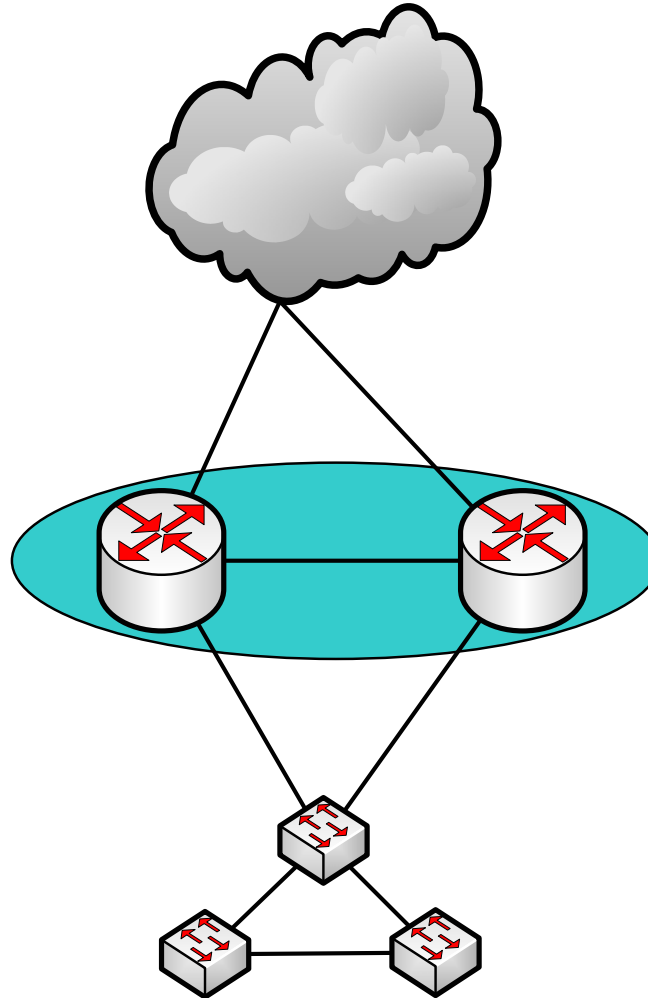
Virtual Router Redundancy Protocol

Router Redundancy-

VRRP is the way for routers to perform physical redundancy to each other.

If one router dies or is unable to function in the appropriate manner, its designated backup will take over the former routers function. They maintain this relationship through the use of HELLO packets and regular updates to make sure that both routers have all the same information. The use of VRRP would be a function to incorporate into an EtherNet/IP design if there is a requirement to attach to a corporate network and there is a requirement to maintain some sort of segregation between the plant floor EtherNet/IP network and the corporate environment.

VRRP Example





Determining the Cost of Redundancy



Using Appropriate Hardware

Based upon years of observations regarding Ethernet networks and the types of devices purchased to make them (namely buying unmanaged switches instead of Managed), it is very typical to actually see the cost differential between managed and unmanaged Ethernet switches exceeded by the lost revenue of an extended downtime event caused by a network outage. The ability to be able to monitor a network and see the application in action can help predict events that can cause outages. An unmanaged switch is in effect a “Blind” switch. It is not possible to see how the network is performing and perform predictive maintenance based upon what you can “see”. Also, the ability to use port mirroring on a managed switch can assist with troubleshooting Application Level issues as you can use a protocol analyzer to see the EtherNet/IP application in operation

Questions to Ask Yourself

- ▶ Is this a new install or and upgrade to a previous installation?
- ▶ Is there any existing cable that can be reused?
- ▶ Is there any existing equipment that can be reused?
- ▶ Has the area of the Installation been determined?
- ▶ Copper or Fiber Optics? This is dependent upon distance and the environment for the installation.
- ▶ Who is the Control System vendor?
- ▶ Will there be a point of connection to the existing plant network? What sort of data is intended to be passed to this network from the plant floor?
- ▶ To what extent has redundancy been considered? Is the network a ring or mesh based network?
- ▶ If Ethernet Network redundancy is not being considered, is it economically feasible to do without it? How many outages are you prepared to pay for in lost revenue? Balance this against the cost of managed vs. unmanaged switches or more advanced Ethernet networking devices like routers.
- ▶ How experienced are the plant controls support people in regards to Ethernet networking and will the IT staff being involved in the support?
- ▶ What is the projected budget for the control system, including the network cabling and equipment?



Questions?