

Control Network Elements & Network Management

- Control Network Elements
- Control Network System Requirements

Control Network Elements

Global View of Control Network

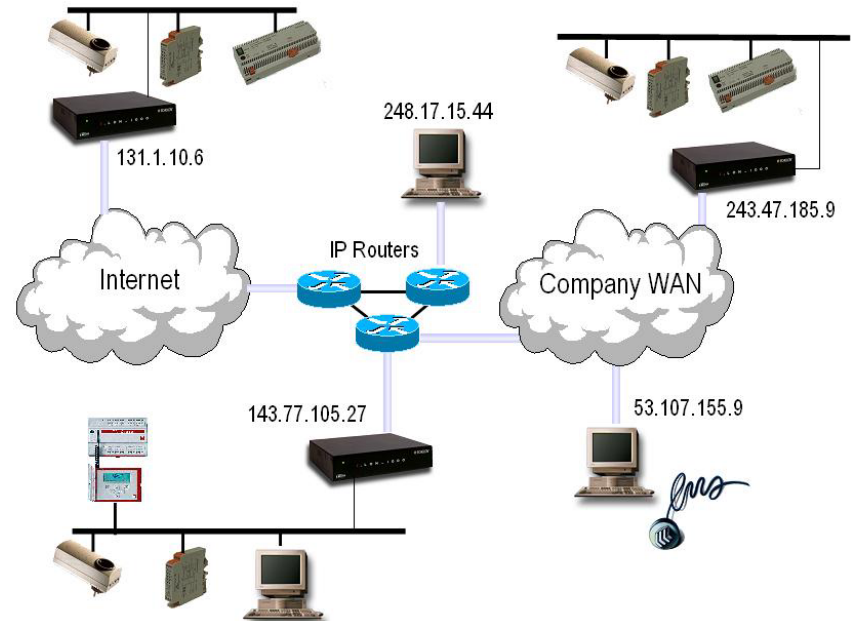
- nodes (sensors, controllers, actuators), channel(s), transceiver(s)
- control networks may also include repeater, bridge, switch, router, hubs, and gateway

Repeater

- Repeaters operate on OSI layer 1
- Physically isolate network segments
- Compensate transmission loss
- Help fan out of the transceiver bus driver if beyond its limit
- Does not check for valid packets

Bridge

- operate on OSI layer 2
- decoupling of network segments for the purpose of
 - load sharing; error limiting.
 - take care of security aspects.



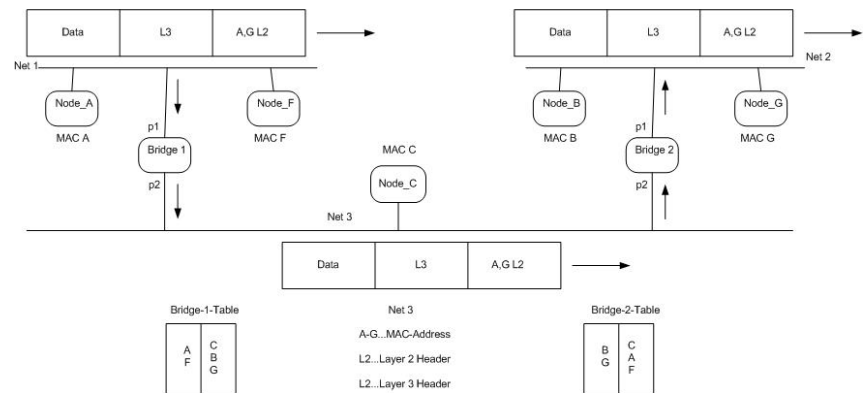
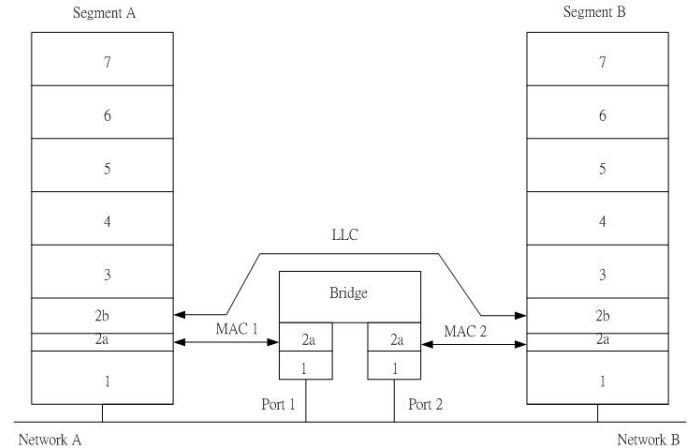
Control Network Elements

