USING BRIDGES, ROUTERS AND GATEWAYS IN DATA ACQUISITION NETWORKS

Tom De Selms
JDANS Lead Engineer
Veridian Engineering
thomas.deselms@veridian.com

ABSTRACT

Using acquisition networks requires an understanding of the capabilities, design constraints and limitations of each available network device. The proper use of bridges, routers and gateways become extremely important in large networks where dissimilar busses, protocols or applications may be found. As data acquisition networks become a reality, the instrumentation network engineer must understand the benefits of each of these network devices and when to use them.

KEY WORDS

Data Acquisition, Networks, Bridges, Routers, Gateways

INTRODUCTION

The use of bridges, routers and gateways in commercial networks is determined by the size of the network, the protocols and applications, the capabilities needed and problem being solved. To understand which network device to use in a data acquisition network, the instrumentation network engineer must first understand the Open Systems Interconnection (OSI) 7-layer model. The use of the OSI 7-layer model helps determine the architecture of the network, how the network devices will be used, the scaling capabilities of the network and its overall interoperability. Using the OSI 7-layer model (or similar model) and the proper network devices will affect how the data is transported and processed. Understanding some of history of the development of these network devices helps the instrumentation network engineer specify the correct network devices. A comparison of the advantages and disadvantages of bridges, routers and gateways gives the instrumentation network engineer a sense for the differences between these devices. These choices will also affect performance areas such as latency, throughput, timing, network system capabilities, cost of the data acquisition network and the ability to adapt to changing requirements.

NETWORK MODELS AND ARCHITECTURES

One of the main differences between bridges, routers and gateways is which layer they operate in the OSI 7-layer model. The OSI 7-layer model separates a network into distinct layers in which the network devices operate. Each layer provides a service to the layer above and below. This layering should be viewed as a useful framework for discussions and design constraints. When deciding which layers to implement and the level of interoperability required, the layers can be joined or split to create a model for specific situations. Each layer is responsible for providing a service to the layer above by using the services of the layer below. Protocols establish rules for communication between layers. The actual communication between layers using the rules of protocols is known as an interface. The Internet community has combined the bottom two layers and the top three layers to create a four-layer model. This Internet model (shown in Figure 1) is the most widely used of the networking model architectures.

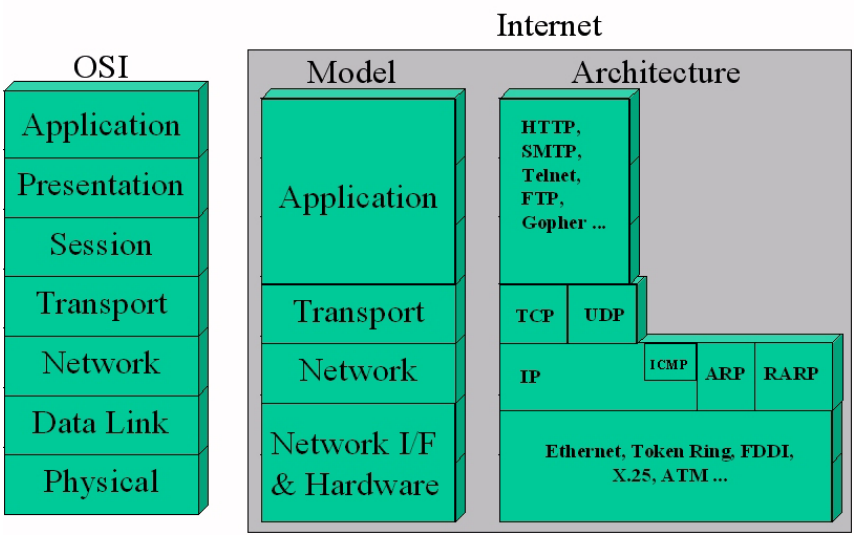

Figure 1 OSI and Internet Models

HISTORY OF BRIDGES, ROUTERS AND GATEWAYS

What is a Bridge? What is a Router? What is a Gateway? Without knowing the answer to these three questions it is difficult to make an intelligent comparison. The International Standards Organization (ISO), which defines Internet standards, does not make the distinction very clear. A bridge is defined as a data link device, a router as a network layer device and a gateway as an application device. Sometimes bridges perform functions a router is supposed to do, sometimes a router performs bridging functions and sometimes gateways perform both functions and more. There is even a Brouter that performs bridging on some protocols and routing on other protocols!