- connect network segments using different layer 2 protocols w.r.t. their media access procedure.
- Perform repeater functions like separating network segments physically

bridges hold forwarding tables that have forwarding flags assigned for the MAC-address of the destination nodes

the size of these tables is directly proportional to the amount of nodes in the logical network

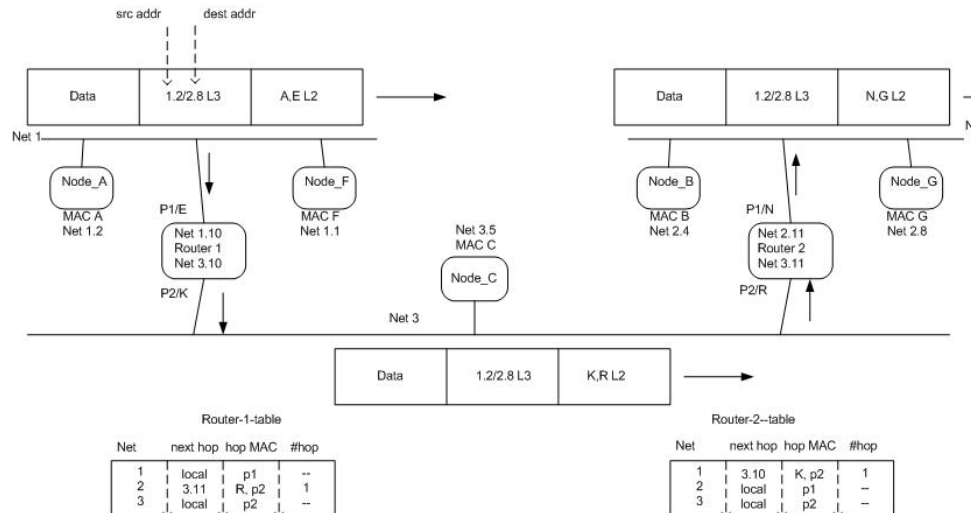
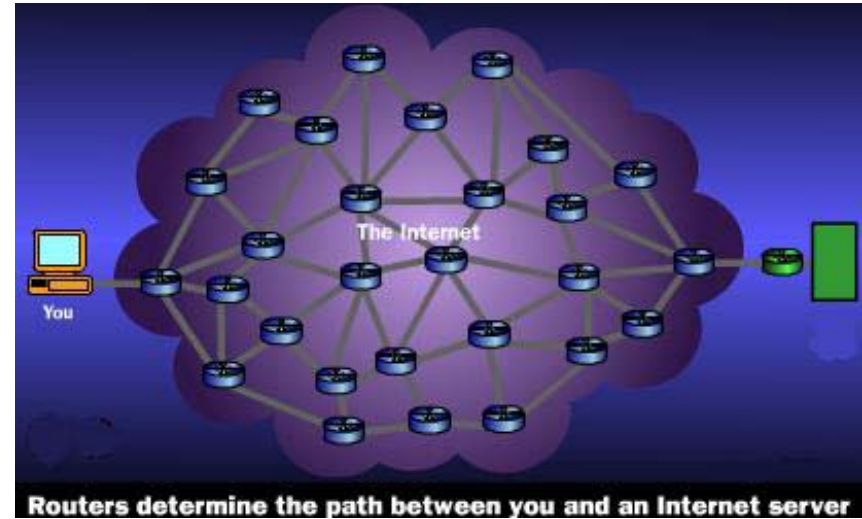
Study: Can you figure out how the forwarding table works as displayed in the right bottom figure?



Control Network Elements

Router

- 📄 Use addresses and protocols based on layer 3
- 📄 Layer 3 addresses are unlike MAC-addresses logical addresses and thus hardware independent
- 📄 Router support structure a network into subnets
- 📄 Assign nodes to a subnet
- 📄 Layer 3 addresses need to be assigned in addition to the MAC-address on each node
- 📄 A router connects adjacent subnets and knows the shortest path to other subnets
- 📄 routers manage only forwarding tables for layer 3 addresses containing forwarding flags for each noticed subnet



Control Network Elements

📁 Routers need to have the following knowledge about:

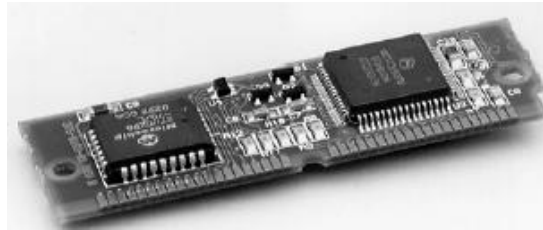
- 📄 the MAC-address of all nodes within the subnet where also one router port belongs.
- 📄 The routes to several destination nodes by knowing the necessary routers.

📁 The requirements for routers are:

- 📄 The transport system needs to have layer 3 functionality (logical layer 3 addresses, protocols support routing, etc..) implemented between two end systems.
- 📄 End systems need to be informed about the location of their belonging router.
- 📄 End systems need to change their layer 3 addresses if they change their locations (subnets).
- 📄 Routers need to exchange information about the network topology by routing protocols in order to keep their routing tables consistent.

📁 Example control network router: Echelon's LonWorks Router

- 📄 can be configured as repeater, bridge or router.



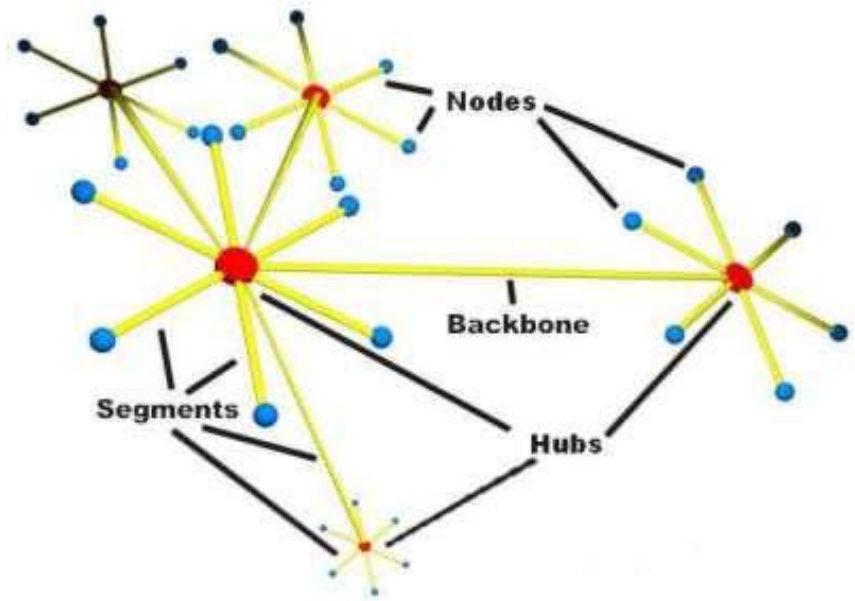
Control Network Elements

Gateway (with respect to control networks)

- In general, gateways operate on top of OSI layer 7
- Serve to connect different communication systems
- The expense in the gateway's application can be very high
 - Depend on degree of difference between application layer interfaces
- Application intensive gateway, called *application gateway*
 - essential disadvantage of an application gateway is the creation of the gateway software itself
 - For every project to be realized, a specific application needs to be created or at least needs to be adapted

Hubs

- One method to build up a bigger network with many nodes: Star-Bus topology



Nodes in particular areas are connected to hubs or switches (creating stars)
Hubs or switches are connected together along the network backbone (like a bus network)

Control Network Elements

Hub takes the signal from each node and sends it to all of the other nodes connected

- Hubs come in several sizes, noted by the number of ports available
- Stackable hub has a special port that can connect it to another hub
 - increase the capacity of the network

As a network grows, there are some potential problems with hubs type configuration, including:

Scalability

- limited shared bandwidth makes it difficult to accommodate significant growth without sacrificing performance