To understand the evolution of bridges and routers during the network revolution gives a better understanding of the thinking behind their development. The history of Ethernet gives an example of the evolution of bridges. Ethernet was originally designed as a bus technology. This topology required routing of the cable throughout the building or office. A more convenient strategy was to use a star topology and to use ordinary telephone cable. The center of the network was called a hub;

it connected the segments together by acting as a repeater. Although the hub acted as a single point of failure, it is less likely to fail than a bus because it normally sits in a closet while a bus, with it's many connections has several potential points of failure. A hub, therefore, is a multiport data link layer repeater. The hub simply transmits every packet it receives to every other port of the hub. If two stations transmitted at the same time a collision would occur just as in the bus topology. The vendors then added "smarts" to the hub so that the hub can make decisions on where to send the packet. This "smarts" in the hub includes the ability to store and forward a packet, it can then make decisions on which port to send the packet and the hub learns where the destinations are and acts to send the packet on those particular ports. Collisions do not happen on these "smart" hubs, because the minimum packet sizes and maximum distances do not apply. The ports on the "smart" hub can be different speeds (10Mbs and 100Mbs). Since the packet is stored and forwarded, the two ports can negotiate the speeds on each port. When two "smart" hubs are connected together, multiple collisions can occur and loops can be created (See Figure 2). Because collisions and loops cause decreased speed and long convergent times, the spanning tree algorithm was applied to enable "smart" hubs to learn the network topology to prevent loops. With the addition of the spanning tree algorithm the "smart" hub became a bridge. The spanning tree algorithm allows bridges to dynamically discover a portion of the network that is loop-free (a tree) and yet has enough connectivity so that where possible, there is a path between every pair of LANs (the tree is spanning).

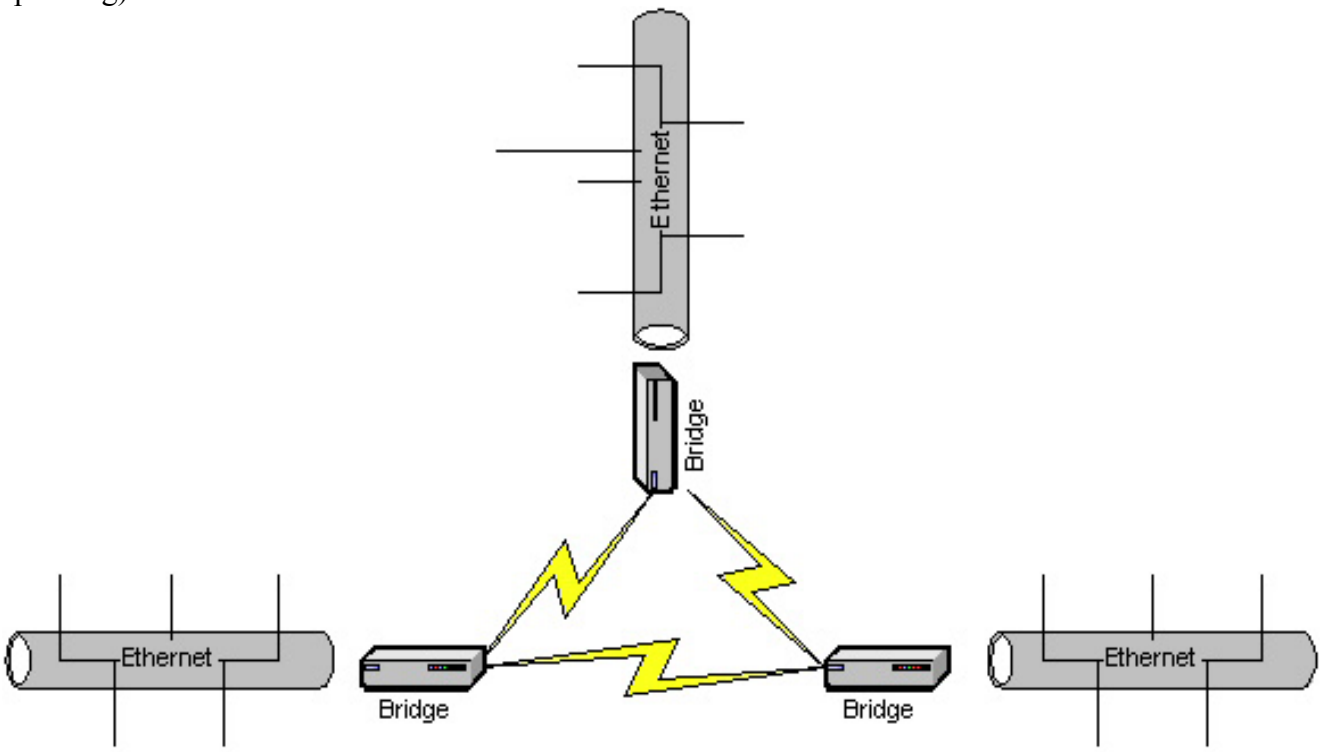

Figure 2 Bridges with Possible Loops

BRIDGES, ROUTERS AND GATEWAYS

As previously stated, bridges operate at the data link layer, they forward packets between physically separate LANs. They listen to the traffic on two separate networks and learn the nodes on each LAN. The reason for this is to leave local traffic on a local LAN and to forward traffic if on an adjacent LAN.