Latency

- This is the amount of time that it takes a packet to get to its destination.
- Latency can increase significantly as you add more nodes
 - not suitable for alarming systems*

Network failure

- one device on a hub can cause problems for other devices attached to the hub due to incorrect speed settings (100 Mbps on a 10-Mbps hub) or excessive broadcasts

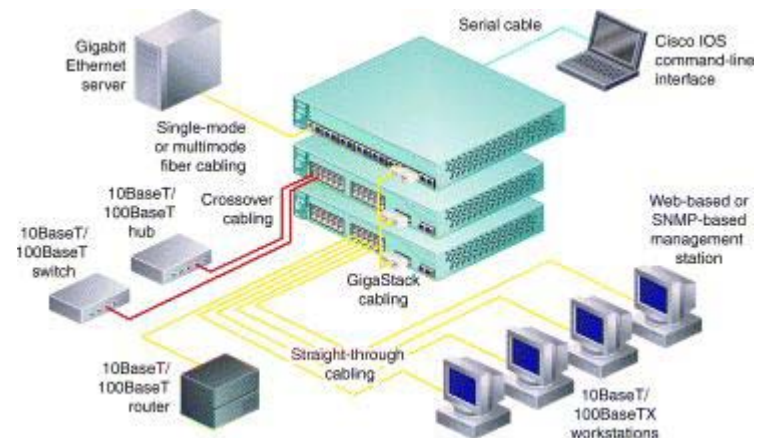
Collisions

- A network with a large number of nodes on the same segment will often have a lot of collisions

Control Network Elements








Switches

- 📄 A switch is like a cloverleaf intersection
 - 📄 each car can take an exit ramp to get to its destination without having to stop and wait for other traffic to go by.
- 📄 A device connected to a switch port has the full bandwidth all to itself.
- 📄 In a fully switched network, switches replace all the hubs of an Ethernet network with a dedicated segment for every node
- 📄 This allows many conversations to occur simultaneously on a switched network
- 📄 Switching allows a network to maintain full-duplex Ethernet



Control Network Elements

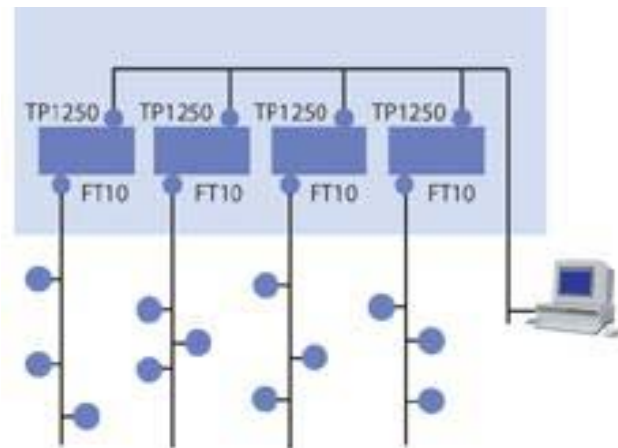
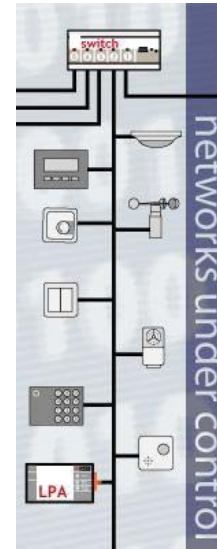
Wondering what makes a switch different from a router?

-  Switches usually work at Layer 2 using MAC addresses
-  Routers work at Layer 3 with Layer 3 addresses (e.g. IP, IPX or Appletalk, depending on which Layer 3 protocols are being used)
-  The algorithms that switches use to decide how to forward packets is different from the algorithms used by routers to forward packets.
 -  One of these differences in the algorithms between switches and routers is how broadcasts are handled
 -  Broadcasts are used any time a device needs to make an announcement to the rest of the network or is unsure of who the recipient of the information should be.
 -  A hub or a switch will pass along any broadcast packets they receive to all the other segments in the broadcast domain.
 -  Without the specific address of another device, Router will not let the data packet through. This is a good thing for keeping networks separate from each other.

Control Network Elements

Application example using Lonworks switch in a control network

- Directly connect 4 FT-10 channels to the high speed TP-1250 backbone
- TP-1250 backbone channel can be used to connect multiple switches
- Normally, it works more like a router than a switch.



Control Network System Requirement













- 📁 **In order to understand and design a better control network, we have to identify the network requirement.**
- 📁 **Network requirements in general can be broken down as follows:**
 - 📄 Scalability & flexibility
 - 📄 Reliability
 - 📄 Architecture
 - 📄 Performance
 - 📄 Network Management
 - 📄 Interoperability

Scalability & flexibility

- ✉ **The size of a network according to their applications is usually designed to be scalable.**
- ✉ **As the sensors/actuators become more complex, not only the number of devices but also the distance and topology need to be modified.**
- ✉ **The size of the network dictates the networks address space**
- ✉ **Regarding to these, some special considerations for a control network:**
 - 📄 How many nodes in total can be supported or what is the address space?
 - 📄 Does it support logical segmentations?
 - 📄 Which network topology is the best for a scalable network?
 - 📄 How does it easily extend the distance?
 - 📄 How does it easily achieve the network scalability?
 - 📄 How does it easily add or remove devices?
- ✉ **The network protocol often has limitations of the total number of nodes on the network and the number of nodes on each channel or each subsystem.**
- ✉ **The expansion of a network is mainly through the segmentation.**



Scalability & flexibility

Take Lonworks technology as an example:



-  Supported by LonTalk protocol, Neuron chip and Lonworks transceivers
-  It provides a scalable free topology network using the free topology transceiver
-  It provides a flat architecture that supports the address requirements of the entire network but allows logical segmentation
-  It support domain, subnet, allowing the logical segmentation through network level routers
-  summary of boundaries:
 -  Number of domains: 248
 -  Number of subnets per domain: 255
 -  Number of nodes per subnet: 127
 -  i.e. a total of 32,385 nodes per domain, and a total of 32K x 2⁴⁸ devices in system.
-  It supports both network variable (NV) and explicit message for network communication
 -  The NV supports an average of 31 bytes of data packet and the max. explicit message size is 228 bytes of data.
-  Adding and removing devices are achieved by using a Lonworks Network Services (LNS) based network management tools

Reliability






The network reliability mainly focuses on the following issues:

-  Reliable message transfer and control loop closure.
-  Fault tolerance, fault isolation and recovery.

Due to the vast applications, a network protocol needs to support a number of message services

-  e.g. unacknowledged, acknowledged, request/response messages services.
-  For each type of message service, it has its mechanism to support the reliability.

Using Lonworks technology as an example, it provides the following services to enhance the protocol services:

-  It supports unacknowledged message service with repeat.
-  It supports unicast and multicast message services, with acknowledgement from each addressed node.
-  Request/response service to ensure that loop has been closed
-  16-bit CRC checking for error detection
-  Sender authentication to ensure authorized messages

Reliability

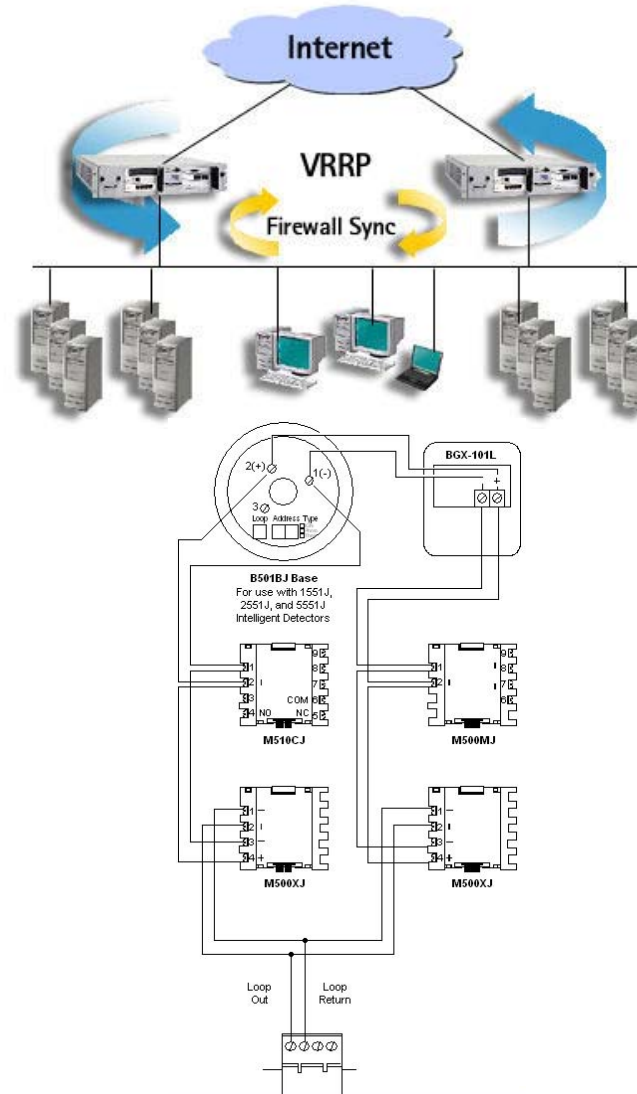
Folder Fault tolerance can be achieved through