In contrast, routers operate at the network layer, they forward packets based on their IP address so they keep a routing table that is used to make routing decisions. A router can use routing protocols to make decisions on the best route to take from one location to another. A router can have multiple ports in which different modules can be inserted for the particular network being used. A router can provide isolation in a network so that if a failure or misconfiguration happens on one area of a network, the whole network will not crash. Consequently a router can route from one networking technology to another.

A gateway acts as a translator between two systems or devices that do not use the same communication protocols, data formatting structures, languages and/or architecture. Unlike a bridge, which simply passes information between two systems without conversion, a gateway repackages information or changes its syntax to match the destination system. Most gateways operate at the application level relative to the OSI 7-layer model. An example of a gateway is an electronic mail gateway, which translates from one vendor's messaging application to another's so that users with different e-mail applications can share messages over the network. A typical email gateway converts messages from a proprietary message format to the industry standard X.400 format.

COMPARISON OF BRIDGES, ROUTERS AND GATEWAYS

The following lists specify some of the advantages and disadvantages of bridges, routers and gateways. These lists are summarized in Table 1. Some disadvantages of bridges, routers and gateways are discussed in these sets of bullets:

- Bridges can use only a subset of the topology (spanning tree). However, routers can use the best path that physically exists between source and destination. Bridges are transparent. They do not modify the packet in any way. A packet transmitted by a bridge cannot be distinguished from a packet transmitted by a node. Packets can proliferate (creating a loop) with bridges when a bridge forwards the packet onto several LANs, and several bridges pick up the packet when it is transmitted onto a LAN.

- Bridge reconfiguration after a topological change is an order of magnitude slower than router reconfiguration after a topological change. This stems from the transparency constraint that makes bridge loops much harder to prevent than router loops. The data link layer header has no hop count to kill off packets in an infinite loop, and the packets can spawn many copies; bridges might forward a packet onto multiple ports, and multiple bridges might pick up a packet transmitted on a shared medium. In contrast, loops are not a disaster with routers, so routers can switch over to new paths as soon as information is received.

- Bridges offer no firewall protection against broadcast storms. Bridges cause multiple LANs to appear as if they are one LAN to the upper layer protocols. When LANs are bridged they become a single LAN from the point of view of the upper layer protocols. Therefore, broadcast storms disable the entire bridged set of LANs. As a result, it is common to limit the size of the LAN and instead break a large topology into smaller IP subnets. The IP subnets must be interconnected through the network layer rather than the data link layer.

- Bridges must drop packets that are too large to forward. Network layer headers contain fragmentation and reassembly information. The data link layer header does not. Therefore, bridges must drop a packet that is too large to forward. Also bridges cannot send an error message back to the source to let it know the packet was dropped because no such packet is defined in the data link layer header.

- Bridges cannot give congestion feedback to the nodes. The network layer protocols have mechanisms such as congestion-experienced flags and source quench messages. The data link layer has no similar mechanism.

Some of the advantages of bridges, routers and gateways are discussed in this set of bullets:

- Bridges are really plug and play. Routers require much more configuration. Although some network layer protocols (Appletalk) are close to being plug and plug and IP is improving, bridges are still much easier to deal with.

- Bridges have a better price to performance ratio than routers. The reason is that routers must parse a network layer header, which is more difficult to parse than a data link header. Routers are getting better but bridges are still faster and cheaper.

- Bridges forward even unroutable protocols. Some upper layer protocols are designed to run over the data link layer. Without a network layer only a bridge can interconnect LANs with respect to protocols. Brouters allow support to these protocols without requiring that other protocols be bridged.

- Bridges allow an IP node to move within the bridged portion of the topology without changing its IP address. So, even if all the nodes run IP, it is useful to build parts of an IP network out of bridges.

- Bridges can extend the length of an existing LAN.

- Routers forward a packet in only one direction and specify the router to which the packet is being forwarded. Therefore, a loop with routers will not cause packet proliferation.