- Redundancy by using duplicated nodes, duplicated connections/paths, or duplicated networks.
- An example is using VRRP.

VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network. Although there are other alternatives, the most common arrangement is to specify one router to serve as the router for forwarding packets from a group of hosts on a LAN. If that router fails, however, there is no way to use another router as a backup. Using VRRP, a *virtual IP address* can be specified manually or with Dynamic Host Configuration Protocol (DHCP) as a default. A virtual IP address is shared among the routers, with one designated as the master router and the others as backups. In case, the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router.)





- Loops are used to allow communications despite a break at one location. (e.g. In Fire circuit)

need to have considerable sophistication in transceiver design






Architecture

A distributed peer-to-peer architecture

-  uses much less bandwidth
-  minimizes the network traffic
-  eliminates the host bottleneck
-  increases the network reliability

A distributed peer-to-peer network works better than a traditional hierarchical network as long as:

-  the address space allows it
-  there are provisions for logical portioning of the network through addressing and traffic filtering
-  the computing power, communication speed and data field sizes for each node are scalable to handle a variety of control tasks.


Using LonWorks as example:

-  It is because of its distributed intelligent, the network reliability and throughput are improved.



Performance

A network's performance depends on the various aspect of the network design






Network architecture

-  A peer-to-peer network architecture allows communication directly across the control loop

Maximum packet size

-  It determines the number of packets and time to complete a transaction
-  Average data field size of a packet from simple sensors to complex actuators is around 4-50 bytes, and considerably more for configuration and calibration data.
 - Note: The average size of Lonworks NV is 31 bytes, while for explicit message is 228 bytes max

Throughput

-  throughput is the amount of data packet that a node/device can transfer in a given time period.
-  e.g. TP-1250 has a max. throughput of *835 packets max. per second*, FT-10 has a max. throughput of *168 packets*
-  As size of control network is ever increasing, for the above example, the TP-1250 backbone bandwidth would be easily get exhausted
-  Come the rescue: IP has excellent characteristics for use as a control network backbone
-  By tunneling ANSI 709.1 on top of an IP infrastructure, the benefits of IP are realized without having to sacrifice the functionality and robustness of LonTalk

Performance

- Estimated throughput of over 50,000 packets per second, a dedicated 100 Mbit LonTalk/IP channel increases the LonTalk backbone capacity by about 60 times.
- Latency issues must be carefully considered when designing a control network that spans an IP network.

Delays through routers and gateways

- If the network layer of a protocol does not contain provisions for network level routing, routers connecting sub-networks have to be implemented at the application layer
- Such an implementation has impact on the application processing power, application code space and ability.

Monitoring control-event driven update

- Sensors need to be polled or scanned at a fixed time interval
- Loops need to be close as fast as they can
- Such a fixed interval scanning is not optimal
- To optimize the network performance, event-driven update is more desirable. It requires
 - an event-driven scheduler at the originating device
 - peer-to-peer access to the network
 - a receiving node that has the communication and computing resources to process information on demand

Network Management

✧ **Network management should include**

- ✧ network installation (integration), commissioning, maintenance, monitoring, controlling and diagnostics.

✧ **Users need a network that can accommodate any number of HMIs, SCADA, and data logging stations, plus the ability to exchange data among different control subsystems and crossing the system boundaries if necessary.**

✧ **End users also need a control network that is easy to expand and reconfigure.**

- ✧ the system should have enough built-in intelligence to automatically update each of the system-level monitoring stations to reflect the changes

✧ **Software commissioning task for a network may consist of loading each intelligent device with**

- ✧ its network configuration (e.g. address and a list of devices with which it shares data)

- ✧ Its application configuration (e.g. setpoint, high/low limit)

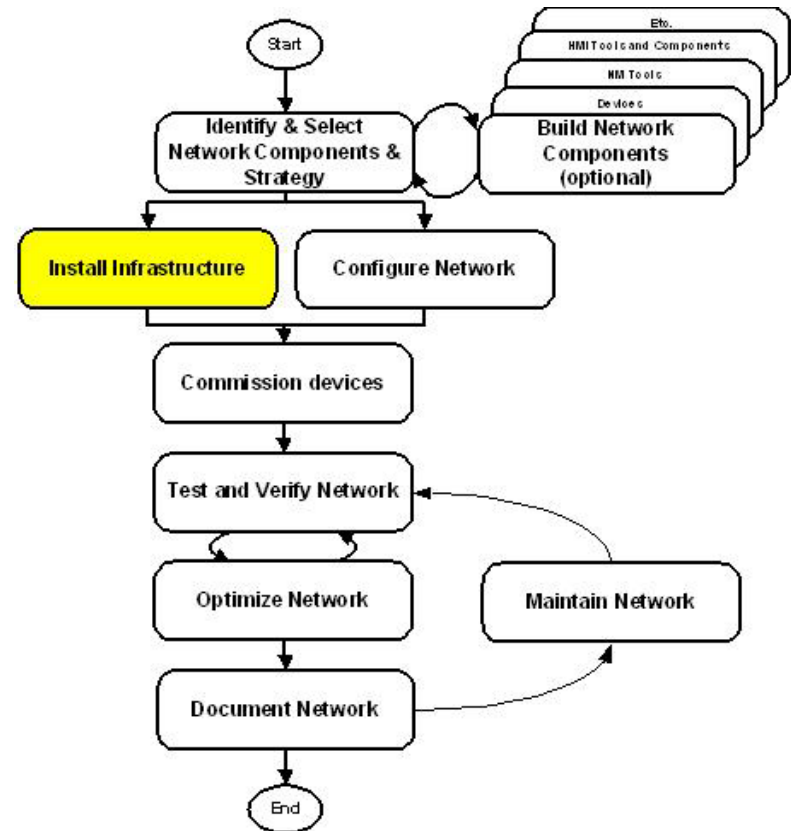
Network Management

Network tools must let multiple installers (or maintenance peoples) work on the system at the same time, without conflict.

A good network management software should

- reduce commissioning time and cost
- great access to data (since the client tools do not need to contain a network database, they can be anything from PC, PDA or simple LCD display).
- simplified systems integration
- increase system up time (as multiple maintenance & repair works can be done simultaneously).





Example Network Management Tool - LonMaker For Windows






Network Management

Use of Network Management Tool in




Identifying & selecting components

-  Describing the project
-  Identifying network architecture
-  Identifying installation and maintenance scenarios
-  Identifying components




Installing the physical network

-  Installing cabling
-  Installing infrastructure devices
-  Installing application devices

Programming the network





-  Acquiring the external interface
-  Configuring devices and objects
-  Binding network variables

Applying the program to the physical network (commissioning)




-  Acquiring the Neuron ID
-  Commissioning routers
-  Commissioning devices and propagating the program

Network Management





Testing & verifying the network

-  *Verifying application devices' health*
-  *Verifying network communications*
-  *Verifying infrastructure devices*
-  *Verifying cabling and termination*





Optimizing or fine-tuning the network

-  *Identifying possible changes*
-  *Modifying infrastructure*
-  *Optimizing connection properties*

Maintaining the network

-  *Replacing application devices*
-  *Updating application devices*
-  *Moving the network tool*
-  *Maintaining the LNS server*

Documenting the network

-  *Creating an operating manual or user's guide*
-  *Documenting network physics and network design & program*
-  *Documenting device health*
-  *Documenting channel and network health*