	Advantages	Disadvantages
Gateway	• Allows complete translation from one app to another app	• Can add significant latency in processing
Router	• Uses best path between source and destination • Fast convergence after topology change • Loops will not cause packet proliferation • Allows subnets to segment a network • Provides feedback to nodes for congestion control	• Require configuration, not plug and play • Adds latency because works at network layer
Bridge	• Plug & Play • Better price to performance ratio • Allows IP node to move within topology • Extends the length of LAN • Forwards without parsing	• Uses only a subset of the topology • Slow during topology changes • No protection against broadcast storms • Drops packets that are too large • Cannot send error message back to node when drop packet • No mechanism for congestion control

Table 1 Advantages and Disadvantages of Bridges, Routers and Gateways

BRIDGES, ROUTERS AND GATEWAYS IN DATA ACQUISITION NETWORKS

The use of bridges, routers and gateways in data acquisition networks requires an understanding of the problem that is being solved. There are different situations where a bridge, router or gateway will meet the needed requirements and capabilities. As an example, a bridge could be a solution to extending a network to an area not normally instrumented, extending a LAN inside a large test vehicle, providing a bridge to a recorder or transmitter or using a bridge between a legacy system and a commercial technology. The use of a router could be used to segment a LAN inside a large test vehicle or to isolate different segments of a network. A gateway provides the use of a complete translation from one application to another. There are several programs currently experimenting/implementing data acquisition networking technologies for the T&E community. Each of these four programs uses networking technology and can be evaluated using the standard OSI 7-layer model. The first program uses bridge technology in the wireless areas. The second uses a combination of wireless, LAN technologies and a Gateway to move data on an aircraft power bus.

The third is a bridge from a legacy system to a commercial technology and the fourth program by NASA uses emerging standards for designing a distributed networking architecture.

The Two-Way Robust Acquisition of Data (2-RAD) program is a program, which uses COTS technology for moving data from the test vehicle to the ground using Wireless Local Areas Networks (WLAN) technologies. This is an example of the use of Ethernet technologies in which the relaying and collecting of data is done using a commercial wireless technology. The standards being used include 802.11A and B which provide relatively high data rates. This technology uses part of the data link layer (Media Access Control layer [MAC]) to transfer packets from a test vehicle to a relay or ground station. In this case, the PCM encoder is being replaced with a MAC layer encoder. The relay devices are acting as a bridge and the data collectors are using IP addresses (network layer) to reorder the data for processing.

The Common Event Network Test-Instrumentation System (CENTS) program uses RF and networking technologies for data acquisition. They use existing power busses on-board the test vehicle as the physical layer for the data acquisition LAN. The architecture model uses an application layer that accesses the MAC Layer for address management. This technology uses the data link layer to move data with the 802.3 CSMA/CD scheme and then encapsulates the 802.3 data format into the 802.11 wireless format. CENTS uses a master controller to provide for LAN control, setup, timing and network IO. The master controller acts as a Gateway. This Gateway function provides the conversion and data formatting for transport to another medium such as a recorder or telemetry.

Another example of a network device being used in data acquisition is the Fibre Channel Bridge to Legacy Instrumentation System. The objective of this program is to develop a commercial product that will perform the CAIS to Fibre Channel bridge function. This SBIR is demonstrating a CAIS to Fibre Channel bridging device that links legacy CAIS busses to a commercial Fibre Channel Bus. The bridge also outputs a standard PCM stream in addition to the Ethernet and Fibre Channel/Arbitrated Loop network. The bridge provides the networking capability by buffering a copy of the PCM output data in local memory, formatting the data into network packets and sending the data via the Fibre Channel and/or Ethernet interfaces. The development of a bridge from the CAIS bus to Fibre Channel Standard demonstrates the utility of moving PCM data to a commercial standard bus technology. This development allows set-up selection either using Ethernet or RS232. The bridge allows IP addresses to be configured from the bridge to the nodes on the network either on the Ethernet interface or the Fibre channel interface. The nodes on the network are configured as IP over Fibre Channel. This bridge uses Fibre Channel protocols for arbitrating on the loop, which is a network layer function (routing function) but the network layer has direct access to the data link layer (bridging function) as a layer between the software and the hardware.

Another networking project by NASA Dryden Flight Research Center is researching advanced network-based and distributed data acquisition tools and methodologies applicable to mobile aerospace environments. The Linux Data Acquisition and Distribution System (LDADS) is a small generic data acquisition node that will allow researchers to explore the feasibility of the Linux operating system and emerging interoperability tools such as Java and Extensible Markup Language (XML) as a platform for distributed control applications. LDADS envisions that in the near future test vehicles will be viewed as nodes collaborating on networks and is exploring the notion of a *real-*

time telemetry and measurement network. The evolution of the Linux operating system, Java programming language and XML has the potential for significant cost savings in aerospace and data acquisition environments. The LDADS project was identified as a systems-oriented, cost effective and leading edge approach for researching real-time measurement and telemetry network problems.

PERFORMANCE ISSUES WITH BRIDGES, ROUTERS AND GATEWAYS

When designing a data acquisition network, performance issues such as latency, timing and the performance of the nodes become critical. The OSI 7-layer model helps to determine where to concentrate to meet the design requirements. When specifying whether to use a bridge or a router it is imperative to look at the protocols being run on the different layers. For example, with only a small number of neighboring nodes on a network, some protocols are encapsulated in the IP header. These routing protocols need not be forwarded by IP, because there is no reason to have an IP header. The IP header makes the message linger and care must be taken to ensure packets don't get routed because this could confuse distant routers into thinking they are neighbors. The alternative to carrying messages in an IO header is to acquire a data link layer protocol type. Because the network layer headers are wasted bits for messages that are neighbor to neighbor why would an engineer choose to run such protocols over the network layer.

1. There may be an API for running over the network layer, so that the application can be built as a user process-whereas that might not be an API for running over the data link layer. Therefore running over the data link layer would require modification to the kernel.
2. It may be bureaucratically difficult to obtain a data link layer-protocol type.
3. In the case of IPv4, it lets you do fragmentation without devising some other mechanism.

If the network design has requirements for a small number of nodes, the test vehicle is small and has the requirement for fast transfer of data, then a bridge will be sufficient. If there is a small area in a test vehicle that needs connectivity to a larger network then also a bridge may work in this situation. If the network design encompasses a large area that need to be separated and isolated from each other, then a router should be used. When using a bridge in a data acquisition network there are special requirements put on the bridge. A bridge must be engineered to have sufficient CPU power. If the bridge's CPU becomes a bottleneck, the bridge will start throwing away packets before it even looks at them. In this situation, there is no way for the bridge to avoid throwing away configuration messages because it can't distinguish a configuration message from a data message without looking at it. Another requirement is that a bridge be able to transmit a configuration message no matter how congested the LAN. All LANs enforce fairness, allowing each station at least a minimal amount of bandwidth. Therefore, no matter how congested the LAN, the bridge will be able to transit a packet eventually. Because it is critical that configuration messages get sent in a timely fashion, a bridge should be engineered so that a configuration message can be put at the front of a queue. In practice underpowered bridges are a problem. A temporary congestion situation causes lost configuration messages, which, in turn, causes loops. Then the congestion resulting from looping and proliferating data packets makes the situation worse.

It is desirable to use a protocol with as little dependence on other layers so that in the future one layer can be replaced without affecting the others. An example of this is to have protocols above the network layer make the assumption that addresses are 4 bytes long. The downside of the principle is that if you do not exploit the special capabilities of a particular technology at one layer, you wind up with the least common denominator. For example, not all data links provide multicast capability but it is useful for routing algorithms to use data link level multicast for neighbor discovery, efficient propagation of information to all LAN neighbors and so on. If this principle of not making special assumptions about the data link layer is followed too strictly, we might not have allowed the network layer to exploit the multicast capabilities of some data link layer technologies.

CONCLUSION

The difference between bridges, routers and gateways begins with the OSI 7-layer model. Knowing what layer the network devices operate at helps to understand why they were designed for that layer and for what purpose. It is critical when designing a network to agree on a model and architecture, otherwise there is a risk that network designs will fill narrowly defined objectives. To begin to understand the differences between network devices it helps to understand some of the history behind their evolution. This evolution from hubs to bridges to switches and routers also follows the evolution of networking technology. The development of the spanning tree algorithm allowed a loop free network and also allows connectivity between every pair of LANs. The use of routers has been described and the advantages and disadvantages of the various network devices.

Four different networking projects have been briefly described that use networking technology for the T&E community. The description of these projects was to illustrate the use of network devices in these projects. The last topic discussed is some of performance issues to be aware of with designing or implementing a data acquisition network.

REFERENCES

Tanenbaum Andrew, Computer Networks, 3rd Edition, Prentice-Hall, Inc., Upper Saddle River, New Jersey, 1996

Stallings, William, High-speed networks: TCP/IP and ATM design principles, Prentice-Hall, Inc., Upper Saddle River, New Jersey, 1998

Perlman Radia, Interconnections: Bridges, Routers, Switches and Internetworking, 2nd Edition, Addison Wesley, Reading, Massachusetts, 2000

Thomas Stephen, IP Switching and Routing Essentials, John Wiley and Sons, Inc., New York, New York, 2002